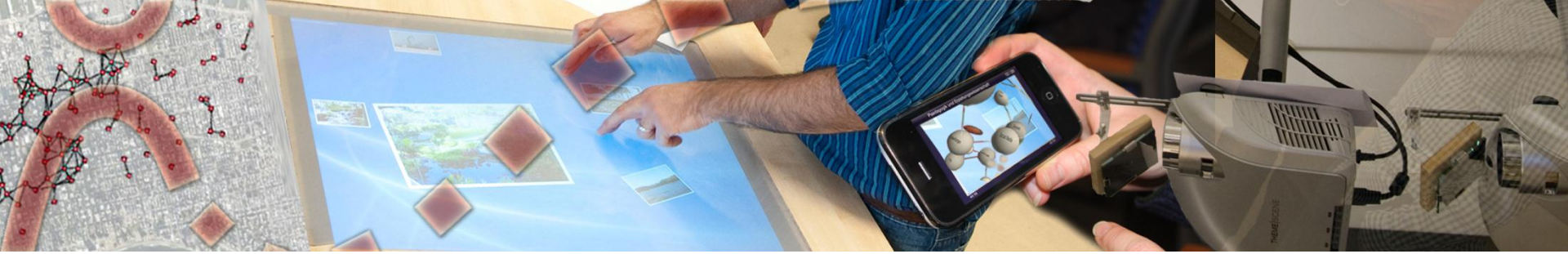
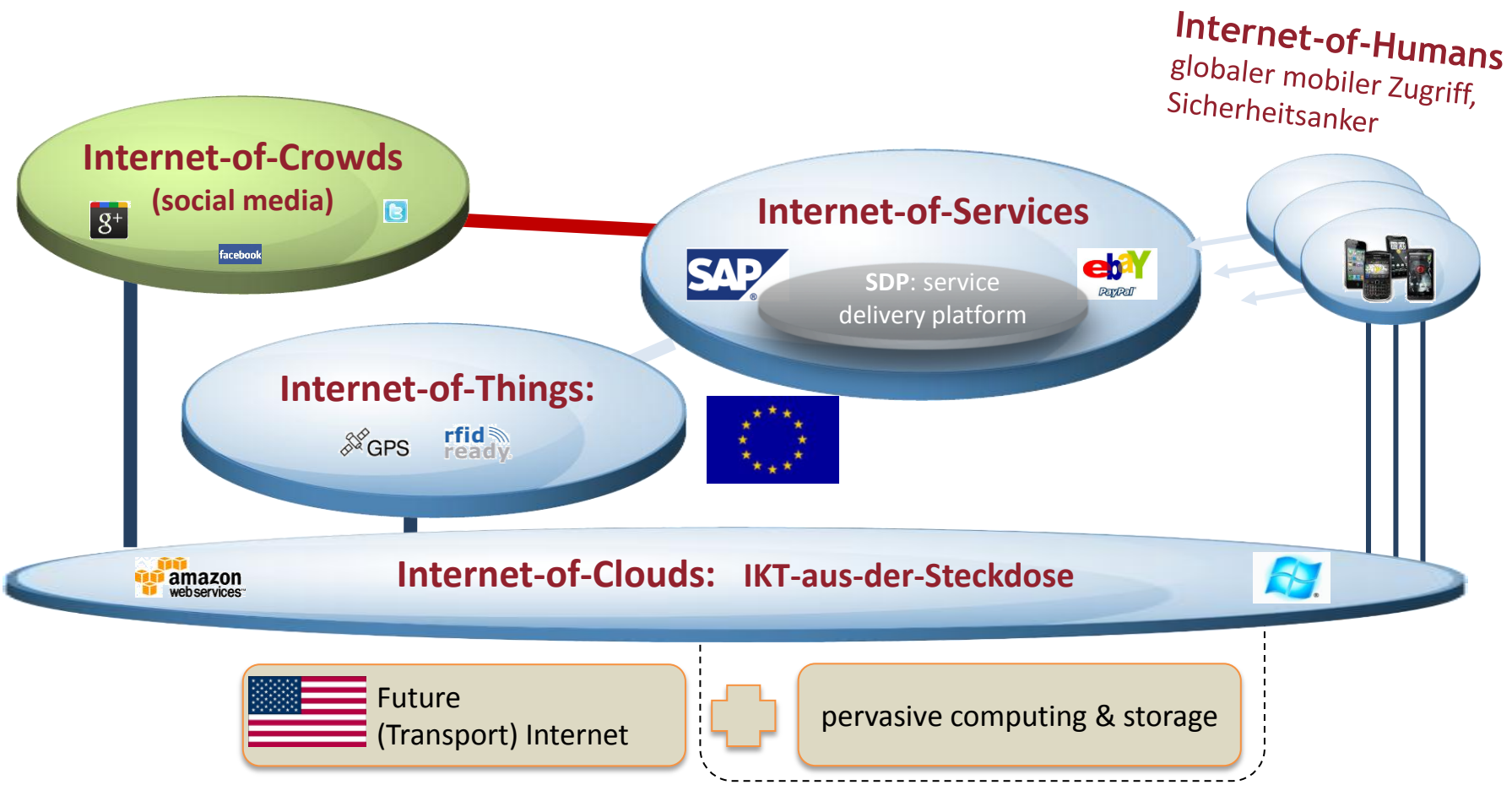


