Technischer Datenschutz und mehrseitige IT-Sicherheit

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

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

Seminar »Sichere und datenschutzgerechte Technikgestaltung in einer mobilen und vernetzten Welt« der Studienstiftung des deutschen Volkes, La Villa (Italien), 27. August 2007

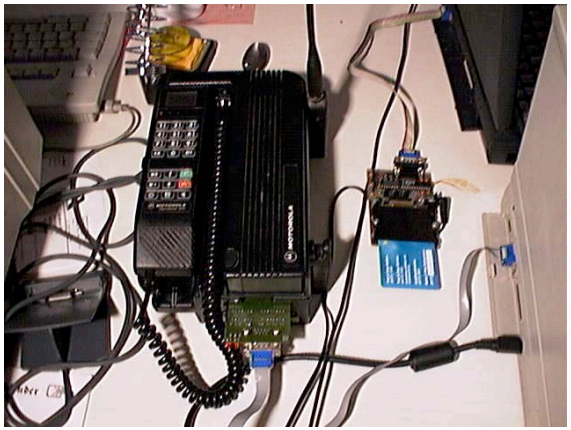
Neue Technik

- wird nicht nur zu legalen Zwecken eingesetzt, sondern kann auch von Kriminellen genutzt werden; Beispiele:
  - Verabredung von Straftaten, Terrorakten
  - Betrug (Kreditkarten-, Produktbetrug)
  - Verbreitung illegaler Inhalte (Kinderpornographie, Raubkopien)
  - ist selbst Ziel krimineller Handlungen (Viren, Würmer, trojanische Pferde)

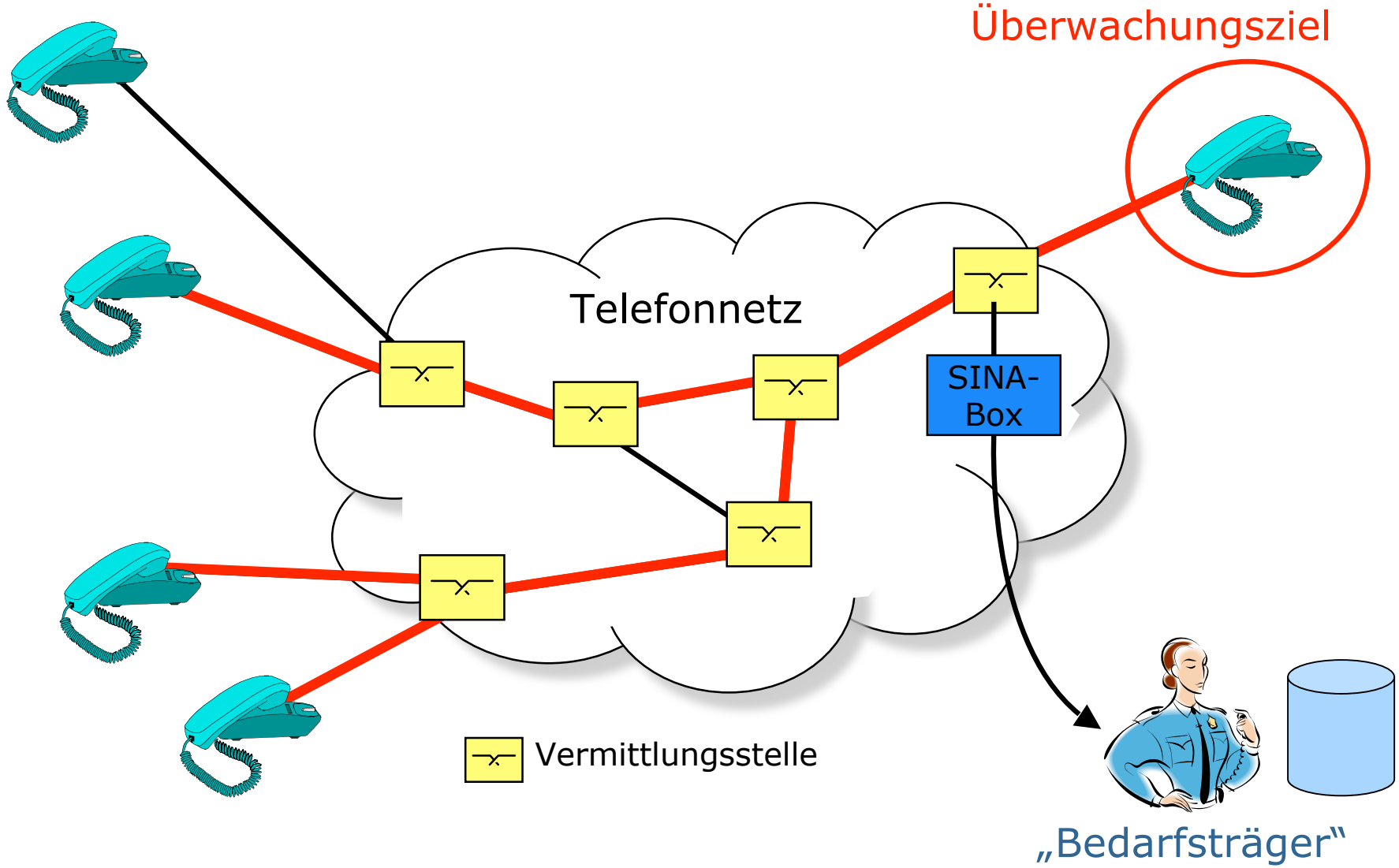
- führt zunächst zu einer Ohnmachtserfahrung des Staates
  - „Das Internet ist kein rechtsfreier Raum."
  - Forderung nach besseren Überwachungsmöglichkeiten des Staates

