Sicherheit im Ubiquitous Computing: Schutz durch Gebote?

Prof. Dr. Günter Müller

Institut für Informatik und Gesellschaft, Abteilung Telematik
Albert-Ludwigs-Universität Freiburg

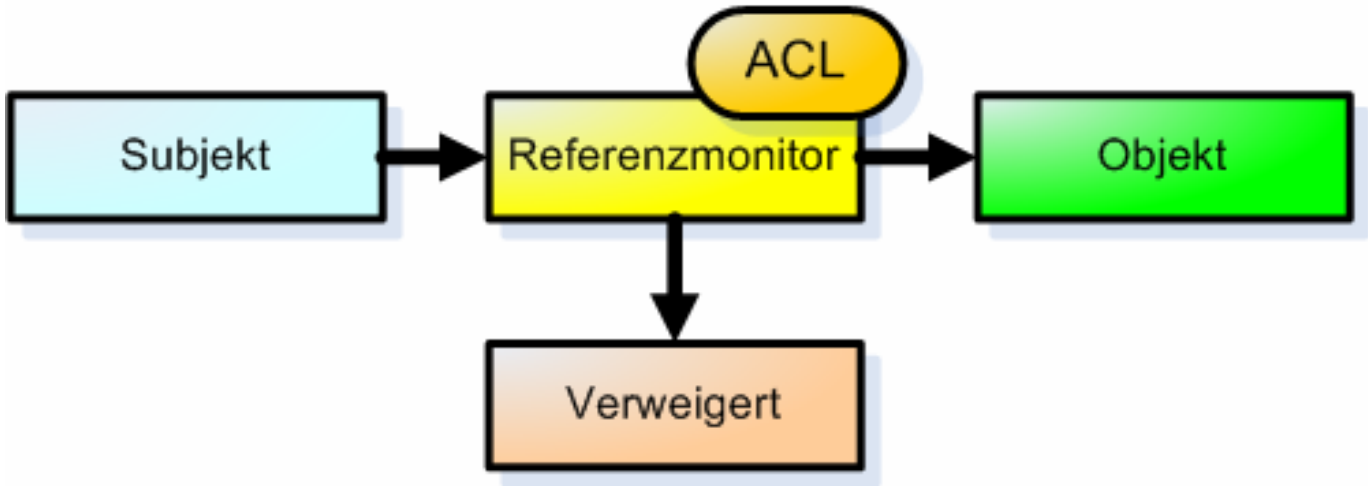
Der Computer im 21. Jahrhundert
Die Informatisierung des Alltags
ETH-Zürich, 22. März 2005

Gliederung

1. Sicherheit war und ist Zugangskontrolle
2. In Informationssystemen mit UC ist Sicherheit anders
3. Sicherheit in UC: „Richtige Antwort auf die falsche Frage“
4. Bisherige Sicherheitsverfahren sind Verbote
5. Zusätzliche Sicherheit: Schutz durch Gebote

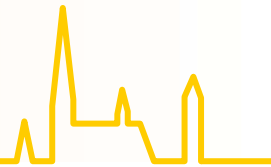
Sicherheit war und ist Zugangskontrolle

Zugangskontrolle = Authentifizierung + Autorisierung



B. Lampson, M. Abadi, M. Burrows, E. Wobber: Authentication in Distributed Systems: Theory and Practice, ACM Transactions on Computer Systems, 10(4), pages 265-310, 1992

Abstraktionsebenen der Sicherheit



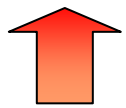
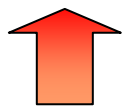
- **Schutzziele**
  - drücken die Erwartungen und Ziele zur Behandlung von Daten und Kommunikation aus.
- **Bedrohung**
  - Ereignisse oder Folge von Ereignissen, die zur Verletzung der *Schutzziele* führen.
  - Die Realisierung einer Bedrohung ist ein *Angriff.*
- **Sicherheitsmechanismen mit Informatik**
  - Ein Sicherheitsdienst kann mit Hilfe kryptographischer Algorithmen und Protokollen sowie mit konventionellen Mitteln realisiert werden.

Herkunft und Umsetzung

- Herkunft dieser Sicht: „geschlossene“ Organisationen (Unis, Industrie, Staat, …)
- Zugriffsregeln beziehen sich auf Benutzeridentitäten
- Die Organisation hat Autorität über ihre Mitglieder
- Die Mitglieder (Benutzer) sind physisch greifbar
- Audit/Log Einträge verweisen auf verantwortliche Personen

- Speichern der Zugriffskontrollregeln:
  - Von Listen (ACLs) zu Zertifikaten
- Parameter in Zugriffskontrollregeln: Benutzeridentitäten
  - Quelle (code origin)
  - Autor (code signature)
  - Integrität (code integrity)
- Basis für Zugriffskontrollregeln:
  - Von Bekannten (Sicherheit (security) zu Unbekanntem (Vertrauen (trust)

Fehler nehmen zu – Sicherheit nimmt ab

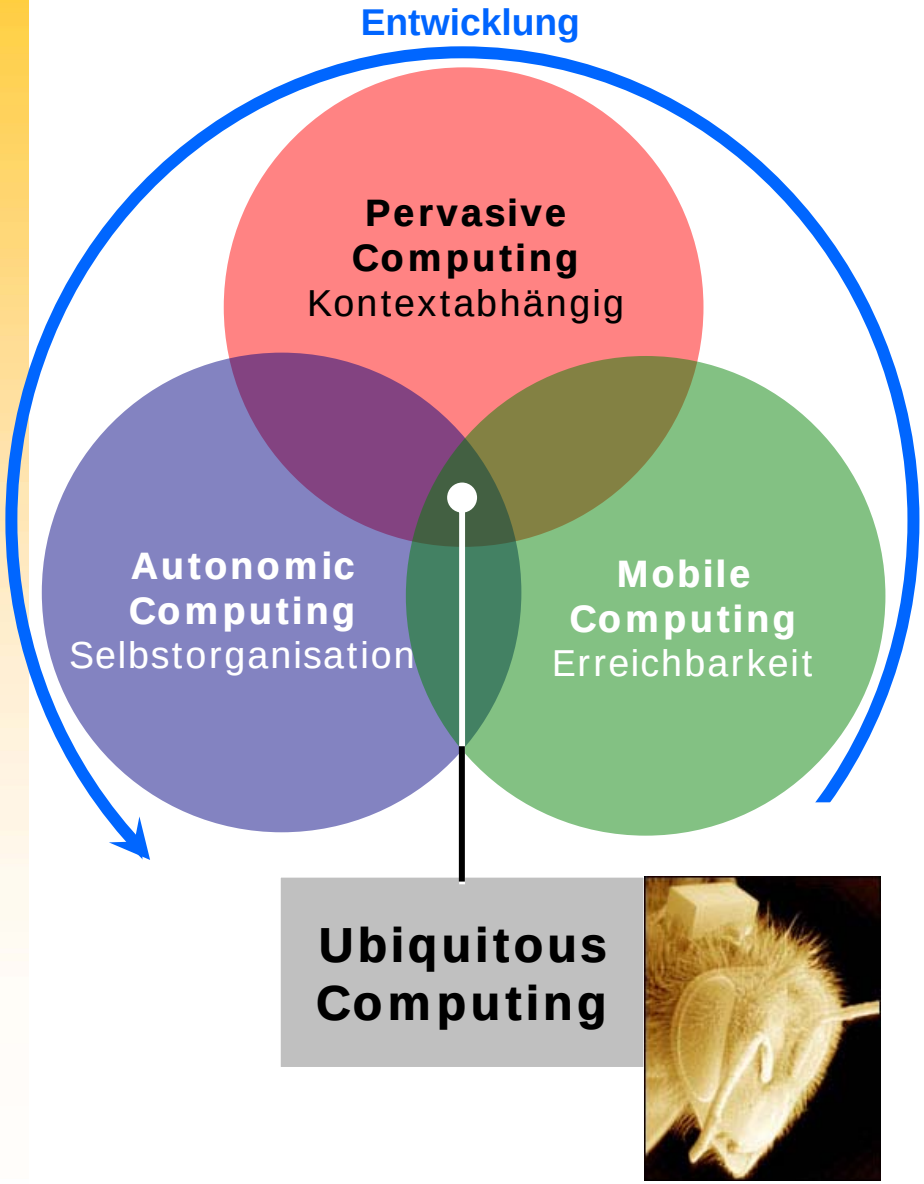
Ursache	Trend	1992-94*	2001*	2004*
Benutzerfehler		98	176	214
Patches		100	175	221
Hardware		49	49	48
System-Software		15	14	14
Software-Inkonsistenzen		18	260	321
Angriffe		5	303	407

*** Minuten (millions of customer minutes / month)**

Gliederung

1. Sicherheit war und ist Zugangskontrolle
2. In Informationssystemen mit UC ist Sicherheit anders
3. Sicherheit in UC: „Richtige Antwort auf die falsche Frage“
4. Bisherige Sicherheitsverfahren sind Verbote
5. Zusätzliche Sicherheit: Schutz durch Gebote

Technische Entwicklung zum UC

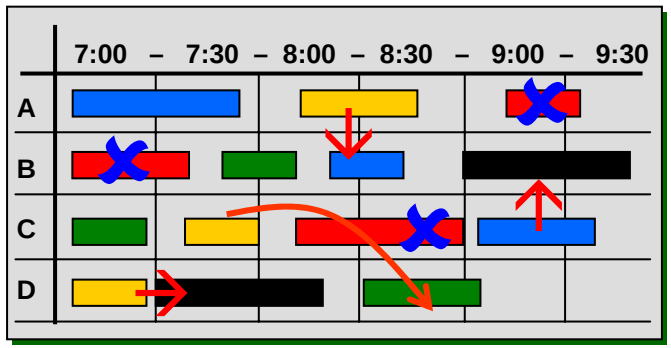


Mobile Computing
Globale Erreichbarkeit

Pervasive Computing
Erkennung des Kontextes
- Location based Services
- Spontane Netze

