

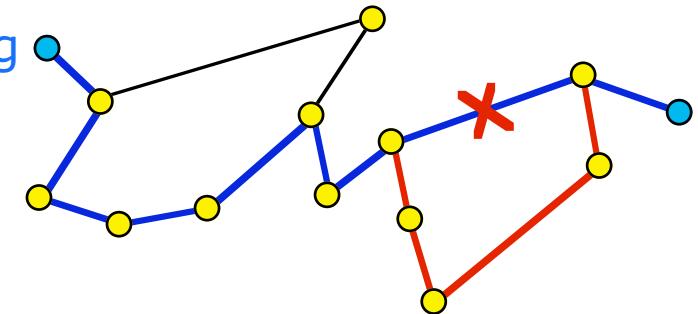


Einführung in die IT-Sicherheit

Schutzziele
Mehrseitige Sicherheit
Angreifermodell

Einführung: Internet

- Architektur
 - stark vermaschter Graph von einzelnen Computernetzen
 - international, organisationsübergreifend
 - weltweit standardisierte Kommunikationsprotokolle
 - ausgewählte Dienste sind ebenfalls standardisiert
 - ursprünglich entwickelt für Hochverfügbarkeit
 - **alternative Routen:**
unterbrochener Kommunikationsweg führt nicht zwangsläufig zu Verlust von Verfügbarkeit
 - **verteiltes System:**
Adresse (URL) und Speicher- bzw. Abrufort können räumlich unabhängig sein
- alle Inhalte werden in Pakete verpackt

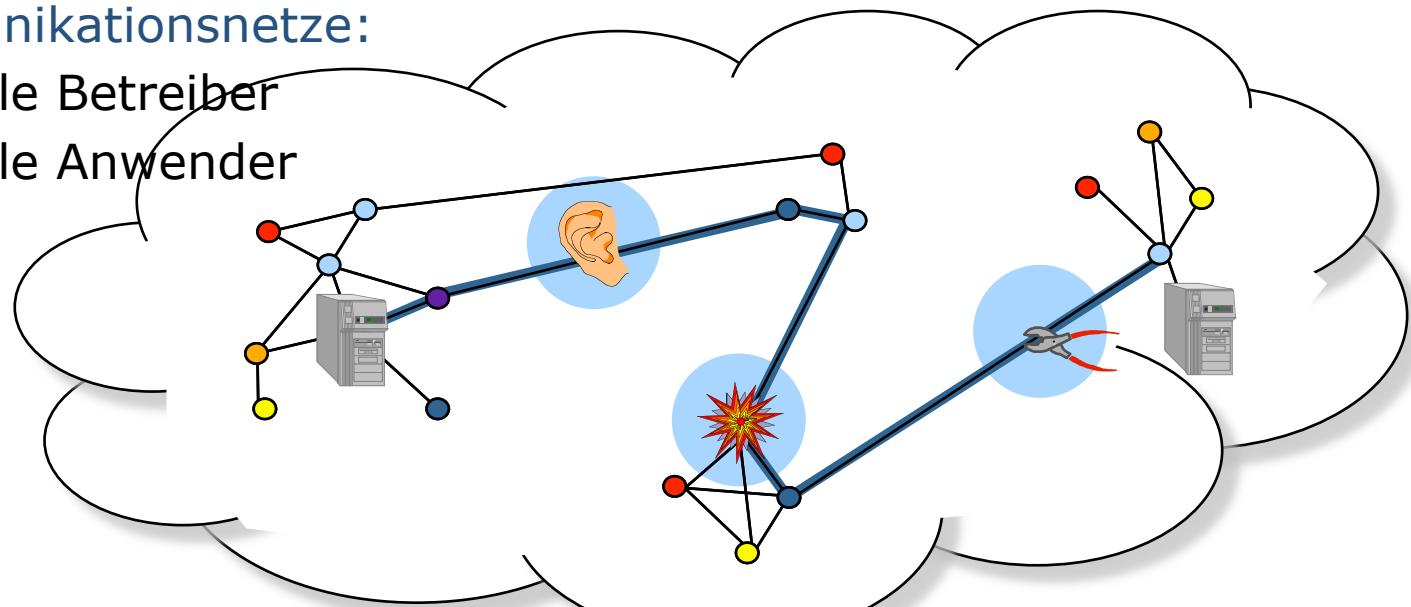


Header (Adresse, ...)

Payload („Bitkette“)

