

Internet Security

Prof. Dr. Thomas Zinner
zinner@net.t-labs.tu-berlin.de
<http://www.net.t-labs.tu-berlin.de/>

Prof. Dr. Jean-Pierre Seifert
jpseifert@sec.t-labs.tu-berlin.de
<http://www.sec.t-labs.tu-berlin.de/>



Slides credits to Anja Feldmann and Jean-Pierre Seifert

1

General information

- ❑ Area: BKS – Hauptstudium Vertiefer
 - Is part of modules from SECT and INET
- ❑ Time: Wednesday: 12:00 – 14:00
- ❑ Room: EW 202
- ❑ Language
 - English (questions can be asked in German as well!)
- ❑ Web site
 - At INET or SECT
- ❑ ISIS:
 - <https://isis.tu-berlin.de/course/view.php?id=12435>
- ❑ Mailing list
 - Use ISIS

2

General information

- Exam
 - For those that need it
 - Oral or written exam after semester end (depends on # of participants)

- Prerequisite: some knowledge of
 - How the Internet works
 - How operating systems work
 - Little bit of undergraduate math for cryptography

- Additional contact persons:
 - Damien Foucard (INET) and Jan Nordholz (SECT)

3

What is this course about?

- Network security? Not quite!

- Focus:
 - Security of networked applications
 - Security of Web browsers
 - Protection of network infrastructure
 - Firewalls
 - Intrusion detection

4

Topics

- ❑ **Basics of secure network protocol design**
 - Using cryptography (not a cryptography class!)
 - The role of correct software

- ❑ **Practical focus**
 - This is not a pure academic-style course
 - You'll see real security holes
 - A lot of (in)security is about doing the unexpected
 - „Think sideways“

5

How to think about insecurity

- ❑ Bad guys don't follow rules
- ❑ Need to understand what sort of attacks are possible to compromise a system
 - Prerequisite to understand what to protect in a system!
- ❑ **This is not the same as actually launching them!**
 - Taking a security class is not an excuse for hacking
 - Hacking is any form of unauthorized access, including exceeding authorized permissions
 - The fact that a file or computer is not properly protected is no excuse for unauthorized access

6

Reading

- Kaufman, Perlman, and Spencer.
Network Security: Private Communication in a Public World,
Second Edition, Prentice Hall, 2002
- Cheswick, Bellovin, and Rubin.
Firewalls and Internet Security: Repelling the Wily Hacker,
Second Edition, Addison-Wesley Professional 2003
- Garfinkel, Spafford, and Schwartz.
Practical Unix & Internet Security,
O'Reilly Media, Inc.
- Matt Bishop.
Computer Security: Art and Science,
Addison-Wesley Professional 2002
- ... (see Web)
- **Research papers** (see Web)

7

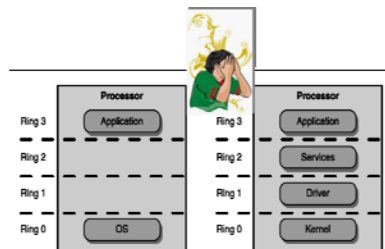
Network security

Overview

8

Dichotomy: Hosts

- ❑ Is (or can be) well-controlled
- ❑ There are well-developed authentication and authorization models
- ❑ Strong notion
 - Of „privileged“ state
 - What programs can use/do



9

Dichotomy: Networks

- ❑ None of the above
- ❑ Anyone can (and does) connect to the network
- ❑ Connectivity can only be controlled in very small, well-regulated environments, and maybe not even then
- ❑ Different OS have different – or no – notions of userIDs and privileges

=> notions of privilege is missing

10

Networking

- Networks interconnect
- Networks always interconnect
- Interconnections happen everywhere, but mainly at the edges

