Wie lässt sich Vertrauen technisch umsetzen?

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

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

Universität Regensburg

"Angst, Kontrolle, Vertrauen" · Impulsreferat · Akademie für politische Bildung Tutzing · 10. Juli 2010

~~Wie~~ Lässt sich Vertrauen technisch umsetzen?

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

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

Universität Regensburg

"Angst, Kontrolle, Vertrauen" · Impulsreferat · Akademie für politische Bildung Tutzing · 10. Juli 2010

Wie läßt sich Vertrauen technisch umsetzen?

- Vertrauen in
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit

- Eigentlich Schutz der ...

Vertraulichkeit

Gegensätzliche Schutzziele?

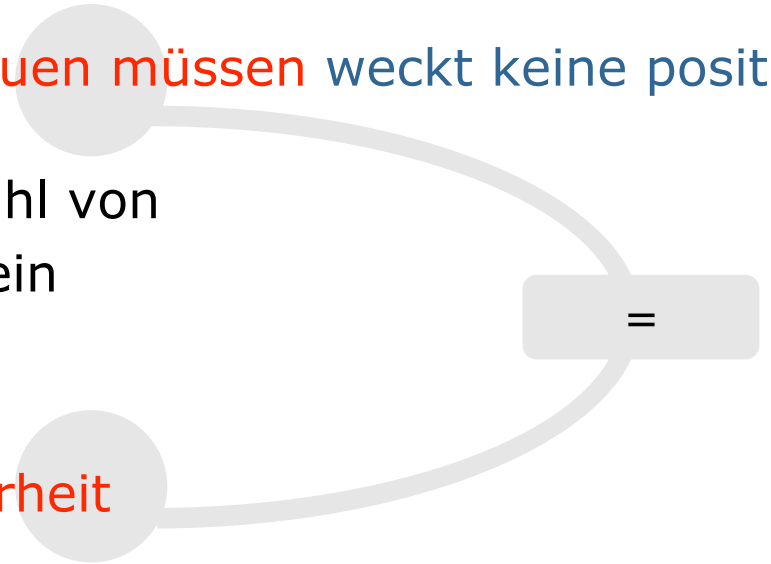
Integrität

Verfügbarkeit

Läßt sich Vertrauen technisch umsetzen?

- Ziel der Informationssicherheit: möglichst wenig Vertrauen in andere setzen müssen
  - Wo keine Sicherheit erreichbar ist, bleibt nur Vertrauen [müssen]

- Zwischenfazit: Vertrauen müssen weckt keine positiven Assoziationen
  - Stattdessen: Gefühl von
    - Ausgeliefert-sein
    - Angst
    - Kontrolle
    - eben: Unsicherheit



- Statt des Begriffs Vertrauen: Vertrauenswürdigkeit
  - Akteure werden in die Lage versetzt die bei der Nutzung von Informationstechnik entstehenden Risiken bzw. verbleibenden Restrisiken (für ihre Privatheit) zuverlässig abzuschätzen

