Datensicherheit und -schutz aus informationstechnischer Sicht

Andreas Pfitzmann

TU Dresden, Fakultät Informatik, D-01062 Dresden
Nöthnitzer Str. 46, Raum 3071
Tel.: 0351/ 463-38277, e-mail: pfitza@inf.tu-dresden.de, http://dud.inf.tu-dresden.de/

Gliederung

Was bedeutet Datensicherheit?
- Was ist zu schützen?
- Vor wem ist zu schützen?
- Wie und wodurch kann Sicherheit erreicht werden?
- Vorausschau auf Schutzmechanismen
- Angreifermodell
- Blindes vs. Überprüfendes Vertrauen

Was bedeutet Datenschutz?

Wichtige Datensicherheitsaspekte im Mautumfeld
- Ich lokalisiere mich vs. Ich werde lokalisiert
- Ich empfange vs. Ich sende
- Ich werde identifiziert vs. Ich bleibe anonym
- Mir wird Berechtigung zugeordnet vs. Ich weise meine Berechtigung nach

Wichtige Datenschutzaspekte im Mautumfeld
- Hilfssheriffisierung der Provider untergräbt Vertrauen
  - Abhörschnittstellen
  - Vorratsdatenspeicherung
- Freiwillige Teilnahme oder faktischer Benutzungszwang?
  - Opt-in vs. Opt-out

Balance gesucht
- Nutzen(verteilung) vs. Risiko(verteilung)

Bedrohungen und korrespondierende Schutzziele

Bedrohungen:	Schutzziele:
1) Informationsgewinn	Vertraulichkeit
2) Modifikation von Information	Integrität
3) Beeinträchtigung der Funktionalität	Verfügbarkeit für berechtigte Nutzer

1)	nicht erkennbar, aber verhinderbar;	nicht rückgängig zu machen
2)+3)	nicht verhinderbar, aber erkennbar;	rückgängig zu machen

Definitionen für die Schutzziele

Vertraulichkeit (confidentiality)

Informationen werden nur Berechtigten bekannt.

Integrität (integrity)

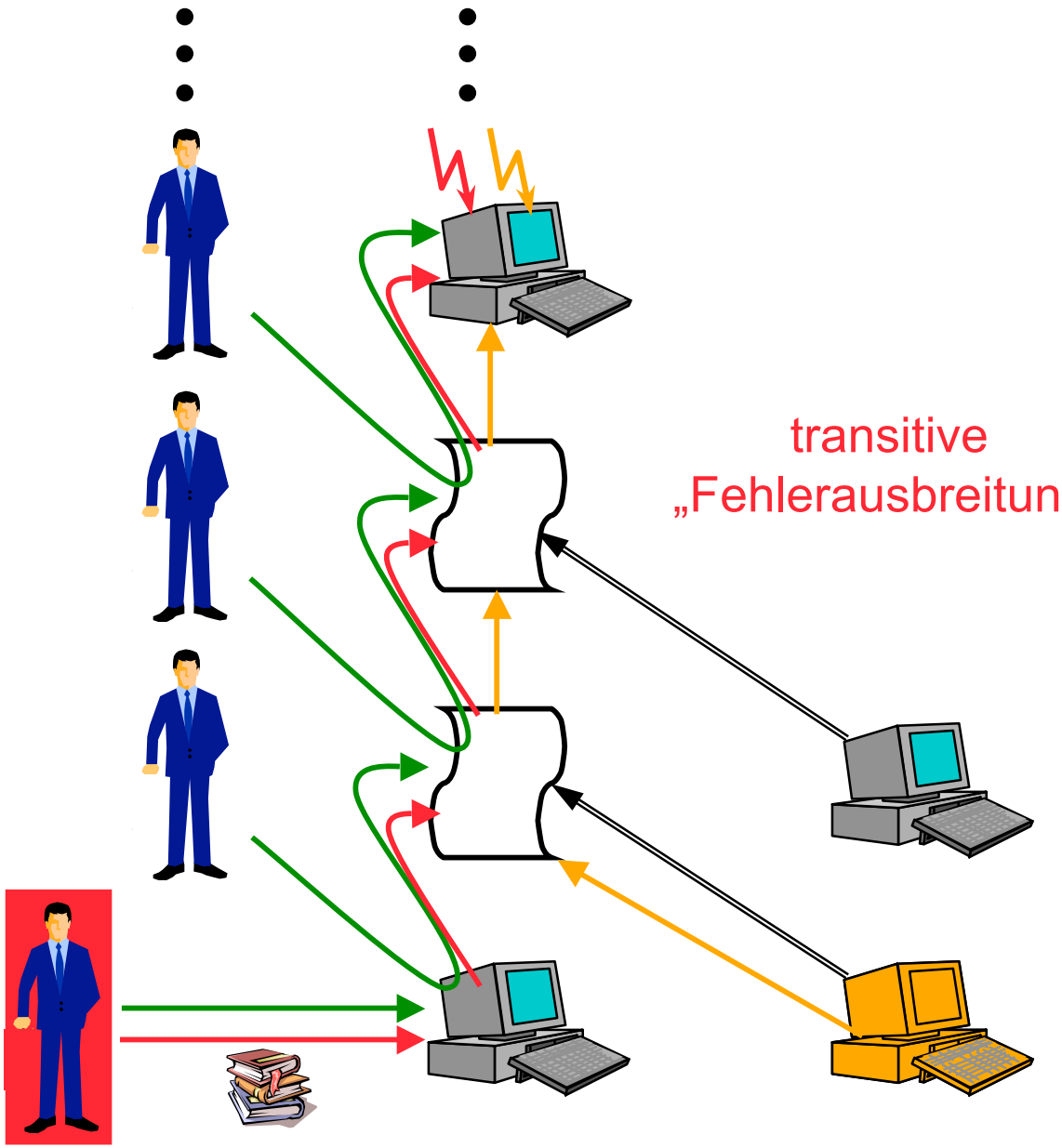
Informationen sind richtig, vollständig und aktuell oder aber dies ist erkennbar nicht der Fall.

