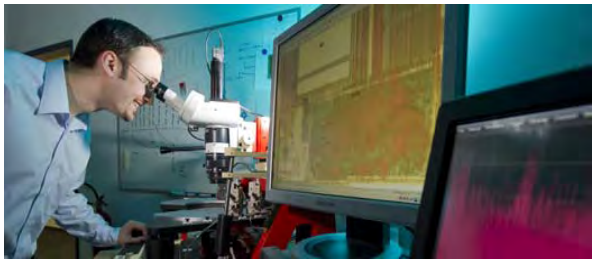
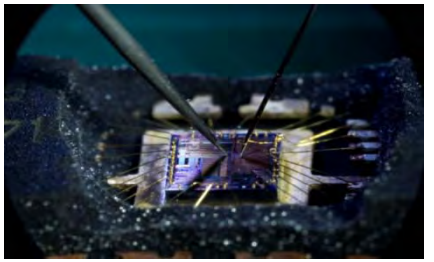
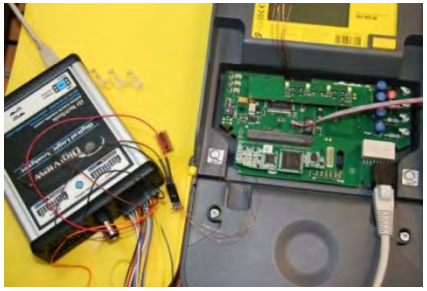
IT-Sicherheit: Herausforderungen für Wissenschaft und Gesellschaft

C. Eckert, TU München, Fraunhofer AISEC



Gliederung

Fraunhofer AISEC

1. Schlüsseltechnologie IKT
2. IKT benötigt Sicherheit
3. Bedrohungen und Herausforderungen (Technologisch)
4. Sicherheit braucht Forschung
5. Take Home Message

Fraunhofer AISEC

These: IKT ist Schlüsseltechnologie für globale Herausforderungen

Energie Umwelt **Mobilität** Sicherheit **Gesundheit**

IKT ist Schlüsseltechnologie

Fraunhofer AISEC

These: IKT ist Schlüsseltechnologie für globale Herausforderungen

Energie Umwelt **Mobilität** Sicherheit **Gesundheit**

IKT ist Schlüsseltechnologie

Fraunhofer AISEC

Zukunft:

- Internet vernetzt Menschen, physische Objekte und Dienste

Beispiele

Energie: z.B. SmartGrids

- Steuern, Überwachen, Planen, Entscheiden

Gesundheit: z.B. personalisierte Medizin

- Überwachte Vitalfunktionen

Mobilität: z.B. Individualverkehr

- Sensorik im Fahrzeug, Car2X

IKT ist Schlüsseltechnologie

Fraunhofer AISEC

IKT: zentrales Nervensystem koordinieren, steuern, überwachen

Energie Umwelt Mobilität Sicherheit Gesundheit

IKT ist Schlüsseltechnologie

Fraunhofer AISEC

It's all about data!

- Daten sind ein schützenswertes Gut
- Daten steuern sicherheitskritische Abläufe/Prozesse
- Daten sind 'Währung' u.a. in sozialen Netzen (Facebook etc.)

Fraunhofer AISEC

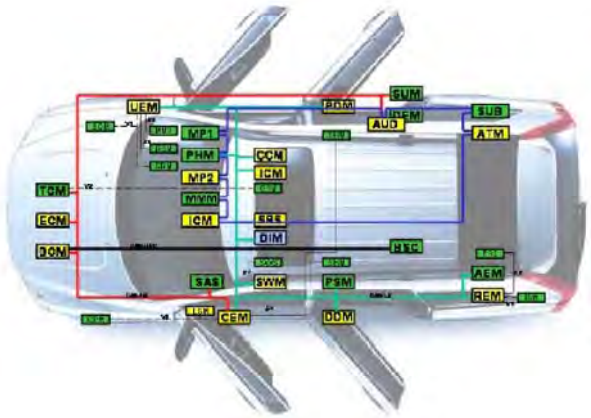
IKT benötigt Sicherheit

- Daten- und Informationsvertraulichkeit
- Prüfbare Identität von Personen und Objekten
- Manipulationsschutz für Daten und auch kompletten Abläufen

