Network Architectures
and Services
NET 2013-08-1

FI & IITM
WS 13/14

Proceedings of the Seminars
Future Internet (FI) and
Innovative Internet Technologies and Mobile Communications (IITM)

Winter Semester 2013/2014

Munich, Germany, 17.10.2013-16.02.2014

Editors

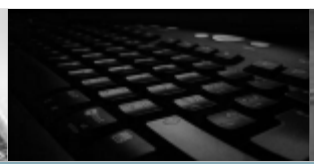
Georg Carle, Daniel Raumer, Lukas Schwaighofer

Organisation

Chair for Network Architectures and Services
Department of Computer Science, Technische Universität München

Technische Universität München





Network Architectures
and Servies
NET 2014-03-1

FI & IITM
WS 13/14

Proceeding zum Seminar Future Internet (FI) und Innovative Internet Technologien und Mobilkommunikation (IITM)

Wintersemester 2013/2014

München, 17. 10. 2013 - 16. 02. 2014

Editoren: Georg Carle, Daniel Raumer, Lukas Schwaighofer

Organisiert durch den Lehrstuhl Netzarchitekturen und Netzdienste (I8),
Fakultät für Informatik, Technische Universität München

Technische Universität München

Proceedings of the Seminars
Future Internet (FI), and Innovative Internet Technologies and Mobile Communication Networks (IITM)
Winter Semester 2013/2014

Editors:

Georg Carle
Lehrstuhl Netzarchitekturen und Netzdienste (I8)
Technische Universität München
D-85748 Garching b. München, Germany
E-mail: carle@net.in.tum.de
Internet: `http://www.net.in.tum.de/~carle/`

Daniel Raumer
Lehrstuhl Netzarchitekturen und Netzdienste (I8)
E-mail: raumer@net.in.tum.de
Internet: `http://www.net.in.tum.de/~raumer/`

Lukas Schwaighofer
Lehrstuhl Netzarchitekturen und Netzdienste (I8)
E-mail: schwaighofer@net.in.tum.de
Internet: `http://www.net.in.tum.de/~schwaighofer/`

Cataloging-in-Publication Data

Seminars FI & IITM WS13/14
Proceedings zu den Seminaren „Future Internet“ (FI) und „Innovative Internettechnologien und Mobilkkommunikation“ (IITM)
München, Germany, 17. 10. 2013 - 16. 02. 2014
ISBN: 3-937201-40-8

ISSN: 1868-2634 (print)
ISSN: 1868-2642 (electronic)
DOI: 10.2313/NET-2014-03-1
Lerhstuhl Netzarchitekturen und Netzdienste (I8) NET 2014-03-1
Series Editor: Georg Carle, Technische Universität München, Germany

Vorwort

Wir präsentieren Ihnen hiermit die Proceedings zu den Seminaren „Future Internet“ (FI) und “Innovative Internettechnologien und Mobilkommunikation” (IITM), die im Wintersemester 2013/2014 an der Fakultät für Informatik der Technischen Universität München stattfanden. Beide Seminare wurden auf Deutsch gehalten. Den Teilnehmerinnen und Teilnehmern stand es aber sowohl für das Paper als auch für den Vortrag frei, Englisch zu benutzen. Dementsprechend finden sich sowohl Englische als auch Deutsche Paper in diesen Proceedings. Einige der Vorträge wurden aufgezeichnet und sind auf unserem Medienportal unter `http://media.net.in.tum.de` abrufbar.

Im Seminar FI wurden Beiträge zu aktuellen Themen der Netzwerkforschung vorgestellt. Die folgenden Themen wurden abgedeckt:

- Messung der TCP-Erweiterung Tail Loss Probe
- Minimierung von Drive Tests in Mobilfunknetzwerken
- Analyse von Traceroutes und rDNS Daten im Internet Census 2012
- Normale Katastrophen und Computersysteme
- Menschliche Entscheidungen und Rationalität
- Ökonomische Anreize bei der HTTPS Authentifizierung
- Überwachung: Gründe und Technische Möglichkeiten
- Überwachung: Gegenmaßnahmen

Auf `http://media.net.in.tum.de/#%23Future_Internet%23WS13` können die aufgezeichneten Vorträge zu diesem Seminar abgerufen werden.

Im Seminar IITM wurden Vorträge aus dem Themenbereich der Netzwerktechnologien inklusive Mobilkommunikationsnetze vorgestellt. Die folgenden Themen wurden abgedeckt:

- Selbstorganisation für heterogene Netzwerke
- Energieverbrauch und mögliche Optimierungen
- Policy-Beschreibungssprachen – Survey

Auf `http://media.net.in.tum.de/#%23IITM%23WS13` können die aufgezeichneten Vorträge zu diesem Seminar abgerufen werden.

Wir hoffen, dass Sie den Beiträgen dieser Seminare wertvolle Anregungen entnehmen können. Falls Sie weiteres Interesse an unseren Arbeiten habe, so finden Sie weitere Informationen auf unserer Homepage `http://www.net.in.tum.de`.

München, März 2014

Georg Carle

Daniel Raumer

Lukas Schwaighofer

Preface

We are very pleased to present you the interesting program of our main seminars on "Future Internet" (FI) and "Innovative Internet Technologies and Mobil Communication" (IITM) which took place in the winter semester 2013/2014. All seminar courses were held in German but the authors were free to write their paper and give their talk in English. Some of the talks were recorded and published on the media portal `http://media.net.in.tum.de`.

In the seminar FI we dealt with issues and innovations in network research. The following topics were covered:

- Measuring TCP Tail Loss Probe Performance
- Minimization of Drive Tests in Mobile Communication Networks
- Analysis of Traceroutes and rDNS Data provided by the Internet Census 2012
- Normal Accidents and Computer Systems
- Human Decisions and Rationality
- Economic Incentives in the HTTPS Authentication Process
- Getting to know Big Brother
- Hiding from Big Brother

Recordings can be accessed on `http://media.net.in.tum.de/#%23Future_Internet%23WS13`.

In the seminar IITM we dealt with different topics in the area of network technologies, including mobile communication networks. The following topics were covered:

- Self Organization for Heterogeneous Networks
- Energy Consumption and Optimization
- Policy Description Languages – Survey

Recordings can be accessed on `http://media.net.in.tum.de/#%23IITM%23WS13`.

We hope that you appreciate the contributions of these seminars. If you are interested in further information about our work, please visit our homepage `http://www.net.in.tum.de`.

Munich, March 2014

Seminarveranstalter

Lehrstuhlinhaber

Georg Carle, Technische Universität München, Germany (I8)

Seminarleitung

Daniel Raumer, Technische Universität München, Germany
Lukas Schwaighofer, Technische Universität München, Germany

Betreuer

Nadine Herold (herold@net.in.tum.de)
Technische Universität München, Mitarbeiterin I8

Ralph Holz (holz@net.in.tum.de)
Technische Universität München, Mitarbeiter I8

Heiko Niedermayer (niedermayer@net.in.tum.de)
Technische Universität München, Mitarbeiter I8

Stephan Posselt (posselt@net.in.tum.de)
Technische Universität München, Mitarbeiter I8

Lukas Schwaighofer (schwaigh@in.tum.de)
Technische Universität München, Mitarbeiter I8

Tsvetko Tsvetkov (tsvetkov@net.in.tum.de)
Technische Universität München, Mitarbeiter I8

Matthias Wachs (wachs@net.in.tum.de)
Technische Universität München, Mitarbeiter I8

Seminarhompage

`http://www.net.in.tum.de/de/lehre/ws1314/seminare/`

Inhaltsverzeichnis

Seminar Future Internet

Session 1: Performance & Optimization

Session 2: Security & Safety

Session 3: Social Impact

Session 4: Surveillance

Seminar Innovative Internet Technologien und Mobilkommunikation

Session 1: Optimization

Session 2: Security

Measuring TCP Tail Loss Probe Performance

Andre Ryll, B.Eng.
Betreuer: Lukas Schwaighofer, M.Sc.
Seminar Future Internet WS2013
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: andre.ryll@tum.de

ABSTRACT

This paper analyzes the performance of the TCP Tail Loss Probe algorithm proposed by Dukkipati et al. in February 2013 under various virtual network conditions. To provide accurate and repeatable measurements and varying network conditions the mininet virtual network is used. Variations include the available bandwidth, round trip time and number of tail loss segments. The tests are done by requesting HTTP data from an nginx web server. Results show that TLP is able to decrease the total transfer time in high-speed networks by 38% and the time until data is retransmitted by 81%. These improvements decrease significantly for higher delay links.

Keywords

TCP, TLP, performance, measurements, comparison, mininet, virtual network, HTTP, iptables, netfilter

1. INTRODUCTION

Loss of data in a network transfer is a general challenge in all connection-oriented protocols. For internet traffic TCP [1] is used as the transport layer for HTTP data. There exist a number of specifications which deal with retransmission behavior of TCP (e.g. [2], [3], [4]). This list has lately been extended by the "Tail Loss Probe" (TLP) algorithm [5]. The TLP internet draft suggests a real-world improvement of the average response time by 7% based on measurements on Google Web servers over several weeks. This paper aims at precisely measuring the response time improvement under various well-defined laboratory conditions to examine benefits and drawbacks of TLP. Variations will include link quality (bandwidth, delay) and the number of lost tail packets. The measurements are done on a single XUbuntu 13.04 Linux machine with a 3.10.6 kernel. To create a simulation with multiple virtual hosts the mininet virtual network is used. Simple HTTP data transfer is accomplished by an nginx[1] web server and the lynx text browser. A user space C/C++ application in conjunction with iptables and netfilter queues allows to precisely drop a specified number of packets at the end of a transfer.

The remainder of this paper is organized as follows: Section 2 reviews the TCP protocol, extensions to it which are essential for TLP and the TLP algorithm itself. Section 3 describes the test setup for data acquisition. This includes mininet, iptables, the user space application and the measurement variations. Section 4 presents the results and the advantages of TLP. Finally section 5 sums up the insight of the measurement results and outlines further options for analysis.

[1]http://nginx.org/

2. TCP

The Transmission Control Protocol (TCP) is a reliable, connection-oriented transport protocol (ISO OSI layer 4 [6]). As it is stream-based it works with bytes (grouped in segments). Higher level protocols can transmit packets over TCP (e.g. HTTP), but TCP itself is not aware of packets. Its counterpart is the simpler User Datagram Protocol (UDP) which works connection-less and packet-based. This section aims at providing an overview of TCP and explains details which are important to understand TLP.

To implement the reliability and retransmission-capabilities the TCP header includes, amongst others, the following important fields:

SYN flag Synchronize sequence number, set once during connection setup to set the initial (arbitrary) sequence number.

FIN flag No more data from the sender.

ACK flag The ACK field is valid. Indicates that this segment acknowledges received data. Always set except in the first segment of a transmission.

ACK field The next expected sequence number of the receiver.

SEQ field segment sequence number. The sequence number in the first (SYN) segment minus the current sequence number indicates the packet data offset in the current stream.

Figure 1 shows a graphical TCP flow representation created by the network analyzer wireshark[2]. In this example a client requested a web page from a server. Flags, content length and transfer direction of a segment are indicated in the green area. The white area shows the sequence and acknowledgment numbers of every segment relative to the first captured segment (implicitly done by wireshark to simplify reading). The connection is established in the first three transfers (TCP 3-way handshake). Afterwards the client sends a HTTP GET request (in this case with a length of

[2]http://www.wireshark.org/

doi: 10.2313/NET-2014-03-1_01

200 bytes) with the desired resource name. The request is acknowledged and followed by the actual data transfer from the server. After the transfer is complete the server wishes to terminate the connection (teardown) by issuing the FIN flag. The client acknowledges every segment and the connection teardown.

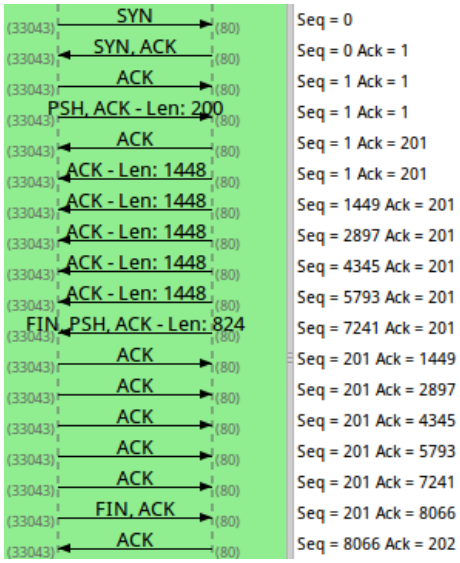


Figure 1: TCP Flow. Green area: Client (left, port 33043) requesting web page via HTTP from server (right, port 80). White area: relative sequence and acknowledgment numbers of the respective segment.

It is important to note, that the client acknowledges every segment in this example. This is not required by the TCP specification. It is sufficient to acknowledge every second segment, given that the segments come in within a short time (RFC1122 section 4.2.3.2. specifies 500ms [7], Linux uses a dynamic approach with a maximum of 200ms [8]). The example transfer is also loss-free. To handle data loss several methods exist, which will be outlined in the following.

The original specification only retransmits segments if they have not been acknowledged after a specified time. This is called RETRANSMISSION TIMEOUT (RTO). Several extensions have been made since TCP was initially specified to improve the retransmission behavior. This includes, amongst others: duplicate ACKs, originally specified in [9], later obsoleted by [2], selective ACKs, specified in [3] and early retransmission, specified in [4].

2.1 Duplicate ACK (DACK)

Duplicate ACKs are acknowledgments from a receiver with the same ACK number, which is not equal to the last expected one of the sender. That means as long as the sender has unacknowledged (but sent) data he expects the ACK number of the receiver to increase with every segment. This explanation is slightly simplified but sufficient for understanding the paper, for a full description see [2].There exist a number of cases which may lead to duplicate ACKs. First of all, a segment may be lost and more data follows. As the receiver does not receive the segment it expects, he sends an ACK with the sequence number he actually expects. This is done for every segment received after the missing segment. Secondly, segments can arrive at the receiver in a different order than they were send due to different paths of the segments through the network. Although all data arrives at the receiver this is an error condition as TCP has to be in-order. Lastly duplicate ACKs may indeed acknowledge duplicate segments. This might for example be caused by a sudden increase in network delay. The transmitters RTO fires and resends a segment which then arrives twice at the receiver. To differentiate between duplicate ACKs from spurious retransmission, out-of-order reception and loss the transmitter waits for three duplicate ACKs before retransmitting data. This mechanism is known as FAST RETRANSMIT as the transmitter does not wait for the retransmission timeout to fire but immediately resends the data. Fast retransmit is described in [2].

2.2 Selective ACK (SACK)

Duplicate ACKs can only inform the transmitter of the next expected sequence. Although more segments after the lost one might have arrived at the receiver the transmitter will need to retransmit data from the point where the first data was lost. To overcome this limitation the SELECTIVE ACK (SACK) option was added to the TCP header [3]. To use SACK both communication partners need to support it. Every SACK-enabled host sets the SACK-permitted option in the SYN packet of the TCP-Handshake. If both hosts support this option it can be used in further communication. If a segment is lost and SACK is allowed the receiver still replies with duplicate ACKs but the ACKs will now have more information about which following segment was successfully received. The SACK option specifies up to three continuous blocks of data, that have been received after one ore more missing blocks (holes). Each block uses a left edge (SLE) of data received and a right edge (SRE) one past the last byte received in that block, both of them are sequence numbers. The transmitter can use the SACK information to precisely resend only data that has been lost and avoids resending data which has been successfully received after a lost segment.

2.3 Early Retransmit (ER)

Selective ACKs provide additional information to the transmitter of data in case of a lost segment. Nevertheless they do not speed up the time until a segment is resend. They help to inform the sender which segments need to be resend. To resend a segment the RTO or three duplicate ACKs (fast retransmit) are still used. The aim of the EARLY RETRANSMIT (ER) algorithm [4] is to lower the number of duplicate ACKs which are needed to retransmit a segment. To achieve this the ER algorithm tries to estimate the remaining number of segments which can be sent. This depends on how much data is available for sending and how much data is allowed to be transmitted before being acknowledged (so called window size). The ER algorithm does not depend on SACK although it can be used with SACK to calculate a more precise estimate of the remaining number of segments. If the window size or the data left is too small to achieve at least three segments in flight, then fast retransmit will never occur as there is no way to generate three duplicate ACKs. In this situation ER reduces the number of required duplicate ACKs to trigger fast retransmit to one or two segments.

doi: 10.2313/NET-2014-03-1_01

2.4 Forward ACK (FACK)

If the window size is large enough and there is enough data to send the retransmission of data still requires at least three duplicate ACKs. To improve this behavior the FORWARD ACK (FACK) algorithm has been proposed [10]. FACK requires SACK in order to work. The FACK algorithm monitors the difference between the first unacknowledged segment and the largest SACKed block (the forward-most byte, hence its name). If the difference is larger than three times the maximum segment size of a TCP segment, then the first unacknowledged segment is retransmitted. If exactly one segment is lost this will happen after receiving three duplicate ACKs. So for only one lost segment FACK and fast retransmission based recovery trigger at the same time. The main advantage of FACK is a situation with multiple lost segments. In these situations it requires only one duplicate ACK when three or more segments are lost to start a recovery.

2.5 Tail Loss Probe (TLP)

All previous solutions to recover lost data are based on the reception of duplicate ACKs to retransmit data before the retransmission timeout (RTO) expires. In situations where the last segments of a transfer (the tail) are lost, there will be no duplicate ACK. So far the only option to recover from such a loss is the RTO. The TAIL LOSS PROBE (TLP) algorithm [5] proposes an improvement to such situations by issuing a "probe segment" before the RTO expires. If multiple segments are unacknowledged and the TLP timer expires the last sent segment is retransmitted. This is the basic idea of the TLP algorithm. Further actions in response to the probe segment are handled by the previously described mechanisms. If exactly one segment at the tail is lost, the probe segment itself repairs the loss, a normal ACK is received. If two or three segment are outstanding ER will lower the threshold for fast retransmit and the duplicate ACK of the probe segment triggers early retransmission. If four or more packets are lost the difference between the last unacknowledged segment and the SRE in the SACK of the probe segment will be large enough to trigger FACK fast recovery. In theory the TLP improves response time to loss in all cases. Table 1 sums up the different options.

losses	after TLP	mechanism
AAAL	AAAA	TLP LOSS DETECTION
AALL	AALS	ER
ALLL	ALLS	ER
LLLL	LLLS	FACK
>=5 L	..LS	FACK

Table 1: TLP recovery options. A: ACKed segment, L: lost segment, S: SACKed segment [5]

3. TEST ENVIRONMENT

To evaluate the performance of TLP a network environment and a possibility to drop tail segments is required. As a physical test setup is hard to reconfigure and inflexible with respect to e.g. bandwidth limitation a network simulation tool has been chosen. All tools are compatible with the Linux operating system, thus a XUbuntu 13.04 32-Bit machine with a 3.10.6 kernel is used for the tests.

3.1 Tool Overview

Two network simulation tools have been investigated. The ns-3 network simulator[3] and the mininet virtual network[4]. ns-3 provides a lot of features for automated testing and data acquisition, although it requires some effort to write a test program. As ns-3 is a simulator the complete network runs in an isolated application. All test programs and algorithms need to be implemented in C/C++ to make them available for measuring. The major drawback of ns-3 is, that it cannot easily interface a recent Linux kernel that supports TLP. Thus ns-3 could not be used for testing TLP performance.

Mininet provides a lightweight virtual network by using functions build into the Linux kernel. Unlike ns-3 it is not a single application but a virtualization technique that allows to create separate network spaces on a single host machine. They share the same file system but processes are executed in their isolated space with specific network configurations. It allows to create everything from simple networks (e.g. 2 hosts, 1 switch) up to very complex topologies, only limited by available processing power. Furthermore it is easily reconfigurable, uses the underlying Linux kernel and can run any Linux program in a virtual host. The Linux traffic control interface can be used to specify delay, bandwidth and loss on a virtual connection. All properties make it ideally suited for TLP performance analysis.

The Linux traffic control interface is not able to precisely drop segments at the end of a transfer. There are two options to achieve this. Mininet switches can be used together with an OpenFlow[5] controller which usually tells the switch how to forward packets by installing rules based on e.g. the MAC addresses in a packet. If a packet does not match a rule it is forwarded to the OpenFlow controller, which investigates the packet and afterwards installs an appropriate rule in the virtual switch. By not installing any rule this can be used to forward all packets passing the switch to the OpenFlow controller which then determines if the packet is at the tail of a transfer and if so drops it. This mechanism has a poor performance, because usually only very few packets are forwarded to the controller for learning and installing appropriate rules afterwards. So although this option works, it is not adequate for rapid tail loss. Another option to drop segments is the use of Linux iptables[6]. As iptables are primarily used for firewall purposes there is no build in option to drop a configurable amount of tail segments. Nevertheless iptables can forward packets to a user space application which then decides to accept or to drop a packet. This is done by using the netfilter queue (NFQUEUE) as a target. Using the libnetfilter library a user space application can process these packets and also access the complete packet content. This option works locally on a (virtual) machine and uses kernel interfaces, thus this approach is quite fast compared to the OpenFlow solution. The user space application is written in C/C++ and provides a good performance.

[3]http://www.nsnam.org/
[4]http://mininet.org/
[5]http://www.opennetworking.org/
[6]http://www.netfilter.org/projects/iptables/

doi: 10.2313/NET-2014-03-1_01

3.2 Setup

The final test setup uses mininet with two hosts and one switch on a XUbuntu 13.04 machine with kernel 3.10.6 and a netfilter user space application using iptables. The setup is depicted in figure 2. To configure this setup the following steps are necessary.

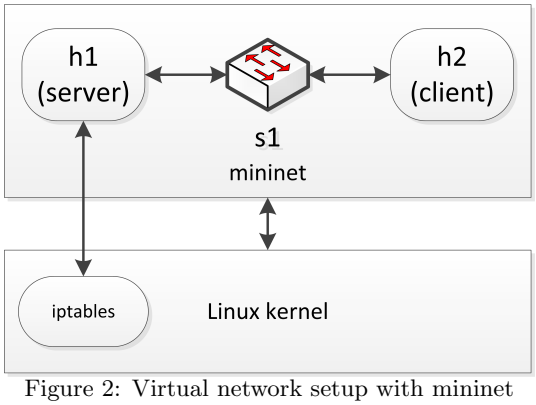


Figure 2: Virtual network setup with mininet

First of all mininet must be started with a configuration of two hosts and one switch. This is done by the command:

```
mn --topo single,2
   --link tc,bw=100,delay=2.5ms
```

This configures mininet with a link bandwidth of 100MBit/s and a delay of 2.5ms per link. Thus the round trip time is 10ms. This setup reflects a common high-speed ethernet environment. The two hosts are named h1 and h2. A terminal to the two hosts can be opened via (entered in the mininet console):

```
xterm h1 h2
```

h1 serves as a web server which is started by typing "nginx" in its command window. Furthermore iptables needs to be configured to pass outbound HTTP traffic (TCP port 80) on interface h1-eth0 to a netfilter queue.

```
iptables -A OUTPUT -o h1-eth0
         -p tcp --sport 80
         -j NFQUEUE --queue-num 0
```

This forwards all TCP traffic leaving h1 to NFQUEUE 0. The iptables and filter setup on virtual host one (h1) is depicted in figure 3. The inbound traffic is passed directly to nginx, whereas the outbound traffic is either accepted directly (non-TCP) or forwarded to the NFQUEUE. The user space application is named "tcpfilter" and can be configured by command line arguments to drop a specified number of packets at the end of an HTTP transfer (e.g. two packets).

```
./tcpfilter 2
```

Implementation details of the tcpfilter are explained in section 3.3. To request a web page from h1 the lynx web browser with the dump option is used on h2. It just requests the web page and dumps it to /dev/null.

```
lynx -dump 10.0.0.1/pk100.html > /dev/null
```

This is repeated several times in a shell script to automatically acquire a set of data. This finalizes the test setup.

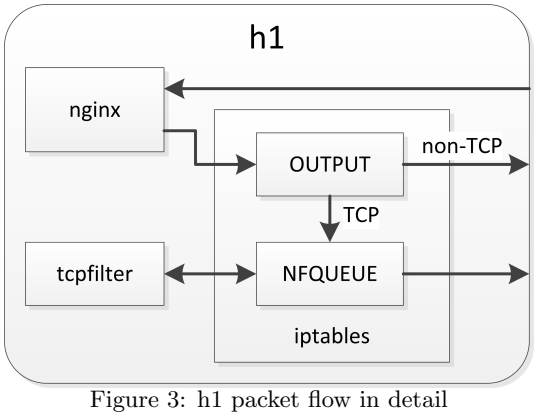


Figure 3: h1 packet flow in detail

3.3 Tail Loss application

The tail loss application tcpfilter is a custom application written in C/C++. It accesses the netfilter queue 0 and processes its packets. For this purpose the complete packet is copied to user space. After packet processing is done it issues a verdict on every packet which can either be ACCEPT or DROP. If drop is selected the kernel silently discards this packet. As this application works on the OUTPUT chain of iptables the packet then never leaves the network interface. This is a simulated packet loss. The number of dropped segments n_{drop} is specified as command line argument to tcpfilter. The algorithm used to generate tail loss is shown in algorithm 1.

As TCP is stream based there is no way of determining the last segment. Thus HTTP is used in the application layer to find the last segment of a transfer. The filter is initially in the idle state. As soon as a HTTP segment (TCP on port 80) is going to be sent it checks the contents of that segment for the string "Content-Length". This indicates that this is the header of a new HTTP transfer. Wireshark analysis show that the content length is always set by nginx for HTML data transfer. It is thus safe to use this field as header indication. The content length is extracted from the header and saved to further track the incoming data. Furthermore the HTTP data length is of this segment is saved to know the maximum data size of a segment.

The filter is now in the transfer state. It is locked on to one transfer by saving its source and destination (IP and port) and the TCP identification. Data that is not belonging to this transfer is accepted, and not processed further. Data for the current transfer is tracked and accepted until it reaches the end of the transfer. As soon as the total transfer size minus the size of the transferred data is smaller than the number of segments to lose at the end times the maximum HTTP size of a segment, the segments are saved in a linked list and no verdict is issued. After a TCP segment for this transfer arrives which has the FIN flag set the saved segments are processed. If the segment with the FIN flag also has HTTP data n_{drop} segments at the tail of the list are dropped, otherwise $n_{drop} + 1$ segments at the tail are dropped. The tcpfilter application thus always drop n_{drop} packets with HTTP data. After the FIN segment the filter enters idle state again and is ready to track the next transfer.

doi: 10.2313/NET-2014-03-1_01

While the drop candidates are in the list, no verdict is issued which may lead to a delay in sending packets. An analysis of the traffic shows that the window size for this transfer is large enough so that the sender transmits more than 20 segments before waiting for an acknowledgment. The time between the first segment in the drop candidate list and the processing due to receiving the FIN flag is thus very short and should not affect the measurements.

Algorithm 1 Creating tail loss

```
Packet p
TransferState s
List candidates
List droppedOnce

if !isHTTP(p) then accept(p)

if exist(p.seq, droppedOnce)
  remove(p.seq, droppedOnce)
  accept(p)

if state == idle and exist(p, "Content-Length") then
  state = xfer
  s.maxHttpSize = p.httpSize
  s.src_dst = p.src_dst
  s.totalLength = extract(p, "Content-Length")
  s.transferred = 0

if state == xfer and p.src_dst == s.src_dst
  bytesRemaining = s.totalLength - s.transferred
  bytesToDrop = n_drop*s.maxHttpSize
  if bytesRemaining < bytesToDrop then
    enqueue(p, candidates)
  else
    accept(p)
  if s.totalLength == s.transferred then
    state = fin

if state == fin and p.fin then
  if p.httpSize == 0 then
    n_drop++
  while size(candidates) > n_drop do
    accept(front(candidates))
  while size(candidates) > 0 do
    enqueue(front(candidates).seq, droppedOnce)
    drop(front(candidates))
  state = idle
```

During transfer processing several nanosecond-accurate timestamps are taken. The first one t_{start} during the transition from idle to transfer. The next are recorded for every drop candidate. The timestamp of the first segment that is finally selected to be dropped is saved to t_{drop}. The next timestamp $t_{retransmit}$ is taken when the first dropped segment is sent again by the Linux kernel. By using t_{drop} and $t_{retransmit}$ the time until a retransmission is started ($t_{recover} = t_{retransmit} - t_{drop}$) can be accurately measured. Finally the time when the segment with the FIN flag is retransmitted t_{end} is recorded. $t_{recover}$ and the total transfer time $t_{total} = t_{end} - t_{start}$ are used to measure the improvements of the TLP algorithm. The tcpfilter applications outputs a row of the following format to the standard output for every transfer:

```
<transfer size>, <transfer segments>,
        <dropped segments>, <t_total>,
        <t_recover>, <isTLP>
```

Experiments show that TLP is not always selected for retransmissions. To remove these transfers from the results tcpfilter outputs the `isTLP` flag. This flag indicates if a retransmission occurred based on TLP or not. TLP retransmissions can easily be detected be checking the first retransmitted segment. If this segment is the last sent segment TLP is used. All other recovery mechanisms retransmit the first lost segment first. The `isTLP` flag is not valid for zero or one dropped segment, as the distinction cannot be made in this case.

3.4 Measurement description

The following section outlines the measurements taken with the test setup to investigate the advantage of TLP in tail loss recovery time and total transfer time. For this purpose all tests are done with a constant transfer size of 100 segments, which equals approximately 144kB in the test setup. The transfer size roughly represents a single web page element, e.g. a graphic or an advertisement. The tcpfilter always drops tail segments, thus the number of segments has no effect on the result. 100 segments are chosen to allow the transmitter to calculate a precise value for the round trip time (RTT) which is used to calculate retransmission timeouts and probe timeouts.

There are in total three different options for the recovery algorithm. One is the new TLP. The previous one working with Early Retransmit is denoted with ER. To further compare the results a dataset is acquired with all TCP extensions (SACK/ER/FACK/TLP) disabled, further denoted 'plain'. These extensions can configured at runtime in the system kernel by using the sysctl interface. All options regarding the tests are found in "net.ipv4". For example, the following command disables TLP.

```
sysctl -w net.ipv4.tcp_early_retrans=2
```

The changes take effect immediately, so there is no need to restart mininet or the whole system. Table 2 shows the configuration for the different algorithms used.

Option	plain	ER	TLP
tcp_early_retrans	0	2	3
tcp_fack	0	1	1
tcp_sack	0	1	1

Table 2: TCP configuration in /proc/sys/net/ipv4

To evaluate the performance under various network conditions three exemplary types are selected as shown in table 3. They do not necessarily reflect real networks but cover a broad range of different conditions. To acquire the measurement dataset all TCP configurations are tested with all network configurations. The tests increase the number of lost tail segments from 0 to 20 and record the time $t_{recover}$ until the first segment is resend and the total transfer time t_{total}. Due to the usage of the mininet virtual network there is no "natural" tail loss during the measurements.

Type	Bandwidth	RTT
high-speed	100MBit/s	10ms
mobile	7.2MBit/s	100ms
satellite	1MBit/s	800ms

Table 3: Network configurations

doi: 10.2313/NET-2014-03-1_01

4. RESULTS

The results are acquired by repeating the measurements for the high-speed and mobile network configuration 100 times and 20 times for the satellite network. The reason for only acquiring 20 samples per number of tail losses in the satellite network is the high round trip time. It takes approximately one hour to obtain a dataset with 420 samples. Table 4 sums up the measurements in the different networks with a loss count of five segments. The previously default option of ER in the linux kernel is the baseline for comparisons. Tail Loss Probe performs best when the round trip time is low. The total transfer time is decreased by 38% in the high-speed network. On a mobile network the time is still 11% lower. The satellite network does not benefit significantly from TLP. Early Retransmit does not improve the transfer time very much compared to plain TCP configuration. This is expected, as ER requires partial information of the received data and duplicate ACKs. Both conditions are not available at a tail drop. When comparing the time to the first retransmission $t_{recover}$ TLP reduces the value significantly by 81% (high-speed network). In the mobile network this reduction drops to 19%. A noticable anomaly is the increase of the recovery time in the plain configuration in the mobile network. As this paper mainly deals with TLP, the evaluation of this anomaly is out of scope.

TCP cfg.	plain		ER	TLP	
100MBit/s, 10ms RTT					
t_{total}	0.3595	+0.6%	0.3574	0.2214	-38%
$t_{recover}$	0.2396	+1.3%	0.2365	0.0447	-81%
7.2MBit/s, 100ms RTT					
t_{total}	1.2091	-1.7%	1.2300	1.0944	-11%
$t_{recover}$	0.4392	+7.8%	0.4073	0.3310	-19%
1MBit/s, 800ms RTT					
t_{total}	8.2145	-0.1%	8.2248	8.1948	-0.4%
$t_{recover}$	2.4792	+0.3%	2.4720	2.4331	-1.6%

Table 4: Recovery algorithm comparison (transfer size: 100 packets, losses: 5). ER configuration serves as baseline.

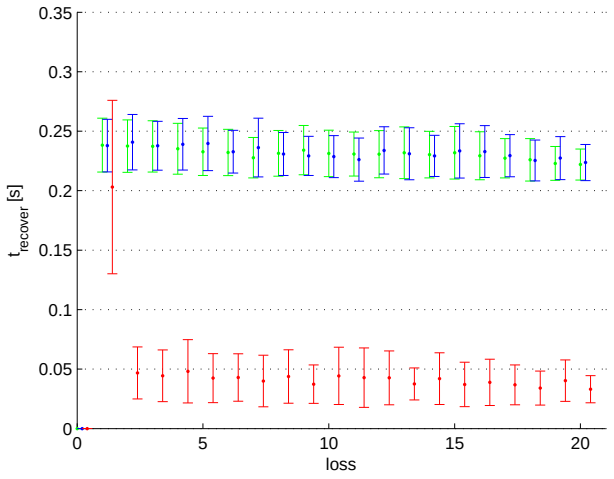
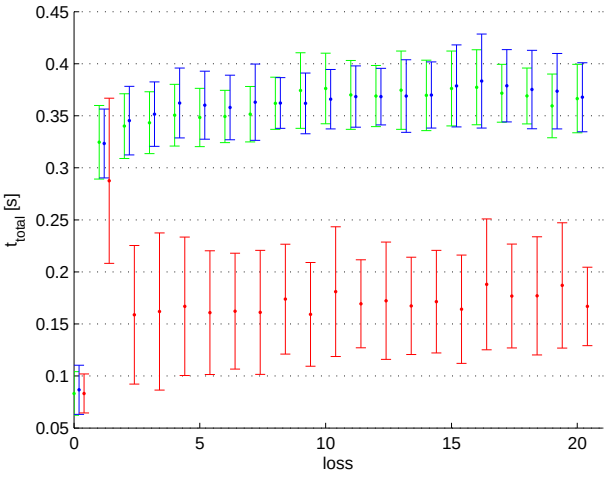
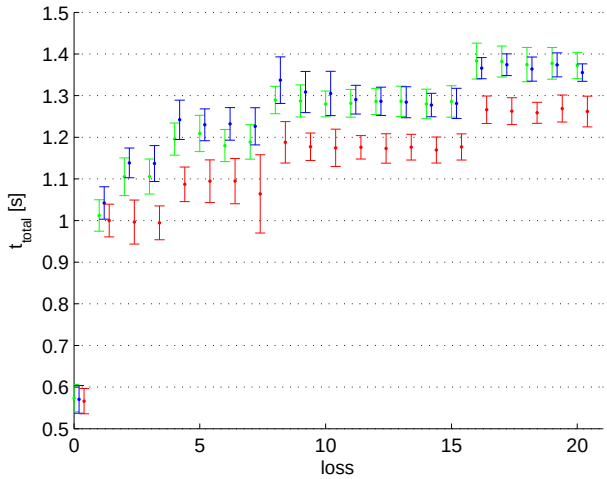


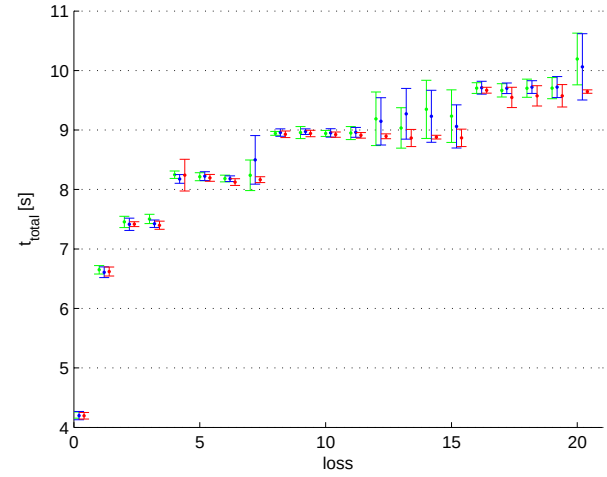
Figure 4: Number of tail losses and time until the first segment is retransmitted. Plain (green), ER (blue), TLP (red). Transfer size 100 segments. High-speed network.



(a) high-speed network



(b) mobile network



(c) satellite network

Figure 5: Number of losses and total transfer time. Plain (green), ER (blue), TLP (red). Transfer size 100 packets.

doi: 10.2313/NET-2014-03-1_01

Figure 4 plots the recovery time versus the number of lost tail segments. The standard deviation is plotted along for each measurement. For a better reading the samples have been slightly shifted on the plot, but the number of losses is always an integer. The results show that the plain implementation and ER perform almost equally. TLP is faster with a factor of approximately 4.5.

Of special interest is the behavior of TLP with a loss of exactly one segment. In this case TLP increases the retransmission timer to accommodate for an eventually delayed ACK. TCP can concatenate two ACKs into a single one if data comes in within short time. To make this concatenation possible the TCP implementation in the Linux kernel waits up to 200ms [8]. This is also the value the TLP retransmission timer is increased when only a single segment is in flight (cf. WCDelAckT in [5], sec. 2.1). Although the data loss is repaired by the tail loss probe segment, it takes approximately twice the time until the transfer is complete (compared to multiple segments in flight).

Figure 5 compares the total transfer time in the three network configurations. In the case of no loss all implementations are equally fast. This also shows that the additional TLP code has no impact on lossless transfers. As noted previously TLP performs bad with a single lost segment. An interesting trend in the mobile and in the satellite network is the slightly increasing transfer time in dependence of the number of lost segments. The tcpfilter drops all segments at once and after the duplicate ACK from the tail loss probe segment ER should immediately resend all segments. Thus the number of tail loss segments should not have such a significant impact. Furthermore the increase in transfer time is not linear. The time increases after 1, 2, 4, 8 and probably 16 packets, which are all exponentials of 2. The reason for the increasing time is most likely the congestion control algorithm used, but this topic is out of the scope of this paper.

The measurements in the satellite network also show that TLP has no substantial benefit for high-delay lines. The recovery time of 2.4s is also higher than expected by the TLP paper. If the flight size is greater than one segment TLP calculates the retransmission timer by multiplying the smoothed RTT by two. This would be 1.6s for the satellite network. For the mobile network this is 0.2s, the measurements show an average of 0.33s. In the high-speed network it should be 0.01s, measured is 0.045s. So the Linux TLP implementation always calculates a higher retransmission timer than specified in the paper. This does not have to be an error in the TLP code but can also be the consequence of the RTT measurement implementation in the Linux kernel.

5. CONCLUSION

The results show that the Tail Loss Probe is an improvement to TCP communication in all tested cases. There is no situation where a non-TLP test result is better. The largest improvement in the time until the first segment is retransmitted (-81%) is recorded in the high-speed network. Total transfer time in such a network with a tail loss is decreased by 38%. The TLP draft reports real-world values from a test with the Google web servers of up to 10% improvement in response time. The values presented in this paper are not comparable to the TLP draft values because in the TLP draft the values are calculated from all transmissions, including those without any tail loss. To compare them one needs to know how many of the transmissions encountered tail loss. It is important to note that TLP has no benefit for a single lost tail segment. Furthermore in high RTT networks TLP does not improve the transfer time. Although especially in these networks a decrease in transfer time would be a great advantage.

The tests included only a small variation of possible measurements. Further options are the transfer size, although this should have no effect with a constant number of tail drops, a generally lossy line or variations in the transfer window size. Furthermore this paper intentionally left out aspects of congestion control and TLP's interference with it. Measurements in this domain require a much complexer user-space application.

6. REFERENCES

[1] J. Postel. Transmission Control Protocol. RFC 793 (Standard), September 1981. Updated by RFCs 1122, 3168.

[2] M. Allman, V. Paxson, and E. Blanton. TCP Congestion Control. RFC 5681 (Draft Standard), September 2009.

[3] M. Mathis, J. Mahdavi, S. Floyd, and A. Romanow. TCP Selective Acknowledgment Options. RFC 2018 (Standards Track), October 1996.

[4] M. Allman, K. Avrachenkov, U. Ayesta, J. Blanton, and P. Hurtig. Early Retransmit for TCP and Stream Control Transmission Protocol (SCTP). RFC 5827 (Experimental), April 2010.

[5] N. Dukkipati, N. Cardwell, Y. Cheng, M. Mathis, and Google Inc. Tail Loss Probe (TLP): An Algorithm for Fast Recovery of Tail Losses. TCP Maintenance Working Group (Internet-Draft), February 2013.

[6] J. D. Day and H. Zimmermann. The OSI reference model. *Proceedings of the IEEE*, 71(12):1334–1340, 1983.

[7] R. Braden. Requirements for Internet Hosts - Communication Layers. RFC 1122 (Standard), October 1989. Updated by RFCs 1349, 4379.

[8] Pasi Sarolahti and Alexey Kuznetsov. Congestion Control in Linux TCP. In *Proceedings of the FREENIX Track: 2002 USENIX Annual Technical Conference*, pages 49–62, Berkeley, CA, USA, 2002. USENIX Association.

[9] M. Allman, V. Paxson, and W. Stevens. TCP Congestion Control. RFC 2581 (Proposed Standard), April 1999. Obsoleted by RFC 5681, updated by RFC 3390.

[10] Matthew Mathis and Jamshid Mahdavi. Forward Acknowledgement: Refining TCP Congestion Control. In *SIGCOMM*, pages 281–291, 1996.

Minimization of Drive Tests (MDT) in Mobile Communication Networks

Daniel Baumann
Supervisor: Tsvetko Tsvetkov
Seminar Future Internet WS2013/2014
Chair for Network Architectures and Services
Department of Computer Science, Technische Universität München
Email: daniel.baumann@in.tum.de

ABSTRACT
Drive tests are used for collecting data of mobile networks. This data is needed for the configuration and the maintenance of mobile networks. In order to execute drive tests, human effort is required. These measurements cover only a small piece of time and location of the network. The new idea is to use each device which is active in the network; this concept is referred to as Minimization of Drive Test (MDT). This means that standard mobiles should be used for measurements to provide data for the operators. The main difference between these tests is that MDT uses cheap mobiles whereas drive tests make use of high developed measurement equipment. This paper demonstrates that MDT can reduce drive tests, but that there are still use cases where MDT cannot replace drive tests.

Keywords
Minimization of Drive Tests, Cellular Networks, Mobile, LTE, SON

1. INTRODUCTION
Mobile communication networks like GSM, UMTS, LTE and TETRA must be monitored and optimized in order to provide a good network coverage and quality of service. One problem could be that coverage holes exist due to the fact that a new building was constructed which shadows a certain area. To detect and improve such problems, radio measurements are needed. These measurements can be done with highly developed equipment directly at the base station or by Drive Tests (DTs) to cover the whole area. They are carried out by cars with measurement equipment. These collect the data in a cell as a snapshot of the cell coverage at a certain time. Furthermore, DTs are used to assess the mobile network performance [3, 4].

The data which was collected with the test equipment can then be post-processed and evaluated for the configuration and failure handling of the networks. Generating and analyzing this measurement data is a large Operation Expenditure (OPEX) and displays only the network state at a defined time and location [4].

In 2008 "Long Term Evolution" (LTE) as part of 3rd Generation Partnership Project (3GPP) Release 8 was published [3]. Today, there is a collection of different technologies like GSM, UMTS, LTE, WLAN and many more. These heterogeneous networks lead to a new complexity with respect to communication and correct configuration. In order to solve this problem, Self-Organizing Networks (SON) was introduced in Release 8, which targets the problem to configure, optimize and heal cellular networks [3, 14]. SON should now simplify the configuration and management of these networks.

The 3GPP also studied and specified solutions in Release 9 under the name "Minimization of Drive Tests" (MDT) in order to reduce the OPEX for drive tests (DT) [4, 15]. It addresses the automation of the measurements and configurations. The main idea is to use each device which is logged in the network for collecting measurement data.

This paper shows use cases and reasons for drive tests and compares the function of MDT and drive tests.

Note that in the following the Base Transceiver Station in GSM (BTS), Node B at UMTS and Evolved Node B (eNB) at LTE are referred with Radio Access Network (RAN) node. In addition, also the Mobile services Switching Center (MSC), Radio Network Controller (RNC) and Mobility Management Entity (MME) a referred with Core Network (CN) node.

The paper is organized as follows. Section 2 describes reasons for drive tests and shows what kind of data the operator needs. The next Section 3 explains how this data is collected. Thereafter, in the Section 4 the idea and vision how drive tests can be minimized is explained. Section 5 picks up the functionality of each and compares them in terms of the operator tasks. In the last Section 7 the comparison of DT and MDT is summarized.

2. OPERATOR TASKS - REASON FOR DT AND MDT
The main goal of network operators is to provide a network with maximum coverage and minimum usage of hardware.

In [15] the 3GPP Technical Specification Group (TSG) RAN defines the main use cases for the minimization of drive tests - which are coverage optimization, mobility optimization, capacity optimization, parametrization for common channels and Quality of Service (QoS) verification. These use cases are shortly described below [3, 15].

1. Coverage optimization
   Coverage is an aspect a user can easily observe and

doi: 10.2313/NET-2014-03-1_02

which mainly influences the user-experience. It is a parameter which the user can use to compare different operators.

Sub-use cases:
Coverage mapping: maps based on signal strength.
Coverage hole detection: areas where call drop and radio link failure happen.
Identification of weak coverage: areas where the signal level is below the level needed to maintain a planned performance requirement.
Detection of excessive interference: due to large overlap of cell coverage areas or an unexpected signal propagation between the cells, excessive interferences can occur. These interferences will degrade the network capacity.
Overshoot coverage detection: in a serving cell a strong signal of another cell is detected, which is far away.
Uplink coverage verification: a weak uplink coverage can cause call setup failure, call drop, bad uplink voice quality. Ideally, the uplink and downlink coverage should be equal, but normally the downlink coverage from the BTS is larger than the uplink coverage.

2. Mobility optimization
   Mobility optimization aims at the minimization of handover failures, which happen when mobiles switch between different cells. It is useful to get measurements at the source and neighbor cells, which are linked to the location.

3. Capacity optimization
   The capacity optimization use case aims at the optimization of network capacity planning. The operator, for example, is interested in those parts of the network where the traffic is unevenly distributed. This data helps to determine places for a new base station.

4. Parametrization for common channels
   The network performance can also be degraded by configurations of the random access, paging or broadcast channels which are not optimized. An analysis of the connection setup delay, for example, helps to optimize the parameters of a BTS.

5. QoS verification
   Aspects like data rate, delay, service response time, packet loss and interrupts are responsible for the QoS. The QoS is not only influenced by the coverage but also by operator specific scheduling of the packet type connections which can lead to bad data rates. The QoS is usually measured with Key Performance Indicators (KPIs), which assess the network. The KPI "Session setup success rate" is, for example, influenced by the performance indicators: RRC establishment success rate, S1 link establishment success rate and ERAB establishment success rate [2].

The drive tests are carried out in the following five scenarios [15]:

1. Deployment of new base stations
   Drive tests are needed when new base stations are deployed. The new base station transmits radio waves in a test mode. Then UL/DL coverage measurements of new and neighbor cells are collected with the help of drive tests. Afterwards the results are used to improve the performance of the cell.

2. Construction of new highways/railways/major buildings
   In areas where new highways, railways or major buildings are constructed the coverage is probably reduced due to a shadowing of the cell. In addition, the volume of network traffic is increased by new buildings. In order to analyze and reconfigure this new usage profile, drive tests are needed.

3. Customer's complaints
   When costumers inform the operator about bad coverage, bad quality of voice or data, the operator also executes drive tests to detect the problem in the relevant area.

4. KPI Alarms at Core Network
   The Operators also monitor the network elements. In order to assess these elements, KPIs are used. Most KPIs are composed of several counters, which contain information like dropped calls or handover failures. The operator can execute drive tests for detailed information. If the amount of failures increase in a certain area, the operator in generally carries out drive tests for detailed information [6].

5. Periodic drive tests
   Periodic drive tests are additionally used to monitor particular cells. They are needed in order to provide a continuously high level quality and to monitor the coverage and throughput of the network [3].

3. DRIVE TESTS

So far, drive tests are the main source for collecting measurement data from cellular networks. As shown in Figure 1, drive tests are usually carried out with the help of measurement cars, which contain systems of scanners and test mobiles. The scanners can be configured to scan all technologies. This is used for detecting interferences and monitoring all accessible base stations. A scanner operates completely passive and is not recognized by the network. As a result, only data which is not encrypted can be collected, which is mostly the signaling and broadcast messages.

Additionally, test mobiles are needed because they are logged in the network and provide, for example, the details for the handover procedures. Furthermore, they are used for checking the speech quality and transfer (up- and download) rates [13].

In the following the functions of scanners and test mobiles are explained more precisely.

3.1 Scanner

Drive tests are mostly carried out by Scanners like TSMW from Rohde & Schwarz, as illustrated in Figure 2. These scanners support the measurements in different networks and positioning with Global Navigation Satellite Systems (GNSSs). The difference to the test mobile is that the scanner has a broadband RF front-end and a baseband processing system. This is the reason why the scanner can support

doi: 10.2313/NET-2014-03-1_02

Figure 1: A measurement car from Rohde & Schwarz [9]

all types of technologies in the defined frequency range. A test mobile normally supports only a few technologies and cannot detect interferences with other networks like DVB-T [13].

The following list contains the advantages of a scanner from [13]:

1. Significantly higher measurement speed than test mobiles:
   High-speed measurements allow better statistics and lower the possibility of missing important problems, such as interferences.

2. Measurements are independent of the network:
   Mobiles only measure channels which are provided by the BTS neighborhood list. The scanner can measure all available channels and allows the detection of hidden neighborhoods.

3. Use of only one unit for different networks and applications:
   Scanners support a number of different technologies like GSM, UMTS, LTE, TETRA and DVB-T.

4. Spectrum analysis provides additional information:
   Spectrum scans with multiple frequency ranges, for example, between 80 MHz and 6 GHz makes it possible to detect in-band and external interferences.

5. Independent of mobile chipsets:
   Scanners have a broadband RF front-end and baseband processing system which is independent from any mobile phone chipset and supports different technologies. Therefore, it can be used as reference system.

6. Higher level and time accuracy compared to mobile based measurements:
   The scanner uses GNSS signals for synchronizing the local clocks and achieves a more precise timing then normal User Equipments (UEs).

7. Scanners are passive:
   Scanners only listen on the broadcast channels and do not influence the network. This makes it possible, for example, to monitor networks on the borderline without roaming costs.

Figure 2: A scanner from Rohde & Schwarz [10]

3.2 Test Mobile

The main feature of the test mobile is that it works in the network and receives the messages. It therefore reflects the behavior of the user mobiles and is used for the operational tests.

This could be: throughput, connection quality, video quality, voice quality, handover and network quality tests. An identifier for network quality could be the ratio of dropped to successful calls [11].

3.3 Data Aggregation Software

With real-time and post-processing tools like R&S ROMES and Network Problem Analyzer (NPA) the data from the scanners and the test mobiles can be analyzed [11].

The major analysis features are [12]:

1. Coverage Analysis
   Provides information where weak coverage, coverage holes or overshoot coverage exists.

2. Interference Analysis
   Provides information where interference exists and from which technology the interference comes.

3. Call Analysis
   Provides information about the number of successful, dropped or blocked calls.

4. Data Transaction Analysis
   Provides information about the response times.

5. Throughput Analysis
   Provides information about the possible data throughput.

doi: 10.2313/NET-2014-03-1_02

6. Neighborhood Analysis
   Checks if the provided neighborhood lists of the base stations are equal to the received broadcast information at the scanner.

7. Handover Analysis
   Shows the duration of handovers or details to a handover failure.

8. Spectrum Analysis
   Provides the information which frequency bands are used and how strong the signals are.

4. MINIMIZATION OF DRIVE TESTS

The problem that drive tests need human effort to collect measurement data and that only spot measurements can be performed, has led to automated solutions which include the UEs from the end user. This approach should provide measurement data for fault detection and optimization in all possible locations covered by the network. The feature for this evolution in the 3GPP standard is named MDT. It started in 2008 in the Next Generation Mobile Networks (NGMN) forum, where the automation of drive tests became operators requirement. The 3GPP also realized the need and followed up on the subject. One of the first studies in 3GPP was in 2009 with the 3GPP Technical Report (TR) 36.805 [3]. The 3GPP started two parallel work items, which are the functioning for MDT in the UE and the MDT management. The MDT in the UE is done by the 3GPP TSG RAN and the MDT management by the 3GPP TSG Service and System Aspects (SA) [3].

The MDT should also "reduce the operational efforts, increase network performance, quality and, at the same time, decrease the maintenance costs" [3].

In the 3GPP TR 36.805 the 3GPP TSG RAN group defined the requirements and constraints for MDT solution. The topics are [15]:

1. The operate shall be able to configure the UE measurements independently from the network configuration.
2. The UE reports measurement logs at a particular event (e.g. radio link failure).
3. The operator shall have the possibility to configure the logging in geographical areas.
4. The measurements must be linked with information which makes it possible to derive the location information.
5. The measurement shall be linked to a time stamp.
6. The terminal for measurements shall provide device type information, for selecting the right terminals for specific measurements.
7. The MDT shall be able to work independently from SON.

The solution shall take the following two constraints into account. The UE measurement logging is an optional feature. To limit the impact on the power consumption one should take the positioning components and UE measurements into account. These UE measurements should as much as possible rely on measurements from the radio resource management [15].

4.1 Architecture

In the beginning of MDT in 3GPP TR 32.827 a user plane and control plane solution was discussed [4].

In the case of the user plane solution, the measurement data is reported by uploading it to a file server. Therefore, the typical data connection is used and the transport is transparent for the radio access network (RAN) and the core network (CN) [3, 17].

At the control plane solution the reporting is controlled by the Operations, Administration, and Maintenance (OAM) system. It is targeted over the eNB/ RNC to the UE via RRC connections. The measurement should then allow to collect and combine the data at the eNB/RNC and send it back to the OAM system [3, 17]. The result of the study phase was that the control plane architecture is better, because the measurement results can be reused for any automated network parameter optimization. With respect to the SON the redundant data handling is avoided [4].

In 3GPP Technical Specification (TS) 34.422 there are two types of MDT in the network signaling perspective and radio configuration perspective defined [4]. These are described in the following.

4.1.1 Area and subscription based MDT

Out of the network signaling perspective, one type is the area based MDT and the other is the subscription based MDT [4].

At the area based MDT the data is collected in an area, which is defined as a list of cells or as a list of tracking/ routing/ location areas [18]. As shown in Figure 3, the MDT activation from the OAM is directly forwarded to the RAN node, which selects the UE of the defined area.

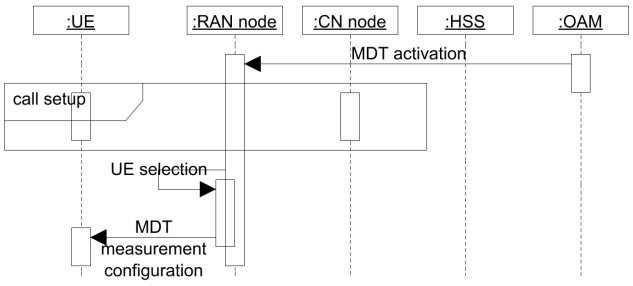


Figure 3: Area based MDT according to [4]

The subscription based MDT addresses the measurement for one specific UE [18, 3]. It is carried out in the OAM by selecting a UE with an unique identifier. As shown in Figure 4, the OAM sends the MDT configuration parameters to the

doi: 10.2313/NET-2014-03-1_02

HSS, which decides if the MDT activation for the selected UE is allowed. The HSS sends the MDT configuration over the CN node and RAN node to the UE [4].

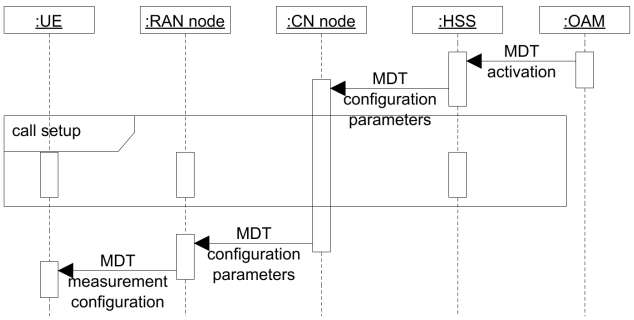


Figure 4: Subscription based MDT according to [4]

4.1.2 Immediate and logged MDT

Out of the radio configuration perspective, one type is the logged MDT and the other the immediate MDT [4].

The immediate MDT allows measurements only in a connected state. It is possible to use several measurement triggers. The UE immediately reports the measurement results, when the configured triggers are met or the reporting configuration matches [16]. These results are collected at the RNC node and as it is shown in Figure 5, this notifies the Trace Collection Entity (TCE), which collects all MDT measurements. After the notification, the TCE uses a file transfer protocol for downloading the MDT log [3].

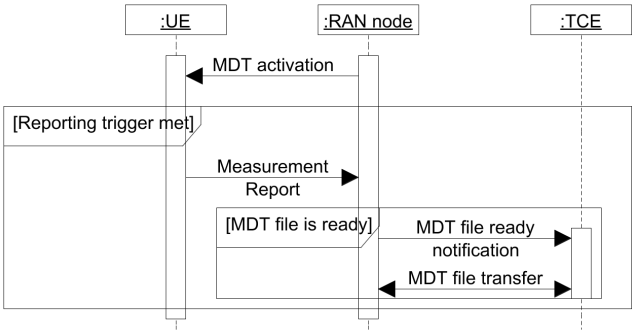


Figure 5: Immediate MDT according to [3]

To support also measurements in the idle state, the logged MDT is used. With the help of logged MDT it is also possible to configure periodical triggers. If this triggers are met, the UE stores the measured information [16]. Additionally, this provides the possibility to store failures if the network is not reachable. The decoupling of measurements and reporting also reduces the battery consumption and the network signaling load. Figure 6 shows that the UE stores the measurements locally and after a defined trigger it is transferred to the RAN node and then to the TCE [3].

For the comparison one should consider that coverage holes can only be detected with the logged MDT, because the immediate MDT does not have a connection to the CN node.

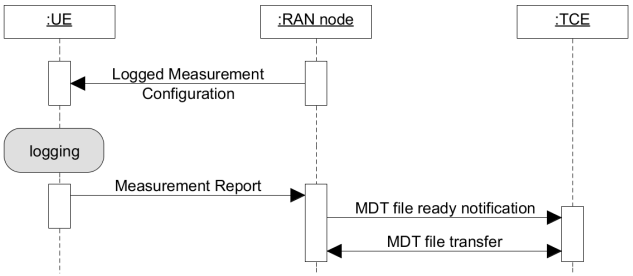


Figure 6: Logged MDT according to [3]

However, the logged MDT is an optional capability and only the immediate MDT is mandatory for the UE [5].

4.1.3 Architecture Elements

The MDT data collection is initiated and controlled by the OAM system. The core network is used for MDT but has no specific MDT logic. The UE and RAN collects the data and sends it to the TCE, which stores the data and can be used for post-processing analysis [5]. This architecture and the usage of the MDT types are shown in Figure 7.

