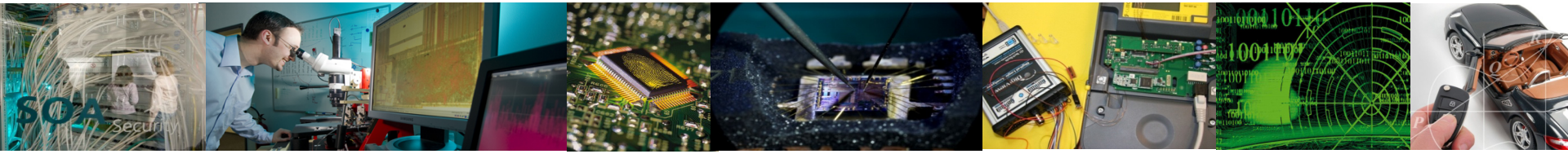
Wireless 2020 Taktiles Internet
Herausforderungen für die IT-Sicherheit

Claudia Eckert

Fraunhofer AISEC & TU München

Wireless 2020, das Taktile Internet

Berlin, 1.10. 2013



Fraunhofer
AISEC


A new device has been found
Device: Airbus A310
Run Auto-configuration?
Start
Cancel
Bluetooth

Gliederung

1. Rolle der IT Sicherheit
2. Wireless 2020
3. Wireless 2020 Sicherheitsherausforderungen
4. Take Home Message

1. Rolle der IT-Sicherheit

IT-Sicherheit

- Sie ermöglicht den Schutz vor unautorisierter Manipulation.
- Sie schützt vor unautorisierter Informationsgewinnung, insbesondere auch vor Eingriffen in die Privatsphäre.
- Sie ermöglicht die eindeutige Identifizierung und Zuordenbarkeit von Akteuren und Aktivitäten.
- Sie schützt vor funktionalen Beeinträchtigungen.

Gliederung

1. Rolle der IT Sicherheit
2. **Wireless 2020**
3. Wireless 2020 Sicherheitsherausforderungen
4. Take Home Message

2. Wireless 2020 Anwendungsfelder

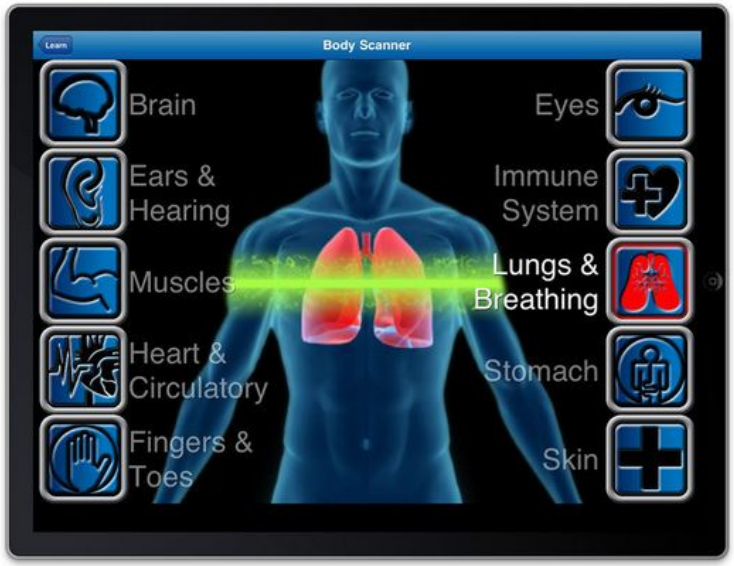
Automatisierungstechnik

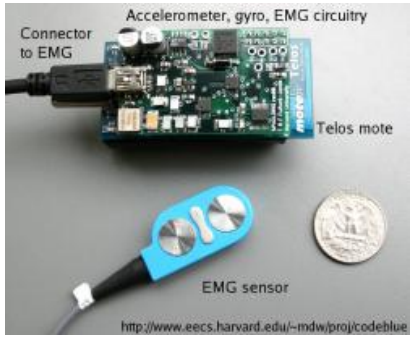
- Instandhaltung und Fernwartung von (bewegten) Objekten mit taktiler Interaktion (Wartung etc.)

