Sichere und verlässliche Datenverarbeitung:

Gefährdungs- und Bedrohungspotentiale der automatischen Datenverarbeitung

Prof. Dr. Hannes Federrath
Lehrstuhl Management der Informationssicherheit Uni Regensburg

http://www-sec.uni-regensburg.de/

Was ist Sicherheit?

Techniken zum Schutz?

Stand der Technik?

Was sind die Prioritäten?

Management der Informationssicherheit

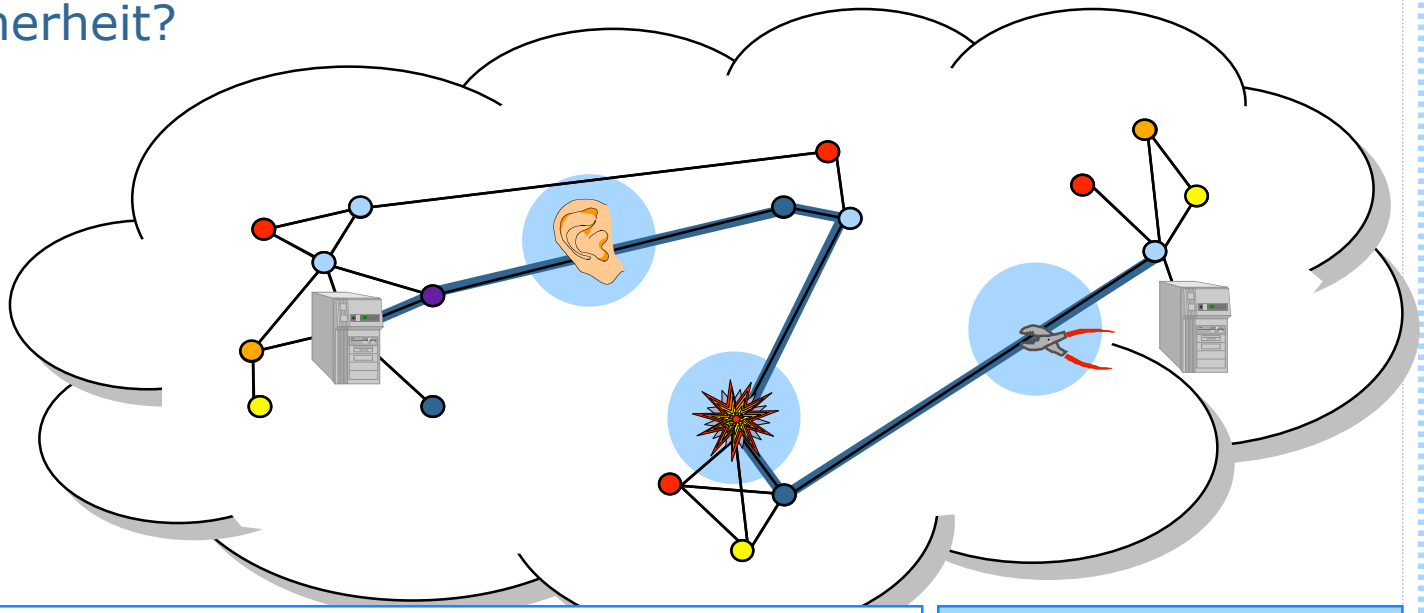
IT-Sicherheitsmanagement versucht, die mit Hilfe von Informationstechnik (IT) realisierten Produktions- und Geschäftsprozesse in Unternehmen und Organisationen systematisch gegen beabsichtigte Angriffe (Security) und unbeabsichtigte Ereignisse (Safety) zu schützen.

- Themen, die am Lehrstuhl bearbeitet werden:
  - Sicherheit in verteilten Systemen und Mehrseitige Sicherheit
  - Datenschutzfreundliche Techniken
  - Sicherheit im Internet
  - Digital Rights Management Systeme
  - Sicherheit im E-Commerce und in mobilen Systemen

- Weitere Informationen:
  - http://www-sec.uni-regensburg.de

Problemstellung

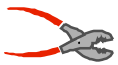
- Was ist Sicherheit?