Sicherheit im künftigen Internet

Prof. Dr. Max Mühlhäuser
Telekooperation
& CASED

Technische Universität Darmstadt

Hintergrund: Future Internet US ↔ EU

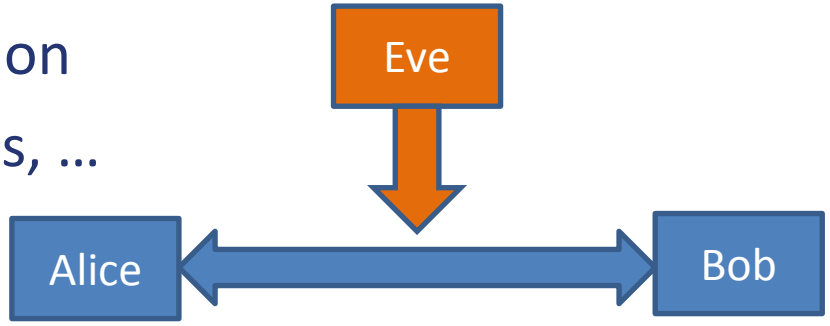


Wesentliche Herausforderungen

Herkömmlicher Fokus:

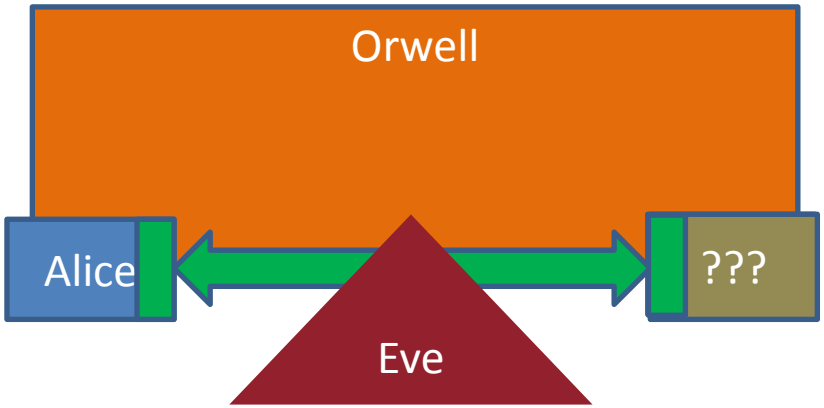
sichere Ende-zu-Ende-Kommunikation

+ DenialOfService-Resistenz, Policies, …



Künftiger Fokus:

- Systemsicherheit (Cloud, mobile&embedded, Langzeit, …)
- Vertrauensbewertung
- Privatsphärenschutz
- Resilienz

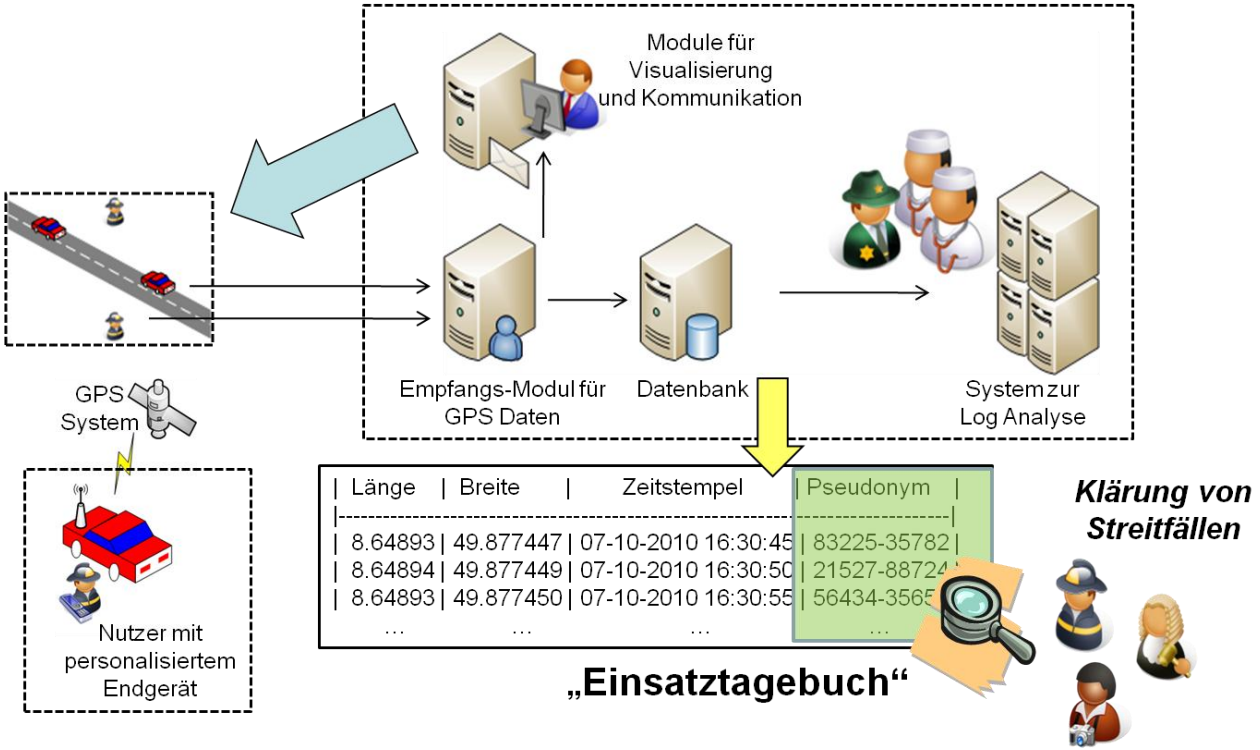


Beispiel: Rettungskräfte-Endgerät

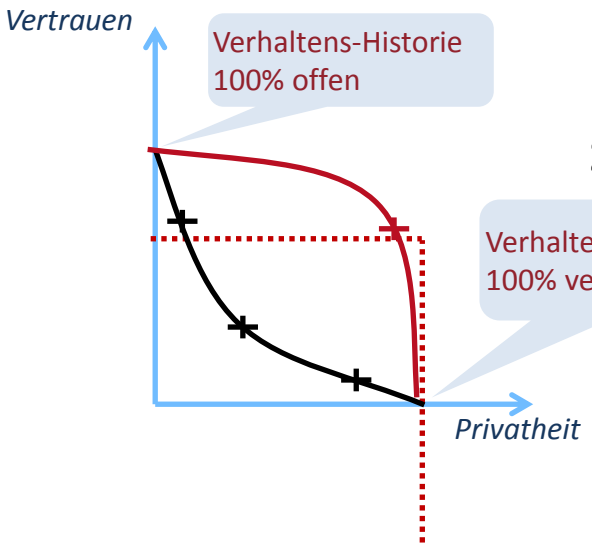
TECHNISCHE UNIVERSITÄT DARMSTADT

Endgerät → Einsatztagebuch + Kommunikation

- Privatheit vs. Nachvollziehbarkeit:
  Transaktions-pseudonymisiertes Einsatztagebuch
- Kommunikation:
  attributbasierte Verschlüsselung

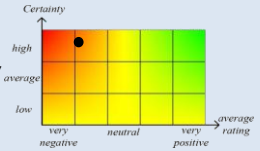


Bsp.: Privatheit vs. Vertrauen



Problem:
Zielkonflikt!

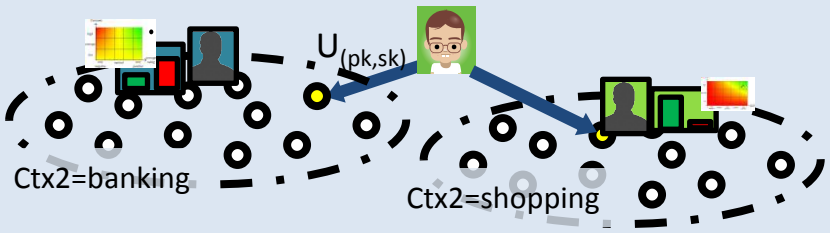
I) CASED Vertrauensmodell:
- robustes ‚computational model'
- strikte Theorie als Basis
- Altern & Attacken (false praise / false accusation) berücksichtigt
- Nutzbarkeit besser denn je



Kombination:
- nicht verlinkbare Identitäten
- Pseudonyme als IDs
- für Kunden, service chains, …
- pro Kontext: Reputation

Optimierung:
robustes Vertrauensmodell
→ ID-Managemet effizienter
(reduziert Zahl der Duplikat-Tests)

II) CASED Pseudonyme:
- rollenbasiert (1 per Kontext)
- Validität & Duplikate überprüfbar (Sybil-Attacken, Whitewashing)
- ‚trusted 3rd party' nur offline nötig
- Nutzerdefinierte Kontexte möglich



KRITische InfraStrukturen KRITIS

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Internet wird genuine KRITIS**
  - 60% Firmen mit U > 50M€: Verluste ab 1 min. Stillstand, 7 Tage Planungsmaximum
  - *Internet der Dienste* wird *die* globale Wirtschaft
- **Kritische Infrastrukturen zunehmend IT-basiert**
  - Energiewende → Beschleunigung
  - Mobile Nutzung, Internet-der-Dinge, allgemeine Zunahme *vernetzter* IT
  - **Outsourcing** vergrößert Sicherheitsprobleme erheblich!
    - Dienstleister vernetzen *ihre* Menschen & Geräte *in* der KRITIS

