Mehrseitige Sicherheit schafft Vertrauen

Prof. Dr. Hannes Federrath
Sicherheit in verteilten Systemen (SVS)

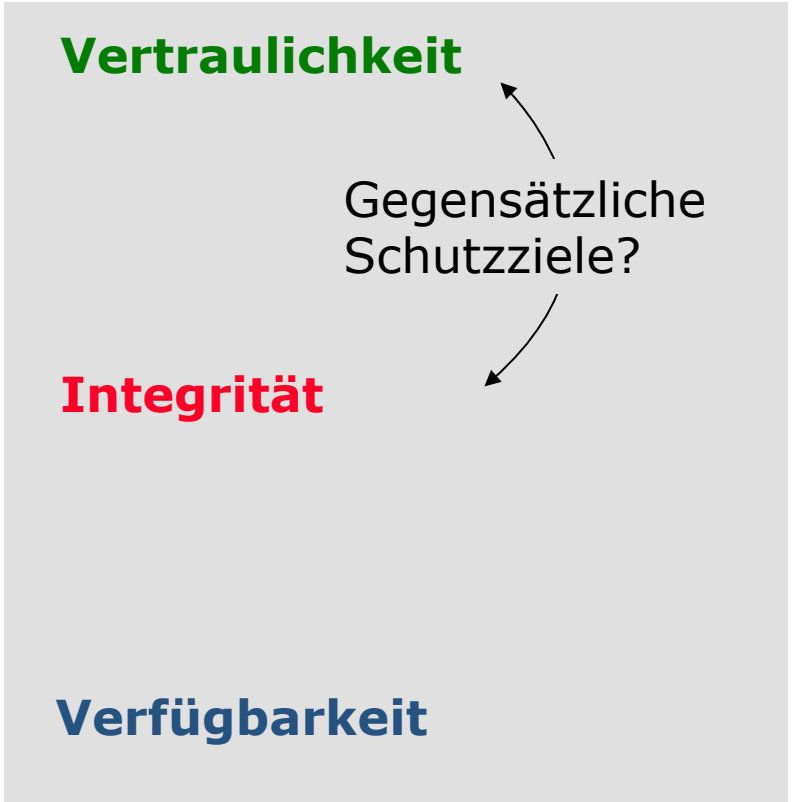
http://svs.informatik.uni-hamburg.de/

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Informatisches Kolloquium
Fachbereich Informatik
16. Januar 2013

Wie lässt sich Vertrauen technisch umsetzen?

- Schutzziele gehen zurück auf Voydock, Kent 1983
- Klassische IT-Sicherheit berücksichtigt im Wesentlichen Risiken, die durch regelwidriges Verhalten in IT-Systemen entstehen.



unbefugter Informationsgewinn

unbefugte Modifikation

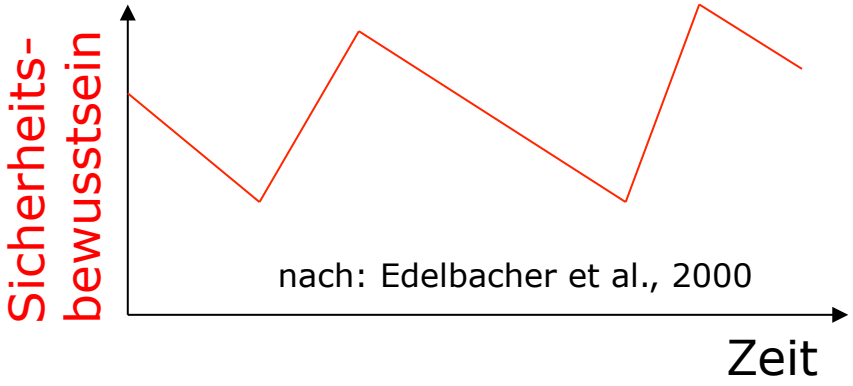
unbefugte Beeinträchtigung der Funktionalität

FUD-Strategie — Fear, Uncertainty, Doubt

Realistische Risikoeinschätzung

vs.

Furcht, Ungewissheit, Zweifel



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)

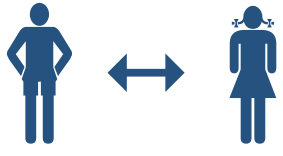
3. Als Staat

- 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

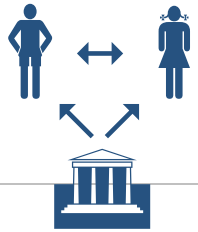
Techniken für Mehrseitige Sicherheit haben das Potential, Nutzer von IT-Systemen von Fremdbestimmung bzgl. ihrer (Un)-Sicherheit zu befreien.

Techniken für Mehrseitige Sicherheit

- Unilateral
  - Kryptographie zur Dateiverschlüsselung
  - Offenlegung Entwurf

- Selbstschutz-Beispiele
  - Verschlüsselung mit PGP, GnuPG
  - Filtersoftware, 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

  - HBCI
  - eGK

- Multilateral
  - Anonymität, Unbeobachtbarkeit und Pseudonymität in Kommunikationsnetzen

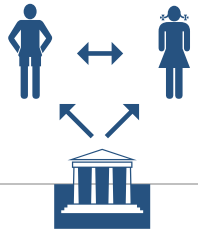
  - Anonymisierer: JAP, TOR

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

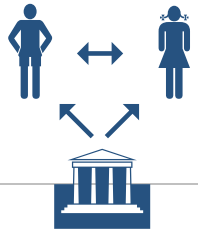
  - Anonymität theoretisch: sehr gut
  - Anonymität praktisch: befriedigend

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

Schlussfolgerungen

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

- Fazit: Vertrauen müssen weckt keine positiven Assoziationen
  - Stattdessen: Gefühl von
    - Angst
    - Unsicherheit
    - Zweifel

=

- 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

Prof. Dr. Hannes Federrath
FB Informatik, AB SVS
Universität Hamburg
Vogt-Kölln-Straße 30
D-22527 Hamburg

E-Mail federrath@informatik.uni-hamburg.de

Telefon +49 40 42883 2358

http://svs.informatik.uni-hamburg.de

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG