



Universität Trier



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

Vorlesung SS 2001: “Sicherheit in offenen Netzen“

Prof. Dr. Christoph Meinel

Informatik, Universität Trier & Institut für Telematik, Trier



INHALTSANGABE

0. Einführung

I. Internet- und Intranet-Sicherheit: Risiken und Angriffspunkte

1. Risikoanalyse und Computerkriminalität
2. Architektur von Internet und Intranets
3. Schwachstellen und Angriffspunkte

II. Internet- und Intranet-Sicherheit: Konzepte und Maßnahmen

4. Sicherheitsziele und Sicherheitsprotokolle
5. Werkzeuge und Verfahren aus der Kryptographie
6. Wichtige Sicherheitsprotokolle und ihre Implementierung
7. Patente und Produkte
8. Putting all together: Sicherheitsarchitektur



Universität Trier



Institut für Telematik
unter Betreuung der
Fraunhofer Gesellschaft

1. Risikoanalyse und Computerkriminalität

- 1.1 Risikoanalyse
- 1.2 Computerkriminalität
- 1.3 Hacker und Viren



Universität Trier



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

2. Architektur von Internet und Intranets

- 2.1 Internet Protocol (IP)
- 2.2 Transmission Control Protokoll (TCP)
- 2.3 User Data Protocol (UDP)
- 2.4 Internetprotokolle für serielle Leitungen
- 2.5 Internet Domain-Name Service (DSN)
- 2.6 Internet Protocol Next Generation (IPv6)
- 2.7 Netze mit mehreren Standorten
- 2.8 World Wide Web
- 2.9 Elektronische Post
- 2.10 Internet News
- 2.11 FTP - File Transport Protocol
- 2.12 Telnet
- 2.13 LDAP
- 2.14 Multimedia



Universität Trier



Institut für Telematik
unter Betreuung der
Fraunhofer Gesellschaft

3. Schwachstellen und Angriffspunkte

- 3.1 Sicherheitsrisiko: Mensch
- 3.2 Sicherheitsrisiko: Netzwerk und Internet
- 3.3 Sicherheitsrisiko: Anwendungen
- 3.4 Sicherheitsrisiko: Betriebssysteme (Unix/Linux, Windows NT/2000)
- 3.5 Sicherheitsrisiko: World Wide Web
- 3.6 Viren, Würmer und Trojanische Pferde



Universität Trier



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

4. Sicherheitsziele und Sicherheitsprotokolle

4.1 Sicherheitsziele

(Vertraulichkeit, Integrität, Authentizität, Nichtabstreitbarkeit)

4.2 Sicherheitsprotokolle



Universität Trier



Institut für Telematik
unter Betreuung der
Fraunhofer Gesellschaft

5. Werkzeuge und Verfahren aus der Kryptographie

5.1 Mathematische Grundlagen

(Wahrscheinlichkeitsrechnung, Informationstheorie
Komplexitätstheorie, Zahlentheorie)

5.2 Zahlentheoretische Referenzprobleme

(Faktorisierung, Diskreter Logarithmus
Primzahltest und Primzahlgenerierung, Zufällige Bitfolgen)

5.3 Algorithmen zur symmetrische Verschlüsselung

5.4 Algorithmen zur asymmetrische Verschlüsselung

5.5 Hash-Funktionen



Universität Trier



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

6. Wichtige Sicherheitsprotokolle und ihre Implementierung

6.1 Protokolle zur Sicherung der Integrität

6.2 Protokolle zur Identifikation und Entity Authentikation

6.3 Protokolle zur Digitalen Signatur

6.4 Protokolle zur Schlüsselerzeugung

6.5 Protokolle zum Schlüsselmanagement



Universität Trier



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

7. Implementationen und Produkte

7.1 Algorithmen im Vergleich

7.2 Verbreitete Implementationen

7.3 Patente und Standards



Universität Trier



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

8. Sicherheitsarchitekturen

- 8.1 Planung und Implementation
- 8.2 Zentrale Komponenten: Firewalls und Lock-Keeper
- 8.3 Überwachung: Intrusion Detection Systeme
- 8.4 Standards und Organisationen



Universität Trier



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

IT-Sicherheitspraktikum



Universität Trier



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

Scheinkriterien

- 1.) Mindestens 50% der möglichen Übungsaufgabenpunkte
in den beiden Semesterhälften
- 2.) Erfolgreiche Teilnahme an Übung und Praktikum
- 3.) Rücksprache



Universität Trier



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

Homepage zur Vorlesung

1.) Anmeldung zur Übung:

<http://eris.uni-trier.de/cgi-bin/cgiwrap/lcms/index.pl>

2.) Übungshomepage:

<http://www.informatik.uni-trier.de/~sack/Sicherheit.html>