Sicherheit in Rechnernetzen

- **Telekommunikationsnetze:**
 - sehr viele Betreiber
 - sehr viele Anwender



Bedrohungen



unbefugter Informationsgewinn



unbefugte Modifikation



unbefugte Beeinträchtigung der Funktionalität

Schutz der

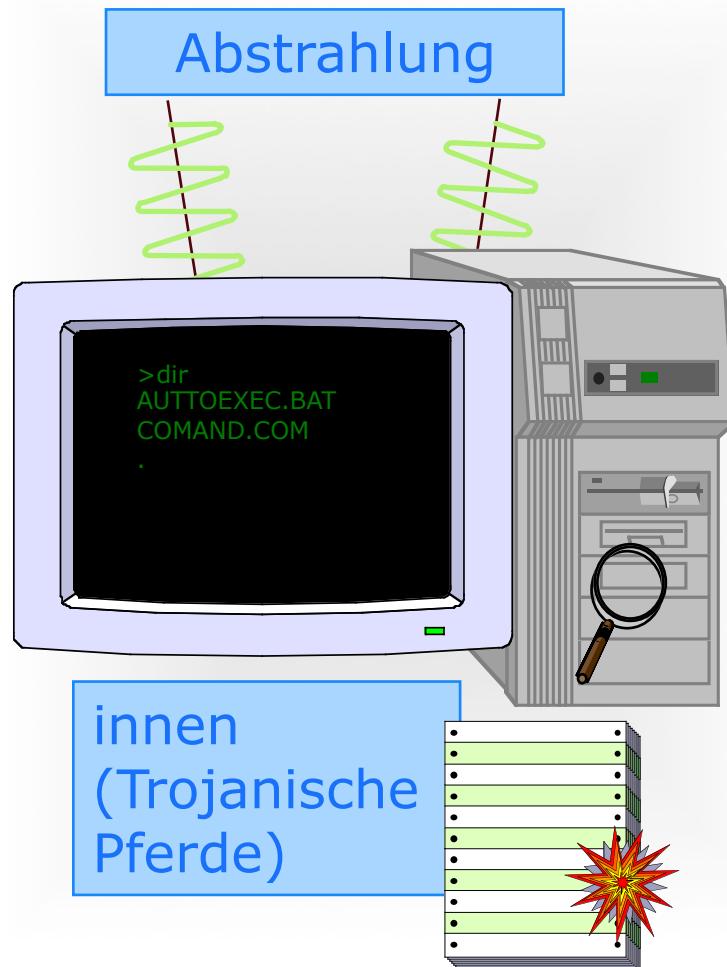
Vertraulichkeit

Integrität

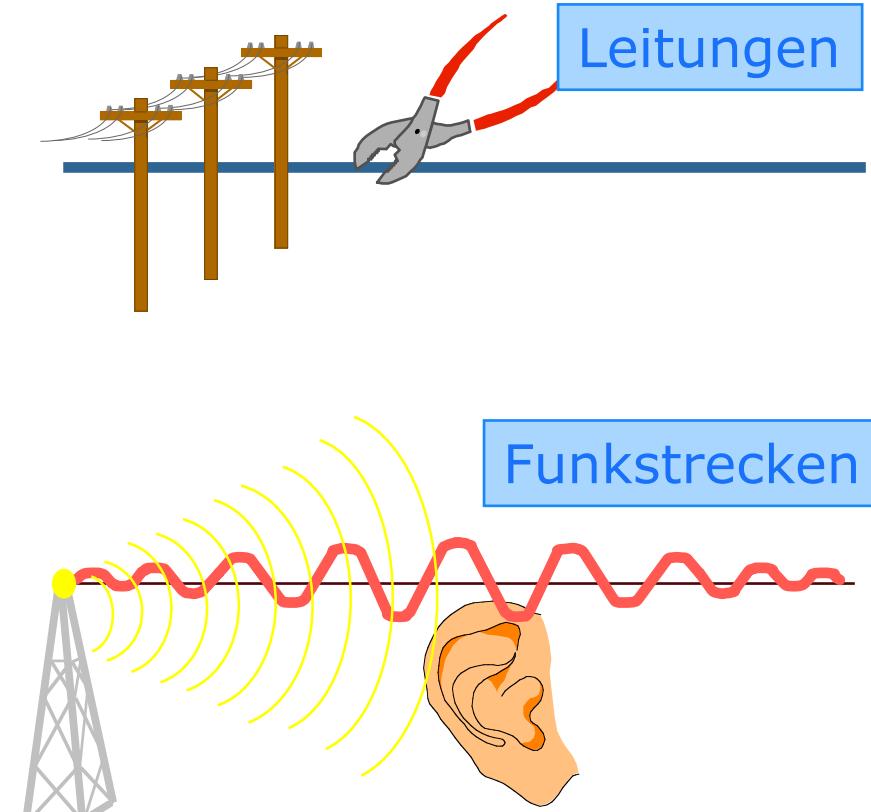
Verfügbarkeit

Angriffspunkte

Rechner

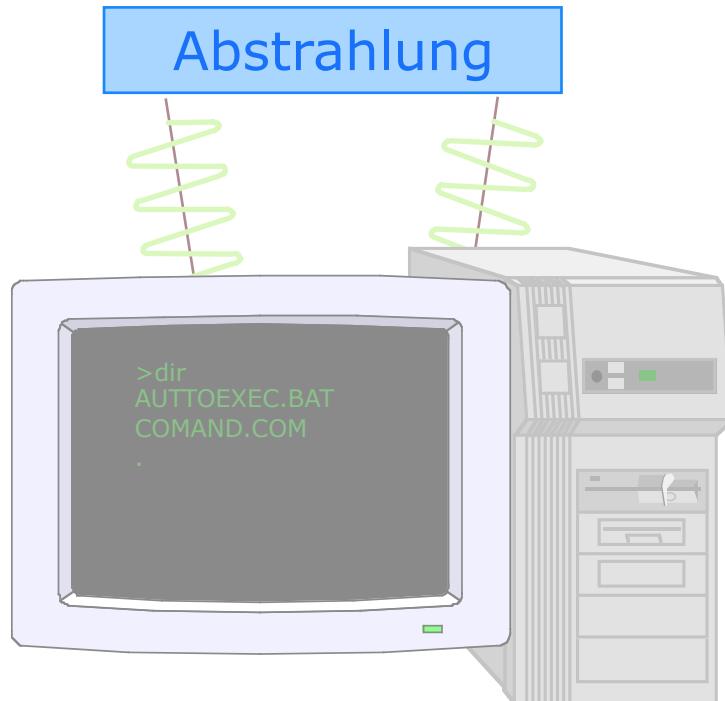


Übertragungswege



Angriffspunkte

Rechner



auch optische
Abstrahlung in
Betracht ziehen!

Computerzeitung Nr. 14

2. April 2002 S. 5

DATENSPIONAGE

Flackernde LEDs verraten Geheimnisse

Auburn (pk) – Wer seine IT völlig abhörsicher machen will, darf wohl nur noch in fensterlosen Räumen arbeiten: Forscher in den USA und Großbritannien haben Wege gefunden, aus dem Licht, das Monitore und Status-LEDs abstrahlen, Daten auszulesen.

Der Lockheed-Martin-Ingenieur Joe Loughry und der Uni-Professor David Umphress aus Auburn in Alabama haben entdeckt, dass die flackernden Leuchtdioden an Rechnern, Modems oder Switches oft in hohem Maße den tatsächlichen Datenstrom widerspiegeln, der durch sie hindurchläuft. Mit einem Fernrohr und entsprechendem Equipment lassen sich auf diese Weise Rechner quasi durchs Fenster ausspionieren – bis zu einer Entfernung von 20 Metern. Allerdings sinkt die Erkennungsquote mit steigender Datenübertragungsrate. Am anfälligsten waren Modems, bei schnellen Ethernet-Karten etwa war Spionieren nicht möglich.

Die Nachrichtendienste scheinen in der Methode denn auch keine große Bedrohung zu sehen. Der US-Supergeheimdienst NSA, bei dem Loughry und Umphress ihr Forschungspapier (www.applied-math.org/optical_tempest.pdf) vor-

sorglich eingereicht hatten, hat es ohne Auflagen zur Veröffentlichung freigegeben. Außerdem, so räumen die Autoren ein, reicht notfalls ein Stück schwarzes Klebeband über dem Lämpchen als Mittel zur Spionageabwehr.

Einen anderen Weg zur Rekonstruktion von Computerdaten aus Licht ist Markus G. Kuhn von der Cambridge University gegangen

