

Netzwerksicherheit [NetSec]

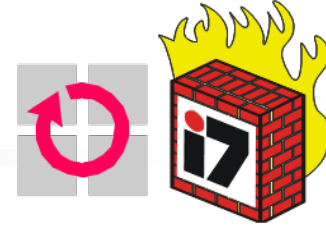
Dr.-Ing. Falko Dressler

Computer Networks and Communication Systems
<http://www7.informatik.uni-erlangen.de/~dressler/>
dressler@informatik.uni-erlangen.de

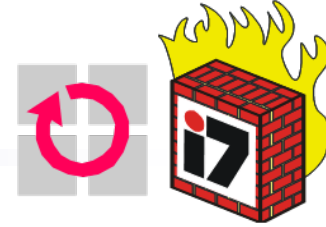
Systemsicherheit [SysSec]

Dr.-Ing. Jürgen Kleinöder

Distributed Systems and Operating Systems
<http://www4.informatik.uni-erlangen.de/~jklein/>
klein@informatik.uni-erlangen.de



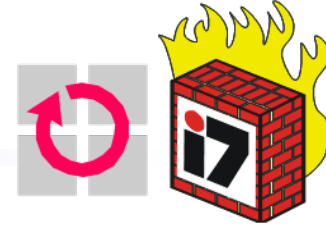
- ❑ **Cryptography**
Basics, symmetric cryptography, asymmetric cryptography
- ❑ **Cryptographic Techniques**
Modification check values, random number generation
- ❑ **Security Protocols**
Cryptographic protocols, integrating security services into communication architectures
- ❑ **Security in Communication Protocols**
Medium access (PPP, 802.1x, WLAN), network layer (IPSec), transport/session layer (SSL, TLS)
- ❑ **Security in Mobile Networks**
Location privacy, pseudonyms, mix networks
- ❑ **Attack Detection**
Attack detection and prevention, IP traceback



Security in the context of operating systems

- ❑ **Authentication**
- ❑ **Authorization**
Access Control Lists, Capabilities
- ❑ **Attack concepts and system weaknesses**
Trojan horses, worms, privileged applications (s-bit problem)
- ❑ **Security concepts**
Sandboxing, mandatory access control (AppArmor, SELinux),
protection domains (Pentium architecture),
secure booting, TPA, Palladium, SmartCards
secure administration, tools for enhancing security

Exercises

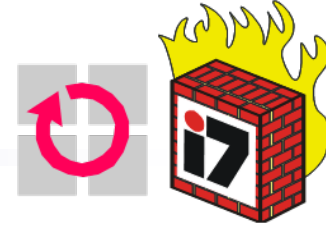


- ❑ Organization
 - ❑ Consolidation of course topics, extended studies
 - ❑ Working groups of 2-3 students
 - ❑ Mix of theoretic and practical exercises

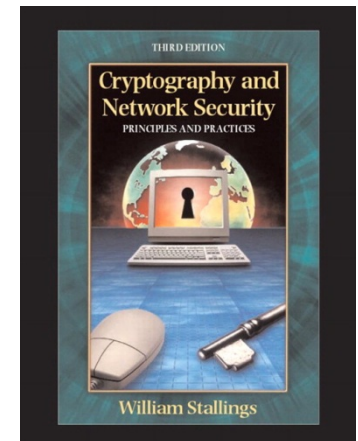
- ❑ Overview
 - ❑ Lab training
 - ❑ Cryptographic algorithms
 - ❑ Certificates, PKI
 - ❑ Security analysis
 - ❑ Network monitoring and analysis
 - ❑ VPN, Firewalls (Linux, Cisco)
 - ❑ WLAN security (how to access secured WLANs)
 - ❑ Attack detection



