

XMAS Lecture

Network Security vs. Network Privacy?

Cornelius Diekmann

Lehrstuhl für Netzarchitekturen und Netzdienste
Institut für Informatik
Technische Universität München

Version: December 17, 2014
Merry Christmas

Network Security – Security

- ▶ So far, when we discussed security, we considered
 - ▶ Confidentiality
 - ▶ Integrity
 - ▶ Accountability
 - ▶ Availability
 - ▶ Controlled Access

Network Security – Security

- ▶ We learned about several technical security measures.
- ▶ For example
 - ▶ IPsec ESP
 - ▶ Confidentiality
 - ▶ Integrity
 - ▶ IPsec AH
 - ▶ Integrity
 - ▶ Kerberos AS
 - ▶ Authentication
 - ▶ Accountability (?)
 - ▶ Kerberos TGS
 - ▶ Controlled Access
 - ▶ IKE DoS protection with cookies¹
 - ▶ Availability
 - ▶ ...

¹DoS Protection with Cookies (02_6_CryptoProtocols.pdf, 68ff)

Network Security – Security

- ▶ So far, we are
 - ▶ encrypting
 - ▶ integrity protecting
 - ▶ authenticating
 - ▶ ensuring availability
 - ▶ controlling access
- ▶ Is this enough?
- ▶ *What about privacy?*

Privacy

- ▶ What about the following packet?

```

▶ Frame 9: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
▶ Ethernet II, Src: IntelCor_ ( ), Dst: SuperMic_ ( )
▶ Internet Protocol Version 4, Src: , Dst:
▶ User Datagram Protocol, Src Port: 18811 (18811), Dst Port: domain (53)
▼ Domain Name System (query)
  [Response In: 13]
  Transaction ID: 0xcb70
  ▶ Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
  ▶ www.pornhub.com: type A, class IN
    
```

- ▶ Okay, it's DNS
- ▶ DNS is not secure, but we can use DNSSEC
- ▶ Now the answer can be integrity protected

Privacy

- ▶ Wait, you want confidentiality?
- ▶ Okay, send the DNSSEC via an ESP tunnel
- ▶ BTW: Who is your DNS provider?

```

▶Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
▶Ethernet II, Src: IntelCor_ ( ), Dst: Sphairon_ ( )
▶Internet Protocol Version 4, Src: 192.168.1.170 (192.168.1.170), Dst: 8.8.8.8 (8.8.8.8)
▶User Datagram Protocol, Src Port: 36471 (36471), Dst Port: domain (53)
▼Domain Name System (query)
  Transaction ID: 0x0bf5
  ▶Flags: 0x0120 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▼Queries
    ▶pornhub.com: type A, class IN
  ▶Additional records
    
```

Privacy – Lessons Learned

Your DNS provider knows what you are doing!

About this Example

- ▶ It is widely acknowledged that there are many pages in the web with dubious content
- ▶ Among the top 500 sites on the web², many serve adult content
- ▶ PornHub is among the 100 most popular web sites globally³
- ▶ We used PornHub as example for this lecture

²<http://www.alexa.com/topsites>

³Rank 72 on Dec 17 2014, <http://www.alexa.com/siteinfo/pornhub.com>

Meta Data

- ▶ We can protect your traffic
 - ▶ But some information needs to be accessible in plaintext
 - ▶ IP source and destination
- ▶ Btw: what is this 31.192.117.132 IP address on TCP port 80 you are visiting?
- ▶

```
curl -v http://31.192.117.132/  
Connected to 31.192.117.132 (31.192.117.132) port 80  
> GET / HTTP/1.1  
> User-Agent: curl/7.35.0  
> Host: 31.192.117.132  
> Accept: */*  
>  
< HTTP/1.1 301 Moved Permanently  
< Date: Tue, 09 Dec 2014 17:27:59 GMT  
< Location: http://www.pornhub.com/
```

Meta Data

- ▶ Okay, Okay, I set up an IPsec tunnel to a secure server
- ▶ The secure server forwards my packets to the Internet
- ▶ You will only see the outer IP header
- ▶ But at some point, the inner packet needs to be given to the Internet
- ▶ Global attacker (e.g., state-level attackers) still know what you are doing



Protest sign, Anti-NSA demonstration “Restore The Fourth”, July 2013

Traffic Analysis

- ▶ Our first slide set mentions something about traffic analysis⁴
- ▶ Maybe I'm not the NSA and cannot see your unencrypted traffic
- ▶ I can still observe
 - ▶ The amount of data you are transmitting
 - ▶ Timing information

⁴01_Intro.pdf, 30

I'll just leave this here

- ▶ Pornhub statistics for Germany

 **8 minutes**
Average visit duration

 **7.3 pages**
Average viewed per visit

PornHub Insights, *Pornhub & Germany*, May 2014,
<http://www.pornhub.com/insights/> retrieved Dec 2014

I'll just leave this here

- ▶ It's not just Germany...
- ▶ Statistics for India

8 min 22 sec

Average Visit Duration

7.32 pages

Average Viewed Per Visit

PornHub Insights, *Pornhub & India*, Nov 2014, <http://www.pornhub.com/insights/>
retrieved Dec 2014

Such Meta Data, Very Traffic Analysis, Wow

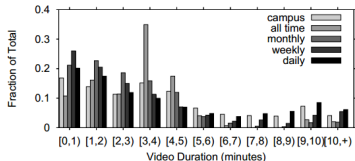
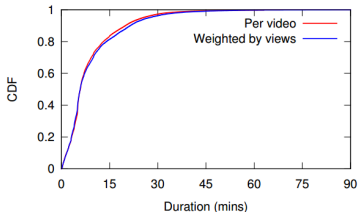
US vs RUSSIA
HOW LONG DO THEY LAST?

	Pages Per Visit	Visit Duration
Washington	8.7 pages	9 min 46 sec
United States	9.0 pages	9 min 53 sec
Moscow	7.9 pages	8 min 37 sec
Russia	7.2 pages	7 min 52 sec

Pornhub

PornHub Insights, *United States vs Russia*, May 2014,
<http://www.pornhub.com/insights/> retrieved Dec 2014

Content Duration of Available Content



Tyson, Gareth, et al. *Demystifying porn 2.0: a look into a major adult video streaming website*. IMC 2013 –
 (YouPorn data)

Gill, Phillipa, et al. *Youtube traffic characterization: a view from the edge*. IMC 2007



**Best wishes for a wonderful Holiday
and a Happy New Year!**