Informationssicherheit 1
SS 2005

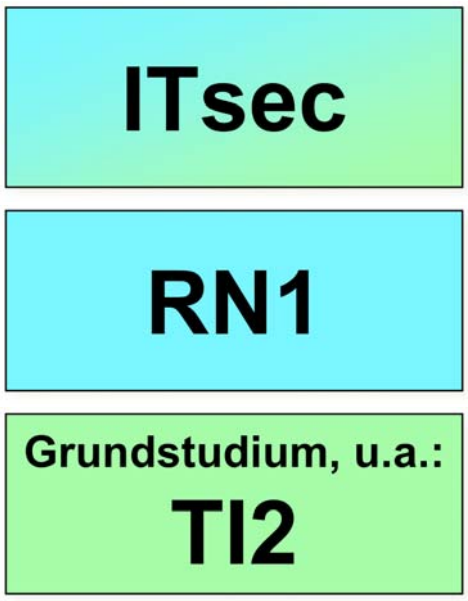
Prof. Dr.-Ing. Carsten Bormann
Dr. Karsten Sohr
Niels Pollem

Center for Computing Technologies

Inhalt: **Security**

- Sicherheitsziele; Zugriffskontrolle
- Schwachstellen; Firewalls
- Kryptographische Grundfunktionen **und ihre Einsatzbereiche**
- **Sicherheitsprotokolle**
  - Authentisierung, Schlüsselverwaltung, …
  - **Kerberos, IKEv2, TLS, EAP-__, SAML, …**
- S.-Management, Smartcards, trusted computing
- S. Engineering, S.-Bewertung

Voraussetzungen für LV Informationssicherheit



- 4./6. Semester: ITsec
  Grundlagen der Informationssicherheit
- 3./5. Semester: RN1
  Grundlagen Netze und Medien (Wahlpflicht)
- 3. Semester: TI2 (DM: TIMI)
  Grundlagen Betriebssysteme und nebenläufige Systeme (Pflicht)

ITsec: Form

- Team
  - Carsten Bormann, Karsten Sohr: „Vorlesung“ (Do 08–10, MZH 1400)
  - Niels Pollem, Karsten Sohr: „Übungen“ (Mo 10–12, MZH 1400)
- Integrierte Veranstaltung:
  - Plenum: Vorlesungen, Demonstrationen, Übungen, …
  - Übungsaufgaben (in Kleingruppen)
- Prüfungsrelevante Studienleistung: 6 CP (ECTS)
  - Übungsaufgaben (alle bearbeitet, ∑ 50 % der Punkte)
  - Fachgespräch am Ende des Semesters

Übungen

- Gruppen von 3 (Ausnahmefall: 2) Personen
- Ausgabe: in Stud.IP
  - I.d.R. wöchentlich
- Abgabe: in Stud.IP
  - I.d.R. eine Woche nach Ausgabe
- Bearbeitung: in der Gruppe
  - Nur so bringen's die Aufgaben
  - Ohnehin kurze Bearbeitungszeit
- Und weil wir Euch nicht trauen:-):
  Fachgespräch am Ende

Medien

- Plenum: hier (Mo 10–12, Do 08–10 MZH 1400)
- Stud.IP*)
  - https://elearning.uni-bremen.de
  - Login: *meinbenutzername*@informatik.uni-bremen.de
  - Dort als Erstes in Gruppen aufteilen
- Web: http://www-rn.tzi.de/lehre/itsec/
- Email: itsec@tzi.org

Literatur (1)

= unbedingt empfohlen

- **Einführende Literatur**
  - **C. Eckert**: *IT-Sicherheit*
    3. Auflage, Oldenbourg-Verlag, 2004,
    Studentenversion (reduzierter Umfang)
  - **R. Anderson**: *Security Engineering*
    John Wiley, 2001
  - **M. Bishop**: Computer Security: Art and Science,
    Addison-Wesley-Longman
- **(Un-) Sichere Software**
  - **J. Viega und G. McGraw**: *Building Secure Software*
    Addison-Wesley, 2002
  - **G. Hoglund und G. McGraw**: *Exploiting Software, How to Break Code*
    Addison-Wesley, 2004

Literatur (2)