Verfügbarkeit (availability)

Informationen sind dort und dann zugänglich, wo und wann sie von Berechtigten gebraucht werden.

- **subsumiert: Daten, Programme, Hardwarestrukturen**
- **es muss geklärt sein, wer in welcher Situation wozu berechtigt ist**
- **kann sich nur auf das Innere eines Systems beziehen**

Transitive Ausbreitung von Fehlern und Angriffen



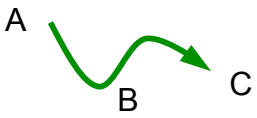
transitive
„Fehlerausbreitung“

Symbolerklärungen

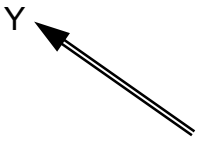
Rechner

Programm

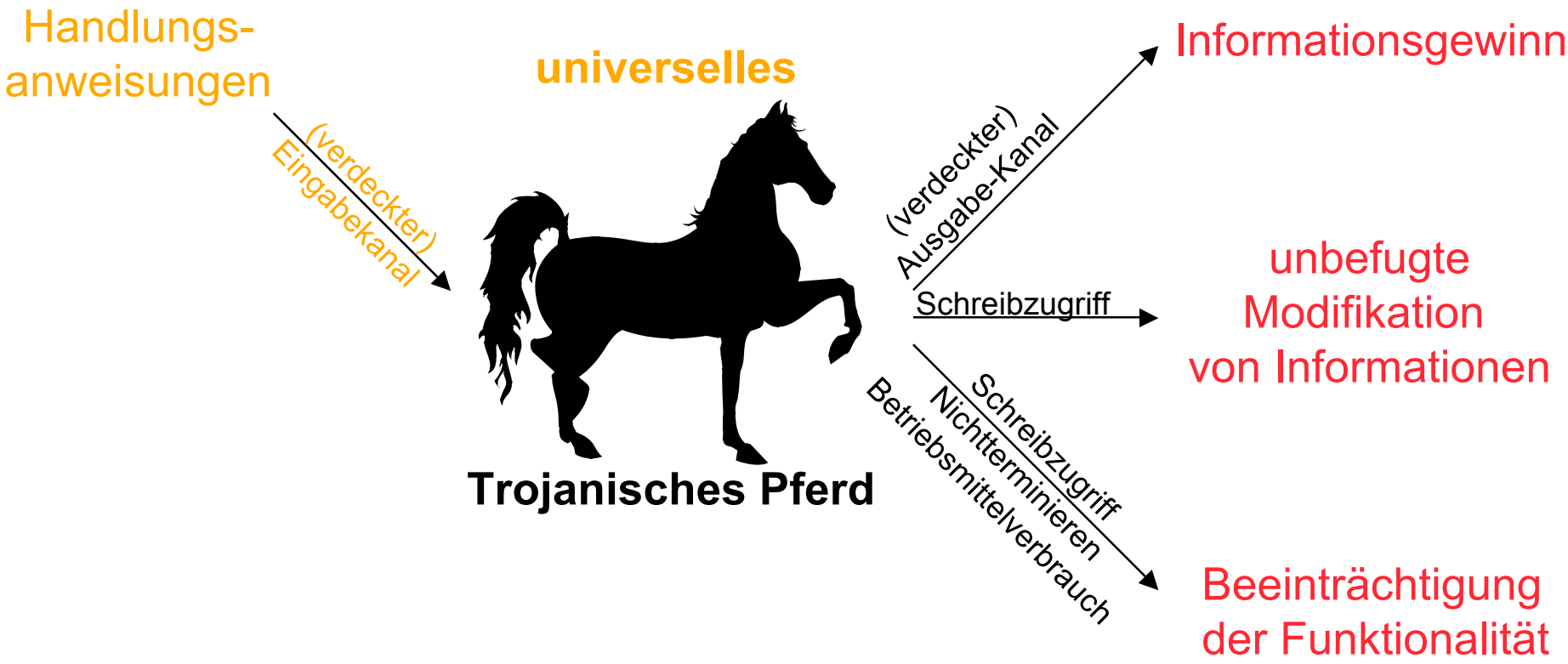
A benutzt B, um
C zu entwerfen



Maschine X führt
Programm Y aus



Universelles Trojanisches Pferd



Vor wem ist zu schützen ?

Naturgesetze und Naturgewalten

- Bauteile altern
- Überspannung (Blitzschlag, EMP)
- Spannungsausfall
- Überschwemmung (Sturmflut, Wasserrohrbruch)
- Temperaturänderungen ...

} Fehler-toleranz

Menschen

- Außenstehende
- Benutzer des Systems
- Betreiber des Systems
- Wartungsdienst
- Produzenten des Systems
- Entwerfer des Systems
- Produzenten der Entwurfs- und Produktionshilfsmittel