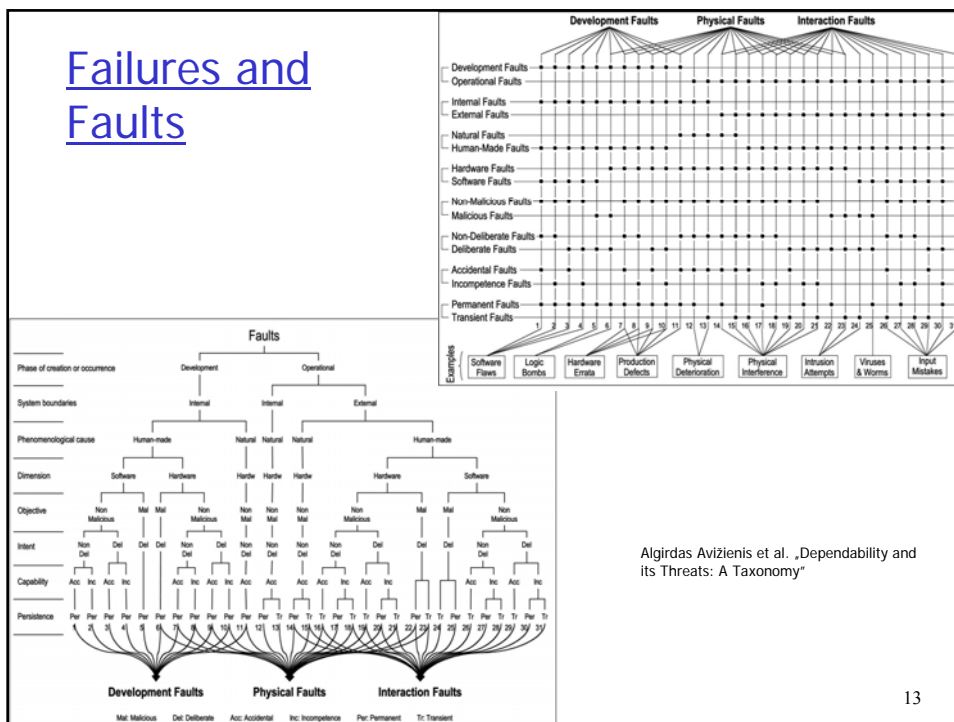
11

Failures

- Benign failures
 - Most network failures are benign
 - The Internet allow for such failures
 - Data corruption
 - Timeouts
 - Dead hosts
 - Routing problems
 - ...
- Rule of thumb:
 - Anything that can happen by accident can happen malicious
 - > much more dangerous!

12

Failures and Faults



13

Principle: Trust nothing

- ❑ A host can/should trust **nothing** that comes over the wire!
- ❑ Any desired protections have to be explicitly supplied
- ❑ There may be help from lower layers that supply protection
 - Yet those layers have to be based on the same principle!
 - Research on such lower layer protection is a very hot topic and far from being solved!

14

Attitude question

- ❑ Unproductive attitudes
 - „Why would anyone ever do that?“
 - „That attack is too complicated“
 - „No one knows how this system works, so they can't attack it“
- ❑ Better attitudes
 - „Programming Satan's Computer“ (Ross Anderson)
 - „Assume that serial number 1 of any device is delivered to the enemy“
 - „You hand your packets to the enemy to deliver; you receive all incoming packets from the enemy“

15

Network security tools

- ❑ Cryptography
- ❑ Network-based access control (firewalls and more)
- ❑ Monitoring

- ❑ Protocol analysis by formal verification

- ❑ Paranoid design!

16

Protocol design

- ❑ Heavy use of crypto and authentication
- ❑ Ensure that sensitive fields are protected
- ❑ Make authentication bilateral
- ❑ Figure out the proper authorization
- ❑ Defend against
 - Eavesdropping
 - Modification
 - Deletion
 - Replay
 - And combinations thereof

17

Buggy software

- ❑ Most network security holes are due to **buggy code**
- ❑ A buggy network-connected program is an insecure one
- ❑ **Correct coding counts for a lot!**

18

Buggy software: Heartbleed

- ❑ Security bug in the OpenSSL cryptography library
 - ❑ TLS heartbeat extension
 - ❑ Periodic check if connection is active by sending up to 16kByte data
 - ❑ Receiver responds with same data fragment
 - ❑ Missing bounds check results in buffer over-read (→ allows to read data from memory)
- ❑ Implications
 - ❑ Possibility to read usernames, passwords, etc...
 - ❑ Software update necessary
 - ❑ Bug reported on April 1; 1.5% of top 800k TLS webpages still vulnerable on May 20

19

Course overview

- ❑ Introduction
 - Attacks and threats, cryptography overview
 - Authentication (Kerberos, SSL)
- ❑ Applications
 - Web, browser, email, ssh
- ❑ Lower layer network security
 - NAT, (IPsec), firewalls
- ❑ Monitoring / information gathering
 - Intrusion detection, network scans
- ❑ Availability
 - Worms, denial of service, network infrastructure

20