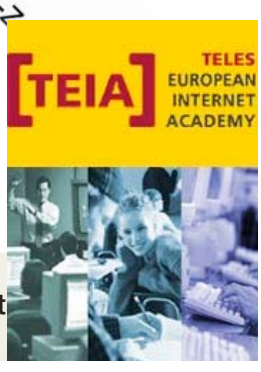
- **Kryptographie**
  - **B. Schneier**: *Applied Cryptography*
    Second Edition, John Wiley & Sons, 1996
  - **J. Buchmann**: *Einführung in die Kryptographie*
    2.erw. Auflage, Springer-Verlag, 2001
- Internetsicherheit
  - **W. Cheswick, S. Bellovin, A. Rubin**:
    Firewalls and Internet Security, 2nd Edition, Wiley 2003
- Auch für Laien interessant...
  - **B. Schneier**: *Secrets & Lies: IT-Sicherheit in einer vernetzten Welt*
    dpunkt-Verlag, 2000 (Englischsprachiges Original: Wiley, 2004)

„Du“

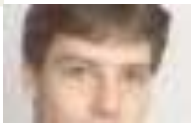
- Wen duzt man als Studi in einer Universität:
  - Studis
  - Wissenschaftliches Personal
  - Junge/junggebliebene :-) Professoren
  - Und auf jeden Fall mich!
- Wen siezt man:
  - Professoren (jedenfalls erst einmal auf Verdacht)
  - Verwaltungsmitarbeiter
- Was soll das alles?
  - Keine Ahnung...

Carsten Bormann

- Promoviert an der TU Berlin 1990
  - Offene Dokumentverarbeitung (ODA/SGML)
    ≈ „XML-Technologien“
- Universität Bremen
  - Honorarprofessor für „Internet-Technologie“
  - TZI-Vorstand (Leitthema NetContent)
  - Vorlesungen in Rechnernetze und Medieninformatik
- UdK Berlin
  - Studiengang „Electronic Business“
    Technical Literacy
- TELES European Internet Academy
  - Zuständig für Qualität der technischen Inhalte



Karsten Sohr



- Promoviert an der Uni Marburg 2001
  - Java-Sicherheit
- Universität Bremen
  - TZI-Geschäftsführer (Sichere Systeme)
  - Formale Methoden und Sicherheit, vor allem für rollenbasierte Zugriffskontrolle

Technologie-Zentrum Informatik

Niels Pollem

- Universität Bremen
  - Wissenschaftlicher Mitarbeiter AG Rechnernetze
  - Hat das Bremer WLAN ausgerollt
  - Fokus: Security

Technologie-Zentrum Informatik

Wie studiert man ITsec?

- Vorlesung: Zuhören, mitdenken, Fragen stellen
  - für die Fans des Mitschreibens: Folien sind im Web
- Übungsaufgaben: bearbeiten
  - Wirklich... In der Gruppe...
- Stud.IP/Web: Eigenständig Stoff bearbeiten
  - Nicht überfliegen wie andere Webseiten
  - Übungsaufgaben/Fragebögen nutzen
- Vor Fachgesprächen: zeitig Stoff durchgehen
  - Fragebögen als Gedächtnisstütze

Noch kurz zum Thema Fragen ...

- Bitte Fragen stellen, wenn etwas unklar ist.
  Keiner von uns kann hellsehen.
- Fragen helfen uns, den nachfolgenden Stoff besser aufzubereiten — also wieder Euch selbst.
- Nein, Fragen sind nicht zu dumm. Hier nicht.
- Es stimmt wirklich: Wer nicht fragt, bleibt dumm.
- Für viele Themen gilt hier: „Last chance to see ...“