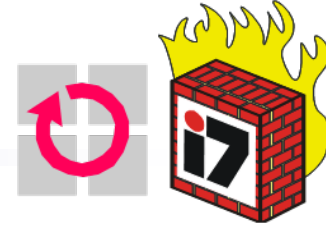
Course Overview



- ❑ Material - NetSec
 - ❑ Günter Schäfer, “*Netzicherheit - Algorithmische Grundlagen und Protokolle*,” dpunkt Verlag, 2003. (an English version is available)
 - ❑ William Stallings, “*Cryptography and Network Security: Principles and Practice*,” Prentice Hall, 3rd ed, 2005.
- ❑ Material – SysSec follows
- ❑ News, updates, handouts, ...
 - <http://www7.informatik.uni-erlangen.de/~dressler/lectures/netzwerksicherheit-ws0708/>
 - http://www4.informatik.uni-erlangen.de/Lehre/WS07/V_SYSSEC/
- ❑ Persons
 - ❑ Dr.-Ing. Falko Dressler (NetSec: lecture and exercises)
 - ❑ Tobias Limmer (NetSec: exercises)
 - ❑ Dr.-Ing. Jürgen Kleinöder (SysSec: lecture)
 - ❑ Michael Gernoth, Reinhard Tartler (SysSec: exercises)



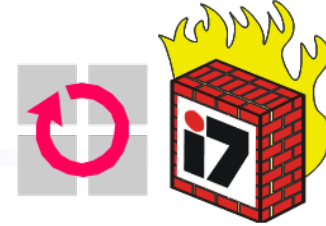
Course Organization



- ❑ Lecture
 - ❑ NetSec: Monday, 14:15-15:45, H5
 - ❑ SysSec: Thursday, 10:15-11:45, H4
 - ❑ Common lectures for NetSec and SysSec on Monday **and** Thursday up to November 5th

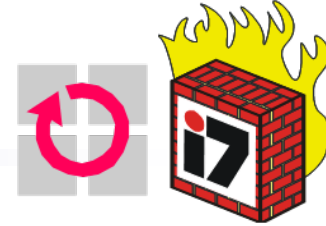
- ❑ Exercises (in groups à 2-3 students) starting in November!
 - ❑ NetSec
 - Tuesday, 14:15-15:45, 01.153 CIP-Pool
 - Tuesday, 16:15-17:45, 01.153 CIP-Pool
 - Thursday, 16:15-17:45, 01.153 CIP-Pool
 - ❑ SysSec
 - Tuesday, 10:15 – 11:45, 0.156
 - Wednesday, 12:00 – 14:00, 01.153 CIP-Pool

- ❑ ... see web page for more up-to-date information



- ❑ Examination
 - ❑ Computer science
 - NetSec in combination with [KS] (main subject: communication systems)
 - NetSec in combination with SysSec (main subject: operating systems)
 - SysSec in combination with Operating Systems or with Distributed Systems (main subject: operating systems)
 - ❑ CE / IuK: oral examination
 - ❑ Exercises are relevant!
- ❑ “Schein”
 - ❑ Oral examination at the end of the semester
 - ❑ “benoteter Schein”: successful processing of ALL exercises, the grade results form the oral examination
 - ❑ “unbenoteter Schein”: successful processing of ALL exercises, at least 50% must be achieved in the oral examination

NetSec - General Course Bibliography



- [Amo94] E. G. Amorosi. *Fundamentals of Computer Security Technology*. Prentice Hall, 1994.
- [Cha95] Brent Chapman and Elizabeth Zwicky. *Building Internet Firewalls*. O'Reilly, 1995.
- [For94b] Warwick Ford. *Computer Communications Security - Principles, Standard Protocols and Techniques*. Prentice Hall, 1994.
- [Gar96] Simson Garfinkel and Gene Spafford. *Practical Internet & Unix Security*. O'Reilly, 1996.
- [KPS95] C. Kaufman, R. Perlman und M. Speciner. *Network Security – Private Communication in a Public World*. Prentice Hall, 1995.
- [Men97a] A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press Series on Discrete Mathematics and Its Applications. CRC Press, 1997.
- [Sch96] B. Schneier. *Applied Cryptography - Second Edition: Protocols, Algorithms and Source Code in C*. John Wiley & Sons, 1996.
- [Sta98a] W. Stallings. *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 2nd ed, 1998.
- [Sti95a] D. R. Stinson. *Cryptography: Theory and Practice (Discrete Mathematics and Its Applications)*. CRC Press, 1995.
- [Sch03] G. Schäfer. *Netzicherheit – Algorithmische Grundlagen und Protokolle*. dpunkt.verlag, 2003.