Lecture Network Security
Chapter 1 – Introduction

University of Bonn, Institute of Computer Science IV, Summer 2016

universitätbonn

Fraunhofer FKIE

Introduction

A short talk I had during a long flight:

He (Passenger in neighbor seat): „Hey, what is your profession?“

Me: „I‘m a researcher.“

He: „Me too. I‘m working at an accelerator ring. What are you doing?“

Me: „I‘m a computer scientist.“

He: „Which field?“

Me: „Network security.“

He: „Hmmm.“

Me: „Hmmm?“

He: „Why are you doing research in network security? Cryptographic algorithms are known for more than 30 years and firewalls exist.“

Me: „Hmmm.“

He: „Hmmm?“

Me: „Have you ever had a worm on your PC?“

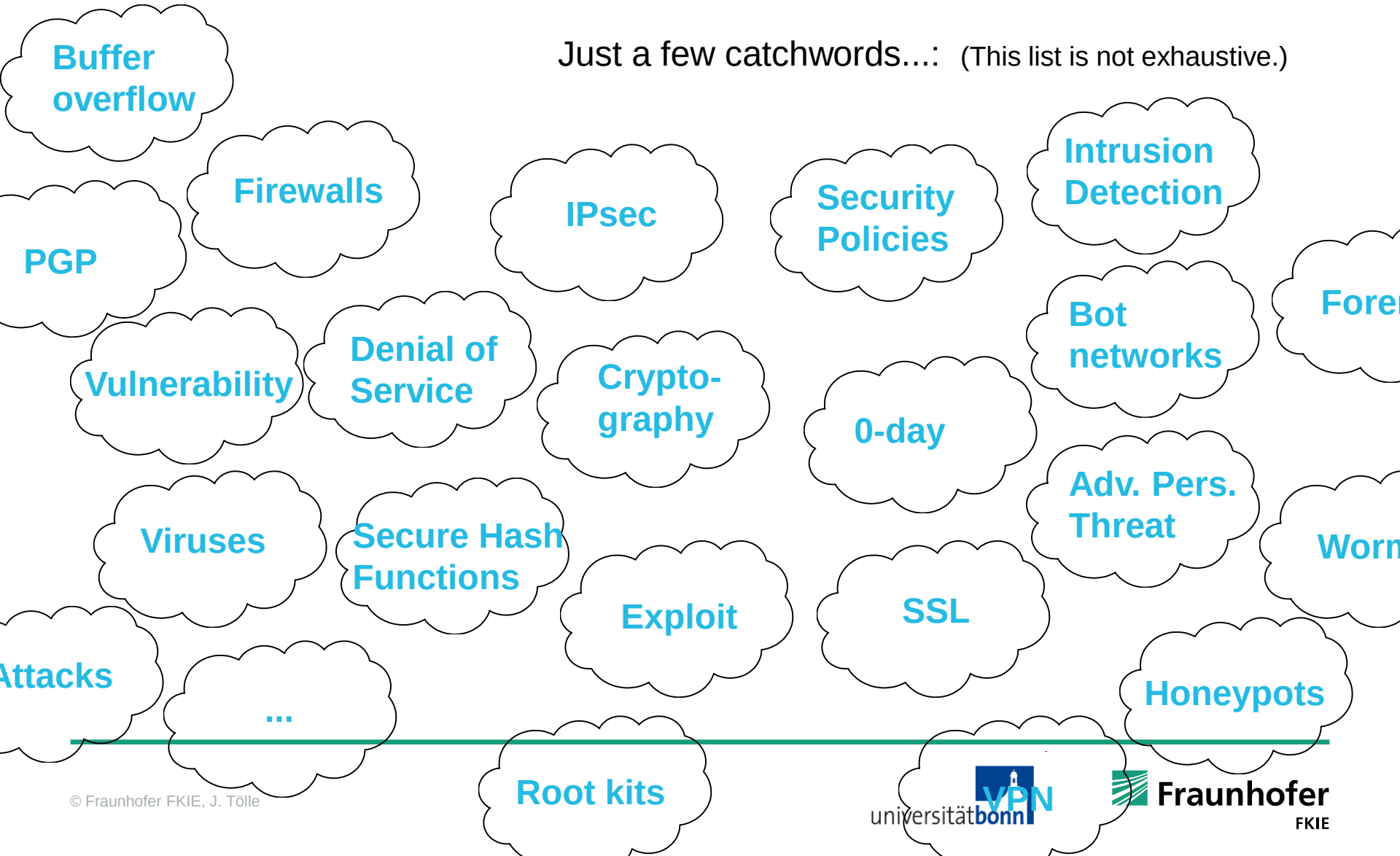
He: „Yes!“

Me: „Why? Cryptographic algorithms are known for more than 30 years and firewalls exist....“

A few Buzzwords

Security in the Internet is a very complex topic.