Neue Technik

- 3 Beispiele zur Motivation
  - wie man es *nicht* machen sollte, wenn der Staat seine Glaubwürdigkeit auf Dauer behalten bzw. zurück erhalten will
    - Telefonüberwachung
    - Mautsystem
    - Fingerabdrücke in Reisepässen



Telefonüberwachung



Telefonüberwachung: Reale Zahlen

Quelle: ct, Heft 10, 2006, S.60

- Deutschland im Jahr 2002:
  - Studie Uni Bielefeld:
    - 21974 Anordnungen
    - mehr als 20 Millionen abgehörte Telefongespräche
    - ca. 1,5 Millionen betroffene Bundesbürger
  - Kriminologisches Institut der Uni Münster:
    - Hochrechnung für 2002:
      knapp 4 Millionen betroffene Bundesbürger
- USA im Jahr 2005:
  - Verwaltungsbüro der US-Gerichtshöfe
    - 1773 Anordnungen von Bundes- und Staatengerichten
      + 625 Anordnungen von Bundesbehörden
    - je Anordnung durchschnittlich betroffene US-Bürger: 107

22.000 ÜA · 100 Betroffene = 2.200.000 Betroffene

80 Mio. Bundesbürger / 2,2 Mio. Betroffene ≈ 40, d.h. jeder 40. Bürger ist betroffen

Telefonüberwachung

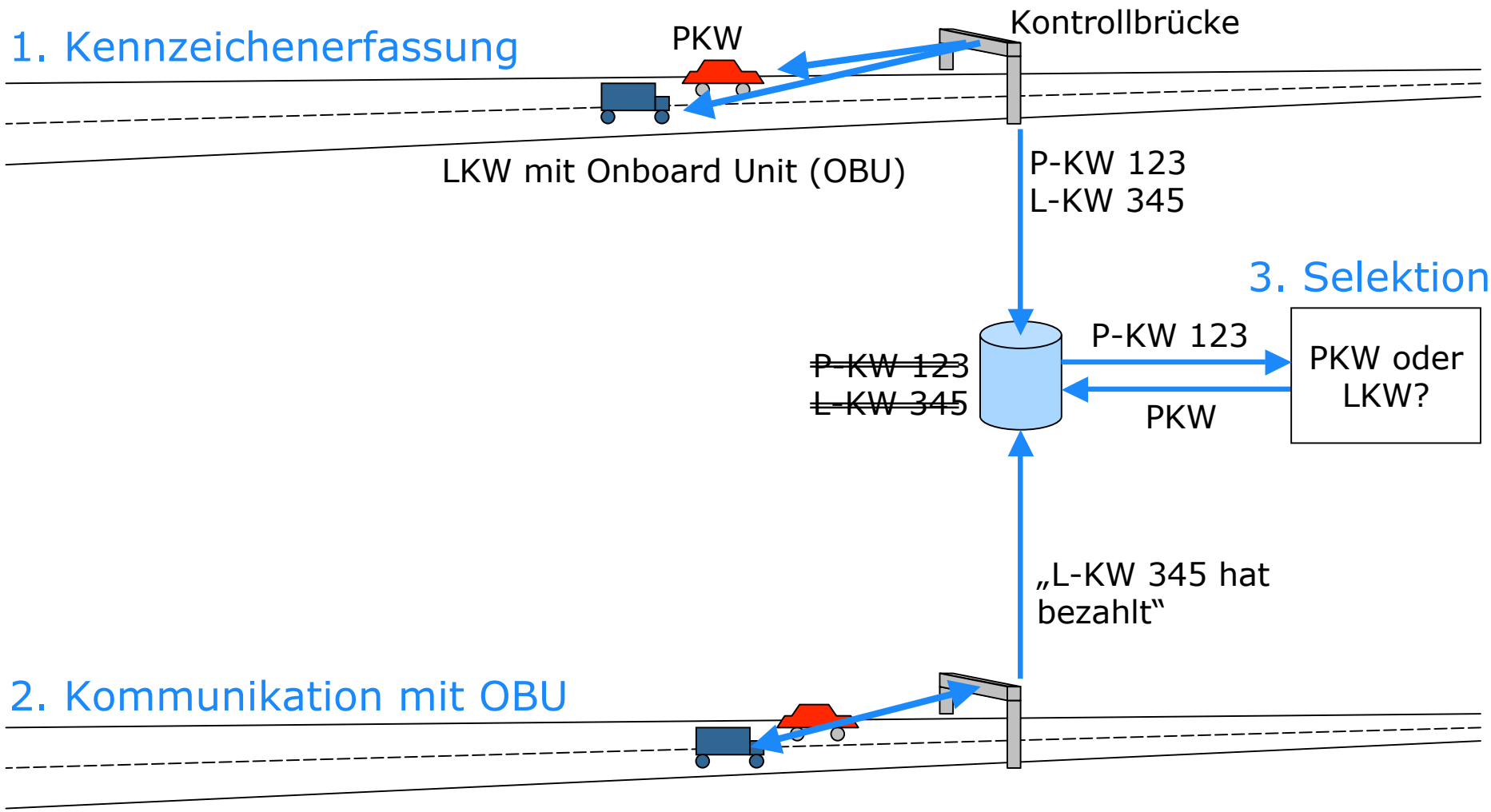
- Gesetzliche Grundlagen:
  - GG Art. 10 (Fernmeldegeheimnis)
  - G-10 Gesetz (Ermächtigung für Nachrichtendienste)
  - § 100 a, b StPO (besonders schwere Straftaten)
- Katalogstraftaten (§ 100 a StPO)
  - Hochverrat
  - Gefährdung des demokratischen Rechtsstaates
  - Geld- oder Wertpapierfälschung
  - schweren Menschenhandel
  - Mord
  - Bandendiebstahl
  - Raub
  - Erpressung
  - Geldwäsche
  - …

- Gutachten der Max-Planck-Instituts für ausländ. und int. Strafrecht:
  - nur ein Bruchteil der Betroffenen wird im Nachhinein informiert
  - Richtervorbehalt läuft ins Leere