Autonomic Computing
Selbst-Management
- Selbst-Konfiguration
- Selbst-Optimierung
- Selbst-Heilung
- Selbst-Schutz

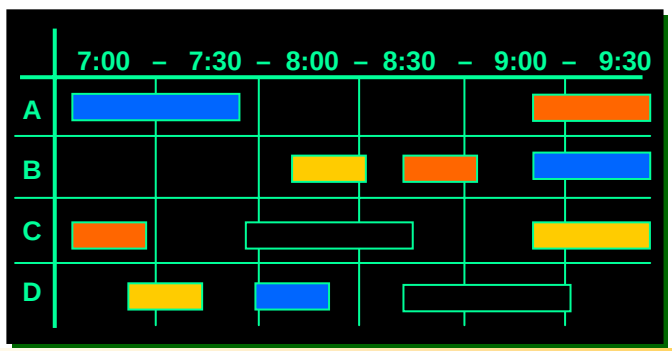
EMIKA: Ubiquitäres System

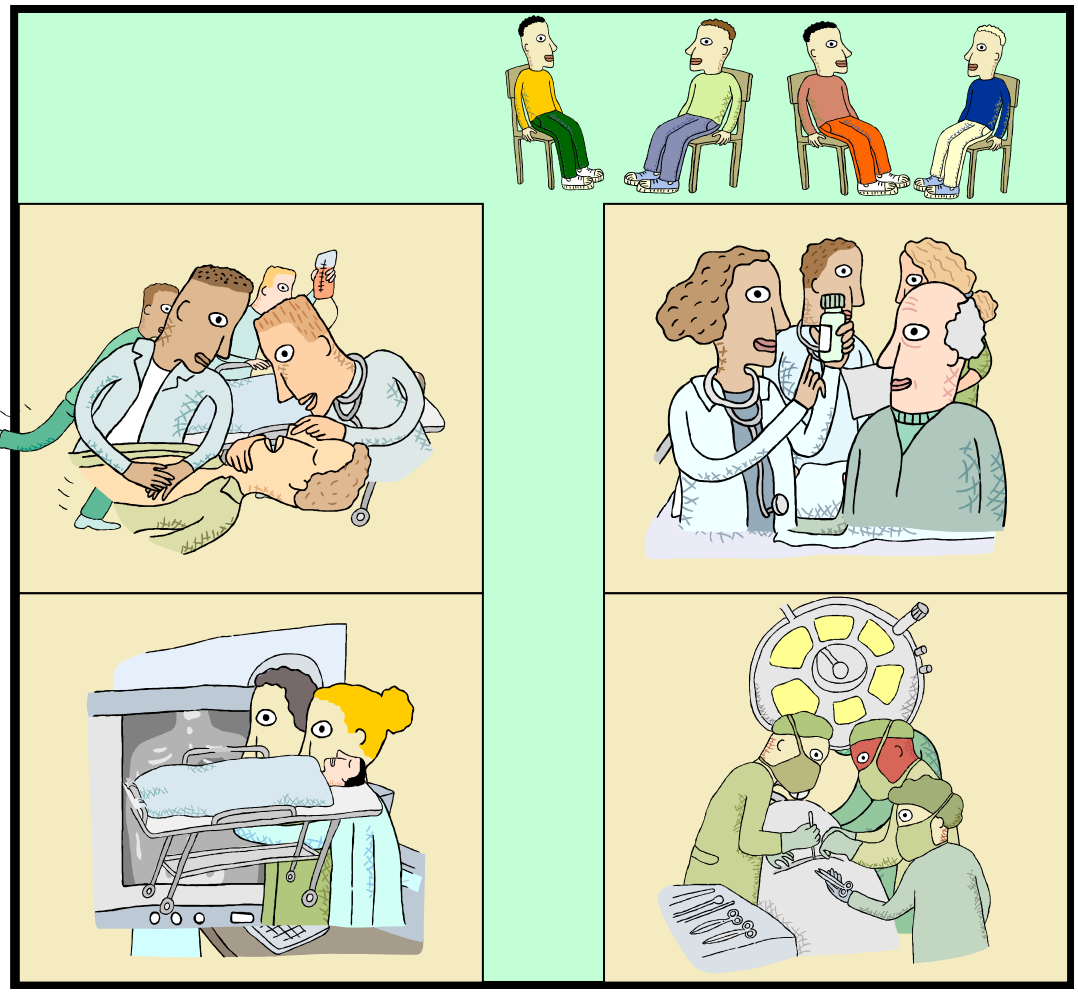


… Notfälle, …

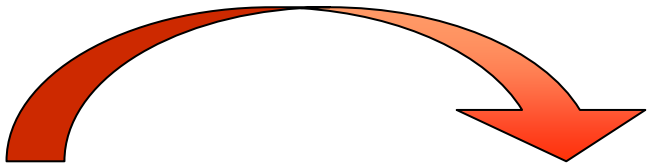
… Verspätungen, …

… Komplikationen





Wechsel der Paradigmen



Klassisches Informationssystem

Ziel: Geringe Software-Wartungskosten

Eigenschaften

- Vorgeplanter Entwurfsprozess
- Implementierung und Test mit großem Aufwand
- Aufgabenstellung genau vorgeschrieben
- Fest definierbare Benutzerschnittstellen