2. Wireless 2020 Anwendungsfelder

Gesundheitsversorgung

- Mobile Vitalüberwachung für personalisierte, ambulante Gesundheitsversorgung
- Gesundheitstelematik: Tele-Diagnostik, Tele-Operation





Beschleunigungssensor, Gyroskop, Elektromyogramm (EMG) zur Überwachung von Schlaganfallpatienten

Fraunhofer AISEC

2. Wireless 2020

Nutzer-zentrische Netze

- Interaktion mit bewegten Objekten mit geringer Latenz
  - Steuerungen von Robotern, Fertigungsanlagen
- Smarte, adaptionsfähige Steuerungsinfrastrukturen
  - Cognitive Radio, smarte Sensoren
- Verschmelzung von virtuellen und physischen Systemen: Cyber Physical Production Systems:
  - Cloud@the Edge

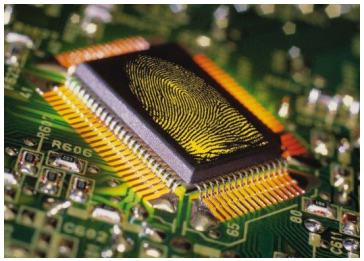
Gliederung

1. Rolle der IT Sicherheit
2. Wireless 2020
3. **Wireless 2020 Sicherheitsherausforderungen**
4. Take Home Message

3. WS2020 Sicherheitsherausforderungen

(1) Sicherheit für smarte Steuerungsinfrastrukturen

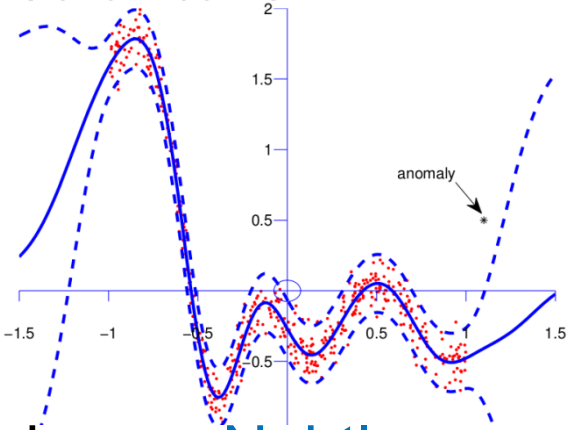
- Sichere, robuste Kommunikation:
  - Ende-zu-Ende (auch bei Multi-Hop)
    leichtgewichtige Verschlüsselung
    bereits auf physikalischer Ebene



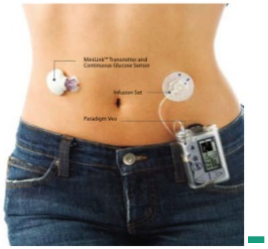
  - Integritätschutz auch für Nutzdaten
    effiziente, skalierende Prüftechniken
  - Effizientes, skalierendes Schlüssel-
    management : erzeugen, verteilen, prüfen, …

3. WS2020 Sicherheitsherausforderungen

(1) Sicherheit für smarte Steuerungsinfrastrukturen



- Resiliente Steuerungsaufgaben:
  - Manipulationserkennung
    Interaktions-Charakteristika zur verbesserten Anomalie-Erkennung
  - Angriffstoleranz durch u.a. Re-Konfigurierung Nahtloses Sicherheitsmanagement, z.B. Schlüssel
- Personalisierte Dienste:
  - Datenschutz, Profilbildung

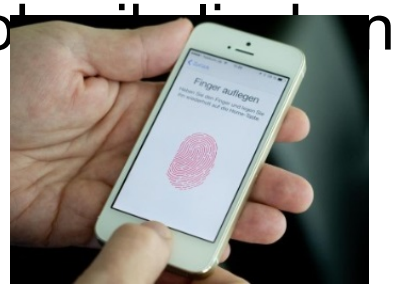


Fraunhofer AISEC

3. WS2020 Sicherheitsherausforderungen

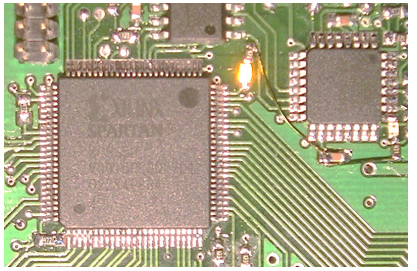
(2) Sicherheit für smarte Sensorik

- Sichere Objekt-Identitäten
  unverfälschbar, einfach prüfbar
  - PUF: Biometrie für Objekte
    basierend auf Material-Eigenschaften,
    Material-Alterung, Stabilität, Recovery
  - PUF: Schlüsselgenerierung abhängig von physikalischen Eigenschaften
  - Mehrfaktor Authentisierung:
    Verhalten (taktil) plus Schlüssel/PIN/Besitz