- Entwerfer der Entwurfs- und Produktionshilfsmittel
- Produzenten der Entwurfs- und Produktionshilfsmittel der Entwurfs- und Produktionshilfsmittel
- Entwerfer ... jeweils auch Benutzer, Betreiber, Wartungsdienst ... des verwendeten Systems

} Trojanisches Pferd
- universell
- transitiv

Welche Schutzmaßnahmen gegen welche Angreifer

Schutz bzgl. / Schutz vor	**Erwünschtes leisten**	**Unerwünschtes verhindern**
Entwerfer und Produzent der Entwurfs- und Produktionshilfsmittel	Zwischensprachen; Zwischenergebnisse, die unabhängig analysiert werden	
Entwerfer des Systems	wie oben + mehrere unabhängige Entwerfer	
Produzenten des Systems	unabhängige Analysen der Produkte	
Wartungsdienst	Kontrolle wie bei neuem Produkt, s. o.	
Betreiber des Systems		physischen Zugriff beschränken, logischen Zugriff beschränken und protokollieren
Benutzer des Systems	physischen und logischen Zugriff beschränken	
Außenstehende	physisch vom System, kryptographisch von den Daten fernhalten	

physische Verteilung und Redundanz

Unbeobachtbarkeit, Anonymität, Unverkettbarkeit:
Erfassungsmöglichkeit „unnötiger Daten“ vermeiden

