Netzwerksicherheit A (NWS A)

Prof. Dr. Norbert Pohlmann
Fachbereich Informatik
Verteilte Systeme und Informationssicherheit

Fachhochschule Gelsenkirchen

Inhalt

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

© Prof. Dr. Norbert Pohlmann, Fachhochschule Gelsenkirchen

Inhalt

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

© Prof. Dr. Norbert Pohlmann, Fachhochschule Gelsenkirchen

Netzwerksicherheit A (NWS A)
→ Einordnung

- **Zielgruppe:**
  - Studierende des Diplomstudiengangs
    mit der Vertiefungsrichtung „Internet und Mobile Netze“ (NWS A)
  - NWS A für Masterstudiengang

- **Stundenumfang:**
  - 4 SWS (2V+1Ü+1P)

- **Voraussetzungen**
  - Idealerweise Grundkenntnisse über TCP/IP-Protokolle.
    (Rechnernetze 1 und 2)
  - Die Vorlesung kann aber auch ohne diese Vorkenntnisse sinnvoll gehört werden!

© Prof. Dr. Norbert Pohlmann, Fachhochschule Gelsenkirchen

Inhalt

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

© Prof. Dr. Norbert Pohlmann, Fachhochschule Gelsenkirchen

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

© Prof. Dr. Norbert Pohlmann, Fachhochschule Gelsenkirchen

Inhalt

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

© Prof. Dr. Norbert Pohlmann, Fachhochschule Gelsenkirchen

Netzwerksicherheit A (NWS A)
→ Vorlesungsinhalt (1/5)

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

- ***VPN-Systeme***
  - Ziele und Anwendungsformen, Konzepte von VPNs
  - VPN-Verfahren
  - VPN-Protokolle (IPSec)
  - Schlüsselaustausch – Methoden/Protokolle (IKE)
  - Kombinationsmöglichkeiten VPN und Firewall-Systeme

© Prof. Dr. Norbert Pohlmann, Fachhochschule Gelsenkirchen

Netzwerksicherheit A (NWS A)
→ Vorlesungsinhalt (2/5)

- ***Firewall-Systeme***
  - Ziele von Firewall-Systemen, Definition eines Firewall-Elementes
  - Elemente eines Firewall-Systems:
    Packet Filter, Stateful Inspection, Adaptive Proxies, Application Proxies
  - Konzepte für Firewall-Systeme
  - Möglichkeiten und Grenzen von Firewall-Systemen
  - Realisierungskonzepte, Praktischer Einsatz von Firewall-Systemen
  - Firewall-Sicherheitspolitik
  - Überprüfung von Firewall-Systemen im Betrieb (Audit)
  - Die Wirkung von Firewall-Systemen

- ***Personal Firewall***
  - Ziel einer Personal Firewall, Sicherheitskomponenten
  - Anwendungsbeispiele

© Prof. Dr. Norbert Pohlmann, Fachhochschule Gelsenkirchen

Netzwerksicherheit A (NWS A)
→ Vorlesungsinhalt (3/5)

- ***Digitale Signatur***
  - Gesetzliche Grundlagen
  - Mechanismen und Prinzipien
  - Anwendungsbeispiele

- ***Public-Key-Infrastruktur (PKI)***
  - Mechanismen und Prinzipien
  - Aufgaben und Komponenten einer PKI
  - Modelle von Public-Key Infratrukturen
  - Probleme mit PKIs in der Praxis, Initiativen in diesem Bereich
  - Gesetzliche Grundlagen, Anwendungsbeispiele

- ***E-Mail-Security***
  - Elemente und Prinzipien
  - Konzepte und praktischer Einsatz

© Prof. Dr. Norbert Pohlmann, Fachhochschule Gelsenkirchen

Netzwerksicherheit A (NWS A)
→ Vorlesungsinhalt (4/5)

- ***Secure Socket Layer (SSL), Transport Layer Security (TLS)***
  - Idee
  - Mechanismen
  - Protokolle und
  - Umsetzungskonzepte

- ***Anti-SPAM-Systeme:***
  - Schäden, Prinzipen
  - Technologien

© Prof. Dr. Norbert Pohlmann, Fachhochschule Gelsenkirchen

Netzwerksicherheit A (NWS A)
→ Vorlesungsinhalt (5/5)

- ***Intrusion Detection***
  - Aufbau und Funktionsweise
  - Auswertungskonzepte
  - Erkennen von Signaturen
  - Erkennen von Anomalien

- ***Security Gateway Konzepte***
  - Authentication-Gateway
  - E-Mail-Gateway (Virtuelle Poststelle)
  - Signatur-Server

© Prof. Dr. Norbert Pohlmann, Fachhochschule Gelsenkirchen

Inhalt

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

© Prof. Dr. Norbert Pohlmann, Fachhochschule Gelsenkirchen

Themen für Ausarbeitungen und Vorträge (Übung)

- Ausarbeitungen und Vortrag sind Voraussetzung für die Klausur!

- Mögliche Themen sind z.B.:
  - Webserver-Sicherheit
  - DNS-Sicherheit
  - „Internet“ Frühwarnsysteme
  - VoIP-Sicherheit / Sicherheitsprobleme
  - Trusted Computing
  - Die 10 größten Probleme im Internet: genauer Beschreibung und Diskussion, warum sie ein Problem sind, und wie groß der potentielle Schaden ist
  - ...
  - weitere Themen, für die Sie sich interessieren, nach Absprache

© Prof. Dr. Norbert Pohlmann, Fachhochschule Gelsenkirchen

Inhalt

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

© Prof. Dr. Norbert Pohlmann, Fachhochschule Gelsenkirchen

Netzwerksicherheit A (NWS A)
→ Praktikum

- Das Praktikum ist Voraussetzung für die Klausur!

- **Themen des Praktikums sind:**
  - **Einrichtung und Überprüfung eines VPN-Systems**
    - in einer Kleingruppe mit Ausarbeitung der Ergebnisse (Aufteilung in der Vorlesung)
  - **Einrichtung und Überprüfung eines Firewall-Systems**
    - in einer Kleingruppe mit Ausarbeitung der Ergebnisse (Aufteilung in der Vorlesung)

- Das Praktikum findet im Raum P 1.05 statt.

© Prof. Dr. Norbert Pohlmann, Fachhochschule Gelsenkirchen

Inhalt

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

© Prof. Dr. Norbert Pohlmann, Fachhochschule Gelsenkirchen

Netzwerksicherheit A (NWS A)
→ Unterlagen

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

© Prof. Dr. Norbert Pohlmann, Fachhochschule Gelsenkirchen

Netzwerksicherheit A (NWS A)
→ Bücher

- N.Pohlmann: **„Firewall-Systeme - Sicherheit für Internet und Intranet, E-Mail-Security, Virtual Private Network, Intrution 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 **Crytology** - 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 Schmeh, **“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 ....

© Prof. Dr. Norbert Pohlmann, Fachhochschule Gelsenkirchen

Netzwerksicherheit A (NWS A)
→ 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, ...

© Prof. Dr. Norbert Pohlmann, Fachhochschule Gelsenkirchen

Netzwerksicherheit A (NWS A)

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

norbert.pohlmann@informatik.fh-gelsenkirchen.de

Fachhochschule Gelsenkirchen