Bedrohungen


unbefugter Informationsgewinn


unbefugte Modifikation


unbefugte Beeinträchtigung der Funktionalität

Schutz der

Vertraulichkeit

Integrität

Verfügbarkeit

Schutzziele: Einordnung

Kommunikationsgegenstand WAS?		**Kommunikationsumstände WANN?, WO?, WER?**
Vertraulichkeit **Verdecktheit**	**Inhalte**	**Anonymität** **Unbeobachtbarkeit** **Sender** **Ort** **Empfänger**
Integrität	**Inhalte**	**Zurechenbarkeit** **Rechtsverbindlichkeit** **Absender** **Bezahlung** **Empfänger**
Verfügbarkeit	**Inhalte**	**Erreichbarkeit** **Nutzer** **Rechner**

Vertraulichkeit

Verdecktheit

Integrität

Zurechenbarkeit

Anonymität

Unbeobachtbarkeit

Verfügbarkeit

Erreichbarkeit

Rechtsverbindlichkeit

Verschlüsselungsverfahren

- **Symmetrische Verschlüsselung, z.B. DES, AES**
  - Kommunikationspartner teilen ein gemeinsames Geheimnis (symmetrischer Schlüssel)
  - Sicherheit basiert meist auf Chaos
  - Schlüssellänge ≥ 128 Bits
- **Asymmetrische Verschlüsselung, z.B. RSA**
  - Jeder Nutzer generiert Schlüsselpaar:
    - *Öffentlichen* Verschlüsselungsschlüssel
    - *Privaten* Entschlüsselungsschlüssel
  - Sicherheit basiert auf zahlentheoretischen Annahmen
  - Schlüssellänge ≥ 1024 Bit
  - Neuerdings: Elliptische Kurven: ca. 160 Bit

Vertraulichkeit

Verdecktheit

Integrität
Zurechenbarkeit

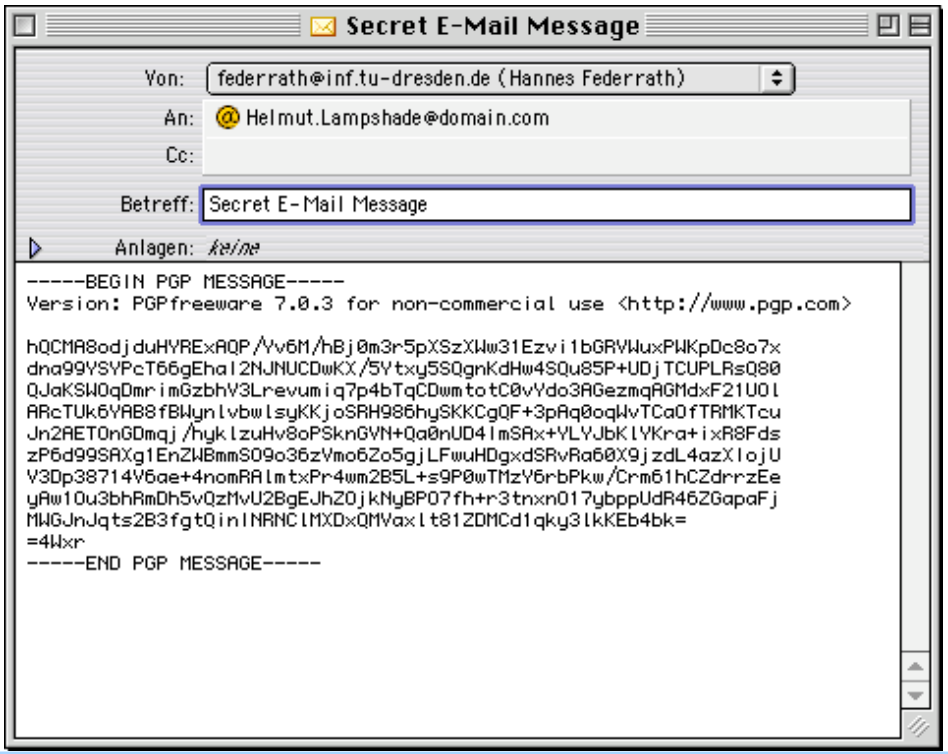
Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