Just a few catchwords...: (This list is not exhaustive.)



Security in the Internet?

Let's start with a few basic questions:

Do we **have** security in the Internet? **No.**

Do we **need** security in the Internet? **Yes.**

By the way: What is security? **It depends. Let's see…**

"Secure" (=reasonable?) system behavior in case of

- faulty configuration
- faulty software components
- faulty hardware components
- technical problems
- catastrophes
- attacks

universitätbonn

Fraunhofer FKIE

Safety vs. Security?

Some Folklore

- Safety is about aeroplanes not crashing,
  security is about my computer not crashing (due to a virus)
- Safety is about functionality,
  security is about secrets
- Safety is protecting the environment from the system,
  security is protecting the system from the environment
- Safety is about unintentional faults,
  security is about intentional faults

„I used to head the Chair of Computer Science 1 at University of Mannheim. Since I work in the area of applied computer security and am constantly trying to cover my traces: From 2002 to 2010 I worked at five different universities under two different names.“

Source: Prof. Felix Freiling, Univ. Erlangen-Nuremberg
http://www.trustsoft.uni-oldenburg.de/en/download/Slides-Freiling-20060727.pdf

Network Security Yesterday and Today

To understand **today's network security** problems…
… it is useful to know about **network history.**

Yesterday:

1957 Soviet Union launches first artificial satellite SPUTNIK
„sputnik shock“ for the United States

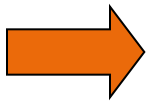
Foundation of NASA, ARPA *(Advanced Research Projects Agency)*

1960s Plans to develop a packet switched communication network
Goal: Resource sharing, „cheap“ and open access to existing computers and to existing peripheral devices
Protocol development and implementation done by students

1969 The first four ARPANET nodes were connected
The ARPANET is the predecessor of the Internet.

Yesterday – The ARPANET

- Users (mainly engineers and scientists) were **highly educated** and trained.
- Only a **very limited number** of persons had access to the network hardware.
- The networks were used to **access information and resources** in a fast and easy to use way.
- There were no threat scenarios (**no attackers**).



There was no **„network security“.**

Security aspects were not in the focus of the design and the implementation of ARPANET/Internet network protocols.

Today – The Internet

The Internet usage today:

- private communication
- online commerce
- online banking
- financial transactions
- control of (critical) infrastructure

} **New services!**

And:

- **millions of users**, unknown to each other
- **untrustworthy** users

Today and Tomorrow – Cyber Warfare

Today, computer network attacks have a political and military dimension:

Cyber Warfare

Some countries have started considering the *cyber space* as a fourth battlefield. In addition to army, navy, and air force, they establish groups of cyber warfare experts.

Cyber defense

means *defensive* actions to protect own systems and computer networks.

Cyber operations

includes *offensive* actions to weaken the communication capabilities of an enemy.

Cyber Warfare – Science fiction?

Is Cyber Warfare science fiction? **No!**

Cyber conflicts:

1999: NATO jets bomb the Chinese embassy in Belgrade, Yugoslavia. Within 12 hours, the *Red Chinese Hacker Alliance* was formed to attack US government websites.

2001: A Chinese fighter jet collided with an U.S. aircraft. 80000 Chinese hackers launched a „self-defense“ cyber war.
(New York Times: *World Wide Web War I*)

1997-2001: During 2nd Russian-Chechen war the Russian Federal Security Service (FSB) knocked down two important Chechen websites to gain information superiority and shape public perception.

Cyber Warfare – No Science fiction

More examples of cyber conflicts:

2007: Estonia re linn”, dedicated to sold
Massive DDoS a nks, parliament, minis

2008: During Ru government websites using D attacks were well prepared.

