

# IT-Sicherheit

## - Sicherheit vernetzter Systeme -

Priv.-Doz. Dr. Helmut Reiser  
Dr. Wolfgang Hommel

Zeit: Montags, 15:15 – 17:45

Ort: Geschwister-Scholl-Platz 1,  
Hörsaal A 014



## Inhaltsübersicht

1. Einleitung
  - Internet Worm versus Slammer
2. Grundlagen
  - OSI Security Architecture und Sicherheitsmanagement
  - Begriffsbildung
  - Security versus Safety
3. Security Engineering
  - Vorgehensmodell: Bedrohungs-/ Risikoanalyse
  - Sicherheitsprobleme: Handelnde Personen, Notationen
  - Bedrohungen (Threats), Angriffe (Attacks), Schwächen (Vulnerabilities), z.B.:
    - Denial of Service
    - Malicious Code
    - Hoax, SPAM
    - Mobile Code
    - Buffer Overflow
    - Account / Password Cracking
    - Hintertüren / Falltüren
    - Rootkits
    - Sniffer
    - Port Scanner
4. Kryptologie, Grundlagen
  - Rechtliche Regelung: StGB
  - Top Cyber Security Risks
  - Sicherheitsanforderungen
  - Terminologie, Notationen
  - Steganographie
  - Kryptographie, Begriffe und Definitionen
  - Kryptoanalyse
5. Symmetrische Kryptosysteme
  - Data Encryption Standard (DES)
  - Advanced Encryption Std. (AES)



## Inhaltsübersicht (2)

### 6. Asymmetrische und Hybride Kryptosysteme

- RSA
- Schlüssellängen und Schlüsselsicherheit
- Hybride Systeme
- Digitale Signatur

### 7. Kryptographische Hash Funktionen

- Konstruktion von Hash-Fkt.
- Angriffe auf Hash-Fkt.
- MD4, MD5
- Whirlpool Hashing

### 8. Sicherheitsmechanismen

- Vertraulichkeit
- Integrität
- Identifikation
- Authentisierung
- Autorisierung und Zugriffskontrolle

### 9. Netz Sicherheit - Schicht 2: Data Link Layer

- Point-to-Point Protocol (PPP)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- IEEE 802.1x

### 10. Schicht 2: WLAN Sicherheit

- WEP
- WPA
- WPA2



## Inhaltsübersicht (3)

### 11. Schicht 3: Network Layer

- IP Gefahren und Schwächen
- IPSec
- Schlüsselverteilung mit IKE

### 12. Schicht 4 - Transport Layer

- TCP / UDP
- Secure Socket Layer / Transport Layer Security (SSL/TLS)

### 13. Schicht 7: Secure Shell (ssh)

- SSH v1 versus SSH v2
- Protokoll-Architektur

### 14. Firewalls und Intrusion Detection Systeme

- Firewall-Klassen
- Firewall-Architekturen
- IDS-Arten

### 15. Beispiele aus der Praxis (LRZ)

### 15. Anti-Spam Maßnahmen

### 16. Beispiele aus der Praxis des LRZ

- Struktur des MWN
- Virtuelle Firewalls
- Nat-O-Mat
- NYX

### 17. Datenschutz

- Persönlichkeitsrechte u. Datenschutz
- Datenspuren und Schutzmaßnahmen

### ● Was ist nicht Gegenstand dieser Vorlesung

- Fortgeschrittenen kryptographische Konzepte ⇒ Vorlesung Kryptologie
- Formale Sicherheitsmodelle und Sicherheitsbeweise



# Einordnung der Vorlesung

## ■ Bereich

- Systemnahe und technische Informatik (ST), Anwendungen der Informatik (A)

## ■ Hörerkreis (LMU)

- Informatik Diplom
- Informatik Master
- Informatik Bachelor („Vertiefende Themen der Informatik für Bachelor“)

## ■ Voraussetzungen

- Grundlegende Kenntnisse der Informatik
- Rechnernetze (wünschenswert und hilfreich)

## ■ Relevanz für Hauptdiplomprüfung

- Vorlesung plus Übung: 3 + 2 SWS
- Credits: 6 ECTS Punkte



# Termine und Organisation

## ■ Vorlesungstermine und Raum:

- Montags von 15:15 – 17:45, Raum A 014 (Geschwister-Scholl Pl. 1)

