Ambient Intelligence User Control

Wer kontrolliert wen und wer kontrolliert das?

Dr.-Ing. Hans-Werner Hein
Verlässliche IT-Systeme

1970	Studium Informatik, Darmstadt und Karlsruhe
	Diplom mit Hauptfach „Theorie der Informatik“
1975	„Wissensbasierte EKG-Analyse“, Karlsruhe
	„Mustererkennung, Bildverarbeitung, Sprachverarbeitung“, Erlangen
1980	Promotion „Automatisches Verstehen gesprochener Sprache“
	„Expertensysteme“, GMD St. Augustin
1985	„Adaptive multimediale Mensch-Maschine-Kommunikation“
	„Maschinelle Intelligenz“, Institut für Roboterforschung Dortmund
1990	„Werkzeugsysteme für Sicherheitsexperten“
	„Sicherheitsprofile nach CC für die digitale Signatur“
1995	„Biometrie und Datenschutz“
	„E-Learning“, Fernuniversität der Niederlande
2000	„Trust Management“
	„Agent Systems und Informationssicherheit“
2004	„User Coaching“

Gesellschaftliches Spannungsfeld

Sicherheit <<< >>> Freiheit

bewahren <<< >>> vermehren

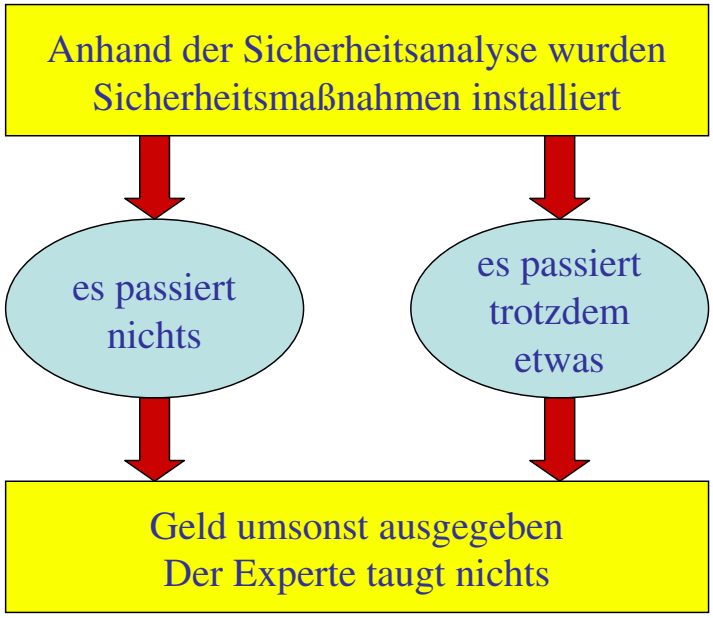
von Werten

€ $ ¥

Ökonomisches Spannungsfeld

lästig ehrenvoll

Dilemma des Sicherheitsexperten



AmI und Mensch

Arbeitsschutz

Beispiel: Drehtür-Unfall am Kölner Flughafen
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (www.BuUA.de)

Ergonomie

Vermeiden menschlicher Handlungsfehler
Benutzerakzeptanz

Mensch-Maschine-Kommunikation

„Bedienen“ oder „Benutzen“?
Metaphorik (Schreibmaschine, Büroarbeitsplatz, Cockpit)
Gesprochene Sprache

AmI und Information

Sensorik und Informationsmanagement

Wo entsteht Information? Wohin fließt Information?
Wo wird Information gespeichert?

Informationsnutzung und Aktorik

Zu welchen Zwecken wird die Information verarbeitet?
Nach wessen Regeln finden automatisierte Handlungen statt?

Informationsräume

Globaler regelfreier Raum (Cyberspace)
Staatlich und gesellschaftlich geregelte öffentliche Räume
Privatvertraglich geregelte organisationsinterne Räume
Informationelle Privatsphäre
Garantiert AmI-freie Reservate
usw.

AmI und Vertrauen

Protokollierung

Zeitlicher Umfang und Inhalte?
Zustimmung nötig? Präsenz (z.B. bei RFIDs)?