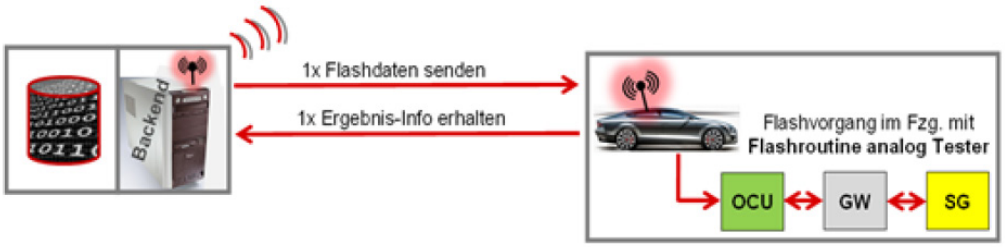
3. WS2020 Sicherheitsherausforderungen

(2) Sicherheit für smarte Sensorik



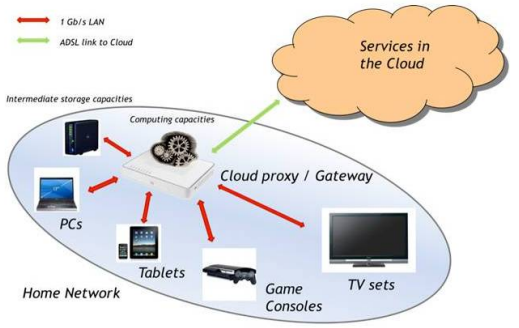
- Plug & Trust: Vertrauensanker
  - Vertrauenswürdige Hardware-Anker
    sicherer Speicher, sichere Zufallszahlengeneratoren
  - Resilient auch gegen physische Angriffe
    FPGAs mit zugeschnittenen, integrierten Sicherheitskonzepten

  - Sicheres Remote Management:
    Over The Air Update



3. WS2020 Sicherheitsherausforderungen

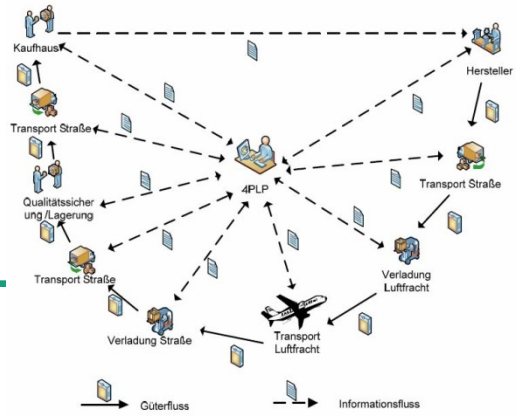
(3) Sicherheit für mobile CPPS



- Cloud@ the edge

  Separierung, Kontrollen im ‚Netz'

  - Zugangs- und Zugriffskontrollen, Virtualisierung
    Ressourcenbeschränkung, Schutz vor Betreiber (trust)
  - Sichere Kooperation: Cross-Domain Datenfusion:
    Daten-Ownership , Vertraulichkeit
  - Mobile , sichere Daten-Zugriffe:
    zuverlässig, geräteunabhängig



3. WS2020 Sicherheitsherausforderungen

(4) Taktiles Internet: Human in the Loop

- Usability
  Akzeptierte Sicherheitskonzepte, mentale Modelle?
- Privacy:
  Taktile Nutzungsverhalten: Rück-schlüsse auf Arbeitsweise

- Neue Schwachstellen durch taktile Interaktion?
  erweiterte Bedrohungs- und Risikoanalysen notw.

Gliederung

1. Rolle der IT Sicherheit
2. Wireless 2020
3. Wireless 2020 Sicherheitsherausforderungen
4. Ausgewählte Beispiele für offene Fragen
5. **Take Home Message**

5. Take Home Message Wireless 2020

Adaptive, personalisierbare Steuerungsinfrastrukturen

- Vertrauenswürdige und robuste Kommunikation:
  - Integrierte E2E-Verschlüsselung, Integritätsschutz
- Vertrauenswürdige, resiliente Sensorik…
  - Objekt-Identitäten (PUF) und Manipulationsschutz
- Sichere, schnelle Anbindung an Cloud-Dienste
  - Cloud in die Netzwerkkomponenten verlagern

Faktor Mensch: Taktile Interaktion

- Zusätzliche Risiken: z.B. Usability, Privacy, aber auch
- Neue Chancen: z.B. Identifizierung, Anomalie-Erkennung

Vielen Dank für Ihre Aufmerksamkeit!

Claudia Eckert

Fraunhofer AISEC, München
TU München, Lehrstuhl für Sicherheit in der Informatik

E-Mail: claudia.eckert@aisec.fraunhofer.de
Internet: http://www.sec.in.tum.de
http://www.aisec.fraunhofer.de

Fraunhofer AISEC