Challenging Topics!
Sometimes previous knowledge required!

Information Session for the Seminar ”Future Internet“

Prof. Dr.-Ing. Georg Carle and I8 research staff
Organization: Daniel Raumer, Lukas Schwaighofer
Contact: seminar@net.in.tum.de

Content

- **Administrative Things for the FI Seminar**
  - Deadlines
  - Responsibilities
  - Grading
- Topic Selection for Seminar Future Internet (FI)

Basic Information

- Lecturer:
  - Prof. Dr.-Ing. Georg Carle
- Organization: seminar@net.in.tum.de
  - Daniel Raumer
  - Lukas Schwaighofer
- Overview
  - Main Language: German
    - we will offer an English track
      (presuming a minimum of 4 participants)
  - Extent: 2 SWS (4 ECTS)
    - 4 ECTS * 30 hours = 120 working hours expected from you
  - Course Type:
    - For M.Sc. Students: Master's Seminar (Master-Seminar)
    - For B.Sc. Students: Advanced Seminar Course (Seminar)

Seminar Deadlines

Deadlines might be shifted depending on number of participants.

	Dates
Topic Selection (room 03.07.023)	**today**
Pick up literature per mail or personal by advisor	Until **21.07.2014**
Advisor meeting (discussion of received literature) – be prepared (MUST)	Until **08.08.2014**
Detailed structure of paper and talk	Until **22.08.2014**
Final slides* discussion with advisor	Until **22.09.2014**
*** Slides must be presentable, otherwise -0.3 degree in grading.**	
Upload paper (1. Version)	**21.09.2014**
Upload Reviews	**05.10.2014**
Talks **Schedule will be published soon**	**29/30.9.2014** **(& 2.10.2014)**
Upload paper (2. Version) and final slides	**26.10.2014**
Publication in Proceeding	**t.b.a.**

Paper Procedure

- First version of your paper
  - Agree on the content with your advisor
  - Use the supplied paper template from the webpage
  - Keep in touch with your advisor
  - Try to finish well in time so you advisor can give you feedback
- Write reviews
  - You will be given two papers of your fellow students
- Final version of your paper
  - Use the received reviews to improve your paper
  - You will also receive some feedback from your advisor
  - If you and your advisor agree → publication in the seminar proceedings

Talks and Papers can be in German or English!

Talk Procedure

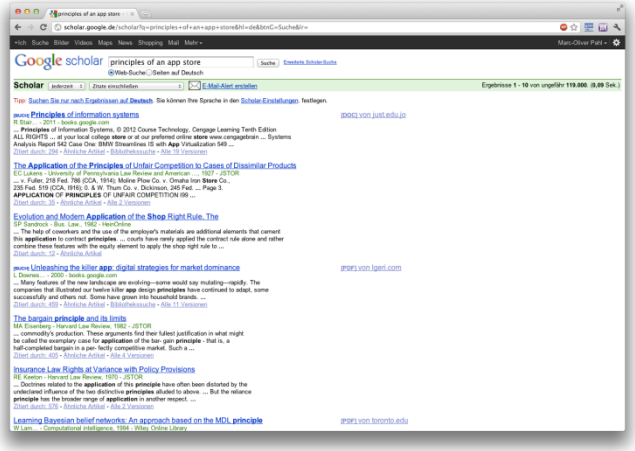
- Prepare your talk
  - Finished slides must be discussed with advisor 1 week before the talk
  - Advisors usually offer the opportunity of test talks
- Give your talk
- Session chair for one talk
  - Introduce the talk
  - Watch the time constraints
  - Try to get the discussion started after the talk (ask at least one question if nobody else does)
- Mandatory attendance on all sessions in your track
  - If you cannot attend for a good reason contact seminar@net.in.tum.de in advance

Talks and Papers can be in German or English!

Topic Handling

- From your advisor(s) you may receive some literature.
  - This is just to get you started

- Find appropriate (scientific) sources yourself
  - scholar.google.com
  - acm.org
  - ieee.org
  - You sources' sources
  - …



Just presenting the given literature is NOT enough

Further Information

- TUM-Online registration
  - If you pick a topic today we will register you for the course
  - You will be able to unregister for 1 week without any consequences
  - Later dropout will be graded as 5.0
- Webpage: http://www.net.in.tum.de/de/lehre/
  - Slides: How to write a paper
  - Slides: How to write a review
- Questions:
  - Contact your advisor
  - For organizational questions: seminar@net.in.tum.de

Grading

Grading parts:

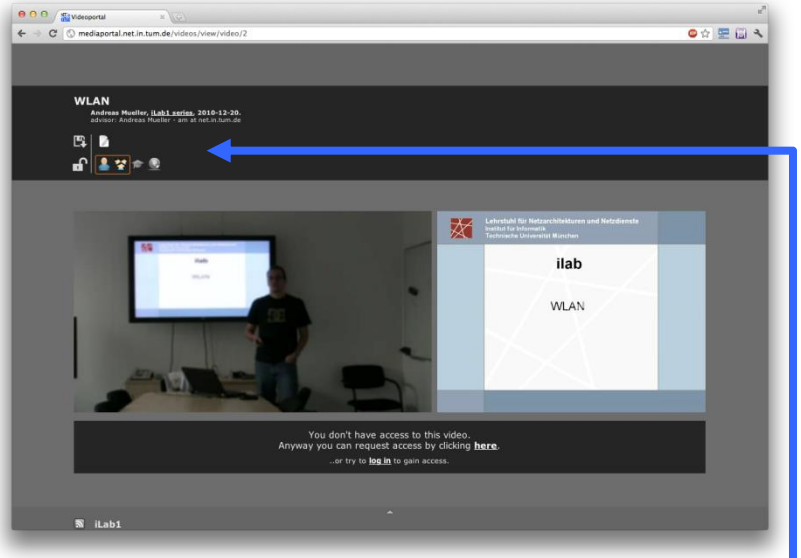
1. Both of your paper submissions (6–8 pages in ACM) (50%)
   - 1st version: 37,5%
   - 2nd version: 12,5%
2. Your talk (20–25min, following discussion and feedback) (25%)
   - Content is graded
   - Personal presentation style is not
3. Your reviews of papers from other seminar participants (25%)

Grading – influencing factors

- Observe the deadlines
  - Advisor meetings are compulsory
  - Use the upload form on our webpage for your submissions
  - 0.3 degrading per day for missed deadlines
- No submission
  - 1st version of paper: Disqualification (Seminar graded as 5.0)
  - Other submissions: Grade 5.0 for the concerning part
- Write the paper yourself
  - Plagiarism → disqualification (and we will check!)
    - Attempted cheating reported to the examination office
  - Summary when and why to cite: http://oxford.library.emory.edu/research-learning/citation-plagiarism/citing.html

You have the chance to get your talk recorded

- Have a **look at yourself** after the talk!
- Your talk was great? Share it and show it to your friends.



You fully control the access!
(Initially only you can access it!)

English Only Track

- We offer an English only track if…
  - At least one non-German native speaker wants to attend the seminar
  - At least four students (in total) agree to do their paper and talk in English
  - **<u>Is this the case today?</u>**

- The English only track will have separate sessions
  - Probably 1-2 sessions (depending on the number of students)

- Attendance not mandatory for talks in the “standard” track
  - Students in the “standard” track also don’t have to participate in the English track talks
  - You are still welcome to join the other track’s talks ☺

- Usually the English track is quite small
  - This means less attendance (if the opportunity to improve your English is not a good enough reason for you…)

Questions?

Content

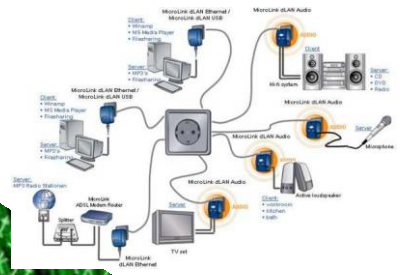
- Administrative Things for the Fi Seminar
  - Deadlines
  - Responsibilities
  - Grading
- **Topic Selection for Seminar Future Internet (FI)**

Challenging Topics!
Usually some previous knowledge required!

Cyber War – What is behind?

Nadine

- Attacking critical infrastructures as war strategy?
  - Stuxnet as one example
  - APT (Advanced Persistent Threat) as new buzzword
  - Is it possible to „hack“ our power supply system?
  - What is real and what is fiction?
  - Is it the „end of the world“?