Bedrohungen

Beispiel: Sensorik im Auto:

- Viele vernetzte ECUs
- GSM-Modul: Ferndiagnose Software-Updates, ..
- **Problem:** Fehlende Kontrollen Einschleusen von Schad-Code, …

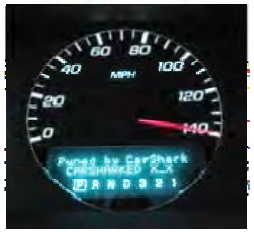


Volvo XC90 (2001)

500 Kbit/sec CAN bus for power train

125 Kbit/sec CAN bus for body electronics

MOST (infotainment system)



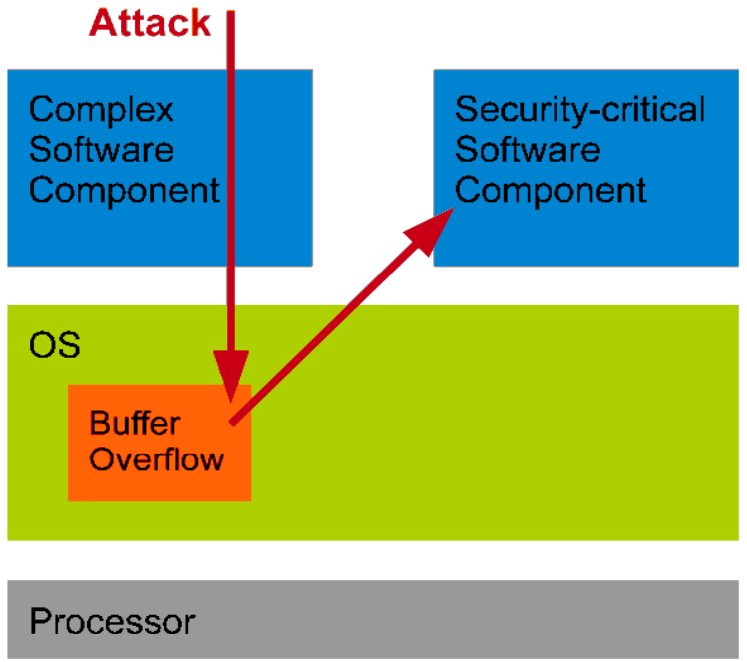
Herausforderungen: u.a.

- **Manipulationsresistente Hardware**
- **Sichere Komponenten-Identifikation (Machine-to-Machine)**

Bedrohungen

Beispiel: Web-Anwendungen

- **Problem**: Programmierung
  Einschleusen von Viren, Trojanern
- **Problem:** Mangelhafte Kontrollen
  unerlaubte Datenzugriffe, …



Herausforderungen:u.a.

- **Zuverlässige Abschottungen (Kaskadeneffekte verhindern)**
- **Selbst-Überwachung (Aufbau eines ‘Immunsystems’)**
- **Autonome Reaktion (kontrollierte ‘Selbst-Heilung’)**