Maximal berücksichtigte Stärke eines Angreifers

Angreifermodell

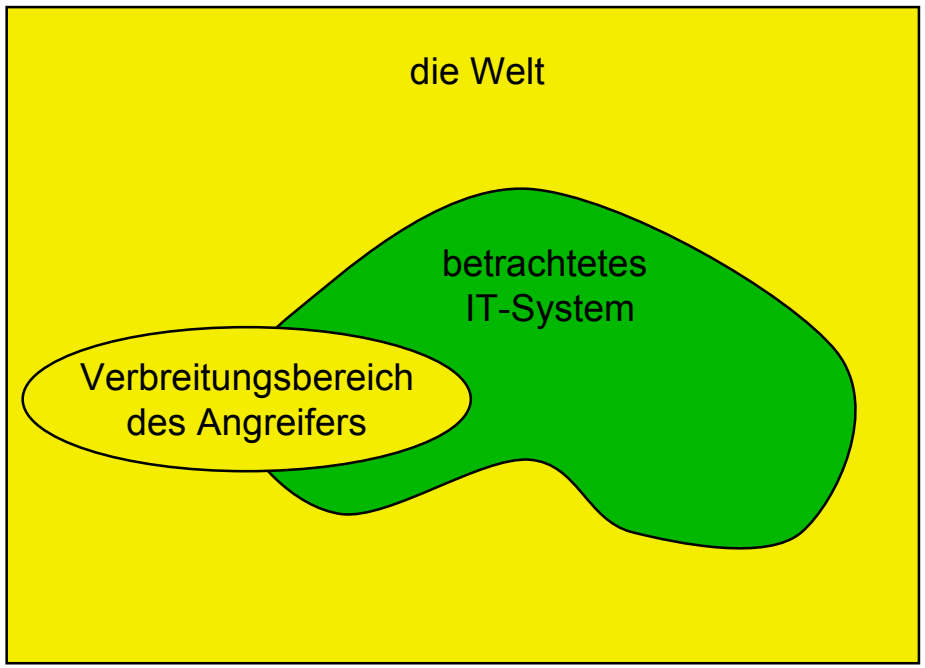
Schutz vor einem allmächtigen Angreifer ist unmöglich.

- Rollen des Angreifers (Außenstehender, Benutzer, Betreiber, Wartungsdienst, Produzent, Entwerfer …), *auch kombiniert*
- Verbreitung des Angreifers
- Verhalten des Angreifers
  - passiv / aktiv
  - beobachtend / verändernd (bzgl. seiner erlaubten Handlungen)
- dumm / intelligent
  - Rechenkapazität:
    - unbeschränkt: informationstheoretisch
    - beschränkt: komplexitätstheoretisch