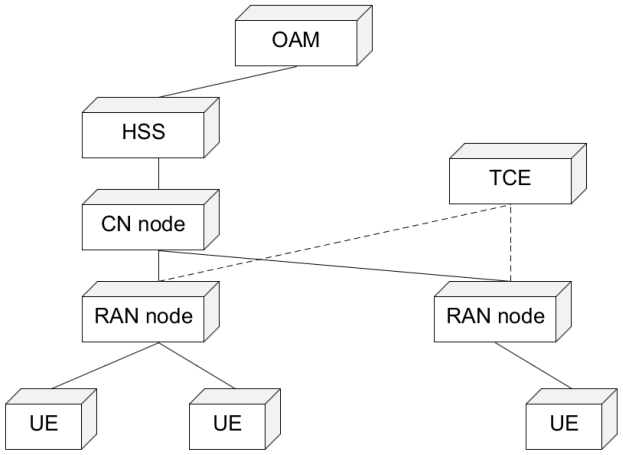


Figure 7: MDT architecture according to [4]

4.2 Managing MDT

The MDT can be configured in the area or subscription based MDT, where the UEs are in the immediate or logged MDT. The configuration of MDT is decided in the OAM which initiates the defined MDT type.

Each constellation between MDT types allows different configurations. In the following is a subset of the MDT configurations parameters from [18] are announced:

1. List of measurements
   It defines the measurements which shall be collected. This could be: data volume, throughput, received signal code power, reference signal received power.
2. Reporting trigger
   It defines if measurement report for UMTS or LTE should be created in a periodical or event based way.

doi: 10.2313/NET-2014-03-1_02

3. Report interval
   It defines the interval of a periodical reporting from 120ms to 1h.

4. Report amount
   It defines the number of measurement reports that should be created.

5. Event threshold
   It defines the threshold for an event based reporting.

6. Logging interval
   It defines the periodicity for logging in logged MDT.

7. Logging duration
   It defines how long an MDT configuration is valid.

8. Area scope
   It defines in which geographical area MDT should be executed. It could be a number of Cells or Tracking/Routing/Location areas.

9. TCE ID
   It is a identifier which can be resolved to the TCE IP at the RAN node.

10. Anonymization of MDT data
    It defines if the measurement results are saved with an IMEI-TAC[1] or no user information.

11. Positioning Method
    It defines if positioning with GNSS or E-Cell ID should be used.

4.3 Location Information

The location information is as important as the radio measurement itself for drive tests, walk tests and MDT. The analysis of the data is only successful with good location information for each measurement.

In MDT 3GPP Release 10 a best effort location acquisition was defined. This means that the measurement can be tagged with location information if it is available for some other location-enabled application [5]. An location-enabled application could be a map application, which already uses the GNSS chip. In Release 11 it is defined that the network can request the UE to use location information for an MDT session. The problem is that this approach can lead to a higher battery consumption. J. Johansson et. al [5] says that the operator "may choose to handle this by subscription agreements, and only use requested location for subscribers that have consented to this." Additionally, an approximate location can be estimated with RF fingerprint measurements. This can be obtained by signal strength measurements of the neighboring cell [5]. Another point is the tagging of RAN-based measurements. This should be done by post-processing with correlating the timestamps of the UE-based DL measurements, which contains already the location information tag.

[1]The first eight digits of the International Mobile Station Equipment Identity

5. COMPARISON BETWEEN DT AND MDT

After the details concerning drive tests and the minimization of drive tests, the DT and MDT is now compared from the perspective of technologies, operator use case and used hardware.

5.1 Technologies

The MDT in 3GPP is defined for UMTS and LTE. However, there are other technologies like GSM, TETRA, DVB-T for which measurements are needed. For instance, GSM is used as communication and signaling network for the railways as GSM-R. There is also a need for coverage measurements. Furthermore, TETRA is now in Germany used by authorities and organizations with security functions like police, fire brigades and emergency rescue services. This organizations require an very robust and good covered network, which requires measurements. This measurements for the mentioned and other technologies can only be carried out by the classical drive tests.

5.2 Use Cases

Section 2 lists the use cases for the operators from the perspective of MDT. In the next subsections these use cases are used for comparing the DT and MDT.

5.2.1 Coverage optimization

Coverage is one of the most important aspects of the network performance which can be directly recognized by the end-user [3].

With the help of MDT it is possible to detect the signal strength and the location of the mobile, which then could be used as coverage indicator [3]. However, the main problem is, that the signal strength between mobiles at the same location and time can differ much more than +-6dB [13]. Another problem is that it is unknown if the mobile is inside a bag or some car which leads to signal lose. If logged MDT is used it is not possible to know if it was a network failure or the mobile. Possibly, this problem could be solved by collecting many measurement data, which then could be merged and statistically evaluated. Another problem is how to get the location inside a building. In [3] it is also suggested to use a GNSS chip as location provider. However, there is also a need for good coverage inside of big buildings like airports. This requires also indoor measurements, but there a GNSS chip is not usable.

With the help of DT and a scanner as a measurement device it is possible to collect coverage measurements in a high quality. The problem here is that it provides only a snapshot of that area, where the DT was executed.

5.2.2 Mobility optimization

Another use case for optimising the mobile network is the mobility optimisation. The aim is to have handover failure rates which are as small as possible. Handover failure can happen if the mobile and networks do not recognize that the user travels from one cell to another and then as consequence of that the user loses the signal from the old cell. Another problem could be that the load is to high and the handover takes too much time. In most cases the call would be dropped. Operators can optimise their network if

they have the following information available. They need to know, between which cells the mobile has switched and the handover times.

It is debatable if the MDT can fully lead to mobility optimisation. This should be possible, because the operator gets the information by the cell ids and locations. Then, if a call was dropped and the signal strength was low, the operator can correlate this information to analyze the handovers. The problem is that the UE only uses the neighbor cells which are in the neighborhood list. If the MDT also measures other channels, then hidden neighborhoods can be detected, too.

With a independent measurement equipment like a scanner together with a test mobile, it is possible to check the network state of both cells and provide information if the handover signals from the network were wrong or the mobile received incorrect information. The scanner also provides measurements for all channels and cells. With these measurements the detection of hidden neighborhood cells is possible.

5.2.3 Capacity optimization

For network capacity planning the operator is interested in the downlink and uplink throughput and data volume [5], for instance, in order to deploy an additional picocell.

In 3GPP Release 11 the throughput and volume measurement at MDT was also addressed. MDT allows to measure the throughput at the RAN. A difference to drive tests is also that MDT uses ordinary user traffic and drive tests applications with known traffic characteristics. By measuring at an application level, the results depends on the size of the data which is transmitted. On transmissions with small size, the scheduling delay could have an impact on the measured throughput. Whereas with large data blocks the result is limited by the transmission medium [5].

With the help of MDT it is possible to measure the amount of traffic within a cell. The location of the sending UE is stored together with the measured data volumes. Per measurement period, the UL and/or DL data volume measurement is carried out by the RAN.

With conventional drive tests it is only possible to measure the available throughput at the UE with a test mobile. It is not possible to measure the data volume of a cell in a selected area or detect areas where users need more data volume.

5.2.4 Parametrization of common channels

The suboptimal configuration of common channel parameters (random access, paging and broadcast channels) can degrade the network performance. For instance, the UE monitors the paging channels, which are needed to react to the incoming calls. If now the information cannot be decoded, the UE is not reachable for other calls [3].

MDT defines in [15] the logging of Paging Control Channel (PCCH) Decoding Error, Broadcast Channel failures. If such a failure happens, the location, time, cell identification and other radio environment measurements are logged.

This is also done with DT, but the problem is here that only a short time is measured and maybe time depended failures are not detected. Usually, operators only find out about problems with the common channels, when they receive customers complaints [15].

5.2.5 Quality of Service verification

The verification of the QoS is another important use case. It is not only the coverage which affects the user experienced QoS, but also, for instance, the scheduling principle for packet type connections which is defined by the operator [3]. The high degree of algorithm flexibility leads to different performances. In general, it is difficult to estimate the QoS from radio measurements such as coverage, path loss or average interference [5].

As already mentioned in Section 5.2.3, in 3GPP Release 11 the throughput and data volume measurement introduced, which provides also QoS verifications. An indication for a QoS problem could be, that the throughput observed by MDT is lower than the expected throughput for the number of users in a period of time. A benefit of the MDT throughput measurement is that real user traffic is used and no additional load on the network is produced [5]. The typical KPIs to assess the QoS can be also estimated by MDT.

With the help of DT the KPIs can be estimated, but the problem is here again that only a snapshot of the selected area is available.

5.3 Hardware

Comparing the DT and MDT out of the hardware perspective, it is obvious that the DT equipment can provide higher measurement rates and accuracy.

A problem with MDT is, that the UE must execute a big part of the measurement and additional information e.g. about position, requires a higher power consumption [5]. It is necessary that the additional hardware is cheap enough. The requirements for low power consumption and prices will lead to less powerful MDT devices than DT equipment.

6. PROBLEM INDOOR

Today more and more measurements are needed indoor for mobile communication networks. The reason is that the data and voice traffic from within buildings have increased and now more calls are made from indoor then outdoor [8]. This requires additional indoor measurements for optimizing the networks for indoor usage. With the typical drive test, which makes use of cars, these areas could not be scanned. However, there are several solutions where a scanner in a backpack can be used. The main problem with indoor measurements is the location accuracy. Outdoor, GNSS can be used with an accuracy less than 2.5 meters [19]. However, it is today indoor not usable due to the signal loss. And for example, for bigger buildings like airports a communication access is important. Because of that, higher positioning accuracies are needed then outside.

But the current indoor positioning solutions do not provide this accuracy. Possibly, this target could be reached with higher developed equipment.

doi: 10.2313/NET-2014-03-1_02

7. CONCLUSION

The MDT features allow new measurements which are user centric and which can help the operators to provide a better communication network.

Parts of the drive test can be carried out with MDT, like coverage, capacity, and QoS. However, for a detailed detection of coverage holes or hidden neighborhoods, a drive test is needed. Furthermore, during the first rollouts of new technologies the MDT cannot be used, because no UEs are in the network. In this case the operator needs the drive test. A drive test is also needed for technologies in which not enough UEs for MDT are used.

It is also a challenge to carry out precise indoor measurements with the mobiles of users, because no GNSS can be used. For the indoor case it is more thinkable to use walk test equipment with special positioning hardware like inertial measurement units (IMUs) [1] or optical devices for visual odometry [7] then MDT.

Overall, one can argue that in the future the MDT will provide great features to solve automatic coverage and QoS measurements in the UMTS and LTE networks.

8. ACKNOWLEDGEMENT

The author gratefully acknowledge the support of Rohde & Schwarz.

9. REFERENCES

[1] M. Angermann, P. Robertson, T. Kemptner, and M. Khider. A High Precision Reference Data Set for Pedestrian Navigation using Foot-Mounted Inertial Sensors. In *International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, September 2010.

[2] ERICSSON. Transparent Network-Performance Verification for LTE Rollouts, September 2012.

[3] S. Hamalainen, H. Sanneck, and C. Sartori. *LTE Self-Organising Networks (SON): Network Management Automation for Operational Efficiency*. Wiley, 2011.

[4] W. A. Hapsari, A. Umesh, M. Iwamura, T. Malgorazata, G. Bodog, and S. Benoist. Minimization of Drive Tests Solution in 3 GPP. *IEEE Communications Magazine*, June 2012.

[5] J. Johansson, W. A. Hapsari, S. Kelley, and G. Bodog. Minimization of Drive Tests in 3 GPP Release 11. *IEEE Communications Magazine*, November 2012.

[6] J. Laiho, A. Wacker, and T. Novosad. *Radio Network Planning and Optimisation for UMTS*. Wiley, 2006.

[7] D. Nister, O. Naroditsky, and J. Bergen. Visual odometry. In *IEEE Conference on Computer Vision and Pattern Recognition*, 2004.

[8] Nokia Solutions and Networks. Coverage and capacity come indoors with In Building Solutions. http://nsn.com/news-events/insight-newsletter/articles/coverage-and-capacity-come-indoors-with-in-building-solutions, March 2012.

[9] Rohde & Schwarz. R&S TS9955 High performance Drive Test System. http://www.rohde-schwarz.com/en/product/ts9955-productstartpage_63493-8705.html, January 2014.

[10] Rohde & Schwarz GmbH & Co. KG. *Radio Network Analyzer R&S TSMW Operating Manual*.

[11] Rohde & Schwarz GmbH & Co. KG. *R&S ROMES4 Drive Test Software Mobile coverage and QoS measurements in wireless communications*.

[12] Rohde & Schwarz GmbH & Co. KG. *R&S ROMES NPA Network Problem Analyzer User Manual*, 2011.

[13] S. Schindler. Rohde & Schwarz Guideline for Scanner-based Drive Tests. Technical report, Rohde & Schwarz, February 2009.

[14] Technical Specification Group Radio Access Network. Self-configuring and self-optimizing network use cases and solutions (Release 8). 3GPP TR 36.902 Version 1.0.0, 3GPP, February 2008.

[15] Technical Specification Group Radio Access Network. Study on Minimization of drive-tests in Next Generation Networks. 3GPP TR 36.805 Version 9.0.0, 3GPP, Dezember 2009.

[16] Technical Specification Group Radio Access Network. Radio measurement collection for Minimization of Drive Tests (MDT). 3GPP TS 37.320 Version 11.3.0, 3GPP, March 2013.

[17] Technical Specification Group Services and System Aspects. Integration of device management information with Itf-N. 3GPP TR 32.827 Version 10.1.0, 3GPP, June 2010.

[18] Technical Specification Group Services and System Aspects. Subscriber and equipment trace;Trace Control and Configuration Management. 3GPP TS 32.422 Version 11.8.1, 3GPP, July 2013.

[19] u-blox AG. *UBX-G6010-ST-TM - u-blox 6 Precision Timing GPS chip*.

Analyse von Traceroutes und rDNS Daten im Internet Census 2012

Stefan Liebald, Stefan König
Email: stefan.liebald@web.de, s.koenig@tum.de
Betreuer: Ralph Holz
Seminar Future Internet SS2013
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München

KURZFASSUNG

In dieser Arbeit untersuchen wir die Ergebnisse des 2012 durchgeführten Internet Census im Hinblick auf Traceroutes und reverse DNS Einträge. Die Untersuchung richtet sich dabei unter anderem auf geographische Aspekte. Zur Auswertung verwendeten wir die spaltenorientierte Datenbank MonetDB sowie Tools zur Umwandlung von IP Adressen in die zugehörigen Autonomen Systeme, beziehungsweise die zugeordneten Länder. Aus den so gewonnenen Daten konnten wir die betroffenen IP Adressen der Traceroutes geographisch zuordnen und Einblicke in die Verteilung der Start und Zielgeräte gewinnen. Desweiteren war es uns möglich Einblicke in die Struktur des Internets zu gewinnen und interessante Traceroutes zu analysieren. Mittels der rDNS Einträge konnten wir eine Übersicht über die Verteilung der einzelnen Domains auf verschiedene Länder gewinnen, sowie die theoretischen Möglichkeiten diverser Länder aufdecken, auf Domains anderer Länder Einfluss zu nehmen.

Schlüsselworte

Internet Census 2012, Carna Botnetz, MonetDB, Traceroutes, rDNS, Auswertung

1. EINLEITUNG

Das Internet ist ein weltweit zusammenhängendes Netzwerk von Rechnern und Rechnernetzwerken. Bedingt durch den dezentralisierten Aufbau dieses enorm großen Netzwerks ist es nicht mehr möglich kurzfristig weiterführende Aussagen über den aktuellen Zustand des Gesamtnetzwerkes zu geben. Der verwendete Adressraum des aktuell noch am gebräuchlichsten Kommunikationsprotokolls IPv4 wird dabei mit 32 Bit Adressen beschrieben, was rund 4,3 Milliarden möglichen verschiedenen Adressen entspricht. Eine Analyse dieser großen Anzahl an verschiedenen adressierbaren Geräten gestaltet sich in der Praxis, aufgrund mangelnder Netzwerk- und Rechenkapazitäten, schwierig. Aufgrund der hochdynamischen Struktur und Architektur muss hierzu ein in kürzester Zeit erstellter Schnappschuss verwendet werden, um die Anzahl von Duplikaten zu verringern. Im Rahmen des Internet Census 2012 wurde ein solche Kartografierung des Internets mit Hilfe eines Botnetzes (Carna Botnet), auf welches im folgenden Abschnitt detailliert eingegangen wird, vorgenommen.

Die mittels Carna gewonnenen Daten bieten eine sehr interessante und umfangreiche Möglichkeit einen Schnappschuss des Internets zu analysieren. Aus Datenströmen, geografischen Standorten und vorhandenen Services können anschließend Aussagen über verschiedenste Parameter, wie eventuelle politische Einflussnahme oder die geografische Verteilung der weltweit genutzten Infrastruktur, getroffen werden.

Ein weiterer wichtiger Punkt der mittels Analyse solcher Daten erreicht werden kann, ist die Analyse des Internets auf Sicherheitsgefährdungen, um diese möglichst zeitnah erkennen oder vorhersagen zu können.

Diese Arbeit konzentriert sich auf zwei der durch den Internet Census 2012 erfassten Datensätze und gliedert sich wie folgt:

Einführend stellt Abschnitt 2 klar, was ein Internet Zensus ist, was genau der Internet Census 2012[1] für Daten erfasst hat und wie dieser durchgeführt wurde. Daraufhin folgt ein Überblick über die von uns zur Analyse verwendete Software sowie über während unserer Arbeit aufgetretene Probleme. In den Abschnitten 4 und 5 gehen wir genauer auf die Datensätze der Traceroutes und rDNS ein. Dabei stellen wir zuerst allgemeine Charakteristika der Daten vor und beschreiben dann unserer Auswertungen. In Abschnitt 6 widmen wir uns schließlich noch verwandten Arbeiten, bevor unsere Arbeit mit einer kurzen Zusammenfassung endet.

2. INTERNET CENSUS 2012

In diesem Abschnitt klären wir einerseits die Frage, was ein Internetzensus überhaupt ist und welche Gründe es dafür gibt einen solchen Zensus durchzuführen. Zum anderen geben wir anschließend eine kurze Einführung speziell in den Internen Census 2012 und erläutern sein Zustandekommen, sowie seinen Inhalt.

2.1 Was ist ein Internet Zensus

Allgemein bekannter ist der Begriff Zensus im Zusammenhang mit der Volkszählung. Eine Volkszählung dient dazu statistische Bevölkerungsdaten zu erheben (z.B. Alter, Einkommen, Beruf,...), um auf deren Grundlage beispielsweise Trends erkennen zu können denen gegengewirkt werden sollte. Ein Beispiel für einen solchen Trend wäre Altersarmut in

[1]Da wir den Internet Census 2012 als Eigennamen dieses Speziellen Zensus ansehen, verwenden wir Census um auf den Census 2012 zu verweisen und das deutsche Zensus, wenn wir allgemein über einen Zensus sprechen.

doi: 10.2313/NET-2014-03-1_03

bestimmten Regionen. Der Begriff Internet Zensus ist nun ganz ähnlich zu Verstehen, allerdings werden in einem solchen Zensus statt Bevölkerungsdaten Daten bezüglich des Internets erhoben (wie es der Name bereits andeutet). Gesammelt werden können dabei beispielsweise IP-Adresse, offene Ports, laufende Services und vieles weitere (siehe Abschnitt 2.4). Eine offizielle Definition des Begriffs „Internetzensus“ existiert allerdings noch nicht.

Analog zum Volkszensus lassen sich aus den Daten Trends Ablesen, welche beispielsweise für Sicherheitsfragestellungen relevant sein können. Ein Beispiel hierfür wäre eine Auswertung des Zensus in Bezug auf die Verbreitung veralteter Softwareversionen (z.B. Webserver) oder, wie im Internet Census 2012 zum Erstellen des Zensus genutzt, die Verbreitung der Verwendung von unsicheren Standard-Passwörtern.

2.2 Was ist der Internet Census 2012

Beim Internet Census 2012 handelt es sich um eine Zusammenführung der Daten aus mehreren IP basierten Scans über das gesamte Internet, welcher im Jahr 2012 durchgeführt wurde. Zur Durchführung dieser Scans wurde auf ein umfangreiches Botnetz (näheres hierzu im Abschnitt 2.3) zurückgegriffen. Der (anonyme) Urheber des Census stellte die Daten anschließend auf verschiedenen Plattformen [26] zur Verfügung. Der zur Verfügung gestellte Download umfasst gepackt rund 1,5 TB (entpackt 9TB) und kann beispielsweise via Bittorrent heruntergeladen werden. Er beinhaltet gepackte, Komma separierte, Klartextdateien, welche leicht aufbereitet und in verschiedene Datenbanksysteme importiert werden können. Einige der Daten können auch direkt im Browser betrachtet werden.

Der Autor nimmt in der gesamten Veröffentlichung keine Interpretation der Daten vor, sondern stellt nur das gesamte Projekt an sich vor. Der gesamte Census bezieht sich nur auf IPv4 Adressen, IPv6 wurde nicht untersucht. Aus diesem Grund werden wir, wenn wir im folgenden von IP Adressen reden, immer von IPv4 Adressen sprechen.

2.3 Carna Botnetz

Das Carna[2] Botnetz stellte die Grundlage zur Erzeugung des Internet Census 2012 dar. Aufgrund der rechtlich problematischen Situation der Datengewinnung bleibt der Autor der Studie anonym, stellt die gewonnenen Daten jedoch der Allgemeinheit zur Verfügung. Das verwendete Botnetz beruhte zum Zeitpunkt des Census auf rund 420.000 Geräten, auf die der Autor über Telnet Zugriff erhalten konnte. Grundlage hierfür waren nicht geänderte Loginnamen und Standardpasswörter, wie zum Beispiel Benutzername: „root“, Passwort: „root“. Die verwendete Software musste, um ein möglichst nicht invasives Netzwerk zu erhalten[3], nach jedem Neustart des Gerätes erneut aufgespielt werden, da sie sich nur im Hauptspeicher installierte. Aus diesem Grund schwankte die Gerätezahl während der gesamten Messung, da neugestartete Geräte nicht mehr verwendet werden konnten bis der Bot gegebenenfalls neu aufgespielt wurde. Die Aussagen bezüglich der möglichst geringen Invasivität durch den Autor konnten mangels Details von uns jedoch nicht weiter geprüft werden. Auch über die verwendeten Geräte werden keine weiteren Aussagen getroffen, diese werden in der Arbeit nur als ressourcenstarke und -schwache Geräte bezeichnet. Die ressourcenarmen Geräte wurden dabei als Endpunkte genutzt, die ressourcenstärkeren Geräte wurden zusätzlich auch zum Einsammeln der gewonnenen Daten der schwachen Geräte genutzt. Viele der durchgeführten Scans basierten auf Möglichkeiten des freien Open Source Tools Nmap [16], einem bekannten Portscanner.

[2] Göttin der römischen Mythologie.

[3] Vom Ersteller des Census wird in seinem Paper klargestellt, das er es als eines seiner Hauptziele ansah, keinen Schaden an übernommenen Geräten anzurichten.

2.4 Messungen

Im Laufe des Census wurde eine Reihe unterschiedlicher Daten gesammelt und schließlich zur Verfügung gestellt. Eine Übersicht über die Struktur der gewonnenen Daten kann in Tabelle 1 eingesehen werden. Die Inhalte werden im folgenden kurz beschrieben:

ICMP Echo Requests: ICMP Echo Requests (Pings) wurden mehrfach über verschieden lange Zeiträume an den gesamten IP Adressraum gesendet, die Antworten wurden gespeichert.

Reverse DNS: Das Domain Name System ordnet jeder Domain eine oder mehrere zugehörige IP Adressen zu und ermöglicht so die Umwandlung von Domain Namen in IP Adressen. Allerdings ist es in vielen Fällen auch möglich einer IP Adresse eine Domain zuzuordnen, dies nennt man „reverse DNS“. Im Internet Census wurde versucht zu möglichst vielen IP Adressen (rund 86% Abdeckung) die zugehörigen reverse DNS Einträge abzurufen. Zu jeder abgefragten IP Adresse wurden die resultierenden Domains oder ein Fehlercode abgespeichert.

Serviceprobes: Die Serviceprobes sind der größte Datensatz des Internet Census, hierfür wurden verschiedene Ports angefragt (geprobt) und deren Antwort gespeichert. Die Ergebnisse bieten die Möglichkeit zur Analyse welche IP Adressen welche Ports geöffnet haben und welche Services auf diesen laufen. Hieraus lassen sich beispielsweise Prognosen über zukünftige Angriffsziele erstellen, ein Beispiel ist der Telnet Port 23, welcher von Carna relativ einfach ausgenutzt werden konnte.

Hostprobes: Mittels Hostprobes wurde geprüft ob ein Host auf Anfragen reagiert. Im Gegensatz zum ICMP Ping Scan wurde bei den Hostprobes zusätzlich auch ein TCP SYN Paket an Port 443, ein TCP ACK Paket an Port 80 und eine ICMP Timestamp Anfrage gesendet. Dies bietet mehr Erkennungsmöglichkeiten ob ein Host online ist als ein einfacher Ping, da die Antwort auf den Ping möglicherweise unterdrückt wird, während auf eine der anderen Anfragen eine Antwort erfolgt.

Syncscans: Bei einem TCP SYN Scan[4] wird versucht eine Verbindung zu einem bestimmten Port aufzubauen. Sollte eine Antwort erfolgen, wird der Aufbau allerdings sofort abgebrochen und die Verbindung kommt nicht zustande. Durch die Antwort kann aber trotzdem auf den Zustand

[4] Der Autor des Internet Census spricht in seiner Arbeit immer von Syncscans, gemeint ist damit aber der bekannte SYN Scan.

doi: 10.2313/NET-2014-03-1_03

Typ	Felder	Anzahl	Größe
ICMP Ping	IP, Timestamp, Ergebnis	52 Mrd.	1,8 TB
Reverse DNS	IP, Timestamp, Ergebnis	10,5 Mrd.	366 GB
Serviceprobes	IP, Timestamp, Status, Ergebnis	180 Mrd.	5,5 TB
Hostprobes	IP, Timestamp, Status, Grund	19,5 Mrd.	771 GB
Syncscans	IP, Timestamp, State, Grund, Protokoll, Ports	2,8 Mrd.	435 GB
TCP IP Fingerprints	IP, Timestamp, Ergebnis	80 Mio.	50 GB
IP ID Sequence	IP, Timestamp, Ergebnis	75 Mio.	2,7GB
Traceroute	Timestamp, Quell IP, Ziel IP, Protokoll, Route	68 Mio.	18 GB

Tabelle 1: Übersicht über durchgeführte Messungen

des Ports geschlossen werden (geschlossen, offen oder gefiltert). In diesem Datensatz werden die Ports aufgelistet, die auf einen SYN Request reagiert haben, bzw. nicht reagiert haben. Durchgeführt wurde der Scan nur für eine Auswahl an bekannteren Ports (z.B. 23 Telnet, 80 http, 443 https) von erreichbaren bzw. antwortenden IP Adressen.

TCP IP Fingerprints: Für einige IP Adressen war es möglich einen TCP/IP Fingerabdruck zu ermitteln. Mit diesem Fingerabdruck ist es unter Umständen möglich detaillierte Eigenschaften, wie Hersteller, Betriebssystem o.Ä. des jeweiligen Geräts zu ermitteln. Grundlage hierfür ist die jeweils eigene Implementierung des TCP/IP Protokollstapels in verschiedenen Betriebssystemen, wodurch sich bestimmte Felder im TCP oder IP Header je nach Betriebssystem unterscheiden. Diese Fingerabdrücke sind allerdings nicht zwangsläufig korrekt, da sich die Felder auch manuell konfigurieren lassen.

IP ID Sequence: Analyse der von den Hosts genutzten Strategien zur Erzeugung der Identifikationsnummern innerhalb des IP Headers.

Traceroutes: In diesem Datensatz sind die Ergebnisse der durchgeführten Traceroutes abgelegt, unter Angabe der einzelnen Hops und deren Laufzeiten. Es ist jedoch keine Information vorhanden ob das Ziel der Traceroutes erreicht wurde.

3. TECHNIK

Bedingt durch die sehr großen Datenmengen und Aufbau der Daten ist es nur schwer möglich die Verarbeitung allein mit potenter Hardware zu ermöglichen, auch die verwendete Datenbanksoftware muss für entsprechend große Datenmengen konstruiert sein. Bedingt durch die schmalen, aber sehr hohen Tabellen (Teils mehreren Milliarden Zeilen bei nur maximal sechs Spalten) bot sich ein auf spaltenweise Verarbeitung spezialisiertes Datenbankmanagementsystem (DBMS) an.

Hierfür standen uns mehrere, erprobte Varianten (MonetDB [15], Greenplum [17][5]) zur Verfügung. Eine weitere Möglichkeit war die Verwendung des zeilenbasierten Datenbanksystems PostgreSQL [18]. MonetDB ist im Gegensatz zu Greenplum eine Open Source Lösung, weswegen wir diesem den Vorzug gaben. PostgreSQL ist zwar ebenfalls Open Source, wurde von uns aber aus Performancegründen hinten angestellt, da einige durchgeführte Benchmarks erhebliche zeitliche Vorteile bei der Auswertung von Anfragen durch MonetDB aufzeigten. Für diesen Test verwendeten wir einen kleinen Teil (1 Millionen Einträge) des in Abschnitt 4 vorgestellten Traceroute Datensatzes. Tabelle 2 zeigt einige Anfragen, sowie die von Monetdb und PostgreSQL benötigte Zeit für deren Abarbeitung[6].

Die Verhältnisse schwankten zwar je nach Anfrage relativ stark, allerdings hatte MonetDB immer einen relativ großen Vorsprung vor PostgreSQL. Bei den Werten gilt zu beachten, dass sich die von PostgreSQL ohne Optimierung durch Indize ergaben, welche MonetDB bei Bedarf von alleine anlegt. Allerdings brachte ein Test mit Indizen nur Geschwindigkeitszunahmen von ungefähr 10%, was immer noch wesentlich langsamer war als MonetDB. Unsere Wahl des DBMS fiel schließlich auf MonetDB, für den Falle des Scheiterns, bedingt durch den Beta Status von MonetDB, wurde PostgreSQL allerdings als Fallback Lösung berücksichtigt. Als Hardware stand uns ein Server mit 24 Kernen und 144 GB Arbeitsspeicher zur Verfügung.

3.1 MonetDB

MonetDB ist ein Open Source Database Managment System, welches speziell auf große Datenmengen und komplexe Querys optimiert wurde. Im Gegensatz zu bekannteren zeilenbasierten DBMS, handelt es sich bei MonetDB um eine spaltenoptimierte Datenbanksoftware. Ein weiteres, sehr wichtiges und performancerelevantes Feature ist die Speziaisierung durch optimale Ausnutzung von CPU Caches. Weiterhin arbeitet MonetDB RAM zentrisch, Änderungen werden zuerst im RAM abgelegt und dann über ein Log File später erst in die Datenbank persistiert. Der größte Nachteil von MonetDB ist der derzeitige Beta Status, die mangelhafte Dokumentation und die noch nicht vollständig unterstützte SQL Syntax.

3.1.1 Probleme

Aufgrund der großen Datenmengen von mehreren Terabyte in Verbindung mit mehreren Milliarden Zeilen kam während der Auswertung auch die leistungsfähige Datenbank MonetDB an die Grenzen der Technik bzw. des Arbeitsspeichers. Bedingt durch die RAM zentrierte Arbeitsweise von MonetDB werden bei Querys die Daten initial in den Arbeitsspeicher geladen, um anschließend ausgewertet zu werden. Bei kleineren Datensätzen stellt dies kein Problem dar.

[5]Greenplum bietet sowohl Zeilen- als auch Spaltenorientierte Datenverarbeitung.

[6]Jede Anfrage wurde von uns mehrfach ausgeführt und eine Durchschnittszeit ermittelt.

doi: 10.2313/NET-2014-03-1_03

Anfrage	Zeit MonetDB	Zeit PostgreSQL	Verhältnis Postgres/MonetDB
select count(*) from data	0,305ms	253ms	829
select count(distinct targetIP) from data	1,1s	7s	6,4
select targetIP, count(distinct targetIP) from data group by targetIP	0,7s	11,2s	16

Tabelle 2: Performanzvergleich verschiedener Anfragen an MonetDB und PostgreSQL

Bei großen Tabellen, wie der RDNS Datensatz aus dem Internet Census waren die vorhanden 144GB RAM jedoch nicht mehr ausreichend um eine gesamte Spalte in den Arbeitsspeicher zu laden. Dies führte zu einer enorm hohen IO Load des Systems. Abhilfe konnte nur durch einen Abbruch des Querys geschaffen werden, dies gestaltete sich als initial schwierig, da das Abbrechen von Querys in MonetDB zum Zeitpunkt der Durchführung nur unzureichend dokumentiert war.

Ähnliche Probleme traten auch beim Einspielen der RDNS Einträge auf. Hier werden von MonetDB die Einträge erst im RAM zwischengespeichert um dann über das Log File persistiert zu werden. Dies führte ebenfalls zu einer permanent sehr hohen IO Load des Systems und konnte von uns nur durch einen Neustart des gesamtes DBMS behoben werden. Weitere gravierende Probleme gibt es bei der Vergabe eines Primärschlüssels während des Imports von großen Datensätzen (bereits im 8 stelligem Bereich). Mit zunehmender Anzahl von importierten Tupeln kann ein immer stärkerer Einbruch der Performance bemerkt werden. Die vermutete Ursache für dieses Verhalten liegt in der automatischen Erzeugung von Indizies. Dieser Einbruch konnte dabei sowohl unter Verwendung einzelner Transaktionen, als auch der Verwendung einer Gesamttransaktion festgestellt werden. Für einen fehlerfreien Import musste später die Datenbank in den Wartungsmodus geschalten werden.

Darüber hinaus gab es während der Entwicklung große Problem mit dem Datentyp für IP-Adressen (INET), dessen Performance bricht unter nicht reproduzierbaren Bedingungen sehr stark ein, sodass eine Nutzung für weiterführende Auswertungen nicht möglich ist. Auch war die MonetDB SQL Python API nicht in der Lage Anfragen nach Daten des Typs INET zu verarbeiten und erzeugte einen Fehler, wenn der INET Typ nicht zuerst auf VARCHAR konvertiert wurde. Es lässt sich jedoch abschließend nicht sagen, ob die aufgetretenen Probleme wirklich alle Probleme des DBMS sind, oder ob sie auf die noch nicht ausgereifte (Python) API zurückzuführen waren.

3.1.2 Fazit

Wenngleich es bei der Anwendung von MonetDB zu größeren Problemen und Unannehmlichkeiten kam, überwogen die Vorteile während der gesamten Auswertung deutlich, vor allem da wir in der Lage waren, die meißten Probleme zu lösen oder zu umgehen. Bereits bei kleineren Datensätzen und selektiven Abfragen konnte MonetDB, bedingt durch die spaltenbasierte Arbeitsweise, extreme Geschwindigkeitsvorteile erzielen. Dieses Verhalten wurde in Tabelle 2 für einen kleinen Datensatz anhand PostgreSQL und MonetDB dargestellt. Die Performance von MonetDB überstieg dabei die Performance von PostgreSQL um Größenordnungen. Wichtig ist dabei Abfragen gezielt auf einzelne Spalten zu beschränken, bei Abfragen auf die gesamte Zeile relativiert sich der Geschwindigkeitsvorteil. Aufgrund der spaltenbasierten Architektur ist MonetDB nur eine praktikable Lösung für spezielle Daten. Für quantitativ kleinere und weniger spezifische Datenmengen stehen hingegen besser geeignete Generalisten zur Verfügung, die dann unter anderem eine deutlich weiter entwickelte Implementierung des SQL Syntax zur Verfügung stellen.

3.2 Geographische Zuordnung von IP-Adressen

Um eine Lokalisierung der verwendeten IP-Adressen durchzuführen gibt es eine Reihe verschiedener Mögchkeiten. Beispielsweise kann die Lokalisierung einer IP-Adresse anhand des Whois Eintrags ihres Autonomen Systems (AS) bestimmt werden. Dabei tritt jedoch das Problem auf, dass so nur das Land in dem das AS registriert ist bestimmt werden kann, jedoch können einzelne Adressen dem AS zugeordnete auch in anderen Ländern liegen. Um eine genauere Geographische Zuordnung einzelner IP-Adressen durchführen zu können, bieten sich Dienste wie MaxMind [13] an, die Datenbanken mit geolokations Informationen einzelner IP-Adressen zur Verfügung stellen. Im Rahmen der Arbeit wurde dabei auf die kostenfrei erhältlichen GeoLite Datenbanken zurückgegriffen. Um IP-Adressen mit diesen Datenbanken abzugleichen steht eine Reihe verschiedener Wege zur Verfügung. Von uns wurden die MaxMind Datenbanken dabei mittels der Python Bibliothek `pygeoip` [19] verwendet, um IP-Adressen auf die zugehörigen Ländercodes abzubilden.

3.2.1 Probleme

Wenngleich die Genauigkeit der Datenbanken von MaxMind selbst mit 99,8 % [12] angegeben wird, gestaltet sich eine Evaluation dieser Angabe im Rahmen der Arbeit als nicht machbar und muss als Grundwahrheit akzeptiert werden. Davon abgesehen gibt es auch bei einer Fehlerquote von 0.02% bereits rund 86 Millionen fehlerhafte Zuordnungen. Laut Maxmind erhöht sich die Unschärfe bei den Städtedaten monatlich um 1.5%. Es stehen jedoch keine älteren Versionen der Datenbanken zum Download bereit. Somit sind zum Zeitpunkt des Census deutlich erhöhte Fehlerquoten im Bereich zwischen 14% (Messungen Dezember 2012) und 26% (Messungen Mai 2012) möglich. Die so entstehende Fehlerquote wird dabei jedoch nur für Städte angegeben, eine Angabe auf Länderebene fehlt dabei. Der länderübergreifende Fehler wird sich, bedingt durch die deutlich gröbere Auflösung, vermutlich deutlich unter 1,5% befinden. Unter der Hypothese eines Worst-Case Szenarios muss dabei von oben genannter Fehlerquote von 14-26% ausgegangen werden. Seitens MaxMind werden jedoch keine weiteren Details bekannt gegeben, weder wie eine Lokalisierung der Adressen vorgenommen wird, noch wie deren Genauigkeit ermittelt

wird.

3.2.2 Fazit

Prinzipiell stellt die Lokalisierung mittels der GeoIP Datenbanken im Vergleich zur Lokalisierung mittels AS ein genaueres, aber auch unabwägbareres Verfahren zur Verfügung. Bei der Lokalisierung mittels der autonomen Systeme ist eine Fehlerquote bereits prinzipbedingt gegeben. Die Lokalisierung mittels der verfügbaren GeoIP Datenbanken bietet im Gegensatz dazu eine Genauigkeit von bis zu theoretischen 98,2%. Faktisch gesehen ist diese Fehlerquote im hier untersuchten Anwendungsfall jedoch viel zu gering. Eine genauere Abschätzung des Fehlers ist, aufgrund vorher genannter Gründe, nicht möglich.

3.3 Zerlegung von Domainnamen

Die Zerlegung von Domainnamen stellt ein Problem dar, da Top Level Domains oft nicht eindeutig zu identifizieren sind. So ist es nicht trivial aus den Domains „www.test.co.uk“ bzw. „www.test.com“ jeweils den Hostnamen zu identifizieren, da nicht bekannt ist welcher Teil der Domain der Hostname ist. Zum Extrahieren der verschiedenen Domainbestandteile gibt es aber die Möglichkeit auf bekannte Suffix Listen zurückzugreifen. In der hier vorliegenden Arbeit wurde die Python Bibliothek `tldextract` [10] von John Kurkowski zurückgegriffen.

3.3.1 Probleme

Auch wenn ein Großteil der Zerlegungen durch `tldextract` korrekt sind, ist bei Datensätzen mit mehr als 1 Milliarde Zeilen bereits eine Fehlerquote von 1% zu hoch. Bei einfacheren Adressen funktioniert `tldextract` einwandfrei, steigt die Anzahl der Ebenen innerhalb einer Adresse jedoch an, so steigt die Fehlerrate stark an. Im rDNS Datensatze existieren stellenweise auch Domains mit einer Länge von mehr als Hundert Zeichen, bei diesen ist ebenfalls eine sehr hohe Fehlerquote zu verzeichnen.

3.3.2 Fazit

`Tldextract` stellt eine gute Variante da um eine Vorverarbeitung von Adressen zu ermöglichen, aufgrund der hohen Anzahl von Adressen und der hohen Fehlerquote bei komplexeren Adressgebilden sind dennoch umfangreiche händische Nacharbeiten nötig um gut weiterverarbeite Resultate zu erhalten. Je nach gewünschten Ergebnisse kann hier jedoch auf weitere Hilfsmittel, wie beispielsweise Excel zurückgegriffen werden, um eine weitere Aufarbeitung der Daten vorzunehmen.

4. TRACEROUTES

Der erste Datensatz, den wir genauer untersuchen wollen, sind die Traceroutes. Traceroute ist ein Programm, welches es Nutzern ermöglicht den Weg nachzuvollziehen, den ein von dem Quellrechner gesendetes Paket auf dem Weg zu seinem Ziel nimmt. Dazu sendet der Host auf dem Traceroute ausgeführt wird zuerst drei Pakete[7] mit einer Time to Live (TTL) von eins aus, wodurch bei dem ersten Router auf der Strecke zum Ziel die TTL auf null dekrementiert wird und eine ICMP Fehler Nachricht[8] an den Traceroute Host gesendet wird. Traceroute sendet nun drei Pakete mit einer TTL von 2 aus, um so die Antworten des zweiten Routers auf der Strecke zum Ziel zu erhalten, aus denen er jeweils dessen IP-Adresse auslesen kann. Dieses Verfahren wird nun solange wiederholt bis die TTL der Pakete groß genug ist, um ihr Ziel zu erreichen. Der Zielrechner antwortet mit einer ICMP Nachricht [9] aus der erkennbar ist, dass das Ziel erreicht wurde. Die Rückgabe von Traceroute besteht aus allen IP-Adressen die sich auf der Strecke befinden und den zugehörigen Übertragungszeiten.

Nachdem wir einleitend allgemeine Eigenschaften und Probleme der Traceroute Daten betrachten, gehen wir dazu über, die Traceroutes auf IP-, AS- und Länderebene zu analysieren. So betrachten wir bei den IP-Traceroutes die Anzahl von genutzten Geräten, sowie die Ziele der Traceroutes. Desweiteren wollen wir herausfinden, welcher Anteil der IP-Adressen in den Traceroutes unbekannt sind, sowie ihre durchschnittliche Hoplänge betrachten. Bezüglich der Autonomen Systeme beschränken wir uns auf eine Erklärung der Differenz in der Anzahl AS-Nummern auf der Route selbst und als Ziel. Als Schwerpunkt dieses Teils der Arbeit betrachten wir schließlich die Traceroutes auf Länderebene und, unter anderem, klären, welche Länder weltweit am wichtigsten sind für die Internetinfrastruktur, wieviele Länder Traceroutes durchschnittlich auf dem Weg zu ihrem Ziel durchquert haben und ob sich interessante Routenverläufe erkennen lassen.

4.1 Eckdaten

Der Urheber des Internet Census erstellte innerhalb von 23 Tagen insgesamt 68.7 Millionen dieser Traceroutes. Als Quellrechner, von denen aus die Traceroutes gestartet wurden, dienten ihm hierzu rund 275.000 seperate Geräte[10], auf die er mittels Telnet zugreifen konnte, welche allerdings über begrenzte Ressourcen verfügten. So war es auf den so erreichbaren Geräten zwar möglich, das bereits installierte Traceroute Programm auszuführen, allerdings konnte nicht der eigentliche Carna Bot hochgeladen und ausgeführt werden, da Beispielsweise der Speicher nicht ausreichend war. Der Autor modifizierte Carna deswegen so, dass er sich über Telnet auf diese Geräte einloggte, die Traceroutes bei aufrechterhaltener Verbindung durchführte und das Ergebnis auf dem Carna Gerät in komprimierter Form speicherte.

Als Ziele für die Traceroutes dienten ihm dabei IP-Adressen, die bereits einmal auf seinen Telnet-Scanner angesprochen hatten und somit sehr wahrscheinlich noch in Verwendung waren. Insgesamt wurden Traceroutes zu rund 64 Millionen verschiedenen IP-Adressen gesendet. Die Ergebnisse der Traceroutes wurden, wie in Tabelle 1 bereits vorgestellt, abgespeichert.

Die Route setzte sich dabei aus einer Folge von Hop, IP-Adresse und Übertragungszeiten zusammen. Tabelle 3 zeigt einige Beispiele für die Daten. Aus Ressourcengründen mussten wir darauf verzichten, die Traceroutes getrennt nach

[7] Default Einstellung

[8] Typ 11 Time exceeded, Code 0 Time to live exceeded in Transit

[9] Typ 0, Code 0 Echo Reply bzw. bei UDP-basiertem Traceroute mit Typ 3 Destination Unreachable, Code 3 Port Unreachable

[10] Diese Geräte sind nicht Teil der 420.000 Geräte auf denen Carna lief.

doi: 10.2313/NET-2014-03-1_03

Timestamp	Quell-IP	Ziel-IP	Protokoll	Traceroute
1340158500	21.196.75.45	112.172.26.154	ICMP	
1340109900	201.200.74.1	125.99.70.79	ICMP	1:10.86.202.1:30ms,40ms,*;2:10.86.202.1:2540ms,2540ms,*;
1340158500	201.196.75.45	211.104.66.50	ICMP	1:10.39.155.45:40ms,30ms,50ms;2::*,*,*;3::*,*,*;

Tabelle 3: Beispiele für Einträge im Traceroutes Datensatz des Internet Census 2012

verwendetem Protokoll[11] zu untersuchen. Unsere folgenden Auswertungen beziehen sich nur auf Quelle, Ziel und den IP-Adressen auf dem Weg zwischen diesen.

4.2 Mapping auf Autonome Systeme und Länder

Um nicht nur die IP-Adressen der Traceroutes zu betrachten, erzeugten wir zwei weitere Datensätze. Als erstes übersetzten wir die IP-Adressen mittels des Pythonscripts `pyasn` [4] in die Nummern der Autonomen Systeme (AS), denen sie zugeordnet waren. Als Grundlage hierzu dienten uns drei Routing Information Base (RIB) Dateien. Diese spiegeln den Zustand von BGP Routern an 3 Zeitpunkten während des Erstellens der Traceroutes wieder. Dadurch dass wir zum Übersetzen der IP-Adressen in AS-Nummern jeweils die RIB Datei verwendet haben welche dem Timestamp der jeweiligen Traceroute am nächsten war, wollten wir eine möglichst große Genauigkeit gewährleisten.

Als zweites erstellten wir eine Übersetzung der IP-Adressen in Ländercodes, um mit den geographischen Standorten der IP-Adressen arbeiten zu können. Für diese Übersetzung nutzten wir das in Abschnitt 3.2 vorgestellte Verfahren mittels der Pure Python GeoIP API (`pygeoip`) und dem GeoLite Country Datensatz von Maxmind. Tabelle 4 zeigt einen kurzen Überblick darüber, wie viele verschiedene IP-Adressen, AS-Nummern und Ländercodes jeweils als Quelle, Ziel oder innerhalb der Traceroutes existieren, beziehungsweise wie viele insgesamt Vorkommen.

Ort	IPv4 Adressen	Autonome Systeme	Länder
Quelle	275.000	535	100
Route	1.900.000	12.921	199
Ziel	64.700.000	41.332	243
Gesamt	65.800.000	41.335	243

Tabelle 4: Überblick über die Anzahl der verschiedenen IP-Adressen, Autonomen Systeme und Ländercodes, gegliedert nach ihrem Vorkommen

Der enorme Unterschied zwischen der Anzahl der verschiedenen IP-Adressen, AS-Nummern und Ländercodes besonders bei den Zielen und der Route sticht hier besonders hervor. Wir waren in der Lage einige Erklärungen dafür zu finden und stellen diese unter anderem in den passenden Abschnitten 4.4 bis 4.6 vor. Dabei ist natürlich zu beachten, dass sich die Ursachen für die Abweichung auf IP-Ebene auch auf AS- und Länder-Ebene auswirken.

4.3 Probleme des Traceroute Datensatzes

[11]Die Traceroutes wurden per ICMP oder UDP erstellt.

Der Traceroutes Datensatz weist einige Probleme auf, welche die Interpretation der Daten wesentlich erschweren oder gar verhindern. Der Autor gibt so beispielsweise nur darüber Auskunft, welche Daten er gesammelt hat und in welchem Format sie gespeichert wurden. Genauere Details darüber, nach welchen Prinzipien beim Erstellen und Messen der Traceroutes vorgegangen wurde, nennt er allerdings nicht. Dies äußert sich beispielsweise darin, dass Traceroutes mit Quelle und Ziel gespeichert wurden, ohne sicherzustellen, ob sie ihr Ziel überhaupt erreicht hatten. Diese Vermutung wird durch Traceroutes untermauert, welche zwar mit Quelle, Ziel und Route abgespeichert wurden, bei denen aber eindeutig das Ziel nicht erreicht wurde. Erkennen konnten wir das durch die Tatsache, dass die von der entsprechende Traceroute gesendeten Pakete immer wieder zwischen den gleichen zwei verschiedenen IP-Adressen hin und her sprangen und somit zum Zeitpunkt der Messung in eine Routingschleife gerieten.

Eine weitere Auffälligkeit, für die wir ohne genauere Angaben seitens des Autors keine Erklärung finden konnten, ist der Fakt, dass manche Traceroutes mit ihrer Nummerierung nicht mit eins beginnen. Hier war es uns unmöglich zu sagen, welche Gründe das hat. Angesichts dieser Probleme sind die gewonnen Ergebnisse mit Vorsicht zu betrachten und eher als eine Art Trend zu verstehen.

4.4 Auswertung der IP-Adressen

Bevor wir uns der Analyse der Daten auf AS- und Länderebene widmen, betrachten wir einige Auswertungen auf IP-Ebene bezüglich fehlender Adressen und der Länge der Traceroutes.

4.4.1 Allgemeines

In seinem Paper zum Internet Census 2012 [26] nennt der Autor als Fazit seiner Arbeit eine Zahl von ungefähr 1.3 Milliarden genutzten IP-Adressen. Legt man diese als Basis zugrunde, so wurden als Quelle der Traceroutes 0,02% des Internets betrachtet, als Ziel immerhin rund 4,97%. Auf den Routen selbst lagen 0,15% der genutzten IP-Adressen, wenn man die unbekannten IP-Adressen nicht mitzählt, die im folgenden Abschnitt kurz erläutert werden.

4.4.2 Fehlende IP-Adressen auf der Route

Einer der Gründe warum, im Vergleich zu den Ziel-IPs, so viel weniger verschiedene IP-Adressen auf der Route selbst liegen, liegt in der Funktionsweise von Traceroute begründet. So ist es jedem Administrator eines Geräts möglich zu Unterbinden, dass dieses ICMP Fehlermeldungen aussendet, welche Traceroute verwendet um die IP-Adresse des Geräts auf dem Pfad zu bestimmen (siehe Abschnitt 4). In solchen Fällen bleibt die IP des entsprechenden Hops unbekannt, da Traceroute keine Rückmeldung erhält. Tabelle 3 zeigt in Beispiel drei bei den Hops 2 und 3 ein solches Verhalten, die IP-Adressen sind unbekannt und daher leer. Es war

doi: 10.2313/NET-2014-03-1_03

uns unmöglich, diese fehlenden IP-Adressen in die Anzahl der verschiedenen Geräte die sich auf den Routen befinden einzubeziehen. Durchschnittlich waren im Traceroute Datensatz 15,2% der IP-Adressen in den Routen[12] unbekannt, was jeder 6.-7. Adresse entspricht. Aussagen darüber, wieviele verschiedene reale IP-Adressen sich dahinter verstecken lassen sich leider nicht treffen. Bei den Zieladressen trat das Problem der unbekannten IPs nicht auf, da der Autor hier anscheinend einfach die Ziel-IP angegeben hat, ohne sicherzustellen, dass die Traceroute sie auch erreicht hat.

4.4.3 Hops

Schließlich betrachteten wir noch die Anzahl der Hops, die die Traceroutes benötigten, um von der Quelle zu ihrem Ziel zu kommen. Mit einem Hop ist dabei die Anzahl der IP-Adressen gemeint, welche zwischen Quelle und Ziel liegen, inklusive dem Ziel. Der erste Eintrag in dem Traceroute Beispiel in Tabelle 3 hätte dementsprechend einen Hop, der zweite drei. Abbildung 1 zeigt wie viele Einträge im Traceroute Datensatz jeweils wieviele Hops benötigten. Die Anzahl Traceroutes ist hierbei in logarithmischer Form angetragen.

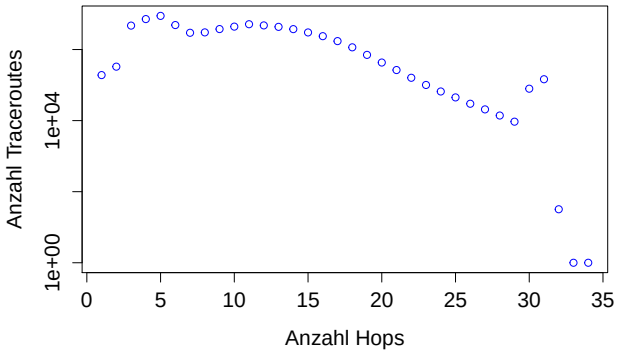


Abbildung 1: Anzahl der Traceroutes nach der Anzahl der Hops von Quelle bis zum Ziel

Aufgefallen ist uns bei diesem Bild vor allem der plötzliche Anstieg an Traceroutes mit 31 beziehungsweise 32 Hops, nachdem bis zu diesem Punkt ein abnehmender Trend in der Anzahl Traceroutes erkennbar war. Unsere Vermutung war, dass sich bei den größeren Hopzahlen vor allem Traceroutes befinden, welche in einer Routingschleife gefangen waren und somit immer zwischen den selben IP-Adressen hin und hersprangen, bis die Time to Live der Pakete 0 erreichte. Normalerweise beträgt die maximale TTL von Paketen (Default Einstellung) die Traceroute aussendet 30, was inklusive Ziel einem Maximum von 31 Hops entspricht. Warum es auch so viele Traceroutes mit 32 Hops (plus jeweils eine mit 33 und 34 Hops) gibt können wir nicht eindeutig erklären, da uns dazu Angaben des Autors des Census fehlen. Möglicherweise liegt der Grund aber in unterschiedlichen Implementierungen von Traceroute auf den übernommenen Geräten. Abbildung 2 zeigt, wie viel Prozent der Traceroutes mit einer bestimmten Hoplänge Routen aufweisen, auf denen die selbe IP-Adresse mehrfach vorkommt.

[12]Die Routen beinhalten nicht Start- und Ziel-IP einer Traceroute.

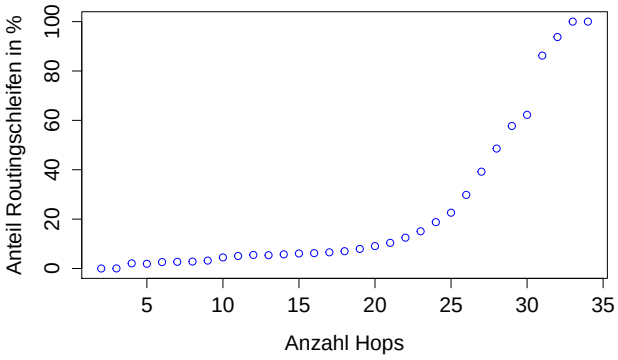


Abbildung 2: Anteil der Traceroutes mit Routingschleifen an gesamten Traceroutes nach Anzahl der Hops von der Quelle bis zum Ziel

Es ist gut zu sehen, dass mit steigender Hopzahl die Wahrscheinlichkeit zunimmt, dass ein Paket in eine Routingschleife gerät. Ab einer Länge von 21 Hops gerieten über 10% der Traceroutes in eine Routingschleife, ab 28 Hops sogar mindestens die Hälfte. Hierbei ist zu beachten, dass wir nur Routingschleifen feststellen konnten, bei denen zumindest eines der an der Schleife beteiligten Geräte auch eine ICMP Fehlermeldung bei ausgelaufener TTL zurück an die Quelle der Traceroute gesendet hat. Sollten alle an einer Schleife beteiligten Geräte ihre Fehlermeldung unterdrückt haben (siehe Abschnitt 4.4.2), konnten wir die Schleife nicht erkennen. Die Prozentwerte der Grafik sind folglich als Mindestwerte zu verstehen. Nutzt man zur Berechnung des Mittelwerts nur jeweils den Anteil an Traceroutes, der keine Schleife enthält, ergibt sich eine durchschnittliche Hopzahl von 9,17 Hops pro Traceroute.

Da eine Routingschleife ein starkes Indiz dafür ist, dass ein gesendetes Paket sein Ziel nicht erreicht hat, lassen sich anhand der Schleifenwahrscheinlichkeiten aus Abbildung 2 Rückschlüsse auf die Traceroutes ziehen, bei denen das im Datensatz angegebene Ziel nicht erreicht wurde. Wir schließen daraus, dass die Aussagekraft der Traceroutes mit steigender Anzahl Hops immer stärker abnimmt, da der Anteil der Routingschleifen für hohe Hopwerte stark ansteigt.

4.5 Auswertung der Autonomen Systeme

Aus Ressourcengründen konnten wir die Autonomen Systeme nicht genauso tiefgehend untersuchen wie die Länder, durch die die Traceroutes verliefen. Allerdings wollten wir zumindest eine Erklärung für die Differenz zwischen der Anzahl AS auf der Route selbst ($\approx$ 13.000) und der Anzahl AS als Ziel der Traceroutes ($\approx$ 41.000) finden.

Aus unserer Sicht deutet diese Differenz darauf hin, dass viele der betroffenen Autonomen Systeme sogenannte Stub- oder Multihomed-AS sind[28]. Das bedeutet, dass diese autonomen Systeme Endpunkte sind, die keinen Verkehr von externen AS an andere externe AS weiterleiten (Transit-AS

doi: 10.2313/NET-2014-03-1_03

). Diese können somit nur als Ziel- oder Quell-AS einer Traceroute vorkommen, nicht aber auf der Route selbst. Die Autonomen Systeme die auf der Route selbst vorkommen sind daher auf jedenfall sogenannte Transit Systeme, die Verkehr von und an andere AS weiterleiten. Ein Beispiel dafür sind Internet Service Provider, wie zum Beispiel die Deutsche Telekom oder AT&T. Der Anteil von Transit-AS an den gesamten AS beträgt somit mindestens 31%. Mindestens deswegen, da wir nicht feststellen können, wie viele der Ziel- und Quell-ASe der Traceroutes wirklich keinen Verkehr weiterleiten.

4.6 Auswertungen auf Länderebene

Von besonderem Interesse für uns waren Auswertungen auf Länderebene. Auf dieser Ebene lassen sich, unter anderem, Schlüsse über die Wege ziehen die Pakete nehmen um von einem Land in ein anderes zu gelangen. Zu beachten gilt hier, dass wen wir von Ländern sprechen alles gemeint ist, was einen Ländercode besitzt. Der Großteil sind durchaus richtige Länder wie Deutschland oder die USA, allerdings haben beispielsweise auch Kontinente Ländercodes.

4.6.1 Herkunft und Ziele

Zur Einführung betrachten wir die Herkunft und die Ziele der Traceroutes des Internet Census 2012. Abbildung 3 veranschaulicht die Länder, aus denen die Traceroutes gestartet wurden.