Reference:
These examples were taken from *Jeffrey Carr, Inside Cyber Warfare, O Reilly, 2010*
This book contains several more examples and details.

Security Risks

The main security risk is the **direct connection of all systems** of the Internet.

Security problems somewhere in the internet can influence many (or even all) computers and their user.

Internet access:

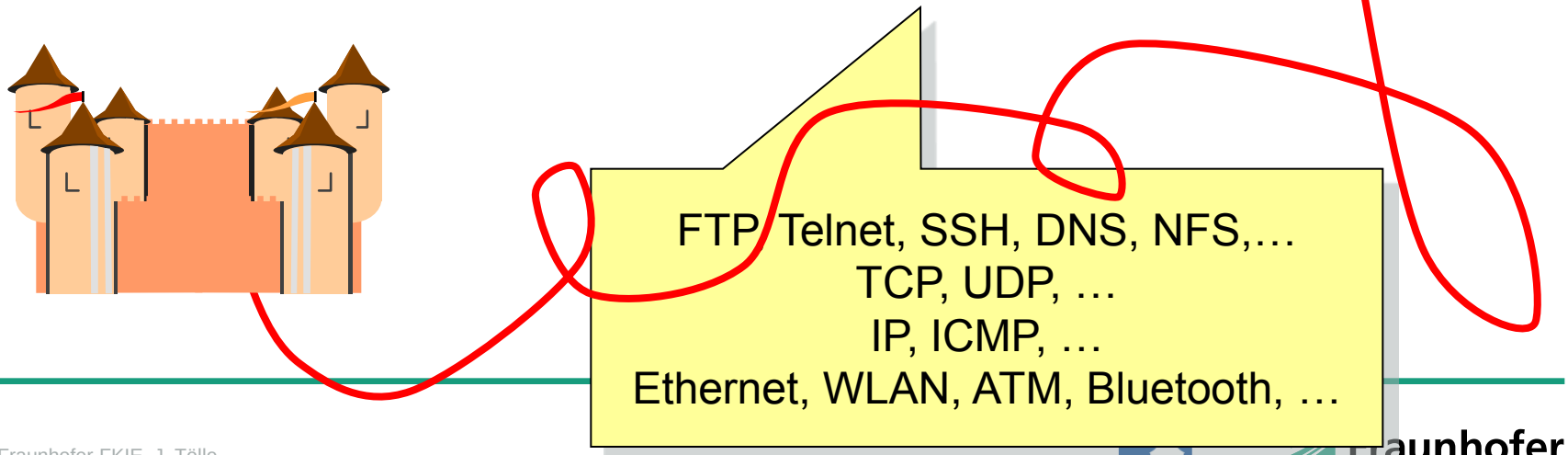
A computer hours of flight away is only (a few hundreds of) milliseconds away.

```
$ ping www.whitehouse.gov
PING e4036.dscb.akamaiedge.net (2.18.236.110) 56(84) bytes of data
64 bytes from 2.18.236.110: icmp_seq=1 ttl=53 time=15.7 ms
64 bytes from 2.18.236.110: icmp_seq=2 ttl=53 time=14.7 ms
$ ping www.cctv.cn
PING www.cctv.cn (202.108.8.82) 56(84) bytes of data.
64 bytes from zz-8-82-a8.bta.net.cn (202.108.8.82): icmp_seq=1 ttl=238 time=250 ms
64 bytes from zz-8-82-a8.bta.net.cn (202.108.8.82): icmp_seq=2 ttl=238 time=242 ms
```

Risks…

Security flaws can be found

- in the configuration and implementation of applications,
- in operating systems,
- in (network) services,
- in **the design of communication protocols**, or
- in **the implementation of communication protocols**.



A Selection of Known Attacks: Spoofing

Spoofing is the usage of a **fake identity**.

In human communication usage of fake identities is common as well, but *common sense* often helps to discover these attacks.

In network protocols information identifying the sender is **usually unprotected**. The recipient often simply **trusts** the sender entry.