Deutsches Mautsystem

- dient der Erhebung von LKW-Straßenbenutzungsgebühren
- Kennzeichen aller durchfahrenden Fahrzeuge werden vorsorglich erfasst
  - PKW und LKW
- Fahrzeuge mit Onboard Unit tauschen Daten mit Kontrollbrücke aus
  - Prepaid System: Alle bezahlten Fahrzeuge werden sofort wieder aus Datenbank gelöscht

Deutsches Mautsystem



Deutsches Mautsystem

- Alle Fahrzeuge werden erfasst (PKW und LKW).
- Gesetzlich verankerte Zweckbindung der Datenerhebung:
  - nur zur Erhebung von Autobahnmaut (LKW)
- Generalbundesanwalt (a.D.) Nehm:
  - Daten sollen auch für Strafverfolgung zur Verfügung stehen (44. Deutscher Verkehrsgerichtstag, Januar 2006)
- Technisch problemlos möglich wären heute schon:
  - Automatische Geschwindigkeitskontrollen
  - Flächendeckende Bewegungsprofile
  - Einführung einer PKW-Maut
- Tollcollect hat für die technische Realisierung dieses perfekten Überwachungssystems den Big Brother Award 2002 erhalten.

Biometrische Reisepässe

- Seit Herbst 2005 zur Verbesserung der inneren Sicherheit eingeführt

- Neue Funktionen:
  - Speicherung eines Fotos und zukünftig zusätzlich eines Fingerabdrucks des Passinhabers auf einem Chip
  - Kontaktloses Auslesen der biometrischen Merkmale aus dem Chip
- Probleme:
  - Biometrische Merkmale
    - erhöhen nicht die Zuverlässigkeit der Identifikation
    - geben möglicherweise Auskunft über weitere Eigenschaften der Person
  - Kontaktlose Chips
    - lassen sich unter bestimmten Umständen leicht von Jedermann auslesen

Fälschen eines Fingerabdrucks

- Vom Chaos Computer Club im Jahre 2005 praktisch demonstriert.

- Fingerabdruck sichtbar machen
- fotografieren
- nachbearbeiten
- ausdrucken
- Leim drauf
- warten
- abziehen

- Von uns im Rahmen einer Fernsehsendung praktisch nachvollzogen
- Ergebnis: Es funktioniert wirklich (nicht).

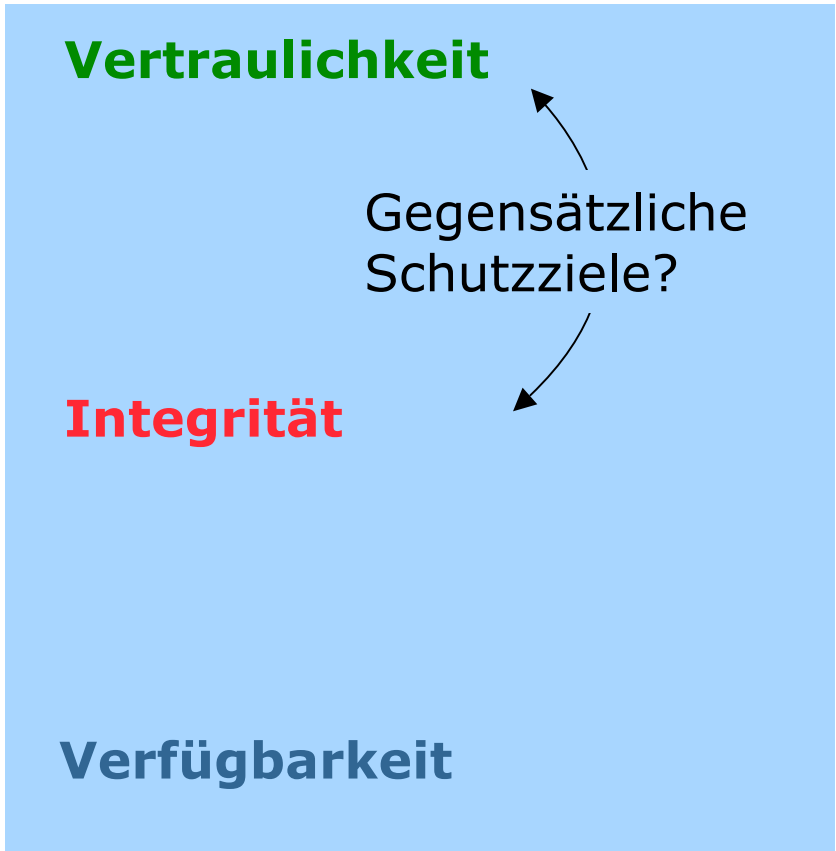
Schutzziele (Voydock, Kent 1983)