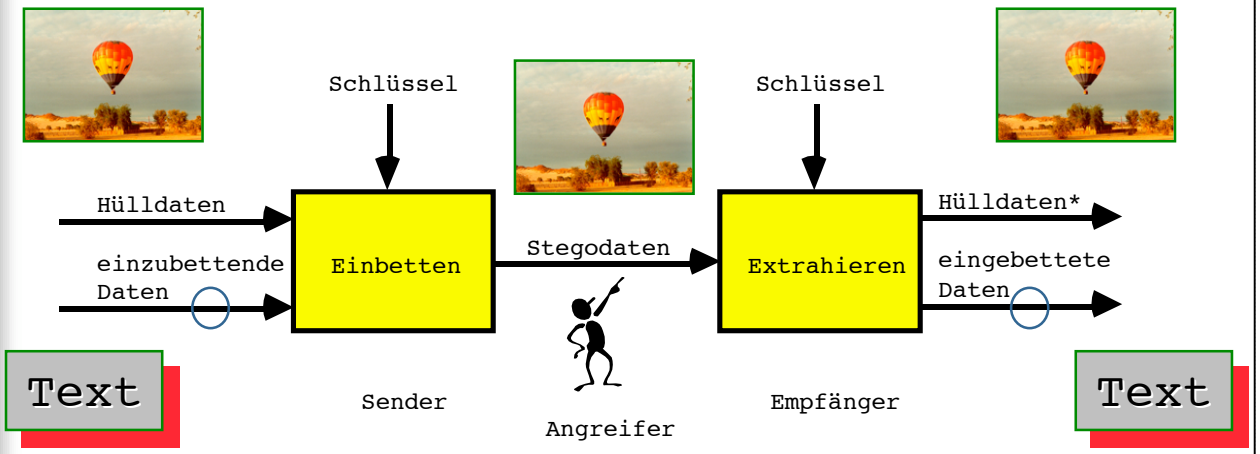
Verschlüsselungssoftware

- Pretty Good Privacy
  - http://www.pgp.com
- Gnu Privacy Guard
  - http://www.gnupg.org



Steganographie

- **Verbergen der Existenz einer geheimen Nachricht**
  - geheimzuhaltende Nachricht wird in eine Hülle eingebettet
  - minimale Veränderungen kaum bzw. nicht erkennbar
  - Veränderungen nicht mit Messmethoden nachweisbar



Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

Message Authentication Codes

- **Symmetrisches Verfahren**
  - Kommunikationspartner teilen ein gemeinsame Geheimnis (symmetrischer Schlüssel)
- **Gehört heute zum Grundschutz**
  - Verfälschungen von Nachrichten (böswillige und zufällige) sind erkennbar
- **Keine Nachweisbarkeit gegenüber Dritten**

Digitale Signatur

- **Asymmetrisches Verfahren, z.B. RSA**
  - Jeder Nutzer generiert Schlüsselpaar:
    - *Öffentlichen* Testschlüssel
    - *Privaten* Sigierschlüssel
- **Nachweisbarkeit gegenüber Dritten**
- **Ebenfalls einsetzbar:**
  - Pretty Good Privacy
  - http://www.pgp.com

Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

Verfahren zum Schutz von Verkehrdaten

- **Adressierungsinformationen können nicht verschlüsselt werden**
  - Problem Verkehrsdaten:
    - Wer mit wem, wann, wie lange, wo, wieviel Information?
  - Problem Interessensdaten:
    - Wer interessiert sich für was?

- **Spezielle Verfahren:**
  - Proxies
  - Mix-Netz
  - DC-Netz
  - Dummy traffic
  - …

Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

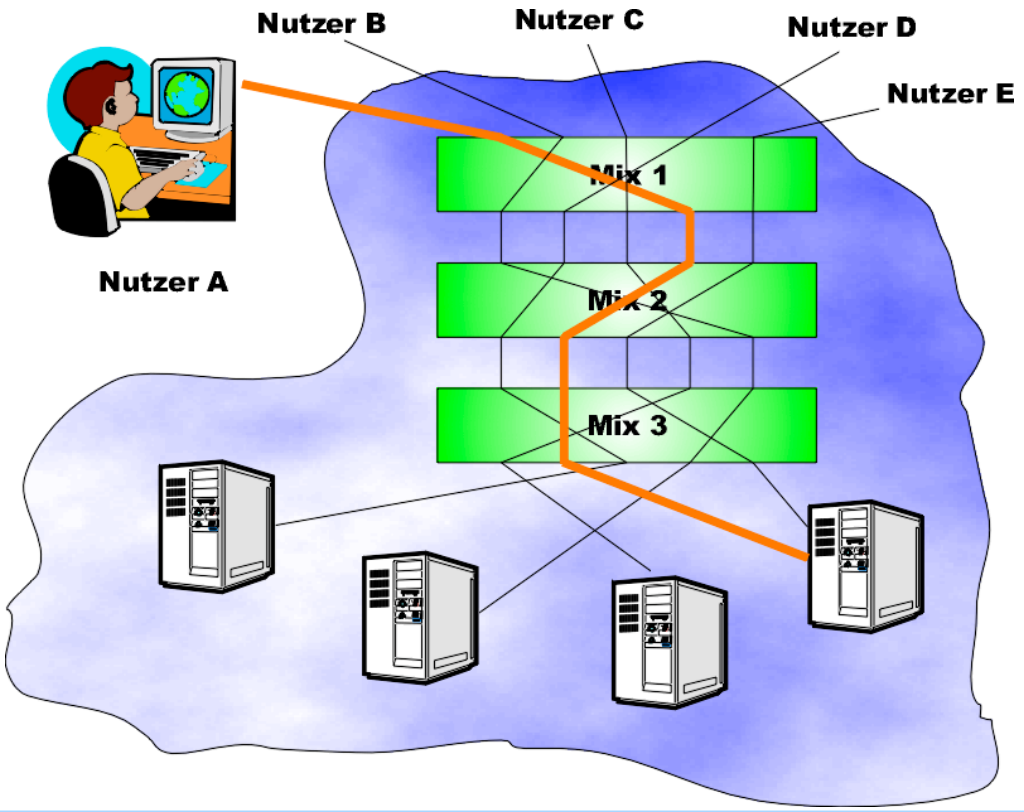
Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