This works well for

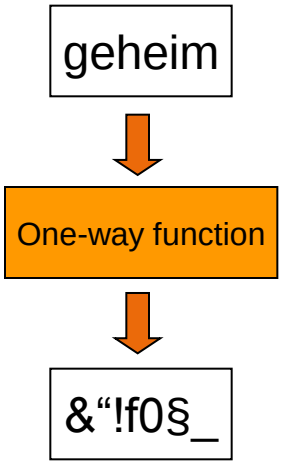
- ARP spoofing
- DNS spoofing (e.g. cache poisoning)
- IP spoofing
- ICMP spoofing (e.g. redirect)
- Mail spoofing (sending mails with forged sender)
- Web spoofing (URL rewriting)
- ...

A Selection of Known Attacks: Brute Force

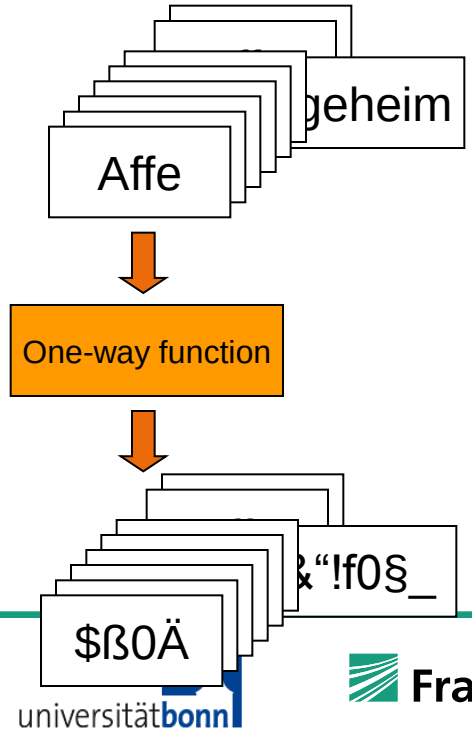
Brute Force Attacks try to break security mechanisms with pure computing power.

Example: Passwords are often encrypted using so-called one-way functions.

A password is encrypted, the **encrypted result is stored**.
If somebody wants access to the system, he enters a password which is encrypted and compared with the stored value. If they are **identical**, **access is granted**.



If this value is known, the following attack is feasible:



universitätbonn

Fraunhofer FKIE

A Selection of Known Attacks: Sniffing

Sniffing means interception of network traffic; e.g. transmission of passwords.

Needed: Access to transmission cables (copper wires, optical fibres).

1954/55: US and UK dig 450 m tunnel from West- to East-Berlin to wiretap soviet telephone lines.

Access in shared transmission media is easier than wiretapping dedicated media.

„old style ethernet“
(a single collision domain)

wireless transmission technologies
- WLAN
- Bluetooth
- radio (HF, VHF,…)

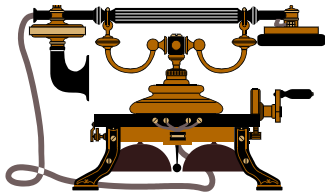
Switched ethernet

Access to switch, installation of mirror port necessary

A Selection of Known Attacks: DoS – Denial of Service

Primary goal of a **Denial of Service** attack (DoS) is **not** an intrusion in order to **steal** or **modify data**, but to **block access** to a system or network for other user.

Real-life examples: „Telephone terror“ or „Pizza attack“



To start a DoS attack, the attacker sends **huge amounts of data** or special crafted **data packets** to the target system. The target breaks down.

Different methods can be used, e.g.

- TCP Syn Flooding
- UDP packets
- ICMP echo request packets („Ping“)
- HTTP requests
- ...

See other chapter for detailled information

A Selection of Known Attacks: DoS – Denial of Service

THE BERNERS STREET HOAX.

Sources:
http://de.wikipedia.org/wiki/Berners_Street_Hoax
http://en.wikipedia.org/wiki/Berners_Street_Hoax

A Selection of Known Attacks: MANET Blackholes

A Blackhole is an attack against the routing mechanism of Mobile Ad-hoc networks (MANETs)

A MANET is a Mobile Ad-hoc Network. **Mobile nodes** are connected with **wireless links**. Communication between nodes not being in direct radio transmission range of each other is done using **multiple hops**.

MANETs do not rely on pre-installed infrastructure.