## ■ Übung; Beginn 04.11.2009

- Mittwochs von 14:15 - 15:45 in E 006 (Geschwister-Scholl Pl. 1)

### □ Übungsleitung:

Stefan Metzger, [metzger@lrz.de](mailto:metzger@lrz.de)

Tobias Lindinger, [lindinge@nm.ifi.lmu.de](mailto:lindinge@nm.ifi.lmu.de)

## ■ Skript:

- Kopien der Folien (pdf) zum Download
- <http://www.nm.ifi.lmu.de/itsec>

## ■ Kontakt:

Helmut Reiser	Wolfgang Hommel
<a href="mailto:reiser@lrz.de">reiser@lrz.de</a>	<a href="mailto:hommel@lrz.de">hommel@lrz.de</a>
LRZ, Raum I.2.070	LRZ, Raum I.1.107

## ■ Sprechstunde:

Montags 11:00 bis 12:00 im LRZ; nach der Vorlesung oder nach Vereinbarung



# Schein

- Anmeldung zur **Übung** und Klausur
- Prüfung zum Erhalt des Scheins
- Notenbonus durch Hausaufgaben
  - Übungsblatt enthält Hausaufgabe
  - Hausaufgabe bei der Übung abgeben
  - Es werden 4 Blätter / Aufgaben gewählt und korrigiert

Anzahl korrekter Lösungen	Bonus	Beispiel
4	2 Stufen	Vorher: 3.0; Nachher: 2.3
2 oder 3	1 Stufe	Vorher: 3.0; Nachher: 2.7
1	0 Stufen	Vorher: 3.0; Nachher: 3.0

- Bonussystem nur wirksam bei **bestandener** Prüfung
- Beste Note 1.0



## Literatur: IT-Sicherheit



- Claudia Eckert  
**IT-Sicherheit**  
5. Auflage,  
Oldenbourg-Verlag, 2007  
ISBN 3486578510  
59,80 €



## Literatur: IT-Sicherheit

Helmar Gerloni  
Barbara Oberhaidinger  
Helmut Reiser  
Jürgen Plate

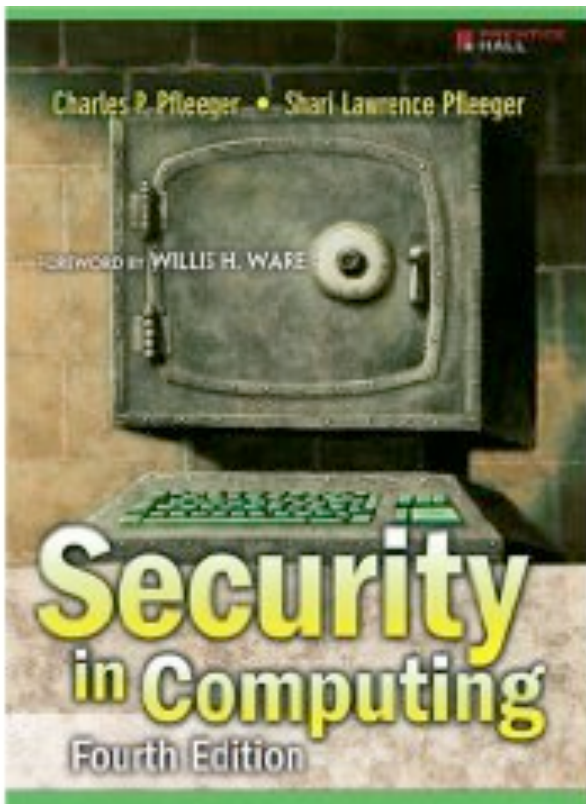
### Praxisbuch Sicherheit für Linux-Server und -Netze



- Helmar Gerloni, Barbara Oberhaidinger, Helmut Reiser, Jürgen Plate  
**Praxisbuch Sicherheit für Linux-Server und -Netze**  
Hanser-Verlag, 2004  
ISBN 3-446-22626-5  
34,90 €