- Klassische IT-Sicherheit berücksichtigt im Wesentlichen Risiken, die durch *regelwidriges Verhalten* in IT-Systemen entstehen.

Vertraulichkeit	unbefugter Informationsgewinn
Integrität	unbefugte Modifikation
Verfügbarkeit	unbefugte Beeinträchtigung der Funktionalität

Mehrseitige Sicherheit (Müller et. al. 1997)

- Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte.



- Voraussetzung
  - regelwidriges Verhalten hält Systeme und Nutzer schadlos
- Ziel
  - gegensätzliche Sicherheitsinteressen werden erkannt, Lösungen ausgehandelt und durchgesetzt

Was ist zu schützen?

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**

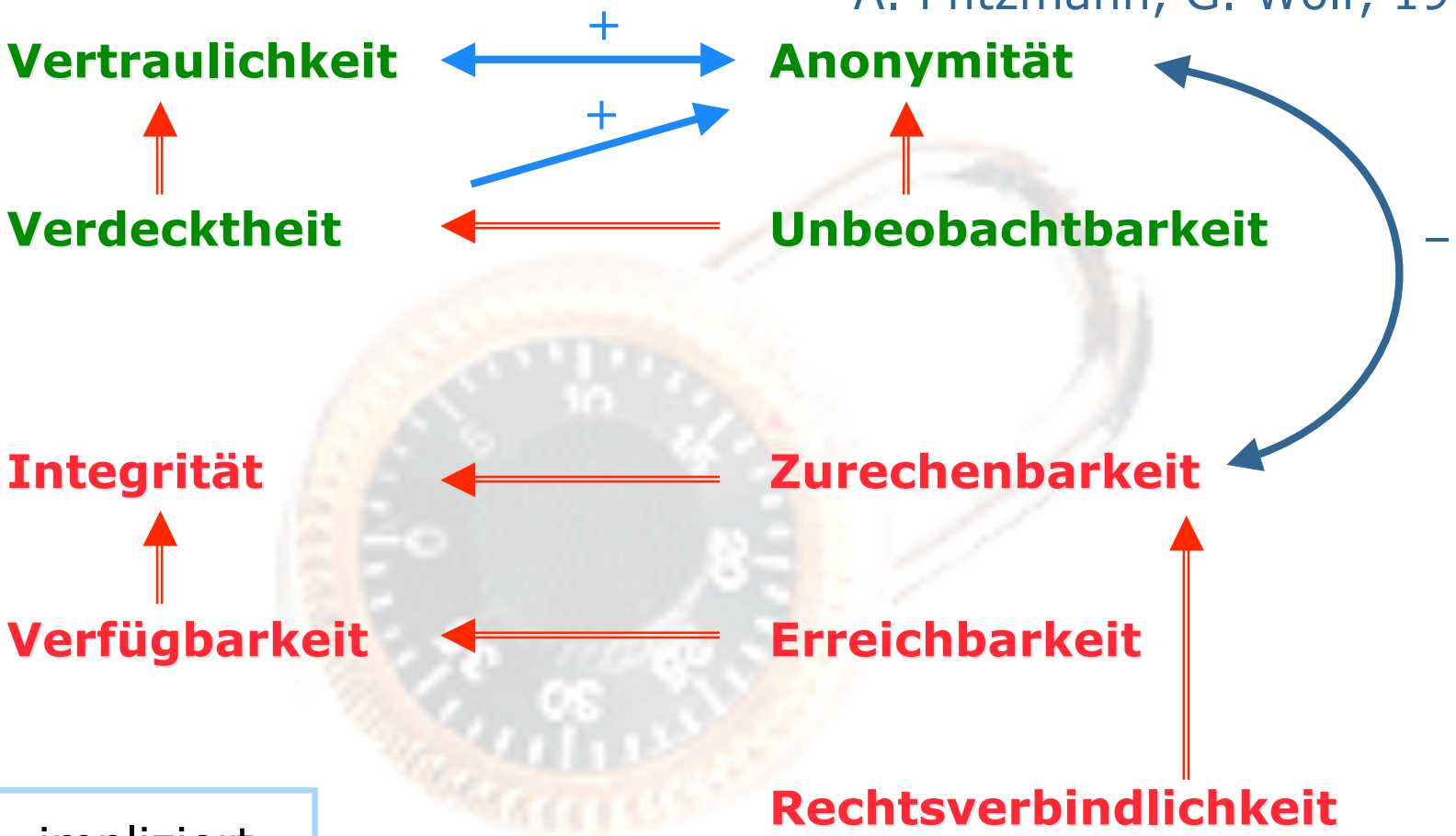
Datenschutz

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

Schutz personenbezogener Daten:
Verkehrsdaten
Interessensdaten

Wechselwirkungen zwischen Schutzzielen

A. Pfitzmann, G. Wolf, 1999



impliziert

\+ verstärkt

– schwächt

Beobachtungen zum Monotonieverhalten:
Vertraulichkeitseigenschaften können nur geringer werden.
Integrität und Zurechenbarkeit können nur größer werden.

Einseitige oder mehrseitige Sicherheit?

Kommunikationspartner haben nicht immer gleiche Sicherheitsinteresssen