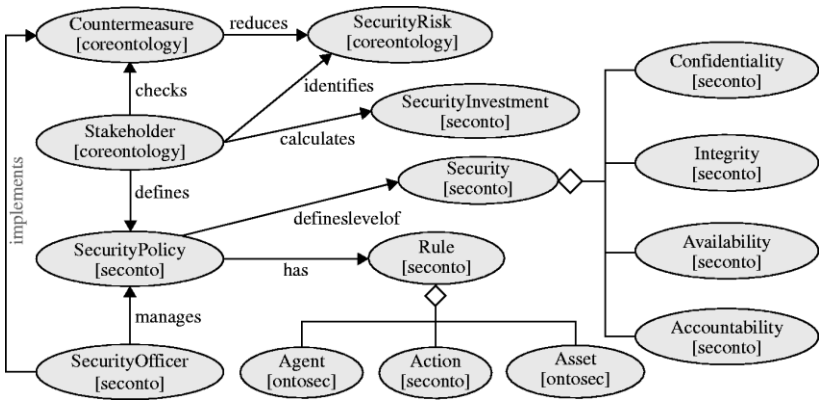


- Your Task:
  - Explore the possible threats for critical infrastructures and industrial networks
  - Structure them and explore some in detail
  - Explore the real risk behind those treats and find out what is behind Cyber war

Attack Taxonomies and Ontologies

Nadine

- Structuring Attacks to:
  - Get an overview of possible attack scenarios and threats
  - To examine categories for IDS Testing
- Methods:
  - Taxonomies and Ontologies
- Your Task:
  - What is the state of the art?
  - What problems have existing approaches?
  - Is it possible to combine existing Taxonomies and Ontologies?



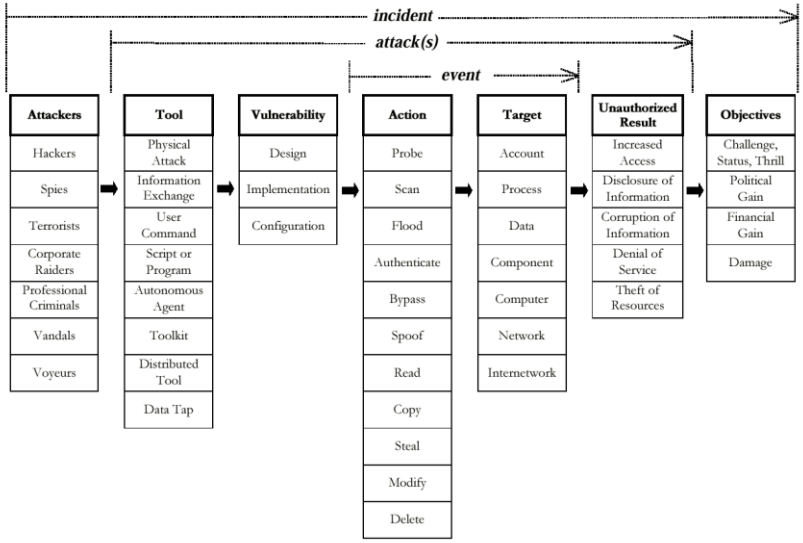
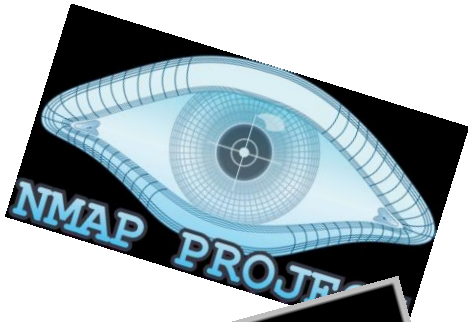


Figure 5.4. Computer and Network Incident Taxonomy

Hands-On: Attack Frameworks and Tools

Nadine

- Is it easy to implement cyber attacks?
  - Popular tools: LOIC (Low Orbit Ion Canon) for DOS, Metasploit, …
  - Linux Packages: hunt (spoof addresses), nmap (port scanning), …



- Your Task:
  - Examine popular tools and explore theire capabilities
  - How easy is it to use these tools?
  - Are they effective?
  - What requirements have to be achieved?

  ➢ You may need to set up a test environment!