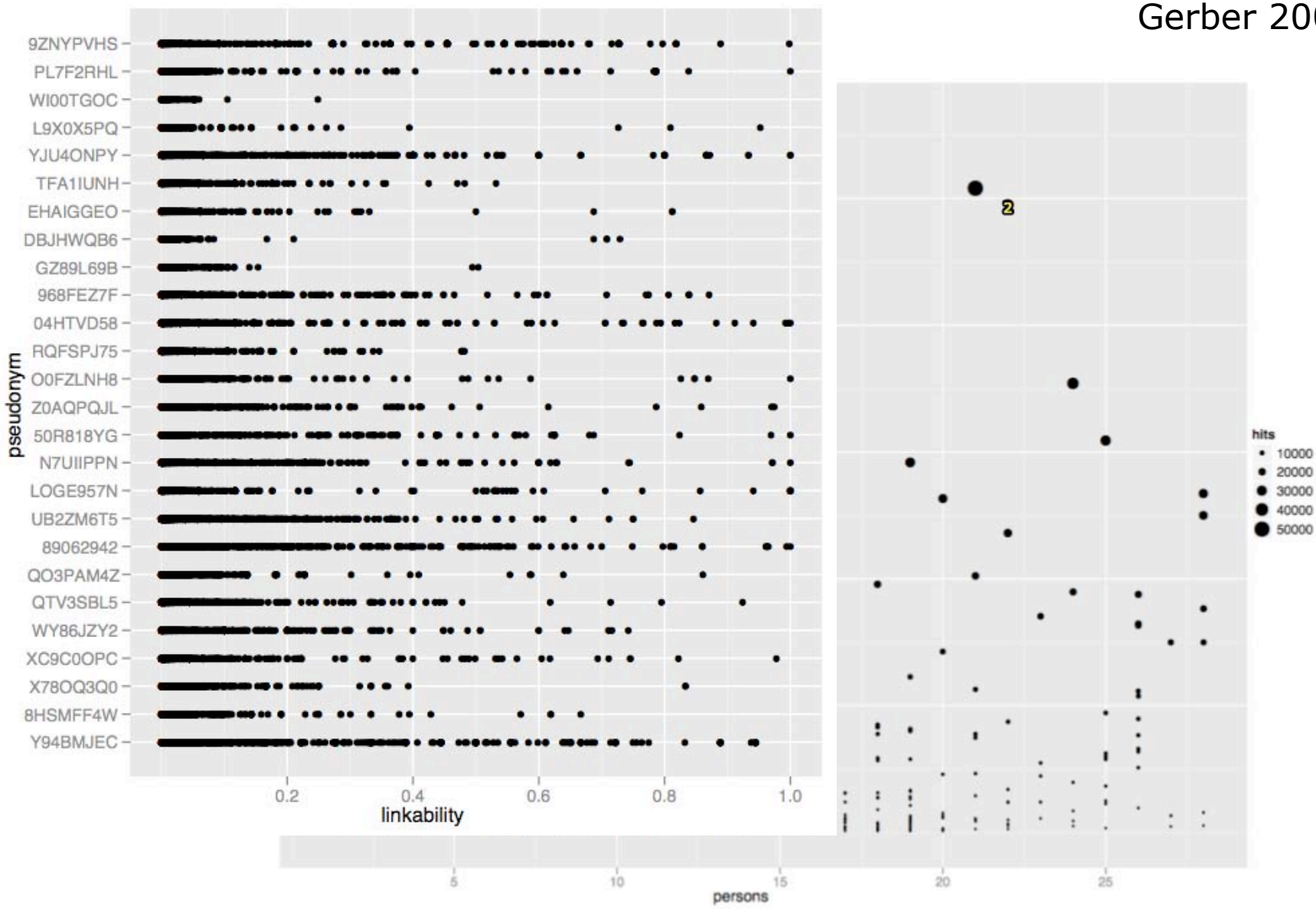
Beispiele, warum Unvertrauen notwendig ist

- Prof. Müglich (vor ca. 3,5 h):
  - „Die Statistiker sind viel weiter als wir glauben“

- Beispiele
  - Website- und DNS-Fingerprinting
  - Leylogger
  - Unsicherheit Fingerabdrücke
  - Usage Timelines inkl.ip-geotagging