Kunde | **Händler**

Der Händler soll an meine Bestellung gebunden sein. ← Digitale Signatur → Der Kunde soll an seine Bestellung gebunden sein.

Digitale Signatur ←

Ich möchte anonym bleiben, solange ich nichts kaufe. ← **Vertrauen nötig** → Der Kunde soll sich identifizieren.

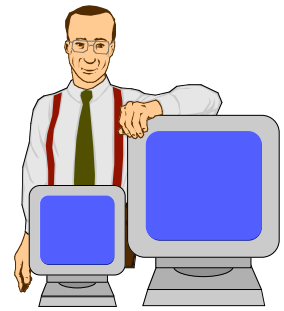
Pseudonymität: Treuhänder kennt Identität des Kunden, prüft Ware und Geld vor Lieferung

Der Zustand der Ware soll einwandfrei sein, sonst: Geld zurück! ←

→ Der Bezahlvorgang soll sicher sein (Kein Betrug durch Kunden).

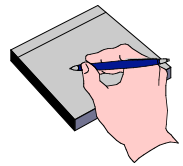
Ich möchte anonym bleiben beim Einkauf. ← Anonyme Zahlungssysteme →

Der Händler soll keine Kundenprofile anlegen dürfen. ← **Vertrauen nötig** Selbstverpflichtung, P3P ←



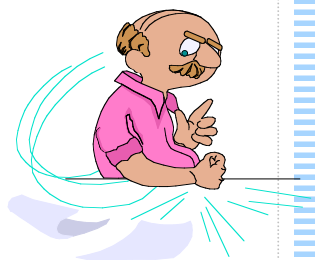
Mehrseitige Sicherheit

- Definition
  - Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung.
- Vorgehen



  1. Sicherheitsinteressen formulieren
     - Setzt Verständnis des Benutzers voraus
     - Gute Bedienoberflächen sind nötig

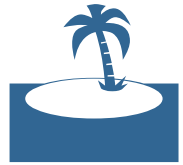
  2. Konflikte erkennen und Lösungen aushandeln
     - Setzt entsprechende Tools und
     - Technische Protokolle voraus