Fraunhofer AISEC

Sichere IKT braucht Forschung

Technologie gestalten: Architekturen

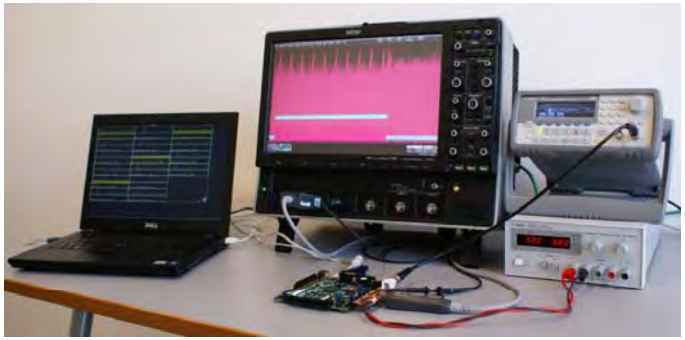
Fraunhofer AISEC

Sicherheitsarchitekturen

Ziel: Resistent gegen Angriffe

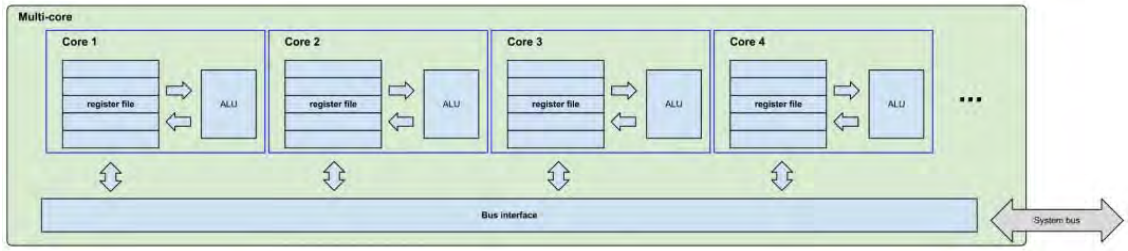
z.B. **Seitenkanal-Angriff:** (Pizza Index)

- Beobachten von Verhaltens-Charakteristika



Ansatz: Angriffs-tolerante Multi-Core-Architekturen

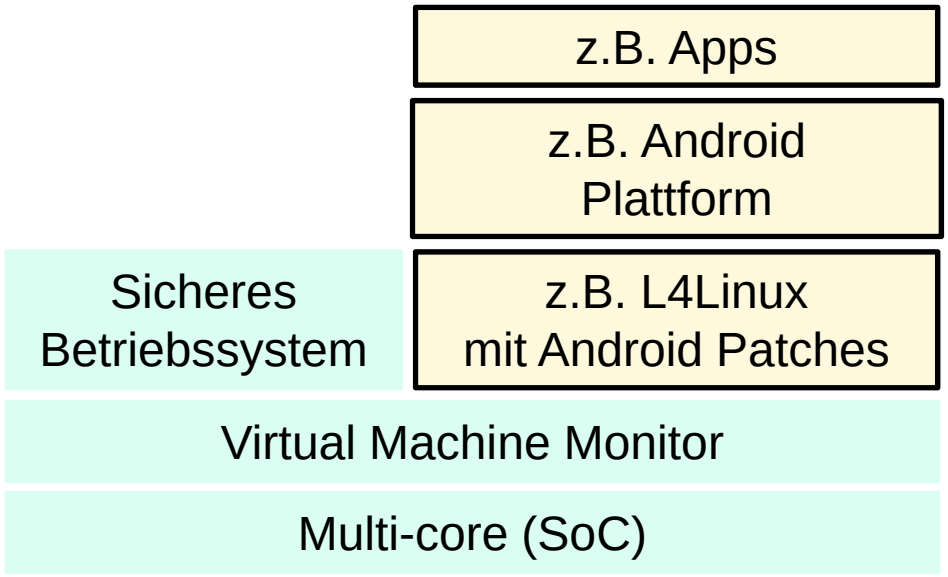
- Verschleiern von Charakteristika: u.a. Randomisierungen
- Neue Algorithmen (parallisiert, verteilt)



Fraunhofer AISEC

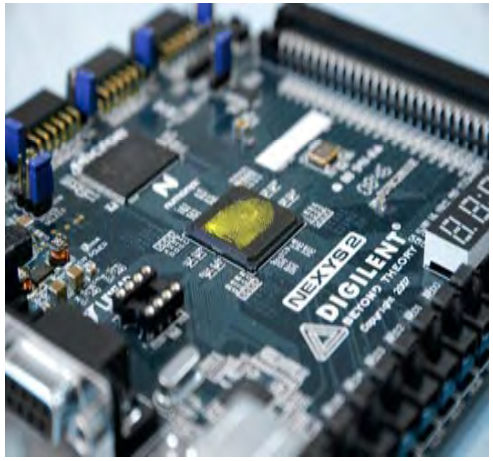
Selbst-überwachende Systeme

- Sicherer Betriebssystem-Kern als ‘Überwacher’
  - Sammelt Verhaltensdaten
    z.B syscall traces
  - Klassifiziert Aktivitäten:
    Normalverhalten
  - Reagiert: Abschalten
    von Diensten, Schließen
    von Ports, …



Biometrie für Objekte

Physical Unclonable Function (PUF)



- Nicht fälschbare Material-Eigenschaften
- PUF: liefert auf eine Anregung (Challenge) eine nicht vorhersagbare Antwort : einzigartig ID

Problem:

- Alterung, Verschmutzung verändern das PUF-Verhalten

Forschung:

- Korrekturdaten (Helper data), Toleranzschwellen
- Nutzen der PUF Eigenschaften in Software-Produkten

Sicherer Betrieb: Angriffserkennung

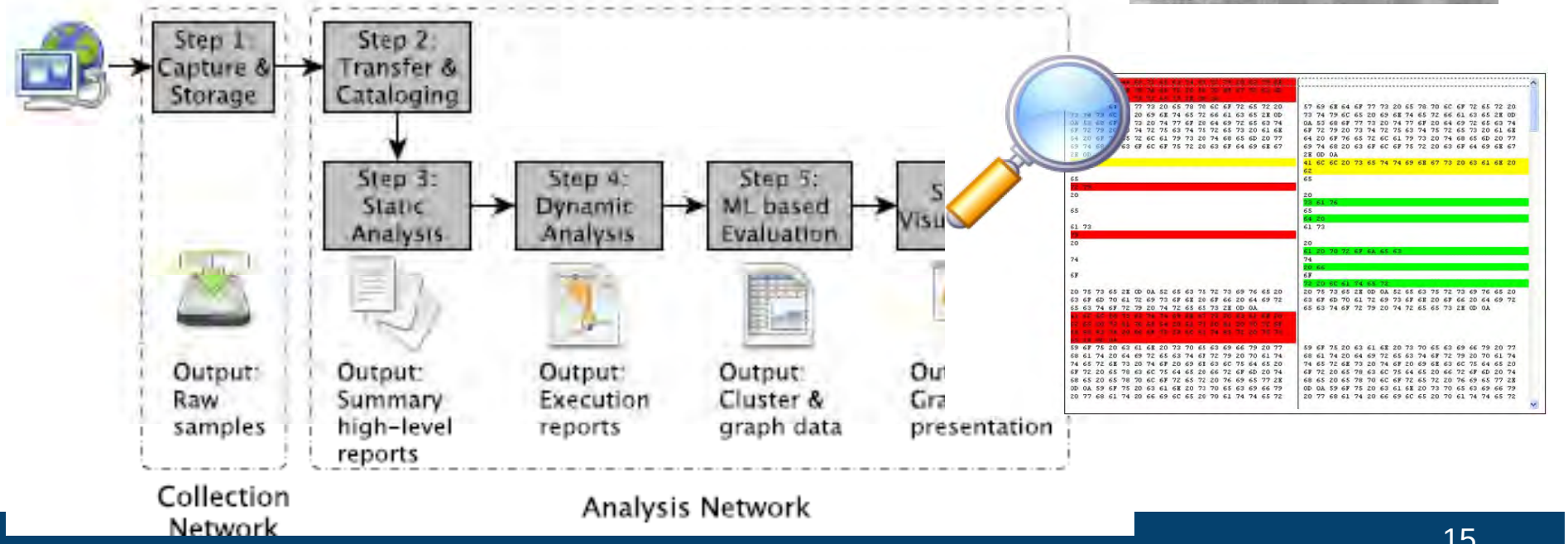
Fraunhofer AISEC

Problem:

- Erkennen von Verhaltens-Abweichungen

Lösung

- Maschinelles Lernen: Klassifikation
- Honey-Net: Lernen von Angriffstechniken



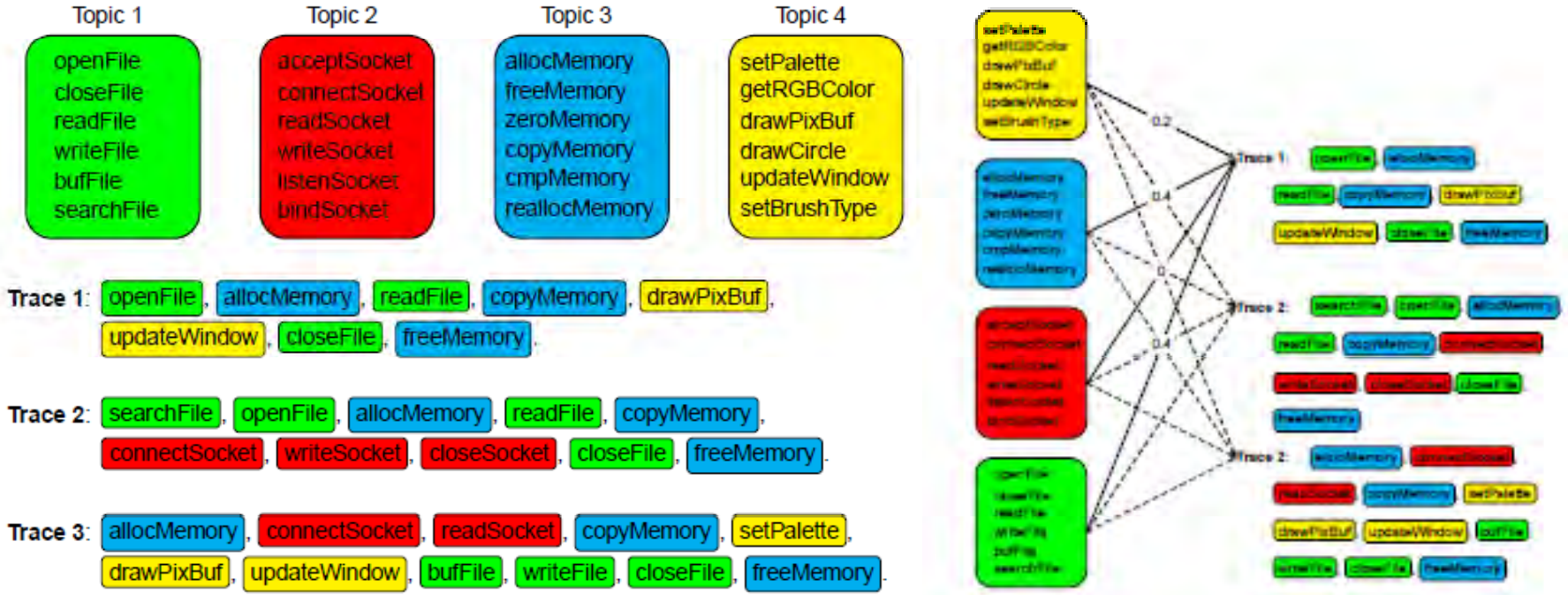
Sicherer Betrieb: Angriffserkennung

Fraunhofer AISEC

Idee: Definition von Topics: Semantische Zusammenhänge

Beispiel: Topic1 Graphikprogramm | Topic 2 Netzverbindung | Topic 3 Dateiverarbeitung | Topic 4 Bildverarbeitung