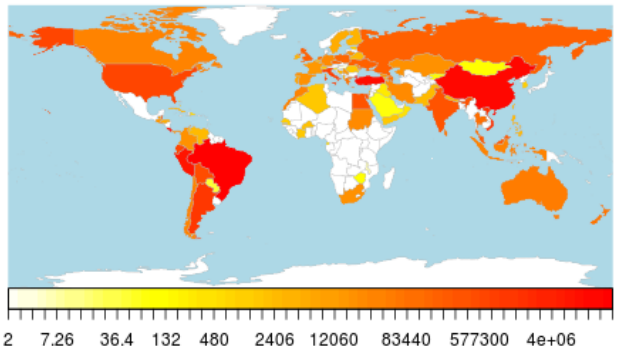


Abbildung 3: Anzahl der Traceroutes die von einem bestimmten Land aus gestartet wurden

Insgesamt wurden für das Erstellen der Traceroutes Geräte aus 100 Ländern genutzt. Tabelle 5 macht hierzu deutlich, dass knapp 50% der im Rahmen des Census erstellten Traceroutes allein aus Brasilien und Costa Rica kommen, beides südamerikanische Länder. Zusammengerechnet sind die Top 5 Länder sogar für knapp 86% der gestarteten Traceroutes verantwortlich.

Land	Anzahl	Anteil Gesamt
Brasilien	20.000.000	29,1%
Costa Rica	13.900.000	20,1%
China	10.600.00	15,4%
Türkei	8.500.00	12,4%
Peru	6.100.00	8,9%

Tabelle 5: Top 5 der Quellenländer für Traceroutes

Abbildung 4 zeigt die Zielländer der Traceroutes und analog dazu Tabelle 6 die Top 5.

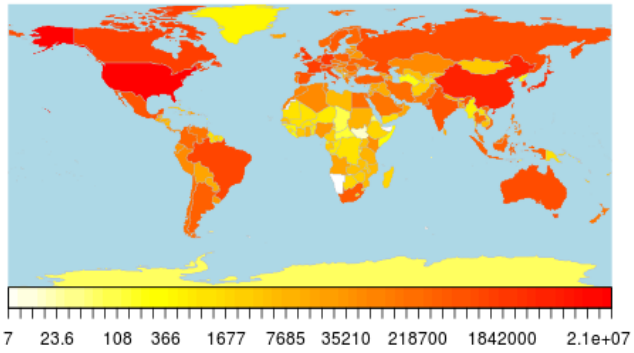


Abbildung 4: Anzahl der Traceroutes die an ein bestimmtes Land gesendet wurden

Land	Anzahl	Anteil Gesamt
USA	28.500.000	40,1%
China	6.200.000	9%
Japan	3.800.000	5,5%
unbekannt	3.500.000	5,1%
Großbritannien	2.300.000	3,3%

Tabelle 6: Top 5 der Zielländer für Traceroutes

Hier sticht einerseits der hohe Anteil an Zielen in die USA ins Auge, andererseits die „unbekannten“ Ziele. Mit unbekannten Zielen beziehen wir uns auf IP-Adressen in den Zielen der Traceroutes, welche mittels der Maxmind GeoIP Daten nicht einem Land zugeordnet werden konnten. Auf die vielen Ziele in den USA werden wir im Folgeabschnitt kurz eingehen.

4.6.2 Anteil betroffener IP-Adressen pro Land

Wesentlich interessanter als die Anzahl der gesamten gestarteten und ankommenden Traceroutes von, beziehungsweise in ein Land erschien uns die Frage, welcher Anteil von verschiedenen IP-Adressen pro Land von den Traceroutes genutzt wurden. Hierzu betrachteten wir zuerst jede IP-Adresse nur einmalig, unabhängig wie oft sie tatsächlich als Quelle oder Ziel einer Route vorkam. Die daraus gewonnene Anzahl betroffener IP-Adressen pro Land normalisierten wir dann mithilfe der Anzahl der dem Land zugeordneten IP-Adressen. Als Quelle der jedem Land zugeordneten IP-Adressen verwendeten wir wieder einen von Maxmind zur Verfügung gestellten Datensatz[14]. Abbildung 5 zeigt dazu, wieviel Prozent der IP-Adressen pro Land als Quelle für Traceroutes dienten.

Dies ist insbesondere deshalb interessant, da der Autor des Census die Traceroutes auf Geräten ausgeführt hat, die einerseits über relativ beschränkte Ressourcen verfügten und andererseits durch einen einfachen Telnet Login benutzt werden konnten. Die Abbildung gibt somit nicht nur einen Überblick über die betroffenen Geräte, sondern zeigt darüber hinaus den Anteil an leicht angreifbaren Geräten[13]. Hierbei ist

[13]Wie bereits erwähnt verwendete der Autor nicht alle angreifbaren Geräte, die wahren Zahlen dürften also noch größer ausfallen.

doi: 10.2313/NET-2014-03-1_03

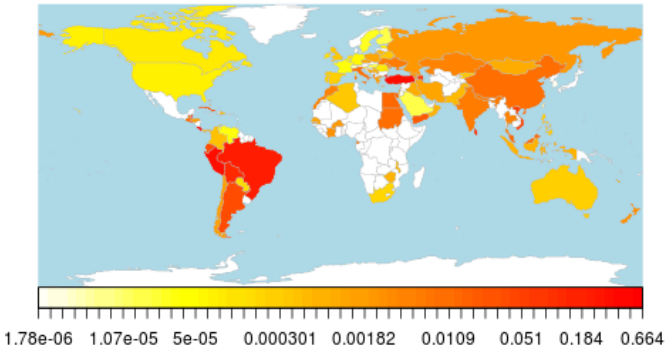


Abbildung 5: Anteil der pro Land betroffenen verschiedenen IP-Adressen als Quelle gegenüber den dem Land zugeordneten IP-Adressen in Prozent

zu beachten, dass weiße Länder auf der Karte nicht zwangsläufig als „sicher“ zu betrachten sind sondern als unbekannt, da aus diesen keine Geräte übernommen wurden. So scheint vor allem Südamerika im Vergleich zum Rest der Welt relativ viele unsichere Geräte zu verwenden, gefolgt von Asien. Europa und Nordamerika hingegen scheinen in dieser Hinsicht vergleichsweise sicher zu sein.

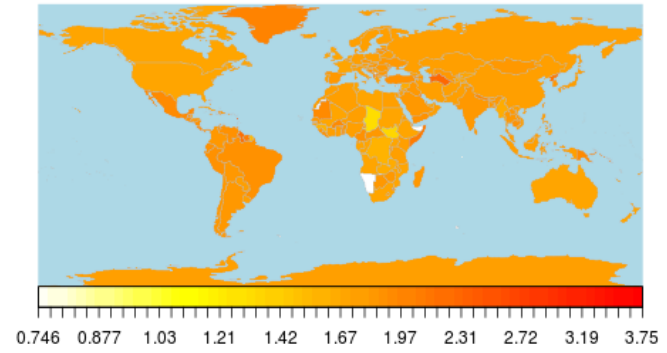


Abbildung 6: Anteil der pro Land betroffenen verschiedenen IP-Adressen als Ziel gegenüber den dem Land zugeordneten IP-Adressen in Prozent

Abbildung 6 zeigt schließlich den Anteil der IP-Adressen eines Landes, welcher als Ziel von mindestens einer Traceroute diente. Hier zeigt sich, dass der im letzten Abschnitt bemerkte große Anteil an Zielen in den USA (40,1%), bezogen auf die Anzahl der den USA zugeordneten IP-Adressen(knapp 1,6 Mrd.[14]), gar nicht so groß ist. Vom Großteil der Länder wurden durchschnittlich zwischen 1,7% und 2% der zugeordneten IP-Adressen adressiert.

4.6.3 Hops

Analog zu den Hops auf IP-Adressebene (siehe Abschnitt 4.4.3) betrachteten wir auch die Hoplänge auf Länderebene. Das bedeutet in diesem Fall die Anzahl der Länder die an einer Traceroute beteiligt waren. Im Unterschied zu den IP-Adressen zählten wir hier also auch das Land aus dem die Traceroute gestartet wurde dazu. Eine Traceroute von Brasilien über Spanien in die USA hätte somit einen Hopwert von 3. Wir betrachteten hierzu nur die Traceroutes, bei denen Start- und Zielland bekannt waren und bei denen nicht alle IP-Adressen auf der IP,Trace unbekannt waren (nicht alle IP-Adressen konnten Länder zugeordnet werden, siehe Abschnitt 3.2). Auch hier berechneten wir, wieviele der Tracroutes, die über eine bestimmte Anzahl von Ländern gehen, eine Routingschleife auf ihrer zugehörigen IP-Trace aufwiesen. Auf Länderebene können Wiederholungen des selben Landes durchaus vorkommen, weswegen uns eine Schleifenerkennung auf dieser Ebene nicht sinnvoll vorkam. Ein Beispiel für eine vermeintliche Schleife auf Länderebene wäre eine Traceroute von Brasilien nach Alaska, auf der die USA doppelt vorkommen (BR->US->CA->US(Alaska)).

[14]Das entspricht ca. 45% der gesamten zugeteilten IP-Adressen.

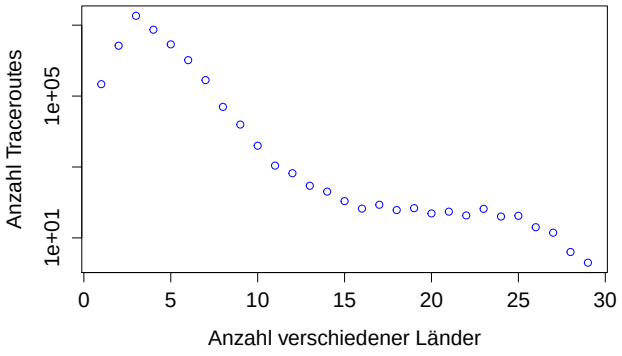


Abbildung 7: Anzahl der Traceroutes nach der Anzahl der Länder von Start- bis zum Zielland

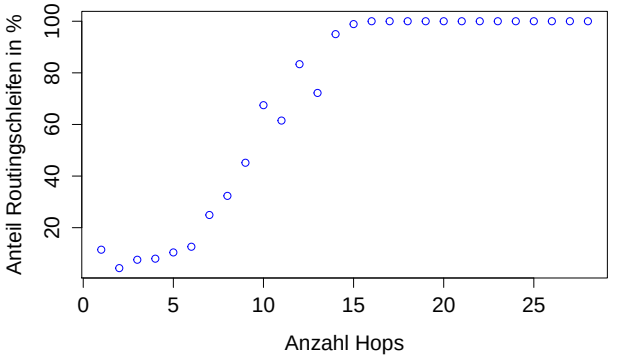


Abbildung 8: Anteil der Traceroutes mit Routingschleifen an gesamten Traceroutes nach Anzahl der Länderhops von Start- bis zum Zielland

Abbildung 7 zeigt wie viele Traceroutes jeweils eine bestimmte Anzahl an Ländern beinhalten. Im Gegensatz zu der Hopzahl bei den IP-Traceroutes, ist hier schon relativ schnell ein Abfall in der Anzahl Traceroutes mit höherem Länder Hopcount zu beobachten. Noch klarer ersichtlich wird dies, wenn man den Anteil an Routingschleifen in Abhängigkeit von der Länderzahl mit einbeieht (Abb. 8). Betrachtet man beide Abbildungen zusammen, sieht man dass der Großteil

der Traceroutes, die sehr wahrscheinlich ihr Ziel erreicht haben, weniger als ungefähr 7 mal das Land wechselten. Der Mittelwert der Anzahl beteiligter Länder an den Traceroutes ohne Schleifen betrug 3,44.

4.6.4 *Interessante Traceroute Verläufe*

Abschließend betrachteten wir auch noch die Strecken selbst, welche Pakete von einem Land in ein anderes nahmen. Einleitend zeigt Abbildung 9 wie oft die verschiedenen Länder auf den Routen (also nicht als Quelle oder Ziel) vorkommen.

Hier ist zu sehen, dass die USA eine wichtige Rolle im Internetverkehr spielt, da sie in vergleichsweise vielen Traceroutes vorkommt (≈ 23%). Auf Platz zwei folgen einige europäische Länder sowie Europa[15] selbst mit 3%-12.5%.

TeleGeography [22] hat eine Karte erstellt, welche alle Unterseekabel enthält die momentan[16] aktiv sind[23]. Auf dieser ist zu erkennen, dass vor allem die Länder häufig in den Traceroutes vorkommen, die eine gute Anbindung an Unterseekabel vorweisen können. Gut zu sehen ist dies auch an den afrikanischen Ländern, von denen fast nur Küstenländer vertreten sind. Auch zu erkennen ist, dass vor allem Afrika für die Differenz der Länderzahl zwischen Ländern auf den Routen (199) und Ländern als Ziel (243) verantwortlich ist, die in Tabelle 4 gezeigt wird. Tabelle 7 zeigt einen Überblick über die am meisten vertretenen Strecken im Traceroute Datensatz.

Ursprung	Ziel	Anzahl
Brasilien	USA	8.300.000
Costa Rica	USA	5.700.000
China	USA	4.400.000
Türkei	USA	3.500.000
Peru	USA	2.500.000

Tabelle 7: Top 5 der Strecken für Traceroutes

Da die GeoIP Daten von Maxmind einen nicht genauer bekannten Fehler aufweisen, entschieden wir uns, nur Länder zu betrachten, die an einer Route mit mindestens 1% an der Summe der Vorkommen aller Länder beteiligt sind.

Als erstes Beispiel suchten wir uns den größten Datensatz mit den Traceroutes von Brasilien in die USA aus und sind auf eine auf den ersten Blick überraschende Tatsache gestoßen. Abbildung 10 zeigt die Länder die Pakete auf dieser Route durchquert haben.

Wir hätten erwartet, dass Pakete entweder von Brasilien aus den direkten Weg in die USA über ein Unterseekabel nehmen oder eventuell noch über die schmale Landbrücke zwischen Nord- und Südamerika gehen. Interessanterweise geht aber ein relativ großer Anteil(≈ 26%) erst nach Spanien, bevor die Pakete über das nächste Unterseekabel zurück nach Amerika gesendet werden. Die Landbrücke wird hingegen gar nicht genutzt. Pakete von USA nach Brasilien nehmen den umgekehrten Weg, allerdings verlaufen nur noch ≈ 14% über Spanien. Kanadas Beteiligung ist unserer

[15] Wie erwähnt hat Europa einen eigenen Coutry Code (EU), den wir nicht auf der Karte abbilden konnten.
[16] Letzter Stand 17.September 2013.

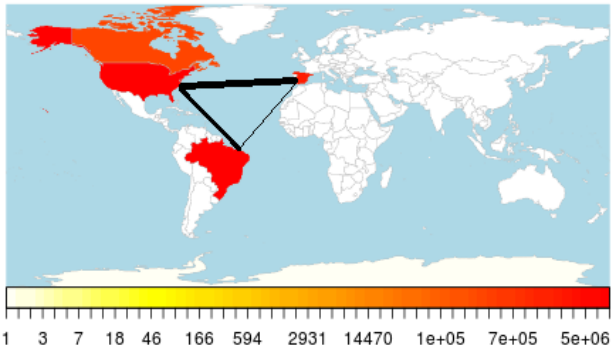


Abbildung 10: Anzahl Beteiligungen von Ländern an Routen von Brasilien in die USA

Meinung nach den Paketen geschuldet die an IP-Adressen in Alaska gesendet wurden. Aus Ressourcengründen war es uns leider nicht möglich eine genauere Auflösung als auf Länderebene vorzunehmen. Auf der Unterseekabelkarte [23] von Telegeography [22] ist zu sehen, dass Brasilien eigentlich relativ gut an die USA angebunden ist, wohingegen Spanien nur über ein einziges Unterseekabel erreichbar ist.

Eine mögliche Erklärung für den Umweg über Spanien könnte der Fakt sein, dass Routingentscheidungen unter anderem auch auf finanzielle Aspekten beruhen und nicht unbedingt nur auf geographischen. Internetanbieter die Pakete über Verbindungen anderer Anbieter routen, müssen diesen häufig Gebühren zahlen. Von daher wird versucht Pakete möglichst über eigene Routen zu versenden, so dass diese Zusatzgebühren möglichst gering ausfallen. Für die Verbindung Brasilien über Spanien in die USA vermuten wir, dass die starke Vertretung von Telefónica in Brasilien und Spanien ein Grund dafür ist, dass die Pakete nicht alle direkt in die USA gesendet werden. Telefónica ist teilweise Miteigentümer eines Unterseekabel jeweils zwischen Brasilien und Spanien, sowie eines weiteren zwischen Spanien und den USA. Daher die Vermutung, dass Telefónica[17] diese Unterseekabel nutzt, um im Vergleich zur direkten Verbindung Kosten einzusparen. In Abbildung 10 wurden die Unterseekabelverbindungen die hier relevant sind schematisch eingetragen, die Dicke der Striche steht hier für die Anzahl der Kabel, nicht zwangsläufig deren Kapazität.

Ebenfalls interessant ist der Verkehr von China nach Deutschland und umgekehrt. So verlaufen rund 17% der Traceroutes von China nach Deutschland über die USA, in umgedrehter Richtung sind es sogar rund 23%. Die beteiligten Länder der Traceroutes von China nach Deutschland sind in Abbildung 11 zu sehen.

Auffällig ist hierbei auch der Fakt, dass ein relativ großer Teil der Daten den direkten Weg ohne Zwischenstationen nimmt. Auch hier scheint der Datenverkehr über ein Unterseekabel abgewickelt zu werden, welches, unter anderem, Deutschland und China direkt verbindet (SeaMeWe-3 [23]).

4.6.5 *Fazit*

[17] Telefónica dient hier vor allem als Beispiel, es kann natürlich noch andere Gründe geben.

doi: 10.2313/NET-2014-03-1_03

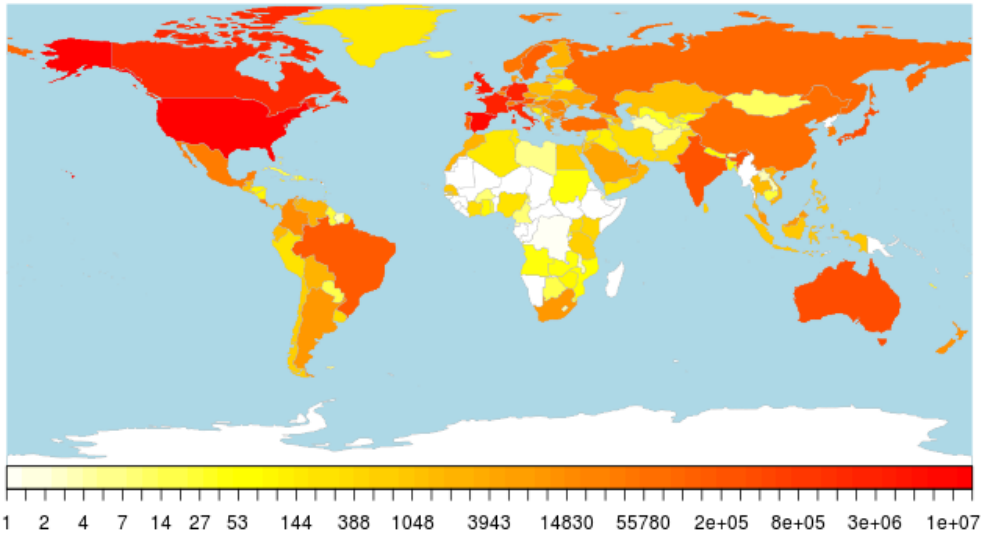


Abbildung 9: Anzahl Beteiligungen von Ländern an allen Traceroutes ohne Start- und Zielland

Zusammenfassend lassen sich aus dem Traceroute Datensatz einige interessante Schlüsse ziehen, beziehungsweise bekannte Vermutungen bestätigen. So sind Nordamerika und Europa Infrastrukturmäßig enorm wichtig für das Internet, viele Pakete werden durch Länder dieser Kontinente gesendet. Ebenfalls interessant sind Südamerika und Asien. Viele Länder in diesen Regionen sind durchaus wichtig für das Internet, allerdings zeigen die Traceroute Daten, dass in diesen Gebieten noch besonders viele Geräte durch einfaches Passwortraten angreifbar sind. Afrika hingegen ist aus Internetsicht noch relativ unerschlossen. Desweiteren sahen wir, dass Pakete um an ihr Ziel zu kommen nicht immer den geographisch gesehen kürzesten Weg nehmen, sondern unter Umständen auch Umwege machen um beispielsweise finanziellen Aspekten gerecht zu werden.

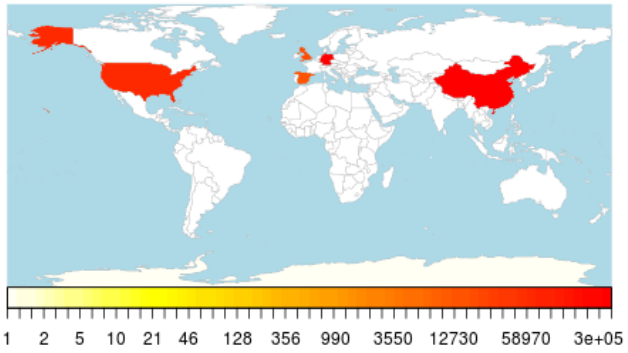


Abbildung 11: Anzahl Beteiligungen von Ländern an Routen von China nach Deutschland

5. RDNS

Das Domain Name System (DNS) ist eine zentrale Datenbank des Internets um eine Abbildung von Namen auf IP-Adressen zu ermöglichen. Dabei kann eine einzelne Domain auf verschiedene IP-Adressen zeigen und eine IP-Adresse kann mehreren Domain Namen zugeordnet sein. Die Zuordnung einzelner IP-Adressen zu deren Domains wird dabei als rDNS (reverse DNS) bezeichnet. Im Rahmen des Internet Census wurde dabei für einen großen Bereich des IPv4 Adressraums der jeweilige reverse DNS Eintrag bestimmt und abgespeichert. Im weiteren Verlauf des Kapitels erfolgt eine Analyse der Daten.

Für das Resultat einer rDNS Abfrage gibt es verschiedene Optionen. Ist ein rDNS Eintrag hinterlegt wird dieser in Form eines Hosts zurückgegeben. Falls kein Eintrag gefunden wurde, wird der Fehlercode (3) zurückgegeben. Eine leere Antwort kann entweder keiner Antwort oder keinem gefundenem Host entsprechen. Darüber hinaus existieren noch eine Reihe weiterer Fehlercodes die in Tabelle 8 näher spezifiziert werden.

5.1 Zahlen und Fakten

Während des Internet Census 2012 wurden im Gesamten 10,5 Milliarden Anfragen bezüglich des rDNS Eintrages gestellt, somit wurde jede verfügbare IP-Adresse im Durchschnitt 2,45 mal abgefragt. Insgesamt wurden dabei 3.7 Milliarden verschiedene IPs abgefragt, was einer Abdeckung von rund 86% entspricht (inkl. privater Blöcke). Von diesen 10,5 Milliarden Anfragen erhielten ca 2.8 Milliarden eine Antwort mit gesetzter rDNS Domain. Dies entspricht einem Anteil von $\approx$ 26%. Folglich lieferten rund 7.8 Milliarden ($\approx$ 76%) angefragte Host Adressen einen Fehlercode, keine oder eine leere Antwort. Über die Antworten mit leerer Nachricht ($\approx 41,7$ Millionen) kann, mangels fehlender Information, keine Aussage getroffen ob deren rDNS Eintrag leer ist, oder der entsprechende Host nicht geantwortet hat. Die Verteilung der Fehlercodes kann in Tabelle 9 betrachtet werden. Weiterhin auffallend ist: Einige der zurückgegeben Fehlercodes sind innerhalb der entsprechenden manpages nicht dokumentiert.

Auffällig ist, dass sämtliche gewonnen Daten deutlich von den „offiziellen“ Daten innerhalb der ursprünglichen Veröffentlichung abweichen. Da jedoch nichts über die genaue Art der Gewinnung der offiziellen Daten bekannt ist, kann nur

doi: 10.2313/NET-2014-03-1_03

Code	Nachricht
0	No error condition.
1	The name server was unable to interpret the query.
2	The name server was unable to process this query due to a problem with the name server.
3	The domain name does not exist
4	The name server does not support the requested kind of query.
5	The name server refuses to reform the specified operation for policy reasons.
65	The reply was truncated or ill-formated.
66	An unknown error occurred.
67	Communication with the server timed out.
68	The request was canceled because the DNS subsystem was shut down.

Tabelle 8: rDNS Fehler Meldungen [6]

gemutmaßt werden wie diese Abweichungen nach Oben (bis maximal Faktor 3) auftreten können. Eine mögliche Ursache ist der untersuchte Zeitraum: Der Autor schreibt in seiner Veröffentlichung, dass nur Messungen zwischen Mai und Oktober berücksichtigt werden. Im Oktober wurden jedoch noch weitere reverse DNS Messungen durchgeführt. Somit ist es wahrscheinlich, dass der hier untersuchte Datensatz signifikant Größer als der (noch nicht vollständige) Datensatz des Autors ist.

Fehlercode	#	%
2	1.690.584.869	21,85
3	5.885.552.163	76,08
5	11.603	0,00015
65	111.054	0,0014
66	1.256.886	0,02
67	40.038.354	0,52
70	118.858.282	1,54

Tabelle 9: Verteilung der Fehlercodes von rDNS Anfragen

5.2 Auswertungen

Aus der Datenbank können eine Reihe verschiedener Daten extrahiert werden, die im folgenden kurz vorgestellt werden. Eine Interpretation und weiterführende Auswertung der Daten wird anschließend im nächsten Abschnitt vorgenommen.

Im Verlauf der Arbeit muss beachtet werden, dass sämtliche Daten über einzelne IP-Adressen genommen wurde. Der Datensatz der reverse DNS Daten umfasst mehr als 10 Milliarden Einträge, eine Speicherung der Daten in eine Tabelle war nicht möglich, da der verfügbare Arbeitsspeicher nicht ausreichte um die gesamte Datenmenge laden zu können. Bedingt dadurch konnten mehrfach vorhanden Domains nicht gefiltert werden und somit entsteht eine gewisse Unschärfe in den Daten. Bei mehr als 10 Milliarden Datensätzen kann jedoch davon ausgegangen werden, dass bedingt durch das Gesetz der großen Zahlen [21] eine starke Korrelation zwischen den absoluten und relativen Werten vorhanden ist.

Weiterhin ist es, aufgrund der Verschlossenheit seitens MaxMind, nicht möglich, detaillierte Aussagen über die Genauigkeit der geographischen Positionen der Domains zu treffen. Es ist weder bekannt wie die Positionen bestimmt werden, noch wie die zugehörigen Fehlerraten ermittelt werden. Um qualitative Aussagen über die nachfolgenden Daten treffen zu können, wäre dies aber unabdingbar.

Begonnen wird zunächst mit der einfachsten Form der Auswertung, einer Abbildung der lokalisierten Domains in die zugehörigen Länder. Siehe hierzu die Abbildung 12 und die zugehörige Tabelle 10. In dieser Ansicht werden dabei nur distinkte Domains betrachtet, somit werden mehrfach genutzte Domains (zum Beispiel dynamische Hosts von Internetzugängen) ignoriert.

Land	# IPs
USA	975.064.787
Japan	282.994.662
Deutschland	138.511.437
Großbritannien	127.073.049
Frankreich	110.419.032
Italien	87.925.156
Niederlande	70.746.202
China	70.081.097
Brasilien	68.774.971
Spanien	62.006.960

Tabelle 10: Top 10 der Länder mit den meisten rDNS Einträgen

Aus der Anzahl der rDNS Einträge pro Land lassen sich Rückschlüsse über die Verbreitung des Internets in den einzelnen Ländern getroffen werden. Ausführungen hierzu werden in Abbildung 13 und der Top 10 Tabelle 11 dargestellt.

Land	Domains/Bewohner
Schweden	4,36
Norwegen	4,30
Niederlande	4,20
Finnland	3,36
USA	3,11
Dänemark	2,72
Taiwan	2,56
Japan	2,24
Schweiz	2,20
Australien	2,17

Tabelle 11: Top 10 Anzahl der Länder mit den meisten rDNS Einträgen pro Person, es werden nur Länder mit mehr als 1 Mio Einwohner angetragen

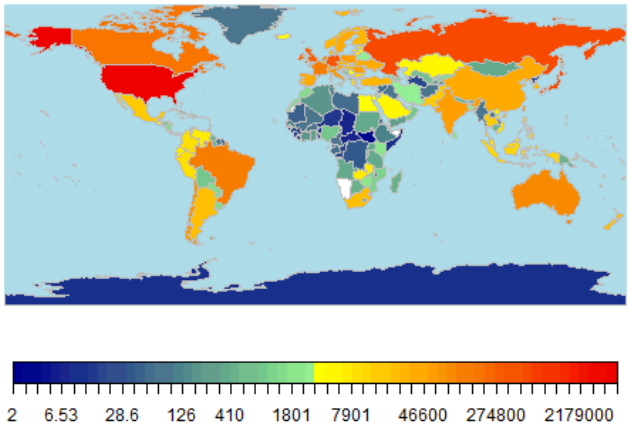


Abbildung 12: Absolute Anzahl der distinkten Domains pro Land

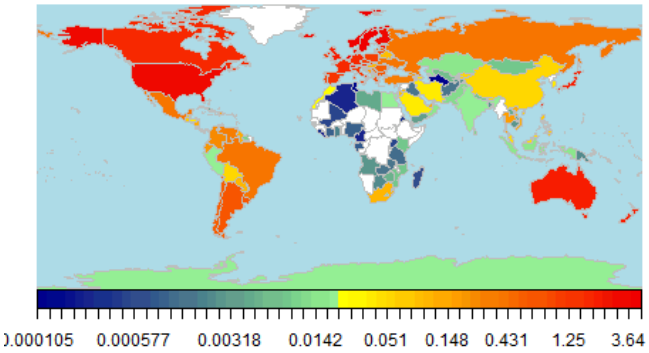


Abbildung 13: Verhältnis Domains pro Einwohner, Länder mit einem Verhältnis von weniger als 10^{-5} Domains pro Person sind weiß dargestellt.

Weiterhin gibt es durch den Datensatz auch die Möglichkeit, die Abhängigkeit einzelner Staaten voneinander darzustellen. Hierfür gibt es zwei verschiedene Varianten. Eine Variante wird in Tabelle 12 und Abbildung 14 gezeigt. Dabei wird anhand des Beispiels der USA gezeigt wie stark einzelne Staaten vom jeweiligen Land abhängig sind. Bei den Auswertungen dieser Abhängigkeiten werden im folgenden nur distinkte Domainnamen herangezogen.

Auch eine Invertierung dieser Ansicht bietet interessante Einblicke in die Infrastruktur verschiedener Länder. Daraus können dann Rückschlüsse über den Einsatzzweck, aber auch diplomatische Beziehungen beziehungsweise Vertrauensverhältnisse gezogen werden. Dies wird anhand der Domains von Deutschland, Togo und Nordkorea gezeigt (siehe hierzu die Abbildungen 15, 16 und 17).

Im Zuge des PRISM [24] Skandals wird abschließend noch eine Analyse über die „5 Eyes“ [5] durchgeführt, deren Resultate aus der Tabelle 14 gezogen werden. Da in dieser Auswertung erneut eine Betrachtung einzelner Hosts von Interesse ist, wird die Auswertung unter Berücksichtigung dynamischer IP Adressen durchgeführt.

5.3 Interpretation

Die einfachste Möglichkeit der Auswertung auf Basis der absoluten Werte der Domains in den verschiedenen Ländern bringt kaum Überraschungen mit sich. Es zeigt sich eine klare Dominanz der westlichen Industrienationen. 9 der 10 Länder sind diesen zugehörigen und stellen die Heimat für 1,7 Milliarden Domains, was einem Anteil von $\approx$ 62% an allen aufgelösten IP-Adressen darstellt.

Wenn die so gewonnen Daten jedoch einer Normalisierung über die aktuelle Einwohnerzahl [1] unterzogen werden, ergeben sich interessante neue Aspekte. So heben sich dann besonders hochtechnisierte Länder wie Taiwan hervor. Aber auch die skandinavischen Länder, die sich zum Zeitpunkt des Census durch eine sehr liberale Haltung bezüglich Urheberrechts und Meinungsfreiheitssachen ausgezeichnet haben, sind in dieser Statistik in den führenden Positionen vertreten. Weiterhin ist auffallend, dass weder Deutschland, Frankreich, noch England in dieser Darstellung in einer der führenden Rollen vertreten sind, obwohl diese Länder innerhalb Europas mithin die wirtschaftlich leistungsfähigsten Staaten darstellen.

Aus der Abhängigkeitsdarstellung einzelner Staaten anhand der USA ergeben sich sodann auch einige interessante Faktoren. So ist zum Beispiel eine protektive Nutzung dieser Abhängigkeit durchaus möglich, aber auch offensiv-aggressive Handlungen sind aus einer zu großen Abhängigkeit möglich. Protektion könnte beispielsweise durch die Auslagerung bzw. redundante Haltung kritischer Systeme durch schützende Nationen erfolgen. So könnte eine tiefgreifende technische Kontrolle, bedingt durch die Abhängigkeit in der Internet Infrastruktur, genutzt werden um unmittelbaren diplomatischen Zwang anzuwenden. Die Resultate am Beispiel der USA werden im Folgenden kurz dargestellt:

Besonders auffällig ist hierbei die sehr starke Abhängigkeit einiger Staaten Afrikas. Aber auch die sehr schwache Abhängigkeit einiger Staaten, beispielsweise sei hier Israel genannt ist auffällig. Obwohl politisch eine tiefe Verbundenheit zwischen den USA und Israel zu beobachten ist, ist nur ein Bruchteil ($< 1\%$) israelischer Domains in den USA gehostet. Die Erklärung dieses Phänomens dürfte aber in der sehr starken technischen Infrastruktur Israels liegen, so dass grundsätzlich kein Bedarf für eine Abhängigkeit Israels von anderen Ländern besteht.

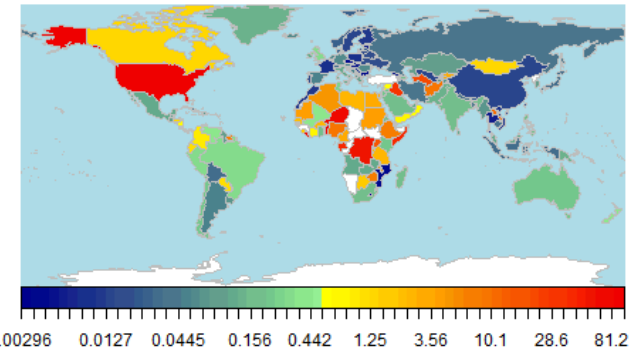


Abbildung 14: Landkarte zur Abhängigkeit einzelner Staaten von den USA in %

doi: 10.2313/NET-2014-03-1_03

Land USA	Domains Total	Domains	Abhängigkeit [%]
USA	6.465.676	6.491.618	99,60
IO	275.933	284.817	96,88
Niederlande	891	1.111	80,20
Rrasilien	9.465	12.284	77,05
Kongo	2.686	4.998	53,74
Jungferninseln	708	1.450	48,83
West-Samoa	20.379	48.317	42,18
Südgeorgien	569	1.463	38,89
Kokosinseln	50.862	130.823	38,88
VC	374	1.057	35,38
Montenegro	10.992	33.947	32,38

Tabelle 12: Top 10 der Länder (zu lange Namen sind mit dem Country Code abgekürzt) mit den Prozentual am meisten in den USA gehosteten Domains, US selbst als Vergleich.

Aber auch die inverse Betrachtungsweise kann interessante Fakten offenbaren. Mit dieser Ansicht können dann Rückschlüsse darüber gezogen werden, welchen Ländern ein Land *A* Teile seiner, mehr oder weniger, kritischen Infrastruktur anvertraut. Auch ein Outsourcing zum Zwecke von Zensurmaßnahmen ist dabei denkbar. Im folgenden Beispiel wird dies anhand Deutschlands veranschaulicht. Naheliegend ist, dass der größte Anteil der länderspezifischen Domains im Heimatland der jeweiligen Domain gehostet wird. Im Falle von Deutschland sind dies mehr als 90%. Somit wäre es beispielsweise für die deutsche Regierung ein leichtes weitreichende Zensurmaßnahmen über den Zugriff auf deutsche Rechenzentrumsbetreiber zu realisieren, da nur innerhalb der eigenen Staatsgrenzen Zwang ausgeübt werden müsste.

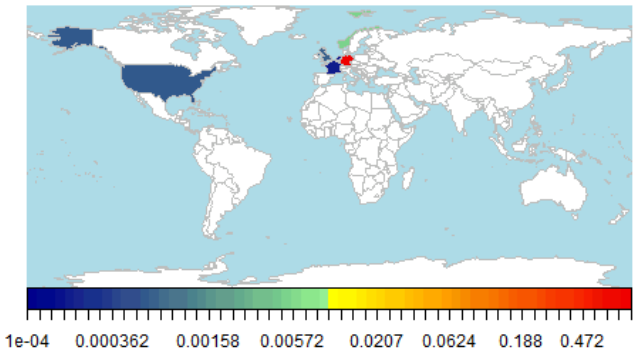


Abbildung 15: Landkarte zur Verteilung von .de Domains über verschiedene Länder in %

Ein gegenteiliges Beispiel, mit einer sehr homogen Verteilen über die einzelnen Ländern stellt die Domain Endung „.to“ [25] von Togo in Abbildung 16 dar. “.to“-Domains sind relativ gleichmäßig über viele verschiedene Länder verteilt. Ursächlich für dies sind aber eher nicht diplomatische Gründe, sondern liegen im Registrierungsprozess der „.to“-Domains begründet. Bei „.to“-Domains ist keine whois Abfrage möglich, sodass der Eigentümer der jeweiligen Domain einen gewissen Grad an Anonymität genießt. Aus diesem Grund werden to Domains oftmals für Webseiten am Rande der Legalität genutzt.

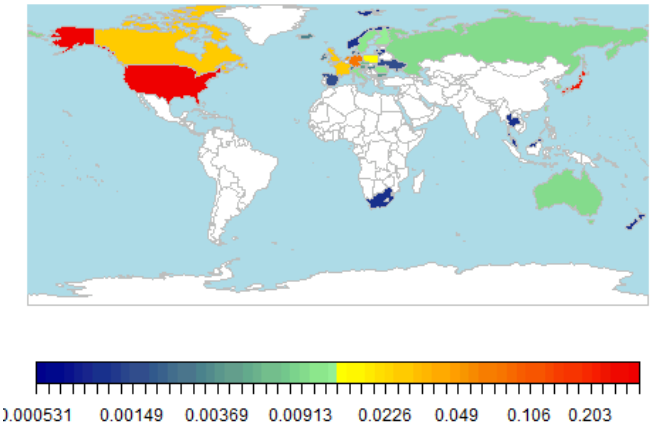


Abbildung 16: Landkarte zur Verteilung von .to Domains über verschiedene Länder in %

Eine sehr interessante Fragestellung fokussiert die geographische Verteilung von Domains diplomatisch isolierter Staaten. Im folgenden Beispiel wird dabei Nordkorea mit der Landesdomain „.kp“ untersucht. Nordkorea ist international weitestgehend diplomatisch isoliert. Nordkorea hat dabei nur einen sehr kleinen Adressblock mit gesamt 1024 IP-Adressen [29]. Bedingt dadurch sind die meisten der Verfügbaren Domains staatlicher Natur - die interessantere Fragestellung ist dabei aber: Welche Länder stellen Nord Korea Kapazitäten zur Verfügung und brechen somit die fast weltweiten (China hat keine Embargos gegen Nordkorea) Embargos. Die Beurteilung, ob faktisch auch ein Bruch der Embargos vorliegt kann dabei von uns nicht abschließend beurteilt werden, da diese Fragestellung komplexe völkerrechtliche Aspekte mit sich bringt [3]. Wie in der Abbildung 17 und der Tabelle 13 zu sehen ist, gibt es bei der Anzahl der nordkoreanischen IPs keine Überraschungen. Hinter den im aufgeführten IP-Adressen steckt dabei hauptsächlich technische Infrastruktur oder regierungsnahe Adressen. Ebenfalls wenig überraschend ist der Fakt, dass keine der Domains oder IP-Adressen von einem deutschen Internetzugang erreichbar ist. Interessanter ist die Domain, die einen großen, internationalen Lieferdienst vermuten lässt, welcher aber seinen Dienst in Nord Korea bereits seit mindestens 2011 wieder eingestellt hat [27], jedoch der zugehörige DNS Eintrag weiterhin vorhanden ist. Weiterhin ist bemerkenswert, dass keinerlei „.nk“ Domains auf chinesischen IP Adressen erreichbar sind, aufgrund der Verbundenheit Nordkoreas mit China [9] wäre dies tendenziell zu erwarten gewesen.

Im Hinblick auf den kürzlichen Spionageskandal der NSA [24] ergibt sich aus dem Census die Möglichkeit, den direkten Zugriffe der großen Geheimdienste, den „Five Eyes“ [5] abzuschätzen. Diese fünf Geheimdienste umfassen dabei die Länder: USA (NSA), England (GCHQ), Neuseeland (GCSB), Australien (DSD) und Kanada (CSEC). Über die genauen Details dieses Zusammenschlusses ist nur wenig bekannt, da die zu Grunde liegenden Verträge geheim sind. Es wird jedoch davon ausgegangen, dass die 5 Augen Einsicht in die gesamten Geheimdienstdaten aller beteiligter Staaten

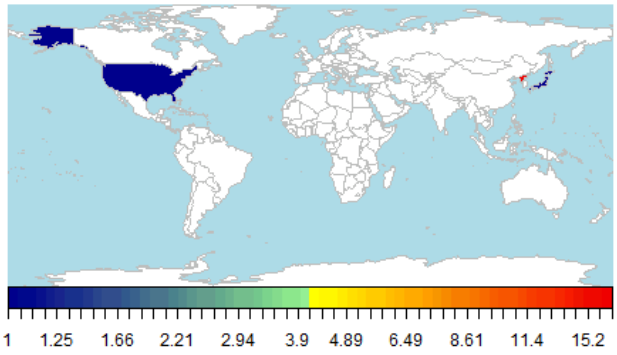


Abbildung 17: Landkarte über die Verteilung nordkoreanischer Domains

#	Domain	Land
1	kita.no.kuni.kara.-83-winter.kp	JP
1	www.globalbusiness.ups.kp	US
1	spinef1.star.net.kp	KP
2	ns1.kptc.kp	KP
2	ns2.kptc.kp	KP
1	mail.silibank.net.kp	KP
2	naenara.com.kp	KP
4	smtp.star-co.net.kp	KP
1	ns1.star.edu.kp	KP
4	mail.star.edu.kp	KP

Tabelle 13: Übersicht über die gesammelten nordkoreanischen Domains. Bedingt durch mehrfach gefundene Einträge können Domains mehrfach auftreten, zb. durch redundante Systeme

haben.

Grundsätzlich muss davon ausgegangen werden, dass diese Geheimdienste in der Lage sind innerländisch den gesamten Datenverkehr zu überwachen und zu manipulieren, da diese mittels der jeweiligen Rechtsprechung (z.B. Patriot Act [11]) die jeweiligen Betreiber zur Kooperation zwingen können. In Tabelle 14 können dabei die Ergebnisse der reinen Domainzahlen betrachtet werden. Gesamt kommen diese fünf Länder auf mehr als 1 Milliarde reverse DNS Einträge, was mehr als 44% aller rDNS Einträge des gesamten Census beträgt. Auch wenn dabei dynamische IP-Adressen etc. inkludiert sind, haben diese 5Geheimdienste, beauftragt mit dem Schutz von weniger als 10% der Weltbevölkerung, indirekten Zugriff auf mehr als 40% der weltweiten Internet Infrastruktur.

Ein weiterer Aspekt ist dabei auch die Abhängigkeit anderer Länder von diesen fünf Augen, diese wird in Abbildung 18 sichtbar. Darin ist klar zu sehen, die Geheimdienste in der Lage sind mehr als 50% der IPs eines fremden Landes zu kontrollieren, analysieren und manipulieren. Für die Top 10 dieser so theoretisch kontrollierbaren Länder kann die Tabelle 15 betrachtet werden.

5.4 Fazit

Wie im vorherigen Abschnitt gesehen, bietet auch der rDNS Datensatz eine Reihe interessanter Ansätze um Aussagen

Land	”5 Eyes”	Gesamtanzahl	Abhängigkeit in [%]
IO	281.251	284.817	98,75
Niger	933	1.111	83,98
Belize	9.671	12.284	78,73
Kongo	3.618	4.998	72,39
CX	5.952	10.768	55,27
VG	781	1.450	53,86
Samoa	21.288	48.317	44,06
GS	643	1.463	43,95
Tuvalu	168.818	391.714	43,10
CC	53.913	130.823	41,21

Tabelle 15: Abhängigkeit einzelner Länder (zu lange Namen sind mit dem Country Code abgekürzt) von den 5 Eyes.

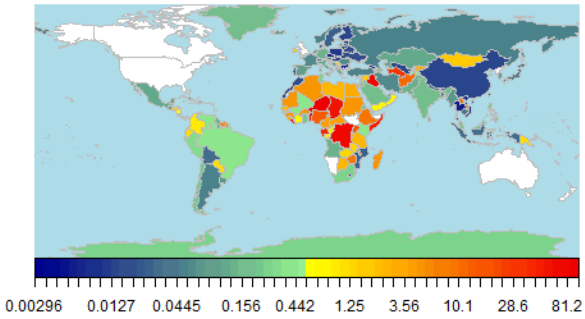


Abbildung 18: Abhängigkeit verschiedener Länder von den „5 eyes“ in %

über den Zustand des Internets durchführen zu können. Die Qualität dieser Aussagen ist dabei aber von vielen externen Faktoren abhängig, die nur schwer zu kontrollieren und evaluieren sind. Auf der einen Seite steht dabei die Qualität des Census Datensatzes. Aufgrund Zeit, aber auch Kapazitätsfaktoren ist eine Evaluierung der Daten im Rahmen dieser Arbeit nicht möglich.

Für die Zukunft können mit diesem Datensatz noch eine Reihe weiterer Experimente durchgeführt werden, hierfür sollte jedoch ein System mit mehr Arbeitsspeicher oder einem anderen, nicht RAM zentrischen, DBMS verwendet werden. Weiterhin wären auch Auswertungen interessant, bei denen auf eine deutlich geringere Abstraktionsebene zurückgegriffen wird. Als Datengrundlage könnten hierfür die, von Maxmind, angebotenen Geolokationsdatensätze auf Stadtebene benutzt werden, die im Verlauf dieser Auswertung nicht berücksichtigt wurden.

6. VERWANDTE ARBEITEN

Im Bereich der Messung und Analyse von Internetverkehr gibt es einige Arbeiten, welche sich direkt oder indirekt mit dem Internet Census 2012 in Verbindung bringen lassen.

So schlugen Mark Allman und Vern Paxson in [2] 2007 einige Richtlinien vor, welche Forschern bei solchen großflächigen Messungen dabei helfen sollen die Daten auszutauschen, ohne dabei in ethische oder rechtliche Probleme zu geraten. Ein Beispiel dafür ist das Aufstellen klarer Regeln was mit den Daten getan werden darf und was nicht (z.B.: ”The user

Geheimdienst	Domains	Anteil [%]	Bevölkerung	Domains pro Einwohner	Gesamtkontrolle [%]
USA	975.064.149	80,05	313.847.465	3,11	35,45
Großbritannien	127.073.049	10,43	63.047.162	2,02	4,62
Kanada	60.007.066	4,93	34.030.586	1,76	2,18
Australien	47.267.158	3,88	21.766.711	2,17	1,72
Neuseeland	8.622.234	0,71	4.290.347	2,01	0,31
Total	1.218.033.656		436.982.271		44,29

Tabelle 14: Übersicht über die Anzahl der von den Five Eyes kontrollierten Domains

may use the data to develop new techniques for finding subverted hosts that are part of botnets."[2]). Anonymisierung und Aggregation von Daten sind weitere Vorschläge für die sichere Weitergabe von Daten. Grundsätzlich wird im von uns betrachteten Teil des Internet Census 2012 keine dieser Regeln angewandt, allerdings bertrat der anonyme Urheber durch Verwendung seines Botnetzes bereits eine Grauzone.

Einen effizienten Scanner für internetweite Scans namens ZMap [7] stellten Durumeric et al. im August 2013 vor. Dieser ist in der Lage, von einem einzelnen Rechner aus den kompletten IPv4 Adressraum in weniger als 45 Minuten auf einen bestimmten offenen Port hin zu untersuchen. Der Schwerpunkt bei der Entwicklung von ZMap lag dabei darauf, den Scan so schnell wie möglich durchzuführen. So geht ZMap beispielsweise davon aus, dass der Scanner weder Quell- noch Zielnetzwerk überlastet. Aufgrund dieser Annahme umgeht NMap [16] den TCP/IP Stack, generiert Ethernet Frames selbst und sendet diese so schnell es dem Hostrechner möglich ist aus. Im Vergleich dazu nutzte der Autor des Census für seine Scans das CARNA Botnetz, welches dezentral auf ungefähr 420.000 Geräten lief. Dabei benutzte der Carna nur so viel Ressourcen, dass der normale Betrieb des genutzten Gerätes nicht eingeschränkt wurde.

Direkt dem Internet Census 2012 gewidmet hat sich Parth Shukla[20]. Sein Schwerpunkt lag dabei aber weniger auf den erhobenen Daten, als vielmehr auf dem CARNA Botnetz und den angreifbaren Geräten. Für diese Analysen verwendete er Daten des Census Authors, welche nicht öffentlich verfügbar sind. Er betrachtete dabei unter anderem Hersteller, Standort und den verfügbaren Speicher der ungefähr 1,2 Millionen angreifbaren Geräte. Den Hersteller konnte Shukla aus den verfügbaren MAC Adressen auslesen, dabei stellte er fest, dass bestimmte Hersteller relativ häufig vertreten waren. Aufgrund einer Länderzuordnung der angreifbaren Hardware machte Shukla sichtbar, dass allein 56% der angreifbaren Geräte China zuordenbar waren. Rund 69% der angreifbaren Geräte besaßen zwischen 32 MB und 256 MB Arbeitsspeicher, es gab allerdings beispielsweise auch eines mit 4,5 TB RAM (China). Abschließend berechnete Shukla noch, dass durchschnittlich ≈0,088 Geräte pro /24 Subnetz[18] durch den von CARNA genutzten Telnet Zugang angreifbar waren. Speziell auf China bezogen waren durchschnittlich sogar ≈0.56 Geräte pro /24 Subnetz verwundbar. Generell bestätigen unsere Untersuchungen diese Unsicherheit in China, allerdings zeigte auch Südamerika gewisse Verwundbarkeiten.

Anja Feldmann betrachtete 2013 den Census Datensatz mit Schwerpunkt auf ICMP Scans genauer[8]. Dabei stellte sie unter anderem fest, dass die Daten zwar authentisch sind, allerdings mit Vorsicht behandelt werden sollten. Grund dafür ist beispielsweise das Fehlen von Angaben, wie genau bestimmte Daten erhoben wurden. Auch konnte sie Veränderungen der Messmethoden im Laufe der Zeit beobachten, was vom Ersteller des Census nicht dokumentiert wurde. Unsere eigenen Beobachtungen zeigen, dass auch der Traceroute und der rDNS Datensatz gewisse Auffälligkeiten vorweisen, welche sich ohne weitergehende Informationen wie die Daten genau erhoben wurden nicht erklären lassen.

[18]Ein /24 Subnetz beinhaltet 256 Adressen.

7. ZUSAMMENFASSUNG

Der Internet Census 2012 bietet mit seinen 9 Terabyte an Daten Unmengen an Analysemöglichkeiten. Nachdem wir uns kurz mit der Methodik befasst haben, mit der der Autor die Daten gesammelt hat (CARNA Botnetz), nahmen wir uns in dieser Arbeit zwei der insgesamt acht Datensätze heraus und untersuchten diese eingehender. Um mit den bis zu 10 Milliarden Einträgen umfassenden Daten möglichst effizient und effektiv umgehen zu können, nahmen wir uns das DBMS MonetDB zu Hilfe. MonetDB fehlten zwar noch einige Features, welche Datenbanksysteme wie PostgreSQL, die wesentlich ausgereifter sind, besitzen, allerdings zeigte MonetDB im Vergleich zu PostgreSQL einen enormen Geschwindigkeitsvorteil bei der Auswertung von Datenbankabfragen. Dieser Vorteil liegt hauptsächlich in der spaltenorientierten Arbeitsweise von MonetDB. Bei Tabellen mit mehr Spalten als Zeilen ist Postgres idR. die bessere Wahl.

Ein weiteres Tool, welches wir verwendeten, war die Pythonbibliothek `pygeoip` um eine Zuordnung der IP-Adressen zu den einzelnen Ländern durchzuführen. Möglich war dies unter Zuhilfenahme der frei verfügbaren MaxMind [13] GeoLite Datenbank. Allerdings waren wir nicht in der Lage, hierzu genaue Fehlerquoten zu bestimmen, die Daten sind also nicht hundertprozentig korrekt.

Die, zur Extraktion der einzelnen Domainbestandteilen, genutzte Bibliothek `tldextract` hinterließ einen gemischten Eindruck. Einerseits wurde durch die Nutzung der Suffix Listen ein großer Teil der Hostadressen korrekt in die einzelnen Bestandteile aufgeteilt, aber bei mehreren Milliarden Einträgen reichte bereits eine sehr niedrige Fehlerquote aus um umfangreiche manuelle Nacharbeiten erforderlich zu machen. So musste jeder erzeugte Datensatz im weiteren Verlauf händisch nachbearbeitet werden um Daten weiter verarbeiten zu können.

Der erste der betrachteten Datensätze bestand aus 68 Millionen Traceroutes, welche von rund 275.000 verschiedenen

Geräten weltweit aus gestartet wurden. Ein Problem, dass die Traceroutes aufwiesen, war die ungenaue Dokumentation des Autors, welcher den Datensatz ohne weitergehende Informationen veröffentlichte. So fanden wir einige Traceroutes, die ihr Ziel aufgrund von aufgetretenen Routingschleifen vermutlich nie gefunden haben, was aber ohne eigene Analyse der Daten nicht ersichtlich wurde, da die Ziel IP der Traces ganz normal angegeben war. Die IP-Adressen der Traces ordneten wir unter anderem auf Länderebene zu, um Rückschlüsse auf die Standorte der verwendeten Geräte und den Weg der versendeten Pakete ziehen zu können. So zeigte sich, dass Pakete teilweise einen geographisch gesehen längeren Weg nahmen als nötig gewesen wäre. Desweiteren wurde aus den Daten ersichtlich, welche Kontinente eine besonders wichtige Rolle für das Internet spielen (Nordamerika, Europa). Dies ist zwar keine neues Erkenntnis, bestätigt aber die bisherigen Annahmen.

Trotz der Tatsache, dass es systematische Abweichungen von der initialen Auswertung des Census Autors gibt und der Problematik der nicht eindeutigen Domainnamen, zeigt der rDNS Datensatz des Census einige interessante Fakten auf und bestätigt gehegte Vermutungen. So war bereits im Vorfeld erwartbar, dass die westlichen Industrienationen das Backbone des Internets darstellen. Zu mehr Erstaunen führt dabei schon, dass die pro Kopf Anbindung in hochtechnisierten Staaten wie Taiwan den gesamten Westen deutlich überbieten. Auch die untersuchte nicht Abhängigkeit einzelner Staaten stellt interessante Aspekte heraus. Die finale Auswertung im Bezug auf den Zusammenschluss der Geheimdienste - den „5 Eyes“ - bestätigt, dass der aktuelle Geheimdienstskandal keinesfalls unterschätzt werden darf. Eine generische Auswertung des Datensatzes gestaltet sich aber, aufgrund der mannigfaltig enthaltenen Informationen als schwierig, so dass eine spezifische und gezielte Auswertung erforderlich ist.

Abschließend lässt sich sagen, dass es uns gelang, in den Daten des Internet Census 2012 einige interessante Fakten zu finden. Und bei dem Umfang der restlichen, von uns hier nicht genauer betrachteten Daten, ist es sehr wahrscheinlich, dass sich hier noch weitere Analysemöglichkeiten bieten.

8. LITERATUR

[1] Übersicht über die Weltbevölkerung. http://www.internetworldstats.com/list2.htm.

[2] M. Allman and V. Paxson. Issues and etiquette concerning use of shared measurement data. In *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, pages 135–140. ACM, 2007.

[3] S. Arnold. Das Handelsembargo - völkerrechtliche, europarechtliche, nationale Grundlage. *Bucerius Law School, Hamburg - Seminararbeit*, 2004.

[4] H. Asghari. Python ip to asn lookup module pyasn. https://code.google.com/p/pyasn/, 2009.

[5] G. Braune. Geheimbund ”Five Eyes Der exklusive Club der Geheimdienste. Tagesspiegel http://www.tagesspiegel.de/politik/geheimbund-five-eyes-der-exklusive-club-der-geheimdienste/8450796.html.

[6] Doxygen. evdns.h file reference. http://monkey.org/~provos/libevent/doxygen/evdns_8h.html, 09 2013.

[7] Z. Durumeric, E. Wustrow, and J. A. Halderman. Zmap: Fast internet-wide scanning and its security applications. In *22nd USENIX Security Symposium*, 2013.

[8] A. Feldmann. Internet census taken by an illegal botnet - a qualitative analysis of the measurement data. In *Talk at Dagstuhl*, 2013.

[9] R. Kirchner. Nordkoreas einziger Verbündeter. http://www.dradio.de/dlf/sendungen/einewelt/1969023/, Januar 2013.

[10] J. Kurkowski. tldextract projekt webseite. https://github.com/john-kurkowski/tldextract.

[11] J. Laas. Der Patriot Act und Datenschutz in der EU. http://www.telemedicus.info/article/2477-Der-Patriot-Act-und-Datenschutz-in-der-EU.html, 12 2012.

[12] Maxmind. Übersicht über die Datenqualität. http://www.maxmind.com/de/city_accuracy.

[13] Maxmind. Offizielle Webseite. http://www.maxmind.com/de/home.

[14] Maxmind. Zugeordnete IP Adressen pro Land. http://www.maxmind.com/de/techinfo.

[15] MonetDB DBMS Projekt Webseite. http://www.monetdb.org, 2013.

[16] Nmap. http://nmap.org/.

[17] Pivotel Greenplum DBMS Projekt Webseite. http://www.gopivotal.com/pivotal-products/data/pivotal-analytic-database.

[18] Postgres DBMS Projekt Webseite. http://www.postgresql.org/.

[19] PyGeoIP Projekt Webseite. https://pypi.python.org/pypi/pygeoip/, 2013.

[20] P. Shukla. Compromised devices of the carna botnet. In *ausCERT 2013*, 2013.

[21] Statista. STATISTA Statistik-Lexikon: Definition Gesetz der großen Zahlen. http://de.statista.com/statistik/lexikon/definition/58/gesetz-der-grossen-zahl/.

[22] TeleGeography. http://www.telegeography.com/.

[23] TeleGeography. Submarine cable map. http://www.submarinecablemap.com/.

[24] The Guardian. Prism. http://www.theguardian.com/world/prism.

[25] Tonic Domain Registry. Tonic Domain Registry. http://www.tonic.to/.

[26] Unbekannt. Internet Census 2012. http://internetcensus2012.bitbucket.org/paper.html, 2012.

[27] UPS. UPS - Trade Embargos Import/Export. http://www.ups.com/ga/CountryRegsPrint?loc=en_US&origcountry=US&destcountry=KP&cat=0150160170110180190200210230240090040140\discretionary{-}{}{}006007008002012010005013003&PrintRegulations=PrintRegulations.

[28] Wikipedia. AS Typen. http://en.wikipedia.org/wiki/Autonomous_System_(Internet).

[29] M. Williams. Wagt Nordkorea den Schritt ins Web? *Computerwoche*, 06 2010.