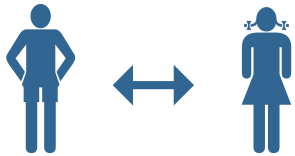
  3. Sicherheitsinteressen durchsetzen
     - Anwender brauchen Werkzeuge zum Selbstschutz
- Randbedingung
  - möglichst wenig Vertrauen in andere setzen müssen, d.h.
  - »Sicherheit mit minimalen Annahmen über andere«

Techniken für Mehrseitige Sicherheit

- Unilateral nutzbar
  - jede(r) kann allein entscheiden



- Bilateral nutzbar
  - nur wenn der Kommunikationspartner kooperiert



- Trilateral nutzbar
  - nur wenn zusätzlich ein vertrauenswürdiger Dritter kooperiert

- Multilateral nutzbar
  - nur wenn viele Partner kooperieren

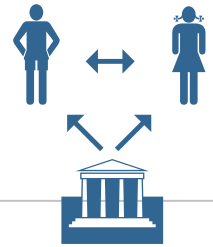
Techniken für Mehrseitige Sicherheit haben das Potential, Nutzer von IT-Systemen von Fremdbestimmung bzgl. ihrer (Un)-Sicherheit zu befreien.

Techniken für Mehrseitige Sicherheit

- Unilateral
  - Kryptographie zur Dateiverschlüsselung
  - Offenlegung Entwurf

- Selbstschutz-Beispiele
  - Verschlüsselung mit PGP, GnuPG
  - Filter: Webwasher, JunkBuster, CookieCooker
  - Personal Firewalls
  - Offene Betriebssysteme: Linux, BSD

- Bilateral
  - Kryptographie und Steganographie zur Kommunikation



  - Sichere Dienste anstelle ihrer unsicheren Vorläufer: telnet → ssh, ftp → scp, http → https

- Trilateral
  - Digitale Signatur und Public Key Infrastructures

- Multilateral
  - Anonymität, Unbeobachtbarkeit und Pseudonymität in Kommunikationsnetzen

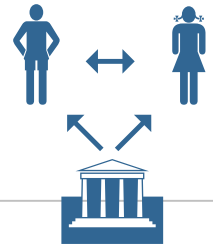
  - Anonymisierer: JAP, TOR

Techniken für Mehrseitige Sicherheit

- Unilateral
  - Kryptographie zur Dateiverschlüsselung
  - Offenlegung Entwurf

- Stand der Forschung?
  - Kryptographie: sehr gut
  - Betriebssysteme theoret.: sehr gut
  - Betriebssysteme praktisch: schlecht

- Bilateral
  - Kryptographie und Steganographie zur Kommunikation



  - Kryptographie: sehr gut
  - Steganographie: gut

- Trilateral
  - Digitale Signatur und Public Key Infrastructures
  - PKI: sehr gut

- Multilateral
  - Anonymität, Unbeobachtbarkeit und Pseudonymität in Kommunikationsnetzen

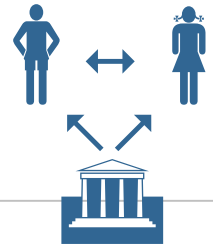
  - Anonymität theoretisch: sehr gut
  - Anonymität praktisch: befriedigend

Techniken für Mehrseitige Sicherheit

- Unilateral
  - Kryptographie zur Dateiverschlüsselung
  - Offenlegung Entwurf

- Regulierungsversuche?
  - Krypto-Verbot läuft leer, da «Kriminelle» auf Steganographie ausweichen können

- Bilateral
  - Kryptographie und Steganographie zur Kommunikation



  - Verbote laufen leer, da Steganographie nicht mehr erkennbar ist

- Trilateral
  - Digitale Signatur und Public Key Infrastructures

- Multilateral
  - Anonymität, Unbeobachtbarkeit und Pseudonymität in Kommunikationsnetzen

  - Vorratsdatenspeicherung ist weitestgehend sinnlos, da «Kriminelle» auf multilateral nutzbare Technik ausweichen, außerdem öffentliche Telefone, Prepaid Handies, offene WLANs, unsichere Bluetooth-Mobilfunkgeräte