Example:
MANET routing with **OLSR** (Optimized Link State Routing) makes use of HELLO and TC (Topology Control) messages, announcing the neighborhood of the sender.

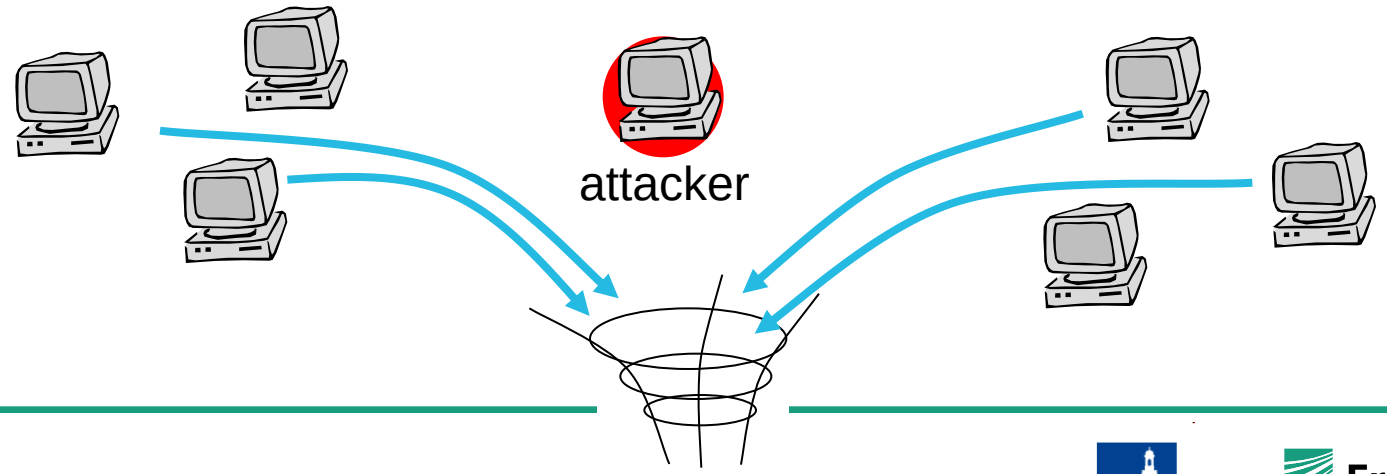
Other nodes base their routing decisions on these messages.

A Selection of Known Attacks: MANET Blackholes (cont'd)

If one node **claims to be a suitable member of routes (e.g. claims to have a lot of neighbors in OLSR according to RFC3626)**, he is likely to become a hop on several routes stored in the routing tables of other nodes.