Normal Accidents and Computer Systems

Michael Dorner
Advisor: Heiko Niedermayer
Seminar Future Internet WS2013/14
Chair for Network Architectures and Services
Department of Computer Science, Technical University Munich
Email: dorner@in.tum.de

ABSTRACT

Accidents happen to all of us. Whether it be small or big ones, sometimes there seems to be no way to avoid them. The more complex our systems get, the harder it gets to understand what caused an accident, and how it could have been prevented. And yet, sometimes the risk of failure is so high, that accidents must not happen. Normal accident theory and high reliability organization are two scientific approaches to deal with accidents in high risk systems in order to predict and explain, respectively prevent accidents. However, both theories come from an era, where analogous technology was dominating, so its its unclear whether they still hold in a world dominated by digital technology. By exploring the implications of the use of computers in traditional systems as well as the implications of HRO and NAT for fully digital systems, it will be shown, that both theories can be applied in both cases with slight modifications and restrictions.

Keywords

accidents, high reliability theory, normal accident theory, critical infrastructure, Internet

1. INTRODUCTION

We live in a world full of amazing technology, which allows us to impact our environment in ways, that would have been considered nothing but magic only a century ago. While most technology was developed to improve the quality of our lives, failure in one of our new technologies may also result in a disaster. The potential extent of such an accidental catastrophe has increased proportionally with the sophistication of our systems and now includes the possibility of total annihilation of life as it is on this planet, trough accidental nuclear war. In order to better understand and hopefully prevent possible accidents caused by new human technology science has made an attempt to better understand these accidents. While accidental nuclear war is actually a concern in this area, it surely also is an extreme case to stress the importance of this research. Normal accident theory (NAT)[13] and high reliability organization (HRO)[15] are two of the more prominent pieces of scientific work which deal with system reliability, organization and accidents. Both originated in the investigation of classical high-risk systems and system accidents in chemical reactors, flight control or nuclear power plant (npp) security. Based on empirical studies, they try to better understand what causes accidents in complex systems respectively what needs to be done to avoid them. However, both are theories based on accidents and systems from a time when a lot of devices were analogous and computers often played only a minor role. Since the processes within computer systems exist within a virtual reality which we created as part of our reality, it is not natural to assume that both theories apply to them in the same way they apply to classical engineering. Thus the goal of this work is to investigate which impact both theories have on our digital systems.

Before heading into this discussion, there will be an introduction into both theories, as well as a short summary of a number of accidents, which were used to motivate both theories. Since the main contributors to both theories had a very spirited discussion about the relation of HRO and NAT, it is necessary to take a look at their relation and find a position suitable for applying both theories to modern computers and computer networks. Subsequently the applicability of both theories in digital systems will be discussed along with the possible consequences one should draw from their application. The paper is finalized by a summary of the findings.

2. BASICS

Neither NAT nor HRO can be considered common knowledge, so it is only normal to explain both shortly before discussing them.

2.1 Normal Accident Theory

Normal Accident Theory originates from Charles Perrow's investigation of an accident at Three Miles Island(TMI), an American nuclear power plant (NPP), which underwent a partial meltdown in 1979. Although it did not cause a larger nuclear disaster like Chernobyl or Fukushima, the accident resulted in an extensive investigation. In the light of this investigation Perrow voiced the opinion[12], that in tightly coupled systems with highly complex interaction accidents through unexpected interaction are normal, thereby giving birth to "Normal Accident Theory". In his subsequently published book on "Normal Accidents" Perrow did not only lay out his theory, but also defined a framework for

doi: 10.2313/NET-2014-03-1_04

the classification of accidents. While a full summary of his framework would be far too extensive, it cannot be avoided to cover some definitions, which will matter later on, when comparing NAT and HRO. In his definitions Perrow divides systems into units, parts, subsystems, and the system itself. He introduces a separation between "component failure accidents", which involve "one or more component failures, that are linked in an anticipated sequence"[13], and "system accidents", which "involve unanticipated interaction of failures"[13]. The system accidents are the ones Perrow considers "normal accidents", since they cannot be prevented according to his theory. It is important to mention that despite their name, "normal accidents" are an exceptional, rare kind of accidents according to Perrow. Another important aspect of his theory is the definition of tight coupling and complex interaction. Perrow defines complex interaction through:

- *Local proximity*: Components are close to each other, thus causing failures in one to possibly affect the other simply because of their proximity.
- *Common-mode connections*: Mainly characterized by their impact on a number of otherwise independent systems. A common-mode failure is the single source for failure in multiple systems, although they may not seem to have a connection with each other at first glance.
- *Interconnected subsystems*: Subsystems are connected with each other, thus likely propagating failure on the subsystem level.
- *Limited substitution of materials*: Materials cannot simply be replaced, making leakage or breakage problematic.
- *Unknown/unfamiliar feedback-loops*: Feedback loops are based on the idea, that the system receives feedback and adjusts its behavior. In the best case this change in behavior is to produce output, which is closer to or is the desired output. However, having a feedback loop within a system, which is not planned for or which is not effectively blocked, if it is not desired, can cause the system behavior to deviate from the expected behavior.
- *Multiple and interacting controls*: Control is e.g. performed via multiple terminals, thus requiring coordination.
- *Indirect information sources*: It is not possible to directly deduce the actual system state from merely observing it, but indicators have to be monitored.
- *Limited understanding of processes*: The process does not allow complete understanding due to either a large number of possibilities or non-deterministic elements.

Among these criteria, especially common-mode connections and feedback loops will frequently be present, but not perceived in complex systems. Systems, which are not complex, i.e. which do not have these characteristics are referred to as "linear" by Perrow.

Just as for complexity Perrow also defined criteria for tight coupling:

- Processing cannot be delayed
- Fixed Order of Sequences
- Only a single method leads to success
- Little slack in resources
- Buffers and redundancy have to be present by design
- Substitution of resources has to be designed in

These characteristics should mostly be self-explanatory, so it is not necessary to give an extensive explanation at this point. One thing, that may not immediately be clear however, is the notion of designed-in buffers/substitutes: components in tightly coupled systems are not easily replaced, and buffering is not possible without components, which are explicitly included by design to allow for it - think about an empty bucket to catch liquid from a leaky pipe and try to find something that does the same for an overheating nuclear fuel rod.
Perrow's work gained a lot of attention back when it was released, and constituted a new point of view on accidents, which was picked up by the a group of researchers in Berkeley in their work on HRO[15]. It was this HRO group's findings, which Scott Sagan later contrasted against Perrows original work in [18]. While the discussion his paper started will be analyzed later on, only Sagan's contributions to NAT are of interest at this point. Perrow himself acknowledged and praised two major contributions to his work by Sagan[14]: the fact, that he outlined a difference in the theoretical models HRO and NAT had used, and his emphasis on group interest as a relevant factor. While Perrow merely clarifies that he was implicitly assuming a *nonrational* garbage can model (see Appendix A) as underlying organizational model in response to the first contribution, he points out Sagan's second finding as a novel, interest-theoretical aspect of his theory. The inclusion of group interest means that some groups, which are part of the governing process of an organization, may put other things first instead of safety (e.g. profit). Although the work cited above is typically a decade or two old NAT is still commonly referenced in scientific articles[17] as well as news articles about major accidents such as Fukushima [11] or financial crisis[20], thus keeping it relevant.

2.2 High Reliability Organization

Since accidents are the main topic of this paper, one may wonder, why it is necessary to introduce a second theory at this point, when NAT is an accident theory of its own. Depending on which position one takes, it is either, because HRO is not a theory of its own, but a complementary organizational strategy to provide high reliability in systems prone to normal accidents, or it is because HRO is a competing theory, which suggests that normal accidents can be prevented by sticking to certain guidelines (in that case one would likely call it HRT - T for theory). However, before it is possible to take either side, it is necessary to understand what HRO is about. High Reliability Organization

was initially driven by two groups of researchers: one at the University of California, Berkeley and the other at the University of Michigan. The "Berkeley group's" main members were LaPorte, Rochelin and Roberts; the "Michigan group" was mainly represented by Weick and Sutcliffe. The research of both groups, which frequently reference each others research, is centered around ways to establish a safety culture in organizations, which operate systems, which are prone to normal accidents. From their own observations of aircraft carriers and flight control[15, 2] they identified a set of properties, which, according to them, help those organizations improve their reliability, thus making them "High Reliability Organizations". Interestingly there is no real agreement on a definition of reliability among the HRO researchers, and it seems that they currently have a rough consensus on reliability as "the ability to maintain and execute error-free operation"[17]. The original research of the Berkeley group[15] and their subsequent work[3, 2, 4, 6] finds the following requirements for an organization to become a HRO:

- Redundancy: Especially the early HRO research outlines the importance of redundancy in personnel and safety mechanisms to better cope with component failures and also to ensure that decision-making involves more than a single operator.
- Prioritization of safety: Government and organization leaders put reliability and safety first. Other aspects, including performance may suffer, but leaders accept the loss of performance to achieve higher reliability and safety.
- Organizational Learning: The organization learns from ongoing operation, thus continuously improving the ability to deal with failures.

The Berkeley group had become a little quiet over the last years, and there is no recent publication from them. Opposed to that the Michigan group still seems to be working actively on their HRO-model, which is fairly frequently updated (last 2011), in their book on "Managing the Unexpected". The focus of the Michigan group is more on the investigation of organization culture, which HROs have to establish. It currently lists five important aspects of organizational culture, which HROs should embrace[21]:

- *Preoccupation with failure*: Members of the organization are not focused on what confirms their ways, but what opposes it, i.e. possibilities to fail are actively perceived, people pay attention to possible new or unknown modes of failure and learning takes place. It reduces overconfidence and encourages a state of mindful operation.
- *Reluctance to simplify*: Organization members are animated to stay wary of the complexity of the system they operate, and thus make more considerate decisions, although likely lowering performance. Some processes, which could in theory be done by a single person may e.g. be performed by a group of equals without a shared perspective to profit from their collective understanding.
- *Sensitivity to operations*: Members are aware of the current situation and its implications.
- *Commitment to resilience*: The organization's capabilities to improvise and react to new situations are constantly maintained and improved.
- *Deference to experience*: The most experienced members make decisions despite hierarchies if failure happens. Decision making is decentralized but based on the culture put in place by centralized organization leaders.

These criteria for an organizational culture are not solely the work of the Michigan group, and is difficult to track which group outlined the importance of a certain aspect at first, but they seem to agree in large parts that these qualities are important to establish a culture in which an organization can operate at high reliability. The main difference between both groups is, as already mentioned, the increased focus on organization culture by the Michigan group, whereas the Berkeley group was also still involving some systems design considerations such as redundancy. In general it is important to outline the relevance of *decentralized, rational decision making* for HROs and their focus on reliability and safety over budgets and performance. LaPorte from the Berkeley group notes in some of his post-Cold-War work on reliability-oriented organizations, that "when either the consensus about their value declines or economic resources in general become more dear, reliability regimes are more difficult to sustain, especially after conspicuous success and/or as system resources become relatively more scarce."[6]. HROs are faced with the challenge to maintain their reliability record under these conditions.

2.3 Important Accidents

After explaining NAT and HRO, we will now shortly take a look at some accidents, which have influenced them and which have drawn attention to this kind of research. The literature on accidents and reliable organization lists a large number of other accidents, and there have also been more fatal ones than those, that are about to be explained, but they make good examples to show up important aspects of both theories, and have thus been chosen. Because most accidents are covered extensively in accident reports created by experts, we will stick to a short description. We will thus take a look at the following points:

- What was the starting point?
- What happened?
- What were the causes for failure?
- What were the consequences of the accident?

2.3.1 Three Miles Island - TMI

What was the starting point: Three Miles Island was and is a npp in Pennsylvania, US. It consists of two reactors, TMI-1 and TMI-2.
What happened: On the 28th of March 1979 there was a partial meltdown in TMI-2 and a small amount of radioactive gas was released

What was the were the causes for failure: Due to previous maintenance work, all feed-water pumps (primary, secondary, emergency), which are required to transport coolant to the reactor were offline. Thus no heat was deduced from the reactor the pressure rose, since pressure and temperature are proportional by the laws of physics if the volume remains the same. An automatic valve opened to reduce the pressure inside the reactor, and should have closed after pressure returned to normal, but instead was stuck open due to mechanical failure. Naturally opening the valve primarily reduced the volume of the coolant inside the reactor, thus leaving it open leads to a lack of coolant. The plant operators failed to recognize this situation, for one because of a misleading indicator light, which displayed wrong information (valve closed), and also because they were preoccupied with the correctness of this light and consequently ignored indicators, which should have let them realize the true nature of the failure they were facing. Ultimately, the lack of cooling caused the nuclear fuel rods to overheat and ultimately the partial meltdown. A detailed description of this accident can be found in [13, 10] and in many other sources, since this accident was very well investigated and a lot of information is available to the public.
What were the consequences of the accident: Luckily, the damages to the environment, as well as the exposure of the population to radioactive material were low, such that it is commonly agreed upon today, that the TMI accident had no observable long-term consequences for the health of the surrounding people. As already mentioned there was a government investigation, which also resulted in Perrow's basic paper on normal accidents. Anti-nuclear protests gained credibility from this accident, especially in the US, but the consequences for the nuclear industry were insignificant. TMI-1 is still operating today, and has a license, which lasts at least until 2034. TMI-2's decontamination officially ended in 1993, although it is still monitored.

2.3.2 *The Bhopal Disaster*

What was the starting point: A pesticide factory in Bhopal, India, surrounded by slums.
What happened: Large amounts of highly toxic gas leaked into the air.
What were the causes for failure: Unlike TMI, the Bhopal accident is not fully resolved until today. What is for sure is that water somehow entered a tank full of methyl isocyanate (MIC), a deadly gas. Water and MIC cause an exothermic reaction, which results in increased pressure. The high pressure lead to the release of several tons of MIC into the air through emergency relief valves. Government investigation found that leaky pipes and valves were most likely to be the reason, and that water had gotten into one of the tanks while they were flushed for cleaning. It further indicates, that the plant was in a horrible condition with several safety measures being non-functional, employees completely untrained to react to accidents, and the plant being understaffed. Cost appeared to be the driving force behind these shortfalls. Although frequently mentioned for its tragic outcome, the accident itself seems to be poorly researched, most likely due to the lack of an independent investigation. The company operating the plant originally claimed that sabotage must have been the reason - very likely to avoid compensation claims - but the government's assessment is considered a fact today.
What were the consequences of the accident: This accident is the often referred to as "worst industrial disaster" in history, and has caused at least 3,787 deaths according to the local government, although others claim, that the number of deaths caused by it are around 25,000. The number of injured people is estimated to be around 500,000 - 600,000 and the area is still not decontaminated. Without taking sides on the cause, it is clear that the surrounding environment of the plant, where many people from the plant lived in slums, the failure to inform surrounding inhabitants of the gas leak, and the lack of an evacuation strategy lead to the disastrous outcome of this accident. As already mentioned severe negligence was very likely the reason for this disaster. An Indian court, in agreement with this point of view, found eight former plant employees guilty of "death by negligence"[19] in 2010 and sentenced them to two years prison and a fine of 2,000$.

2.3.3 *Challenger*

What was the starting point: The Challenger was one of the Space Shuttles of the US Space Program **What happened**: The Shuttle was torn apart by the aerodynamic forces mid-air after its launch on the 26th of January, 1986
What were the causes for failure: Two redundant o-rings, did both not seal one of a tank correctly due to cold weather, gas leaked, and one of the rockets used to boost the shuttle during take-off was no longer correctly attached to the space-vehicle. The resulting changes in aerodynamics increased the physical forces to an extent, which exceeded the limit the shuttle could take. Problems with the o-ring were known to the manufacturer beforehand, but instead of grounding all space shuttles, they added this behavior to the acceptable conditions, because it would work under normal conditions. **What were the consequences of the accident**: Subsequent flights were canceled and all shuttles were grounded for 32 months. A commission was mandated to investigate the accident. The commission found the design of the o-ring to be faulty and thus NASA or the manufacturer should have grounded all shuttles until the issue was resolved. On a side note: Richard Feynman, a member of the commission, was so appalled by NASA's "reliability culture"[1], that he insisted on adding personal notes to the report, for it to have his name on it. The report [16] is still publicly available from NASA.

3. NORMAL ACCIDENTS AND HIGH RELIABILITY ORGANIZATIONS - A CONTRADICTION!?

During the explanation of both HRO and NAT, it was already mentioned that the authors of both theories had an argument about whether HRO complemented NAT, or whether it was a competing theory of its own. The discussion between Perrow and La Porte was sparked by Sagan's work on the "Limits of Safety"[18]. While the main topic of his book was the safety of nuclear weapons and defense systems, he had also investigated both HRO (referred to as HRT by him) and NAT in this context, and found that they are competing theories, which exclude each other. Perrow agreed with Sagan's analysis and complimented him on his work and his contributions to NAT. LaPorte and Rochelin on the other hand, representing the Berkeley group, did not agree at all

and explicitly addressed Sagan's as well as Perrow's arguments in a paper with the sole purpose to contradict them. Of all the points made in this discussion there are three, which seem to touch central issues of both theories the most, and which will be investigated to justify the position, which will be taken with respect to both theories for the rest of this paper.

3.1 Possibility of Error-Free Operation

The possibility of error-free operation is something that obviously contradicts NAT, which claims that some accidents cannot be avoided. Therefore if HRO would actually claim to offer a way of error-free operation, this would already be the point where we could stop and side with NAT, because HRO's claims would be implausible for the present and impossible to prove for the future. As a matter of fact, it is true that La Porte and Rochelin have claimed to have learned "the degree and character of effort necessary to overcome the inherent limitation of securing consistent, failure free operations"[5], but La Porte claimed that Sagan had misunderstood this statement. According to his statement on the issue in [5] they thought that the required effort would be too big to be surmounted. Therefore, and also because HRO in general contains elements like learning from errors and near-misses which contradict the idea that error-free operation can be achieved, it should not be seen as realistic goal of HRO - otherwise it would likely also be referred to as total or complete reliability theory by its authors. Even Perrow seemed to think that both theories agree that error-free operation is not a realistic goalPerrowLoS. Interpreting the explanation of La Porte[5], the relationship between effort and gain in reliability assumed by HRO appears to be similar to the acceleration to the speed of light: the closer one comes to 100%, the more the effort required to come any closer increases. Both, tight coupling and highly complex interactivity, seem to increase the required effort even further. In connection with Perrow's explanations on how interactive complexity and tight coupling cause unpredictable interaction of failures in [13] it appears that both experienced the same phenomenon, but HRO focused on how organizations dealt with this challenge, while Perrow payed more attention to what factors contribute to it. Ultimately, it is safe to say that both HRO and NAT agree, that error-free operation is not possible.

3.2 Effectiveness of HRO Methods

Another thing that NAT theorists had criticized about HRO, was the effectiveness of their methods in general. Sagan and Perrow both voiced the opinion that some of the techniques HRO relies on do not have any provable beneficial effect. While some of their criticism directly addresses concepts of HRO, they also doubt the benefits of their methods in general.

3.2.1 Specific Criticism

First of all, we will turn to Perrow's criticism of specific methods which HRO suggests. His specific criticism in [14] addresses thee concepts:

Centralization and Decentralization. This point is one of the few where HRO and NAT truly conflict, and where it is not possible to convincingly argue for either side. While HRO suggests a centrally imposed HRO-culture which is executed in a decentralized fashion by all organization members, NAT expects that both models cannot be combined, Perrow explained[14]. While he considered both concepts essential to deal with complex interactivity respectively tight coupling, he also thought that they cannot be combined. As already mentioned is possible to side with either party here, but HRO's model offers more opportunities, as it considers mixed forms of both concepts a possibility and also dynamic shifts from one concept to the other. Since La Porte el al give credible proof that this can work in reality, e.g. aircraft carrier operation, their opinion is just as justifiable as Perrow's, who refers to his theoretical explanation in[13]. HRO's more dynamic approach to decision making, which is also offers the possibility to shift decision making in centralized organizations, e.g. from the highest ranking to the most experienced person, as the principle "deference to experience" dictates it, seems more promising than simply surrendering to the fact that aspects of two mutually exclusive concepts are required.

Training. While training for emergencies is intuitively a necessary measure, the implications of HRO's understanding of training go way beyond regular emergency drills: it expects that organizations forgo routine and stability in exchange for challenge and variety to improve the experience of the employees with irregular circumstances. While this may make sense in some situations, Perrow's argument[14], that this is not an option for systems with especially high risk like npps, is a striking one for high risk organizations. Even in regular organizations this is unlikely to be an option because it will likely decrease productivity. It is however not surprising that La Porte et al observe this kind of behavior in organizations like an aircraft carrier, which practically does nothing but training in times of peace. For regular organizations the kind of learning HRO suggests does seem unreasonable to implement though. While it is certainly not wrong to stay wary and have the preoccupation with failure HRO-culture demands, intentionally mixing up regular operation seems just unreasonable for most organizations.

Learning. The aspect of organizational learning is closely related to that of training, since more training would obviously result in more learning. Therefor if learning was an effective measure, the relevance of training would also increase. Perrow also criticizes this aspect of HRO based on an extensive list of examples where organizational learning did not happen[14], and with an earlier study on accident investigations, which found that accident-investigations typically only investigate those sub-systems which failed and not the role of other sub-systems in this failure, which may obstruct learning. The latter argument is also supported by the fact that accident investigations often stop after assigning blame - often to the operator - as [7] found. This hunt for a scapegoat which follows many accidents is also a reason why the full set of failures and their interaction will likely remain undiscovered. Therefor a solely beneficial effect from this kind of organizational learning cannot be ascertained in general. Learning from biased investigations may even worsen the error handling of the organization. The arguable benefits of learning from accidents and near-misses also further limits the benefits one should expect from the kind of training HRO suggests. Therefor siding with NAT on this arguments seems to be the better choice.

doi: 10.2313/NET-2014-03-1_04

3.2.2 General Criticism

General Applicability of HRO Methods. What Perrow and Sagan criticized most in the HRO-methods is that they come from organizations which have not experienced failure. HRO tried to determine factors, which allow them to achieve this high reliability; Perrow refused this approach as "selecting on the dependent variable"[14]. He thought that just because the organizations observed have shown common approaches during failure-free operation, this does not mean that those approaches are helpful to achieve failure-free operation in general. The fact that a future accident may expose a new, previously unpredictable cause, i.e. it is a normal accident, is what makes NAT practically impossible to falsify and any error-preventive measure impossible to prove. Proving error-free operation measures seems to be an undecidable problem, because it would require the prove of future properties of a system, which is typically undecidable, although we will forgo a proof of this property here. In consequence it is true, that HRO's usefulness cannot be proven beyond the point of no doubt, but it is very common to apply theories, which show desirable effects in practice until they are proven wrong. Examples are the application of mathematical theories in finance and politics, like game theory, large parts of all social sciences, which are not proven conclusively in a manner satisfactory for many STEM-scientists, and the different models that have been used to describe atoms throughout the 20th century, which were wrong or incomplete and yet allowed for major scientific advancements. It is also the fact that severe negligence of HRO principles has caused some of the most serious accidents, that supports HRO's claim to enhance reliability: among the three examples listed earlier on, both the Challenger and the Bhopal disaster could have probably been prevented by a more HRO-influenced organization. Because HRO methods could have likely prevented or reduced the extent of these accidents, it would be unjust to generally dismiss them, because they come from organizations which have not failed, especially could have prevented accidents.

Applicability of HRO Methods to Normal Accident-Prone Systems. The second general criticism of NAT's advocates is that HRO is not applicable to those systems, where "normal accidents" are especially likely to occur. According to Perrow these systems all have a high degree of coupling and interactive complexity, which the organizations HRO investigated have not. Perrow and La Porte rant on about this classification issue quite a while in [14] respectively [5]. As explained earlier, these two criteria are determined by a set of factors, which Perrow nicely outlined in his book[13]. The problem is that "high" and "tight" are not defined in any objective way, therefor their meaning is completely bound to the subjective perception of the person looking at an organization. It is like asking two people to name a big number: if you ask a computer scientist he may come up with something like 2^{128}, while a normal person might just say one million. Perrow's comments on this topic in his book show, that he is fully aware of the subjectivity of his categorizations and the fact that he is lacking a metric[13]. Given these considerations, it is very likely, that the HRO groups, having a different mindset than Perrow, simply came to a different categorization. In fact it seems that nothing but the subjective estimation of the person applying NAT serves as the function, which projects organizations into this fourfold table. Analogous to the principle that ambiguities in a contract are held against the party who put up a contract in US law practice, the subjective definition of when a system is tightly coupled with highly complex interactions should be held against Perrow, therefore voiding his argument that HRO does not investigate organizations with tight coupling and highly interactive complexity, simply because they are not well enough defined. HRO's applicability to what Perrow considers "normal accident-prone" is still limited, due to the effort required to further increase the reliability of systems, which are already very close to error-free operation. Since Perrow himself declares that some of the recent history's worst accidents like Bhopal, the Challenger-crash, the Exxon Valdez and Chernobyl were not normal accidents[14], HRO would be a great contribution if accidents like those could be avoided through it.

4. ACCIDENTS IN COMPUTERS AND COMPUTER NETWORKS

After an extensive discussion of two major pieces of work on accidents/accident prevention the actual matter of accidents in computer networks can now be addressed. The two theories presented are not the only ones of interest to this area, but their relationship is complex enough already and the introduction of other models such as Leveson's STAMP[9, 7] or even her more basic work on "Safeware"[8] would simply add to the confusion. All of the previously presented systems have huge catastrophic potential for the real world, something which is sometimes said to be a difference between traditional systems and computer networks. Computers and computer networks are sometimes thought of as a world of their own, although they have already begun to have a notable impact on real world objects. The fact that we have seen not any major accident caused by computers does not mean that they do not carry the potential for causing such accidents. With smart grids and the Internet of Things coming some of our everyday life is already moving into the digital world, but technologies which are a bit further away like autonomous cars or robots will definitely mean that digital systems can cause just as catastrophic accidents as analogous ones. For accident theory, computer technology introduces two different aspects: computers which conquer the domain of classical systems, and computer systems themselves, which follow entirely new laws with respect to their internal operation.

4.1 Computers in Classical System Accidents

Classical systems are the ones that rely on clever use of physics and other sciences exploring the laws of nature, e.g. chemistry to make our natural system behave in a the way we want it to. Because nature is not exactly obedient, those are also the systems that carry higher risk the more extreme our nature hacks are. For these systems the introduction of computer systems often means that control is taken from a human and given to a computer, which is merely supervised by a human to ensure its correct operation. This change in control is often going to add complexity, because the human supervisor gets less direct information from the system and if the computer is networked and uses information provided by other computers this may introduce new ways of propagating error throughout the system. But in general a computer is a component that can fail just as much as any

other part. Most operators do no have complete knowledge of the system they supervise at every level, but know the in- and outputs, and possibly intermediate results their system will produce. Because these results are not physical in the case of a computer, communicating the exact situation to the outside will be an important challenge. If the internal state is not communicated correctly and clearly to the outside, computers will significantly impair HRO-operation, because operators might not notice a near-miss and may not be able to stay aware of what is happening inside the system as HRO demands it. Furthermore the much faster development lifecycle which often changes existing systems drastically may reduce the benefits of experience. Yet one should not expect that the "culture of reliability" looses importance, because there will still be people operating the system somewhere in the background which need to pay even closer attention to whether the system runs as expected. We can expect that the effort will increase though, since we have added yet another level of complexity to our systems. While HRO faces some challenges in its transition to the digital world, NAT is golden. Because one of its assumptions has always been that adding new means to prevent accidents to a system will also introduce new ways of failure, it is not to be expected that it looses any ground. Since computers are no more than a part of traditional systems, their internal behavior is not as important at this point as the behavior they show to the outside, i.e. the signals they send and receive to and from other components. Since we are not just switching to digital for fun, but because of the huge potential of this technical innovation, we should also expect to see new modes of failure, especially when we try to handle failures that analogous systems could experience through "smart" systems. NAT assures us that even when we go smart, we will see failure that those smart devices wont be able to handle.

4.2 Accidents in Computer-Systems

4.2.1 Software and System Accidents

Software accidents, are accidents where software behaves in an unspecified way. Most often they are bugs, and thus simple component failures. Software bugs are quite difficult to combine with HRO, since HRO relies on a certain mindset which people inside HROs share, which is not applicable to computers as they are not. Therefor HRO does not apply to software and computer systems. Software and the internal workings of a computer also limit NAT to some extent, because "normal accidents" are caused mainly by things that are unexpected or not well understood, which may not exist in a system that we created ourselves. The only reason why we could expect "normal accidents" in software on a single computer is non-deterministic execution which causes data-races, but if enough attention is payed to synchronize this should not happen. Besides, many of the factors that increase complexity or tight coupling are factors that computer design limits by design e.g. through out-of-order execution, best effort service, and dynamic scheduling. Therefor the probability for normal accidents on a software level is quite low, although it may well increase when we build more advanced systems, where timing guarantees and similar features matter. In single, non-networked computers, normal accidents should therefor be possible to prevent. Networked computers are very likely different: if we take the Internet of today for example we see a fairly loosely coupled system, which has best effort service and optional reliability in transport. As soon we use TCP to gain reliable transport, we add a certain level of complexity to the Internet, because all of a sudden we have a feedback loop, namely the TCP congestion control mechanism, which complicates things significantly, as it influences the shape of the traffic. If we add more guarantees to the Internet such as QoS-guarantees, we complicate the interaction of the packets even more and if they go over the same link with dynamic bandwidth allocations, the Internet may well become complex enough for us to loose oversight and experience "normal accidents". That should not stop us from advancing our technology, but we should stay conscious of the fact that complicated systems will show failure that we cannot anticipate. What complicates this situation even more is that we cannot effectively monitor the Internet with respect to how data flows globally and therefor our feedback from the Internet may be poor or incomplete. Because the Internet is the backbone of many of the amazing visions for the future, anything that is built on top of it, has the base level of complexity and coupling that comes from the Internet. All of the technologies built on top add to this base level may worsen the situation, especially cloud computing, which is probably one of the best examples for a common-mode connection. While cloud-based data-warehousing is a huge trend at the moment, mission-critical services should thus not run at a single data-center to prevent catastrophic common-mode failures. If the service is important enough, e.g. power supply, using a dedicated physically separate network may even be a good choice to make sure the complexity from the Internet cannot cause unexpected failure. For the global Internet it is impossible to say whether normal accidents will or will not become a major issue, because it is hard to predict what the Internet will evolve into. Although it looks like managed services and QoS will gain importance, it would be a common interest of all users to keep the basic network as simple as possible to keep the base complexity and coupling low.

4.2.2 Computer Operation and Administration

Apart from flawed software or systems themselves, there is also the aspect of their operation. While software may behave as specified if it is patched correctly, errors may arise if it is misconfigured or not administrated correctly. HRO's principles are generally applicable to the operation of computer systems as much as they are applicable to any other organization, with the exception that they require communication between operators and administrators in IT. While administration must put an emphasis on offering a stable environment for its users, they should pay attention to bugs and issue that may indicate systematic problems. Although this combination should usually allow administration to improve the experience of its operators, this synergy is often limited by the fact that operation and administration are not done by the same organization. The trend towards outsourcing administration or buying things -as-a-Service in the cloud make HRO almost impossible to realize in many scenarios, because the administration has extremely limited information about the system state form the user point of of view, which usually offers more insight into the weaknesses and problems of the current system. Since the communication between users and administration is typically limited to complaints, this makes it very hard for administration to realize the culture of reliability. Although HRO is a bit hamstrung by this, this area should usually not be very prone

to "normal accidents" because most of our systems consists of many small and independent machines, which are quite linear.

5. CONCLUSION

In the end there is much to learn form both NAT and HRO. While NAT mainly highlights the importance of paying attention to the level of complexity and coupling we introduce by our designs, it also reminds us to stay wary of the possibility of unexpected failures. HRO teaches us the importance of decentralization and the focus on reliability. Its culture of reliability should prove valuable to almost any companies in the future in operation and is expected to maintain its effectiveness in traditional systems even though it may require extra effort to compensate for the culture-free decision making of computer systems. The combination of both theories during design and operation can surely help organizations on- and off-line avoid accidents, although they seem to leave some room for other theories especially when it comes to design which avoids normal-accidents and operation strategies, which do not rely strongly on human intelligence.

6. REFERENCES

[1] Feynman R.Appendix F - Personal observations on the reliability of the Shuttle, in "Report of the PRESIDENTIAL COMMISSION on the Space Shuttle Challenger Accident"

[2] LaPorte, Todd R. :*The United States air traffic control system: increasing reliability in the midst of rapid growth*, 1988.

[3] LaPorte T.R. : *High Reliability Organizations: The Research Challenge*, HRO Project Paper, Institute of Governmental Studies, University of California

[4] La Porte, Todd R. and Consolini, Paula: *Working in Practice But Not in Theory: Theoretical Challenges of High-Reliability Organizations*, in Journal of Public Admin- istration Research and Theory, 1, 1991, pp. 19-47

[5] La Porte, Todd R. and Rochlin, Gene I.: *A Rejoinder to Perrow*, in Journal of Contingencies and Crisis Management Vol. 2, Nr. 4, 12/1994

[6] La Porte, Todd R..: *High Reliability Organizations: Unlikely, Demanding and At Risk*, in Journal of Contingencies and Crisis Management Vol. 4, Nr. 2, 06/1996

[7] Leveson, Nancy :*A new accident model for engineering safer systems*, in Safety Science 42.4 pp.237-270, 2004

[8] Leveson, Nancy :*Safeware: system safety and computers*. ACM, 1995.

[9] Marais, Karen and Dulac, Nicolas and Nancy Leveson:*Beyond Normal Accidents and High Reliability Organizations: The Need for an Alternative Approach to Safety in Complex Systems*, Engineering Systems Division Symposium, MIT, Cambridge, MA March. 2004

[10] Nuclear Research Commission(NRC): Backgrounder on the Three Miles Island Accident, http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html

[11] Osnos, E. : *The Fallout*, The New Yorker, 11/17/2011, http://www.newyorker.com/reporting/2011/10/17/111017fa_fact_osnos?currentPage=all

[12] Perrow, Charles.: *The President's Commission and the Normal Accident*, in D. Sils, C. Wolf and V. Shelanski, Accident at Three Mile Island: The Human Dimensions, Westview, Boulder, pp.173-184

[13] Perrow, Charles.: *Normal Accidents*, Princeton University Press, 1999

[14] Perrow, Charles: *The limits of safety: the enhancement of a theory of accidents., in* Journal of contingencies and crisis management 2.4 (1994): 212-220.

[15] Rochlin, Gene I., Todd R. La Porte, and Karlene H. Roberts : *The self-designing high-reliability organization: Aircraft carrier flight operations at sea*, in Naval War College Review 40.4: 76-90, 1987

[16] Rogers Commission:*Report of the PRESIDENTIAL COMMISSION on the Space Shuttle Challenger Accident*,, http://history.nasa.gov/rogersrep/v1ch4.htm

[17] Rouncefield M. and Bubsy J.: *D 7.2.1*,2013

[18] Sagan, Scott.: *Limits of Safety: Organizations, Accidents, and Nuclear Weapons*, Princeton University Press, 1993

[19] Soutik Biswas:*Bhopal trial: Eight convicted over India gas disaster*, BBC News, http://news.bbc.co.uk/2/hi/south_asia/8725140.stm

[20] Surowiecki, J. : *Bonds Unbound*, The New Yorker, 02/11/2008, http://www.newyorker.com/talk/financial/2008/02/11/080211ta_talk_surowiecki

[21] Weick, K., and Sutcliffe K.: *Managing the unexpected: Resilient performance in an age of uncertainty* Vol. 8. John Wiley & Sons, 2011.

Appendix A - Garbage Can Model

The garbage can model is a model for organizational decision making, which was originally established by M. Cohen, J. March and J. Olsen. It has been adapted later on, and thus multiple versions can be found. The characteristic trait of this model is however the fact that it **assumes decision making to be based on stochastic events** involving a set of streams, such as policies, politics and rather than rational analysis.

Menschliche Entscheidungen und Rationalität

Anton Brandl
Betreuer: Heiko Niedermayer
Seminar Future Internet WS2013/14
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: brandlan@in.tum.de

KURZFASSUNG

Ziel dieser Publikation ist es, einen Überblick über wichtige Theorien menschlichen Verhaltens in Entscheidungssituationen zu geben. Es wird dabei auf folgende drei Forschungsfelder eingegangen: Die Rational-Choice Theorien, Theorien begrenzter Rationalität und Grundlagen der Spieltheorie. Dabei werden grundlegende Modelle miteinander verglichen und anhand von Studien bewertet. Es wird gezeigt, dass es gute Möglichkeiten zur Vorhersage menschlichen Verhaltens gibt, jedoch keine dieser Verfahren ein Patentrezept darstellt.

Schlüsselworte

Begrenzte Rationalität, Rational-Choice Theorie, Spieltheorie, Heuristiken, IKT

1. EINLEITUNG

Beim Entwurf eines Systems ist es wichtig, ein Augenmerk auf den Benutzer zu richten, welcher das System später bedienen soll. Im Gegensatz zu Maschinen sind die Verhaltensweisen von Menschen aber hochgradig nichttrivial. Um dennoch ein gelingendes Konzept entwerfen zu können, lohnt es sich, menschliches Verhalten zu erforschen.

Bei der Lektüre von Publikationen der Verhaltensforschung fällt auf, dass sich die Theorien zum menschlichen Verhalten teilweise stark unterscheiden. Auf der einen Seite stehen Theorien, welche besagen, dass Menschen nach einem rationalen Schema Entscheidungen treffen, um so einen möglichst großen Nutzen zu erlangen. Da jeder Mensch seinen Nutzen maximieren möchte, lassen sich daraus relativ einfach aussagekräftige Modelle erarbeiten. Mit solchen Modellen ist es dann möglich, das Verhalten einzelner Personen vorherzusagen und dieses bewusst zu steuern.

Gegen solche Modelle sprechen jedoch Beispiele, aus denen hervorgeht, dass der Mensch nicht immer den eigenen Nutzen maximiert und teilweise sogar gänzlich irrational handelt. Grundlegend ist die Annahme, dass der Mensch beschränkt ist und zum Zeitpunkt seiner Entscheidungen nicht auf alle möglichen Informationen zugreifen kann. So werden in der Praxis häufig Heuristiken angewandt, um dennoch eine akzeptable Entscheidung treffen zu können.

Im ersten Abschnitt wird ein Überblick über die Spieltheorie gegeben, da sie durch ihre normativen Modelle einen wichtigen Beitrag zum untersuchten Thema leistet.

Im zweiten Abschnitt wird auf die Rational Choice Theorie (RC-Theorie) eingegangen.

Der dritten Abschnitt wird dem Forschungsprogramm der „begrenzten Rationalität“ gewidmet. Dieses ist versucht Lücken der RC-Theorie zu füllen und wird deshalb auch oft mit dieser verglichen.

Abschließend wird auf die Bedeutung der Verhaltensforschung für die Internet- und Kommunikationstechnologie hingewiesen.

2. DIE SPIELTHEORIE

2.1 Einleitung

Bei einem Fußballspiel kommt es zum Elfmeterschießen. Der Torwart steht nicht ganz in der Mitte zwischen den beiden Pfosten. Dadurch ist es schwieriger für ihn, einen Ball zu fangen, wenn der Schütze in das entferntere, rechte Eck zielt. Dies weiß ein Schütze und zielt deshalb oft auf die freie Seite. Diese Verhaltensweise kennt ein erfahrener Torwart natürlich und kann so den Schützen gezielt steuern, auf eine bestimmte Seite zu schießen. Dadurch hat der Torwart den Vorteil, sich schon in Gedanken darauf vorbereiten zu können, um dann rechtzeitig auf die rechte Seite zu hechten. Dies erhöht die Wahrscheinlichkeit, dass der Torwart den Ball abwehren kann.

Ein erfahrener Schütze weiß allerdings auch, dass ein Torwart diese Taktik manchmal gezielt anwendet. Er kann sich also dafür entscheiden, scheinbar irrational auf die besser geschützte linke Hälfte zu schießen, da der Torwart dies nicht erwartet. Doch was ist, wenn der Torwart diese Taktik voraus sieht? Eine ähnliche Fragestellung untersucht [13]. Das Nash Gleichgewicht (Abschnitt 2.2) bietet eine Lösung für dieses Spiel.

Die Spieltheorie beschäftigt sich mit derartigen Entscheidungen für mehrere beteiligte Akteure. Ein wesentlicher Bestandteil sind die Erwartungen über die Entscheidungen der Spieler, welche die Entscheidungen aller Spieler beeinflussen. Das Ziel der Spieler ist immer ihren persönlichen Nutzen zu maximieren. Sie handeln egoistisch und helfen den anderen Spielern nur, wenn sie dadurch einen Vorteil erlangen.

2.2 Das Nash-Gleichgewicht

Das Nash-Gleichgewicht ist ein elementares Lösungskonzept der Spieltheorie. Es ist nur dann erreicht, wenn sich beide Spieler in einer stabilen Situation befinden, wenn es sich also für keinen der Spieler lohnt, die Strategie zu ändern.

doi: 10.2313/NET-2014-03-1_05

Tabelle 1: Einfaches Spiel

		Student 2	
		Anstrengen	Entspannen
Student 1	Anstrengen	(2,2)	(1,1)
	Entspannen	(1,1)	(0,0)

Tabelle 2: Haftstrafen beider Spieler in Jahren

		Spieler 2	
		Schweigen	Gestehen
Spieler 1	Schweigen	(4,4)	(15,1)
	Gestehen	(1,15)	(10,10)

2.2.1 Beispiel

Diese Situation wird an folgendem Beispiel deutlich: Es gebe zwei Studenten, welche zusammen an einem Projekt arbeiten. Beide haben die Wahl, sich für das Gelingen der Arbeit anzustrengen, oder sich zu entspannen und zu hoffen, dass der Partner genügend arbeitet.

Falls keiner der Beiden sich anstrengt, wird das Ergebnis für beide sehr schlecht werden. Strengt nur einer sich an, bekommt das Team eine durchschnittliche Note. Bei beidseitiger Anstrengung wird die Note für Beide am Besten.

Tabelle 1 zeigt die Nutzenfunktion für beide Spieler in Abhängigkeit ihrer Strategien. Einer schlechten Note wird der Nutzenwert 0 zugewiesen, einer durchschnittlichen Note der Wert 1 und einer guten Note den Wert 2.

Nun gibt es für jeden Spieler eine Entscheidung. Die Voraussetzung für ein Nash-Gleichgewicht ist, dass es für keinen Spieler einen Anreiz gibt, von der eigenen Strategie abzuweichen. Beim Prüfen der Fälle fällt auf, dass deshalb nur eine Strategienkombination stabil ist. Dies ist auch intuitiv, denn nur wenn sich beide Studenten anstrengen, können sie den maximalen Nutzen erlangen. Bei allen anderen Strategiekombinationen kann die Situation durch einen Studenten verbessert werden und ist deshalb nicht stabil.

2.2.2 Verschiedene Arten von Gleichgewichten

Es gibt zwei verschiedene Arten von Nash-Gleichgewichten: Pure strategy Gleichgewichte und mixed strategy Gleichgewichte. Eine „pure strategy“ bedeutet, dass es eine Ideallösung gibt, welche immer die beste Lösung ist. Die Strategie muss selbst dann noch gut sein, wenn der Gegner von dieser Strategie weiß. Im klassischen Gefangenendilemma (Abschnitt 2.3) wäre das Gestehen eine solche pure strategy. Beidseitiges Gestehen ist ein pure strategy Gleichgewicht, da keiner der beiden Spieler durch Abweichen von der Strategie einen Vorteil erlangt.

Eine mixed strategy bezeichnet das Auswählen einer Strategie mit einer gewissen Wahrscheinlichkeit. Das Verhalten ist also randomisiert. Eine mixed strategy kann also durch die Variation der Wahrscheinlichkeiten, eine bestimmte Strategie auszuwählen, verändert werden. Natürlich ist das mixed strategy Nash Gleichgewicht eine Besetzung von Wahrscheinlichkeiten für die Strategien durch beide Spieler, von der keiner der beiden Spieler von sich aus abweichen will. [19]

Beim Beispiel des Elfmeterschießens (Abschnitt 2.1) kann den Strategien „nach links schießen“ und „nach rechts schießen“ entsprechend eine gewisse Wahrscheinlichkeit zugewiesen werden. In [13] wurde gezeigt, dass für dieses Spiel ein solches Gleichgewicht existiert.

2.3 Probleme der Spieltheorie

Ein Nash-Gleichgewicht muss allerdings nicht zwingend die Ideallösung sein. Dieses Problem sieht man unter Anderem beim Gefangenendilemma: Zwei Gefangene werden unabhängig voneinander befragt und aufgefordert, ihre gemeinsame Tat zu gestehen. Die beiden Gefangenen werden im Modell Spieler genannt und versuchen ihren Nutzen zu maximieren. In diesem Fall ist der Nutzen besonders hoch, wenn der Richterspruch angenehm ausfällt.

Für die Dauer der Haftstrafe hängt es davon ab, ob die Spieler die Tat gestehen, bzw. ob einer der Spieler die Tat gesteht. Kooperieren beide Angeklagte, so erhalten sie ein strafmilderndes Urteil und damit eine Haftstrafe von nur 10 Jahren. Gesteht keiner der Beiden, so können sie nicht überführt werden und erhalten für einige kleinere Vergehen eine Haftstrafe von nur jeweils 4 Jahren. Um einen Anreiz für ein Geständnis zu geben, wird die Kronzeugenregelung angewandt, welche eine Strafreduktion von drei Jahren mit sich bringt, fall nur einer der Angeklagten gesteht. Somit wird im letzten Fall ein Angeklagter für 1 Jahr inhaftiert, der andere für 15 Jahre. Die Strafen in Abhängigkeit der Aktionen der Spieler sind in Tabelle 2 zusammengefasst. [9]

Die Spieltheorie geht davon aus, dass Spieler 1 bei seiner Entscheidung mögliche Entscheidungen seines Gegenspielers berücksichtigt. Die möglichen Entscheidungen sind in diesem Fall sehr überschaubar: Für den Fall, dass sich Spieler 2 entschieden hat, die Tat zu gestehen, bringt ein Geständnis einen größeren Nutzen mit sich, als zu schweigen. Der Spieler wird dann nämlich statt 15 Jahren nur 10 Jahre inhaftiert. Doch auch für den Fall, dass Spieler 2 an seiner Lüge festhält ist ein Geständnis besser, denn dann reduziert sich die Strafe von 4 Jahren auf 1 Jahr. Die Strategie zu Gestehen ist in jedem Fall die bessere Alternative, man nennt sie deshalb dominant. [9]

Obwohl also eine gemeinsame Lüge zusammen nur zu 8 Jahren Haft führt, werden sich die rational handelnden Spieler laut Spieltheorie für ein Geständnis entscheiden, welches zu insgesamt 20 Jahren Haft führt (siehe Abschnitt 2.2). Erstere Strategie ist nicht stabil, da es einen guten Grund gibt, von der Strategie abzuweichen. Dieses Prinzip funktioniert, da die beiden Spieler keinen bindenden Vertrag vereinbaren können.

Was aber geschieht, wenn es sich um ein widerholtes Spiel handelt. Wenn also die beiden Angeklagten auch in der Zukunft vorhaben, Verbrechen zusammen zu begehen. Dann hat das Abweichen von der gemeinsamen Strategie, nicht zu gestehen, negative Folgen. Es gibt zwei Varianten solcher wiederholter Spiele: Mit einer begrenzten, oder mit einer unbegrenzten Anzahl an Wiederholungen.

Falls die Spieler wissen, dass die gespielte Wiederholung die

letzte ist, werden sie sich wieder wie im Spiel ohne Wiederholungen verhalten und den Mitspieler verraten, da sie nach dem letzten Spiel nicht mehr auf ihn angewiesen sind. Da beide Spieler dies tun, wird das zweitletzte Spiel das letzte Spiel, in dem eine Entscheidung gefunden werden muss. Jetzt verhält es sich wieder wie im letzten Spiel, da man ja sowiso davon ausgeht, vom Gegenspieler im letzten Zug verraten zu werden. Durch Induktion kann dies theoretisch bis zum ersten Spiel fortgesetzt werden. Demnach verhalten sich die Spieler wie im Einzelfall.[20]

Ist die Zahl der Wiederholungen hingegen unbegrenzt, so stellt sich dieses Phänomen logischerweise nicht ein.

Ein praktisches Problem der Spieltheorie ist, dass es nicht immer offensichtlich ist, welche Art von Spiel gerade gespielt wird. Dies kann ein Grund für falsche Verhaltensprognosen und irrationales Verhalten sein.

3. DIE RATIONAL CHOICE THEORIE

Rationales Verhalten bedeutet laut Rational Choice Theorie, dass eine feste Entscheidungstheorie angewandt und nach ihr gehandelt wurde. Dabei kann das Ziel sehr unterschiedlich sein. Die klassische RC-Theorie im Sinne des homo-oeconomicus Modells sieht dabei die reine Nutzenmaximierung als Ziel. Dieses Modell ist jedoch überholt und es konnte öfters gezeigt werden, dass es nicht der Realität entspricht. (vgl. Kapitel 4) Menschen maximieren nicht immer ihren eigenen Nutzen. Andere Modelle sehen das Ziel in der Maximierung des erwarteten Nutzens (Neumann-Morgenstern-Theorie), oder des subjektiv erwarteten Nutzens (SEU-Theorie).

Der Begriff der Rational Choice Theorie (kurz RC-Theorie) wird vielfach verwendet, wenn gezeigt werden soll, dass menschliches Verhalten durchdacht ist und einem rationalen Aufbau genügt. Die Theorie besagt, dass Menschen mit eingeschränkten Ressourcen versuchen, das beste Ergebnis zu erhalten. Das beste Ergebnis ist definiert, als das Szenario mit dem höchsten Nutzen.

Es folgen vier wichtige Axiome für die RC-Theorie:

1. Akteure stehen im Zentrum des Interesse.
2. Die Akteure besitzen beschränkte Ressourcen.
3. Es gibt mindestens zwei Wahlalternativen. Für die Alternativen existieren Präferenzen.
4. Es existiert eine klare Entscheidungsregel, welche entscheidet, wie sich der Akteur verhält.

Die Akteure sind normalerweise Personen. Man kann die Modelle aber auch auf andere Bereiche anwenden, denn auch Staaten oder Organisationen können als Akteure interpretiert werden. (vgl. auch [12])

Die Ressourcen der Akteure können verschiedenartig sein. Darunter fallen materielle Güter, oder Geld. Natürlich kann aber auch Zeit als ein Gut interpretiert werden, ebenso soziale Anerkennung. Grundsätzlich streben die Akteure nach einer Maximierung der Ressourcen. Restriktionen können durch Regelungen und Gesetze gegeben sein und schränken den Handlungsspielraum ein.

Präferenzen sind als Vorlieben der Akteure zu verstehen. Um Aussagen über die Präferenzen eines Akteurs zu treffen wird eine Nutzenfunktion eingeführt, welche die Güter auf einen ordinalen Nutzenwert abbildet. So können verschiedene Alternativen nach ihrem Nutzen gegenübergestellt werden. Der Akteur präferiert die Alternative mit dem höchsten Nutzenwert.

Entscheidungsregeln können je nach RC-Theorie sehr unterschiedlich geartet sein. Meistens geht es bei der Entscheidungsregel allerdings um Maximierung. Bei der Neumann-Morgenstern-Theorie wird der erwartete, bei der SEU-Theorie der subjektiv erwartete Nutzen maximiert. Der subjektiv erwartete Nutzen kann variieren, je nachdem, wie wichtig ein bestimmtes Gut für den Akteur ist. Es gibt allerdings auch andere Entscheidungsregeln. Ein Beispiel für eine solche Regel ist Minimax. Es ist eine sehr pessimistische Regel, die vom schlechtest möglichen Fall ausgeht. Sie versucht das größte Unglück in einem Szenario zu vermindern. [3]

4. BEGRENZTE RATIONALITÄT

4.1 Einleitung: Der Framing-Effekt

Obwohl die Rational-Choice Theorie in vielen Fällen gut verwendet werden kann, um Menschliches Verhalten zu modellieren, gibt es dennoch verschiedene Studien und Beispiele, welche der Theorie des rationalen Agenten teilweise widersprechen.

Die Präsentation von Auswahlmöglichkeit bei einer Entscheidungsfrage (choice architecture) scheint einen Einfluss auf die Entscheidung von Menschen zu haben, obwohl die Information immer noch dieselbe ist. Der Effekt wird als Framing-Effekt bezeichnet. [6]

Laut RC-Theorie dürfte die Entscheidung aber nicht von der Präsentation der Alternativen abhängig sein.

4.2 Definition

Die Rational-Choice Theorie geht davon aus, dass die Akteure alle nötigen Informationen zur Verfügung haben und dann gezielt abwägen, welche Entscheidung den größten Nutzen nach sich zieht. Eine Gegenbewegung zeigt sich im Forschungsprogramm der Begrenzten Rationalität (bounded rationality, BR) ab. Diese gründet auf der kognitiven Beschränktheit von Menschen. Dadurch würde nicht immer die optimale Entscheidung getroffen.

Dieses Feld ist kein Modell oder eine Theorie, sondern eine ganze Sammlung von Theorien. Laut [14] ist der Hauptgegner der BR die RC-Theorie. Der Begriff der begrenzten Rationalität wird jedoch häufig auch anders interpretiert und nur auf das Entscheidungsmodell des „satisficing“ eingeschränkt und der Rational-Choice Theorie untergeordnet (ein Beispiel ist [3]).

Die begrenzte Rationalität grenzt sich von Optimierung und Irrationalität ab[16]. Die Akteure versuchen dabei rational zu handeln und schaffen dies auch zu einem gewissen Grad.

doi: 10.2313/NET-2014-03-1_05

Das Gebiet der begrenzten Rationalität (BR) ist sehr weitläufig und hat in punkto Komplexität und Studienanzahl eine ähnliche Größenordnung, wie die Rational-Choice Theorie. [14]

Theorien der BR sind folgende Punkte gemein:

1. Die kognitiven Leistungsfähigkeit von Menschen ist beschränkt
2. Diese Beschränkung beeinflusst die Entscheidungen der Menschen
3. Je komplexer die Entscheidung, desto stärker werden die Entscheidungen beeinflusst.

Beschränkungen (constraints) können verschiedene Formen annehmen. Eine triviale Beschränkung ist fehlende Information. Der Mensch besitzt ein stark begrenztes Kurzzeitgedächtnis und kann so nur wenige Informationen gleichzeitig verarbeiten [18]. Alleine aus diesem Grund können nicht alle verfügbaren Informationen aufgenommen werden, manchmal liegen Akteuren auch schlicht wichtige Informationen nicht vor.

Aus diesem Grund ist es offensichtlich, dass die Beschränkung die Entscheidungen beeinflusst.

Studien zeigen, dass sich das vorhergesagte Verhalten von Menschen bei BR-Theorien und RC-Theorien stark unterscheiden kann. Dieser Effekt ist allerdings hauptsächlich bei sehr komplexen Entscheidungen zu bemerken. Ist die Entscheidung einfacher, so ist der Nachteil durch selektive Wahrnehmung (Beschränktheit) kleiner. Bei einfachen Spielen liegt zum Zeitpunkt der Entscheidungsfindung ein großer Teil der relevanten Informationen vor. So entspricht das Verhalten in der Anfangsphase eines Schachspiels meist nicht dem objektiven Idealverhalten (sofern ein solches existiert), da die Möglichkeiten eines Zuges sehr vielfältig sind und das Problem dadurch komplex. In der Endphase eines Schachspiels hingegen konvergieren die von beiden Theorien erwarteten Züge.

Im Laufe der Zeit haben sich aus der von Herbert Simons angestoßenen bounded rationality zwei Zweige ergeben: Der optimistische und der pessimistische Ansatz. Auf der einen Seite wird untersucht, wie es sein kann, dass Menschen trotz der Einschränkungen sehr gute Leistungen in komplexen Entscheidungsfragen erbringen können. Wie kann es sein, dass manche Leute sehr gut in einem Schachspiel entscheiden, während andere relativ schlechte Züge machen? Auf der anderen Seite wird das Phänomen untersucht, dass Menschen manchmal sogar in sehr einfachen Situationen nicht die optimale Option auswählen. Dies zeigt den großen Einfluss von Framing (Abschnitt 4.1) auf die Entscheidungen. Eine zentrale Theorie in diesem Forschungsfeld ist die von Kahneman und Tversky veröffentlichte Prospect Theory (Abschnitt 4.4)[14]

4.2.1 Studie: Bereitschaft zur Organspende

Welchen Einfluss die Art der Fragestellung auf die Entscheidung hat, zeigt eine Untersuchung der Organspenden in Europa. Es wurde die relative Anzahl der Organspender im Verhältnis zur Gesamtbevölkerung untersucht. Dabei wurden große Unterschiede festgestellt. Besonders interessant waren die Unterschiede bei Nachbarländern mit ähnlicher Mentalität, jedoch sehr unterschiedlichen Ergebnissen. So existierte in Deutschland ein Spenderanteil von 12 Prozent und in Österreich ein Anteil von 99,98 Prozent. Als Erklärung für diese große Varianz wurden verschiedene Hypothesen aufgestellt, doch es ist auffallend, dass in allen Ländern mit einer sehr hohen Beteiligung eine Zustimmung zu einer Organspende die Standardauswahl auf dem Formular war. Die Bevölkerung hatte trotzdem die Möglichkeit, sich gegen die Organspende zu entscheiden. (opt-out) Diese Länder sind in Abbildung 1 als blaue Balken gekennzeichnet. Andererseits war in Ländern mit relativ geringer Beteiligung die Ablehnung als gesetzlicher Standard definiert. Man musste also explizit einer Organspende im Todesfall zustimmen (opt-in). Die Regierung der Niederlanden versuchte mit wenig Erfolg den Anteil der Spender zu erhöhen und versandten sowohl Informationsmaterial, als auch Formulare. Vielleicht wäre die Lösung aber viel einfacher gewesen: Eine Zustimmung als gesetzlichen Standard zu definieren. [7]

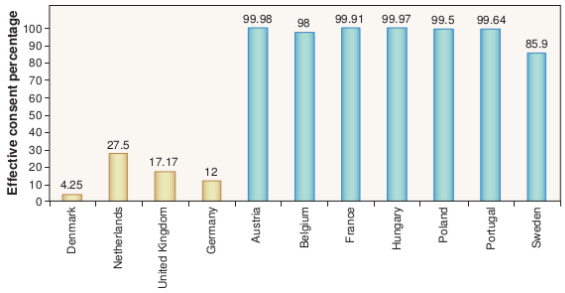


Abbildung 1: Organspender nach Land. Blau: opt-out, Silber: opt-in [7]

Es liegt der Schluss nahe, dass sich Menschen eher für eine Standardauswahl entscheiden. Verstärkt wird dieser Effekt, wenn die Entscheidung sehr komplex ist und erst abgewägt werden muss, welche Alternative die bessere ist. Ein möglicher Grund für die Bevorzugung des Standards ist die loss aversion (siehe Abschnitt 4.4). Wer sich für die Alternative entscheidet, lehnt schließlich gleichzeitig den Standard ab. Da die meisten Bürger allerdings unentschlossen sind und Angst vor Verlust haben, wollen sie sich nicht auf eine Alternative einlassen.

Weitere Erklärungen sind, dass ein Standard als Empfehlung einer Autorität interpretiert werden kann, oder einfach die Tatsache, dass eine Entscheidung nicht bequem ist und Anstrengungen mit sich zieht. [7]

Trotz derartiger Erklärungen steht diese Beobachtung im Gegensatz zu Rational-Choice Theorien.

4.2.2 Rechtfertigung für Verhalten

Befragungen in den untersuchten Ländern ergaben, dass die meisten Menschen ihre Entscheidung für oder wider Organspende begründen konnten. Allerdings ist es nach Analyse der Studienergebnisse nahe liegend, dass die gefällten Entscheidungen hauptsächlich von der Präsentation der Al-

doi: 10.2313/NET-2014-03-1_05

ternativen abhängig sind.