Smart Buildings vs. Data Privacy Laws

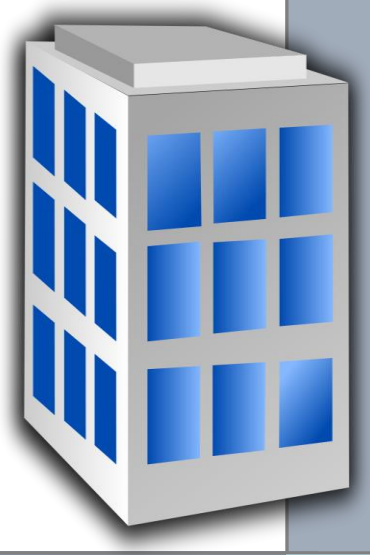
Holger/Marcel

- Smart Buildings are equipped with sensors, actors and automation systems that, e.g.,
  - … increase our comfort.
  - … optimize a building's energy consumption.

- **Problem:**
  - Sensor data (power consumption, temperature, luminosity, etc.) might be abused for the surveillance of employees.
    - E.g.: Correlate records of time worked and power consumption.
  - A conflict between technology and law is created.

- **Your Task:**
  - Perform a study on the legal
  - situation (use law texts, blogs, etc.).
  - Perform a study on the state
  - of the art (scientific papers, etc.).
  - Present your findings.

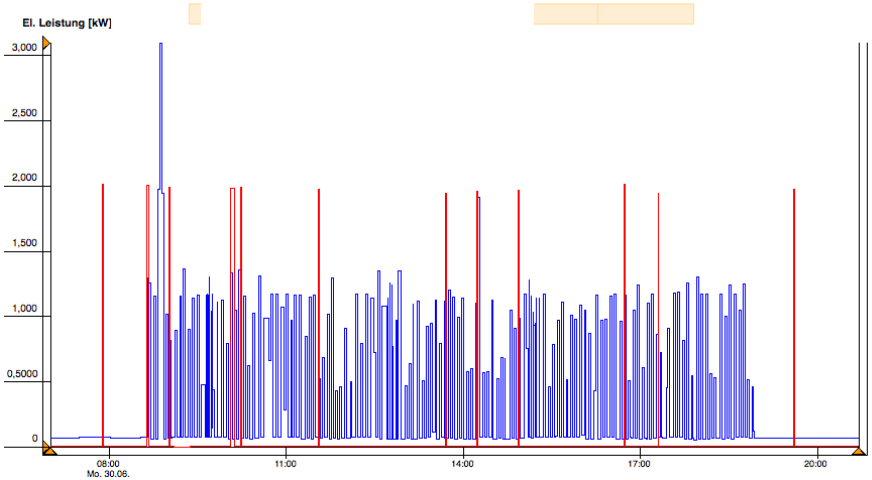
vs.



Data Mining in Energy Logs

Marcel/Holger

- We just learned that energy logs
- contain (personal) data.
  - Example: Log of our kitchen



- Idea: Analyze a dataset recorded
- with our logging system.
  - Electricity
  - Temperature logs of one office

- **Goals:**
  - Research on data mining tools
  - and apply your new skills to the dataset
  - Identify patterns, individual devices, maybe even habits of users.
  - Document work procedure and findings.

- **Caveat:**
  - Requires constant cooperation with your supervisors.
  - You need to sign a data confidentiality statement!

Measuring Privacy

Holger/Marcel

- Most of us have an intuition of what privacy means
  - It is normally about personal data
  - The aim is to keep some information away from a specified audience

- **Problem:**
  - It should be able to rate an IT-system concerning its ability to preserve the privacy of its user
  - It's getting really difficult when trying to find a compromise between „show everything“ and „show nothing“
  - To rate such systems, some metrics for measuring privacy (and its breaches) is necessary

- **Your Task:**
  - Research different approaches of measuring privacy
  - Compare them and assess the applicability in the context of smart buildings.

freenetproject.org

Holger

- Problem: International intelligence agencies monitor the Internet ⍰ ⍰

- One way how to circumvent supervision are anonymizing proxies
  - Gateways to the “good old” internet giving you an anonymous IP.
  - Examples: TOR, AN.ON, etc.