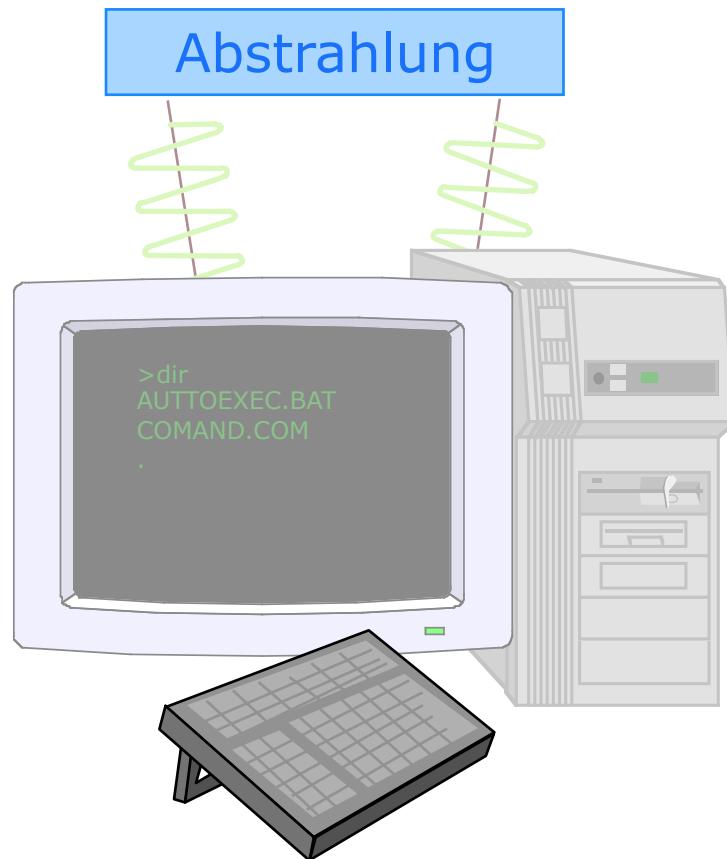


Verräterisch: Flackernde LEDs lassen Rückschlüsse auf die Daten zu.
Foto: Koller

gen (www.cl.cam.ac.uk/~mgk25/icee02-optical.pdf). Er hat aus der Reflexion eines Monitorbilds an einer 1,5 Meter entfernten weißen Wand mithilfe spezieller Algorithmen den auf dem Bildschirm dargestellten Text weitgehend rekonstruiert – mithilfe von starken Teleskopen auch aus 100 Metern Entfernung.

Angriffspunkte

Rechner



... auch Tastaturklappern?

Sicherheitsproblem: Tastaturgeräusch verrät Passwort

Michael Kanellos, Joachim Kaufmann | 15.09.05, 15:15 Uhr

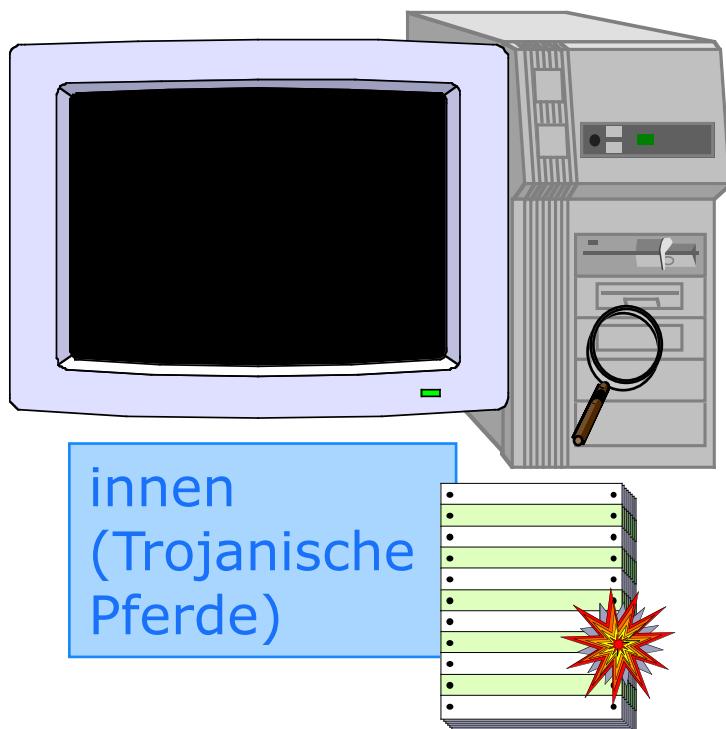
Wissenschaftler an der University of Berkeley in Kalifornien haben eine Software entwickelt, die anhand der Tastaturgeräusche den eingetippten Text ausgibt. Das Verfahren funktioniert mit über 90 Prozent Genauigkeit und könnte auch für Passwörter eine neue Gefahr darstellen. Mit mehreren zehn Minuten langen Tonaufzeichnungen von tippenden Anwendern wurden 96 Prozent der Zeichen richtig erkannt. Die Technik wurde auch von Hintergrundmusik oder klingelnden Handys nicht beeinträchtigt.

Die Studie der University of Berkeley weist besonders auf die Gefahr für Passwörter hin. "Das ist kein geheimnisvoller Angriff. Er benötigt etwas Know-how im Bereich der Computerwissenschaften, ansonsten braucht man nur noch einige Komponenten, die frei verfügbar sind. Wir haben das mit einem Zehn-Dollar-Mikrofon gemacht", so Universitätsprofessor Doug Tygar. "Über Passwörter als Mechanismus für die Authentifizierung solle neu nachgedacht werden."

Zum selben Ergebnis sind auch Analysten einer Security-Konferenz von Gartner gekommen, die diese Woche in London abgehalten wurde. Das Risiko, dass Passwörter geknackt werden, steige immer weiter, da entsprechende Tools leichter zu beziehen seien. Aufgrund des immer schwierigeren Umgangs mit komplexen Passwörtern ergeben sich den Experten zufolge neue Risiken.

Quelle: http://www.zdnet.de/news/wirtschaft_sicherheit_security_sicherheitsproblem_tastaturgeraeusch_verraet_passwort_story-39001024-39136538-1.htm

Angriffspunkte



Angreifer kann alle drei Schutzziele verletzen:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Sicherheit: Abgrenzung von Security & Safety

SECURITY

Schutz gegen beabsichtigte Angriffe

Vertraulichkeit

- Abhörsicherheit
- Sicherheit gegen unbefugten Gerätezugriff
- Anonymität
- Unbeobachtbarkeit

Integrität

- Übertragungsintegrität
- Zurechenbarkeit
- Abrechnungsintegrität

Verfügbarkeit

- Ermöglichen von Kommunikation

SAFETY

Schutz vor unbeabsichtigten Ereignissen

Fehlertoleranz

Verfügbarkeit

- Funktionssicherheit
- Technische Sicherheit
- Schutz vor Überspannung, Überschwemmung, Temperaturschwankungen
- Schutz vor Spannungsausfall

Sonstige Schutzziele

- Maßnahmen gegen hohe Gesundheitsbelastung
- ...

Sicherheit

Informationssicherheit

Freiheit v. Gefährd. f.d. *Daten* des IT-Systems

Vertraulichkeit

- Abhörsicherheit
- Sicherheit gegen unbefugten Gerätezugriff
- Anonymität
- Unbeobachtbarkeit

Integrität

- Übertragungsintegrität
- Zurechenbarkeit
- Abrechnungsintegrität

Verfügbarkeit

- Ermöglichen von Kommunikation

Technische Sicherheit

Freiheit v. Gefährd. f.d. *Umgebung* des IT-Systems

Verfügbarkeit

- Funktionssicherheit
- Technische Sicherheit
- Schutz vor Überspannung, Überschwemmung, Temperaturschwankungen
- Schutz vor Spannungsausfall

Zuverlässigkeit (reliability)