Hochdynamisches System mit UC

Ziel: Eignung für ständig wechselnde Umgebung

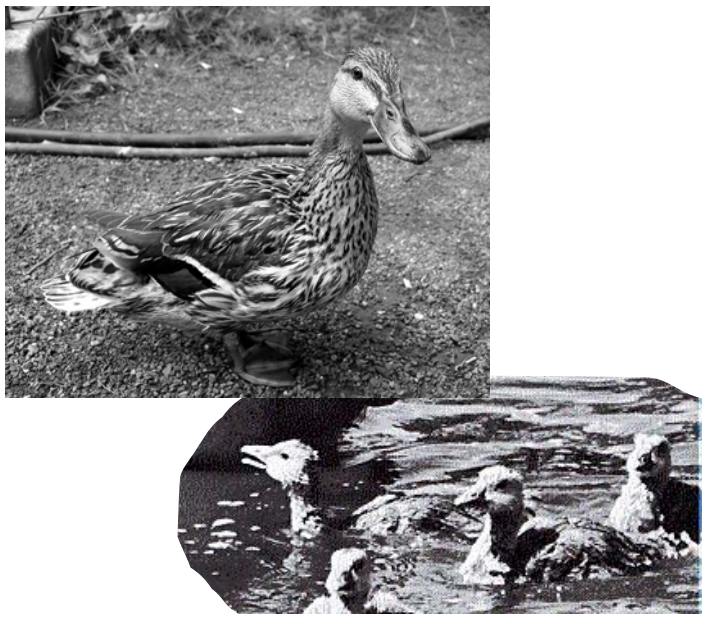
Eigenschaften

- Flexible Anpassung an die Umgebung
- Unvollständige Spezifikation
- Kontinuierliche Neuverhandlung der Beziehungen (emergente Strukturen)
- **Sicherheit bedeutet nicht mehr nur Abwehr von Gefahren**

Gliederung

1. Sicherheit war und ist Zugangskontrolle
2. In Informationssystemen mit UC ist Sicherheit anders
3. Sicherheit in UC: „Richtige Antwort auf die falsche Frage“
4. Bisherige Sicherheitsverfahren sind Verbote
5. Zusätzliche Sicherheit: Schutz durch Gebote

Aktuelle Sicherheitsansätze für UC



„Resurrecting Ducklings“ [Stajano]

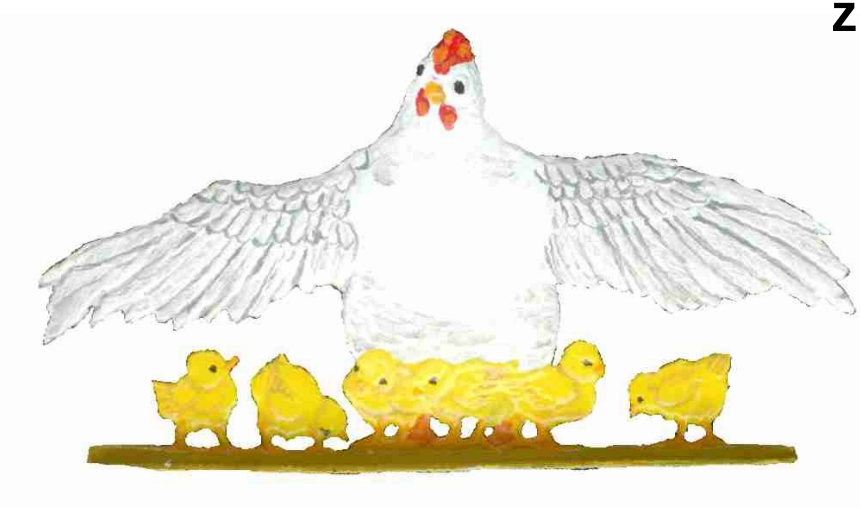
- Besitzer kontaktiert
  Gerät direkt nach Inbetriebnahme
  - Austausch geheimer Schlüssel über sicheren Kanal
- Gerät identifiziert seinen Besitzer über ersten Kontakt

Richtige Antwort auf die **richtige** Frage? → **Meistens schon !!**

Zugangskontrolle	=	Authentifizierung	+	Autorisierung
		Personen (Identität)	+	Ja/Nein

Die richtige Frage lautet…

„Was ist die Mutter?“



Weg von Benutzer- und Geräteidentität zu Parametern von Code

- Quelle (Herkunft des Codes)
- Autor (Signatur des Codes)

- Programm (Identität des Codes)
- **Bewiesene Funktionalität (Verhalten des Codes)**

Sicherheit in UC ist Softwareproblem

Ziel: Sicherheit in UC sollte ermöglichen,

dass "Sicherheits-Politiken" trotz veränderlicher und feindlicher Umstände immer gelten."