## Literatur: IT-Sicherheit

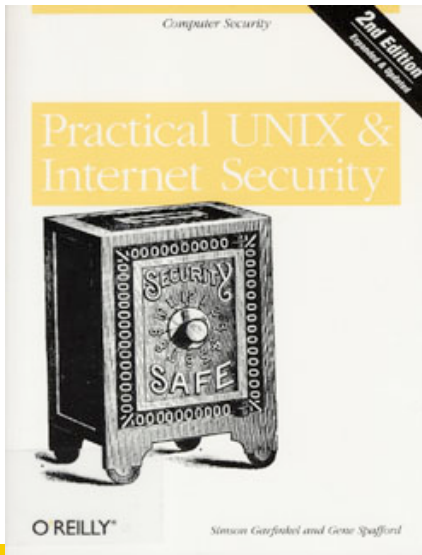


- Charles P. Pfleeger, Shari L. Pfleeger  
**Security in Computing**  
4. Auflage,  
Pearson, 2006 / 2008  
ISBN 978-8120334151  
70 \$

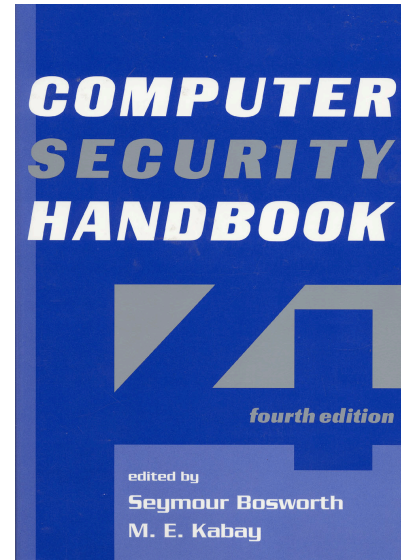


# Literatur: IT-Sicherheit

- Simson Garfinkel, Gene Spafford  
**Practical UNIX & Internet Security**  
O'Reilly, 2003  
ISBN 0596003234  
ca. 50 €



- Seymour Bosworth, M.E. Kabay  
**Computer Security Handbook**  
John Wiley & Sons, 2003  
ISBN 0-471-41258-9  
ca. 90 – 100 €



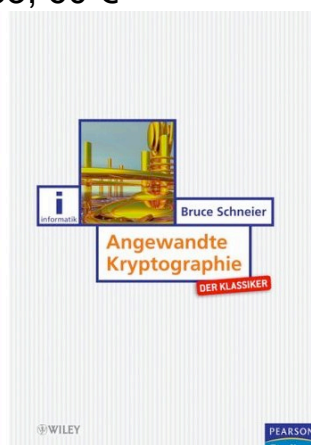
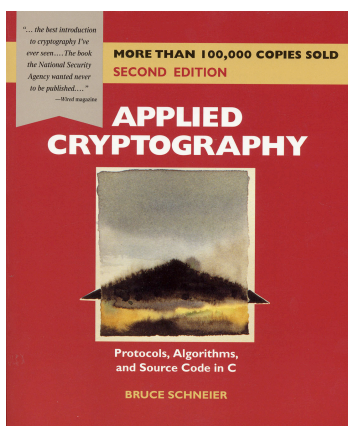
© Helmut Reiser, LRZ, WS 09/10

IT-Sicherheit

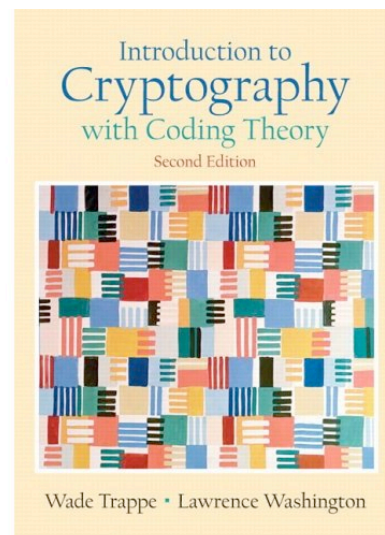
11

# Literatur: Kryptologie

- Bruce Schneier  
**Applied Cryptography**  
John Wiley & Sons, 1996  
ISBN 0-471-11709-9  
69 €  
**Angewandte Kryptographie**  
Pearson Studium, 2005  
ISBN 3827372283, 60 €



- Wade Trappe, Lawrence C. Washington  
Washington  
**Introduction to Cryptography with Coding Theory**  
Prentice Hall, 2005  
ISBN 978-0131862395  
83 €