Verfahren zum Schutz von Verkehrdaten

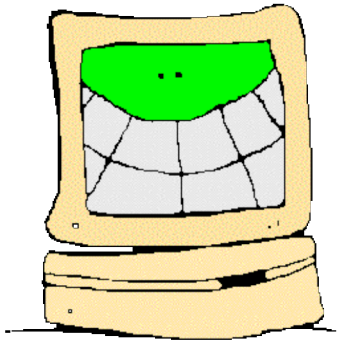
- **Anonymisierung von Web-Zugriffen**
  - JAP-Software
  - http://www.anon-online.de



- **Verfügbarkeit**
  - Nutzbarkeit von Diensten und Ressourcen, wenn ein Teilnehmer sie benutzen will.
- **Erreichbarkeit**
  - Zu einer Ressource (Nutzer oder Maschine) kann Kontakt aufgenommen werden, wenn gewünscht.
- **»Mechanismen«**
  - Mehrfach redundante Leitungsführung
  - Diversitärer Entwurf der Komponenten
  - Starke Vermaschung der Kommunikationsverbindungen
- **Techniken zur Verteilung von Kontrolle**
  - Offenlegung von Designkriterien und Algorithmen
  - Open Source Software
  - Sichere Betriebssysteme

Denial-of-Service-Angriffe

- **Schwachstellen im Systemdesign**
  - Mail-Bombing – Spamming
  - Broadcast-Storm
  - SYN-Flooding
- **Implementationsfehler**
  - Ping of Death
  - WinNuke
  - Teardrop und Nachfahren