IT-Sicherheit:
Einführung

Center for Computing Technologies

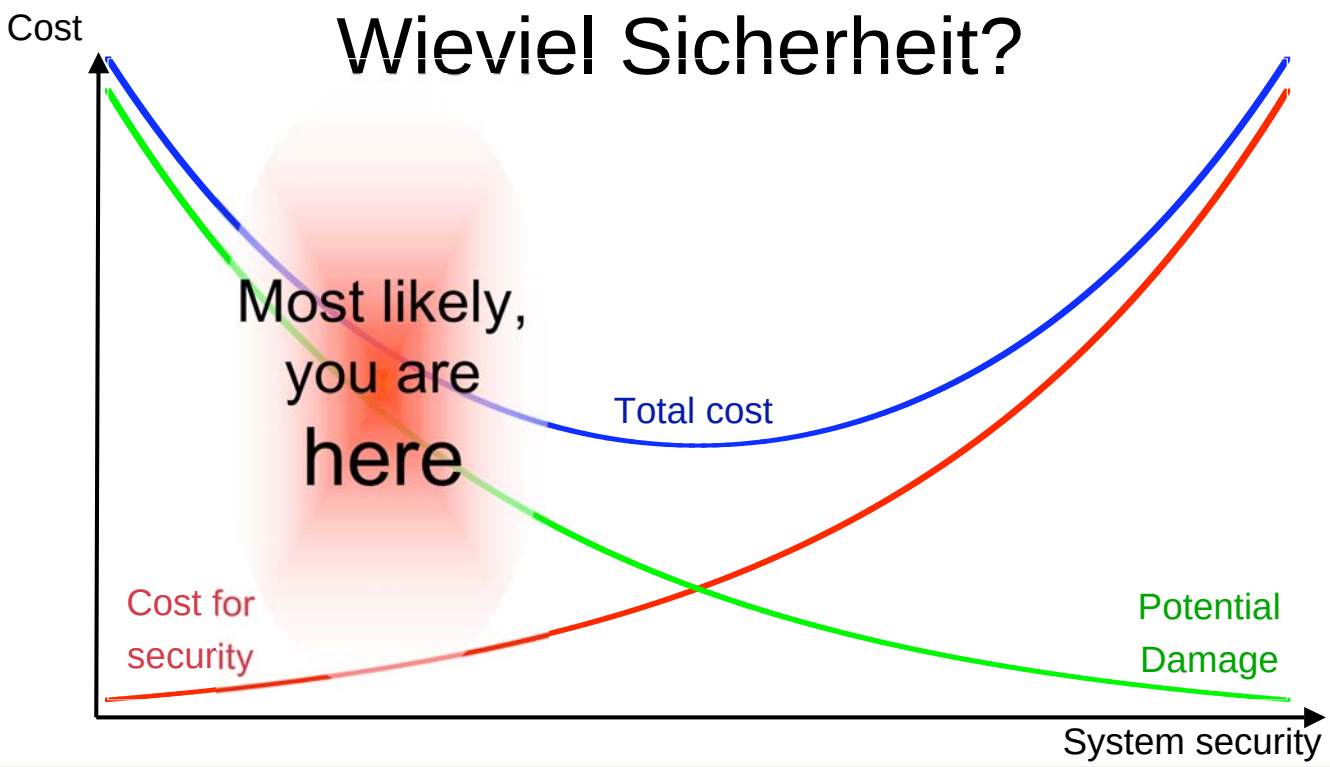
Wozu Sicherheit?

- Erwartung an IT-Systeme: **Verläßlichkeit**
  - Immer mehr, immer wichtigere Aufgaben werden IT-Systemen übertragen
- Problem: Bugs, Abstürze, Fehlfunktionen
- Problem: **Böse Absicht** (aber auch böse Zufälle)

Stark vereinfacht:

- Sicherheit *(Safety)*: System tut immer, was es soll
- Sicherheit *(**Security**):* System tut nie, was es nicht soll

Universität Bremen



Sicherheitsprobleme

- Für ein **System** bestehen **Sicherheitsziele *(security objectives)***
- Sicherheitssysteme haben **Schwachstellen (*weaknesses*)**
- **Verwundbarkeiten *(vulnerabilities)*** erlauben das Umgehen (oder den Mißbrauch) von Sicherheitsmechanismen
- Eine **Bedrohung *(threat)*** ist die Möglichkeit eines **Angriffs *(attack)***
- Angriffe erzeugen u.U. **Schaden *(damage)***
- **Risiko *(Risk)*** = p(attack) × cost(damage)

Sicherheitssysteme

- Erfolgreiche Angriffe
  - Verhindern *(prevention)*
  - Erkennen *(detection)*
  - Eingrenzen (Schadensbegrenzung) *(containment)*
- Sicherheitsregeln ***(security policy)***
  - Richtlinien; Schulung der Mitarbeiter
  - Notfallplanung, -training
  - Management-Unterstützung, Schutz der Sicherheitsverantwortlichen

Wer sind die Angreifer?