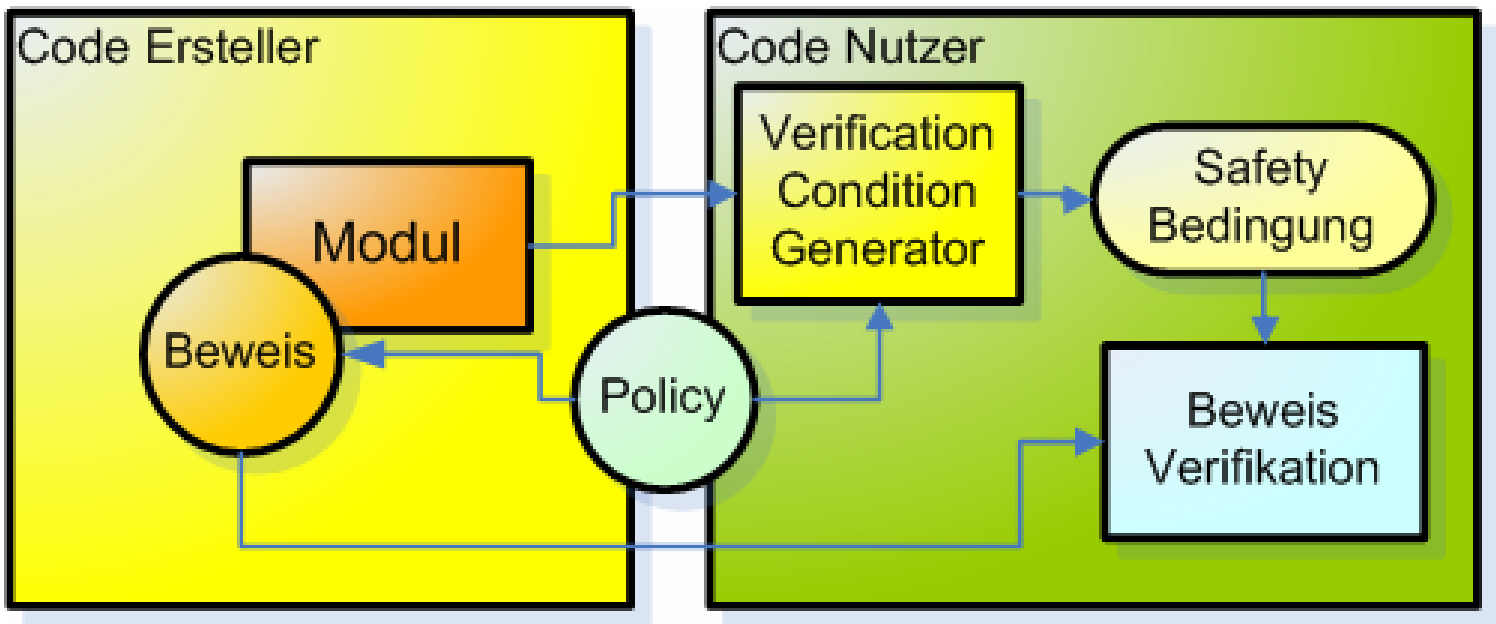
Wann kann man auf Sicherheitsverletzungen eingehen?

- Vor Ausführung:
  analyze, reject, rewrite
- Während der Ausführung:
  monitor, log, halt, change
- Nach der Ausführung:
  roll back, restore, audit, sue, call police

Davor: Verifizieren leichter als Erstellen

Proof-Carrying Code

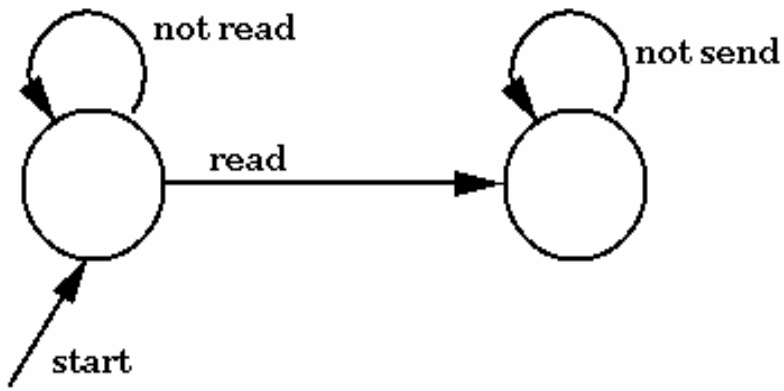
- Vor der Ausführung überprüfen, ob Patch/Erweiterung bösartig



Während: nur nächster Schritt ist bekannt

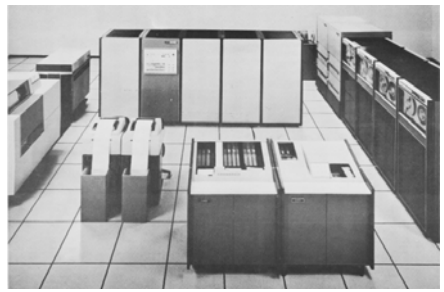
Execution Monitor

- Kontrolliert zur Laufzeit und verhindern Verstöße gegen Sicherheitsrichtlinien (Beispiel: Firewall und ACL)



Resource: http://www.cs.cornell.edu/Info/People/ulfar/

Nachher:



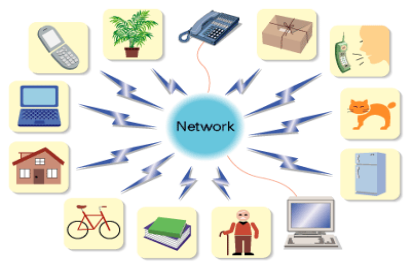
Rollback/Restore

- Zustände
- Synchronisierung von Geräten

Audit durch Dritte

- Aufzeichnung (Logging)
- Zurechenbarkeit

→ **Nicht** möglich in hochdynamischen Systemen!