Dies würde aber bedeuten, dass die Argumente nicht dazu verwendet wurden, eine möglichst gute Entscheidung zu treffen, sondern um die eigene Entscheidung im Nachhinein zu begründen. Dies steht im Gegensatz zur Modellvorstellung eines rationalen Agenten, welcher daran interessiert ist, den eigenen Nutzen (oder den Erwartungsnutzen) zu maximieren. Dieses Verhalten kann durch die Verfügbarkeitsheuristik (availability) erklärt werden. Durch die eigene Entscheidung für oder gegen die Organspende sind Argumente, welche die eigene Entscheidung unterstützen, besser abrufbar, als die Argumente der Gegenseite. Das erzeugt ein Gefühl, die richtige Entscheidung getroffen zu haben.

4.3 Heuristiken

4.3.1 Übersicht

Wie in Abschnitt 4.2 gezeigt wurde, müssen Entscheidungen häufig mit unzureichender Information getroffen werden. Kahneman und Tversky argumentieren, dass Heuristiken verwendet werden, um trotz Unsicherheit zu einer genügend guten Lösung zu kommen.[11]

Als Heuristik wird allgemein eine auf Regeln basierte Strategie verstanden, welche in den meisten Fällen zu einer ausreichend guten Entscheidung führt[17]. Eine Heuristik garantiert keine korrekte Lösung. Heuristiken stehen also im Gegensatz zu Algorithmen, welche eine korrekte Lösung finden, solange eine solche existiert und alle Parameter korrekt sind. Heuristiken können als Abkürzungen gesehen werden, welche eine schnellere Entscheidungsfällung erlauben. Sie funktionieren sogar unter unvollständigen oder unsicheren Informationen. [14]

Das Verwenden von Heuristiken für die Entscheidungsfindung ist nicht grundlegend gut oder schlecht, denn es ist sowohl der Grund für relativ gute Ergebnisse in schwierigen Situationen, wie auch für kognitive Verzerrungen. Im Gegensatz zu einem ausgeprägten algorithmischen Vorgehen haben Heuristiken zwar den Nachteil weniger effektiv zu sein und oftmals keine optimalen Lösungen zu finden. Dafür sind sie aber effizienter und schneller lösbar.

Kahneman und Tversky haben in [11] Heuristiken für Entscheidungen unter Unsicherheit untersucht und drei Heuristiken definiert, aus denen sich alle anderen Heuristiken ableiten lassen: Verfügbarkeitsheuristik (availability), Repräsentativitätsheuristik (representativeness), Ankerheuristik (anchoring). Mit diesen Heuristiken kann man mehrere kognitive Verzerrungen bei der Urteilsfindung unter Unsicherheit erklären. So gibt es den Fehler, dass die Häufigkeit von Ereignissen zu hoch geschätzt wird, falls man sich gut an die Ereignisse erinnern kann.

Auf die Frage, warum kognitive Verzerrungen (biases) so schwer zu erkennen und zu verhindern sind, lohnt es sich, etwas in die Kognitionswissenschaft einzutauchen. Diese besagt, dass der Mensch zwei Denkmodi benutzt. Diese werden als System 1 und System 2 bezeichnet. System 1 ist für die Intuition zuständig, während System 2 langsame Gedankengänge ausführt. Für alltägliche Aufgaben, wie Gehen, wird System 1 verwendet, bei komplexeren Aufgaben das System 2. System 1 ist für die Großzahl unserer Gedanken zuständig und versucht ständig, ein kohärentes Bild von der Umgebung zu erstellen. Deshalb ist es sehr auf den Kontext ausgerichtet. Als Beispiel wird das Wort Bank auf eine Weise interpretiert, welche gerade in den Kontext passt. Eine Bank kann ein Kreditinstitut sein. Alternativbedeutungen des Wortes (Sandbank, Parkbank) gehen dabei aber verloren.

Wie schnell durch den Kontext ein falsches Urteil entsteht zeigt Abbildung 2. Die Quadrate im Zentrum haben in beiden Abbildungen die selbe Helligkeit. Das linke wird aber häufig als heller interpretiert, als das rechte Quadrat. Das System 1 ist der Wahrnehmung sehr ähnlich, deshalb können Erkenntnisse über derartige optische Illusionen auch für die Erforschung von System 1 genutzt werden.

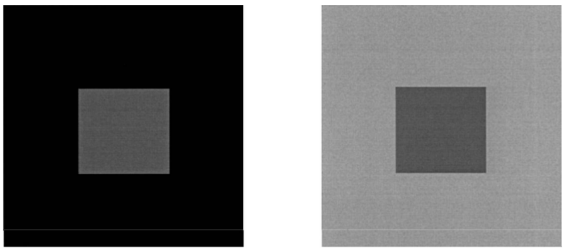


Abbildung 2: Kontextabhängige Wahrnehmung der Helligkeit [4]

4.3.2 Beispiel: Die Ankerheuristik

Um das Prinzip von Heuristiken besser zu verdeutlichen wird hier an einem Beispiel auf die Ankerheuristik eingegangen. Die Ankerheuristik besagt, dass die Umgebung einen Einfluss auf das Urteil von Personen hat. Für die Entscheidungsfindung wird von einem Ankerwert ausgegangen und relativ dazu die Lösung gesucht. Es spielt dabei keine Rolle wie dieser beliebige Wert erzeugt wird.

Natürlich können so auch Entscheidungen bewusst beeinflusst werden. In vielen Studien wird den Probanden ein zufälliger Wert gegeben. Meist folgt eine kurze kognitive Aufgabe mit dem Ziel der besseren Einprägung. So wird die Zugänglichkeit (availability) des Ankerwertes erhöht. Es konnte mehrfach gezeigt werden, dass in darauffolgenden Urteilsaufgaben eine starke Korrelation zwischen dem Ankerwert und abgegebenen Schätzwerten bestand (siehe [5], [10]). Dieser „Framing-Effekt“ widerspricht klar dem Rationalitätskriterium der Invarianz, denn er sagt aus, dass eine Botschaft bei gleichem Inhalt das Verhalten unterschiedlich beeinflussen kann.[6]

So konnte gezeigt werden, dass sogar die Urteilskraft von Experten durch solche zufällige Ankerwerte beeinflusst werden können. In einer Studie würfelten Richter zuerst mit einem Würfel, um eine zufällige Ankerzahl zu erhalten. Danach mussten sie verschiedene Fälle bewerten und es konnte ein Zusammenhang zwischen der gewürfelten Zahl und der Entscheidung der Richter statistisch nachgewiesen werden. Dabei wirkte sich eine längere Berufserfahrung bei den Richtern nicht als förderlich aus. Einer Hypothese zufolge erhöhte das Werfen einer höheren Würfelzahl die Verfügbarkeit von Urteilen über schwerwiegendere Verbrechen

und damit auch die Verfügbarkeit der belastenden Teile des Falles. Dies soll zu einer höheren Strafe geführt haben. [10]

Die Ankerheuristik wird oft in der Ökonomie verwendet, um einen wirtschaftlichen Nutzen zu erzielen. Dies kann beispielsweise in der Preisstrategie der Firma Apple gesehen werden. Die ersten iPads wurden für einen sehr hohen Preis verkauft. Bereits nach einer Woche wurde der Preis jedoch dramatisch gesenkt. Obwohl der neue Preis im Vergleich zu ähnlicher Technologie immer noch relativ hoch war, wurde das Produkt sehr gut verkauft. Es liegt nahe, dass der Einstiegspreis des Produkts eine Art Ankerwert war, an dem zukünftige Preise gemessen wurden. [1]

4.4 Prospect Theory

Die Prospect Theory wurde von Kahneman und Tversky entwickelt. Sie soll zeigen, warum menschliches Verhalten teilweie stark von dem eines rationalen Agenten abweicht und ist eine Alternative zu RC-Theorien, wie der Erwartungsnutzen-Theorie. [8]

Laut Prospect Theory werden Entscheidungen relativ zu einem Referenzpunkt evaluiert. Sie besagt desweiteren, dass Menschen risikoscheu sind, wenn sie eine Entscheidung mit Aussicht auf Gewinn treffen müssen und risikofreudig bei Entscheidungen eigenen Verlusts. Diese Einstellung wird mit der „loss aversion“ begründet. Es bedeutet, dass die Angst vor Verlust größer ist, als die Freude über Gewinn. [4]

5. VERWANDTE ARBEITEN

[21] beschäftigt sich mit betriebswirtschaftlichen Analysen in der Informations- und Kommunikationstechnologie. Die Arbeit geht dabei sowohl auf quantitative Kosten-Nutzen Analysen, als auch auf qualitative Analyse mit Hilfe von Modellen ein. Für Letzteres wird die Spieltheorie als Grundlage herangezogen, um das Verhalten zweier Spieler im Wettbewerb zu modellieren. Zur Analyse wird ein Entscheidungsmodell vorgeschlagen.

[22] beschreibt Erfahrungen beim Design von Systemen mit spieltheoretischen Ansätzen. Dabei dokumentieren die Autoren ihre Versuche, Protokolle so zu entwerfen, dass ISPs einen Anreiz haben, möglichst kurze Routingwege erstellen und nicht die eigennützige „early exit“ auszuführen. Ähnlich gehen sie im Kontext von Multi-Hop Drahtlosnetzwerken vor und setzen ein System auf, welches Betrüger kontrollieren soll. Sie stellen jedoch praktische Schwierigkeiten mit dem normativen Ansatz fest und müssen schließlich leicht davon abweichen.

[23] versucht etwas Ähnliches. Mit einem spieltheoretischen Ansatz soll eine Kooperationsbereitschaft von Knoten in drahtlosen Ad Hoc Netzwerken sichergestellt werden. Im Gegensatz zu [22] wird hier der Versuchsausgang als erfolgreich dargestellt.

6. ZUSAMMENFASSUNG

Zusammenfassend kann gesagt werden, dass die Spieltheorie durch ihren algorithmischen Ansatz sehr gut anwendbar ist. Ein zentrales Resultat der Arbeit ist jedoch, dass die Spieltheorie nicht immer die Praxis widerspiegelt. Sie geht von Idealmenschen aus, welche nicht systematisch in eine Richtung beeinflusst werden können. Ein häufiges Problem bei der praktischen Anwendung der Spieltheorie ist auch, dass die Spieler teilweise nicht wissen, in welchem Spiel sie sich befinden.

Die Entwicklung des Filesharingsystems Bittorrent zeigt uns, wie ein System mit Hilfe der Spieltheorie eingesetzt werden kann. Wenn die Upload-Kapazitäten eines Peers ausgeschöpft sind werden eher Pakete an kooperierende Peers gesendet, als an solche, welche selber nur aus dem System zu profitieren versuchen.

Heuristiken und kognitive Verzerrungen sind ebenso bei der Entwicklung eines Systems zu beachten. Theorien und Studien begrenzter Rationalität zeigen eindrucksvoll, wie stark das Verhalten von der rationalen Norm abweichen kann.

Eine klare Vorhersage für menschliches Verhalten ist deshalb nicht möglich. Wegen der besonderen Wichtigkeit ist es umso mehr zu empfehlen, in Testphasen zu untersuchen, wie sich die Benutzer verhalten.

Eine mögliche Lösung des Problems ist eine Modifikation der Spieltheorie, welche behavioristische Untersuchungen berücksichtigt.

Ist ein System allerdings rein technisch und muss nicht mit menschlichen Benutzern agieren, so bietet die Spieltheorie sicherlich gute Lösungsansätze.

7. LITERATUR

[1] Dan Ariely: *A Beginner's Guide to Irrational Behavior* coursera `https://www.coursera.org/course/behavioralecon`

[2] Berninghaus, S. K., Ehrhart, K. M., Güth, W. (2010). *Strategische Spiele Eine Einfuhrung In Die Spieltheorie* Springer DE.

[3] Diekmann, Andreas, and Thomas Voss: *Die Theorie rationalen Handelns. Stand und Perspektiven* Rational Choice Theorie: Probleme und Perspektiven (2004): 13-29.

[4] Kahneman, Daniel. *Maps of bounded rationality: Psychology for behavioral economics* The American economic review 93.5 (2003): 1449-1475.

[5] Daniel Kahneman, Paul Slovic, Amos Tversky: *Judgment under uncertainty: Heuristics and biases.* Cambridge University Press, Cambridge (UK) 1982.

[6] D. Kahneman und A. Tversky (Hrsg.), (2000): *Choices, values and frames.* Cambridge University Press, Cambridge

[7] Johnson, Eric, and Daniel Goldstein: *Do defaults save lives?* science 302 (2003): 1338-1339.

[8] Gilovich, Thomas, Dale Griffin, and Daniel Kahneman, eds. *Heuristics and biases: The psychology of intuitive judgment* Cambridge University Press, 2002.

[9] Sieg, G. (2010). *Spieltheorie* Oldenbourg Wissenschaftsverlag, München, 3. Auflage.

[10] Englich, Birte, Thomas Mussweiler, and Fritz Strack. *Playing dice with criminal sentences: The influence of irrelevant anchors on experts' judicial decision making* Personality and Social Psychology Bulletin 32.2

(2006): 188-200.

[11] Amos Tversky, Daniel Kahneman (1974): *Judgment under Uncertainty: Heuristics and Biases*, in: Science, Vol. 185, S. 1124-1131

[12] Graham Allison, Phillip Zelikow: *Essence of Decision. Explaining the Cuban Missile Crisis* 2. Auflage, 1999, S. 1-55, hier S. 27f.

[13] Azar, Ofer H., and Michael Bar-Eli. *Do soccer players play the mixed-strategy Nash equilibrium?* Applied Economics 43.25 (2011): 3591-3601

[14] *International encyclopedia of the social & behavioral sciences.* Amsterdam/New York, NY: Elsevier, 2001.

[15] Meehl, Paul E. *Clinical versus statistical prediction: A theoretical analysis and a review of the evidence.* (1954).

[16] Gigerenzer, Gerd, and Reinhard Selten, eds. Bounded rationality: *The adaptative toolbox* Mit Press, 2002.

[17] Simon, Herbert A. *Theories of bounded rationality* Decision and organization 1 (1972): 161-176.

[18] Miller, George A. *The magical number seven, plus or minus two: some limits on our capacity for processing information.* Psychological review 63.2 (1956): 81.

[19] Nash, John. *Non-cooperative games.* The Annals of Mathematics 54.2 (1951): 286-295.

[20] Gächter, S., Kovác, J. (1999), *Intrinsic Motivation and Extrinsic Incentives in a Repeated Game with Incomplete Contracts*, in: Journal of Economic Psychology, 20. Jg., Nr. 3, 1999, S. 251-284; hier: S. 262

[21] Georgios N. Angelou, Anastasios A. Economides *A multi-criteria game theory and real-options model for irreversible ICT investment decisions* Telecommunications Policy, Volume 33, Issues 10-11, November-December 2009, Pages 686-705

[22] Mahajan, Ratul, et al. *Experiences applying game theory to system design.* Proceedings of the ACM SIGCOMM workshop on Practice and theory of incentives in networked systems. ACM, 2004.

[23] Srinivasan, Vikram, et al. *Cooperation in wireless ad hoc networks.* INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies. Vol. 2. IEEE, 2003.

doi: 10.2313/NET-2014-03-1_05

Economic Incentives in the HTTPS Authentication Process

Rémy Degenne
Advisor: Heiko Niedermayer
Seminar Future Internet SS2013
Chair for Network Architectures and Services
Department of Informatics, Technische Universität München
Email: remy.degenne@tum.de

ABSTRACT

In this paper, the authentication system of the HTTPS protocol is considered from an economical perspective. The use of SSL certificates to authenticate web servers has a number of known technical flaws but is widely used. The different actors of the HTTPS authentication system are identified and the study of their roles and incentives for security shows the lack of a clear reason to progress towards a more secure system.

Keywords

HTTPS, Certificate, SSL, Incentives, CA, Security

1. INTRODUCTION

Many websites ask the user for sensitive data like a login and password, that could be used for other purposes, or credit card informations. To send these informations safely, the transmission must be encrypted and the user must be sure of the identity of the organization managing the server. A safe authentication process is essential to establish trust between the user and the organization. This is usually done by using the HTTPS protocol in which Certification Authorities are used to confirm the identity of the server. This system was the victim of multiple successful attacks and is widely criticized. Here we will describe this authentication process and analyze the possible reasons leading the different actors of the process to increase the security.

2. HTTPS AUTHENTICATION PROCESS AND THE USE OF CERTIFICATES

2.1 HTTPS

HTTPS is designed to be a secured version of the HTTP protocol and is widely used to protect sensitive data, like payment information during an online transaction. It is in fact the HTTP protocol stacked on top of a SSL or TLS layer (Secure Sockets Layer / Transport Layer Security) and has the security of these underlying protocols.

One aspect of the SSL/TLS protection system is an identification of the server. When somebody reaches a domain using HTTPS, the server must confirm its identity by providing a valid certificate prior to any data exchange between the client and the server. If it fails to provide valid credentials, the browser will show a warning, informing the user that the identity of the server could not be verified and that she should not proceed as seen in Figure 1.

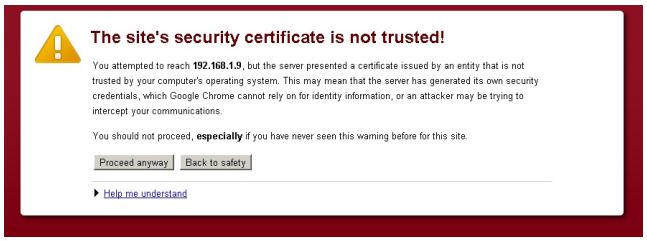


Figure 1: Google Chrome warning - untrusted certificate

The major web browsers include visual clues to tell a user that a website is using HTTPS, like coloring of the address bar or the use of a lock icon. The purpose is to help the user know that the web site is really the one it claims to be and that any exchanged data will be encrypted.

Figure 2: Internet Explorer HTTPS visual clues

2.2 The SSL certificates

The purpose of a SSL certificate is to be sure of the identity of one server. The certification system is centralized and rely on a group of trusted actors that will in turn sell certificates to servers that they trust [12].

Certificates are created by Certification Authorities (CA). Each CA issues a root certificate to identify itself. The Internet browser stores a list of such certificates corresponding to every CA it trusts that allows it to verify the identity of these authorities.

To be identified by a browser using the SSL certification system, a web server must acquire a certificate from one of the trusted Certification Authorities. The link between a server and a root CA must not be direct : a CA can give (or more likely sell) a certificate to an agent that will itself create other certificates and distribute them. A browser will consider that a certificate is valid if it is possible to follow the trust chain back to a known trusted CA.

There are different types of certificates corresponding to different visual clues in the web browsers. To deliver a Domain Validation (DV) certificate, a CA usually checks that the

doi: 10.2313/NET-2014-03-1_06

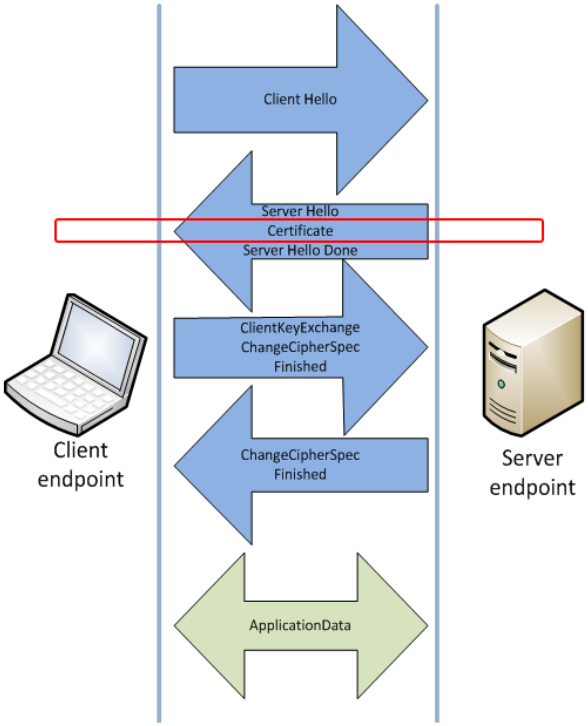


Figure 3: HTTPS Handshake

person owns the validated domain. An Organization Certificate (OV) can be issued after verifying the identity of the organization and will display additional information in the Internet browsers about the organization. There are also Extended Validation (EV) certificates that are designed to have e reinforced security. To obtain one of these an organization must usually have contact with the CA by letter, by phone or face to face and provide proof of its identity, right to use the domain and additional information concerning the organization.

The possible cases of a wrong authentication process are the following :

1. The certificate provided is expired.

2. The certificate can not be verified. it can be self-signed or created by a CA that is not trusted by the browser.

3. The certificate was made for a domain name that does not match the name of the issuer.

4. The certificate is not valid.

The browsers show different warnings for these errors to inform the user about the nature of the problem.

3. THE CERTIFICATION AUTHORITIES AND THE CERTIFICATE MARKET

The actors of the authentication process are the Certification Authorities, the browsers, the organizations or individuals who manage the servers and the users. The Certification Authorities sell certificates to the owners of the servers who buy them to give the user a proof of the identity of the server and thus to allow the user to trust any transaction with this server.

The browser has an important role in the certificate validation because it decides which Certification Authorities can be trusted in its validation process. This makes the organizations managing the major browsers important actors in the definition of the certificate attribution procedures.

The user has contacts with the servers through the browser and expects to be able to use the services provided safely. the user does not have direct contact with the Certification Authorities.

There exists many Certification Authorities trusted by the major internet browsers, in many countries. Microsoft trusts 333 root Certification Authorities [1] and more than a thousand Certification Authorities with the secondary authorities. Few big Certification Authorities that have a huge part of the market. Symantec, Comodo and Godaddy together have more than 75% of the market share.

The certificates sold by the majors Certification Authorities have the same practical value, as these Certification Authorities are trusted by all common browsers. A valid certificate from one trusted CA allows authentication as well as one from an other trusted CA. As presented in [5], a situation with identical products like this one should lead to a competition based on the price of the product. this is not the case and the prices vary greatly between the different Certification Authorities and a few Certification Authorities sells the majority of the certificates on the market. The market shows little signs of a price competition as the Certification Authorities with higher market shares also have high prices.

The Certification Authorities sell the same product but offer different services with the certificates, like support to help for the deployment of the certificates and HTTPS or additional security audit.

4. TECHNICAL FLAWS

The SSL certificate authentication presents a number of known flaws and successful attacks on Certification Authorities did occur.

4.1 A Difficult Deployment

A first problem limiting the use of HTTPS is the impossibility to embed objects that do not support HTTPS in a page. A page using HTTPS wanting to include such an object will trigger a security warning, asking the user if he wants to obtain only the HTTPS content. Many web sites rely on such components, like advertisement banners. This leads to a number of web sites not supporting HTTPS. Some web sites can also want to use HTTPS and become unexpectedly faced with such embedded content that only supports HTTP. A user would face a warning but could need to ignore it to use the web site properly and would lose any security benefits from HTTPS.

4.2 A Weakest-Link Problem

The biggest problem in the certification system is the possibility for any CA to give a certificate for any domain name.

doi: 10.2313/NET-2014-03-1_06

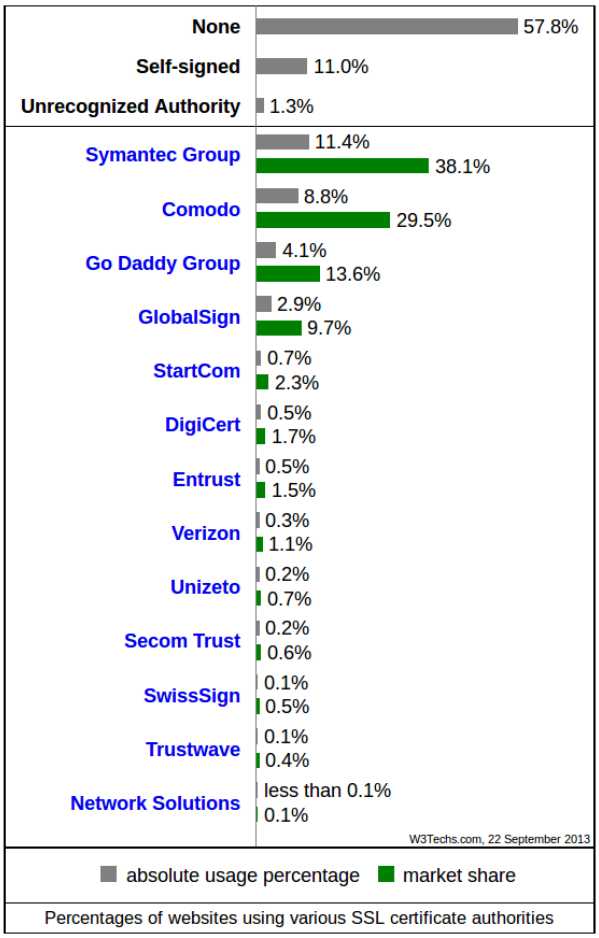


Figure 4: The SSL Certification Market

For example google.com already has a certificate but any CA can issue a different certificate for it that will also be considered valid by the browsers, regardless of the owner of the certificate. A compromised CA, for example a secondary CA that was successfully bought by a malicious agent, can issue certificates for any name to anybody and the certificate will be considered valid. This means that a successful attack on the weakest CA compromises the entire system. The browsers trust more than a thousand Certification Authorities in more than 40 countries.

A successful attack on a CA, DigiNotar, occurred in 2011. Hundreds of false certificates were issued for domain names including the ones of Google, Yahoo! and Mozilla. Man-in-the-middle attacks using the fraudulent certificates were reported in Iran. When this was revealed, DigiNotar was removed from the trusted Certification Authorities lists in the major browsers and went bankrupt. Others successful attacks occurred also on companies having a big market share like Comodo [6]. The certificates issued were revoked and this CA is still trusted by the browsers.

There are widely accepted Certification Authorities in many countries and most of these countries own a CA or have the power to demand false certificates to use them as they want. The certificate system technically allows any of these governments to transgress the security rules.

4.3 Warnings only

An other problem with the certificate system is in the nature of the response to a invalid certificate. The browsers only display a warning that will be ignored by 20% of the users for untrusted certificates errors such as certificates with a wrong name, according to [2]. This means that an attacker wanting to impersonate a known web site will succeed in those cases without needing any real certificate.

4.4 Certificate revocation

When a certificate is misused, it has to be revoked. There are two existing revocation processes : Certificate Revocation Lists (CRL) and the Online Certificate Status Protocol (OCSP).

A CRL is a list maintained by a CA and downloaded regularly by a browser to be checked locally. As the CRL can become a big file the clients employ a caching strategy, meaning that the list is not always up to date [3]. An other reason for this list to be outdated is the rate at which the CA updates the list. An other problem is that browsers tend to ignore parts of these lists to avoid preventing access to popular websites.

With the Online Certificate Status Protocol, the client sends a request to the CA to know if a certificate is valid. This implies that a client must contact the CA each time that it contacts a web site and causes a latency in the HTTPS handshake. The same type of cache problem on the side of the CA as with CRLs is possible, as the CA must also update its lists. A browser will not prevent a user to reach a site if the CA cannot be contacted, because this connection can be impossible for example in the case of a user contacting a payment portal for a public internet access who is prevented to reach any other site until the payment is done. Finally, OCSP allows the CA to gain information on all web sites with certificates that the user visits and this is a Privacy problem.

5. ACTORS AND THEIR SECURITY INCENTIVES

There are four types of actors in the certificate authentication system : certification authorities, browser vendors, server owners and users. All these actors have few incentives to increase the security of the certificate authentication system as it is.

5.1 Certification Authorities

It is difficult to know the details of the security of the Certification Authorities. DigiNotar was audited after the successful attacks it suffered and it appears that they did not use an antivirus software and had weak root passwords among other problems.

The security procedures to verify the identity of the certificate buyers are almost non-existent for Domain Validation certificates and depend greatly on the CA for Organization Validation certificates. The Extended Validation certificates

are subject to strict rules defined in concert with the major browser vendors.

Liability could be a security incentive for the Certification Authorities but the Certification Authorities place all responsibility on their clients (the servers), who denies this responsibility in their user's terms of agreement. Thus the companies that make the certificates are not responsible of their failure. The reputation loss could be a significant cost in this case but the successful attacks on VeriSign and Comodo did not lead to a ban of their certificates and the big Certification Authorities are considered 'too-big-to-fail' and thus have a weaker incentive.

5.2 Browsers

The organization behind an internet browser has two main purposes that dictates their policy regarding the authentication security. They have to make sure that the user can access as much web sites as possible and that the user does it safely. These two goals can conflict and a browser can have a lower security policy in order to increase its usability.

Some web sites do not support HTTPS and the ones supporting it are not all safe. According to SSL Pulse [8], only 24.6% of the 168,000 most visited web sites can be considered secure, and only 823 support HTTP Strict Transport Security, a protocol that restricts data exchange to HTTPS only. A browser cannot offer only access to sites well protected without preventing the use of a huge part of the web. The warning procedure in case of an authentication problem is also designed to allow the user to enjoy web services in an environment where the HTTPS protocol is not perfectly applied.

The attacks on Comodo and DigiNotar are a good example of an adaptation of the security policy according to usability requirements. DigiNotar was a minor actor of the certificate market and the browsers removed their certificates from the trusted Certification Authorities lists as a result of the security breach. In the case of Comodo, holder of 12% of the market share according to [1], the browsers did not remove the CA from the trusted Certification Authorities lists but made an effort to remove only compromised certificates. [1] argues that this is a too-big-to-fail case : one browser can not remove all Comodo certificates without preventing its users to access a large part of the major web sites.

The browser organizations are also agents with the power to negotiate security features with the Certification Authorities. They are the ones who decide if a CA is trusted or not and as such can influence the certificate deliverance procedures. The CA/Browser Forum for example regroups many Certification Authorities and browser software vendors and aims to define the Extended Validation certificate standard [15]. As noticed before, it is difficult for a browser to ban an important CA and thus this power of decision of the browser providers is limited.

Browsers vendors have an incentive to provide a good level of security to the user because it is part of the service quality of this browser but this is strongly mitigated by usability concerns and leads to browsers having a fail tolerant policy.

5.3 Organizations owning servers

The organizations managing servers are the clients of the Certification Authorities and buy certificates to make the user trust their service. Only 35% of the top 1000 web sites have a SSL certificate and 6.8% have an Extended Validation certificate. A server owner uses a certificate in most cases to protect payment and login data transfers.

As every certificate has the same use regardless of the CA that issued it, a great number of server owners buy cheap Domain Validation certificates [5] that allow them to use the HTTPS protocol but do not give the user any information on the identity of the owner of the certificate. Many companies also buy valid certificates but use them wrong for costs reasons : a company can for example have a valid certificate for a domain and use it also for subdomains. this is one of the factors explaining the great number of domain mismatches in valid certificates (see figure 5) [5]. The difficulty and the cost of maintaining a correct deployment of the certificates is an other factor.

The CA with higher costs are also big actors of the market, especially for Extended Validation certificates. [1] explains this fact by the support sold with the certificate, by a reputation factor, by the pressure on the buyer from his hierarchy resulting in the choice of a leader of the market perceived as safer and by the perception that these leaders are too big to see their certificates invalidated. This last reason is the result of a preference for a maintained usability in case of a failure of the certificate system over the avoidance of a security risk.

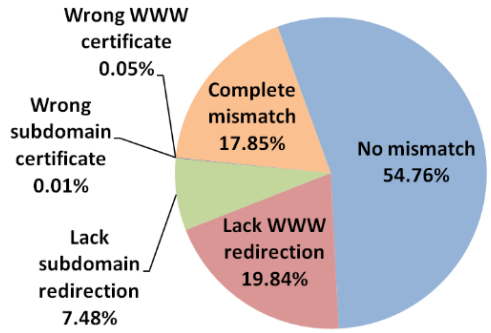


Figure 5: Domain mismatch among trusted unique certificates with valid signatures

The companies using certificates want to send trust messages to the users but weight their security efforts with their costs. An organization that does not choose to use an Extended Validation certificate has no interest in doing more than what is requested to have the user navigate their site without security warnings.

[4] shows that the EV certificates does not increase significantly the trust of the user. A consequence is that a company gains all possible trust benefits by using a Domain Validation certificate, that does not even provide information on the identity of the owner.

doi: 10.2313/NET-2014-03-1_06

5.4 Users

Studies like [2] suggest that a large part of the users ignore the SSL errors. At least 20% of the users would ignore a warning that the name in the certificate and the name of the domain do not match. This percentage is larger with the other types of errors. The type of certificate seems to have few effect on the trust a user places on a web site [4]. Certificates designed to convey more trust like Extended Validation certificates do not increase the perceived trustworthiness of a server. In a study presented in [18], 48% of the participating users stated that nothing bad was happening when confronted to a certification error.

The environment of the user is also misleading. Some web sites use 'trust seals' provided by the Certification Authorities that are shown in the content of a page and should help the user to know that the site is secured [20]. These seals are a content of the page and thus do not provide any real security information. They are misleading for this reason and for their effect on the confusion between browser chrome and page content present in many users, who do not know where a valid security visual clue can be shown [19]. An other caracteristic of the web environment is the irregularity of the appearance of HTTPS clues. Some websites use HTTPS only for a sign-in page and use HTTP everywhere else. Thus, it is usual to visit a page without HTTPS or to see the HTTPS indicators disappear between two pages. The actual situation is one in which the users know only little about security and the practical use of HTTPS make it hard to make good use of the security visual clues.

The user lacks information to control the authentication process. As the browsers accepts certificates silently when they are valid, only a minority of users caring much for security will try to know which CA signed a certificate. A user does not know in general which CA he should trust and will not detect a suspicious CA.

The user who cares much about the security places himself in the same situation as described for a browser : the number of sites he can access is really small and he loses much in terms of usability.

According to [9], a user ignoring certificate warnings gains from this. The user who try to avoid malicious sites will make some effort in the process and try to adapt to the warnings and this is a cost.

The potential gain is to avoid a man-in-the-middle attack, but if the user only adapts to the warnings it is likely that he has a dangerous usage of the sites anyway. For example, accessing the site without typing https:// in the url often means that the user accesses the HTTP site and is then redirected to the HTTPS site. In this case, the attack can occur before the HTTPS site is reached. Worse, as almost none of the phishing sites published on PhishTank use certificates [9] [14], almost every warning is a false positive. Sites using certificates are nearly 100% honest. Ignoring the security warnings completely can be a winning decision in this context. The 'stupid' user is in fact acting as a rational agent.

Table 1: Security incentives for the HTTPS actors

Actor	Security incentives
User	Protect his data
Server	Send a trust message
Browser	Provide good service to the user
Certificate Authority	Reputation loss in case of fail

Table 2: Factors limitating the increase of security

Actor	Limitations
User	Limited control, effort cost
Server	Costs of additional security
Browser	Usability in conflict with security
Certificate Authority	Small consequences of a fail

6. TECHNICAL SOLUTIONS AND ECONOMIC INCENTIVES

Technical and regulatory approaches are currently studied to avoid the problems of the current HTTPS system. A regulation is a possible tool that the users can use collectively to influence the other actors of the process, something that they cannot do individually.

6.1 Technical improvements

Here are presented three improvements currently in use or proposed. These are small changes and they do not address the weakest-link problem of the certificate system.

Google Chrome use a mechanism named Public Key Pinning to authenticate the most visited web sites. This is a whitelist system where the browser stores the keys corresponding to the major servers and the certificates of these servers must correspond to the known keys. It allows the extension of the usability of these sites in the case of a corrupted CA but is only possible for a few web sites. A variant of this certificate pinning is a mechanism in which a server can tell a browser to remenber a given certificate for a given amount of time and that the certificate will not change in this time period. During later connections, the browser can verify that the certificate did not change. Indeed a change of certificate is likely to be the sign of a fraudulous certificate because a server typically change its certificate once in a year.

in [3] a Short-Lived certificate is proposed to make the revocation of certificates easier and avoid certificate revocation lists : a certificate becomes obsolete after a few days and is then invalid if it is not renewed. The expired certificates must be strictly refused for this method to increase the effectiveness of the revocation process.

A strong form of HTTPS was proposed in 2012 to allow the administrator of a web site to set the server as 'HTTPS only'. This is named HSTS for HTTP Strict Transport Security [23]. In this case, the server can only be accessed through HTTPS and any certification problem ends the connection instead of only raising a warning. The client browser remenbers that the site should only be accessed by HTTPS and will also raise an error if it tries to use HTTP. This is a good way of making sure that any connection to the server will benefit from the HTTPS security but has a num-

doi: 10.2313/NET-2014-03-1_06

ber of drawbacks. The first one is the cost of this system for the server organization. As we saw earlier, many web sites have an implementation of the certicication system that is not perfect, and many warnings are raised due to benign mistakes, like a certificate valid for a domain name but not for a specific subdomain. In the case of HSTS, an imperfect implementation leads to a unusable web site. A second problem is contained in the principle of HSTS: if for some reason the certificate is not valid, even if the web site administrator is not responsible for the failure, the site will not be accessible. This can be a wanted feature to maintain strict security but can hurt the usability.

A complementary approach to reinforce the security of HTTPS is to improve the quality of the information given to the user. In the current system, the security is user-centered [17], meaning that the user has to make the decision to pass through a warning or not. To be efficient, this system needs a clever user. The improvement of the security can be a consequence of the improvement of the visual information provided to the user, as studied in [19].

6.2 The European Regulation

As most of the major Certificate Authorities are under the jurisdiction of the European Union, an EU law can affect the certification system and could be the incentive that is needed to increase the security. The EU Commission proposed in June 2012 such a regulation. The texts is targeted at the Certificate Authorities and does not affect the browsers or the web sites. It places the liability on the CAs for any damage caused by a security problem related to the issued certificates. In [1], it is noted that a small company like DigiNotar could not have survived this liability in many cases as it could be the cause of damage to companies as big as Google : a liability spread along the HTTPS chain depending on the causes of the problem could be a better approach.

The EU proposes to control the security levels of the Certification Authorities and to force them to report incidents and their effects. indeed VeriSign did not reveal the breaches in their security before it was discovered by Reuters two years later. on the other side, the EU proposal does not address the issue of the HTTPS implementation in the websites. The enforcement of the security controls is left to the member states.

This regulation proposal aims to control a number of Certification Authorities in the EU to impact the HTTPS system globally but this does not solve the principal design problem of the CA system. As the fall of any CA in the world means the failure of the entire HTTPS trust mechanism, a local regulation without the removal of this technical issue may fail to address the core of the problem.

7. CONCLUSION

The HTTPS protocol is the widely used mean of authentication of websites and it suffers from important technical flaws. These technical flaws are combined with a situation in which nobody gains clearly by enforcing strict security. Some Certification Authorities are too big to be in danger when they suffer a security breach, the browsers need to guaranty security but it is in conflict with the usability, the companies owning servers have few means to show their security efforts and as a result few reasons to pay for them and the user, who is the most interested in an increase in security, has almost no information or control over the process. There are some efforts to find technical solutions as well as new regulations for web authentication

8. REFERENCES

[1] Hadi Asghari, Michel J.G. van Eeten, Axel M. Arnbak and Nico A.N.M. van Eijk: *Security Economics in the HTTPS Value Chain*, In Proceeding of the Twelfth Workshop on the Economics of Information Security, 2013

[2] Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., and Cranor, L. F. (2009, August): *Crying Wolf: An Empirical Study of SSL Warning Effectiveness*. In USENIX Security Symposium (pp. 399-416)

[3] Topalovic, Emin, Brennan Saeta, Lin-Shung Huang, Collin Jackson, and Dan Boneh: *Towards Short-Lived Certificates*, Web 2.0 Security and Privacy (2012).

[4] Jani Suomalainen: *Quantifying the Value of SSL Certification with Web Reputation Metrics*, ICIMP 2012 : The Seventh International Conference on Internet Monitoring and Protection, 2012

[5] Vratonjic, Nevena, Julien Freudiger, Vincent Bindschaedler, and Jean-Pierre Hubaux: *The inconvenient truth about web certificates* In Economics of Information Security and Privacy III, pp. 79-117. Springer New York, 2013.

[6] *Comodo admits two more registration authorities hacked* `http://www.infosecurity-magazine.com/view/16986/comodo-admits-two-more-registration-authorities-hacked`

[7] *Key Internet operator VeriSign hit by hackers* `http://www.reuters.com/article/2012/02/02/us-hacking-verisign-idUSTRE8110Z820120202`

[8] *SSL Pulse page* `https://www.trustworthyinternet.org/ssl-pulse/`

[9] Herley, Cormac. *So long, and no thanks for the externalities: the rational rejection of security advice by users* In Proceedings of the 2009 workshop on New security paradigms workshop, pp. 133-144. ACM, 2009.

[10] *W3Techs Web technology Surveys* `http://w3techs.com/technologies/overview/ssl_certificat`

[11] FUNG, Adonis PH; CHEUNG, K. W: *SSLock: sustaining the trust on entities brought by SSL* In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. ACM, 2010. S. 204-213.

[12] Pradeep Kumar Panwar, Devendra Kumar: *Security through SSL*, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 12, December 2012

[13] Adams, Anne, and Martina Angela Sasse: *Users are not the enemy* Communications of the ACM 42, no. 12 (1999): 40-46.

[14] *PhishTank page* `http://www.phishtank.com`

[15] *CA/Browser Forum* `https://www.cabforum.org/forum.html`

[16] Ye, Eileen, Yougu Yuan, Sean Smith: *Web spoofing revisited: SSL and beyond*, 2002.

[17] Zurko, Mary Ellen: *User-centered security: Stepping up to the grand challenge.* In Computer Security Applications Conference, 21st Annual, pp. 14-pp. IEEE, 2005.

[18] Friedman, Batya, David Hurley, Daniel C. Howe, Edward Felten, and Helen Nissenbaum. *Users' conceptions of web security: A comparative study.* In CHI'02 extended abstracts on Human factors in computing systems, pp. 746-747. ACM, 2002.

[19] Whalen, Tara, and Kori M. Inkpen. *Gathering evidence: use of visual security cues in web browsers.* In Proceedings of Graphics Interface 2005, pp. 137-144. Canadian Human-Computer Communications Society, 2005.

[20] Stebila, Douglas. *Reinforcing bad behaviour: the misuse of security indicators on popular websites.* In Proceedings of the 22nd Conference of the Computer-Human Interaction Special Interest Group of Australia on Computer-Human Interaction, pp. 248-251. ACM, 2010.

[21] Boehme, Rainer, and Tyler Moore. *The Iterated Weakest Link–A Model of Adaptive Security Investment.* 2009.

[22] Flinn, Scott, and Joanna Lumsden. *User perceptions of privacy and security on the web.* 2005.

[23] Hodges, Jeff, Collin Jackson, and Adam Barth: *Http strict transport security (hsts).* `http://tools.ietf.org/html/draft-ietf-websec-strict-transport-sec-04` 2012.

doi: 10.2313/NET-2014-03-1_06

Getting to know Big Brother

Stefanie Einwang
Betreuer: Matthias Wachs
Seminar Future Internet WS2013/14
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: stefanie.einwang@tum.de

KURZFASSUNG

Es gibt verschiedene Ursachen, warum der Datenverkehr im Internet von verschiedenen Parteien abgehört, manipuliert, verändert oder zensiert wird. Dies geschieht vor allem durch die Filterung von Daten, dem Blockieren von Inhalten oder dem Entfernen von Informationen. Teilweise sind die Ursachen für diese Eingriffe als Hilfe oder Schutz der Bevölkerung anzusehen, bei einigen Gründen spricht dies jedoch eher für die zielgerichtete Beeinflussung der Menschen, um die eigenen Ziele besser zu erreichen. In diesem Paper werden die Gründe und technischen Möglichkeiten erklärt, wie und warum der „Big Brother" auf den Datenverkehr im Internet und auf die Computer zugreift.

Schlüsselworte

Contentfilter, Cookies, Deep Packet Inspection, DNS Manipulation, Firewall, Tracking, Web Bugs

1. EINLEITUNG

Seit den Enthüllungen von Edward Snowden über die Überwachungsprogramme Tempora, Prism und XKeyscore entstehen viele Diskussionen über den Datenschutz und die damit verbundene Überwachung der Bürger. Auch die Politik beschäftigt sich mit dem Thema, jedoch ist noch nicht klar, in welchem Ausmaß E-Mails, Telefongespräche, Chatverläufe oder Ähnliches abgehört und aufgezeichnet werden.

Allerdings kommen immer mehr Fragen auf, die die Internetnutzer zunehmend verunsichern: Wer überwacht den Datenverkehr? Wer wird überwacht? Was wird verändert oder abgehört? Mit welchen Mitteln? Diese Fragestellungen werden im Folgenden beantwortet und geben eine Auskunft darüber, ob der „Big Brother" nur eine Gefahr darstellt, oder möglicherweise auch einen Nutzen mit sich bringt.

So wird im Abschnitt 2 zunächst ein Überblick über den Wandel des Internets von der Entstehung bis heute gegeben, im Abschnitt 3 werden die verschiedenen Interessensgruppen, deren Gründe und Vorgehensweisen dargestellt und abschließend werden im Abschnitt 4 die technischen Grundlagen und Verfahren erläutert.

2. WANDEL DES INTERNETS IM LAUFE DER ZEIT

Zu Beginn der Entwicklungen des Internets war die passive Weiterleitung von IP-Paketen und das Ende-zu-Ende Prinzip die gebräuchliche Architektur. Beim Ende-zu-Ende Argument werden die anwendungsspezifischen Funktionalitäten in den oberen Schichten des Netzwerks implementiert, sodass die unteren Schichten lediglich anwendungsunabhängige Funktionen ausführen, um sämtliche Anwendungen zu unterstützen. Das Internet war dabei ein neutrales Netzwerk, das an zentralen Vermittlungsstellen verwaltet und gesteuert wurde. Die Netzwerkneutralität stellt sicher, dass alle Webseiten und Inhalte gleich behandelt und Anwendungen nicht ausgeschlossen oder bei ihrer Ausführung behindert werden. [5] Es gab keine Einflussnahme auf den Zugang zum Internet und die Informationen, die von den Nutzern konsumiert wurden.

Zwischen 1979 und 1983 wurde das ISO/OSI Schichtenmodell als theoretische Grundlage zur Kommunikation im Internet oder innerhalb von Rechnernetzen entwickelt. Dabei wird zwischen den folgenden sieben Schichten unterschieden, aufsteigend von unten nach oben: Physikalische Schicht, Sicherungsschicht, Vermittlungsschicht, Transportschicht, Sitzungsschicht, Darstellungsschicht und Anwendungsschicht. Jeder Schicht wird dabei vorgegeben, was sie zu tun hat, aber nicht auf welche Weise. Diese strikte Trennung existiert in der Praxis jedoch nicht, da man einerseits die Kommunikationsprotokolle nicht einer bestimmten Schicht zuordnen kann, da dies von der Sichtweise des Betrachters abhängig ist, und andererseits die Trennung der Schichten nicht mit anderen Interessen der Kommunikation übereinstimmen kann. [9]

Auch bei der Implementierung der Funktionalitäten des Internets gibt es heutzutage keine strikte Trennung der anwendungsspezifischen und anwendungsunspezifischen Funktionalitäten mehr. Im Gegensatz zum früher herrschenden Ende-zu-Ende-Prinzip werden jetzt auch anwendungsunspezifische Funktionen in den unteren Schichten implementiert. Dies kann zwar die Ausführung der Anwendungen optimieren, jedoch können die unteren Schichten aber so auch die einzelnen Anwendungen beeinflussen oder blockieren. So kann auch auf die Übermittlung der Daten zugegriffen werden, was zur Überwachung und Manipulation der Inhalte führt. Auf diese Weise geht auch das Prinzip der Netzneutralität verloren, was eine weitere Innovationsfähigkeit des Internets einschränken könnte, da wettbewerbsstärkere Firmen kleinere oder neu entstandene Unternehmen und deren Anwendungen unterdrücken können. [7]

Die Nutzung des Internets ändert sich immer weiter, im Jahr 2012 verwenden rund ein Drittel der Weltbevölkerung das Internet, um Neuigkeiten zu lesen, in Kommunikation zu treten oder ihrer Arbeit nachzugehen. Durch diesen Zuwachs haben vor allem Regierungen das Interesse, die Inhalte zu überprüfen und überwachen oder Zensur zu betreiben, indem Webseiten und deren Informationen gefiltert werden. [12] Dieses Eingreifen in

doi: 10.2313/NET-2014-03-1_07

den Datenverkehr ist länderspezifisch, das bedeutet, dass die Bevölkerung von manchen Ländern Webseiten betrachten und Inhalte veröffentlichen kann, die in anderen blockiert werden.

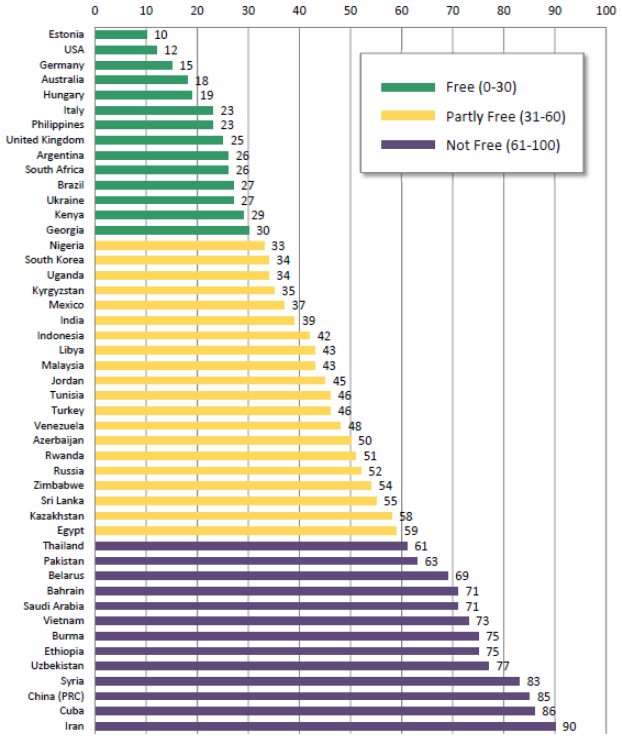


Abbildung 1: Grad der Freiheit im Internet [12], S.21

Der Grad der Internetfreiheit ist in Abbildung 1 dargestellt. Dies wurde in drei Kategorien untersucht, zunächst wie stark die Bevölkerung beim Zugriff auf das Internet oder digitale Medien gehindert wird, zusätzlich inwieweit der Inhalt begrenzt wird und zum Schluss, ob gegen die Benutzerrechte verstoßen wird. [12] Hier ist zu erkennen, dass die Menschen im Iran und in Cuba fast keine Freiheiten haben, im Gegensatz zu Estland und den USA.

Es gibt aber auch weitere andere Manipulationsarten. Das Mit- oder Abhören des Datenverkehrs, das Verändern der übermittelten Daten oder das Unterdrücken der Ausführung bestimmter Anwendungen.

Die technischen Grundlagen für den Einsatz dieser Arten und in welchen Verfahren sie verwendet werden, wird im Folgenden beschrieben. Zunächst wird aber auf die Parteien eingegangen, warum und wie sie diese Vorgehensweisen nutzen.

3. EINFLUSSNEHMENDE INTERESSENSGRUPPEN

Es gibt viele verschiedene Interessensgruppen, die Überwachung und Manipulation des Datenverkehrs veranlassen, um an Daten und Inhalte der Nutzer zu gelangen. Die vier größten Gruppen sind die Politik, Firmen, Webstatistikersteller und Provider, auf deren Motivation und Vorgehensweisen im folgenden Abschnitt genauer eingegangen wird.

3.1 Politik

In Deutschland steht die Politik aktuell im Fokus der Diskussionen bezüglich der Überwachung im Internet und dem dazugehörigen Datenschutz der Bürger. Dazu gehören der von der Regierung finanziell ausgerüstete Bundesnachrichtendienst, die Landeskriminalämter, das Bundeskriminalamt, das Zollkriminalamt, sowie der Militärischer Abschirmdienst. [6]

Der Militärische Abschirmdienst soll die Sicherheit der Bundeswehr gewährleisten. Dazu müssen Informationen gesammelt werden, was einerseits innerhalb der Bundeswehr geschieht und andererseits außerhalb, da auch von hier Gefahren ausgehen können. Dafür bedarf es einer Sicherheitsüberprüfung, um sämtliche Objekte oder Informationen überwachen zu können.

Das Zollkriminalamt ist für die Steuerung von Ermittlungen bei Steuerhinterziehungen, Schmuggeln von Drogen oder anderen illegalen Substanzen und ähnlichen Delikten verantwortlich. Für diese Aufgabe hat das ZKA die Erlaubnis, Informationen zu sammeln, bei Verdacht erfolgt auch eine Online-Überwachung.

Im Inland sind das Bundeskriminalamt und die Landeskriminalämter für den Schutz der Bürger und für die Aufklärung von Straftaten zuständig. Zu diesem Zweck werden Datenbanken geführt, die alle wichtigen Informationen enthalten und die polizeiliche Zusammenarbeit organisieren. Sämtliche mögliche Straftäter oder vermeintliche Vorhaben werden dabei erfasst, was datenschutzrechtlich sehr bedenklich ist. Bei stärkeren Verdachtsmomenten kann außerdem eine Online-Durchsuchung angeordnet werden, um sämtliche Kommunikationsdaten zu analysieren.

Der Bundesnachrichtendienst ist als einziger Geheimdienst für die Auslandsaufklärung zuständig. Ziel des BND ist es, Informationen über das Ausland zu sammeln die für die Sicherheit und die Politik Deutschlands von Bedeutung sind. Dafür wird neben den offenen Quellen wie Zeitungen oder Berichten auch die Telefon- und Internetüberwachung eingesetzt, um an nachrichtendienstlich relevante Informationen zu gelangen. Auf diese Weise können auch internationale Straftaten und Terrorangriffe besser verfolgt und aufgeklärt werden.

Auch der Jugendschutz ist eine Motivation für die Politik, die Inhalte der Webseiten zu überprüfen und gegebenenfalls zu blockieren. Als Vorbild dient hier Großbritannien, die ab Januar 2014 einen sogenannten Pornofilter einführen, der den Zugriff nur bei einer durchgeführten Registrierung erlaubt, die eine Altersbeschränkung von 18 Jahren beinhaltet.

3.2 Firmen

Firmen haben unterschiedliche Anforderungen an das Internet, sodass sowohl die eigenen Produkte gut vermarktet werden können, als auch die Produktivität innerhalb der Firma weiter ansteigt. Ebenso ist die Sicherheit der eigenen Netze eine wichtige Anforderung und soll durch das Eingreifen in den Datenverkehr gewährleistet werden.

Die Motivation lässt sich in zwei große Teile gliedern. Zunächst steht die Sicherheit des eigenen Netzwerks im Vordergrund. Aus diesem Grund werden die Techniken bei den Mitarbeitern eingesetzt. Das private Surfen am Arbeitsplatz soll eingeschränkt werden. Denn dadurch Arbeitsplatz geht die Produktivität zurück, da dem Unternehmen wertvolle Arbeitszeit der Angestellten

verloren geht und die Kapazität der Bandbreite des Internets für produktive Arbeit eingeschränkt ist. Außerdem kann der Mitarbeiter durch private Inhalte Schadsoftware ins Netzwerk einführen, indem E-Mails geöffnet oder Dateien heruntergeladen werden. Auch rechtlich kann das Unternehmen durch das Downloaden von illegalen oder lizenzrechtlich geschützten Inhalten zur Verantwortung gezogen werden. Zudem können vertrauliche Informationen durch die Mitarbeiter nach außen gelangen, was den Konkurrenzunternehmen möglicherweise einen Vorteil verschaffen könnte.

Anhand dieser Probleme, die die Firmen intern lösen müssen werden verschiedene Herangehensweisen eingesetzt. Die häufig zum privaten Surfen verwendeten Webseiten werden mit Hilfe eines Contentfilters gesperrt, sodass keine Zugriffe erfolgen können. Zudem werden sämtliche ein- und ausgehenden Datenpakete über Firewalls überprüft, um einerseits die Sicherheit zu gewährleisten, dass keine Schadsoftware in das Netzwerk gelangen kann, andererseits keine sensiblen Daten nach außen gelangen können. Jedoch werden durch diese Filterungen möglicherweise auch nützliche Inhalte ausgeblendet, wenn sie durch die Firewall oder den Contentfilter blockiert werden, was der Firma wiederum schaden kann.

Als zweiten Ansatz der Motivation lassen sich die Kontrolle des Erfolgs und die Steigerung der Arbeitsleistung und des Produktabsatzes anführen. Hier möchte die Firma das Verhalten ihrer Kunden überwachen, um die Reaktion auf die Einführung neuer Produkte oder Werbemails zu untersuchen. Auch die Kontrolle des Erfolgs ist ein wichtiges Ziel, denn für die Firmen stellt sich die Frage, ob sie ihr Geld wirklich produktiv und effizient investieren. Anhand der Ergebnisse der Analysen des Kundenverhaltens wird die Webseite weiter verbessert und an den Kunden angepasst, sodass der Wert des Unternehmens und damit der Umsatz gesteigert werden.

Dies wird einerseits über Webstatistiken erreicht, die von einem Webstatistikersteller bezogen werden können, oder durch den Einsatz von Cookies oder Web Bugs, die das Nutzerverhalten aufzeichnen und speichern. Diese Datenerhebung ist in § 15 Abs. 3 TMG geregelt: „Der Dienstanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht." [3] Damit kann zielgerichtete Werbung geschalten werden, die anhand des Surfverhaltens auf den Nutzer zugeschnitten ist. Außerdem kann dir Firma nach der Analyse der eingesetzten Web Bugs erkennen, wie der Kunde auf Werbemails reagiert, ob und wann er sie liest, ob er danach auf die Homepage zugreift und diese gegebenenfalls besser auf den Nutzer abstimmen. [12]

3.3 Webstatistikersteller

Der bekannteste Webstatistikersteller in Deutschland ist Google Analytics, was sich auch an der Abbildung 2 erkennen lässt. Google Analytics bietet den Webseiten Betreibern verschiedene Möglichkeiten an, ihre Homepages analysieren zu lassen, beispielsweise die Anzahl und Zeitpunkte der Besuche, den Anteil der wiederholten Besucher der Seite, oder die Benachrichtigungsfunktion bei auffälligen Veränderungen. Dieses Angebot richtet sich an Unternehmen, die ihre Webpräsenz überprüfen und gegebenenfalls durch andere Angebote wie Google AdWords erweitern wollen. [4]

Aber es gibt auch andere Anbieter, die mit der Analyse und dem Sammeln von Nutzerdaten ihr Geld verdienen, zum Beispiel Piwik oder AWStats.

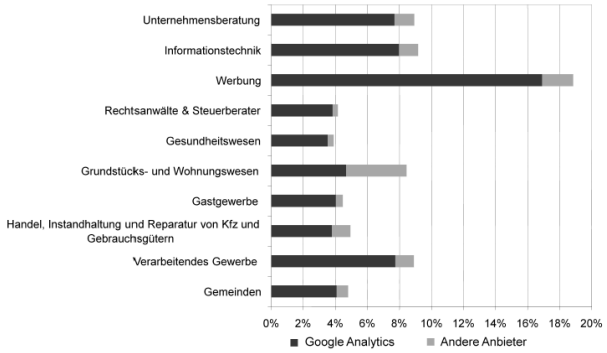


Abbildung 2: Webstatistiknutzer [8]

Anbieter der Webstatistiken machen mit der Analyse von Nutzerdaten ihren Umsatz. Mittlerweile haben sich zudem Informationsallianzen gebildet, über die die Informationen der Nutzer ausgetauscht und weiterverkauft werden. Damit können die umfassenden Wegprotokolle der einzelnen Personen immer weiter und genauer fortgesetzt und anderen Firmen weiterverkauft werden.

Um die Webstatistiken zu erstellen, wird meist mit eigenen erstellten Cookies oder Web Bugs gearbeitet. Hier entscheidet alleine der Dienstleister, welche Daten auf welche Art und Weise gespeichert und analysiert werden.