- Korrektheit

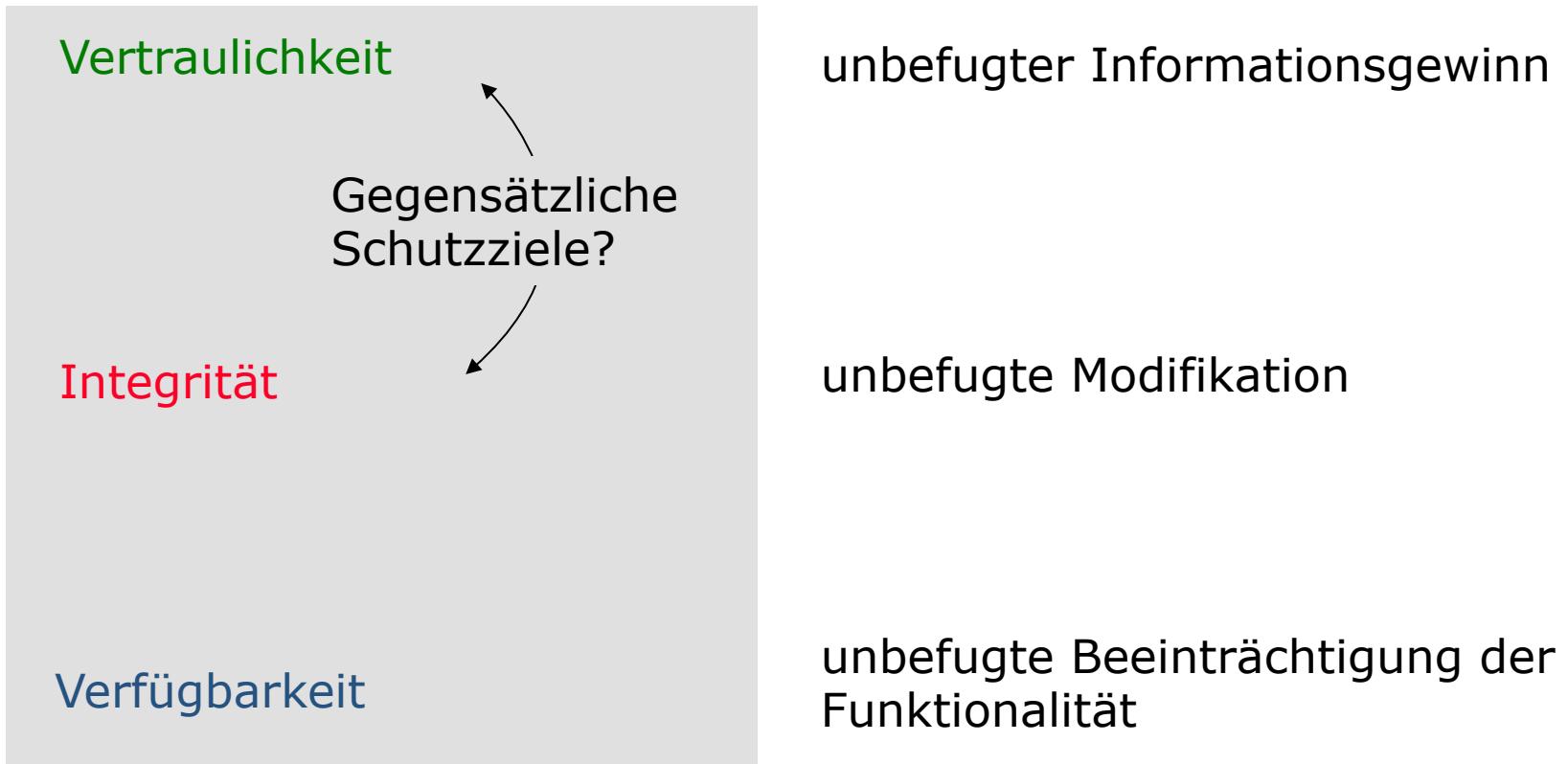
Sonstige Schutzziele

- Maßnahmen gegen hohe Gesundheitsbelastung
- ...

Schutzziele

Voydock, Kent 1983

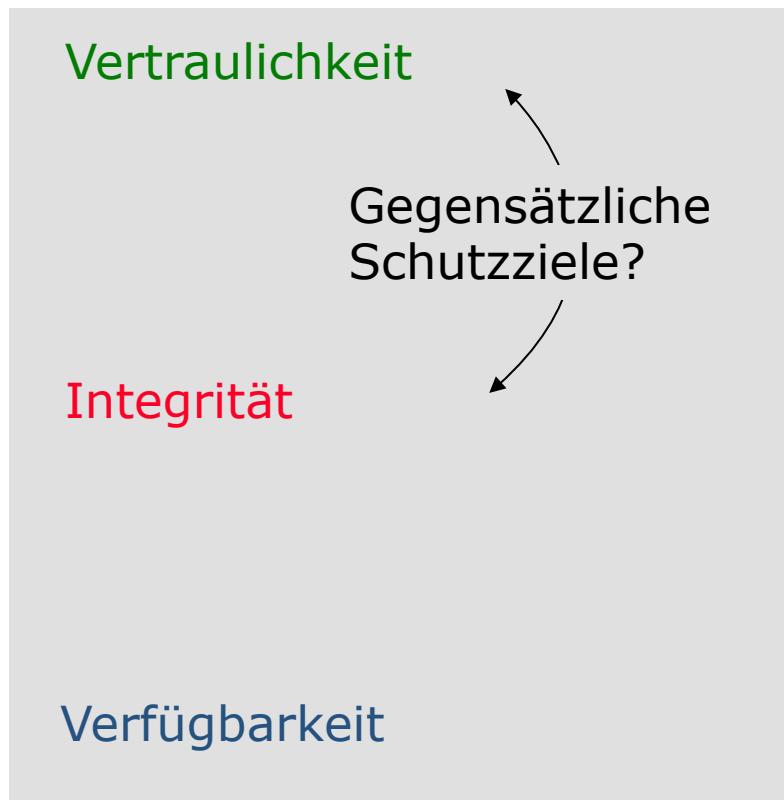
- Klassische IT-Sicherheit berücksichtigt im Wesentlichen Risiken, die durch *regelwidriges Verhalten* in IT-Systemen entstehen.



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

Schutzziele der mehrseitigen Sicherheit

Kommunikationsgegenstand

Was?, Worüber?

Inhaltsdaten

Vertraulichkeit

Verdecktheit

Inhalte

Integrität

Inhalte

Verfügbarkeit

Inhalte

Kommunikationsumstände

Wann?, Wo?, Wer?

Verkehrsdaten

Anonymität

Unbeobachtbarkeit

Sender

Ort

Empfänger

Zurechenbarkeit

Rechtsverbindlichkeit

Absender

Bezahlung

Empfänger

Erreichbarkeit

Nutzer

Rechner

Vertraulichkeit: Schutzziele und Angreifermodell

Inhaltsdaten

Vertraulichkeit
Verdecktheit

Inhalte

Verkehrsdaten

Anonymität
Unbeobachtbarkeit

Sender

Ort

Empfänger

- **Outsider**
 - Abhören auf Kommunikationsleitungen
 - Verkehrsanalysen
- **Insider**
 - Netzbetreiber oder bösartige Mitarbeiter (Verkehrsprofile)
 - Staatliche Organisationen (insb. fremde)

Vertraulichkeit: Verfahren und Algorithmen

Was wird geschützt?

Beispiele für Verfahren

Beispiele für Algorithmen

Inhaltsdaten

Vertraulichkeit

Verschlüsselung

Inhalte

DES, 3-DES, OTP, IDEA, AES,
RSA, ElGamal, ...

Verdecktheit

Steganographie

Inhalte + Existenz

F5, ...