Website- und DNS-Fingerprinting

Gerber 2009



Keylogger

- http://www.youtube.com/watch?v=8FYPHb828f4

- anbringen
- …
- warten
- entfernen
- auslesen
- …

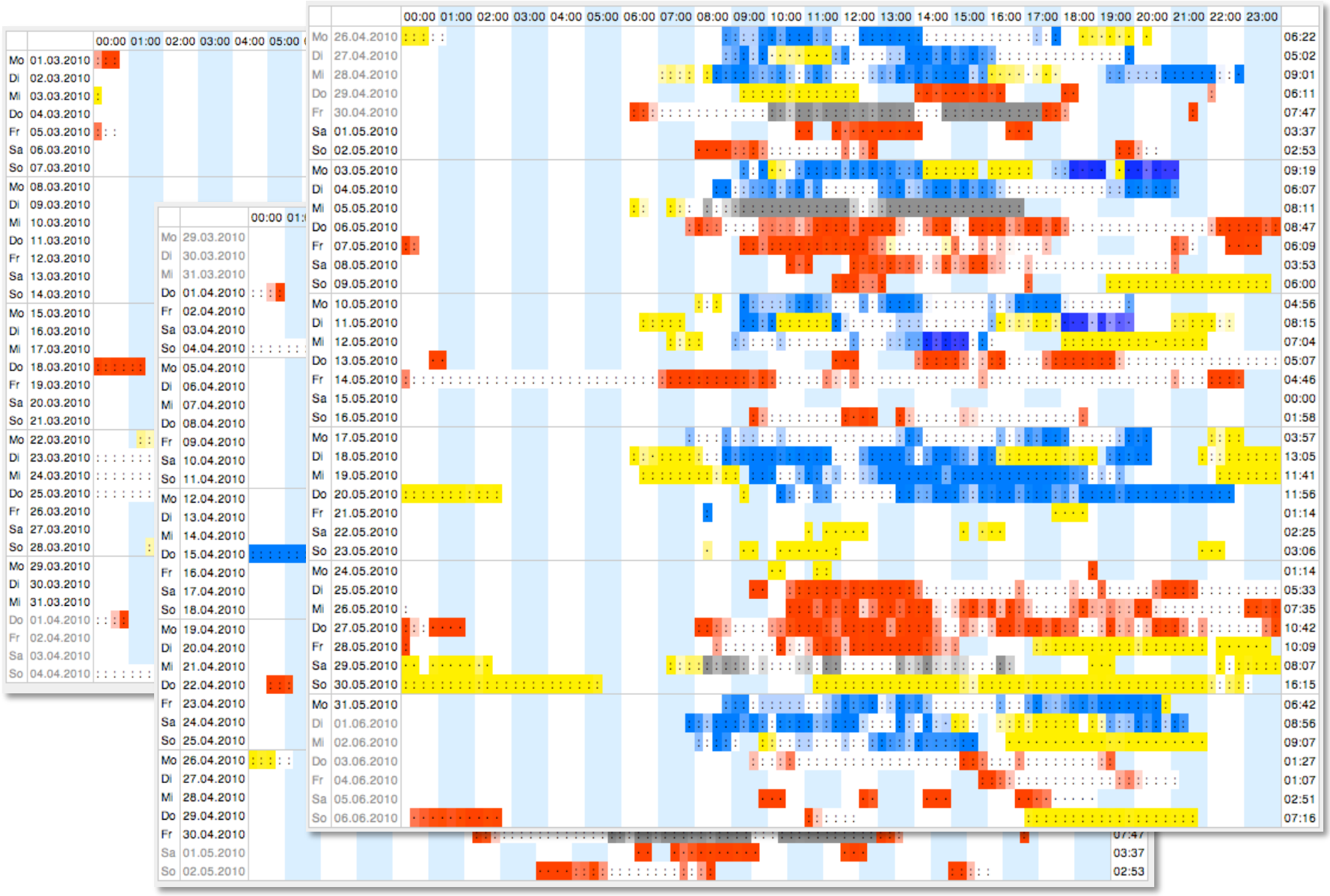
Fälschen eines Fingerabdrucks

- 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).

Usage Timelines inkl. ip-geo-tagging



Wege zu mehr Vertrauenswürdigkeit/Sicherheit/Verlässlichkeit

1. Als Anbieter von Technik

- Transparenz (i.S.v. Verstehbarkeit, Beherrschbarkeit)
- Offenheit (keine verdeckten kanäle, wohldefinierte Schnittstellen)
- Überprüfbarkeit (durch Experten: Auditierung/Zertifizierung, durch Nutzer: Testfälle)

2. Als Nutzer von Technik

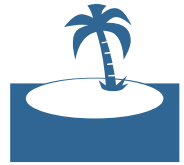
- Sensibilität (Respekt vor der Privatheit anderer)
- Vorsicht (i.S.v. Vermeidung riskanter Kommunikation)
- Selbstschutz (Einsatz von Schutzsoftware)

3. Als Staat

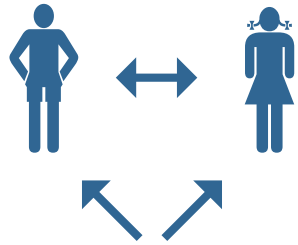
- Ausschöpfen des rechtlichen Rahmens
- Verbesserung des Wissensstands von Nutzern und Anbietern
- Technologieförderung (nicht nur Sicherheitsforschung im Bereich Anti-Terror)

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

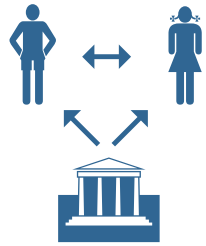
- Multilateral nutzbar
  - nur wenn viele Partner kooperieren

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

- Bilateral
  - Kryptographie und Steganographie zur Kommunikation



- Trilateral
  - Digitale Signatur und Public Key Infrastructures

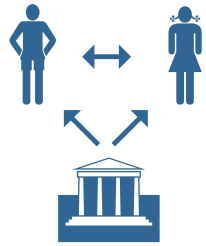
- Multilateral
  - Anonymität, Unbeobachtbarkeit und Pseudonymität in Kommunikationsnetzen

- Selbstschutz-Beispiele
  - Verschlüsselung mit PGP, GnuPG
  - Filtersoftware, Personal Firewalls
  - Offene Betriebssysteme: Linux, BSD
  - Sichere Dienste anstelle ihrer unsicheren Vorläufer: telnet → ssh, ftp → scp, http → https
  - HBCI
  - eGK
  - Anonymisierer: JAP, TOR

Techniken für Mehrseitige Sicherheit

- Unilateral
  - Kryptographie zur Dateiverschlüsselung
  - Offenlegung Entwurf

- Bilateral
  - Kryptographie und Steganographie zur Kommunikation



- Trilateral
  - Digitale Signatur und Public Key Infrastructures

- Multilateral
  - Anonymität, Unbeobachtbarkeit und Pseudonymität in Kommunikationsnetzen

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

  - Kryptographie: sehr gut
  - Steganographie: gut

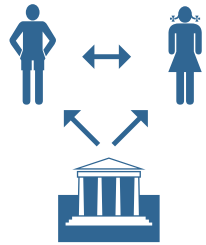
  - PKI: sehr gut

  - Anonymität theoretisch: sehr gut
  - Anonymität praktisch: befriedigend

Techniken für Mehrseitige Sicherheit

- Unilateral
  - Kryptographie zur Dateiverschlüsselung
  - Offenlegung Entwurf

- Bilateral
  - Kryptographie und Steganographie zur Kommunikation



- Trilateral
  - Digitale Signatur und Public Key Infrastructures

- Multilateral
  - Anonymität, Unbeobachtbarkeit und Pseudonymität in Kommunikationsnetzen

- Regulierungsversuche?
  - Krypto-Verbot läuft leer, da «Kriminelle» auf Steganographie ausweichen können
  - Verbote laufen leer, da Steganographie nicht mehr erkennbar ist
  - Vorratsdatenspeicherung ist weitestgehend sinnlos, da «Kriminelle» auf multilateral nutzbare Technik ausweichen, außerdem öffentliche Telefone, Prepaid Handies, offene WLANs, unsichere Bluetooth-Mobilfunkgeräte

Prof. Dr. Hannes Federrath
Lehrstuhl Management der Informationssicherheit
Universität Regensburg
D-93040 Regensburg

E-Mail: hannes.federrath@wiwi.uni-regensburg.de
WWW: http://www-sec.uni-regensburg.de

Phone +49-941-943-2870
Telefax +49-941-943-2888