Eine andere Möglichkeit der Datenerhebung sind Log Dateien. Diese werden vom Betreiber der Webseite erstellt und dann an den Webstatistikersteller weitergegeben, wodurch der Inhaber der Webseite die Kontrolle über die Nutzerdaten hat. [8]

3.4 Provider

Zu den Providern gehören sowohl die Internet- als auch die Mobilfunkbetreiber, die Internetzugänge und Leitungen, sowie Mobilfunknetze zur Nutzung anbieten.

Die Provider haben das Ziel, bestimmte Anwendungen zu sperren, die die Kosten der Nutzung für Dienste des Providers umgehen. Dazu gehören beispielsweise Skype und Voice over IP statt Telefonie oder Instant Messaging statt SMS. Zudem möchten die Anbieter durch Messung der Verkehrsströme herausfinden, an welchen Orten das Netz oder die Leitungen besser ausgebaut werden müssen. Dies geschieht über die Stateful packet Inspection, in der war nicht der Inhalt der Pakete, aber die Art und Menge der Kommunikation überprüft werden kann. [13]

Um die Sicherheit der Computer der Kunden sicherzustellen, werden die ein- und ausgehenden E-Mails und andere ausgetauschte Daten auf Schadsoftware geprüft. Dazu wird die Deep Packet Inspection eingesetzt, allerdings ohne Einsicht von Mitarbeitern, um den Datenschutz der Kunden zu gewährleisten. [13]

doi: 10.2313/NET-2014-03-1_07

4. TECHNISCHE VERFAHREN

Die in 3 aufgezeigten Motivationen der einzelnen Interessensgruppen ziehen eine Reihe technischer Verfahren nach sich, die die Speicherung und die Analyse von Nutzerdaten, die Überwachung von Datenflüssen, oder das Filtern und die Manipulation von Informationen ermöglichen. Diese werden im nächsten Abschnitt genauer erläutert.

4.1 Man-In-The-Middle Angriff

Hauptangriffsziel des Man-In-The-Middle Angriffs ist das Online Banking, aber auch E-Mail Accounts werden ausspioniert. Mit dieser Angriffsmethode werden besonders sensible Daten ausspioniert, mit denen Missbrauch betrieben werden kann.

Bei einem Man-In-The-Middle Angriff dringt der Angreifer in eine Verbindung zwischen zwei Kommunikationspartnern und kann die ausgetauschten Daten in Echtzeit einsehen oder sogar manipulieren. Beide Parteien sehen nicht, dass sie unfreiwillig mit dem dazwischen sitzendem Angreifer kommunizieren, statt ihrem eigentlich erwarteten Kommunikationspartner. Mit diesem Angriff kann auch eine verschlüsselte Verbindung durch Angreifer entschlüsselt und eingesehen werden. [1]

Physikalisch kann dies durch einen direkten Zugriff auf die Leitungen erfolgen, über die der Datenverkehr ausgetauscht wird. In einem WLAN Netzwerk wird meist Snarfing eingesetzt. Die Geräte im Netzwerk werden aufgespürt und im Falle einer Sicherheitslücke wird diese zum Angriff verwendet. Da private WLAN Netze meist verschlüsselt sind, ist die Gefahr in unverschlüsselten öffentlichen WLAN Hotspots deutlich höher. Hier kann auch ein WLAN-Access Point durch einen Hacker nachgeahmt werden, der eine bessere Signalqualität als der original Access Point aufweist. Meldet sich ein mobiles Endgerät an seinem Access Point an, leitet er die Daten zwar zum eigentlichen Access Point weiter, kann aber den gesamten Datenverkehr mitverfolgen. Der Nutzer bekommt von diesem Vorgang nichts mit und kann wie gewohnt im Netz surfen.

Eine Angriffstechnik im lokalen Netz ist das ARP-Spoofing. Dabei werden gefälschte ARP-Pakete zu den Hosts geschickt. Dadurch werden die ARP-Tabellen im Netzwerk so verändert, dass der Datenverkehr dann überwacht werden kann. Um dies zu erreichen müssen beide Hosts, deren Kommunikation überwacht wird, ihre Pakete an den Angreifer schicken. Deshalb sendet er an Host 1 das manipulierte ARP-Paket mit der eigenen MAC-Adresse, statt der von Host 2, und an Host 2 die Nachricht, in der ebenfalls die MAC-Adresse vom Angreifer eingetragen ist. Somit schicken beide Hosts ihre Pakete an den Hacker weiter, der sich damit in der Mitte der Kommunikation befindet.

Eine andere Möglichkeit sind DHCP basierende Angriffe. Dabei simuliert der Angreifer den DHCP-Server, der die IP-Adressen in einem Netzwerk vergibt. Sendet ein Rechner im Netz eine Anfrage nach einer IP-Adresse, antwortet der vorgespielte DHCP-Server schneller als der echte DHCP-Server. Deshalb wird er und seine falsche angegebene Gateway Adresse von den Clients im Netzwerk akzeptiert. Er bekommt auf diesem Weg alle Anfragen der Clients und kann diese einsehen, verändern und weiterleiten. Die Antworten des Webbrowsers kann er abfangen, wenn er den DNS-Server kontrolliert. Hier gibt er seine eigene MAC-Adresse an, sodass alle Pakete zusätzlich zur eigentlichen Zieladresse auch an ihn adressiert werden. [1]

4.2 Cross-Site Scripting

Ziel des Cross-Site Scripting ist es, durch einen in einen Computer oder Webserver eingeschleusten Schadcode die sensiblen Daten des Nutzers zu erlangen und diesem damit zu durch Missbrauch zu schaden oder mit Hilfe dieser Daten das Nutzungsprofil zu erweitern.

Beim Cross-Site-Scripting, kurz XSS, nutzt ein Angreifer eine Sicherheitslücke einer Webanwendung, um Formulare, Passwörter und Cookies des Nutzers auszuspähen. Damit kann er die Cookies manipulieren, die Sitzung übernehmen und die Daten des Nutzers einsehen, verändern oder entfernen. Einsicht in die Daten bekommt der Angreifer meist durch gezielte Täuschung des Anwenders, indem er ihm ein Formular anzeigt, in das die persönlichen Daten eingetragen werden sollen. Zudem hat er die Möglichkeit, Schadcode auf dem Rechner des Anwenders auszuführen, um weitere Informationen zu erreichen. [2]

Die Hacker verwenden meist JavaScript oder Visual Basic Script um einen manipulierten Link auf einem Webserver einzubauen. Dieser wird dann in einem Cookie gespeichert, sodass er bei jedem Aufruf an den jeweiligen Client mitgeschickt wird. Der Link erscheint dem Browser vertrauenswürdig, da er auf einen seriösen Server verlinkt ist. Klickt der Benutzer diesen Link nun an, wird der Code ausgeführt und der Angreifer hat uneingeschränkten Zugriff auf die Sitzung des Opfers. Dieser Vorgang des Angriffs ist in Abbildung 3 dargestellt. Der rote Pfeil zeigt, dass die Daten an den Angreifer gesendet werden, da das infizierte Cookie den Schadcode ausgeführt hat.

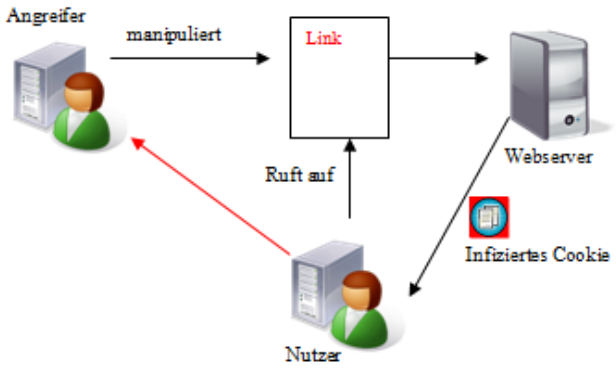


Abbildung 3: Cross-Site-Scripting Angriff

Es gibt drei verschiedene Arten des Cross-Site-Scripting, das persistente, das reflexive und das DOM-basierte XSS.

Beim DOM-basierten Cross-Site-Scripting werden die statischen HTML-Seiten für den Angriff verwendet. Unterstützen sie die Ausführung von JavaScript, wird der Schadcode an das Skript geschickt, das diesen ohne Prüfung ausführt. Für die Durchführung dieses Angriffs wird sowohl ein Skript gebraucht, das Eingabewerte von Daten nicht überprüft, wie auch eine vom Angreifer manipulierte URL, die aufgerufen wird.

Im Gegensatz zum DOM-basierten XSS wird sowohl beim reflexiven als auch beim persistenten Cross-Site-Scripting die Webanwendung auf dem Server miteinbezogen. Beim reflexiven Angriff manipuliert der Hacker die URL und kann damit den dynamischen Teil der Webseite verändern. So kann er den Schadcode temporär in die Webseite einfügen und dann zur Ausführung bringen.

doi: 10.2313/NET-2014-03-1_07

Der Unterschied vom reflexiven zum persistenten Cross-Site-Scripting besteht darin, dass beim persistenten Angriff der Schadcode nicht auf dem Client, sondern auf dem Webserver gespeichert ist und bei jedem Aufruf wieder von neuem ausgeführt wird. Um den Schadcode in der Datenbank des Servers zu platzieren, benutzt der Angreifer Webanwendungen, über die Nutzer Inhalte in die Datenbanken einfügen können. Dazu gehören zum Beispiel Kommentar- oder Gästebuchfunktionen. [14]

4.3 Firewall

Eine Firewall schützt PCs oder Netzwerke vor Angreifern oder schädlichen Inhalten. Dabei können mit bestimmten Filterregeln gezielte Überwachungsmaßnahmen eingeleitet werden, um zum Beispiel die Mitarbeiter einer Firma beim privaten Surfen einzuschränken.

Es wird zwischen der Stateless Firewall, der Stateful Firewall und der Application Level Firewall unterschieden. Je nach Art der Firewall wird die Kommunikation unterschiedlich stark oder schnell geprüft.

Die Stateless Firewall arbeitet auf der Transportschicht und überprüft die Header der ein- und ausgehenden Datenpakete nach bestimmten Filterregeln. Die Filterregeln werden vom Nutzer statisch festgelegt, anhand deren entscheiden wird, wie mit dem Paket umgegangen wird. Dabei werden meist die IP-Adressen von Absender und Empfänger, die Ports, die verwendeten Protokolle und die Netzschnittstellen nach den Kriterien gefiltert. Je nach Ergebnis, wird das Paket dann weitergeleite, verworfen oder an den Absender zurückgeschickt. Das Problem dabei ist aber, dass die Pakete nur isoliert betrachtet werden, das heißt ohne die Informationen über die Filterung der vorgehenden oder nachfolgenden Pakete. Zudem wird der Datenteil der Pakete nicht überprüft. Der Vorteil der Stateless Firewall ist, dass sie sehr schnell arbeitet und einfache Filterregeln beinhaltet, die vom Nutzer bearbeitet werden können.

Die Stateful Firewall betrachtet nicht einzelne Pakete der ein- und ausgehenden Verbindungen, sondern untersucht die Pakete zusammen und prüft zusätzlich den Zustand der Netzwerkverbindung. Dieser unterscheidet sich anhand des verwendeten Protokolls, ist das Protokoll zustandslos, wie http, kann der Zustand nicht analysiert werden. Bei einem zustandsbehafteten Protokoll speichert die Firewall immer wieder Informationen des untersuchten Datenverkehrs und passt damit die Filterregelungen auf den aktuellen Kontext an, sodass die Qualität der Filterung steigt. Dazu gehören beispielsweise die Protokollierung der verwendeten Ports, um Antworten nur am angegebenen Port anzunehmen, oder die Speicherung des Kontextes, sodass erkannt werden kann, ob ein Paket eine Antwort auf ein anderes ist, oder ob die Pakete zusammengehören. Die Stateful Firewall fängt zwar mehr zweifelhafte Inhalte ab, ist aber schwer zu implementieren und bei der Filterung sehr langsam.

Die Application Level Firewall arbeitet auf der Anwendungsschicht und untersucht nicht nur die IP-Adressen, Ports und Netzschnittstellen, sondern auch den Inhalt der Datenpakete. Für jedes Anwendungsprotokoll gibt es für die Filterung einen eigenen Proxy. Dieser baut als neuer Kommunikationspartner eine eigene Verbindung zum Ziel auf, sodass zwei eigenständige Verbindungen entstehen. Dabei werden die Pakete zu einem Datenstrom zusammengefasst und überprüft, anschließend werden sie in neue IP-Pakete verpackt und weitergeleitet. Durch Position als Kommunikationspartner kann er den Kommunikationsfluss beobachten, und auf dieser Basis die Pakete weiter filtern. Diese durchlaufen den gesamten ISO/OSI Stack, sodass zudem der Zustand der Verbindung überwacht werden kann. Die Vorteile der Application Layer Firewall sind also die Überprüfung des Protokolls, die Untersuchung des Inhalts auf Schadsoftware, sowie die Möglichkeit, weitere Dienste wie Virenfilter miteinzubinden. Durch diesen Umfang an Funktionen dauert die Filterung der Datenpakete länger, die Implementierung ist langwieriger als bei der Stateful Firewall und es wird für jedes Anwendungsprotokoll ein eigener Proxy benötigt.

Welche Firewall in welchem System eingesetzt werden sollte, hängt von der erwarteten Leistung der Filterung und dem Sicherheitsniveau ab.

4.4 Deep Packet Inspection (DPI)

Die Deep Packet Inspection ist einerseits für die Sicherheit eines Netzwerks von Bedeutung, da eingehende Datenpakete auf schädlichen Inhalt geprüft werden können, andererseits wird sie dazu verwendet, Inhalte der Nutzer auszuspähen und diese für die eigene Zielerreichung zu verwenden.

Bei der DPI werden sowohl der Header als auch der Datenbereich von Datenpaketen auf unerwünschte Programme oder Anwendungen und Spam überprüft. Dies unterscheidet die DPI von der Stateful Packet Inspection, die lediglich den Header der Pakete untersucht. Bei der Deep Packet Inspection kann der Inhalt des IP-Pakets verworfen oder verändert werden, und die Weiterleitung des ganzen Pakets zeitlich zurückgehalten werden. Sie wird beispielsweise bei Anti-Viren-Software, Contentfiltern oder Firewalls eingesetzt, um Kontrolle über die ein- und ausgehenden Datenpakete zu erhalten.

Für die Nutzung der DPI in Firewalls kann das Pattern Matching oder die Untersuchung der Protokollabweichungen eingesetzt werden. Für das Pattern Matching werden Datenbanken benötigt, in denen bekannte Angriffe auf Netzwerke gespeichert sind. Mit diesen Einträgen der Datenbank werden die Pakete verglichen und bei einem positiven Ergebnis blockiert. Unbekannte Angriffsarten können mit dem Pattern Matching nicht erkannt werden. Bei der Analyse des Pakets auf Protokollabweichungen können auch solche unbekannten Angriffe verhindert werden. Im Gegensatz zum Pattern Matching werden bei diesem Verfahren die erlaubten Verhaltensweisen des Protokolls definiert. Auf Grundlage dieser Festlegungen werden alle erlaubten bekannten Attacken weitergeleitet, unbekannte und nicht erlaubte werden blockiert.

Eine DPI, die Pakete mit Fehlern oder unerwünschten Inhalten in Echtzeit blockieren kann, ist ein Intrusion Prevention System. Diese Fähigkeit wird durch eigene Funktionen des IPS erlangt, indem mit einer Kombination aus Pattern Matching, Stateful Inspection und Anomalieerkennung gearbeitet wird. So wird auch das Netzwerk selbst geschützt, und nicht nur die Angriffe darauf verhindert.

Jedoch gibt es auch einige Nachteile bei der Nutzung der Deep Packet Inspection. Es wird eine eigene Hardware benötigt, die die Ressourcen für die DPI bereitstellt. Zudem müssen regelmäßige Updates durchgeführt werden, um die Software auf dem neuesten Stand des Schutzes zu halten.

doi: 10.2313/NET-2014-03-1_07

4.5 Contentfilter

Der Contentfilter wird meist zur Blockierung unangemessener, anstößiger oder verbotener Inhalte verwendet, sodass die Nutzer des Internets vor diesen Webseiten geschützt werden. In Ländern, in denen Inhalte zensiert werden, wie beispielsweise China oder der Iran, werden diese Contentfilter aber auch dafür verwendet, dass die Webseiten auf Inhalte überprüft werden, die laut der Regierung nicht veröffentlicht werden dürfen.

Der Contentfilter überprüft anhand einer Filterliste den Datenverkehr, um illegale Seiten zu sperren oder anstößige Inhalte auszublenden. Er erleichtert die Kontrolle des Datenaustausches, ohne dass der Nutzer dies merkt. Dies geschieht anhand der eingegebenen Webadresse oder ausgewählter Wörter, Sätze, Bildern und auffälligen E-Mail Anhängen. Die Filterliste wird über regelmäßige Updates durch den Hersteller immer auf dem aktuellsten Stand gehalten.

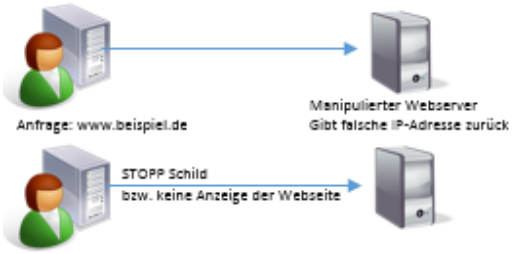


Abbildung 4: DNS-Sperre

Dabei werden verschiedene Verfahren verwendet. Nicht vertrauenswürdige Adressen können in einer Schwarzen Liste gespeichert werden, vertrauenswürdige in einer Weißen Liste. Anhand dieser Schwarzen Liste kann dann die DNS-Sperre eingesetzt werden. Der DNS-Server übersetzt bei einem Aufruf einer Webseite die Webadresse in die zugehörige IP-Adresse. Wenn eine DNS-Sperre im Einsatz ist, wird der DNS-Server manipuliert, sodass er beim Aufruf einer Adresse, die auf der Schwarzen Liste steht, keine IP-Adresse zurückliefert, also keine Verbindung zur Webseite aufbaut. Dieses in Abbildung 4 dargestellte Verfahren kann jedoch leicht umgangen werden. Schwieriger zu umgehen, dafür fehleranfälliger, ist die Sperrung der IP-Adresse. Auch dieses Verfahren funktioniert nur über die Einträge einer Schwarzen Liste. Wird eine eingetragene IP-Adresse aufgerufen, leitet der Router die Daten nicht weiter und blockiert sie. Da aber unter einer IP-Adresse viele Webseiten liegen, werden durch die Sperre auch vertrauenswürdige Seiten blockiert, was zu einer hohen Fehleranfälligkeit führt.

Wenn die Filterung auf Wort- oder Grafikerkennung aufbaut, werden entweder einfache oder intelligente Contentfilter verwendet. Einfache Filter überprüfen das Vorkommen bestimmter Auswahlkriterien. Ist dies mindestens einmal der Fall, wird die Webseite gesperrt. Die künstliche Intelligenz, die der intelligente Filter beinhaltet, untersucht das Vorkommen der Auswahlkriterien zusätzlich nach der Relevanz. Erst wenn ein bestimmter Grad der Überschreitung der Grenzen erreicht wird, blockiert er die Seite. Damit erkennt der intelligente Filter mit einer höheren Wahrscheinlichkeit, ob eine Webseite vertrauenswürdig ist, oder nicht.

Bei der Worterkennung wird der Quellcode des HTML-Dokuments nach bestimmten Wörtern oder Wortfolgen untersucht. Ist ein nicht erlaubter Teil vorhanden, wird der Inhalt gesperrt und ist für den Nutzer nicht mehr sichtbar. Bei der Grafikerkennung reicht diese Untersuchung des Quelltextes nicht aus. Hier werden die Bilder nach bestimmten Farben, Farbkombinationen, Formen und Zusammenhängen gescannt. Verstößt eines dieser Merkmale gegen die Filterregeln, wird die Webseite blockiert. Die heuristischen Verfahren kombinieren die Bild- und Grafikerkennung. Damit wird die Fehlerrate reduziert, das heißt, es werden weniger vertrauenswürdige Webseiten fälschlicherweise gesperrt.

Contentfilter können an verschiedenen Stellen in den Datenverkehr eingreifen, als Software oder Teil des Netzwerks in Proxys, Firewalls oder DLPs. Sie können bereits im Netzwerk eines Betriebs vorhanden sein, sodass alle ein- sowie ausgehenden Informationen der vorhandenen Arbeitsplätze im Netzwerk überprüft und gefiltert werden. Die Einstellungen werden dabei vom Besitzer des Netzwerks vorgenommen. Ein E-Mail-Filter überprüft den Text, Anhänge und Bilder der E-Mail auf unerwünschte Inhalte. Zudem wird untersucht, ob die Absenderadresse auf der Schwarzen Liste steht. Der am einfachsten einzusetzende Filter ist der im Browser integrierte Filter, der Anfragen direkt untersucht und gegebenenfalls sofort blockiert, wie auch die Filter in Suchmaschinen. Aber ein Contentfilter kann auch direkt auf dem Computer installiert sein, um den Datenverkehr auch auf schädliche Software zu überprüfen. Dieser kann durch den Administrator eingestellt und verändert werden.

Jedoch gibt es auch einige Probleme beim Einsatz von Contentfiltern. Die Software kann zu stark oder zu schwach blockieren, was zum Scunthorpe Problem führen kann. Dabei werden Webseiten oder E-Mails blockiert, die eine Zeichenfolge enthalten, die eigentlich in Ordnung ist, aber in einem unangemessenen Wort vorkommt. [10] Zudem gibt es Wörter, die zwei oder mehr Bedeutungen besitzen, und eine davon durch einen Contentfilter erkannt und somit der Inhalt gesperrt wird. Bei einer zu schwachen Blockierleistung werden dem Nutzer Inhalte angezeigt, die eigentlich durch den Filter blockiert hätten werden sollen.

4.6 Cookies und Web Bugs

Bei der Verwendung von Cookies auf Webseiten werden die persönlichen Einstellungen des Nutzers gespeichert, beispielsweise der Nutzername und das Kennwort eines Profils, den Warenkorb in einem Online Shop oder Benutzereinstellungen bei Online Suchdiensten. So kann die Webseite auf den Benutzer angepasst und ein Profil über die Webseitenbesuche angelegt werden. Zunächst wird nur die IP-Adresse des Besuchers gespeichert, gibt dieser aber seine Personalien an, werden diese mit der IP-Adresse verknüpft, sodass daraus ein genaues persönliches Profil entsteht. Dieses Verfahren wird meist von Firmen mit Online Shops oder Webseiten genutzt, die das Nutzungsverhalten der Besucher beobachten oder die Seite besser auf die Bedürfnisse des Kunden anpassen möchten.

Ein Cookie ist eine Datei, die die Lebensdauer, den Namen und den Inhalt als Textwert enthält, der vom Webserver festgelegt wird. Auf diese Wiese werden Informationen im Browser gespeichert, und der Nutzer wird bei einem erneuten Besuch wieder erkannt. Ohne Cookies ist dies nicht möglich, da das im Internet meist verwendete HTTP-Protokoll zustandslos ist. Das bedeutet, dass alle Anfragen als unabhängige, einzelne Transaktionen ausgeführt werden, ohne Informationen über die

doi: 10.2313/NET-2014-03-1_07

Sitzung auszutauschen. Abhilfe dagegen schaffen Cookies, deren Erzeugung und Austausch im Folgenden genauer erklärt wird.

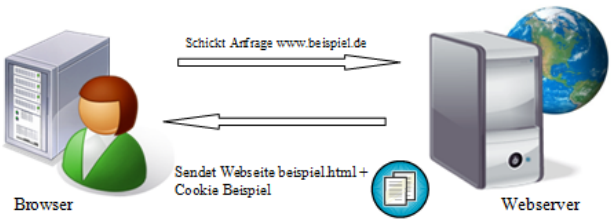


Abbildung 5: Austausch zwischen Browser und Webserver

Wie in Abbildung 5 dargestellt, kann das Cookie zwischen dem Browser und dem Webserver der besuchten Seite ausgetauscht werden. Dabei wird die Eingabe der Webadresse durch den Nutzer als Anfrage an den Webserver geschickt. Dieser beantwortet die Anfrage und sendet den Inhalt der Webseite und die Cookies zurück an den Browser, der im Anschluss die Cookies speichert und die Webseite darstellt. Wird die Seite nun erneut aufgerufen, können über die gespeicherten Cookies die persönlichen Einstellungen des Nutzers wieder aufgerufen und erweitert werden.

Die Web Bugs können im Gegensatz zur den Cookies auch über die Grenzen der einzelnen Webserver hinaus Daten sammeln und zusammenfügen. Damit können die Nutzungsprofile über die gesamte Sitzung erweitert und die Reihenfolge der angeklickten Webseiten gesammelt werden. Es lässt sich zudem erkennen, ob und wann E-Mails gelesen wurden, welcher Browser verwendet wird und welche IP-Adresse der Besucher benutzt. [11]

Web Bugs werden vom Anbieter als transparentes Bild oder Werbung in seine Webseite eingefügt. Hinter diesem Bild versteckt sich ein Link des dritten Servers. Der Benutzer bemerkt nicht, dass seine verwendete IP-Adresse, die URL der besuchten Webseite, die URL des Web Bugs, der Zeitpunkt seines Besuchs, der von ihm benutzt Browser und vorher gesetzte Cookies an den dritten Server geschickt werden, der damit das Bewegungsprofil über die Webservergrenzen hinaus erstellt.

4.7 Registrierungspflicht bei SIM Karten und Internetcafés

Zur besseren Strafverfolgung und Überwachung der Bürger besteht wie in der Schweiz und einigen anderen EU-Ländern auch in Deutschland eine Registrierungspflicht für SIM Karten, sowohl für Prepaid-, als auch für Vertragskarten. Bei Abschluss eines Vertrags sind die persönlichen Daten anzugeben, sodass der Nutzer eindeutig identifiziert werden kann. Bei der Nutzung einer Prepaidkarte muss der Kunde diese nach dem Kauf zunächst freischalten. Dies geschieht, wie auch bei Vertragsabschluss, mit den persönlichen Daten. Ohne diese Freischaltung erfolgt keine Einwahl ins Netz des Mobilfunkbetreibers.

Jedoch wird dieses Gesetz immer wieder umgangen. Einerseits ist durch den Tausch oder die Weitergabe keine Verfolgung der Daten möglich, da hierbei keine Verpflichtung zur erneuten Freischaltung mit den aktuellen Daten besteht, andererseits gibt es im Internet Unternehmen, die anonyme SIM Karten vertreiben.

Auch in Internetcafés wird die Anonymität der Nutzer unterbunden, da die Personalien aufgenommen werden und in der Datenbank des Betreibers des Internetcafés gespeichert werden.

In Deutschland herrscht bis zum heutigen Zeitpunkt allerdings keine Ausweispflicht, was manche Nutzer des kostenpflichtigen Zugangs zum Internet dazu führt, illegale Seiten, Posts, Bilder oder Ähnliches zu suchen und weiterzuverbreiten. Um bei Missbrauch des Internetzugangs jedoch eine Strafverfolgung zu ermöglichen, ist meist Videoüberwachung im Einsatz, um Besucher identifizieren und notwendige Ermittlungen einleiten zu können.

5. ZUSAMMENFASSUNG

Anhand des Papers kann man erkennen, dass es viele technische Möglichkeiten der Überwachung, der Manipulation oder dem Verändern des Datenverkehrs gibt. Diese Verfahren werden auf sämtlichen Ebenen der Kommunikation eingesetzt, von den physikalischen Leitungen durch einen Man-In-The-Middle Angriff bis hin in die oberste Schicht, wo die Cookies im Browser gespeichert werden, der die Anwendung des Nutzers darstellt.

Da die unterschiedlichen Interessensgruppen verschiedene Ziele haben, und aus diesem Grund versuchen, Anwendungen der Konkurrenten in ihrer Ausführung zu behindern schränkt sich die Netzneutralität immer weiter ein. Auch die Motivationen für dieses Eingreifen in den Datenverkehr sind vielfältig, hier liegt der Schwerpunkt vor allem auf der Durchsetzung der eigenen Interessen. Aber auch die Belange der Nutzer werden an manchen Stellen berücksichtigt, beispielsweise bei der Anpassung der Webseiten an die Kunden und deren Bedürfnisse oder beim Schutz der Bevölkerung vor Terrorangriffen oder Straftätern.

Aber die Möglichkeiten der Überwachung des Datenverkehrs und der Modifikation der Inhalte entwickeln sich immer weiter, entweder durch neue Programmiersprachen, oder auch durch die wachsende Zahl mobiler Endgeräte, die durch das mobile Internet oder Hotspots leichter zum Ziel eines Angriffs werden. Viele Nutzer sind mit dem Umgang ihrer Daten auch unvorsichtig, und prüfen nicht, wem sie ihre persönlichen Angaben hinterlassen. Aus diesen Gründen sollten sich die Anwender vor allem mit den Maßnahmen zum Schutz gegen Angriffe vertraut machen, um dem Datendiebstahl selbst entgegenzuwirken.

6. REFERENZEN

[1] A. Aurand, „LAN-Sicherheit", dpunkt.verlag, September 2004

[2] D. Fox, „Cross Site Scripting", Datenschutz und Datensicherheit, 11/2012

[3] Diensteanbieter im Sinne des TMG: Bundesrepublik Deutschland, http://www.gesetze-im-internet.de/tmg/__15.html, aufgerufen am 10.09.2013

[4] Google Analytics, http://www.google.com/analytics/, aufgerufen am 04.09.2013

[5] J. Kruse, "Internet-Überlast, Netzneutralität und Service-Qualität", Wirtschaftsdienst, 03/2008

[6] K. Selchert, http://www.geheimdienste.org/, aufgerufen am 22.10.2013

[7] M. Bärwol, „Netzneutralität: Fünf Fragen und Antworten", 18.01.2011

[8] N. Lepperhoff, B. Petersdorf, „Datenschutz bei Webstatistiken", Datenschutz und Datensicherheit, 04/2008

[9] Prof. Dr.-Ing. G. Carle, “Grundlagen Rechnernetze und verteilte Systeme”, 2013

[10] Professional Security Magazine Online, „The Scunthorpe Problem“, 12.09.2013

[11] R. Grimm, „Spuren im Netz“, Datenschutz und Datensicherheit, 02/2012

[12] S. Kelly, S. Cook, M. Truong, „Freedom on the Net 2012“, Freedom House, September 2012

[13] Telekom AG, http://www.telekom.com/verantwortung/datenschutz/1932, aufgerufen am 22.10.2013

[14] Vulnerability-Lab, „CROSS-SITE-SCRIPTING“, Juli 2011

doi: 10.2313/NET-2014-03-1_07

Hiding from Big Brother

Martin Schanzenbach, B.Sc.
Betreuer: Dipl.Inf. Matthias Wachs
Seminar Future Internet WS2013
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: schanzen@in.tum.de

ABSTRACT

The present state of Internet surveillance and censorship has prompted the development of sophisticated anonymization and encryption protocols. The importance of anonymity and data encryption has already set foot in people's minds. In this paper, we discuss why it is necessary to not only hide the contents and involved parties of communications, but also the communication itself. We present some of the techniques suitable for hiding communications effectively and finally elaborate possible future implications the use of those technologies would have on Internet usage.

Keywords

Big Brother, Censorship, Obfuscation, Steganography, Morphing

1. MOTIVATION

Our Internet communications today are not only heavily censored in some parts of the world, but also heavily monitored by intelligence agencies, corporations and nation states. Specialized industrial sectors produce technology for surveillance, censorship and with it, oppression of civil liberties[18]. We are no longer dealing with attackers of limited power and influence. Today's communication systems are under attack by states and large corporations with sheer endless capabilities. Especially considering recent revelations that states are performing large scale surveillance of the Internet[7], protocol designers of privacy enhancing software must rethink their threat model. The current state of our security infrastructure is in a sorry state[11] and even implementations of some basic cryptographic routines might be affected[23, 24].

A prime example for this problem in today's world are China's efforts to censor and monitor the Internet. Dissident blogs and non conforming opinions are not tolerated content[19]. At the same time, tools like Tor, that provide anonymization to allow free expression of opinions, are fought and it's users incriminated. Tor is a tool that allows users to browse the Internet anonymously and provides Chinese users with the ability to access the Internet beyond the Great Firewall of China[27]. However, the Chinese government has long blocked the access to the public Tor servers needed to connect to the service. As a result, non-public, "intermediate" servers have been emerging called "bridges", that allow access to the Tor network. But even the undisclosed IP addresses of bridges are blocked after use in many cases[21]. This indicates, that services and traffic are actively monitored and traced.

Hiding only the contents of your communication using encryption is no longer enough. If you are talking with a known dissident or you are using censorship circumventing software it does not really matter what the contents of your communication are. It makes you suspicious and in some places of the world this is enough to put you in danger. The above is the classical dissident versus state scenario. One could say that any attempt in hiding is the same as criminals trying not to get caught by the police. After all, in the affected states the dissident is treated as a criminal. As this is the case, we have to hide this data and communication. We need solutions to completely hide our information, services and data traffic. Only then can we assure that we are not being labeled "suspicious" by mentioned authorities when using other anonymizing tools. In this paper we will introduce the concepts "anonymous clients", "anonymous services" as well as "anonymous traffic and content" along with real world examples. Finally, we will discuss the viability of those technologies and the impact wide-spread use might have on the Internet. In this paper we will discuss some anonymity tools that are used today. Furthermore, we will discuss their viability in our current situation.

There are further cases where communication partners do not want a third party to actually notice their communication in the first place. Copyright holders often watermark their content, invisible to the user but readable either by devices that can process the content or becoming readable if the content is copied. Both methods are used to enforce Direct Right Management (DRM) for intellectual property. Telecommunication companies might as well want to secretly add information to network traffic and packets to discriminate between traffic flows and "prefer" some packets over others. For example an internet service provider could charge companies that provide services over the internet for a prioritized treatment of their traffic, giving them an edge over competitors. Even though a clear violation of net neutrality, it is a use case for hiding information. In this work we will largely focus on the dissident versus state scenario.

The remainder of this paper is structured as follows: First we will introduce our attacker in Section 2. Then we will present some related work on information hiding in Section 3. In Section 4 we present various anonymization techniques. Finally, in Section 5 and Section 6 we will reflect on the viability and implications of those anonymization techniques.

doi: 10.2313/NET-2014-03-1_08

2. THREAT MODEL

In our threat model the adversary is unable to break cryptographic primitives. But, we acknowledge the fact that the implementations of such primitives can be compromised[23, 24]. The attacker is powerful enough to block, disrupt or alter the network communication between two parties. In particular, the adversary is more powerful than the communication partners, but does not control the software they use. The adversary is suspicious of unknown or unreadable information like encrypted communication that does not match any known protocol. He knows our employed techniques and will censor accordingly. In other words, if he is not able to identify our communication as "acceptable" by his standards, he will try to attack our communication. We also assume that our attacker has extensive legal power, as any nation state has. Thus it is possible for him to coerce legal entities like companies to redact any information, including user information, related to any services they provide.

As [26] we define a "whitelisting censor" that has defined a set of allowed technologies and protocols. He monitors communication at least on vital crossings and collects metadata like IP addresses and communication frequency as well as communication content. It is enough to imagine a state forcing ISPs to backup all connection data and perform deep packet inspection, as well as using them to block certain technologies or hosts all together. Any technology, protocol, host etc. not on the whitelist is considered suspicious and will be attacked or blocked. On the other hand whitelisted traffic is considered, for example economically, essential by the censor and will not be blocked.

Accordingly we define a "blacklisting censor" that, upon identifying an unacceptable communication over some technology or protocol, will add an entry to a blacklist. However, this means that if new technologies, protocols or hosts emerge, the blacklisting censor would always first have to identify this and put a new entry on his list, while the whitelisting censor doesn't. The blacklisting censor is obviously less restrictive. So, in general, we consider the whitelisting censor to be stronger. If we can hide from a whitelisting censor, we can also hide from a blacklisting censor.

3. RELATED WORK

Hiding information is an old idea, very useful for wartime communication of allied forces. Secretly communicating can give one side of a conflict an advantage. Especially political or military espionage comes to mind. One concept to hide information is Steganography[22]. Steganography is the art, or science, of hiding information inside information. The resulting information including the hidden part is then called "Steganogram", "Stegofile" or "Stegotext". It should be noted that by successfully using Steganography no third party can read the hidden information unless it knows the Steganography technique used and is actively looking for it. In this matter it serves the same purpose as encryption. However, it might still be useful to encrypt the hidden information to make it more "random" and thus look like noise. As with encryption Kerckhoffs' principle can be applied to Steganography. The security of the system must not depend on the attackers ignorance of the used algorithms that encode and transform the information payload into a Stegotext. In the early days of Steganography this was not an issue, as the attacker was usually a human being whose detection tools were limited to his senses. Today, however, digital communication and forensics tools are a valid reason to keep Kerckhoffs' principle in mind. One example for Steganography is "Echo Hiding". Echo Hiding uses the features of the human auditory system. When listening to audio from speakers what we hear is the music itself including echoes coming from walls and furniture. However, we do not consciously recognize those echoes. Echo Hiding hides data in an audio stream that when heard sound like "natural" echoes[6].

Information hiding was already employed a long time ago using letters, newspapers or custom contraptions. As those techniques are only of limited use in digital information hiding this section will only give a brief overview. However, as the techniques are very simple the concept can be easily grasped and for digital information hiding the basic idea is the same. For instance, using "invisible" ink make of lemon juice can be used to hide texts on seemingly empty paper, or even better, between the lines of other undiscriminating texts. The receiver can make the hidden message visible by applying heat to the paper. Any intermediate party involved in the transport of the text or actively spying on the communication cannot read the hidden message unless he knows that it has been added and how it has been added. Another technique called "Microdot", conceived by Emanuel Goldberg[2] and mostly used in World War 2, is a lot more sophisticated than the invisible ink, but basically the same concept: The information is hidden in the dots of an "i" or a punctuation character of an inconspicuous text like a newspaper article. A picture of the information to be hidden is taken and its size scaled down to the size of a dot in the text. Because of the small size of the resulting dot it cannot be distinguished from a regular dot by the human eye. Additionally, it is chemically treated to appear as black as the other characters. The receiver uses a microscope and inverse chemical processes to retrieve the hidden message. The theoretical issue of those approaches is that if someone is aware of the technique employed and looks for hidden messages explicitly, it is easy to expose the hidden information. This is because the techniques violate the Kerckhoff principle[14]: The viability of the systems depend on the fact that the attacker does not know how it works and that it is applied.

Finally, transportation mediums that are not actually intended to be used for communication at all can be (mis-)used for exactly that purpose. This has been mostly an issue in regards to information security. For example, the electromagnetic field of a CRT computer monitor can be easily measured and used to recreate the displayed image. Also, electromagnetic fields of a PC change depending on the operations the CPU (or other components) perform. This effect can be used by malicious software to "radiate" otherwise inaccessible information in the device to a remote attacker. However, covert channels can also be used to secretly communicate because it is simply not expected to be used in this way. A very sophisticated example is "meteor burst communication", which uses "the transient radio paths provided by ionized trails of meteors entering the atmosphere to send data packets between a mobile station and a base"[20].

4. ANONYMITY

Initially, we need to to clarify our concept and understanding of "anonymity". In anonymity discussions the "level" of anonymity greatly varies from conversation partner to conversation partner. Ground zero in such a scale would be the discussion about the display of real names in social networks or forum comments. However, for us, anonymity should guarantee that companies, states etc. are unable to find a connection between your data and your identity[1]. Anything in between those two is not considered to be anonymity but "pseudonymity". A prime example are IP addresses in Internet communication. Every user uses at least one IP address to communicate. The address itself does not reveal a lot of information about it's user. However, in combination with the customer data in the ISP's databases the IP address is the key to trace back the user's communications and personal data.

We need to anonymize communication partners as well as the content of the exchanged information to assure anonymous communication. In the following we present concepts that provide anonymity of clients, service and content, repectively.

4.1 Anonymous Clients

Anonymizing the source of a communication on the Internet usually involves obfuscation or hiding of the respective source IP address. Proxies and Virtual Private Neworks are common tools to achieve this. However, there is also more sophisticated software like Tor.

4.1.1 Proxies

Using proxies is a straight forward way to hide the source of communication. Proxies are surrogates that are used to hide the source IP address. If a user wants to browse a website he contacts the proxy server and tells it to do so for him. The webserver will only ever communicate with the proxy's IP address (Figure 1). A common protocol for proxies is SOCKS. One major disadvantage of proxies is that they only support HTTP and sometimes HTTPS. Any other protocol will not be proxied and the IP address not hidden. Another issue is that the proxy operator's integrity greatly determines the viability of this anonymization service. All connection information might be stored on the proxy server.

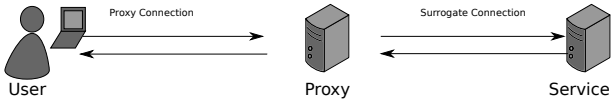


Figure 1: Illustration of a proxied connection.

4.1.2 Virtual Private Networks

Virtual Private Network (VPN) tunnels provide the user with an encrypted tunnel that can be used to access services. The user connects to a VPN-Gateway and redirects his traffic though it. All the traffic exits the tunnel at the exit point and to the service it looks like the user's IP is that of the exit point (Figure 2). The user's real IP remains unknown to the service and service and source cannot be correlated. VPN tunnels are usually fee-based services operated by companies. However, as with proxies, the VPN-Gateway is the first target for any attacker that wants to learn the user's IP addresses. Thus, the anonymity provided depends on the integrity of the service provider. In terms of anonymity, the VPN tunnels have no advantage over proxy's. But they offer broader protocol support, higher data rates and reliability. The latter two usually only if it is a paid service.

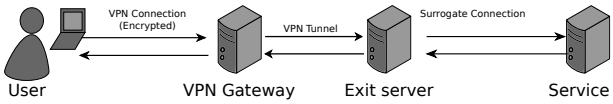


Figure 2: Illustration of a VPN tunnel.

4.1.3 The Onion Router

A popular anonymizing tool is called "The Onion Router"[4], Tor. In the Tor system, the user uses a client called the "Onion-Proxy" or the "Tor-Browser" to connect to the Tor network, a set of connected Tor servers listed in a directory on directory servers. When the user wants to send data to a service it selects a subset of Tor servers and retrieves their public keys from the directory servers. The data is encrypted successively with the public keys and sent to the first server (the one corresponding with the last public key used to encrypt the data). Upon receiving the encrypted packet the server will decrypt the first encryption layer and send the resulting packet to the next server. This scheme continues until the final encryption layer is decrypted. This final server is called the "Exit-Node" and is the surrogate for the user's connection (Figure 3). Client-to-Server and Server-to-Server communication inside the Tor network is also encrypted. In Tor the only server that learns the user's IP is the first server the user sends the encrypted packet to. However, this server does not know the destination of the IP packet, as it cannot decrypt the contents. Any intermediate servers learn nothing about the user and the Exit-Node only learns about the destination of the IP packet. But as the Exit-Node can read the contents of the IP packet it is important that the payload is encrypted using End-to-End encryption like TLS/SSL with the service.

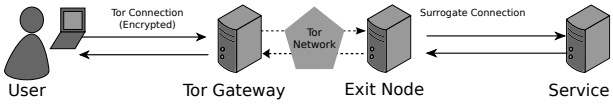


Figure 3: Illustration of a Tor connection.

4.1.4 Anonymous Remailer

For email, anonymous remailer systems can be used[8]. Basic anonymous remailer receive emails from users and strip all headers that can be used to identify the sender. Four kinds of Remailer can be distinguished: Type 0-3. The higher the number the more anonymity can be provided. A Type-3 Remailer is the Mixminion system[3]. One feature of Mixminion is that there is not one remailer, but a set of

doi: 10.2313/NET-2014-03-1_08

anonymizing remailer that communicate using encryption. The sender of an email encrypts the email with the public keys of the remailer servers, similar to the Tor system. A large problem with Mixminion is it's small user base and the fact that the software is still in alpha stadium.

4.2 Anonymous Services

Anonymizing the destination of a communication means we have to hide the service that is communicated with. The approach is called "service hiding". Hiding the service allows the host to remain inconspicuous. If the host is not suspected of running a certain service the censor is looking for, it might fall under the radar and will not be as actively surveilled like a host obviously running the service.

4.2.1 Well Known Ports

As simple and trivial as it sounds, using a different port than the "well known"[13] port of a service can be considered hiding a service. In fact, it is common practice to fool port filters[30].

A technique used to detect running services is the "port scan". A port scan is an attack, where the attacker attempts to connect to all possible ports on the host, trying to enumerate all services that are running. In this process the attacker often learns other important information like operating system, software versions and computer architecture. A firewall can block port scans in general, but as the service provider wants to provide access to the respective services to its users, those ports cannot be blocked.

4.2.2 Port Knocking

A solution to the port scan problem is called "port knocking". Initially, the port is blocked and it is not possible to connect. Only after the client "knocks" by sending a designated knock packet to a predefined port the actual service port will open and can be accessed. The knock packet can be a simple empty protocol data unit directed to the service port or a more sophisticated scheme where it contains a cryptographic identifier[29] or consists of a series of knocks[15]. In either case, an attacker cannot know if a port knocking scheme is used simply by examining the running services on a server. A port scan will always yield no results, as ports are blocked by default.

However, it is important that the port knocking service itself is not detectable, since that service will become the target for an attacker. Not to mention that a port knocking service is anything but inconspicuous in our threat model. The SilentKnock[25] technique was designed with this in mind. SilentKnock assumes that a key and synchronization parameters are exchanged out of band between all the clients and the server. A client initiates a connection using TCP and the respective initial packet (SYN) contains a hidden authenticator token generated from the data exchanged out of band. If the server can verify the token, TCP connection establishment continues, otherwise it fails. The authentication token is a keyed Message Authentication Code (MAC) that is hidden inside TCP header fields containing sequence number and time stamp[17]. It is important to note here that if connection establishment fails, the service will remain silent, instead of returning an error message or actively terminate the connection request, to counteract any probing.

4.2.3 Tor Hidden Services

Another technique to hide services is part of Tor. The goal of "Tor hidden services" is to hide the location and the existence of the service in the network[4]. Initially the service provider chooses a public/private key pair. If a user wants to connect to the service it uses the public key of the service to anonymously connect to a public "introduction point (IP)" using the Tor software. The service is also connected to the IP. Using the now existing connection a "rendezvous point" is negotiated, that is subsequently used by user and service to establish a connection. The user does not learn the IP address of the service and vice versa. Since the service only accepts connections via Tor, attacks like port scanning are useless, considering that the connection establishment in this scheme is additionally relying on a lot of computing intensive cryptography.

4.3 Anonymization of Traffic and Content

Hiding the content and existence of our communication requires sophisticated approaches based on the concept of "Steganography". Content and traffic can be obfuscated in various ways. The difficult problem is making them look inconspicuous.

4.3.1 Obfuscation

Obfuscation aims to alter the communication beyond recognition for an attacker. A very simple way to obfuscate traffic is *encryption*. Encryption protocols are advertised as providing data confidentiality for services on the Internet[5]. An encryption algorithm uses an "encryption key" and "encryption function" to transform plaintext into "cyphertext". The cyphertext can be decrypted using a "decryption key" and a "decryption function". In cryptography we differenciate between two types or encryption: Public and private key encryption. Private key encryption uses the same "secret key" for encryption and decryption. Public key encryption uses different keys for encryption, the "public key", and decryption, the "private key".

Encrypted messages result in protocol data and message content that is no longer readable to any attacker. Thus forbidden conversations (content) and conversation mechanisms (protocols) can be hidden. In particular, encryption defeats any deep package inspection (DPI) mechanisms. Common protocols and software using encryption are HTTPS via TLS/SSL or Skype[1]. Skype audio and video calls are encrypted. HTTPS and the x.509 public key infrastructure (PKI) are used by banks, shops and email providers to encrypt transactions on the Web and protect the users from any third party learning personal information like credit card numbers. This is done by encrypting all sensitive data on the user's PC and sending it to the service where it is decrypted, called "End-to-End encryption". Any third party intercepting the data in-flight will not be able to extract the information.

Two major issues using encryption like TLS/SSL should be mentioned here: First, only the content of the communication between two parties in encrypted (anonymized), not the communication itself. It is easy to learn the identity of the communication partners because the IP addresses are not

[1] http://www.skype.com

doi: 10.2313/NET-2014-03-1_08

encrypted. The second problem is the x.509 PKI. The PKI forms the corner stone of the TLS/SSL system and must be integer. However, as [11] has analyzed, the x.509 PKI is easy to compromise. Furthermore, statistical methods allow attackers to identify traffic patterns, like those of Skype or HTTP traffic[10]. Even if packet contents cannot be read using DPI because the attacker does not have enough resources, traffic patterns like timings and packet size can reveal the protocol used to communicate. An example of such a "statistical classification technique" is the SPID algorithm by Hjelmvik and John[9].

4.3.2 Traffic Hiding

In the face of a very powerful attacker, as defined in our threat model, it is not unlikely that each and every communication is monitored. This includes all the network traffic that is occurring. Using anonymization tools like Tor, it is possible to conceal the identities of either one or the other communication partner. An entity observing the traffic can only know the entity on one side of the communication. However, through statistical analysis an attacker can determine the protocol and in some cases even the content of the communication[9]. Consequently, given a communication between A and B using the protocol P, the attacker can either learn that A is talking using protocol P to somebody *or* that B is talking using protocol P to somebody, but never both. However, as stated in our threat model, simply the use of protocol P might prompt the attacker to block or otherwise attack the communication. As such, it is also necessary to hide the traffic itself.

One approach is to modify traffic patterns in such a way, that the protocol employed is no longer recognizable. Modifying the packet size and the timings the packets are sent will obfuscate the traffic flow. An example implementation of this scheme is the Tor software. Tor servers exchange packets in equally spaced "cells"[4], fixed length messages of 512 bytes. Actual payload data is sliced into 512 byte messages and payload slices smaller than 512 bytes are *padded*. Tor cells are packed into TLS/SSL application data, adding a layer of obfuscation discussed above. Unfortunately, it is exactly those 512 byte cells that make Tor detectable as shown by [26] using statistical analysis. But even if such a sophisticated classification of traffic is not employed by the attacker, the encrypted traffic itself is suspicious. As already mentioned, in China SSL/TLS connections are automatically probed, quickly exposing any Tor activity[27]. Furthermore, in the case of a whitelisting censor, obfuscated traffic not matching whitelisted traffic will automatically be blocked.

A more recent idea to hide from censoring authorities is called "traffic morphing". Whitelisted network traffic is, in our threat model, essential and, if censored, could result in economic disadvantages or other negative effects for the censor. In other words it is inconspicuous because whitelisted (or not blacklisted) by the censor. A traffic "morphing function" can transform any traffic pattern into such a whitelisted pattern, without the censor being able to detect this transformation. A concept best described as "hiding conspicuous traffic inside normal traffic". Even if the censor is aware that there is a technique that allows this transformation and there are users using this technique, he should be unable to distinguish between traffic that contains hidden traffic and normal traffic. The only option he has is to blacklist the previously whitelisted pattern. However, as elaborated above, the censor might be uncomfortable doing that.

StegoTorus[26] is a plugin for the Tor software that aims to add the features of "undetectability" and "unblockability" to Tor. Tor itself tries to conceal it's traffic already using obfuscation techniques. However, as the authors of [26] state, this traffic can be identified as Tor traffic and it can be attacked to learn the protocol of it's original traffic. To counter this, StegoTorus applies Steganography to make Tor traffic look like traffic produced by other client software. Additionally, the equally sized "cells" output by Tor are "chopped", resulting in variable-length "blocks" encrypted with a novel cryptosystem that makes the cyphertext indistinguishable from random data. The authors have created plugins to make the traffic look like either an encrypted peer-to-peer protocol or HTTP. Furthermore, StegoTorus is pluggable to contain more sophisticated Steganography techniques. This is useful as the authors themselves claim[26] that the current Steganography plugin implementations are vulnerable in the face of powerful attackers performing targeted attacks. In the presence of our censor it might be necessary to adjust the cover protocol to one that is on the whitelist or not on the blacklist.

Another approach that also uses Tor's plugin system is SkypeMorph[16]. SkypeMorph aims to hide Tor traffic inside Skype traffic. Skype traffic, or more specifically encrypted video chat traffic, is very suitable for hiding information. First of all in a regular Skype session there is constant flow of information in the form of audio and video data. This constant flow allows the source traffic to be morphed into Stegotext with very little delay, unlike for example HTTP traffic, which does not usually exhibit a constant flow of packets and thus the data rate is not very high. Also, Skype traffic is encrypted which means our traffic is obfuscated by design. A SkypeMorph connection is established by calling a contact using Skype. This results in three prerequisites: Tor, the SkypeMorph plugin, a SkypeMorph bridge to connect to and Skype accounts. The SkypeMorph session is initiated by exchanging public key material over the Skype text chat with an out of band selected bridge. The bridge's Skype ID needs to be added to the client's contact list beforehand. Once a shared secret has been generated by client and bridge, a Skype video call is initiated. Using this "Skype tunnel" the actual Tor traffic is shaped to look like a Skype video call and this data is sent instead of audio and video data. However, we consider this method to have a major flaw: A Skype account is needed and the integrity of the Skype authentication servers as well as the official API kit (which is used by SkypeMorph) is crucial. In our threat model relying on the integrity of a U.S.-based company is a major flaw, as it can easily be coerced to submit potentially incriminating data (at least the Skype account information) and disable bridge accounts due to suspicious activity.

ScrambleSuit[28] is a thin protocol layer above TCP. It aims to negate the shortcomings of Tor by adding the feature of non-blockability using a polymorphic payload and a simple authentication mechanism. ScrambleSuit connections can only be established if both parties can prove their knowledge

of a secret that is shared out-of-band. It is proposed that the Tor bridge distribution mechanism should be used for this purpose. The authors extensively discuss possible authentication mechanisms including Uniform Diffie-Hellman and Session Tickets. As mentioned ScrambleSuit also provides traffic analysis resistance by flexibly generating "protocol shapes" that resemble common "whitelisted" protocols. Protocol shapes are determined in ScrambleSuit by packet length and inter-arrival times between packets. ScrambleSuit servers can, unlike SilentKnock systems, be actively probed. However, since the probing client cannot authenticate itself without the shared secret, the server will simply not answer. The attacker will only learn that the server is online and accepting connection on the given port. Clearly ScrambleSuit has an advantage over SkypeMorph because it doesn't rely on a service provided by a U.S.-based company. Choosing ScrambleSuit over StegoTorus is also advisable, as it already supports common, by today's censors whitelisted , protocols and includes a scheme where our bridge cannot easily be probed.

5. ISSUES

In this Chapter we want to look at some of the issues of the presented technologies. We clearly defined our attackers as very powerful and highly suspicious. But, we only considered low-level network anonymization and hiding practices. In reality, it might be easier for an attacker to deanonymize users from higher-layer protocols, such as plain (as in unencrypted) HTTP, DNS or email. Furthermore, the proposed solutions all trade anonymity for convenience and performance. A development that, we think, is undesirable in a free Internet.

5.1 The High-Level Issue

All the software and techniques discussed above require the user to always have privacy in mind. A careless user can be deanonymized no matter how sophisticated his traffic or services and information is hidden. In this respect, anonymization technologies can be deceptive. For instance, HTTP usage over Tor can lead to information leakage[12] that cannot be contained by such low-level protocols presented here. While we consider the presented techniques, unless otherwise stated, technically sound, careless usage of higher level protocols such as HTTP, email or DNS can also lead to deanonymization. Spy- and malware, i.e a compromised host system, will circumvent any deanonymization software. Without a user's privacy conscience, the best anonymization protocol is useless. A first rule of thumb can be to always use encrypted End-to-End protocols over the hidden and anonymized channels. But even then, the user needs to carefully select the information passed on to the other side and judge how well it can be trusted with it.

5.2 Interdependencies of Hiding Tools

In recent years something that looks more and more like an arms race between censoring authorities and dissident censors can be observed. Whenever a new or improved privacy enhancing technology is employed, there is a response designed to counteract and render it useless. At the same time, when such a tool becomes blocked or otherwise compromised, it is no longer used or, if possible, improved to be immune against the attack.

The problem that arises, though, is that the power, capabilities and knowledge of our attacker are usually unknown. It is generally assumed that an adversary can not theoretically break cryptographic primitives, but he can exploit bugs and weaknesses in the implementations. Those are, of course, not disclosed by an attacker, as it is his own personal back door.

Paradoxically, it might also not be in the victims interest to immediately disclose and fix vulnerabilities in the software's implementation. At first, this seems counter intuitive but it is actually a smart move in the presence of an active attacker on our systems: If a vulnerability is quickly disclosed and a fix released, the adversary will no longer waste his time to find this exploit. On the other hand, if there is a fix and the vulnerability is not disclosed before the attacker can produce an exploit, valuable time is bought for the service provider and users. When the time comes, and the adversary exploits this vulnerability, we can simply patch your software with an already prepared fix, rendering the attackers efforts useless instantly. This is an approach taken for example by the Tor project.

Both sides of this battle have evolved over the past years and employ complex techniques to either impose or circumvent censorship. For users, if this trend continues, it means they will have to use increasingly inefficient and complex software systems to freely communicate. An arms race like this threatens the usability and stability of the Internet and with it today's primary social interaction medium.

We defined our attacker as an entity is not looking to block all communication (i.e. "turn off the internet"). Only communication that he deems necessary to censor will be censored. He will try to walk a thin line between generating digital civil unrest and major economic losses because of censorship and annoying but acceptable limitations. Here, we have reached a point in our discussion where the power of our attacker is limited by the actions and reactions of the general public and private sector instead of science and technology. Maybe a time will come where the Internet has become so over-engineered, heavily surveilled and probed that users no longer accept the status quo and rise by creating a new one.

6. DISCUSSION

We have examined various technologies under the assumption that hiding communication is as important an issue as anonymization communication partners in today's censored and monitored computer networks. While the presented technologies offer various degrees of effectiveness they all share the common problem of complexity. Also, they provide the user with a deceptive feeling of security while at the same time being technically sound. In this regard, we have shown how, in our point of view, the development of hiding and anonymization technology might continue in the face of monitoring and censoring attackers. Not all is lost in the battle between anonymity and incisive intrusion of digital life. However, unless fundamental changes in our social and political mind happen, the resulting technologies are but a crutch to move in a broken Internet.

doi: 10.2313/NET-2014-03-1_08

7. REFERENCES

[1] H. Bleich. Mythos anonymität. *c't 2013 Heft 20*, 2013.

[2] M. K. Buckland. Histories, heritages, and the past: The case of emanuel goldberg. *The History and Heritage of Scientific and Technical Information Systems*, pages 39–45, 2004.

[3] G. Danezis, R. Dingledine, and N. Mathewson. Mixminion: Design of a type iii anonymous remailer protocol. In *Security and Privacy, 2003. Proceedings. 2003 Symposium on*, pages 2–15. IEEE, 2003.

[4] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second-generation onion router. Technical report, DTIC Document, 2004.

[5] A. Exner. *Secure Socket Layer (SSL)-Sicherheit im Internet*. GRIN Verlag, 2008.

[6] D. Gruhl, A. Lu, and W. Bender. Echo hiding. In R. Anderson, editor, *Information Hiding*, volume 1174 of *Lecture Notes in Computer Science*, pages 295–315. Springer Berlin Heidelberg, 1996.

[7] Guardian. The nsa files. *http://www.theguardian.com/world/the-nsa-files, Accessed 21.09.2013*, 2013.

[8] C. Gulcu and G. Tsudik. Mixing e-mail with babel. In *Network and Distributed System Security, 1996., Proceedings of the Symposium on*, pages 2–16. IEEE, 1996.

[9] E. Hjelmvik and W. John. Statistical protocol identification with spid: Preliminary results. In *6th Swedish National Computer Networking Workshop (SNCNW)*, 2009.

[10] E. Hjelmvik and W. John. Breaking and improving protocol obfuscation. Technical report, Department of Computer Science and Engineering, Chalmers University of Technology, 2010.