KRITIS → KRITIS

KRITIIS → Resilienz

TECHNISCHE UNIVERSITÄT DARMSTADT

- Fokus Schad-SW → Fokus „Notbetrieb“

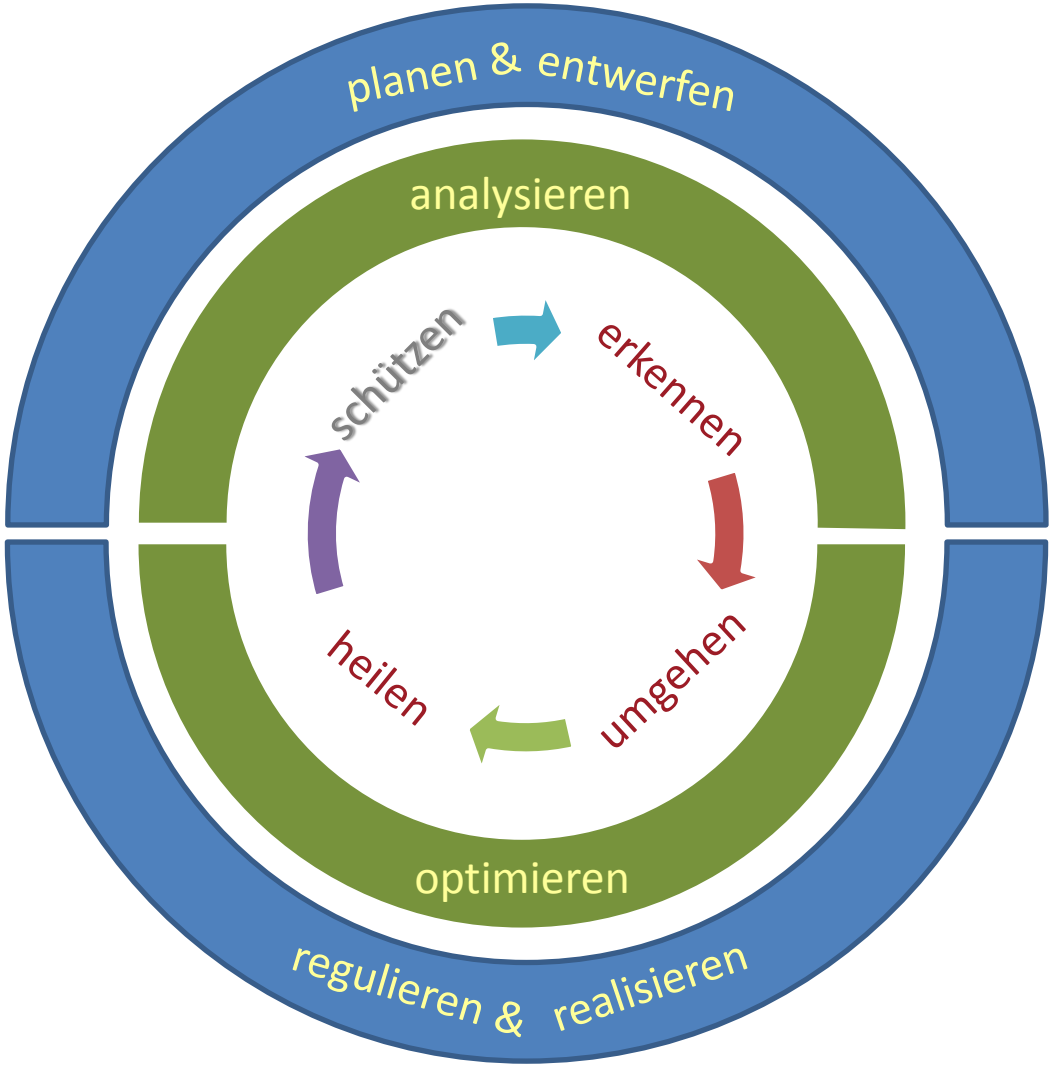
- Bewusstsein für
  - Professionalität (Staaten, Organisiertes Verbrechen)
  - Angriffsrisiko ‚von innen‘ (angelieferte Firmware/Chips, Mitarbeiter)
  - unvermeidbares Restrisiko für alle denkbaren Schäden
  - Verschmelzung aller Schadens-Arten (böswillig oder nicht)

Kernbotschaft:

Resilienz *muss* bei Planung & Strategie beginnen!

Resilienz: Schema

- Realzeit-Zyklus
- Iterative Verbesserung
- Strategische / Nationale Planung



Zusammenfassung

TECHNISCHE UNIVERSITÄT DARMSTADT

- Erheblich vielseitigere Aspekte der IT-Sicherheit
  - Privatheitsschutz
  - Vertrauensbewertung
  - spezielle Ansätze für spezielle ‚Systeme' (Cloud, Embedded, Langzeit …)

- **KRITIIS stellen Resilienz in den Fokus**
  - Thema steckt vergleichsweise in den Kinderschuhen
  - ‚Ausrollen' erfordert deutlich mehr Planung vorab
  - herkömmlicher Schutz ist nur ‚kleiner' Bestandteil
  - erhebliche Kosten → Mehrfachnutzen maximieren