Rufen Sie sofort die Polizei an…

Gliederung

1. Szenario für ein Informationssystem mit UC
2. Sicherheit war und ist Zugangskontrolle
3. Die richtige Antwort auf die falsche Frage
4. **Sicherheitsverfahren sind Verbote**
5. Schutz durch Gebote

Sicherheit durch Verbote?

Sicherheitsmechanismen sind Verbote (verhindern, dass „etwas Böses“ stattfindet)

Beispiele

- Verbot: kein Patient erhält Leserechte auf andere Akten
  Schutzziel Vertraulichkeit: Verschlüsselung

- Verbot: Krankenschwester dürfen Akten nicht ändern
  Schutzziel Integrität: Zugangskontrolle

- Verbot: Ärzte dürfen eine gestellte Diagnose nicht abstreiten
  Schutzziel Zurechenbarkeit: Digitale Signatur

Sicherheit in UC ist vielmehr: **etwas Gutes soll passieren**

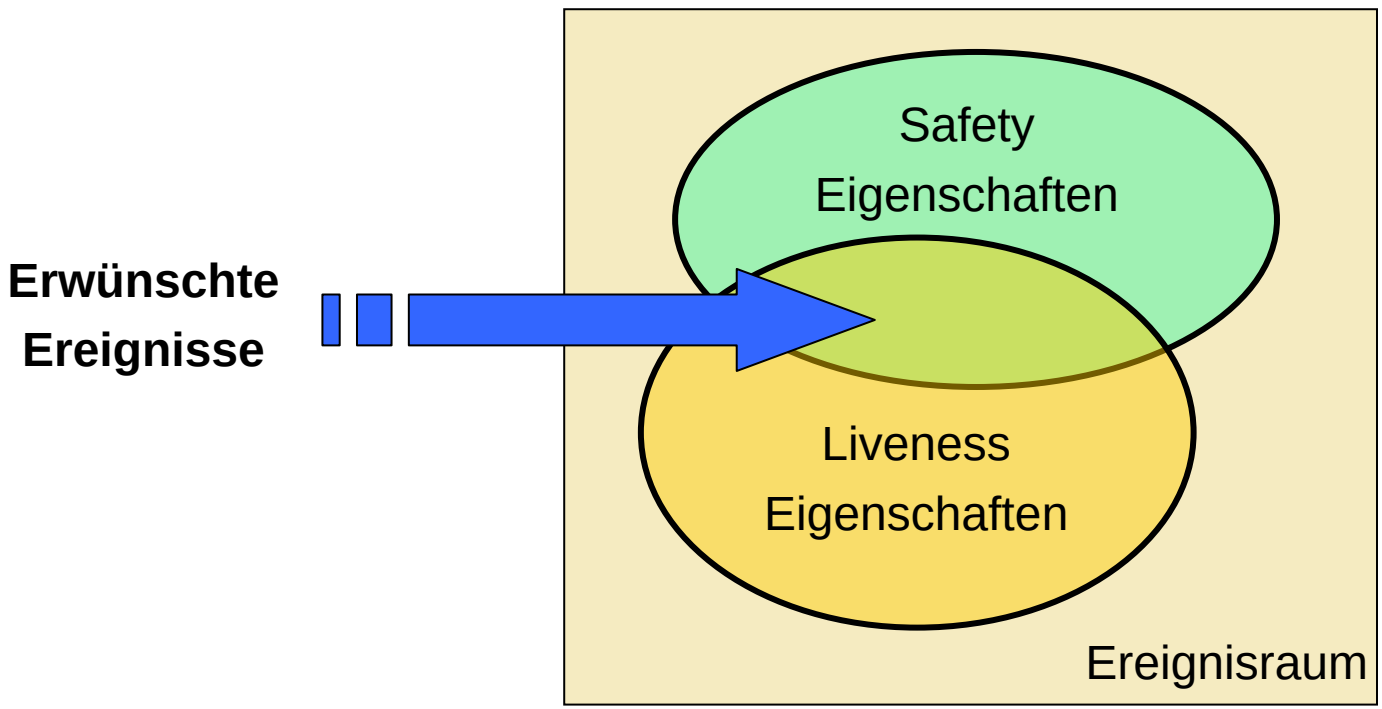
- **Gebot:** Alle Patienten sollen behandelt werden