Verkehrsdaten

Anonymität Unbeobachtbarkeit

Sender

Ort

Empfänger

Web-Anonymisierer,
Remailer, anonyme
Zahlungssysteme

Pseudonyme, Proxies,
umkodierende Mixe, DC
Netz, Private Information
Retrieval, ...

Integrität und Zurechenbarkeit, Rechtsverbindlichkeit

Verfahren

Algorithmen

Inhaltsdaten

Integrität

Inhalte

Message Authentication Codes

Challenge-Response-Authentikation

Kommunikationsumstände
Wann?, Wo?, Wer?

Zurechenbarkeit
Rechtsverbindlichkeit

auch:
Authentizität
Unabstreichbarkeit

Absender

Bezahlung

Empfänger

Digitale Signaturen

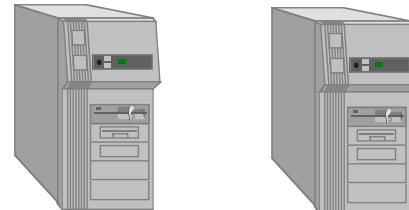
RSA, ElGamal, ...

Verfügbarkeit: Redundanz und Diversität

Redundanz

Mehrfache Auslegung von Systemkomponenten

Bei Ausfall übernimmt Ersatzkomponente



Diversität

Verschiedenartigkeit der Herkünfte

Tolerieren von systemat. Fehlern und verdeckten trojanischen Pferden

Unabhängige Entwicklung von redundanten (Software)-Komponenten

Verfügbarkeit

Inhalte

Erreichbarkeit

Nutzer

Rechner

Schutzziele: Definitionen

- **Vertraulichkeit:** Geheimhaltung von Daten während der Übertragung. Niemand außer den Kommunikationspartnern kann den Inhalt der Kommunikation erkennen.
Verdecktheit: Versteckte Übertragung von vertraulichen Daten. Niemand außer den Kommunikationspartnern kann die Existenz eines vertraulichen Inhalts erkennen.
- **Anonymität:** Nutzer können Ressourcen und Dienste benutzen, ohne ihre Identität zu offenbaren. Selbst der Kommunikationspartner erfährt nicht die Identität.
Unbeobachtbarkeit: Nutzer können Ressourcen und Dienste benutzen, ohne dass andere dies beobachten können. Dritte können weder das Senden noch den Erhalt von Nachrichten beobachten.
- **Integrität:** Modifikationen der kommunizierten Inhalte (Absender eingeschlossen) werden durch den Empfänger erkannt.
Zurechenbarkeit: Sendern bzw. Empfängern von Informationen kann das Senden bzw. der Empfang der Informationen bewiesen werden. Wechselwirkungen zwischen Schutzz Zielen
- **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.
Rechtsverbindlichkeit: Ein Nutzer kann rechtlich belangt werden, um seine Verantwortlichkeiten innerhalb einer angemessenen Zeit zu erfüllen.

Einseitige oder mehrseitige Sicherheit?

Kommunikationspartner haben nicht immer gleiche Sicherheitsinteressen

Kunde

Der Händler soll an meine Bestellung gebunden sein.

Ich möchte anonym bleiben, solange ich nichts kaufe.

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

Ich möchte anonym bleiben beim Einkauf.

Der Händler soll keine Kundenprofile anlegen dürfen.

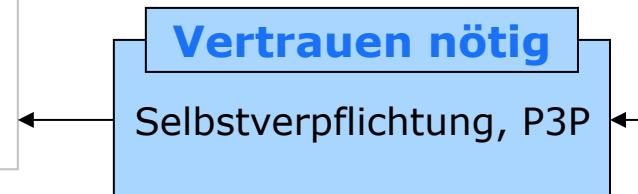
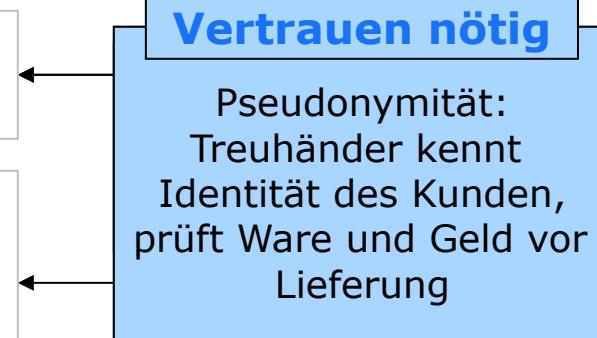
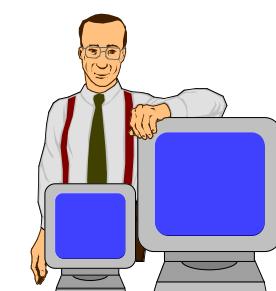


Händler

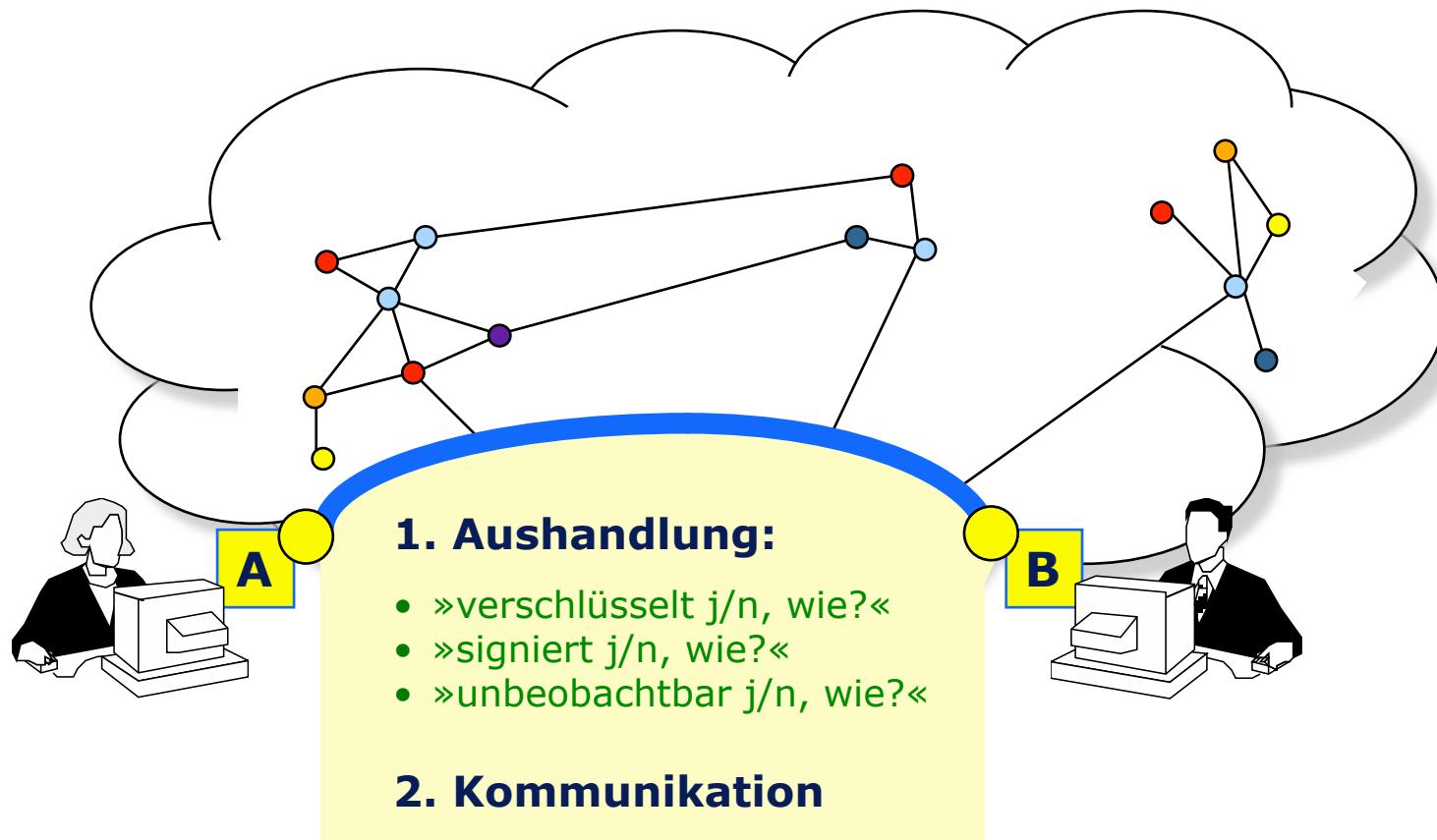
Der Kunde soll an seine Bestellung gebunden sein.