When the node is part of several routes, he can

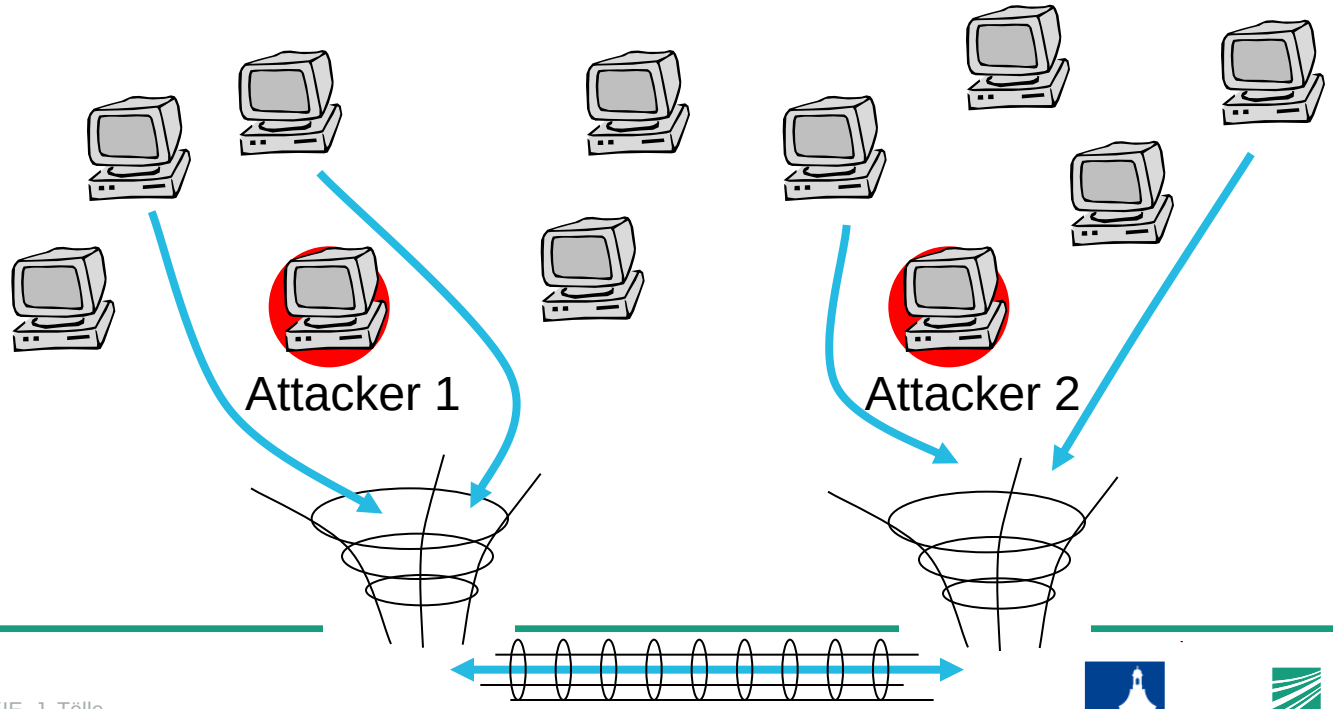
- wiretap the communication,
- (selectively) drop packets,
- send forged answers.



A Selection of Known Attacks: MANET Wormholes

A Wormhole is an attack against the routing mechanism of Mobile Ad-hoc networks (MANETs)

The blackhole idea can be extended to a so-called **wormhole** when two independent MANET nodes cooperate and exchange data packets via an out-of-band channel.



universitätbonn

Fraunhofer FKIE

A Selection of Known Attacks: Cross Site Scripting – XSS

Cross Site Scripting means exploiting a vulnerability trusting untrustworty data.

Example: user input may be malformed.
„<script> *code; code;* </script>“

Both client (e.g. web browser) and server (web server) can be vulnerable.

Related attack: SQL injection

Sending SQL statements with special characters (e.g. **;** or ****) directly to the server.
A server might return additional contents of the database.

Protection:

- **Never trust** external input or code.
- Check whether the input is composed according to the **specification**.
- Filtering known attacks is **not sufficient**!

Never trust the client!

Reference: http://www.bsi.de/literat/studien/websec/WebSec.pdf

A Selection of Known Attacks: Shellshock

Expoiting shell vulnerabilty

Published in 2014, already existed for a quarter of a century…

Targeted to UNIX bash shell

Invalid check of environment variables, interpreted as functions
“processes trailing strings after certain malformed function definitions in the values of environment variables, which allows remote attackers to write to files or possibly have unknown other impact via a crafted environment”

(Source: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7169)

Vulnerability was exploited within hours after disclosure and availability of patches!

See CVE-2014-6271, CVE-2014-7169

A Selection of Known Attacks: ???

Exploiting human laziness…

Not yet finally confirmed:
"Lemotdepassedeyoutube"

http://www.arretsurimages.net/breves/2015-04-11/Lemotdepassedeyoutube-TV5Monde-admet-une-bourde-id18809

http://tvmag.lefigaro.fr/le-scan-tele/insolite/2015/04/10/28009-20150410ARTFIG00214-les-mots-de-passe-de-tv5-monde-devoiles-sur-france-2.php

universitätbonn

Fraunhofer FKIE

A Selection of Known Attacks: Some really old classics…

- **Source Routing .....** Enforcing a communication channel can help attackers
- **SNMP .....** No encryption in SNMPv1, just „community string“
- **NFS .....** Allows modification of system files
- **X11 .....** Interception of in- and output
- **sendmail .....** Programming errors allow access to system files
- **operating system ...** Permanently new flaws, e.g. in the network stack

Summary

Summary

- Internet history: ARPAnet and security
- Security Risks
- Spoofing
- Brute Force Attacks
- Denial of Service
- MANET attacks
- and many more…