- **Schutzziel Verfügbarkeit**: System funktioniert zuverlässig

Erwünscht = Verbot und Gebot

Safety Eigenschaften: Ereignisse, die **nicht auftreten** dürfen

Liveness Eigenschaften: Ereignisse, die **auftreten** müssen

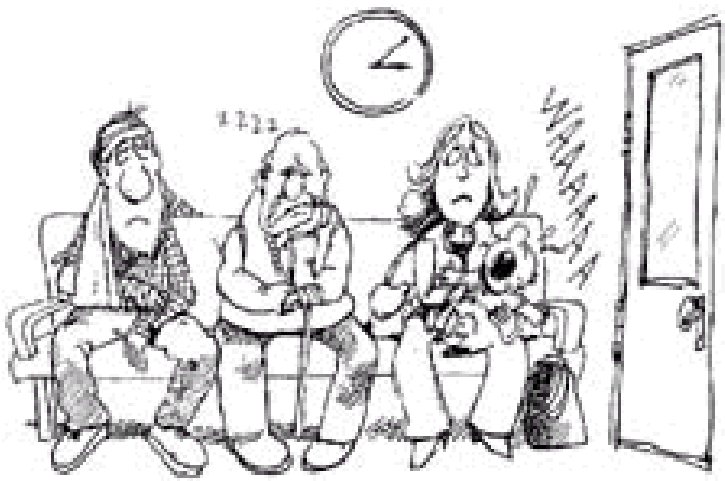


Gliederung

1. Szenario für ein Informationssystem mit UC
2. Sicherheit war und ist Zugangskontrolle
3. Die richtige Antwort auf die falsche Frage
4. Sicherheitsverfahren sind Verbote
5. **Schutz durch Gebote**

Schutz durch Gebote

„Sie kommen gleich dran“



Problem:

- **Gebote sind Verbote, deren aktueller Status nicht in endlicher Zeit entscheidbar ist**

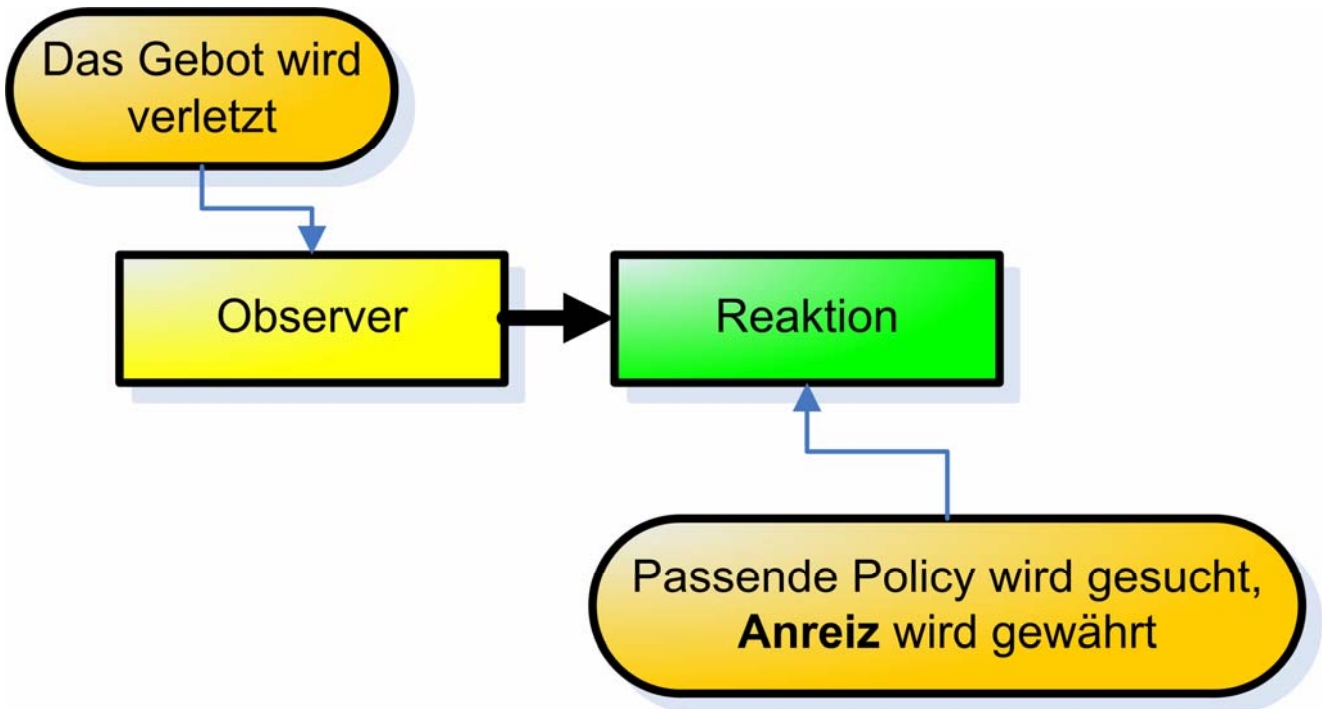
Lösungsansätze:

- Gebote sind umfassender als Verbote
- Gebote müssen formuliert werden
- Gebote müssen überwacht werden
- Gebote müssen über Anreizsysteme gesteuert werden

