

Netzwerksicherheit (NWS)

Prof. Dr. Norbert Pohlmann

Fachbereich Informatik

Verteilte Systeme und Informationssicherheit



Inhalt

- **Einordnung**
- **Lernziele**
- **Vorlesungsinhalt**
- **Themen für Ausarbeitungen und Vorträge (Übung)**
- **Praktikum**
- **Unterlagen / Literatur**

■ Einordnung

- Lernziele
- Vorlesungsinhalt
- Themen für Ausarbeitungen und Vorträge (Übung)
- Praktikum
- Unterlagen / Literatur

Netzwerksicherheit (NWS)

→ Einordnung

■ Zielgruppe:

- Studierende des Bachelorstudiengangs mit der Vertiefungsrichtung „Internet und Mobile Netze“ (NWS)
- Wahlmodul für die anderen

■ Stundenumfang:

- 4 SWS (2V+1Ü+1P)

■ Voraussetzungen

- Rechnernetze 1 oder Netzwerke
- Betriebssysteme
- Die Vorlesung kann aber auch ohne diese Vorkenntnisse sinnvoll gehört werden!

Inhalt

- Einordnung
- **Lernziele**
- Vorlesungsinhalt
- Themen für Ausarbeitungen und Vorträge (Übung)
- Praktikum
- Unterlagen / Literatur

Netzwerksicherheit (NWS)

→ Lernziele

- Gutes Verständnis von möglichen Angriffen und geeigneten Gegenmaßnahmen
- Erlangen der Kenntnisse über den Aufbau, die Prinzipien, die Architektur und die Funktionsweise von Sicherheitskomponenten und -systemen
- Sammeln von Erfahrungen bei der Ausarbeitung und Präsentation von neuen Themen aus dem Bereich IT-Sicherheit
- Gewinnen von praktischen Erfahrungen über die Nutzung und die Wirkung von Sicherheitssystemen
- Erleben der Notwendigkeit und Wichtigkeit der IT-Sicherheit

Inhalt

- Einordnung

- Lernziele

- **Vorlesungsinhalt**

- Themen für Ausarbeitungen und Vorträge (Übung)

- Praktikum

- Unterlagen / Literatur

Netzwerksicherheit (NWS)

→ Vorlesungsinhalt (1/3)

■ **Einführung**

- IT-Sicherheit als Wirkungs- und Handlungszusammenhang
- Sicherheitsbedürfnisse, Bedrohungen, Angriffe
- Schadenskategorien, Eintrittswahrscheinlichkeiten

■ **Kryptographie und Grundlagen**

- Grundlagen der Verschlüsselung
- Elementarverschlüsselungen
- Private-Key-Verfahren, Public-Key-Verfahren, Kryptoanalyse,
- Hashfunktionen, Schlüsselgenerierung

■ **Internet-Frühwarnsysteme**

- Internet-Analyse-System
- Internet-Verfügbarkeits-System

Netzwerksicherheit (NWS)

→ Vorlesungsinhalt (2/3)

- **Authentikationsverfahren**
 - Grundsätzliche Prinzipien
 - unterschiedliche Algorithmen und Verfahren

- **Biometrische Verfahren**
 - Mechanismen und Prinzipien
 - Unterschiedliche Verfahren

- **Sicherheitsmodule**
 - SmartCards
 - TPMs
 - high-security und high-performance Lösungen

Netzwerksicherheit (NWS)

→ Vorlesungsinhalt (3/3)

- **Sicherheitsplattform (Trusted Computing)**
 - Architektur
 - Mechanismen

- **Anti-Mailware-Systeme**
 - Viren, Würmer und trojanische Pferde
 - Lokale und zentrale Schutzmaßnahmen

- **Verschlüsselungssysteme**
 - Dateiverschlüsselung
 - Verzeichnisverschlüsselung
 - Festplattenverschlüsselung

Inhalt

- Einordnung
- Lernziele
- Vorlesungsinhalt
- **Themen für Ausarbeitungen u. Vorträge (Übung)**
- Praktikum
- Unterlagen / Literatur

Themen für Ausarbeitungen und Vorträge (Übung)