Der Kunde soll sich identifizieren.

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

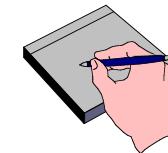


Formulierung und Aushandlung



Mehrseitige Sicherheit

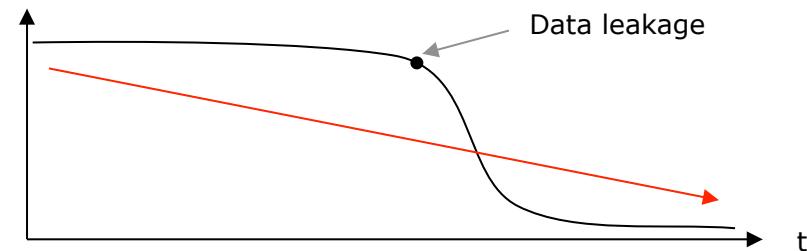
- **Definition**
 - Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung.
- **Vorgehen**
 1. Sicherheitsinteressen formulieren
 - Setzt Verständnis des Benutzers 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«



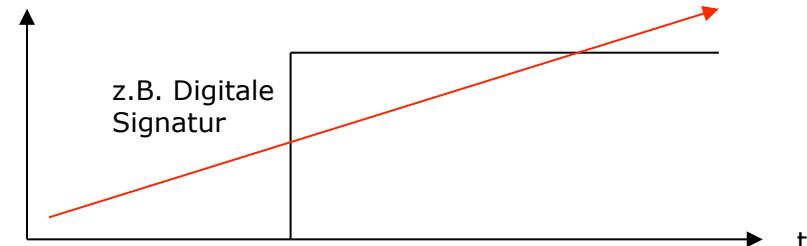
Beobachtungen zum Monotonieverhalten

- Das Monotonieverhalten von Schutzz Zielen gibt Hinweise auf die Prioritäten bei der Umsetzung von Schutzz Zielen und das praktisch erreichbare Schutzniveau.

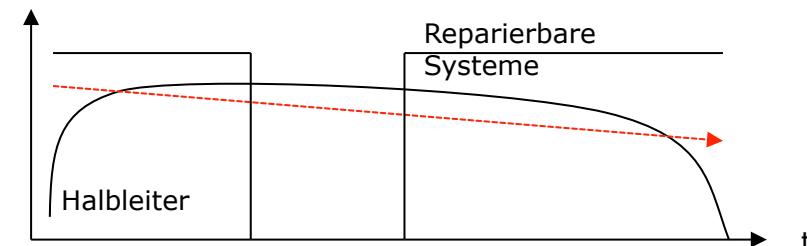
Vertraulichkeit



Integrität

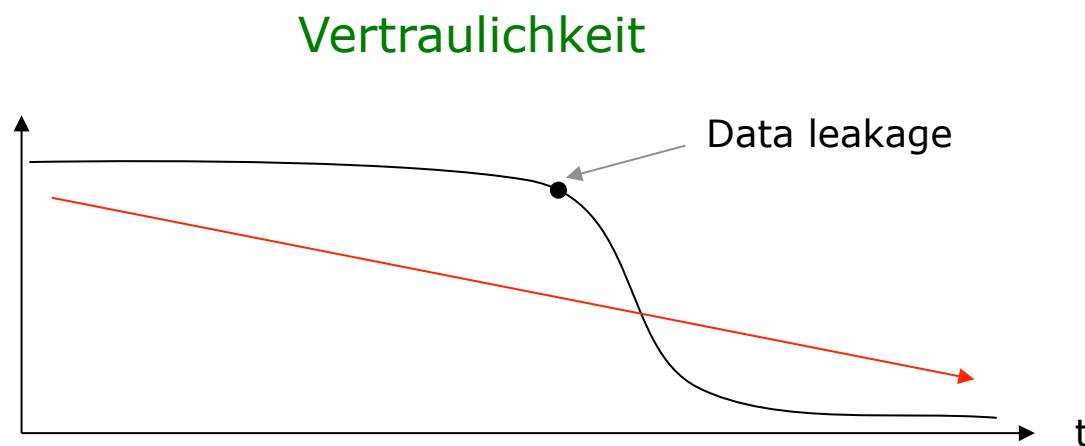


Verfügbarkeit



Beobachtungen zum Monotonieverhalten

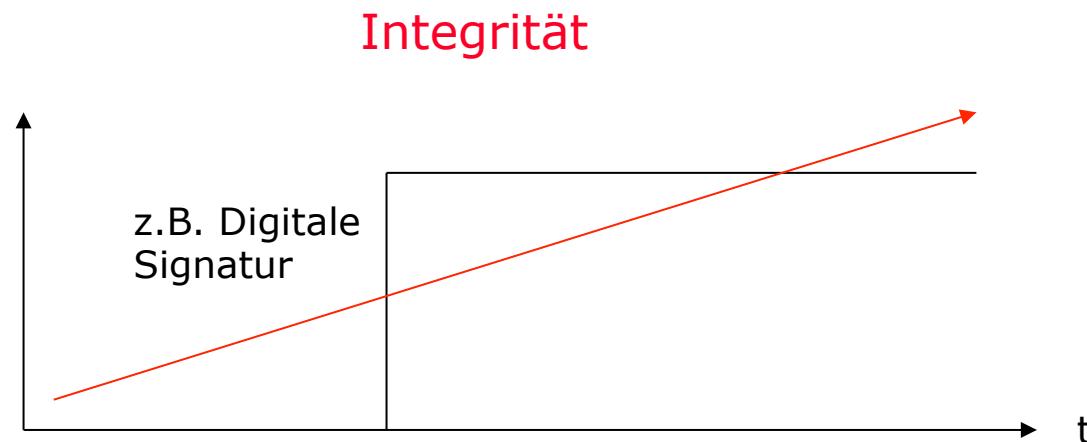
- Vertraulichkeit, Verdecktheit, Anonymität und Unbeobachtbarkeit können nur geringer werden.