Vorher

Nachher

Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

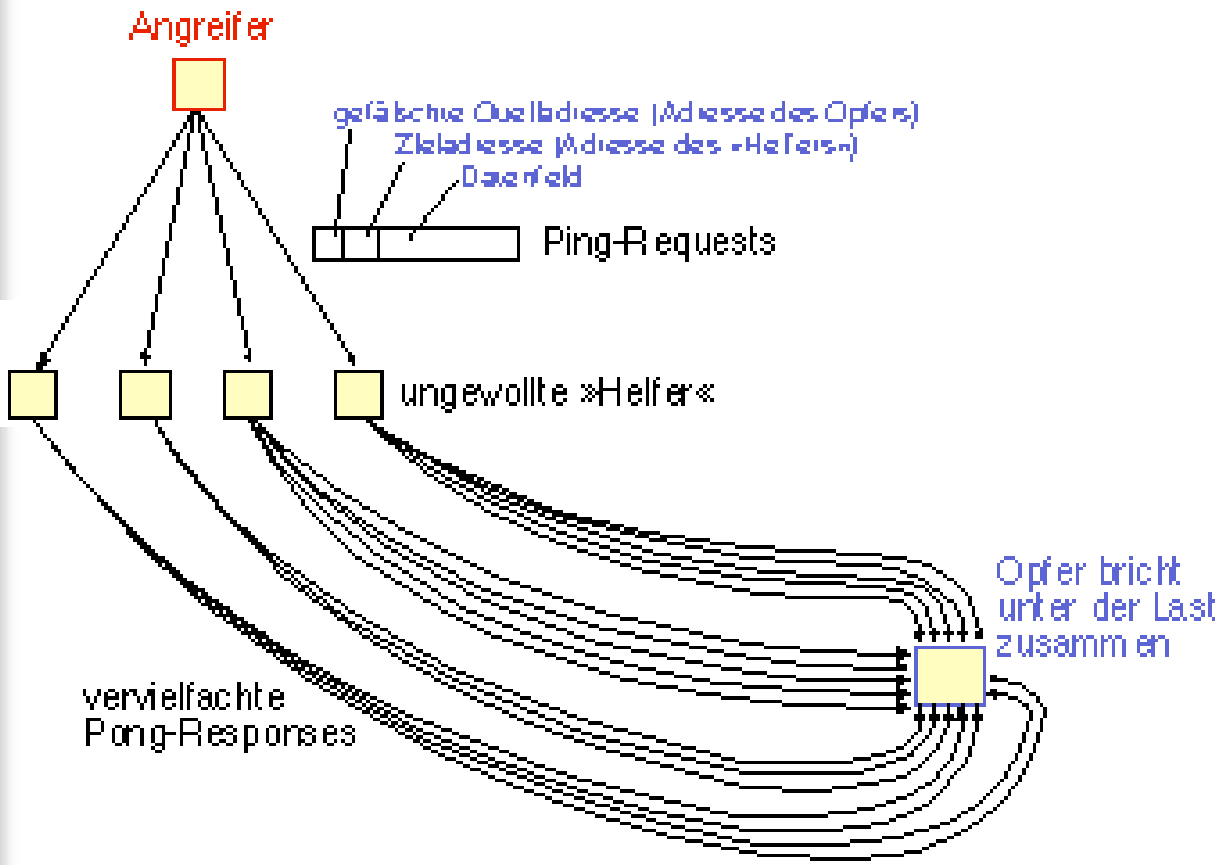
Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

Denial-of-Service-Angriffe

- **Smurf IP Denial-of-Service Attack (CERT Advisory CA-1998-01)**



- **Rechtsverbindlichkeit**
  - Ein Nutzer kann rechtlich belangt werden, um seine Verantwortlichkeiten innerhalb einer angemessenen Zeit zu erfüllen.
  - Kann nicht technisch geschaffen werden
- **Rechtsverbindlichkeit der Digitalen Signatur**
  - Klare Regeln bzgl. Beweiswert
  - Zertifizierung von Schlüsseln (Public Key Infrastructure PKI)
- **Sicherheit der Netzkomponenten**
  - Zertifizierung von Netzkomponenten
  - Physische Sicherheit, immer dann, wenn Vertrauen in fremde Netzkomponente aufgebracht werden muss.

Stand der Sicherheitstechnik

- Viele Verfahren sind theoretisch ausgereift und sichere Technik ist teilweise verfügbar:
  - meistens noch Detailprobleme
  - selten Grundsatzprobleme:
    - Beispiel: Wie realisiert man eine dauerhaft sichere, nicht ausforschbare Hardware (z.B. zur Aufbewahrung von kryptographischen Schlüsseln)

- Defizite:
  - Integration von Sicherheitsfunktionen in existierende Systeme
  - Mehrseitig sichere Technik: Beachtung von Sicherheit
    - der Betreiber und der Betroffenen

    bereits beim Systemdesign berücksichtigen
  - Schulung, Sensibilisierung, Weiterbildung im Bereich Sicherheit

Was sind die Prioritäten?

- Mehr Transparenz erreichen
  - Offenlegung des Quellcodes
  - Förderung von Open Source
- Möglichkeiten zum Selbstschutz stärken und fördern
  - leicht bedienbare Tools
- Mehr Diversität erreichen
  - Sichere Betriebssoftware
  - Sichere Hardware *für* denjenigen, der sie betreibt
- Investitions- und Urheberschutz erhalten
  - Digital Rights Management Systeme
  - Sichere Hardware *gegen* denjenigen, der sie betreibt

Selbstschutz-Tools: Beispiele

- Verschlüsselung, Signatur
  - PGP, GnuPG
- Filter
  - Webwasher, JunkBuster, CookieCooker
- Personal Firewall
  - Norton Personal Firewall, Zone Alarm
- Anonymisierer
  - Anonymizer, JAP
- Sichere Dienste anstelle ihrer unsicheren Vorläufer verwenden
  - telnet ssh, ftp scp, http https
- Betriebssysteme mit Zugriffskontrolle/Rechtevergabe/OpenSource
  - Linux, BSD