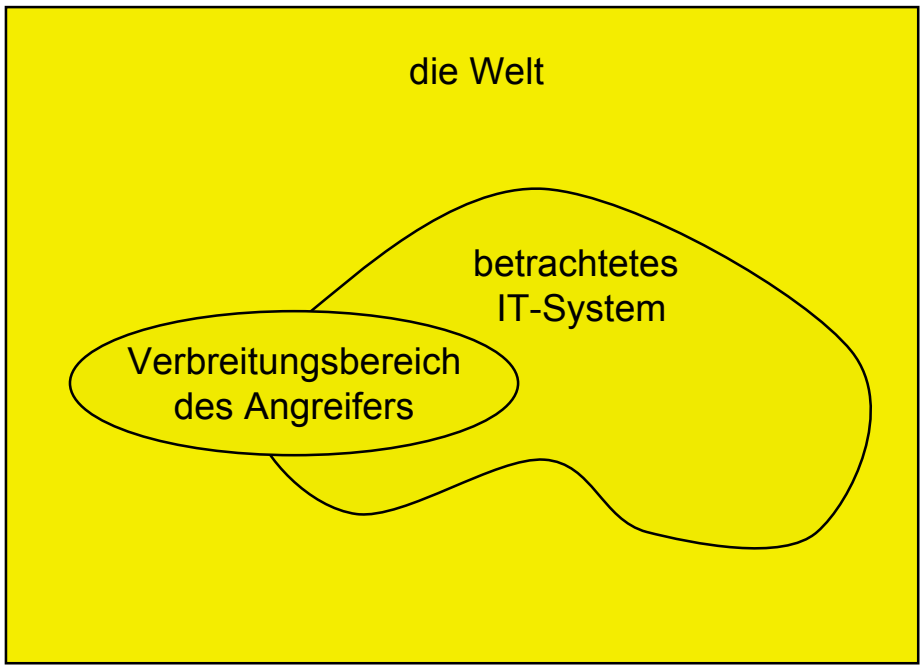
Geld

Zeit

Beobachtender vs. verändernder Angreifer



beobachtender Angreifer



verändernder Angreifer

nur erlaubtes Verhalten

auch verbotenes Verhalten

Blindes vs. Überprüfendes Vertrauen

Beispiele

- Mental Poker
- Massenspeicher: USB-Stick, Festplatte

Blindes Vertrauen: Ich kann nicht überprüfen, ob mein Vertrauen gerechtfertigt ist bzw. war.

Überprüfendes Vertrauen: Ich kann überprüfen, ob mein Vertrauen gerechtfertigt war ... Und daran mein Verhalten anpassen.

Vertrauen in die Wahrung von Vertraulichkeitseigenschaften ist nahezu immer blind, Vertrauen in die Wahrung von Integritäts- und Verfügbarkeitseigenschaften ist typischerweise überprüfend.

Was bedeutet Datenschutz?

Umsetzung des **Grundrechts auf Informationelle Selbstbestimmung**: Jeder hat das **Recht, grundsätzlich selbst zu bestimmen, wer bei welcher Gelegenheit was über ihn weiß**.

„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. […] Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist. Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art 2 Abs. 1 in Verbindung mit Art 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf "informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig.“

BVerfG 15. Dez. 1983

Wichtige Datensicherheitsaspekte im Mautumfeld

Ich lokalisiere mich GPS	vs.	Ich werde lokalisiert mobilfunk- oder RFID-basiert
Ich empfange GPS, Radio	vs.	Ich sende mobilfunk- oder RFID-basiert
Ich werde identifiziert Dig. Signaturen, Adressen, analoge Funkcharakteristika	vs.	Ich bleibe anonym Dig. Pseudonyme, nur empfangen oder aufwendiger Schutz des Senders
Mir wird Berechtigung zugeordnet aufbauend auf Identifizierung	vs.	Ich weise meine Berechtigung nach Tickets, umrechenbare Credentials

Wichtige Datenschutzaspekte im Mautumfeld

- Hilfssheriffisierung der Provider untergräbt Vertrauen
  - Abhörschnittstellen
  - Vorratsdatenspeicherung

- Freiwillige Teilnahme oder faktischer Benutzungszwang?
  - Opt-in vs. Opt-out

Balance gesucht

- Nutzen(verteilung) vs. Risiko(verteilung)
  - Innerhalb von Anwendungen
  - Über Anwendungen und Infrastrukturen hinweg
  - Schutz der strukturell Schwächeren
    - Macht
    - Know how
    - (Infrastruktur)Nutzer

Gemeinsamer Rahmen für Datensicherheit und Datenschutz?

- Wäre sehr wünschenswert
- Durchaus denkbar:

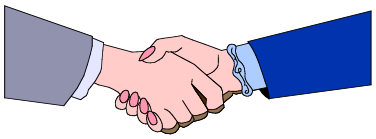
Mehrseitige Sicherheit

Mehrseitige Sicherheit

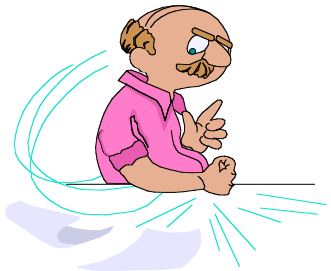
- Jeder Beteiligte hat eigene Sicherheitsinteressen.

- Jeder Beteiligte kann seine Sicherheitsinteressen formulieren.

- Konflikte werden erkannt und Lösungen ausgehandelt.



- Jeder Beteiligte kann seine Sicherheitsinteressen in den ausgehandelten Lösungen durchsetzen.



Sicherheit mit minimalen Annahmen über andere