- A different approach is used by the Freenet project:
  - Anonymity is no add-on but a fundamental part of the system design.
    - Distributed infrastructure (P2P network)
    - Specific routing protocols
  - Further features: censorship resistance; darknet

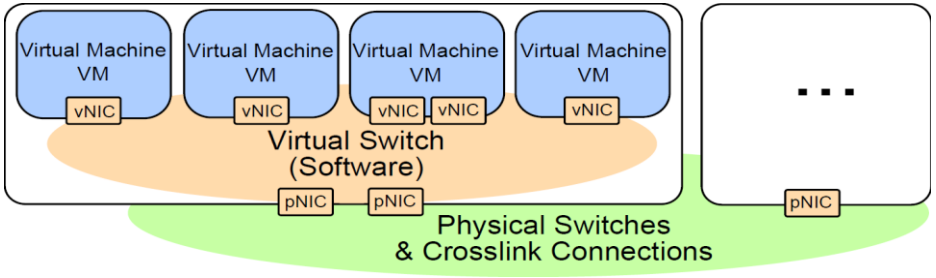
- Goals:
  - Explain motivation and goals of the project.
  - Explain protocols and system design.
  - Find and present related work.

Freenet
THE FREE NETWORK

Virtual Switches: State of the Art in 2015

Daniel, Florian

- **A virtual switch shuffles packets between VMs only in software**
  - Software is more flexible then hardware
  - Can be enriched with middle box functions
  - can go beyond 10Gbit Ethernet



- **Your Task:**
  - Get familiar with concepts and architectures of virtual switches
  - Survey existing approaches
    - choose meaningful criteria for compare!
  - Academically approaches go beyond the state of the art in productive networks → also discuss these approaches

- Starting point:

  Open vSwitch, Contrail vRouter, DPDK vSwitch, VALE, etc.

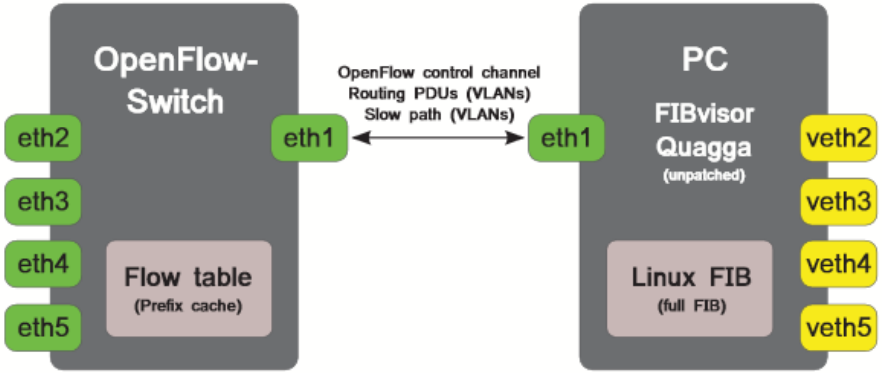
Innovative Future Router Architectures

Florian, Daniel

- Software router and switches…
  - … empower short development cycles for new features ☺
  - … are cost-efficient ☺
  - … but provide comparatively poor (forwarding) performance ☹

- Hardware routers have long development cycles, lead to vendor-lock-in, and are expensive

→ Idea: combine L3-switches or cheap routers with a server and software



*) Graphic taken from Poster: "FIBIUM - Towards Hardware Accelerated Software Routers"

<u>Goal:</u>

- Describe the problems with Routers (e.g. costs, vendor lock-ins, limited capabilities, etc.)
- Shortly summarize the benefits of software router/switches and those of hardware router/switches
- How can innovative architectures look like?
- Describe approaches (RouteFlow, FIBIUM, and own findings) and compare them.
- Perhaps you will have to describe background that leverages these approaches (e.g. OpenFlow)

(Continuation as Master's or Bachelor's Thesis is possible.)

Possible starting literature:

[1] N.Sarrar, S.Uhlig, A.Feldmann, R.Sherwood, and X.Huang, "Leveraging Zipf's law for traffic offloading" SIGCOMM CCR (2012)
[2] A.Vidal, F.Verdi, E.Fernandes, C.Rothenberg, and M.Salvador, "Building upon RouteFlow: a SDN development experience.", SBRC'2013 (2013)

What‘s New in the Linux Network Stack?

Paul, Daniel

- **The Linux network stack consists of many parts**
  - Protocol Implementations (IP, TCP, UDP, SCTP, …)
  - Firewalls (iptables/netfilter)
  - User space networking (virtualization, VPN) support (TUN and TAP)
  - Switches and routers (Bridge, IP forwarding, Open vSwitch)
  - All of them are under constant development and new features are added regularly

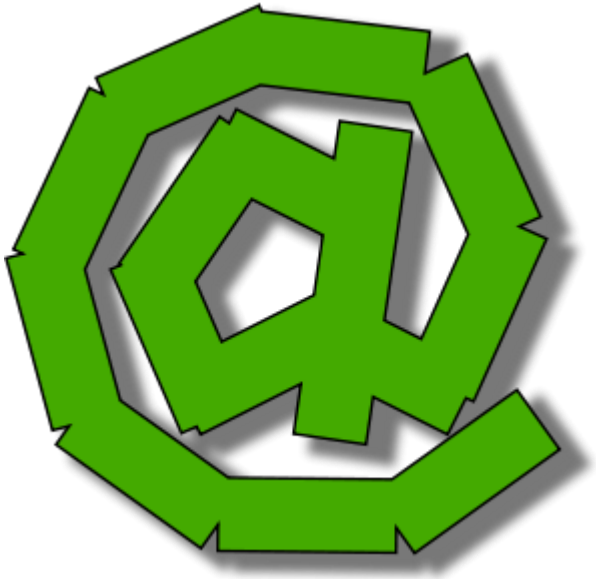
- **Your Task**
  - Get familiar with the Linux network stack
  - Literature review, changes since Linux 3.7
  - Identify new features and improvements
  - Point out possible weaknesses and limitations

⚠ Basic knowledge of Linux required to dive into Linux code

E-Mail Extensions

Lukas, Benjamin

- SMTP is an ancient protocol
  - Used since 1980s
  - Designed before SPAM et al.
- Extensions are introduced to deal with emerging problems



- **Your Task:**
  - Research “current” extensions
    - Sender Policy Framework (SPF)
    - Domain Keys Identified Mail (DKIM)
    - Domain-based Message Authentication, Reporting & Conformance (DMARC)
    - Others you find interesting
  - What are their respective effects
    - What are they designed to improve / mitigate?
    - Do they cause any problems?
  - How do they work together?
  - What is used by “big players”

Network Time Security

Benjamin, Lukas

- Network time protocol (NTP) without proper security
- New proposal: “Network time security” (NTS)

NTP after security evaluation (not to scale). Picture by Todd Kopriva.

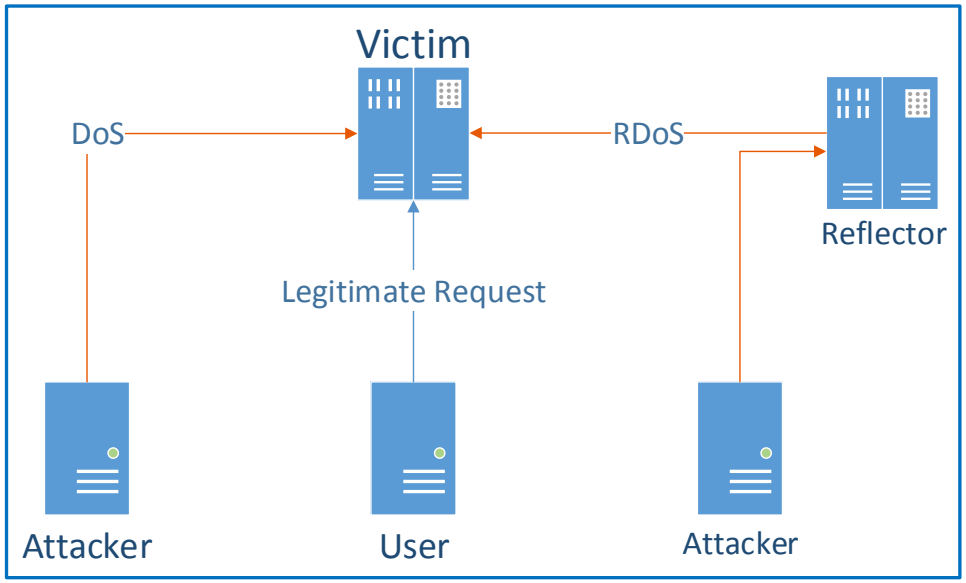
Your task:

- Understand NTPv4 and its security properties and weaknesses
- Understand NTS
- Analyze and evaluate NTS security properties
  - Trust model
  - Authentication
  - Transport security
  - DoS