[11] R. Holz, L. Braun, N. Kammenhuber, G. Carle, and T. U. München. The ssl landscape - a thorough analysis of the x.509 pki using active and passive measurements.

[12] M. Huber, M. Mulazzani, and E. Weippl. Tor http usage and information leakage. In *Communications and Multimedia Security*, pages 245–255. Springer, 2010.

[13] IANA. Service name and transport protocol port number registry. *http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml, Accessed 21.09.2013*, 2013.

[14] A. Kerckhoffs. *La cryptographie militaire*. University Microfilms, 1978.

[15] M. Krzywinski. Port knocking: Network authentication across closed ports. *SysAdmin Magazine 12(6),*, 2003.

[16] H. M. Moghaddam, B. Li, M. Derakhshani, and I. Goldberg. SkypeMorph: Protocol Obfuscation for Tor Bridges. In *Computer and Communications Security*, Raleigh, NC, USA, 2012. ACM. http://www.cypherpunks.ca/ iang/pubs/skypemorph-ccs.pdf.

[17] S. J. Murdoch and S. Lewis. Embedding covert channels into tcp/ip. In *Proceedings of the 7th international conference on Information Hiding*, IH'05, pages 247–261, Berlin, Heidelberg, 2005. Springer-Verlag.

[18] K. Page. Gamma attempting to export surveillance tech out of switzerland. *https://www.privacyinternational.org/blog/gamma-attempting-to-export-surveillance-tech-out-of-switzerland, Accessed 21.09.2013*, 2013.

[19] W. S. J. Paul Mozur. An inside look at china's censorship tools. *http://blogs.wsj.com/chinarealtime/2013/08/30/an-inside-look-at-chinas-censorship-tools, Accessed 21.09.2013*, 2013.

[20] F. A. P. Petitcolas, R. Anderson, and M. Kuhn. Information hiding-a survey. *Proceedings of the IEEE*, 87(7):1062–1078, 1999.

[21] Phobos. China blocking tor: Round two. *https://blog.torproject.org/blog/china-blocking-tor-round-two, Accessed 15.09.13*, 2013.

[22] N. Provos and P. Honeyman. Hide and seek: An introduction to steganography. *Security & Privacy, IEEE*, 1(3):32–44, 2003.

[23] B. Schneier. Nsa surveillance: A guide to staying secure, 2013.

[24] B. Schneier. The us government has betrayed the internet. we need to take it back, 2013.

[25] E. Y. Vasserman, N. Hopper, J. Laxson, and J. Tyra. Silentknock: practical, provably undetectable authentication. In *Proceedings of the 12th European conference on Research in Computer Security*, ESORICS'07, pages 122–138, Berlin, Heidelberg, 2007. Springer-Verlag.

[26] Z. Weinberg, J. Wang, V. Yegneswaran, L. Briesemeister, S. Cheung, F. Wang, and D. Boneh. StegoTorus: A Camouflage Proxy for the Tor Anonymity System. In *Computer and Communications Security*, Raleigh, NC, USA, 2012. ACM. http://web.mit.edu/frankw/www/papers/ccs2012.pdf.

[27] P. Winter and S. Lindskog. How the Great Firewall of China is Blocking Tor. In *Free and Open Communications on the Internet*, Bellevue, WA, USA, 2012. USENIX Association. https://www.usenix.org/system/files/conference/foci12/foci12-final2.pdf.

[28] P. Winter, T. Pulls, and J. Fuss. ScrambleSuit: A Polymorphic Network Protocol to Circumvent Censorship. In *Workshop on Privacy in the Electronic Society*, Berlin, Germany, 2013. ACM. http://www.cs.kau.se/philwint/pdf/wpes2013.pdf.

[29] D. Worth. Cok: Cryptographic one-time knocking. *Talk slides, Black Hat USA*, 2004.

[30] S. Zander, T. Nguyen, and G. Armitage. Automated traffic classification and application identification using machine learning. In *Local Computer Networks, 2005. 30th Anniversary. The IEEE Conference on*, pages 250–257. IEEE, 2005.

Selbstorganisation für heterogene Netzwerke

Christian Burger-Ringer
Betreuer: Tsvetko Tsvetkov
Hauptseminar Innovative Internettechnologien und Mobilkommunikation WS13/14
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: christian.burger.ringer@gmail.com

KURZFASSUNG

Die stetig wachsende Nachfrage nach mobiler Kommunikation hat um das Jahr 2007 zu einem exponentiellen Anstieg des mobilen Datenverkehrs geführt. Die Telekommunikations-Infrastruktur muss durch sogenannte Low-Power Nodes (LPN) erweitert werden, um höchste Netzwerk-Abdeckung und -Performanz zu gewährleisten, wodurch auch die Anzahl der Netzwerkelemente (NE) um eine Größenordnung steigt. Damit es in einem solchen heterogenen Netzwerk (hetNet) nicht zu einer parallelen Explosion der Kosten kommt, sind Mobilfunkbetreiber auf die Selbst-Organisation des Netzwerks angewiesen. Der vorliegende Artikel bespricht wichtige Konzepte der Selbst-Organisation (Selbst-Konfiguration, -Optimierung, -Heilung) und geht auf Herausforderungen des Forschungsfeldes ein.

Schlüsselworte

Heterogene Netzwerke, Selbstorganisation, Mobilfunk

1. EINFÜHRUNG

Wie Abbildung 1 zeigt, kommt es heute zu einem nahezu exponentiellen Anstieg des Datenverkehrs. Dies ist vor allem auf die Verbreitung von mobilen Endgeräten mit entsprechendem Datenservice (z.B. Smartphones, Tablets) und mobile Modems zurückzuführen. Der Ericsson Mobility Report prognostiziert zwischen 2013 und 2019 eine Verzehnfachung des Datenaufkommens [5].

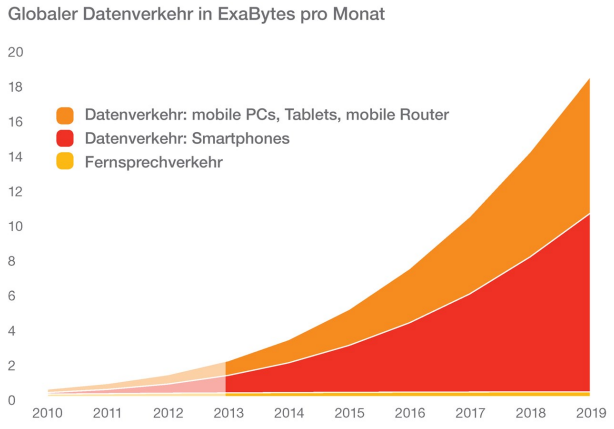


Abbildung 1: Entwicklung des globalen Datenverkehrs seit 2010 mit Prognose bis 2019 [5]

Nutzer erwarten sich nach Möglichkeit unbegrenzte Kapazität, höchste Performanz und beste Netzabdeckung. Bereits heute wäre es in Ballungsräumen nicht mehr denkbar, diese Anforderungen ausschließlich durch herkömmliche Makro-Basisstationen (MBS) zu gewährleisten. Somit wird die Telekommunikations-Infrastruktur durch LPN unterstützt, welche Nutzern in Innen- wie Außenräumen gute Servicequalität bieten [4]. Da LPN jedoch nur geringe Reichweite von bis zu 100 Metern bieten, wird davon ausgegangen, dass zehn mal mehr LPN als Makro Basistationen erforderlich sind.

Traditionell war die Installation, der Betrieb und die Wartung von Basisstationen mit hohen Kosten verbunden. Durch die Vervielfachung der Basisstationen sind Mobilfunkbetreiber darauf angewiesen, den manuellen Aufwand auf ein Minimum zu reduzieren. Auch das Aufkommen von Femto-Zellen, einer Unterkategorie der LPN, welche von Nutzern oder Firmen installiert werden, machen einer plug & play Installation notwendig. Aus diesen Gründen ist die Selbst-Organisation besonders in heterogenen Netzwerken unentbehrlich.

2005 schrieben Prehofer und Bettstetter: Telekommunikations-Netzwerke haben das Potential der Selbst-Organisation noch nicht voll ausgeschöpft; viele Funktionen erfordern noch immer erheblichen manuellen Konfigurationsaufwand (vgl. [10]). Durch das 3rd Generation Partnership Project (3GPP) wurde 2008 innerhalb des Releases 8 die Selbstorganisation von Netzwerken erstmals explizit in den Standardisierungsprozess aufgenommen [2].

Die vorliegende Arbeit ist wie folgt gegliedert: Im zweiten Abschnitt wird eine knapper Überblick zu hetNet und deren Elementen gegeben. In Abschnitt 3 wird in das Thema der Selbst-Organisierenden Netzwerke (SON) eingeführt. Abschnitt 4 zeigt wie die Managementarchitektur in hetNet aufgebaut ist. In den Abschnitten 5-7 werden die detailliert auf die Teilaspekte Selbst-Konfiguration, -Optimierung, -Heilung von SON in Hinblick auf hetNet eingegangen. Der Abschnitt 8 gibt einen Ausblick für zukünftige Entwicklungen und Forschungstrends. Zuletzt wird noch ein Resümee gezogen.

2. ÜBERBLICK HETNET

Wie Abbildung 2 zeigt, sind hetNet mehrschichtig und bestehen aus verschiedenartigen Netzwerkelementen (NE). Bei den NE wird grob zwischen MBS und LPN unterschieden. LPN untergliedern sich wiederum in [11][3]:

doi: 10.2313/NET-2014-03-1_09

1. **Remote-Radio-Heads** stellen ein verteiltes Antennen-System dar und sind mit der MBS über ein Glasfaserkabel verbunden.
2. **Micro-Basisstationen** haben den selben Aufbau wie MBS, ihr Reichweite liegt bei ca. 100 Metern.
3. **Picto-Basisstationen** haben den selben Aufbau wie MBS, ihr Reichweite liegt zwischen 20 und 50 Metern.
4. **Femto-Zellen** weden nicht vom Mobilfunkbetreiber installiert, sondern vom Kunden an den eigenen Breitbandzugang angeschlossen. Ihre Reichweite liegt zwischen 10 und 20 Metern. Entspricht eine Femto-Zelle dem LTE-Standard, so wird sie auch Home evolved NodeB (HeNB) genannt.
5. **Relais-Knoten** sind zwar vollwertige Basisstationen, haben jedoch keine verkabelte Anbindung zum Netzwerk. Daher ist der Relais-Knoten immer mit einer herkömmlichen Basisstation kabellos verbunden.

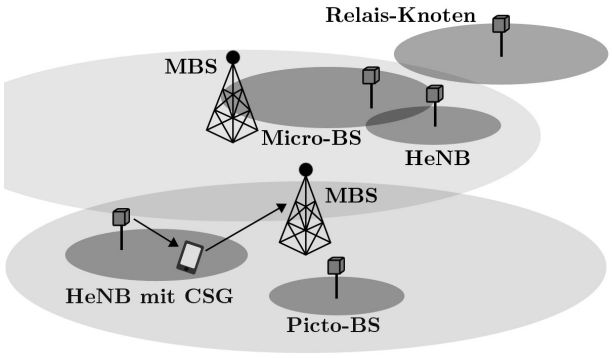


Abbildung 2: hetNet Szenario mit MBS in Kombination mit mehreren LPN [4]

3. ÜBERBLICK SON

Für den Mobilfunkbetreiber liegt das Potential der SON einerseits in der Reduzierung der Kosten für die Aufstellung & Installation der NE (CAPEX) und den Betrieb der NE (OPEX). Andererseits wäre es nicht mehr möglich, angesichts der steigenden Zahl an NE in hetNet, den Prozess des Betriebs, der Verwaltung und der Wartung des Netzwerks (operation, administration, maintenance; OAM) manuell durchzuführen [7]. Um eine brauchbare Roadmap für die Entwicklung der SON zu konzipieren, definierte die NGMN (Next Generation Mobile Networks) Vereinigung die wichtigsten Anwendungsfälle bzw. Probleme im Rahmen des Aufbaus und Betriebs eines Mobilfunknetzes [8] [9]. Die Anwendungsfälle lassen sich grob in die vier Kategorien Planung, Installation, Optimierung und Instandhaltung einteilen. Zur Illustration werden im Folgenden beispielhaft die Anwendungsfälle der Installation genannt: [I01] Hardware-Installation, [I02] Netzwerk-Authentifikation, [I03] Software-Installation, [I04] Transportparameter-Einstellung, [I05] Funkparameter-Einstellung, [I06] Verbindungs-Test.

Die Anwendungsfälle legen die Anforderungen an SON fest und sind somit der Ausgangspunkt für SON-Funktionen, die im Standardisierungsprozess des 3GPP (teilweise) definiert wurden. Zu den SON-Funktionen zählen unter anderem:

- Automatische Nachbarschafts Beziehungen (Automatic Neighbour Relationship Setup; ANR)
- Optimierung der Mobilitäts-Robustheit (Mobility Robustness Optimization; MRO)
- Lastverteilung (Mobility Load Balancing; MLB)
- Abdeckungs- & Kapazitätsoptimierung (Coverage and Capacity Optimization; CCO)
- Minimierung der Drive Tests (Minimization of Drive Tests; MDT)
- Zellenausfall-Kompensation (Cell Outrage Compensation; COC)

In Anlehnung an den Lebenszyklus (Planung, Installation, Optimierung und Instandhaltung) setzt sich, wie Abbildung 3 zeigt, die OAM Architektur von SON aus vier Teilbereichen zusammen: Planung, Selbst-Konfiguration, -Optimierung & -Heilung. Innerhalb der Teilbereiche kommen die entsprechenden SON-Funktionen zum Einsatz. So wird in der Planungs- & Konfigurations-Phase die Aufstellung, Installation & Konfiguration neuer NE vorgenommen. Hingegen befasst sich die Selbst-Optimierung mit der Verbesserung der Performanz und die Selbst-Heilung mit der Ermittlung & Lösung von Netzwerkfehlern.

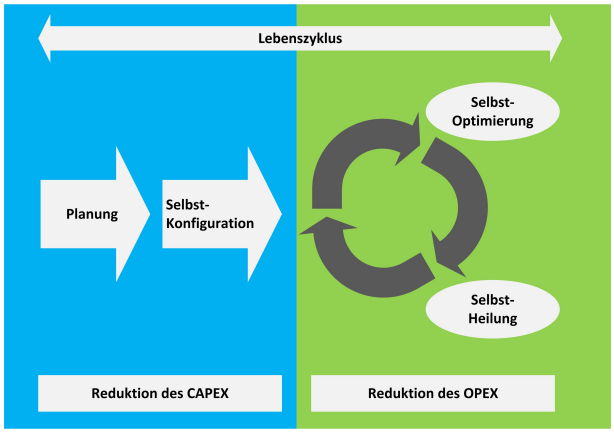


Abbildung 3: SON in OAM [13][14]

4. MANAGEMENTARCHITEKTUR

Das Netzwerk wird durch die Managementarchitektur betrieben und gesteuert, die in Abbildung 4 schematisch dargestellt wird. Der Betreiber steuert das gesamte Netzwerk über das Netzwerkmanagementsystem (NM), welches über die Nord-Schnittstelle (Itf-N) mit dem Domänenmanager (DM) interagieren kann. Jedem DM sind wiederum eine Reihe von NE zugewiesen. Grundsätzlich werden die Netzwerkregeln (wie z.B. Konfigurationsparameter, Referenzwerte) vom NM an den DM und vom DM über die Süd-Schnittstelle (Itf-S) an die einzelnen NE übertragen. Hingegen werden Informationen zur Performanz, zu Fehlern und zu abgeschlossenen Konfigurationen in umgekehrter Richtung vom NE aufwärts übertragen. Einzelnen Performanz-Informationen eines Netzwerkelements (wie z.B. Anzahl der Verbindungsversuche, Anzahl der erfolgreichen Verbindungsversuche) werden auf höherer Ebene zu Leistungskennzahlen (KPI) aggregiert [6].

doi: 10.2313/NET-2014-03-1_09

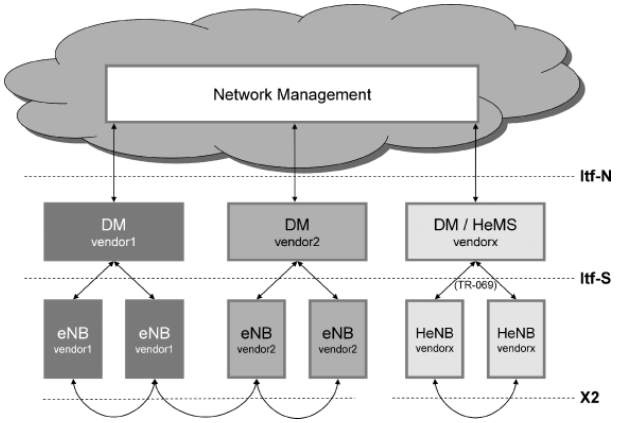


Abbildung 4: LTE Managementarchitektur [11]

5. SELBST-KONFIGURATION

Ein neues NE muss sich möglichst selbstständig in Betrieb nehmen und mit dem Netzwerk verbinden können. Natürlich erfordert die Installation von MBS höhere manuelle Intervention, als LPN die weitestgehend auf einer plug & play Installation basieren. Der Selbst-Konfigurationsprozess kann hierbei in folgende fünf Phasen untergliedert werden [11][6]:

1. **Aufbau einer grundlegenden Netzwerkverbindung:** Dem NE wird eine vorläufige IP-Adresse zugewiesen.
2. **Aufbau einer sicheren Netzwerkverbindung mit dem Auto-Connection Server:** Das Sicherheitszertifikat wird vom Netzbetreiber heruntergeladen. Dadurch wird es dem NE unter anderem ermöglicht, mit Nachbarknoten Informationen auszutauschen.
3. **Standortbestimmung:** Der genaue Standort des NE wird benötigt, sodass das OAM-System die Konfigurationsparameter (wie z.B. Sendeleistung und Antennenausrichtung) entsprechend berechnen kann.
4. **Verbindung mit dem OAM-System:** Die erforderliche Software wird heruntergeladen und installiert. Die Transport- und Konfigurationsparameter werden übergeben.
5. **Aufbau einer sicheren Verbindung:** Die provisorische Verbindung mit dem Auto-Connection Server wird getrennt. Im Falle von HeNB wird eine verschlüsselte Verbindung mit dem DM bzw. dem HeNB-Management-System über eine standardisiertes Itf-S (nach Standard TR-069) hergestellt. eNB werden über ein herstellerspezifisches Itf-S mit dem DM des Herstellers verbunden. Über die X2-Schnittstelle kann zudem eine Verbindung zwischen Nachbarknoten hergestellt werden.

Mit Ausnahme von Relais-Knoten ist der beschriebene Konfigurationsprozess weitestgehend herstellerspezifisch. Da Relais-Knoten keine verkabelte Anbindung zum Netzwerk haben, weicht der Selbst-Konfigurationsprozess vom dargestellten Ablauf ab und wurde teilweise standardisiert.

6. SELBST-OPTIMIERUNG

Die Anforderungen an die Selbst-Optimierung wurden durch das 3GPP definiert. Wie Abbildung 3 zeigt, dient die Selbst-Optimierung vorallem der Reduktion des OPEX. Durch entsprechende SON-Maßnahmen gelingt es den manuellen Wartungsaufwand auf ein Minimum zu reduzieren. Das vorliegende Kapitel zeigt die Aspekte auf, die die Selbst-Organisation umfasst.

6.1 Automatische Nachbarschaftsbeziehungen

Eine zentrale Anforderung an Mobilfunknetzwerke ist es, die Verbindung zwischen Endgerät und Netzwerk aufrecht zu erhalten, wenn sich das Endgerät aus dem Abdeckungsbereich des bedienenden Knotens bewegt. Hierbei wird das Endgerät von einem Knoten an einen anderen übergeben. Dieser Prozess wird auch Handover (HO) genannt. Um einen reibungslosen HO zu gewährleisten, ist es erforderlich, dass die Nachbarschaftsbeziehungen zwischen den Knoten bekannt sind [15].

Die Herstellung von Nachbarschaftsbeziehungen ist in Nicht-SON mit größtem Aufwand verbunden, da die Beziehungen einzeln vorkonfiguriert werden müssen. Daher ist die automatisierte Konfiguration der Nachbarschaftsbeziehungen (automatic neighbor relation; ANR) - vorallem in hetNet - einen Schlüsselanforderung an SON. In GSM und UMTS wird die ANR zentral Basisstations- bzw. Funknetzwerkssteuerung vorgenommen. Da in LTE keine zentrale Kontrollinstanz die ANR steuert, wird der HO zwischen den Knoten direkt über X2-Schnittstelle abgewickelt. Alternativ kann in LTE der HO auch über Itf-S koordiniert werden [16] (siehe Abbildung 4).

6.2 Identitäts-Management

In der Phase der Selbst-Konfiguration werden den Knoten PCI (Physical Layer Cell Identity) zugewiesen, wobei beispielsweise in LTE nur 504 verschiedene PCI Kombinationen existieren. Haben zwei Knoten in der selben Nachbarschaft die selbe PCI, so kann es zu den Fehlern PCI-Verwechslung oder PCI-Kollision kommen. Die PCI-Verwechslung tritt ein, sobald zwei benachbarte Zellen die selbe PCI haben, ihr Abdeckungsbereiche sich jedoch nicht überlappen (siehe Abbildung 5). Zur PCI-Kollision kommt es hingegen, sobald zwei benachbarte Knoten nicht nur die selbe PCI haben, sondern ihre Abdeckungsbereiche sich auch überlappen (siehe Abbildung 5 & 6). Die Mehrfachzuweisung von PCI in der selben Nachbarschaft, kann nur durch die Überprüfung der ECGI (Evolved Cell Global Identifier) - einer eindeutigen Knoten-Identifikationsnummer - erkannt werden [6].

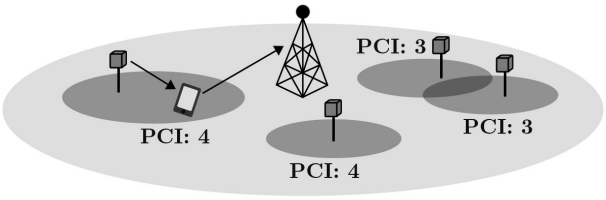


Abbildung 5: PCI-Verwechslung und PCI-Kollision

Grundsätzlich bestehen zwei Möglichkeiten, um eine PCI-Verwechslung aufzufinden:

doi: 10.2313/NET-2014-03-1_09

1. Ein Endgerät wird von einem LPN bedient. Das Endgerät entdeckt eine MBS. Der LPN fordert das Endgerät auf, ihr die ECGI der MBS zu übermitteln. Durch diese Information kann eine X2-Verbindung zwischen der MBS und dem LPN aufgebaut werden. Ist die X2-Verbindung aufgebaut, so erkennt die MBS, dass sich in ihrem Abdeckungsbereich zwei LPN mit derselben PCI befinden [18].

2. Alternativ können vermehrte HO-Fehler ein Indikator für eine PCI-Kollision sein. In diesem Fall werden die verfügbare Endgeräte von der MBS aufgefordert, die ECGI des LPN mit der entsprechenden PCI zu übermitteln. Wenn zu der entsprechenden PCI mindestens zwei verschiedene ECGI zurückgeliefert werden, konnte die PCI-Verwechslung erfolgreich erkannt werden [18].

Eine PCI-Kollision kann von den betroffenen LPN nicht als solche erkannt werden. Allerdings identifiziert die MBS diese als eine PCI-Verwechslung. Nachdem eine PCI-Verwechslung erkannt wurde, wird das OAM benachrichtigt. Daraufhin wird eine zentralisierte Neukonfiguration der PCI vorgenommen, indem einem der betroffenen Knoten eine neue noch verfügbare PCI zugewiesen wird [18].

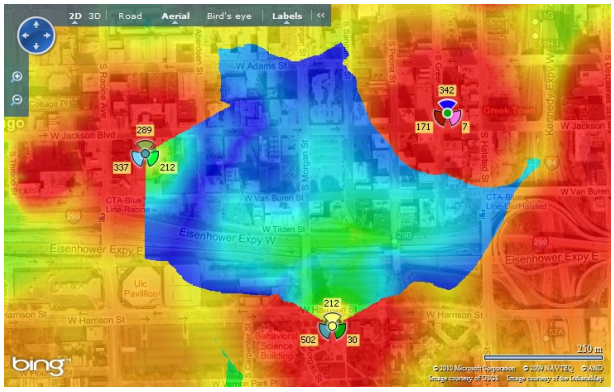


Abbildung 6: Signalqualität-Karte bei einer PCI-Kollision. Die roten Bereiche zeigen hohe Signalqualität; die blauen Bereiche zeigen niedrige Signalqualität [17]

6.3 Interferenz Management

In hetNet ist die Interferenz ein zentrales Thema, da in mehrschichtigen Netzwerken die Wahrscheinlichkeit der Wellen-Überlagerung höher ist, als in reinen Makro-Netzwerken. Dies ist vorallem auf die Wiederverwendung der Frequenzbereiche durch die NE zurückzuführen. Die schwierigsten Interferenzkonstellationen ergeben sich, sobald ein HeNB als Closed Subscriber Group (CSG) konfiguriert wird. In einer CSG werden nur angemeldete Nutzer vom HeNB bedient. Nutzer die nicht zur CSG gehören sich jedoch in der Nähe des Knotens befinden, werden im Downlink starke Interferenz erfahren, vorallem wenn das nächste freie NE in einiger Entfernung und die Signalstärke nur mehr schwach ist. Auch im Uplink wird die geschlossenen HeNB starke Interferenz erfahren, da ein nicht angemeldetes Endgerät mit hoher Signalstärke senden muss, sodass das bedienende NE das Signal noch empfangen kann [11].

Grundsätzlich gibt es zwei Möglichkeiten um mit Interferenzproblemen in CSG umzugehen: Verringerung der Signalstärke und Aufteilung der Trägerfrequenz. Die Veringerung der Signalstärke des geschlossenen HeNB führt dazu, dass die Endgeräte geringere Interferenz erfahren. Mithilfe von verfügbaren Endgeräten findet der HeNB die Signalstärke des nächsten offenen NE heraus. Je nachdem, wie er seine eigene Signalstärke einstellt, wird die Signalstärke des offenen NE besser oder schlechter. Reduziert der geschlossene HeNB allerdings seine Signalstärke, so verringert sich auch sein Abdeckungsbereich. Bei der Aufteilung der Trägerfrequenz sendet der geschlossene HeNB nur in einem bestimmten Frequenzbereich. Dadurch gibt es für nicht angemeldete NE die Möglichkeit auf interferenzfreien Frequenzbereichen zu senden [11].

6.4 Optimierung der Mobilitäts-Robustheit

Nomen est omen: Die Mobilität ist ein zentrales Merkmal der Mobiltelefonie. Folglich ist die Mobilitäts-Robustheits-Optimierung (MRO) zwangsläufig eine wesentliche Anforderung an SON. Die Ziele der MRO sind folgende [12]:

- **Minimierung der Anrufunterbrechungen:** Eine bestehende Telefonverbindung wird unterbrochen da das Endgerät die Verbindung zum RAN (Radio Access Network) verliert
- **Minimierung der Verbindungsfehler:** Bei Verbindungsfehlern (Radio Link Failures; RLF) verliert das Endgerät ebenfalls die Verbindung zum RAN. Allerdings kann die Verbindung wieder aufgebaut werden, bevor es zu einer Anrufunterbrechung kommt.
- **Minimierung überflüssiger HO:** Hierbei handelt es sich unter Anderem so genannte Ping-Pongs, wobei es innerhalb kurzer Zeit zu wiederholten HO zwischen zwei Zellen kommt. Hierdurch kommt es zu einer Verschwendung von Netzwerkressourcen.
- **Minimierung von Problemen im Ruhemodus:** Durch Kontrollmechanismen muss garantiert werden, dass das UE jederzeit eine Verbindung aufbauen kann.

Die genannten Fälle lassen sich auf folgende Probleme zurückführen:

1. **Verfrühter HO:** Zelle A übergibt das UE an Zelle B. Die Verbindung des UE zu Zelle B ist allerdings zu schwach, sodass es möglicherweise zu einem RLF kommt.
2. **Verspäteter HO:** Zelle A übergibt das UE nicht an Zelle B, obwohl ein HO möglich wäre. Die Verbindung zu Zelle A wird zu schwach, sodass es möglicherweise zu einem RLF kommt.
3. **HO zur falschen Zelle:** Zelle A sollte das UE an Zelle B übergeben, stattdessen wird das UE jedoch an Zelle C übergeben, sodass es möglicherweise zu einem RLF kommt.
4. **Ping-Pong:** Zelle A übergibt das UE an Zelle B. Nach kurzer Zeit findet wieder ein HO von Zelle B zu Zelle A statt.

5. **Kurze Verweildauer:** Zelle A übergibt das UE an Zelle B und Zelle B übergibt das UE an Zelle C, obwohl Zelle A das UE auch direkt an Zelle C übergeben hätte können.
6. **Überflüssiger HO von vorrangigen zu nachrangigen Standards:** Das UE wird bspw. von einem LTE an ein 3G Netzwerk übergeben, obwohl sich das UE nach wie vor im Abdeckungsbereich des LTE-Netzwerks befindet.
7. **HO direkt nach der Verbindung:** Im Ruhemodus (ïdle mode") wird die Verbindung durch das UE aufgebaut. Im Verbindungsmodus ("connected mode") bestimmt die Zelle über den HO. Findet direkt nach der Verbindung des UE mit Zelle A ein HO zu Zelle B statt, so ist dieser HO überflüssig und die Parameter des Ruhe- & Verbindungsmodus müssen neu konfiguriert werden.

In LTE-Netzwerken wird der HO von dem betroffenen Endgerät aktiv unterstützt. Hierbei sendet das Endgerät einen Messreport (MR) an sein bedienendes NE, sobald ein bestimmtes Kriterium eintritt. Eine Sammlung dieser Kriterien findet sich in [19]. Beispielhaft wird hier das Event A3 angeführt, wobei ein MR gesandt wird, sobald folgende Aussage wahr ist:

$$\gamma_i^{(dB)} + \lambda_i^{(dB)} > \gamma_s^{(dB)} + \lambda_s^{(dB)} + \Delta^{(dB)} \quad (1)$$

Hierbei bezeichnet s das bedienende und i das potentielle NE; Δ bezeichnet die HO-Schwelle um überflüssige HO zu verhindern; γ steht entweder für die Signalstärke oder die Signalqualität; λ bezeichnet die vorhandene Frequenzabweichung (zur Reduktion der Interferenz). Wenn beispielsweise $\lambda_i^{(dB)} = \lambda_s^{(dB)}$ wird dem bedienenden NE ein MR gesandt, sobald die Signalstärke eines potentiellen NE besser ist und auch die HO-Schwelle überschritten wird ($\gamma_i^{(dB)} > \gamma_s^{(dB)} + \Delta^{(dB)}$).

Sobald das Endgerät einen MR an sein bedienendes Quell-NE sendet, wird dieses einen HO einleiten. Wenn das potentielle Ziel-NE den HO akzeptiert, so übermittelt das Quell-NE die Direktzugriffsinformationen an das Endgerät, welches sich daraufhin direkt mit dem Ziel-NE verbinden kann (siehe Abbildung 7).

Das Hauptziel der MRO ist die Realisierung an die eingangs genannten Ziele Minimierung von Anrufunterbrechungen, Verbindungsfehlern, überflüssigen HO und Problemen im Ruhemodus. Hierzu werden relevante Daten gesammelt und analysiert. Verliert das UE beispielsweise die Verbindung zum RAN (Radio Access Network) so werden nach erneutem Verbindungsaufbau unter anderem folgende Informationen übertragen: zuletzt bedienendes NE, Signalstärke, Messwerte der potentiellen Nachbarzellen, GPS-Daten, Dauer bis zum erneuten Verbindungsaufbau, etc. [6]. Wird vom OAM-System ein Verbesserungspotential ausgelotet, so werden die Konfigurationsparameter entsprechend angepasst. Wird beispielsweise ein Ping-Pong zwischen zwei Zellen erkannt, so kann das OAM-System beispielsweise die HO-Schwelle Δ erhöhen [6].

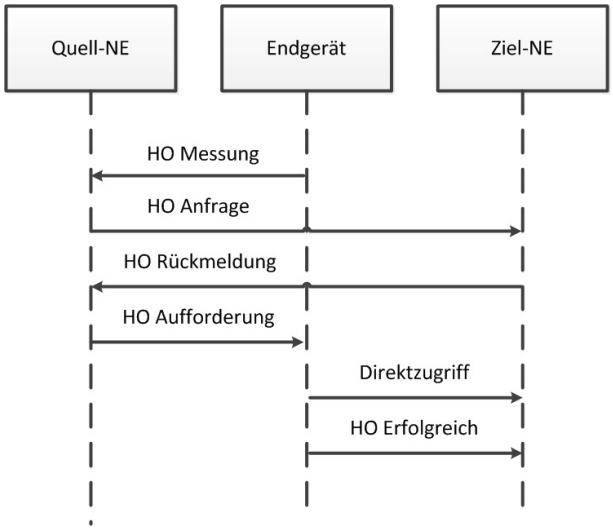


Abbildung 7: Ein HO in einem LTE Netzwerk über die X2-Schnittstelle

6.5 Lastverteilung

Die Mechanismen zur Lastverteilung (Mobility Load Balancing; MLB) wurden vom 3GPP eingeführt, um die Überlastung einzelner NE zu verhindern und das Datenaufkommen gleichmäßig auf die verfügbaren NE zu verteilen. Als Indikatoren für die Überlastung einzelner NE gilt die Häufung von HO-Fehlern bei dem betroffenen Knoten. Die Algorithmen zur Lastverteilung brauchen natürlich immer die Lastinformationen der benachbarten Zellen. Diese können sich auf die Auslastung der Hardware und die Auslastung des Netzwerks beziehen [11].

In hetNet ist es zudem häufig der Fall, dass LPN weniger Datenvolumen zugeteilt wird als MBS, was Mechanismen zur Lastverteilung erforderlich macht. Wie in Abbildung 8 gezeigt wird, ist die Erhöhung der Übertragungsstärke des NE und somit ihres Abdeckungsbereichs eine Möglichkeit, um das Problem zu adressieren. Natürlich ist die Möglichkeit dieses Vorgehen von der Leistungsfähigkeit des einzelnen NE abhängig [11].

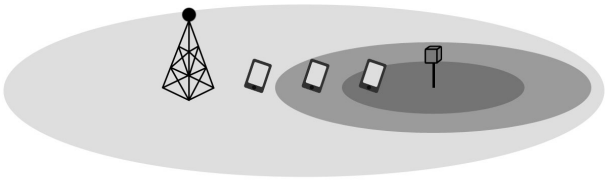


Abbildung 8: Erhöhung der Übertragungsstärke eines LPN, um eine effiziente Lastverteilung zu erreichen.

7. SELBST-HEILUNG

Da LPN natürlich weniger fortgeschritten sind wie MBS, drohen in hetNet die Kosten für das Fehler-Management mit der Anzahl an LPN zu steigen. Eine Anforderung an SON ist somit, die Kosten für das Fehler-Management möglichst gering zu halten. Daher werden Mechanismen zur Selbst-

Heilung in den NE und/oder im OAM-System implementiert. Folgende Anwendungsfälle für die Selbst-Heilung sind denkbar:

- **Ausfall-Erkennung:** Erkennung von NE die keine Daten übertragen oder auf Anfragen nicht reagieren.
- **Ausfall-Behebung:** Module des NE werden neu gestartet.
- **Ausfall-Kompensation:** Wenn eine Ausfall-Behebung nicht erfolgreich durchgeführt werden konnte, wird das NE ausgeschaltet und Nachbarzellen kompensieren nach Möglichkeit den Ausfall.
- **Rückkehr zum Ausgangszustand nach einer Ausfall-Kompensation:** Nachdem das fehlerhafte NE wieder funktionsfähig ist, kehrt das Mobilnetzwerk wieder in seinen Ausgangszustand zurück.

Innerhalb des 3GPP wurden bestimmte Auslöße-Zustände für die Selbst-Heilung (Triggering Conditions of Self-Healing; TCoSH) definiert, welche ständig überwacht werden. Sobald eine TCoSH eintritt, wird ein entsprechender Selbst-Heilungsprozess ausgelöst. Hierbei kann durch Tests herausgefunden werden, welche Maßnahmen zur Behebung des Ausfalls nötig sind. Bevor die entsprechenden Schritte jedoch durchgeführt werden, wird die aktuelle Konfiguration gesichert und das OAM-System wird zu den geplanten Selbst-Heilungs-Maßnahmen benachrichtigt. Eine mögliche Maßnahme zur Kompensation eines NE-Ausfalls ist beispielsweise die Erhöhung der Downlink-Übertragungsstärke mit einer einhergehenden Erweiterung des Abdeckungsbereichs. Im Uplink kann die Übertragungsstärke der Endgeräte reduziert werden, sodass Interferenz nach Möglichkeit vermieden wird [6].

Im Vergleich zu anderen Fehlern ist die Erkennung von schlafenden Zellen (ßleeping cells") besonders schwer. Schlafende Zellen senden und empfangen keine Daten, sind aus Sicht des OAM-Systems jedoch voll einsatzfähig. die weder Daten senden noch empfangen - um einiges komplizierter. In [20] wird empfohlen durch eine Datenanalyse ein Muster in so genannten Diffusions-Landkarten zu finden um schlafende Zellen zu erkennen.

8. ZUKÜNFTIGE ENTWICKLUNGEN

Die hohe Anzahl an LPN in hetNet führt zu wesentlichen Interferenzproblemen, für welche bisher noch nicht ausreichend Lösungen entwickelt wurden. Die Bewältigung dieses Problems liegt sicherlich in der Zuweisung von Frequenzbereichen an NE und die Regulation der Übertragungsstärke. Erst durch ausgefeiltere Selbstorganisations-Maßnahmen, können sich NE erfolgreich in ihre Nachbarschaft eingliedern und zugleich durch Parameteranpassungen intelligent auf Änderungen in ihrer unmittelbaren Nachbarschaft einstellen[7].

Weiters können LPN zusätzlich verbessert werden, indem Techniken wie Reinforcement Learning (RL) implementiert werden. Hierbei können die Konfigurations-Parameter unabhängig von Nachbarknoten angepasst werden. Dadurch müssen weniger Daten zwischen den NE ausgetauscht werden, wodurch sich NE u.U. besser in das Gesamtsystem einfügen. Eine weitere Möglichkeit die Interferenzprobleme zu adressieren, ist die Coordinated Multi Points Methode, welche eine wichtige Technologie innerhalb der LTE-Advanced darstellt [7].

9. ZUSAMMENFASSUNG

Die vorliegende Arbeit gab einen Einblick in das Thema der selbstorganisierenden heterogenen Netzwerke. Wie gezeigt wurde, ist die Heterogenität innerhalb des LTE und UMTS Mobilfunkstandards zu einer unumgänglichen Realität geworden, da optimale Kapazität, Performanz und Netzabdeckung nicht anders gewährleistet werden können. Parallel dazu muss das Netzwerk durch die steigende Komplexität die Fähigkeit zur Selbstorganisation erwerben. Aus diesem Grund waren die SON-Funktionalitäten innerhalb des 3GPP LTE Standardisierungsprozesses von Anfang an dabei. Nur durch intensive Forschung in der Wissenschaft und der Wirtschaft, ist es möglich den Anforderungen der Nutzer gerecht zu werden.

In der Arbeit wurde gezeigt, welche Aspekte die Selbstorganisation umfasst. Schrittweise wurden die Konzepte der Selbst-Konfiguration, -Optimierung & -Heilung besprochen. All diese Aspekte der Selbstorganisation wurden spezifisch in Hinblick auf heterogene Netzwerke diskutiert. Ziel der Arbeit war es, dem Leser einen fundierten Einblick in das Thema zu verschaffen und die Kernthemen des Forschungsfeldes zu beleuchten.

10. LITERATUR

[1] G. Mulligan: *The 6LoWPAN Architecture*, In Proceedings of the 4th Workshop on Embedded Networked Sensors (EmNets), pages 78-82, ACM New York, NY, USA, 2007

[2] *3GPP work items on Self-Organizing Networks (v0.0.9),* Sep, 2013.

[3] X. Chu, D. Lopez-Perez, F. Gunnarsson, and Y. Yang, "Introduction," in *Heterogeneous cellular networks. Theory, simulation, and deployment.* X. Chu, D. Lopez-Perez, Y. Yang, F. Gunnarsson, Eds. Cambridge: Cambridge University Press, 2013, pp. 1–14.

[4] A. Damnjanovic, J. Montojo, Y. Wei, T. Ji, T. Luo, and M. Vajapeyam, et al., "A survey on 3GPP heterogeneous networks," *IEEE Wireless Commun.,* vol. 18, pp. 10–21, 2011.

[5] *Ericsson Mobility Report. On the Pulse of the Networked Society.* Stockholm, Schweden, Nov, 2013.

[6] F. Gunnarsson, "Self-Organization," in *Heterogeneous cellular networks. Theory, simulation, and deployment.* X. Chu, D. Lopez-Perez, Y. Yang, F. Gunnarsson, Eds. Cambridge: Cambridge University Press, 2013, pp. 145–178.

[7] M. M. S. Marwangi, N. Fisal, S. K. S. Yusof, R. A. Rashid, A. S. A. Ghafar, and F. A. Saparudin, et al., "Challenges and practical implementation of self-organizing networks in LTE/LTE-Advanced systems," in *ICIMU 2011 : Proceedings of the 5th international Conference on Information Technology & Multimedia:* IEEE, 2011, pp. 1–5.

[8] F. Lehser, NGMN Informative List of SON Use Cases,

Next Generation Mobile Networks, 2007.

[9] F. Lehser, NGNM Use Cases related to Self Organising Network, *Next Generation Mobile Networks,* 2008.

[10] C. Prehofer and C. Bettstetter, "Self-organization in communication networks: principles and design paradigms," *IEEE Commun. Mag.,* vol. 43, pp. 78–85, 2005.

[11] C. Sartori, H. Sanneck, K. Pedersen, J. Pekonen, I. Viering, and D. Laselva, "SON for Heterogeneous Networks (hetNet)," in *LTE self-organising networks (SON). Network management automation for operational efficiency.* S. Hämäläinen, H. Sanneck, C. Sartori, Eds. Hoboken, N.J: Wiley, 2012, pp. 357–378.

[12] D. Laselva, I. Viering, D. Rose, J. Wigard, S. Hämäläinen, and K. Kordybach, et al., "Self-Optimisation," in *LTE self-organising networks (SON). Network management automation for operational efficiency.* S. Hämäläinen, H. Sanneck, C. Sartori, Eds. Hoboken, N.J: Wiley, 2012.

[13] N. Shah, Self Organizing Networks, LTE and OPEX, `http://shahneil.com/2010/04/son-lte-opex/`, 2013.

[14] R. Waldhauser, M. Staufer, S. Hämäläinen, H. Sanneck, H. Tang, and C. Schmelz, et al., "Self-Organizing Networks (SON)," in *LTE self-organising networks (SON). Network management automation for operational efficiency.* S. Hämäläinen, H. Sanneck, C. Sartori, Eds. Hoboken, N.J: Wiley, 2012, pp. 39–80.

[15] J. Zec, O. Stan, R. A. Garcia, N. Faour, C. Neophytou, and K. Hameied, et al., "Multi-Technology Self-Planning," in *Self-Organizing Networks (SON): Self-Planning, Self-Optimization and Self-Healing for GSM, UMTS and LTE.* J. Ramiro, K. Hamied, Eds.: Wiley, 2011.

[16] M. Sauter, "Long Term Evolution (LTE)," in *Grundkurs mobile Kommunikationssysteme. UMTS, HSDPA und LTE, GSM, GPRS und Wireless LAN.* 4th ed. M. Sauter, Ed. Wiesbaden: Vieweg + Teubner, 2011, pp. 279–336.

[17] Keima Limited, *Planning an LTE network. Use Overture to plan and analyze an LTE network,* http://overtureonline.com/Support/Tutorials/Planning/Technology/LTE.aspx, 2010.

[18] M. Amirijoo, P. Frenger, F. Gunnarsson, H. Kallin, J. Moe, and K. Zetterberg, "Neighbor Cell Relation List and Physical Cell Identity Self-Organization in LTE", in *ICC Workshops - 2008 IEEE International Conference on Communications Workshops*: IEEE, 2008, pp. 37–41.

[19] 3GPP, *Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC). Protocol specification Release 11 (TS 36.331) V11.5.0,* Sep, 2013.

[20] F. Chernogorov, J. Turkka, T. Ristaniemi, and A. Averbuch, "Detection of Sleeping Cells in LTE Networks Using Diffusion Maps," in *2011 IEEE 73rd Vehicular Technology Conference (VTC Spring): IEEE*, 2011, pp. 1–5.

doi: 10.2313/NET-2014-03-1_09

Internet Science – Energy Consumption and Optimization

Michael Reithmeier
Betreuer: Heiko Niedermayer
Innovative Internettechnologien und Mobilkommunikation WS1314
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: reithmei@in.tum.de

ABSTRACT

Energy saving is a mandatory part of environmental protection. At the same time it is difficult to get an overview what influences energy consumption and conservation. Therefore, a quick overview from statistics about energy usage is presented, focusing on private households and consumers. It is followed by an introduction to several methods aiming at consumer's behaviour to save energy. Starting from providing simple energy-information to users, more concepts like feedback, competition, pricing pressure or influencing decisions are discussed. The last section shows typical problems like personal habits and routines, industry and marketing or the rebound effect, that emerge along energy-saving scenarios, using the results from the previous insights.

Keywords

Energy, Consumption, Save, Environment, Smartmeter, Consumers, Behaviour, Influence

1. ENERGY CONSUMPTION OVERVIEW

Our whole life is governed by energy. We either consume it directly by turning up our heater or unwittingly by triggering an online search. However, only a minority of people really knows, how much energy they are consuming all day through. Energy just seems to be an abstract thing, everybody pretends to know about. It is available every time we need it, but in fact, most of the time we really don't care about energy. However, there exist these situations where energy comes to our mind, for example the moment when we open our energy bill, or when we see a TV report about ice bears struggling with melting ice floes.
In the first part of this work, we'll take a look at the amounts of energy that is actually consumed at daily basis. There is plenty of energy-statistics available, but most of them are quite abstract due to the fact that they aggregate the numbers of thousands or even millions of people. Therefore, our main goal is to get an impression about the proportions of different energy-consuming fields and to identify the real power-eating technologies peoples are dealing with.

1.1 Energy Consumption by fields

The most abstract view on energy consumption is given by a summation of the total required energy for a country like Germany, the so called *Primary energy consumption*. It includes all raw energy forms that are used to satisfy the demand both on production goods (*Non-energetic consumption*) and secondary energy like electrical energy or fuel (*End-energy consumption*).

In 2012, Germany had a *Primary energy consumption* of about 13757 PJoule (fig.1). Thereof, 7.1% (978 PJoule) were transformed to production goods and only about 65.4% (8998 PJoule) went further as *Secondary Energy*. Unfortunately, the remaining 27.5% (3781 PJoule) rested in the conversion from raw energy sources as coal or natural gas to goods or secondary energy. In other words: about one third of our used energy is lost – before even using it [5].

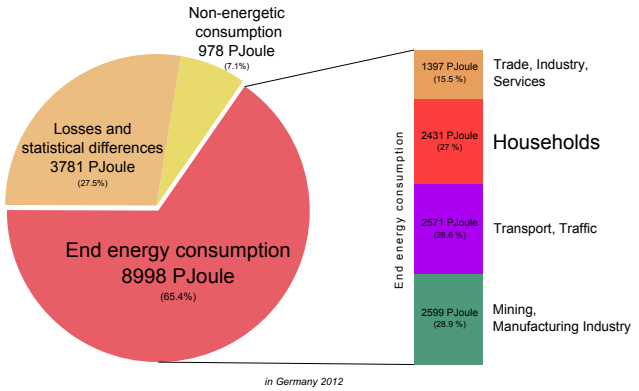


Figure 1: Primary / Secondary energy consumption in Germany 2012 [5]

If we now look at the produced *secondary energy*, we can distinguish four main fields of usage. The biggest consumption share has heavy industry and mining sector with 2599 PJoule (28.9%). Second largest field is traffic and transportation (2571 PJoule, 28.6%). With about 27% (2431 PJoule), private households go on rank three, followed by Trade, Industry and Services (1397 PJoule, 15.5%).
Thus, private households energy demand is about 18 percent of the total German primary energy consumption.

1.2 Private Energy Consumption

As we're interested in the Optimization Potential for consumers, we turn special attention to statistics regarding the use of energy in private households.
Figure 2 shows the average distribution of energy use in German households for 2010. Each histogram bar represents one typical energy source, as they appear for domestic use. The colours indicate the different application fields like *Room heating*, *lighting* or *information technologies*.
The most obvious fact from fig.2 is indicated by the large share of red blocks, which symbolize energy spent on heat-

doi: 10.2313/NET-2014-03-1_10

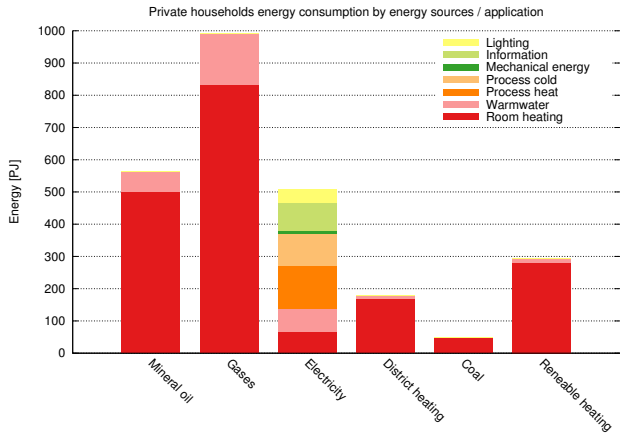


Figure 2: Private households energy consumption by energy sources/application in Germany 2010 [6]

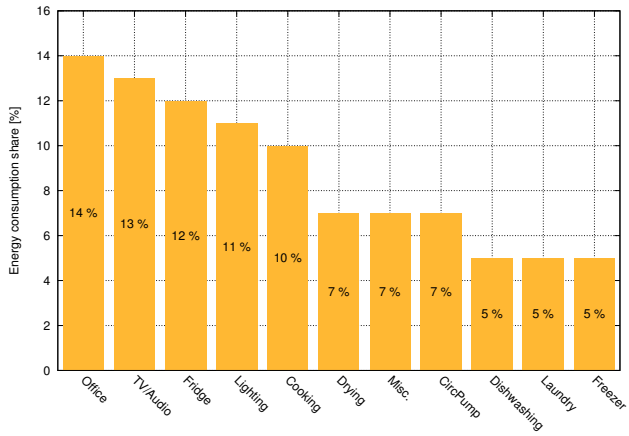


Figure 3: Energy consumption shares (without heating, German study 2011 [4])

ing. About 85% of private households energy is needed for the heating of rooms and warm water.
That means in turn, that only about 15% of domestic energy consumption is coming from general electric devices.

A report made from 380.000 datasets in 2011 attempts to demonstrate domestic energy usage, excluding heating and warm water (fig.3). It states that office equipment forms the largest share (14%) of electrical power, followed by TV and Audio devices (13%), the fridge (12%), lighting (11%) and other household devices [4]. Replacing the term *office equipment* with *computer equipment*, we get – together with the TV and Audio part – a share of 27 percent for end users Information and Communication Technology devices.

To get an impression of today's energy consumption values and its costs, the author did some measurements in his own household. Table 1 is divided into two categories. The first part *Long term energy consumption (per year)* lists some extrapolated values for the long term use of typical devices, the second part *Short time energy consumption (per use)* focuses on devices with high but short loads and presents the costs per use. The results suggest, that costs measured

Long time energy consumption (per year)			
Fridge:		202 kWh/a	47.14€/a
Desktop-PC1:	∼120W	311 kWh/a	72.48€/a
Desktop-PC2:	∼80W	145 kWh/a	33.78€/a
Notebook:	∼15W	26.3 kWh/a	6.11€/a
Router:	∼7W	37.8 kWh/a	8.80€/a
NAS (2bay):	∼15.5W	134.5 kWh/a	31.34€/a
Short time energy consumption (per use)			
Laundry (40°):		0.58 kWh	0.14€
Water kettle (1L):	∼2200W	0.13 kWh	0.03€
Microwave:	∼500W	0.03 kWh	0.01€
Espresso:	∼1000W	0.04 kWh	0.01€
Vac cleaner (15 min):	∼1000W	0.25 kWh	0.06€
			@ €0.233/kWh

Table 1: Own measurements of typical household activities

per use seem to be quite low compared to the estimated annual costs for longer used devices. Another issue is the growing number of always-on devices. Most of them have low wattages, but viewed together and for a long period, they sum up to a quite considerable cost factor.

1.3 Trends and change in Energy use

Energy use can not be seen as a static quantity, it is always varying over time. This is also one of the reasons, why people often have difficulties comparing energy consumption values.
If we look at the German energy consumption of the last twenty years, at first glance, there seems to be no big change over time (fig.4).

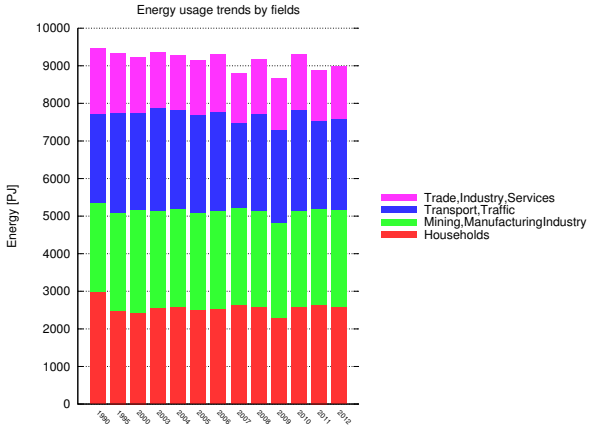


Figure 4: Energy usage trends by fields

But taking into consideration the units scales of the graph, the amount of yearly used energy is actually fluctuating by about 500 PJoule. 500 PJoule correspond to about 138.9 billion kWh, that is approximately the electricity consumption of Norway in 1998 (according to WolframAlpha). This also illustrates the fact, that humans have difficulties to grasp energy consumption values, especially with high quantities or absolute numbers.

doi: 10.2313/NET-2014-03-1_10

Special observance is required for the fast changing ICT sector. Figure 5 from [13] visualizes the worldwide energy consumption for Information and Communication Technology. Whereas the rising number of LCD-monitors eats up the energy saving inducted by replacing CRT- by LCD-models, there is a clear trend towards a more demanding network sector. In almost the same manner, Data centers grow continuously and consume more and more energy. Overall, the share of ICT products in the global electricity consumption has grown from 4% in 2007 to 4.7% in 2012 and the recent growing rate of worldwide electrical ICT consumption is estimated at 6.6% per year [13].

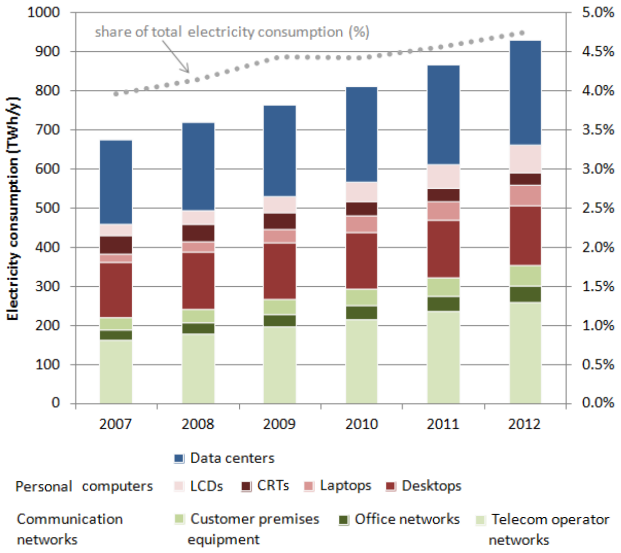


Figure 5: Trends in ICT energy usage (cf.[13])

2. SEVERAL IDEAS TO MAKE PEOPLE SAVE ENERGY

Nearly as long as there had been energy use, people have made attempts to save energy. Originally, the saving has been motivated by limited resources, but over the last decades, several new goals like climate protection and sustainability appeared.

There is a huge innovation market for energy-saving technologies, and almost every industry promotes its products as *environmental friendly*. What many companies disregard, is the *human factor* for energy saving. Technology can only be used effectively and energy-saving, if people use it the right way. Polls have shown, that consumers are willing to save energy, and feel themselves as *energy-aware*: "66 percent of global consumers say that they prefer to buy products and services from companies that give back to society" [2] and a representative survey of the German Department of the Environment concluded, that about 78% of German people consider themselves as sufficiently energy-conscious and ecology-minded [10].

The following section will present some concepts that tempt to make people save more energy, beginning with the most simple, then going to the more demanding and sophisticated methods.

2.1 Information

The most straightforward approach to make consumers save energy is to inform them about energy consumption. Such consumer information often comes in brochures, flyers and is typically provided by the energy suppliers, the authorities or some other institution that either wants to gain reputation or just has financial benefits from that information campaign. Providing general information is by far the easiest and cheapest method to reach better energy saving, but the impact on energy consumption is known to be very little [10, 2, 9, 14]. It turns out, that users are basically not able or willingly enough to transform the received information into practice. General information seems to have a lack of some basic principles of human behaviour: Mainly it is missing *Motivation*[9, 14] and *Feedback*[19].

An example from [2] demonstrates this fact. In 2009, all fast-food restaurants in New York City were forced to label their menus with calorie-count information. The desired effect – reducing obesity rates – did not arise.

However, there are several ways to improve the results of information about energy saving. One critical parameter is time. If information is given frequently, the user will tendentiously be more motivated to deal with the proposals [9, 19] and thus it is more likely that the information really reaches the recipient.

Other projects make use of target-group-specific mediators like students or children, that were trained as *Energy advisers*. They should take advantage of the affinity to their audience, to help imparting the knowledge about energy saving.

2.2 User specific Feedback and Smart-meters

Households differ in many ways, therefore providing universal energy-saving advice is a difficult task. Quite better results can be obtained by giving user-specific feedback concerning the amount and time of consumed energy. By identifying the user's individual consumption, most power-eating devices and power-wasting habits, the feedback generation is able to adapt exactly to the needs of the consumer. At the same time, feedback helps to direct the consumers attention towards *specific goals* [14] and has the potential to ensure *long-term motivation*.

There are various types of energy feedback generation. A simple form of feedback is the energy bill, that every consumer receives regularly. Typically, it states the used amount of energy since the last bill. Feedback with energy bills is quite easy to implement, and that's why it has to be considered, although it is not the best method for long-term motivation. Here, the quality of feedback mainly depends on the time interval the bills are sent in, the visualisation of the numbers and a comparison or ranking that allows the people to get an idea about their consumption status [9, 12].

More precise feedback can be achieved with the help of *Smart-meter* measurements. A Smart-meter normally replaces the old power meter at the consumers house, and then constantly records the energy consumption level over time, ranging from 15-minutes intervals over 1-hour intervals up to daily consumption reports. Smart-meters differ

doi: 10.2313/NET-2014-03-1_10

in the way they publish collected information. The original Smart-meters were designed to inform the power suppliers about the current load of their customers. From that data, they are able to forecast peak-load times and to maintain the grids efficiency and stability. Unfortunately, this centralized approach led to a perception of Smart-meters as a form of supervising, user-controlling system [1].
This impression from the users influenced the technology to make the information also available for the consumers. Most of these systems just allow the consumer to login to a web-portal, where they can browse through their latest energy consumption history, and some of the systems even give hints and tips for smarter energy usage or show the environmental impact.
A key point for good Smart-meters is the detection of *device-specific consumption*, and thus providing a detailed view about the households energy profile. There exist new algorithms that allow the user to train his Smart-meter for a certain device, just by pressing a train button and then switching the device on and off. The device signatures that are extracted like that, can then be used for improving the feedback information, or it can be uploaded and aggregated in comparison databases, so that Smart-meters are able to estimate, which device was powered on, even without training from its user [19]. Several projects go the other way round, they include tiny Smart-meters in every device, either sending the consumption values to the central Smart-meter, or displaying it directly on the device.
Especially the last approach seems to quite successful, as it gives information to the user in the exact moment, when he uses the device and thus has the potential to change following actions: "Oh, the heater used so much? Mhh, I should turn it down now...".