Gebote in hochdynamischen Systemen

Schutz durch Gebote

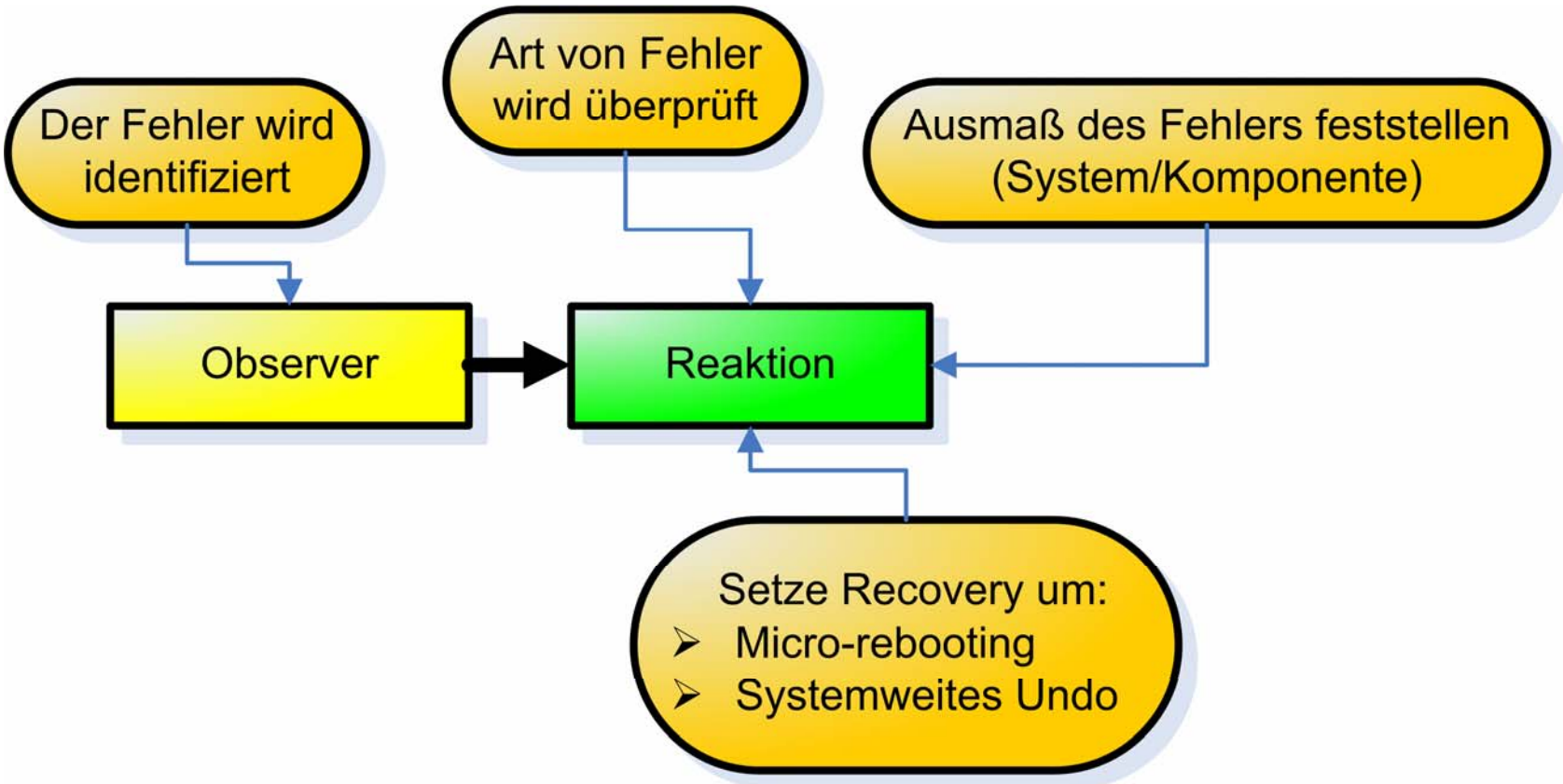
- Anreizbasierter Ansatz zur Erhöhung der Sicherheit



Beispiel: Verfügbarkeit durch ROC

Recovery-oriented Computing

- „availability through a repair-centric approach“



ROC: http://roc.cs.berkeley.edu/

Sicherheit: Schutz durch Gebote

Verbote sind **immer** sicher, aber **nicht dauerhaft** verlässlich

➔ Es ändert sich alles, damit alles gleich bleibt

1. Wenn Zugriffsregeln nicht länger nur Benutzeridentitäten enthalten, und wenn Authentifizieren nicht nur Identitäten prüft, sondern Beweise fordert, dann bleibt die Definition von Sicherheit stabil

2. Wenn Autorisierung nicht nur bedeutet, dass eine gegebene Benutzeridentität in der Zugriffskontrollliste enthalten ist, sondern eine bewiesene Funktionalität, dann bleibt die Definition von Sicherheit stabil

Gebote sind **nicht immer** sicher, aber **dauerhaft verlässlich**