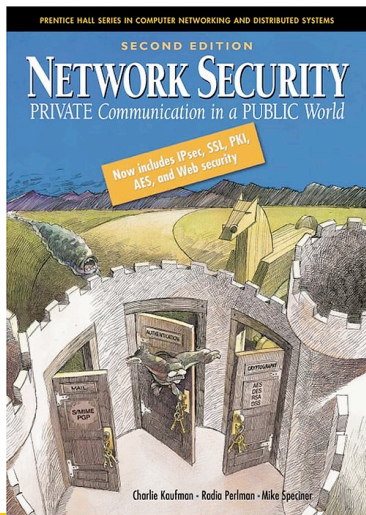
© Helmut Reiser, LRZ, WS 09/10

IT-Sicherheit

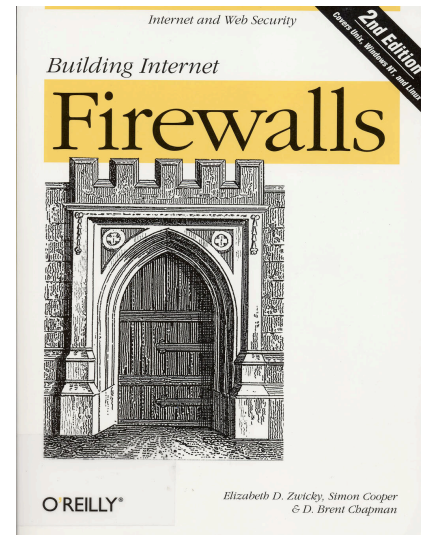
12

# Literatur: Firewalls, Netzsicherheit

- Charly Kaufman, Radia Perlman, Mike Speciner  
**Network Security**, 2nd Ed.  
Prentice Hall, 2002  
ISBN 0-13-046019-2  
ca. 54 €



- Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman  
**Building Internet Firewalls**  
O'Reilly, 2002  
ISBN 1-56592-871-7  
ca. 50 €



© Helmut Reiser, LRZ, WS 09/10

IT-Sicherheit

13

## Literaturliste

- Eine umfangreichere Literaturliste wird im Web zur Verfügung gestellt:

[www.nm.ifi.lmu.de/itsec](http://www.nm.ifi.lmu.de/itsec)

## Weitere Veranstaltungen in diesem Semester

### ■ Vorlesungen:

- Grid Computing (Prof. Dr. Kranzlmüller, Dr. M. Schiffers)  
Mittwochs 9:00 – 12:00, LMU Hauptgebäude A017  
[www.nm.ifi.lmu.de/grid/](http://www.nm.ifi.lmu.de/grid/)
- IT-Management (Prof. Dr. Kranzlmüller, Dr. T. Schaaf)  
Donnerstags 14:00-17:00; 2. Semesterhälfte Dienstags 14:00-16:00  
[www.nm.ifi.lmu.de/itmgmt/](http://www.nm.ifi.lmu.de/itmgmt/)

### ■ Praktika:

- Rechnernetze (Prof. Dr. Kranzlmüller, Dr. V. Danciu, F. Liu, M. Metzker)  
[www.nm.ifi.lmu.de/rnp](http://www.nm.ifi.lmu.de/rnp)

### ■ Kompaktseminar:

- Prozessorientiertes IT-Service Management (R. Kuhlig, Dr. M. Brenner, Dr. T. Schaaf, Prof. Dr. Kranzlmüller),  
[www.nm.ifi.lmu.de/itsm](http://www.nm.ifi.lmu.de/itsm)



## Weitere Veranstaltungen in diesem Semester

### ■ Diplomarbeiten:

[www.nm.ifi.lmu.de/teaching/Ausschreibungen/Diplomarbeiten](http://www.nm.ifi.lmu.de/teaching/Ausschreibungen/Diplomarbeiten)

### ■ Fortgeschrittenenpraktika, Systementwicklungsprojekte

[www.nm.ifi.lmu.de/teaching/Ausschreibungen/Fopras](http://www.nm.ifi.lmu.de/teaching/Ausschreibungen/Fopras)





# Forschung: MNM Team



**MNM**  
TEAM  
MUNICH NETWORK MANAGEMENT TEAM



der Bundeswehr  
*Universität*  *München*