Despite all advantages of Smart-meters there are also some downsides. First, the mentioned privacy and security issue. Secondly, many Smart-meters use their proprietary interfaces, which decrease interoperability. Then, users have to accept the received feedback and turn it into practice. Anyway, the long-term motivation of users seems to be the hardest point to achieve. For example, a German field experiment found out, that after two month of web-based feedback, only about 5% of test-consumers still seriously used the webportal. We will see some of the assumed reasons for that in the next chapters.
One last drawback is the acquisition costs for Smart-meters, that are not easy to amortize by energy-saving. The range of achieved energy savings with feedback information goes from negative savings – more on that later – to usually 5% to 10%, in rare cases up to 20% [9, 12, 14]. This percentages will often not be enough to compensate the price of modern Smart-meters.

2.3 Motivation from interactive comparison and competition

Informing the user and giving feedback is only the first step towards reasonable energy saving.
Behavioural experts see information as the base layer of a behavioural model, which leads to consciousness about a problem or individual possibilities. The second stage is formed by implicit and explicit comparisons. The implicit comparisons are made by *social and personal norms*, whereas the explicit comparisons are based on hard facts like the energy bill, historical consumption feedback or comparisons between users (See [9, 14]).
We already found out, that *setting energy-saving goals* is one of the key points to achieve good energy savings. Therefore, the main focus should go to *comparable feedback information*, that clearly shows the consumer, how his energy footprint performs compared to other users/households with different appliances and usage strategies. After receiving optimal feedback, the consumer will then develop self-set improvement goals, thus directing more attention to the respective tasks [14].
For the formation of this goals, the social environment and its interactive component is often underestimated. If a consumer is confronted personally with a low conservation goal, he is more likely to accept higher goals afterwards. This method is called the "foot-in-the-door technique" and can be used for raising better energy saving goals, especially for an effective introduction to energy saving [14].

At the same time, it is also highly important to keep *long term motivation*, for example by providing interactive elements and decision points. The most obvious method is to promote competition between consumers. "*Gamification*" of energy saving among friends has great potential to motivate consumers and to get them interested in energy saving. Games can also be used for training environmental and energy-aware behaviours, as they provide both interactive and motivating concepts [16, 1, 19].

There had been several projects with collaborative and interactive energy-feedback systems. "PowerPedia" is one example for a social, energy-profile sharing Smartphone application. Users can measure their devices in realtime, and compare them either with devices from a community-driven online database, or just with friends over social networks [19]. The integration of energy feedback in *existing systems* (smartphones, social networks, etc.) is a necessary task, because users should keep *regular contact* with their energy reports, so that they can react on occurring changes immediately. Considering all these advantages, knowledge transfer from the games industry to the energy saving field is imaginable and highly recommended.

2.4 Price-driven energy saving

According to the economic principle of demand and price, high energy prices should also decrease energy consumption. So the assumption is, if energy becomes less affordable, consumers will automatically try to save energy.
A short look on the facts reveals a price increase for German Electrical Energy from €16.65/kWh in 2000 to about €25.14/kWh in 2012 (+51%), that was mainly influenced from the German *EEG reallocation charge* [8]. For exact the same period of time, the consumed energy has also risen from 1780 PJoule (2000) to 1869 PJoule (2012) (+5%) [5]. Assuming unchanged technological conditions, this may suggest, that consumers are not fast enough to adopt to changing energy prices by reducing consumption.

The same conclusion comes from a Swiss study, aiming at the *price elasticity* of households [17]. It states a very low and slow reaction to rising electricity prices, mainly caused by insufficient consumer knowledge on how to save energy.

doi: 10.2313/NET-2014-03-1_10

But who knows, perhaps one day, the continuing increase of the *EEG reallocation charge* may have a positive impact on energy conservation.

2.5 Taking control of user decisions

Sometimes, feedback information or even high energy prices may not be enough to trigger ecological-friendly behaviour. Due to the overwhelming complexity of modern systems, it is difficult for the consumers to identify the right decisions at the right time, only based on the abstract information they get. The field of decision consumers have to deal with, ranges from buying-decisions in the markets down to setting their washing machine temperature. There exist situations, where consumers need the help of an advisor or *decision maker*.

For Smart-meters, the decision maker is a device connected to the user's *Smart Meter Gateway*. It is controlled by the *Smart Meter Gateway Administrator* (mainly the energy grid operators), and can cut the power in case of power shortage or when the user consumed energy far over normal level. In such cases, the consumer is first informed about the situation in order to reduce the current load. If no action follows, the Smart Meter Gateway will partially shut down energy lines [3, 1]. In reality, however, these smart decision makers are still rare and only tested among industrial consumers.

But the concept of influencing consumer decisions is promising in various ways. It is fact, that several fast decisions in tiny moments can have a major influence on our energetic footprint. If we manage to identify these "crucial moments" [2], and provide "decision helpers" for them, we can avoid massive energy consumption. The article from Dan Ariely and Aline Grüneisen [2] proposes to use children to effectively train their parents behaviour towards environmental-friendly decisions, like buying energy-efficient lamps instead of conventional light bulbs.

In 2009, the European Union pioneered the "control-driven energy saving" by imposing legal prohibition on inefficient light bulbs. The consumers reacted with rage and some of them found clever ways to circumvent the ban, for example by selling "small heating devices" that look like light bulbs, but are officially used for heating.

A more encouraging approach comes from user experiments with the so called *anchoring bias*. The assumption is, that consumers are highly influenced by predefined default parameters, when using their appliances or making decisions. Researchers figured out a low-level cognitive link between consumers decisions and the decisions of their environment, so that they unconsciously try to orientate their choices on existing decision results [14].
For the industry, that implies a conscientious adjustment of default settings for energy-consuming devices, because consumers will mostly trust the parameters predefined by the manufacturers. In return, companies that do not care on reasonable energy-presets, should be outlawed by society.
A good *negative example* to study, is the new generation of gaming consoles *Playstation 4* and *Xbox One*. They both implement the new EuP-energy-saving standard, that demands a standby consumption under 1Watt, but in fact, neither Sony or Microsoft enable it by default. Despite that, the *Xbox One* has a default standby consumption of 19 Watt and *Playstation 4* draws 6 Watt. Not enough, both manufacturers prevent the users to enable the real energy-saving mode by extremely long loading times and inconvenient handling [7].

3. MAIN REASONS FOR PROBLEMS IN ENERGY SAVING

As presented so far, there is a lot of effort to reduce energy consumption. Technological progress allows the development of smart energy saving systems and maximizes the effective output of appliances. However, energy saving is not only achieved by technology (*hard energy-saving factors*), but also by the users behaviour and lifestyle (*soft energy-saving factors*) [10]. For the *soft* factors it is important to know both sides that influence consumers: the reinforcing strategies and also the points that discourage users to save energy. In the following, we look at some of the effects counteracting energy conservation.

3.1 Personal comfort: Habits and Routines

Typical consumers have no time to think about energy. They are stuck in *daily business* and their *routines*, and are simply not aware of any *energetic problem*. Other problems seem to be more important, and so there is little to no effort made for energy saving.
Some users are one step further, they already *identified* potential *energy saving spots*, but they are lacking the required knowledge how to save. At this point, even if consumers acquired the needed *knowledge about energy conservation*, many have *fears* turning it into practice [10].
For example, choosing a smaller and more economical car is a commendable step towards climate protection, but many consumers like their car as sort of a status symbol and hence would never go without it. Here, anxieties come from apprehended *restrictions* and from fears towards *social isolation* caused by reduced lifestyle [10].
Another barrier, that has negative influence on energy saving, are the still too low energy prices. Taking some citizen's Christmas illumination as an example, it seems, that *wasting energy is still affordable and tolerated by society*. If energy prices were higher, or perhaps coupled to usage scenarios, there would be more motivation from consumers point of view to save energy. There exists no real consequences for irresponsible energy use, despite the pure energy costs, which are nonetheless affordable by *wealthy energy wasters*.

For all that reasons, it seems especially important to have some sort of energy saving pioneers (In [18], they are called *sociometric stars*), that act as role models for consumers and help them to overcome their passive behaviour. Users should be given reasons, why it is exactly them, that have to save energy. At the same time, irresponsible usages of energy should be denounced more heavily in public.

3.2 Influence from Industry and Advertisement

Today's consumers live in a commercialized world, that is dominated by a huge number of profit-orientated companies. These companies – and in particular the corresponding

doi: 10.2313/NET-2014-03-1_10

Figure 6: Forces against Behavioural change for energy saving (cf. [10])

marketing departments – have the goal to promote and sell their products, regardless of the energetic impact for customers. Compared to the number of marketing employees, environmentalists are largely outnumbered with their efforts to show energy-efficient living.
We in the role of customers are already used to the "shiny" products from the industry, and let them influence our decisions what to buy or to use. For example, a producer of electrical-powered heaters advertises his products as cheap and simple to use. Attracted by the advertising promises, consumers buy the heater with the aim to get a cheap and fast heating. Later, it turns out, that the manufacturer of the heater concealed the high energy consumption and costs, just to achieve larger sales.
The omnipresent manipulation from the industry makes it difficult for consumers to adopt to energy-friendly behaviours. It demands much endurance and a strong-minded behaviour to resist against all the attractions that economy provides with its markets.

3.3 Unclear return on investment for energy-saving

Effort for energy saving technologies is also dependant on economical circumstances. In 2012, the European Union appealed for a 80%-deployment of Smart-meters until 2020, under reserve, that the overall result is positive. Therefore, a call for studies to evaluate the benefits of Smart-meters was raised. For that, every country investigated the economic potential along with deployment and other issues. Austria for example concluded a positive outcome, they calculated the total required investment to about €4.4 billion, linked to a energy saving worth €5 billion (29.6 TWh) for 2011 to 2017. Surprisingly, Germany predicts a negative outcome. Here, they estimate the investment to €21 billion, with only €6.4 billion as efficiency gain between 2014 and 2022 [15, 3, 11].
Again, the decision for – or against – a specific energy-saving technology *depends on the information we have* about it. Here, the Austrians decided to invest in the broad deployment of Smart-meters, whereas the Germans will first introduce Smart-meters for large-scale consumers with over 6000 kWh per year.
Regrettably, choices are generally not only made by rational thoughts. Instead, choices are mostly based on very limited, estimated or even wrong facts [18]. For the domestic energy consumption this typically includes the *monthly bill* (made from interpolated values), *remembered usage history* and *personal perception* of the energetic environment.
All in all, economists regard analyses on energy use as a hard problem, because it is influenced by various determinants like consumer *behaviour*, *technology* and energy *pricing* [18].

3.4 Underestimated Rebound Effects

By far the most undesirable effect that counteracts energy saving, is the so called *Rebound Effect*. The Rebound Effect describes the behaviour of consumers, who overreact after a successful energy-saving change: With the first operation of a new saving technology, consuming energy may become cheaper or easier, resulting in more extensive use than before. If the additional consumption eats up the saved energy benefit, it causes the *Rebound Effect*.
The classical example is the deployment of a new central heating, replacing de-central heaters. Heating rooms is now simplified, and therefore more rooms are being heated, which can lead to even higher energy use than before [10].

4. STEPS TOWARDS BETTER ENERGY USAGE

To understand, how and why people are saving energy, you have to look at different aspects simultaneously. First, an evaluation of the current situation has to be established, by creating *significant energy consumption statistics* in the desired energy-sector and gaining an insight to *user's habits and life*.
From that stage, ideas can be developed, how to guide consumers to better energy usage, for example with *personal feedback* or *interactive methods*. *Behavioral science* tells us some principle aspects like *long-term-motivation*, *goal-setting* or *anchoring bias*, that always have to be considered when thinking about user-involved processes. The potential coming from gaming and social comparisons also seems particularly promising here, but it needs to integrate seamlessly into the life of consumers.

Creating energy saving plans is also *highly complex*, and identifying concepts, that have *positive benefit and low costs at the same time*, is not easy. Especially *several industries* and *markets* are hard opponents to efficient energy use, because they often manage to interfere energy perception or long term energy plans.

It also turned out, that many decisions for energy-related topics are made using *wrong information*, *inaccurate estimation* or *vague perception*, resulting in *undesired symptoms* like the Rebound Effect. Sometimes it may even be useful, to *take control over consumer decisions*, simply to prevent irresponsible energy wasting.

doi: 10.2313/NET-2014-03-1_10

5. REFERENCES

[1] A. Bourazeri, J. Pitt, P. Almajano, I. Rodriguez, and M. Lopez-Sanchez. Meet the Meter: Visualising SmartGrids using Self-Organising Electronic Institutions and Serious Games. In *2012 IEEE SIXTH INTERNATIONAL CONFERENCE ON SELF-ADAPTIVE AND SELF-ORGANIZING SYSTEMS WORKSHOPS (SASOW)*, pages 145–150

[2] A. G. Dan Ariely. How to turn consumers green. Online, March 2013.

[3] B. der Energie-und Wasserwirtschaft e.V. (Im Auftrag des BMWI). Kosten-Nutzen-Analyse für einen flächendeckenden Einsatz intelligenter Zähler. Online, http://www.bmwi.de/DE/Mediathek/publikationen did=586064.html, 2013.

[4] N. EnergieAgentur. Erhebung „Wo im Haushalt bleibt der Strom?“. *Anteile, Verbrauchswerte und Kosten von*, 12:–, 2011.

[5] A. Energiebilanzen eV. Auswertungstabellen zur Energiebilanz für die Bundesrepublik Deutschland 1990 bis 2012, 2013.

[6] A. Energiebilanzen eV. Endenergieverbrauch in privaten Haushalten nach Energieträgern und Anwendungsbereichen, 2013.

[7] N. Ernst. Stromverschwender im Wohnzimmer. online, November 2013.

[8] K. N. et al. Steigende EEG-Umlage: Unerwünschte Verteilungseffekte können vermindert werden. *DIW WochenberIcht*, 41:–, 2012 / 79. Jahrgang.

[9] C. Fischer. Influencing electricity consumption via consumer feedback: a review of experience. *ECEEE 2007 Summer Study Proceedings*, -:1873–1884, 2007.

[10] S. Z. A. für Hochbauten. Schlussbericht Nutzerverhalten beim Wohnen. Analyse, Relevanz und Potenzial von Massnahmen zur Reduktion des Energieverbrauchs (Effizienz und Suffizienz), Juni 2011.

[11] F. Greis. Intelligente Stromzähler, Rasen mähen bei vollmond. online, November 2013.

[12] Intelliekon. Nachhaltiger Energiekonsum von Eaushalten durch intelligente Zähler-, Kommunikations- und Tarifsysteme. Ergebnisbericht – November 2011. Fraunhofer Institut für Solare Energiesysteme ISE Heidenhofstrasse 2, 79110 Freiburg, 2011.

[13] B. Lannoo, S. Lambert, W. V. Heddeghem, M. Pickavet, F. Kuipers, G. Koutitas, H. Niavis, M. T. Beck, A. Fischer, H. de Meer, P. Alcock, T. Papaioannou, N. H. Viet, T. Plagemann, and J. Aracil. Overview of ICT Energy Consumption. In *Deliverable D8.1.*, 02/2013 2013.

[14] L. McCalley. From motivation and cognition theories to everyday applications and back again: the case of product-integrated information and feedback. *ENERGY POLICY*, 34(2):129–137, JAN 2006.

[15] PricewaterhouseCoopers Österreich. Studie zur Analyse der Kosten-Nutzen einer österreichweiten einführung von Smart Metering, 2010.

[16] M.-O. Pahl, H. Niedermayer, H. Kinkelin, and G. Carle. Enabling sustainable smart neighborhoods. In *3rd IFIP Conference on Sustainable Internet and ICT for Sustainability 2013 (SustainIT 2013)*, Palermo, Italy, Oct. 2013.

[17] B. Simmons-Süer, E. Atukeren, and C. Busch. Elastizitäten und Substitutionsmöglichkeiten der Elektrizitätsnachfrage: Literaturübersicht mit besonderem Fokus auf den Schweizer Strommarkt ; Studie im Auftrag der Economiesuisse. KOF Studien 26, KOF, Zürich, 2011.

[18] P. C. Stern. Blind spots in policy analysis: What economics doesn't say about energy use. *Journal of Policy Analysis and Management*, 5(2):200–227, 1986.

[19] M. Weiss, T. Staake et al. PowerPedia: changing energy usage with the help of a community-based smartphone application. *PERSONAL AND UBIQUITOUS COMPUTING*, 16(6):655–664, AUG 2012.

Policy-Beschreibungssprachen - Survey

Norbert Schmidbartl
Betreuer: Nadine Herold, M.Sc. Dipl.-Inf. Stephan Posselt
Seminar Innovative Internettechnologien und Mobilkommunikation WS1314
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: schmidba@in.tum.de

Kurzfassung

Um Abweichungen von einem gewünschten Systemzustand zu erkennen, können Monitore, zum Beispiel in Rechnernetzen, für Überwachungszwecke eingesetzt werden. Eine wichtige Frage, die sich bei der Verwendung dieser Monitore stellt, ist, wie mit Alarmen sinnvoll umgegangen werden kann. Speziell zur Lösung dieser Problemstellung eignet sich der Einsatz verschiedener Policy-Beschreibungssprachen, mithilfe derer man Bedingungen für Ereignisse (Alarmmeldungen) definieren kann, die dann automatisiert bestimmte Aktionen auslösen können. Dieses Paper beschäftigt sich mit dem Aufbau und der Eignung verschiedener Policy-Systeme und -Sprachen, beleuchtet Vor- und Nachteile, und vergleicht die Mächtigkeit dieser Sprachen. Es werden zudem aktuelle Lösungsansätze und Ideen vorgestellt, die sich mit möglichen Optimierungen der bestehenden Systeme beschäftigen.

Schlüsselworte

Policy, IDS, Monitor, Beschreibungssprache, Trigger

1. Einleitung

Um die Sicherheit und den reibungslosen Ablauf moderner IT-Systeme gewährleisten zu können, werden heutzutage in vielen Szenarien Intrusion-Detection-Systeme (IDS) und andere Monitore eingesetzt. Sobald eine Abweichung von einem gewünschten Systemzustand auftritt, wird eine entsprechende Meldung bzw. Alarm ausgegeben. Dadurch können unter Umständen sehr viele Meldungen generiert werden. Der Einsatz von Policy-Systemen hilft, angemessen, schnell und präzise auf diese Daten reagieren zu können. Im Vordergrund steht als Motivation eine weitgehende Automatisierung bestehender Vorgänge. Um dies zu ermöglichen, sollten bestimmte Rahmenbedingungen durch die Policy-Systeme erfüllt werden: Die genauen Umstände des Alarms sollten festgestellt werden können, und es sollte automatisiert eine Auswahl an adäquaten Reaktionen getroffen werden. Policies können demzufolge als Richtlinien betrachtet werden, nach denen automatisch geeignete Verhaltensweisen eines Systems ausgewählt werden. [2]

Die verschiedenen Policy-Sprachen unterscheiden sich in ihrer Struktur und Konzeption, weshalb sich die Frage stellt, in welchen Punkten die jeweiligen Beschreibungssprachen in Bezug auf Mächtigkeit und Eignung für IDS und andere Monitore Vorteile aufweisen können. Policy-Beschreibungssprachen sind ein mächtiges Werkzeug, mit deren Hilfe Aufgabenstellungen, die ansonsten manuell bearbeitet werden müssten, einheitlich, schnell und autonom gelöst werden können. Richtlinien und Bedingungen, die den Zustand des Gesamtsystems betreffen, sollten immer eingehalten werden. Es sollte eine Beschreibungssprache gefunden werden, die diese Einschränkungen beachtet, aber trotzdem mächtig genug ist, um damit flexible Richtlinien definieren zu können. Wichtige Eigenschaften, die eine Policy-Beschreibungssprache unterstützen sollte, sind somit [10]:

1. Konsistenz: Die Policies, die für ein System geschrieben wurden, sollten nicht in sich selbst (und anderen Policies gegenüber) widersprüchlich sein.
2. Präzision: Die Richtlinien, die durch die Policies ausgedrückt werden, sollten klar formuliert und eindeutig sein, also nur eine Interpretation zulassen.
3. Kompatibilität: Die Policies müssen mit den Eigenschaften und Funktionalitäten des Systems, für das sie geschrieben wurden, harmonieren.
4. intuitive Verwendbarkeit: die Policies sollten benutzerfreundlich und möglichst einfach verwaltet werden können.

Policie-Sprachen lassen sich zudem grundsätzlich zwei Kategorien (Level) zuordnen: Der Kategorie der Low-Level-Policies, die sich durch eine maschinelle Interpretier- und Verwendbarkeit auszeichnen, und der Kategorie der High-Level-Policies, die sich am intuitiven Verständnis der Menschen orientieren. High-Level-Policies können durch den Einsatz von Low-Level-Policies in Policy-Systemarchitekturen realisiert werden. Das Policy Management Tool kann zudem High-Level-Policies, die für Menschen leicht verständlich sind, in Low-Level-Policies übersetzen, die wiederum für die Verarbeitung durch Computer optimiert sind. [10]

Die folgenden Kapitel geben einen Überblick über bestehende Policy-Systeme und -Sprachen, und zeigen Einsatzmöglichkeiten, neue Entwicklungen sowie Lösungsansätze auf.

2. Policy-Systeme im Überblick

Um den konkreten Einsatz und den Nutzen von Policy-Beschreibungssprachen besser verstehen zu können, ist es wichtig, ein prinzipielles Verständnis dafür zu entwickeln, wie moderne Policy-Systeme aufgebaut sind, wie sich ein typischer Workflow in solch einer Umgebung gestaltet kann, und wie mithilfe dieser Policy-Systeme auf bestimmte Typen von Ereignissen angemessen reagiert werden kann. In den folgenden Kapiteln werden diese Fragestellungen näher beleuchtet.

doi: 10.2313/NET-2014-03-1_11

2.1 Policy-Architekturen

Es existieren mittlerweile Standards, an denen sich moderne Policy-Architekturen orientieren sollten. Einige dieser Vorgaben stammen von der IETF (Internet Engineering Task Force), die in den RFCs (Request for Comments) 2748 und 2753 näher beschrieben werden [10]. Ein Policy-System besteht demnach grundsätzlich aus vier Einheiten: den Policy Enforcement Points (PEP), einem Policy Decision Point (PDP), einem Policy Management Tool sowie aus mindestens einem Policy Repository (PR) [1]. Wie die einzelnen Komponenten zueinander in Relation stehen, kann Abbildung 1 entnommen werden.

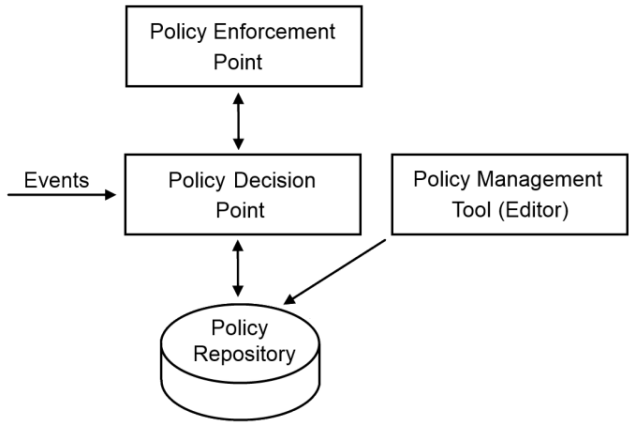


Abbildung 1. Policy Systemarchitektur (IETF) [1][2][10]

Die Komponenten übernehmen folgende Aufgaben [13]:

1. Policy Decision Point (PDP): Der PDP interpretiert die in den PRs gespeicherten Policies und schickt passende Instruktionen an den PEP.
2. Policy Enforcement Point (PEP): Der PEP führt die Anweisungen des PDP aus. Jedes Gerät des Systems besitzt einen eigenen PEP, dem genau ein PDP zugeordnet ist. In den Policies muss somit spezifiziert sein, welcher PEP zuständig ist.
3. Policy Management Tool: Administratoren können dieses Werkzeug nutzen, um Policies in das System einzupflegen. Das Policy Management Tool stellt somit eine Schnittstelle zwischen dem PR, in dem Policies gespeichert werden, und den Administratoren dar. Es existieren Policy Management Tools, die von Menschen generierte, leicht lesbare High-Level-Policies in maschinenlesbare Low-Level-Policies übersetzen können.
4. Policy Repository (PR): im PR werden alle Policies, die vom Policy Management Tool erzeugt werden, gespeichert. Sie können bei Bedarf vom PDP abgerufen werden.

Die Grundkomponenten der Policy-Systemarchitektur können für die Kommunikation untereinander unterschiedliche Protokolle verwenden, wie z.B. COPS, SNMP, HTTP oder telnet. Für die Kommunikation mit dem PR ist das LDAP-Protokoll (Lightweight Directory Access Protocol) ein weit verbreiteter Standard [2]. Die später vorgestellten Policy-Sprachen verwenden in ihren Implementierungen ähnliche Architekturen, in denen sich Einheiten analog zu den hier vorgestellten Komponenten finden lassen.

2.2 Workflow und mögliche Szenarien

Ein typischer Ablauf innerhalb eines Rechnernetzwerks kann sich beispielsweise wie folgt gestalten: Ein IDS oder ein anderer Monitor löst einen Alarm aus. Dies erfolgt, sobald ein verdächtiges Verhalten oder ein fehlerhafter Zustand festgestellt wurde. Durch statische Analysen, der Verwendung von Filtern und bekannten Angriffssignaturen sowie heuristischen Methoden können solche Angriffe und Fehlerzustände erkannt und anschließend gemeldet werden. Wie solch ein Alarm im Detail kommuniziert werden kann, unterscheidet sich von System zu System. Eine Meldung kann direkt, zum Beispiel per E-Mail, an einen Administrator geschickt werden, es kann aber auch ein Policy-System angesprochen werden, das anhand von gespeicherten Richtlinien automatisch entscheidet, wie weiter vorgegangen werden soll. Abbildung 2 soll die Zusammenhänge zwischen den einzelnen Komponenten veranschaulichen. [12]

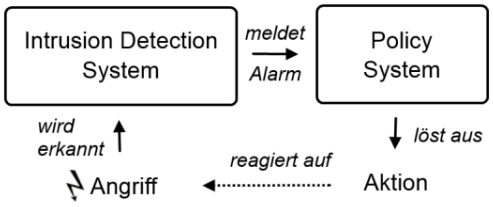


Abbildung 2. Typisches Szenario – Workflow

2.3 Umgang mit Alarmen

Sobald ein Ereignis einem Policy-System gemeldet wurde, sollten die vorhandenen Richtlinien automatisch eine geeignete Reaktion definieren, falls bestimmte Bedingungen hierfür erfüllt sind. In diesem Zusammenhang ist es wichtig zu wissen, dass IDS mit einer gewissen Wahrscheinlichkeit „false-positives“ (Fehlalarme) liefern können, also eine Meldung nicht unbedingt auf einem tatsächlichen Fehlerzustand oder Angriff beruhen muss. Das Policy-System kann nur dann optimal auf solche Fehlalarme reagieren, falls die genauen Umstände des Alarms dem Policy-System bekannt sind. Wichtige System– und Umgebungsvariablen sollten deshalb von den Policy-Systemen abrufbar sein, und es sollten die für die Meldung zuständigen Stellen, also Personen (Administratoren) oder Security Systeme, situationsbedingt ausgewählt und automatisch benachrichtigt werden können. Trotzdem sollte Wert darauf gelegt werden, dass die Privatheit sensibler Daten gewährleistet bleibt, und nicht beispielsweise durch das Einschleusen fehlerhafter Policies sensible Sicherheitslücken (z.B. durch fälschlicherweise geöffnete Ports) entstehen. Ein Policy-System, das komplett auf den Zugriff auf System- und Umgebungsvariablen verzichtet, kann jedoch nur sehr eingeschränkt und oberflächlich auf Angriffe reagieren. Bei der näheren Beschreibung und Beurteilung der in diesem Paper vorgestellten Policy-Beschreibungssprachen wird deshalb darauf geachtet, wie und in welchem Umfang entsprechende Systemparameter von den Policies im Bedingungsteil abgefragt werden können. [12]

2.4 Geeignete Reaktionen

Bestimmte Ereignisse können dazu führen, dass Policies, die im PR gespeichert sind, vom PDP und PEP ausgewertet werden.

doi: 10.2313/NET-2014-03-1_11

Diese Art von Ereignis wird nachfolgend als „Trigger“ bezeichnet. Das Ereignis, das die Auswertung anstößt, sollte in den Richtlinien klar definiert werden. Nachdem ein Trigger-Ereignis die Auswertung einer Policy angestoßen hat, und der Bedingungsteil erfüllt wird, sollte die automatische Ausführung einer Aktion erfolgen. Zu diesem Zeitpunkt wird davon ausgegangen, dass kein Fehlalarm vorliegt. Es sollte exakt auf den Fehlerzustand und eine mögliche Bedrohung reagiert werden. So können beispielsweise betroffene Verbindungen unterbrochen und fehlerhafte Daten geändert oder verworfen werden. Zudem könnte zum Beispiel eine angeschlossene Firewall den Umstanden entsprechend konfiguriert werden. In vielen Fällen ist es sinnvoll, den zuständigen Administrator über den eigentlichen Vorfall zu informieren, falls eine automatische Korrektur fehlschlägt, oder das Problem nicht komplett beseitigt werden konnte. [12]

3. Einordnung und Analyse verschiedener Policy-Sprachen

Nicht alle Policy-Beschreibungssprachen eignen sich für den Einsatz in den vorgestellten Szenarien. So sind die Ereignisse, die die Auswertung einer Policy anstoßen, teilweise vordefiniert und somit nicht flexibel genug. Zwingende Voraussetzung ist, dass falls ein Ereignisse (Trigger) eintritt, ein dazugehöriger Bedingungsteil der Policy zuverlässig ausgewertet wird. Die Policy-Systeme sollten verbindlich und umgehend auf Meldungen (Ereignisse) des IDS reagieren. Dies ist bei einigen Policy-Spezifikationen nicht möglich. [1]

Auf eine Gruppe von Policy-Sprachen, die diese Voraussetzungen größtenteils nicht vollständig erfüllen können, aber trotzdem im IDS- und Monitor-Umfeld Anwendungsgebiete als Ergänzung finden können (zum Beispiel im Bedingungsteil), sei an dieser Stelle hingewiesen: Es handelt sich um die sogenannten Traffic-Flow-Policy-Sprachen, die mittels Pattern-Matching beliebige Datenströme auswerten können. Beispiele hierfür wären SLR, PAX-PDL sowie PDL. [11]

Eine der verbreitetsten XML-Policy-Sprachen, XACML, kann nur auf eine bestimmte Art von Events reagieren, nämlich Zugriffsversuche, und ist für unser Szenario nicht geeignet. Entsprechende Erweiterungen sind denkbar, im Moment existieren aber dazu noch keine Implementierungen. [11]

In den nachfolgenden Kapiteln beschäftigt sich dieses Paper ausschließlich mit Policy-Beschreibungssprachen, die sich bei den vorgestellten Szenarien als Policy-Instanz einsetzen lassen.

3.1 Wichtige Kriterien und Eigenschaften

Geeignete Policies weisen im Allgemeinen einige gemeinsame Eigenschaften auf. Jedes der Systeme muss sich mit den folgenden Entitäten auseinandersetzen, um eine automatisierte Bearbeitung eingehender Alarme gewährleisten zu können. [1]

1. Ereignisse (Events) führen zur Auswertung bestimmter Policies. Systemänderungen wie zum Beispiel IDS-Alarme sowie Benutzereingaben können solche Trigger darstellen. Die Ereignis-Definitionen können meist kombiniert, negiert sowie chronologisch gereiht werden. Die separate Definition von Ereignissen dient der Optimierung, kann aber prinzipiell auch innerhalb des Bedingungsteils erfolgen.
2. Bedingungen (Conditions): Tritt ein Ereignis ein, werden Bedingungen ausgewertet, die an den Systemzustand und diversen Umgebungsvariablen gerichtet sein können. Die Auswertung des Bedingungsteils liefert meist die booleschen Werte „true“ oder „false“ zurück.
3. Aktionen (Actions): Ist die Bedingung erfüllt („true“), wird mindestens eine Aktion, die den Systemzustand ändert, automatisch ausgeführt.

Das Event-Condition-Action-Pattern (ECA) kann, wie in Abbildung 3 verbildlicht, in Kurzform folgendermaßen beschrieben werden:

ON (Event) IF (Condition) THEN (Action)

Eine weitere Grundstruktur vieler Policies sieht zudem wie folgt aus[1]:

IF (Condition) THEN (Action)

ECA stellt eine Optimierung dar: die Trigger (Ereignisse), die die Auswertung des Bedingungsteils (Condition) bewirken, können separat definiert werden. Der Bedingungsteil wird, im Vergleich zum IF-THEN-Pattern, erst dann ausgewertet, falls solch ein Ereignis tatsächlich eintritt, wodurch System-Ressourcen eingespart werden können [1]. Es sollte darauf geachtet werden, dass Ereignisse und Bedingungen trotzdem flexibel genug im ECA-Pattern definiert werden können, und mögliche Einschränkungen aufgrund der Event-Condition-Aufteilung nicht benötigte Funktionalitäten beeinträchtigen.

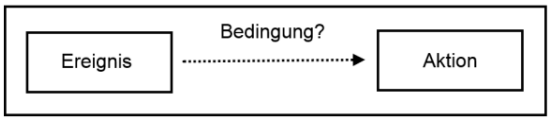


Abbildung 3: Event-Condition-Action

Im Gegensatz dazu muss bei der Verwendung einer IF-THEN-Struktur das Ereignis, dass die Ausführungen der Aktion auslöst, innerhalb des Bedingungsteils definiert werden. Es stellt sich somit die Frage, wann solch eine Policy ausgewertet werden soll. Einige Policy-Sprachen sehen eine Auswertung der Policies nur vor, falls ein ganz bestimmter Typ von Ereignis eintritt. Das wäre für den genannten Anwendungsfall zu unflexibel. Zudem wäre es möglich, bei jedem Ereignis die Conditions aller gespeicherter Policies auszuwerten, was gegenüber ECA bei umfangreichen Bedingungsteilen rechenaufwändiger wäre. Der Bedingungsteil der IF-THEN-Policies kann zudem standardmäßig in bestimmten Zeitintervallen ausgewertet werden, wodurch ein Zugriff auf alle Policies nicht mehr bei jedem einzelnen Event nötig ist, sondern die Menge aller zwischenzeitlich eingetretenen Events auf einmal geprüft werden kann. Dies erlaubt aber weder eine asynchrone Verarbeitung der Alarme, noch stellt es eine optimale Nutzung der vorhandenen Systemressourcen dar. Allerdings sind sowohl die ECA-Struktur als auch das IF-THEN-Pattern prinzipiell für die hier vorgestellten Szenarien geeignet, falls die Ereignisse mithilfe der Beschreibungssprache flexibel genug definiert werden können. [1]

Ein weiteres Kriterium, das die Verwendbarkeit von Policy-Beschreibungssprachen stark beeinflusst, ist die Flexibilität und Komplexität der Grammatik. Interessant ist hierbei, wie sich bestehende Definitionen kombinieren lassen. Für den Bedingungsteil ist es wichtig, dass flexibel und dennoch mit der nötigen Präzision definiert werden kann, welcher Zustand zu einer

doi: 10.2313/NET-2014-03-1_11

positiven Auswertung („true“) führt. Beschreibungen sollten im Idealfall durch Aggregation, durch Negation, durch die Verwendung von Ereignissequenzen und Gruppierungen auch für komplexere Systemzustände angepasst werden können. Dadurch erhöht sich die Wiederverwendbarkeit der Policies (Modularisierung).

3.2 Vergleich verschiedener Policy-Beschreibungssprachen

Im Folgenden werden verschiedene Policy-Beschreibungssprachen näher betrachtet, Vor- und Nachteile aufgezeigt sowie ihre Eignung für IDS und andere Monitore dargestellt.

3.2.1 PONDER

PONDER ist eine deklarative, objekt-orientierte Sprache, mit deren Hilfe man in erster Linie Policies für verteilte Systeme schreiben kann. Neben der Definition von Autorisierungs-Policies ist es möglich, Ereignis-getriggerte „Obligation Policies“ zu definieren [13]. Diese Art der Policies eignet sich hervorragend für unser Szenario. Es ist zudem möglich, Policies zu gruppieren, beziehungsweise in Relation zueinander zu setzen (Composite Policies) [2]. Die Grammatik von PONDER ist in EBNF (Erweiterte Backus-Naur-Form) beschrieben, und kann jederzeit eingesehen werden. [9]

Ein Vorteil, den die Obligation-Policies von PONDER bieten, ist die ECA–Struktur, die eine präzise, ereignisabhängige Definition von Policies erlaubt [1]. Es können externe Skripte und Programmteile ohne Probleme von PONDER importiert werden, der Funktionsumfang kann somit theoretisch beliebig erweitert werden. Wichtige Systemparameter und Umgebungsvariablen können von PONDER-Policies abgefragt und verarbeitet werden. [9]

Betrachten wir nun zunächst den grundsätzlichen Aufbau einer PONDER Obligation Policy [10]:

inst	**oblig**	*Policy-Titel*”**{**”
	on	*Event-Spezifikation*;
	subject [*Typ*]	*Domäne***;**
	[**target** [*Typ*]	*Domäne***;**]
	do	*Aktionsliste***;**
	[**catch**	*Ausnahmebehandlung***;**]
	[**when**	*Bedingungsteil***;**] ”**}**”

Das ECA-Konzept wird bei PONDER durch die Schlüsselwörter

on (Event) when (Condition) do (Action)

umgesetzt. Ein weiteres wichtiges Kriterium, das PONDER erfüllt, ist, dass Ereignisse präzise beschrieben werden können. Ein Ereignis kann grundsätzlich eintreten, sobald ein Basisereignis (Trigger) dem Policy-System gemeldet wird. Zudem können Ereignisbeschreibungen durch Operatoren kombiniert werden (Tabelle 1).

Tabelle 1. Event Compositions in PONDER [9]

Operator	Erklärung (Trigger)
e1 && e2	e1 und e2 treten auf
e + t	tritt nach einer Zeitspanne t nach e auf
{e1 ;e2}!e3	e1 tritt vor e2 auf, ohne e3 dazwischen
e1 | e2	e1 tritt vor e2 auf
n * e	e tritt genau n-mal auf

Nach dem Keyword „do“ kann in PONDER entweder eine einzelne Aktion, oder eine Komposition, bestehend aus mehreren Aktionen, beschrieben werden. Aktionen können sequenziell oder nebenläufig ausgeführt werden. Eine Aktion kann in PONDER importiert werden, und ist somit sehr flexibel. [10]

Falls eine Ausnahme auftritt, kann entsprechend reagiert werden (catch). Der Bedingungsteil (when) in PONDER ist ein Ausdruck in der Object Constraint Language Version 3 (OCL), und somit mächtig genug, komplexere Bedingungen zu beschreiben. Auf die Systemzeit kann ohne die Verwendung externer Skripte zugegriffen werden. Externe Ressourcen, Methoden und Systemvariablen können in PONDER verwendet werden.

Tabelle 2. Action Compositions in PONDER [9]

Operator	Erklärung (Ausführung)
a1 -> a2	a2 muss a1 folgen (sequenziell)
a1 || a2	a1 oder a2 muss terminieren (nebenläufig)
a1 && a2	a1 und a2 müssen terminieren (nebenläufig)
a1 | a2	falls a1 nicht ausgeführt werden kann: a2

Für PONDER existieren zahlreiche Implementierungen, Management-Tools sowie Dokumentationen. Zudem ist die Struktur des Policy-Systems dem IETF-Modell, das in Kapitel 3 vorgestellt wurde, relativ ähnlich. Der LDAP-Standard kann für die Kommunikation mit dem PR genutzt werden. [10]

Alles in allem lässt sich festhalten, dass sich PONDER bei Szenarien im Umfeld von IDS oder anderen Monitoren ohne bedeutende Einschränkungen gut einsetzen lässt. Zu PONDER gibt es zudem viele Implementierungen, und das Policy-System hat sich in bereits der Praxis bewährt.

3.2.2 Ponder2

Wenn man Syntax und Funktionsumfang von Ponder2 näher betrachtet, fällt auf, dass es mit dem als Vorgänger bezeichneten PONDER nicht mehr viel gemein hat. Ponder2-Policies sind in der sogenannten PonderTalk-Sprache verfasst [14]. PonderTalk orientiert sich stark an Smalltalk, einer objektorientierten Programmiersprache. Der Umstand, dass eine vollwertige, objektorientierte Sprache als Vorbild für PonderTalk genommen wurde, verdeutlicht, dass hier größten Wert auf den Funktionsumfang und die Mächtigkeit der Sprache gelegt wurde. Es können beliebige Daten, die von den Policies genutzt werden, in PonderXML (an XML angelehnt) gespeichert und organisiert werden, worauf dann zudem XPath-Anfragen möglich sind.

doi: 10.2313/NET-2014-03-1_11

Außerdem können sogenannte „Managed Objects“ (analog zu Smalltalk-Klassen) in Java geschrieben werden, die die Grundbausteine eines Ponder2-Systems bilden und Funktionalitäten für die Policies bereitstellen. [14]

Die Policies, die für unsere Szenarien interessant sind, werden auch in Ponder2 „Obligation Policies“ genannt, und es wird wieder explizit von einem ECA-Pattern gesprochen. Es können somit Events, Conditions und Actions separat in PonderTalk definiert werden. [14]

Eine Policy in Ponder2 kann beispielsweise wie folgt aussehen [15]:

Event in Ponder2:

```
template := root/factory/event create: #( "monitor" "value" ).
root/event at: "monitor" put: template.
```

Obligation Policy in Ponder2:

```
policy := root/factory/ecapolicy create.
policy event: root/event/monitor;
       condition: [ :value | value > 100 ];
       action: [ :monitor :value |
            root print: "Monitor " +
            monitor + " has value " + value
       ];
       active: true.
```

Aus dem Beispielcode ist ersichtlich, das XPath-ahnliche Anfragen den Typ der Policy bestimmen, sowie das Ereignis definieren. Condition- und Action-Teil sind in Ponder2 in der PonderTalk-Syntax beschrieben. Die ECA – Eigenschaften der Ponder2-Richtlinien können somit in PonderXML und PonderTalk festgelegt werden. Zudem können Ponder2-Obligation-Policies aus XML-Dateien erstellt werden [15]. Durch die Verwendung von verbreiteten Standards und sehr umfangreichen Sprachen wie PonderTalk und Java sind dem Zugriff auf Systemressourcen prinzipiell wenig Grenzen gesetzt. Im Rahmen des ECA-Patterns können Ressourcen des Systems abgerufen und abgefragt werden. Allerdings ist die Kombination von Events im Vergleich zu PONDER etwas aufwändiger, es muss auf Workarounds zurückgegriffen werden. [14]

Durch die Komplexität des Systems und die vielen verwendeten Sprachen (PonderTalk, Java, PonderXML) erhöht sich allerdings der Aufwand, der insgesamt für die Verwaltung eines Ponder2-System gegenüber PONDER nötig ist. Wenn man allerdings den Funktionsumfang und Mächtigkeit betrachtet, ist Ponder2 bestens für eine Verwendung im IDS- und Monitorumfeld geeignet.

3.2.3 PDL/PPDL

Policies, die in der Policy Description Language (PDL), beziehungsweise deren Erweiterung PPDL (Preferential PDL) geschrieben sind, verwenden, ähnlich wie PONDER, die ECA-Struktur zur Formulierung ihrer Richtlinien. Die PDL-Spezifikation sieht grundsätzlich folgenden Aufbau der Policies vor[1] [3][6]:

(Event) causes (Action) if (Condition)

Eine Besonderheit von PPDL ist hierbei, dass Policies der Form

true causes (Action) if (Condition)

erlaubt sind, was die Policy auf eine simple IF-THEN-Form reduzieren würde [7]. PPDL erweitert PDL zudem um globale Richtlinien der Form

never (Action 1, Action 2, …, Action n) if (Condition)

die eine simultane Ausführung von Action 1, Action 2 , …, Action n verhindert, sobald die Bedingung (Condition) erfüllt ist. Diese Aktionen dürfen dann nach dieser Richtlinie nur sequenziell ausgeführt werden. Dies ist sinnvoll, wenn die Aktionen auf gemeinsame Ressourcen zugreifen möchten. [7]

Es wird darauf hingewiesen, dass die Auswertung einer Policy, ähnlich wie bei PONDER, auch durch eine Kombination mehrerer (Basis-)Events ausgelöst werden kann. Es wird zwischen Basisevents E und komplexen Events (E) unterschieden. Events können durch UND- (&) beziehungsweise ODER (|)- Operatoren verknüpft werden, sequentiell (E1, E2, E3, E4) oder als Wiederholung eines einzelnen Basisevents definiert werden (^E). Bedingungen bestehen aus mehreren Teilbedingungen. Diese umfassen Prädikaten, die durch gängige Operatoren in Relation gesetzt werden können (=, !=, <, <=, >, >=). [3]

Eine weitere Besonderheit von PPDL ist, dass die Auswertung von Policies, die durch Ereignisse ausgelöst werden, wiederum neue Ereignismeldungen (Trigger) auslösen können. Dies geschieht durch das Schlüsselwort „trigger“:

(Event 1) triggers (Event 2) causes (Action) if (Condition)

Die Wiederverwendbarkeit von Policies kann mithilfe solcher Konstrukte durch Modularisierung deutlich erhöht werden. [7]

PPDL kann zudem theoretisch auf beliebige Systemparameter oder primitive Systemfunktionen im Rahmen des ECA-Patterns zugreifen, womit die Umstände eines Alarms von einer PPDL-Policy jederzeit geprüft werden können. [3] [7]

Die Autoren von PDL/ PPDL gehen einen anderen Weg als die Schaffer von PONDER. Sie definieren zuerst die High-Level-Syntax von PDL/PPDL. Um dann jedoch eine maschinelle Interpretierbarkeit der Policy-Semantik zu erreichen, wird erläutert, wie eine PDL-Policy in PROLOG (Programmation en Logique) [6], beziehungsweise eine PPDL-Policy in LPOD (Logic Programs with Ordered Disjunctions) oder ASP (Answer Set Programming)- Code übersetzt werden kann [7]. Es existieren zudem Shell-Skripte, die diesen Code dann ausführen können, außerdem ist ein Übersetzer von PPDL in LPOD in Arbeit. In Zukunft soll die Präzision, sowie die Konsistenz von PDL weiter erhöht werden. [8]

Im Vergleich zu PONDER gibt es weniger ausgereifte Implementierungen, und der Funktionsumfang von PPDL ist geringer. In der Theorie jedoch ist PPDL als Policy Beschreibungssprache im Umfeld von IDS und andere Monitoren mit dem ECA-Konzept gut geeignet. [8]

3.2.4 SPL

Die Security Policy Language (SPL) wurde in der Version 3.0 zuletzt 2007 spezifiziert, ist also eine im Vergleich zu den anderen Policy-Beschreibungssprachen eine relativ junge Sprache. Dies wird deutlich, wenn man die Auszeichnungssprache betrachtet, in der SPL-Policies verfasst werden: XML. Dies kann in Hinblick auf die fortschreitende Standardisierung gewisser Richtlinien als langfristiger Vorteil gegenüber anderen Sprachen betrachtet werden. [4]

doi: 10.2313/NET-2014-03-1_11

SPL wird durch das POSITIF Framework unterstützt, und umfasst ähnlich wie PONDER eine Reihe von unterschiedlichen Policy-Typen (Authentication, Authorization, Filtering, Channel Protection sowie Operational Policies). [4]

Das XML-Format von SPL lässt eine hierarchische, standardisierte Beschreibung der einzelnen Elemente der Policy-Spezifikation zu. Es können Rollen verteilt, Privilegien vergeben und Filter-Regeln gesetzt werden, die den Netzwerk-Traffic überwachen sollen. [4]

Alle Policies der SPL enthalten folgende Eigenschaften im XML-Format: Name der Policy, Beschreibung der Policy in natürlicher Sprache, Richtlinien wie die Policy genutzt werden soll (formlos), eine Enabled-Eigenschaft, die die Policy aktiviert, und eine ValidityTimePeriod-Eigenschaft, die beschreibt, in welchem Zeitintervall die Richtlinien, die durch die Policy beschreiben werden, aktiv sind. Einmal ausgeführte Aktionen können dadurch allerdings nicht wieder automatisch rückgängig gemacht werden. [4]

Die Operational-Policies haben folgenden Aufbau:

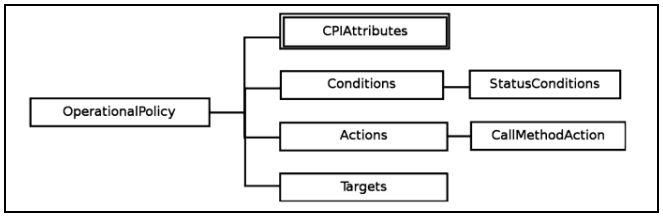


Abbildung 4. Operational Policy [4]

Die Condition-Eigenschaft beinhaltet die Bedingungen für die eigentliche Auswertung der Policy. Im Moment kann allerdings nur der Status von einem System-Element abgefragt werden. Da die Alarme theoretisch auch über ein System-Element übergeben werden können, wäre eine Verwendung in einem IDS-Szenario denkbar. Events, also Trigger lassen sich nicht explizit definieren. Das Action-Element kann eine beliebige Methode inklusive Parameter enthalten, es kann somit theoretisch jede denkbare Funktion als Aktion automatisch ausgeführt werden. Um die Policies strukturieren zu können existieren Policy Groups. [4]

SPL erweckt ähnlich wie PPDL einen etwas unfertigen Eindruck. Trotzdem ist ein Einsatz zumindest in der Theorie denkbar. Die Verwendung des XML-Formats erlaubt hierbei eine präzise, eindeutige und leicht verständliche Beschreibung diverser Richtlinien. [4]

3.2.5 CIM-SPL

Die Common Information Model Simplified Policy Language (CIM-SPL) basiert, wie die Abkürzung erkennen lässt, auf dem Common Information Model (CIM). Die DMTF Policy Working Group, die diese Spezifikation geschaffen hat, betont, dass es sich hierbei um eine

IF (Condition) THEN (Action)

Beschreibungssprache handelt. Die eigentlichen Trigger sind bei diesem Schema implizit in der Condition enthalten. [1] [5]

CIM-SPL wurde laut der DMTF Policy Working Group von PONDER sowie PDL beeinflusst. So können wie bei den Vorbildern Policies gruppiert werden. Außerdem ist eine Verschachtelung möglich. Auf diese Weise können Policy-Hierarchien aufgebaut werden. [5]

CIM-SPL verwendet wie PONDER und PPDL nicht die XML-Auszeichnungssprache. Die Grundstruktur einer Policy unter CIM-SPL sieht meist wie folgt aus [5]:

```
Policy {
  Declaration {
    <List of constant definition> (Optional)
    <List of macro definitions> (Optional)
   }
   Condition {       (Optional)
        <If Condition>
   }
   Decision {        (Required)
        <Then Decision>
   }
}: Priority
Condition {
    <Boolean Expression> (An expression that results
    in a Boolean constant after evaluation)
}
Decision {
    <action block>
}
```

Condition enthält die Bedingungen (als booleschen Ausdruck), die erfüllt sein müssen, um eine Entscheidung (Decision) zu treffen. Decision enthält die Action-Beschreibungen, die automatisch ausgeführt werden, falls die Bedingungen erüllt sind. Für die Beschreibung der Richtlinie und der Bedingungen stehen numerische, boolsche sowie relationale Operatoren zur Verfügung. Außerdem wird eine Vielzahl an Zeichenkettenoperationen nativ angeboten. Eine ganze Reihe weiterer Funktionen vereinfachen die Verwendung von CIM-SPL und erlauben die Abfrage von Systemzuständen. Bedingungen können ähnlich wie bei PONDER kombiniert werden. [5]

Es lässt sich sagen, dass CIM-SPL ein umfangreiches Spektrum an Anwendungsmöglichkeiten bietet. Die vielen Funktionalitäten, die direkt in CIM-SPL angeboten werden, und nicht erst importiert werden müssen, erhöhren die Konsitenz und die Stabilität. Die Verwendbarkeit von CIM-SPL nimmt dadurch zu. [5]

3.3 Vergleich der Mächtigkeit der Sprachen

Mithilfe der vorgestellten Sprachen lassen sich Richtlinien definieren, die präzise beschreiben, wie ein System angemessen auf einen Alarm reagieren sollte. Allerdings unterscheiden sich die Sprachen in ihrer Komplexität und Flexibilität. Einen Überblick über die Mächtigkeit der in diesem Paper vorgestellten Sprachen kann der Tabelle 3 entnommen werden. Es wird angegeben (++,+,o,-,--), wie umfangreich die Funktionalitäten der jeweiligen Sprache in den beschriebenen Bereichen (Auszeichnungssprache, ECA, Verwendbarkeit) relativ zu den anderen Beschreibungssprachen sind. Falls Implementierungen noch unvollständig, oder noch nicht vorhanden sind (Stand 2013), oder sich das System in der jetzigen Form nur mit diversen Workarounds für das IDS-Szenario eignet, ist dies durch ein „tba“ gekennzeichnet. Eine Sprache erfüllt das ECA-Kriterium nur, falls sie ausdrücklich als solche von den Autoren gekennzeichnet wurde. [1][3][4][7][11][13]

doi: 10.2313/NET-2014-03-1_11

Alle in diesem Paper vorgestellten Policy-Beschreibungssprachen lassen sich zumindest theoretisch in Verbindung mit IDS nutzen. Es bleibt festzuhalten dass sich die hier vorgestellten Sprachen teilweise stark in ihrer tatsächlichen Verwendbarkeit unterscheiden. PONDER, Ponder2 und die auf CIM aufbauenden Sprachen haben sich in der Praxis bewährt. [1]

Tabelle 3. Policy-Sprachen im Vergleich

	PON.	**Ponder2**	**PPDL**	**SPL**	**CIM-SPL**
ECA	Ja	Ja	Ja	Nein	Nein
Implementierungen	Ja	Ja	tba	Ja	Ja
IDS	Ja	Ja	Ja	tba	Ja
XML	-	o	-	+	-
Events	++	+	++	-	o
Condition	+	++	+	o	++
Action	++	++	++	+	++
Verwendbarkeit	+	+	o	o	+

PONDER eignet sich tendenziell für Systeme mit zentralem Rechner, die LDAP oder CIM verwenden. Die Verwendung von CIM-SPL ist vor allem dann sinnvoll, falls aufbauend auf CIM ein Policy-System für IDS konstruiert werden soll. Ponder2 weist hingegen darauf hin, dass es vor allem für hochskalierende, verteilte Systeme gedacht ist. Zudem ist Ponder2 nicht von LDAP oder CIM abhängig. Für größere Projekte mit höherem Verwaltungsaufwand eignet sich deshalb, laut Angabe der Autoren, Ponder2 besonders gut[14]. Für PPDL und SPL fehlen noch ausgereifte Implementierungen und Praxistests im Umfeld von IDS und anderen Monitoren. [1] [8][13]

Falls verwendbare Implementierungen vorhanden sind, wie beispielsweise bei PONDER der Fall, können die Policy-Beschreibungssprachen überall da eingesetzt werden, wo nach strikten Richtlinien automatisch auf Ereignisse reagiert werden muss. In verteilten System und diversen Rechnernetzen werden heutzutage in den meisten Fällen Monitore und IDS eingesetzt, die den Ablauf der Programme überwachen, und die durch Policy-Systeme sinnvoll ergänzt werden können. Ein Intrusion-Detection-System kann so ergänzt werden, dass es vollautomatisch die wichtigsten Sicherheitsmechanismen des verteilten Systems aktivieren und wichtige Systemressourcen schützen kann. Im Zusammenspiel mit anderen Sicherheitskomponenten bilden diese IDS in vielen Rechnernetzen mittlerweile den Kern der eigentlichen IT Sicherheit. [12]

4. Zusammenfassung

Die Verwendung von Policy-Beschreibungssprachen im Umfeld von IDS und anderen Monitoren ist besonders nützlich, wenn automatisch auf Alarme reagiert werden muss. Der Funktionsumfang und die Verwendbarkeit der unterschiedlichen Policy-Beschreibungssprachen können hierbei deutlich variieren, weshalb vor Einsatz eines neuen Policy-Systems geprüft werden sollte, welche Anforderungen an die Beschreibungssprache gestellt werden, ob einfache Lösungen vorhanden sind, oder ob zumindest auf Workarounds zurückgegriffen werden kann. Wenn man das Spektrum verfügbarere Policy-Sprachen als Ganzes betrachtet, fällt auf, dass zu einigen Beschreibungssprachen bisher nur unvollständige Implementierungen und rein theoretische Ansätze zu finden sind. Viele neue Ideen, fortschreitende Standardisierungen und verbreitete Policies wie PONDER[1], die ständig weiterentwickelt werden, machen das Universum der Policy-Beschreibungssprachen zu einem sehr dynamischen und fortschrittlichen wissenschaftlichen Terrain. Es bleibt abzuwarten, welche Policy-Beschreibungssprachen sich letztendlich in der Praxis langfristig bewähren werden. [1][3]

5. Literatur

[1] Weili Han, Chang Lei, Software School, Fudan University, Shanghai (2012), China. A survey on policy languages in network and security management.

[2] Alexander Keller, Heiko Ludwig (2004), Policy-basiertes Management: State-of-the-Art und zukünftige Fragestellungen

[3] Vitalian Danciu (2003), Entwicklung einer policy-basierten Managementanwendung für das prozeßorientierte Abrechnungsmanagement

[4] Positif.org (2007) Security Policy Language (SPL) - User Manual

[5] Distributed Management Task Force (2009), CIM Simplified Policy Language (CIM-SPL)

[6] Jorge Lobo, Dandeep Bhatia, Ahmim Naqvi (1999), A Policy Description Language

[7] Elisa Bertino, Alessandra Mileo (2005), PDL with Preferences

[8] Prof. Elisa Bertino (2004), PPDL: Preferential Policy Description Language, http://mag.dsi.unimi.it/PPDL/, zugegriffen: 10.12.2013

[9] Nicodemos Damianou, Naranker Dulay, Emil Lupu, Morris Sloman, Imperial College Research Report (2000), Ponder: A Language for Specifying Security and Management Policies for Distributed Systems

[10] Patricia Marcu (2005), Reference Installation of the Ponder Policy Toolkit

[11] Mohamed al-Morsy, Hossam M. Faheema (2009), A new standard security policy language

[12] BSI, Bundesamt für Sicherheit in der Informationstechnik, Intrusion-Detection-Systeme (IDS) (2013), http://l.hh.de/obnQZs, zugegriffen: 01.12.2013

[13] Matthias Ebert (2006), Konzeption und Implementierung einer policy-basierten Privacy Management Architektur für föderierte Identitätsmanagementsysteme am Beispiel Shibboleth

[14] Kevin Twidle, Naranker Dulay, Emil Lupu and Morris Sloman (2009), Ponder2: A Policy System for Autonomous Pervasive Environments

[15] Kevin Twidle (2008), ObligationPolicies, http://ponder2.net/cgi-bin/moin.cgi/ObligationPolicies, zugegriffen: 18.12.2013

ISBN 3-937201-40-8
DOI 10.2313/NET-2014-03-1

ISSN 1868-2634 (print)
ISSN 1868-2642 (electronic)