Zertifizierung

Sicherheitsprofile: Common Criteria 2.1 ISO/IEC 15408 (www.bsi.de/cc)
Kostet Zeit und Expertise, gilt nur für einige Zeit, leider wenig bekannt

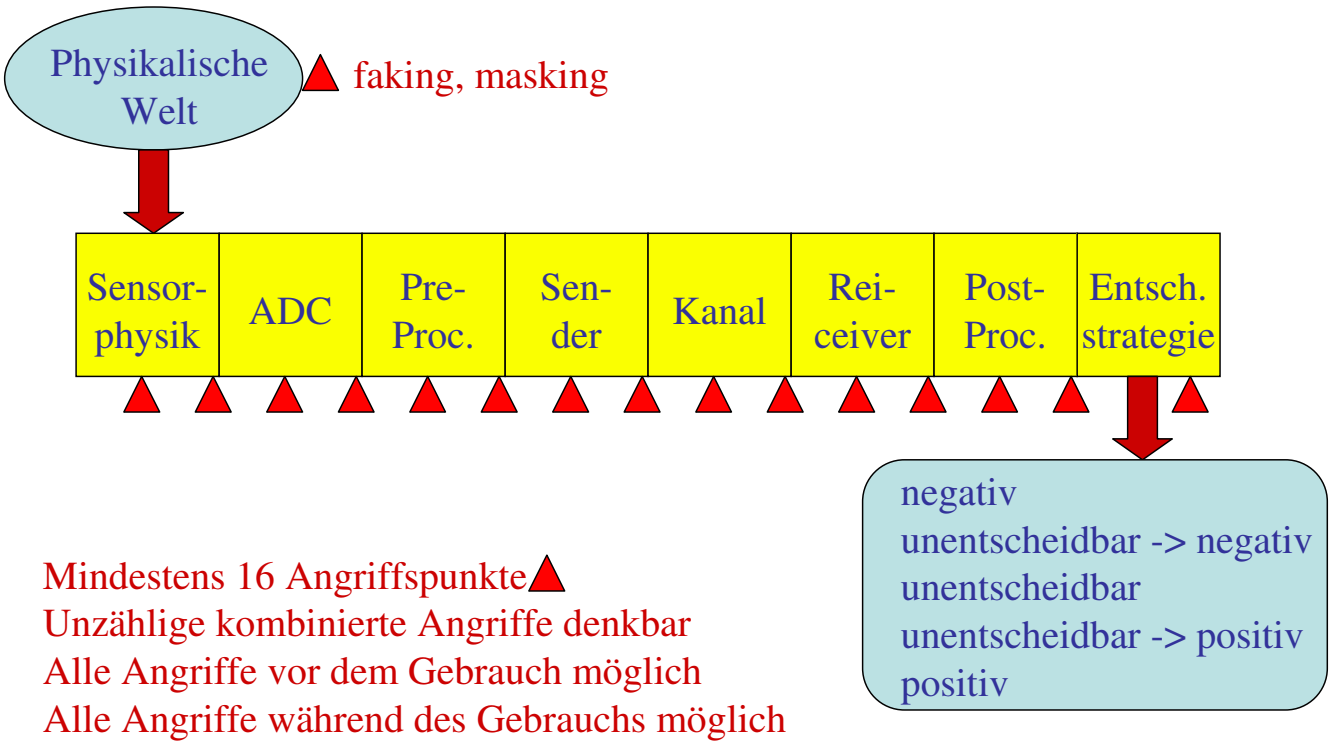
Haftung

Wer darf Befehle geben?
Wer darf Funktionskriterien (Einstellungen) ändern?
Haftung in Hersteller-gemischten Umgebungen?

Trust Management

Open Source?
Operative Transparenz, z.B. Fehlfunktions-Berichte?

zur Sicherheitsprofilierung von Biometrie



Mindestens 16 Angriffspunkte
Unzählige kombinierte Angriffe denkbar
Alle Angriffe vor dem Gebrauch möglich
Alle Angriffe während des Gebrauchs möglich

zur Zertifizierung

Zertifizierung sollte man „weitgehend“ vermeiden

denn sie dauert lang
benötigt seltene Experten
gilt nur für begrenzte Zeit
hat wenig Kundenresonanz
muss bei technischen Anpassungen wiederholt werden

MINUS-Vermeiden

Sicherheitsaspekte werden ignoriert, marginalisiert, von Projektphase zu Projektphase verschoben. Es werden zwar reichlich Wichtigkeitserklärungen abgegeben, aber nichts passiert. Eventuell wird das Thema an eine inkompetente Instanz delegiert ...

PLUS-Vermeiden

Sicherheitsprofil als Teil der Konzeptionsphase verstehen
Trennen von wichtigen und unwichtigen Sicherheitsaspekten
Zu zertifizierende Anteile kleinkörnig und simpel halten
(hier ist Ingenieurskunst gefragt!)

AmI und User Control

User Control 1

Monitoring und Profiling der Benutzer

User Control 2

Prüfbarkeit und Schaltbarkeit durch die Benutzer

Erfahrung

Bei neuen ICT-Architekturen lassen sich
Querschnitts-Aspekte, deren technisches Fundament
nicht am Anfang der Entwicklung gelegt wurde,
nicht nachträglich einfordern.