Exploring DDoS Defense Mechanisms

Oliver

- Distributed Denial of Service Attacks
  - Major threat to networks and Internet services
  - DDoS detection has been focus of many studies
  - Detection only first step, mitigation and defense is next



- Your Task:
  - Get familiar with DDoS attacks and their implications
  - Find and compare different DDoS defense mechanisms in literature
  - How do they work? What do they rely on?
  - Point out weaknesses and potential remedies

[1] JCY Chou et.al “Proactive surge protection: a defense mechanism for bandwidth-based attacks”, IEEE/ACM Transactions on Networking 2009

[2] J. Snijders “DDoS Damage Control -- Cheap & effective”, RIPE68 2014

Internet Science – Behavioural Aspects (Heiko)

- Network or Security Engineers often blaim the stupid user. Now, is this claim correct or are the engineers just missing something important?

- Others claim that Internet is machine-to-machine only. No humans ever involved (even at IETF?).

	Care for security	Do not care.
Care for security		
Security, wtf ???		

- Your task:
  - Motivate relation behaviourism and IT
  - Present 1-2 claims presented in related articles.
  - Use other sources to justify and/or question the claims. (e.g. from behavioural sciences)

- Potential Sources:
  - http://weis2014.econinfosec.org/program.html or previous workshops under http://weis2014.econinfosec.org/past.php

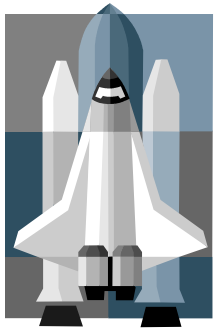
Internet Science – Attacking in Cyber Conflicts (Heiko)

- Assume you found a hole („zero day exploit“) in the defense of someone else, maybe a competitor or enemy

- It may be useful now, but maybe more useful later. Yet there is also the danger of ….
- Question: When is it time to attack (and steal the frog)?
- Potential extension: How can you model such scenarios with games? How was data for model parameters in the source below obtained?
- Sources:
  - Axelrod, Iliev, „Timing of cyber conflict“, http://www.pnas.org/content/early/2014/01/08/1322638111
  - More to be given. Also: Find more sources yourself.

Internet Science – Critical Infrastructures (Heiko)

- Something is critical when people *really* miss it once it is gone.



- Your task:
  - What is a critical infrastructure? Seek definitions.
  - What are players and stakeholders in it?
  - How do humans play a role?
  - How to make it reliable?
  - How to make it secure?
  - What makes it fail?

Internet Science – Models for User-Generated Content (Heiko)

- Today, people on the Internet do not primarily watch Hollywood movies anymore, instead they watch:

- There are many models for popularity of movies, businesses, and all kinds of other things and tastes (e.g. Zipf‘s Law).

- This may hold true also for user-generated content, but for short-lived content like Youtube videos or blog posts, the big question is more,
  - What is popular now?
  - How much of it will be popular the next hour or tomorrow?
  - How long does content live?
  - How can we model and simulate these changes?

- Your task:
  - Look at the Shot Noise Model (SNM) for popularity modelling.

Machine Learning for Network Intrusion Detection

Johannes

- Network Intrusion detection commonly uses signatures of known malicious Traffic
  - No detection of unknown attacks
  - Use Machine Learning to learn normal behavior
  - Raise alerts when encountering anomalies

Pic or it didn't happen

- Your Task:
  - Get familiar with the concept of network intrusion detection
  - How is/can Machine Learning be used for network intrusion detection?
  - What are the Challenges of using Machine Learning for network intrusion detection? [1]

[1] R. Sommer, V. Paxson: "Outside the closed world: On using machine learning for network intrusion detection", *IEEE Symposium on Security and Privacy, 2010*.

Choose your Topics

- We will send you an E-Mail today
  - Contains the list of possible topics in short form (Comment on PDF)
  - All “by default” indicated as your first priority

- Sort the topics according to your preferences
  - The actual order of the items is irrelevant, only the number matters
    - 1 is the highest priority
  - You can indicate equal priority by using the same number more often

- There is no advantage in avoiding popular topics! The matching algorithm works roughly as follows
  1. Go through the students in a random order
  2. Give each student the topic with the highest preference that is still available

You have to send us your preferences by Tuesday (tomorrow)!

Questions?