Sensible Daten müssen besonders sorgsam und mit hoher Priorisierung geschützt werden.

Beobachtungen zum Monotonieverhalten

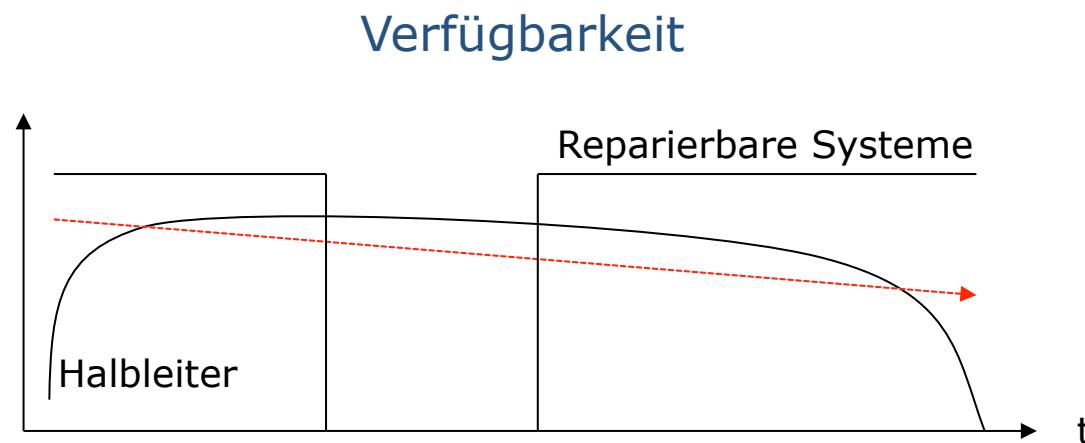
- Integrität, Zurechenbarkeit und Rechtsverbindlichkeit können nur größer werden.



Ist einmal die Authentizität von Daten (auf technischer Ebene) festgestellt, geht sie nicht mehr verloren.

Beobachtungen zum Monotonieverhalten

- Verfügbarkeit und Erreichbarkeit verhalten nicht monoton (häufig unstetig und doch langfristig meist regressiv).



Es sind stets nur probabilistische Aussagen zur Verfügbarkeit möglich.

Vor wem ist zu schützen?

- **Angreifer**
 - Außenstehende,
 - Benutzer des Systems,
 - Kommunikationspartner,
 - 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 der ...



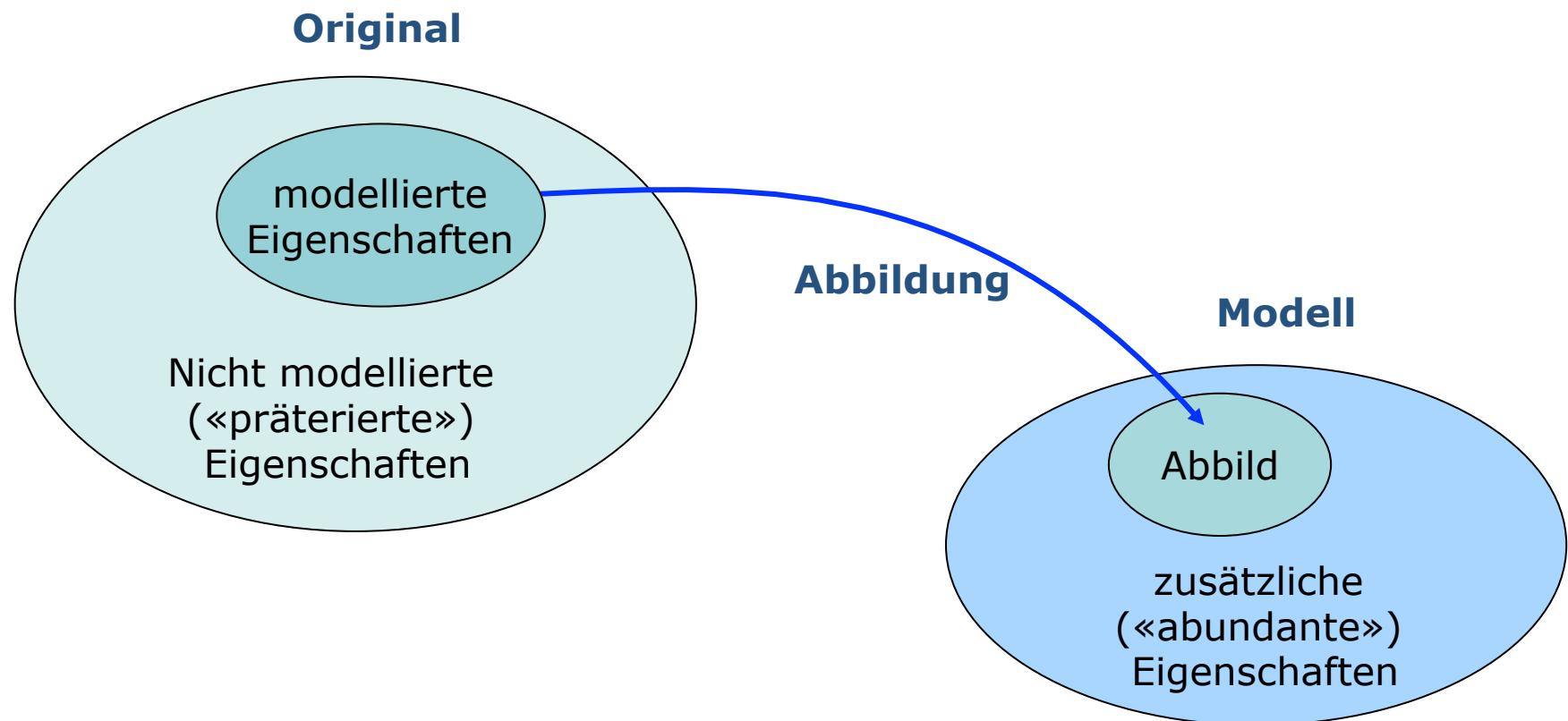
Angreifermodell

Schutz vor einem allmächtigen Angreifer ist unmöglich.

Das Angreifermodell definiert die maximal berücksichtigte Stärke eines Angreifers, gegen den ein Schutzmechanismus gerade noch wirkt.

- Es beschreibt
 - Rollen des Angreifers (Außenstehender, Benutzer, Betreiber, Wartungsdienst, Produzent, Entwerfer ...), auch kombiniert
 - Verbreitung des Angreifers (Stellen im System, an denen der Angreifer Informationen gewinnen oder Systemzustände verändern kann)
 - Verhalten des Angreifers
 - passiv / aktiv, beobachtend / verändernd
 - Rechenkapazität des Angreifers
 - unbeschränkt: informationstheoretisch
 - beschränkt: komplexitätstheoretisch
-
- The diagram consists of two blue rectangular boxes stacked vertically. The top box is labeled 'Geld' and the bottom box is labeled 'Zeit'. A vertical blue line connects them. From the top of this vertical line, another vertical blue line extends upwards and to the left, ending in a small square bracket that encloses the first bullet point of the list. From the bottom of this vertical line, another vertical blue line extends downwards and to the left, ending in a small square bracket that encloses the last bullet point of the list.

