



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Vorlesung: **Internet-Sicherheit B** **(ISB)**

Prof. Dr. (TU NN)

Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
<http://www.internet-sicherheit.de>

if(is)
internet-sicherheit.

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

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

Internet-Sicherheit B (ISB)

→ Einordnung

- **Zielgruppe:**

- Masterstudiengang

- **Stundenumfang:**

- 4 SWS (2V+1Ü+1P)

- **Voraussetzungen**

- Idealerweise Grundkenntnisse über TCP/IP-Protokolle u. Kryptographie. (Internet-Protokolle und Grundlagen der IT-Sicherheit)
- Die Vorlesung kann aber auch ohne diese Vorkenntnisse sinnvoll gehört werden!

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

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

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

Internet-Sicherheit B (ISB)

→ Vorlesungsinhalt (1/3)

- **Trusted Computing**
 - TPM (Aufbau und Funktionen)
 - TC Funktionen (Trusted Boot, Binding, Sealing and (Remote) Attestation)
 - Trusted Computing Base
 - Sicherheitsplattform (Idee, Ziele, Methoden, ...)
 - Anwendungsbeispiele
- **Trusted Network Connect (TNC)**
 - grundsätzliche Idee
 - TNC Architektur
 - T-NAC (Idee, Ziele, Methoden, ...)

Internet-Sicherheit B (ISB)

→ Vorlesungsinhalt (2/3)

- **Public-Key-Infrastruktur (PKI):**
 - Aufgaben,
 - Komponenten,
 - gesetzlicher Hintergrund,
 - Modelle,
 - Umsetzungskonzepte und
 - praktische Beispiele
- **Digitale Signatur:**
 - Gesetzliche Grundlagen,
 - Mechanismen und Prinzipien,
 - Anwendungsbeispiele
 - Architektur und die Funktionsweise

Internet-Sicherheit B (ISB)

→ Vorlesungsinhalt (3/3)

- **E-Mail-Security:**
 - Elemente,
 - Konzepte und
 - praktischer Einsatz

- **Anti-Spam-System:**
 - Schäden
 - Quellen
 - Anti-Spam-Technologien (Kopfzeilenanalyse, Textanalyse, Blacklist, Distributed Checksum Clearinghouse (DCC))
 - Distributed IP Reputation System

- **Botnetze**

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

Themen für Ausarbeitungen und Vorträge (Übung)

- Ausarbeitungen und Vortrag sind Voraussetzung für die Klausur!
- Mögliche Themen sind z.B.:
 - Neue Schwachstellen
 - Neue Bedrohungen
 - Neue Angriffe
 - Neue Sicherheitsmechanismen
 - Veränderungen im Internet
 - ...
 - 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

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

Internet-Sicherheit B (ISB)

→ Praktikum

- Das ISB-Praktikum wird über einen eigenen Moodlekurs koordiniert.
- Der Moodlekurs für das ISB-Praktikum ist zu finden unter.
... ▶ **Kurse (Informatik) ▶ BUGZEL**
- Es wird kein Schlüssel für diesen Moodlekurs benötigt.
- Das Eintragen in die Praktikumsgruppen ist ab sofort möglich.
- **Info über Start – Moodle**

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

Internet-Sicherheit B (ISB)

→ Unterlagen

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

- Claudia Eckert: „IT-Sicherheit“, ISBN-13: 9783486589993, 6. überarbeitete. Aufl., Oldenbourg Verlag, 2009
- 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.Langensbach, O. Ulrich (Hrsg.): **„Elektronische Signaturen - Kulturelle Rahmenbedingungen“** einer technischen Entwicklung, Springer Verlag, Berlin
- und sehr viele mehr (siehe in den Vorlesungen)

- 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, ...



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Vorlesung: Internet-Sicherheit B (ISB)

**Vielen Dank für Ihre Aufmerksamkeit
Fragen ?**

Prof. Dr. (TU NN)

Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
<http://www.internet-sicherheit.de>

if(is)
internet-sicherheit.