- **Insider** (faul, frustriert, kriminell)
  - Evtl. als Folge von **Social Engineering**
- **„Hacker“** (Cracker), „script kiddies“
  - Pures Interesse, Spaß/Spannung/Sucht, Geltungssucht!
- **Professionelle** Angreifer (Spionage, Geheimdienste)
- Organisiertes **Verbrechen**
  - Z.B. Erpressung
  - Z.B. Ausschalten eines Konkurrenten

Sicherheitsziele

- Geheimhaltung/Datenschutz/Vertraulichkeit
  - Anonymität
- Integrität/Authentizität
- Zurechenbarkeit/Verbindlichkeit
- Verfügbarkeit

Geheimhaltung/Datenschutz/ Vertraulichkeit

- Geheimhaltung ***(secrecy)***: Einschränkung des Zugriffs
- Vertraulichkeit ***(confidentiality)***: Verpflichtung zur Geheimhaltung der Informationen anderer
- Datenschutz ***(privacy)***: Recht auf Schutz eigener (persönlicher) Informationen

- Achtung: Oft ist die Tatsache einer Kommunikationshandlung bereits geheimzuhaltende Information (vs. ***traffic analysis***)

Anonymität

- Anonymität (**anonymity**): Durchführung von Handlungen ohne Preisgabe der Identität
  - Evtl. auch Preisgabe eines **Pseudonyms**

Integrität/Authentizität

- Integrität (***integrity***) der Daten: Schutz vor **unautorisierter** und **unbemerkter** Veränderung von Daten.

  (vgl. Integritätsbegriff aus den Datenbanken)

- Authentizität (***authenticity***): Information ist **integer** und **frisch**; eindeutig einer **Identität** zuzuordnen

Zurechenbarkeit/Verbindlichkeit

- Zurechenbarkeit (***accountability***): Eine durchgeführte Handlung kann einem Kommunikationspartner eindeutig zugeordnet werden.
- Verbindlichkeit (***non-repudiation***): kein unzulässiges Abstreiten durchgeführter Handlungen

  Notwendig beispielsweise für:
  - Abschließen von elektronischen Kaufverträgen
  - digital unterschriebene Gerichtsanträge

Verfügbarkeit

- Verfügbarkeit *(**availability**)*: Schutz vor unbefugter Beeinträchtigung der Funktionalität von Komponenten, Diensten etc.
  - vs. Denial-of-Service- (DoS-) Angriffe
- Ergibt zusammen mit Korrektheit: Verläßlichkeit ***(dependability):*** Funktionssicherheit; zuverlässige Erbringung der Funktion ***(reliability)***

Wo liegen die Schwachstellen?

- Schlechtes **Design**
  - (z.B. fehlende Kontrollen, zu grobe Rechtevergabe)
- Schlechte **Implementierung**
  - (z.B. Pufferüberläufe, schwache Mechanismen, Umgehungswege)
- Schlechte **Systemadministration**
  - (z.B. Account mit Standardpaßwort, offene Ports in Firewall, Einsatz ungeeigneter Systeme und Werkzeuge)
- Schlechtes **Management**
  - (z.B. unklare Sicherheitspolitik, unklare Sicherheitsregeln, fehlendes Sicherheitsbewußtsein der Mitarbeiter, keine Mittel für Sicherheitsüberprüfungen)

Designprinzipien für sichere Systeme (1)

- **Principle of Economy of Mechanism**

  The protection mechanism should have a simple and small design.
- **Principle of Fail-safe Defaults**

  The protection mechanism should deny access by default, and grant access only when explicit permission exists.
- **Principle of Complete Mediation**

  The protection mechanism should check every access to every object.

Designprinzipien für sichere Systeme (2)

- **Principle of Open Design**

  The protection mechanism should not depend on attackers being ignorant of its design to succeed (no ***security by obscurity***).
  It may however be based on the attacker's ignorance of specific information such as passwords or cipher keys.
- **Principle of Separation of Privilege**

  The protection mechanism should grant access based on more than one piece of information.

Designprinzipien für sichere Systeme (3)

- **Principle of Least Privilege**

  The protection mechanism should force every process to operate with the minimum privileges needed to perform its task.
- **Principle of Least Common Mechanism**

  The protection mechanism should be shared as little as possible among users.
- **Principle of Psychological Acceptability**

  The protection mechanism should be easy to use (at least as easy as not using it).

Nächster Termin

Mo, 18.04.2005 10–12 Uhr:

- Grundlagen Sicherheit: Szenarien

Übungsblatt 1 auf Stud.IP, s.:
https://elearning.uni-bremen.de