Original und Modell nach H. Stachowiak



H. Stachowiak: Allgemeine Modelltheorie. Springer-Verlag, Wien 1973

Merkmale eines Modells



1. Abbildung:

- Modelle stehen immer in Bezug zu einem Original, das sie abbilden.

2. Verkürzung:

- erfassen i. Allg. nicht alle Attribute des durch sie repräsentierten Originals

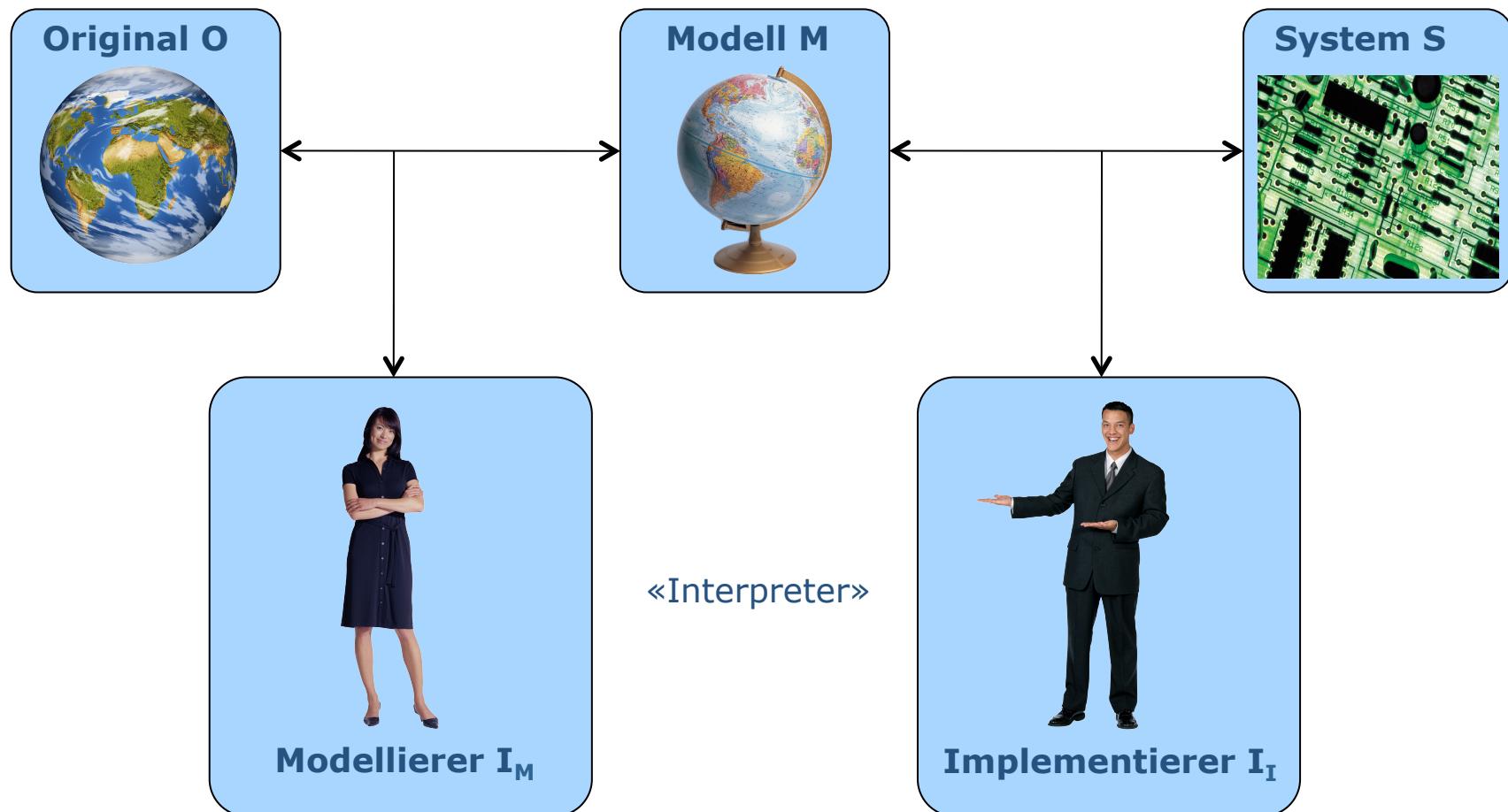
3. Pragmatismus:

- sind ihren Originalen nicht per se eindeutig zugeordnet, sondern ihre Ersetzungsfunktion erfüllen sie für bestimmte Subjekte unter bestimmten Einschränkungen

- Unterscheidung

- Deskriptives Modell (z.B. Stadtplan): beschreibt ein Original zum leichteren Verständnis
 - Präskriptives Modell (z.B. Bebauungsplan): trägt zur Erstellung eines Originals bei (z.B. Entwurfsmodell)

Modell als Nach- und Vorbild im Software-Prozess

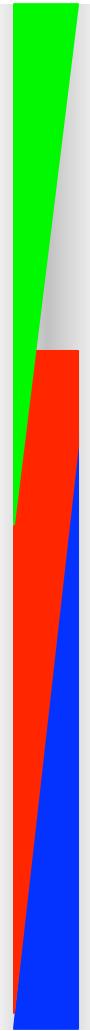


W. Hesse, H.C. Mayr: Modellierung in der Softwaretechnik: eine Bestandsaufnahme. Informatik-Spektrum 31/5 (2008) 381

Verhalten des Angreifers

	Aktiv	Passiv	Verletzbare Schutzziele
Beobachtend	(√) (etwas Berechtigtes tun und dabei Information gewinnen)	√	Vertraulichkeit
Verändernd	√	Ø	Vertraulichkeit, Integrität, Verfügbarkeit

Angriffsformen

- **Passive Angriffe**
 - Lauschangriff (eavesdropping)
 - Verkehrsflussanalyse (traffic analysis)
 - **Aktive Angriffe**
 - Maskerade (masquerading)
 - Man-in-the-middle attack
 - Verändern von Daten (modification)
 - Einfügen von Daten (injection)
 - Wiederholen (replay)
 - Fluten (flooding, spamming)
 - Dienstverweigerung (denial of service)
- 
- Vertraulichkeit
- Integrität
- Verfügbarkeit

Typische Angriffsfolge

1. Informationsgewinnung

- IP-Adressen, Passwörter, Eindringpunkte

Beispiele: Social Engineering, Security/Port Scanner

2. Angriff (über das Netz)

- Ausnutzen von Schwächen, Missbrauch von Daten



3. Erweiterung der Rechte

- insb. Schaffen einer unauffälligen Hintertür

4. Spuren verwischen

- Löschen oder Manipulieren von Log-Dateien

Schutz z.B. TrueWORM – Write Once Read Multiple mittels CD-R, DVD±R