- Ausarbeitungen und Vortrag sind Voraussetzung für die Klausur!
- Mögliche Themen sind z.B.:
 - Verbreitung von Viren und Verbreitung von Signaturen
 - Zeitfenster und weitere Lösungen
 - Botnetze
 - Trojaner
 - Honey Pots
 - Die 10 größten Probleme im Internet: genauer Beschreibung und Diskussion, warum sie ein Problem sind, und wie groß ist der potentielle Schaden (2 Personen)
 - ...
 - weitere Themen, für die Sie sich interessieren, nach Absprache

Inhalt

- Einordnung
- Lernziele
- Vorlesungsinhalt
- Themen für Ausarbeitungen und Vorträge (Übung)
- **Praktikum**
- Unterlagen / Literatur

Netzwerksicherheit (NWS)

→ Praktikum

- Das Praktikum ist Voraussetzung für die Klausur!
- Themen des Praktikums sind:
 - **Kryptographie und Kryptoanalyse**
(Termine werden in der Vorlesung verabredet)
 - **Analysen mit dem IAS**
 - in einer Kleingruppe mit Ausarbeitung der Ergebnisse
 - **Einrichtung einer Sicherheitsplattform**
 - in einer Kleingruppe mit Ausarbeitung der Ergebnisse
- Das Praktikum findet im Raum P 1.05 statt.

Inhalt

- Einordnung
- Lernziele
- Vorlesungsinhalt
- Themen für Ausarbeitungen und Vorträge (Übung)
- Praktikum
- **Unterlagen / Literatur**

Netzwerksicherheit (NWS)

→ Unterlagen

- Folien stelle ich als PDF zur Verfügung
- Web-Server: <http://www.internet-sicherheit.de/institut-lehre.html>
 - Username: student2003
 - Passwort: fuzzy25

Netzwerksicherheit (NWS)

→ Bücher

- N.Pohlmann: „**Firewall-Systeme - Sicherheit für Internet und Intranet, E-Mail-Security, Virtual Private Network, Intrusion Detection-System, Personal Firewalls**“, 5. aktualisierte und erweiterte Auflage, ISBN 3-8266-0988-3, MITP-Verlag, Bonn 2002
- M.a Campo, N.Pohlmann: „**Virtual Private Network (VPN)**“, 2. aktualisierte und erweiterte Auflage, ISBN 3-8266-0882-8; MITP-Verlag, Bonn 2003
- G.Simmons(Hrsg.): „**Contemporary Cryptology - The Science of Information Integrity**“, IEEE Press, New York
- F.P.Heider, D. Kraus, M. Welschenbach: „**Mathematische Methoden der Kryptoanalyse**“, Vieweg Verlag 1985
- A. Beutelspacher, „**Geheimsprachen**“, 1997, Beck'sche Verlagsanstalt
- B. Schneier, „**Applied Cryptography**“, „**Secrets&Lies**“, „**Practical Cryptography**“, John Wiley & Sons
- Klaus Schmeih, „**Kryptographie und PKIs im Internet**“, 2001, dpunkt
- C.Langenbach, O. Ulrich (Hrsg.): „**Elektronische Signaturen - Kulturelle Rahmenbedingungen**“ einer technischen Entwicklung, Springer Verlag, Berlin
- und sehr viele mehr

Netzwerksicherheit (NWS)

→ Zeitschriften

- DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag
- KES - Kommunikations- und EDV-Sicherheit, SecMedia Verlag
- Network Computing - CMP-WEKA Verlag
- GIT - Sicherheit + Management - Magazin für Safety und Security, GIT Verlag
- IT-Sicherheit - Praxis der Daten- und Netzsicherheit, DATAKONTEXT-Fachverlag
- Information Security Bulletin – Deutsche Ausgabe, Fachzeitschrift für Führungskräfte im IT-Sicherheitsbereich, CHI Publishing Ltd.
- WIK – Zeitschrift für die Sicherheit der Wirtschaft, SecMedia Verlag
- www.bsi.de, www.teletrust.de, www.bridge-ca.org, www.regtp.de, ...

Netzwerksicherheit (NWS)

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

norbert.pohlmann@informatik.fh-gelsenkirchen.de