Machinelles Lernen: Clustern von Events zu Topics (Normalverhalten)



Ein Blick hinter die Kulissen: Parameter Estimation with Gibbs Sampling

Fraunhofer AISEC

$$\prod_{d=1}^{D} P(y_d|d,\theta) \times \int \prod_{z=1}^{T}\prod_{v=1}^{V} \psi_{z,v}^{m_{z,v}} \prod_{z=1}^{T}\left[\frac{\Gamma(\sum_{v=1}^{V}\beta_v)}{\prod_{v=1}^{V}\Gamma(\beta_v)}\prod_{v=1}^{V}\psi_{z,v}^{\beta_v-1}\right] d\Psi$$

$$\times \int \prod_{d=1}^{D}\prod_{z=1}^{T}\prod_{z'=1}^{T} \varphi_{d,z,z'}^{n_{d,z,z'}} \prod_{d=1}^{D}\prod_{z=1}^{T}\left[\frac{\Gamma(\sum_{z=1}^{T}\alpha_z)}{\prod_{z=1}^{T}\Gamma(\alpha_z)}\prod_{z'=1}^{T}\varphi_{d,z,z'}^{\alpha_{z'}-1}\right] d\Phi$$

$$= \left[\frac{\Gamma(\sum_{v=1}^{V}\beta_v)}{\prod_{v=1}^{V}\Gamma(\beta_v)}\right]^{T} \times \left[\frac{\Gamma(\sum_{z=1}^{T}\alpha_z)}{\prod_{z=1}^{T}\Gamma(\alpha_z)}\right]^{D\,T} \times \prod_{d=1}^{D} P(y_d|d,\theta)$$

$$\times \prod_{z=1}^{T}\int \prod_{v=1}^{V} \psi_{z,v}^{m_{z,v}+\beta_v-1} d\Psi \times \prod_{d=1}^{D}\prod_{z=1}^{T}\int \prod_{z'=1}^{T} \varphi_{d,z,z'}^{n_{d,z,z'}+\alpha_{z'}-1} d\Phi$$

$$\propto \prod_{d=1}^{D}[1+\exp(-\sum_{z,z'}\theta_{z,z'}n_{d,z,z'})]^{-1} \prod_{z=1}^{T}\frac{\prod_{v=1}^{V}\Gamma(m_{z,v}+\beta_v)}{\Gamma(\sum_{v=1}^{V}m_{z,v}+\beta_v)}$$

$$\prod_{d=1}^{D}\prod_{z=1}^{T}\frac{\prod_{z'=1}^{T}\Gamma(n_{d,z,z'}+\alpha_{z'})}{\Gamma(\sum_{z'=1}^{T}n_{d,z,z'}+\alpha_{z'})}.$$

Fraunhofer AISEC

Zukunft benötigt IKT

Koordinierung, Steuerung, Kontrolle

IKT ist verletzlich

Verletzlichkeit der Nutzer, der Gesellschaft

IKT benötigt Sicherheit

Technologie Gestaltung, Forschung, Bildung, Kultur

Herausforderungen

Wissenschaft:

- Technologiegestaltung: sicher, nutzbar, nachhaltig

Politik:

- Rahmenvorgaben: Zuckerbrot und Peitsche
  Anreizmodelle und gesetzliche Auflagen

Wirtschaft:

- Vertrauen schaffen: Transparenz und Kontrollierbarkeit

Gesellschaft:

- Sicherheitskultur: Ausbildung, Wertvorstellungen

Und zu guter Letzt …

Fraunhofer AISEC

Herausforderung:
Sinnvoll

Herausforderung:
Angemessen

Vielen Dank für Ihre Aufmerksamkeit

Claudia Eckert

TU München, Lehrstuhl für Sicherheit in der Informatik

Fraunhofer AISEC, München

E-Mail: claudia.eckert@sec.in.tum.de

Internet:

http://www.aisec.fraunhofer.de