Trusted Resilient IDS (TRIDS)

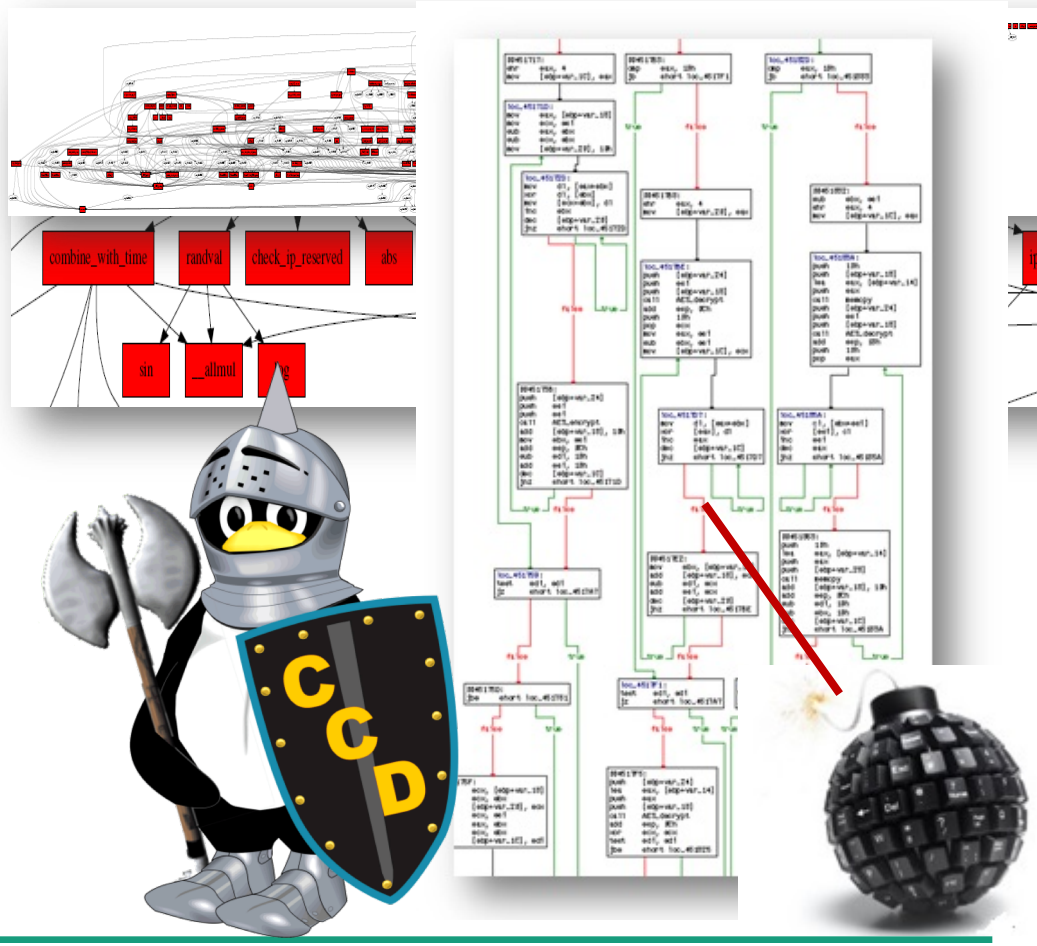
Sicherheit im Kollektiv

Mittwoch, 11. Juli 2018 – Innovationstagung / CODE – 2018, München

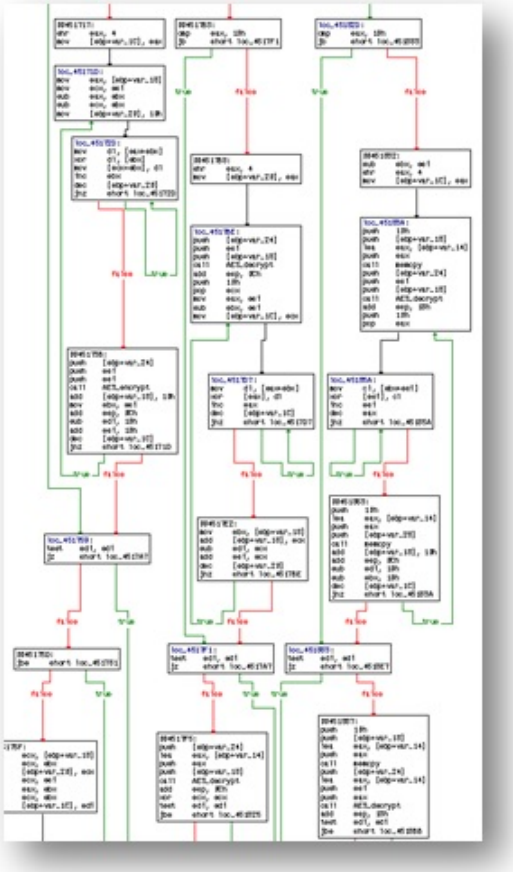
Fraunhofer FKIE

Klassisches Wirken von Schadcode (Exploitation + Payload)

- Software Execution Monitoring
- Verify Control Flow
- Detect Exploitation



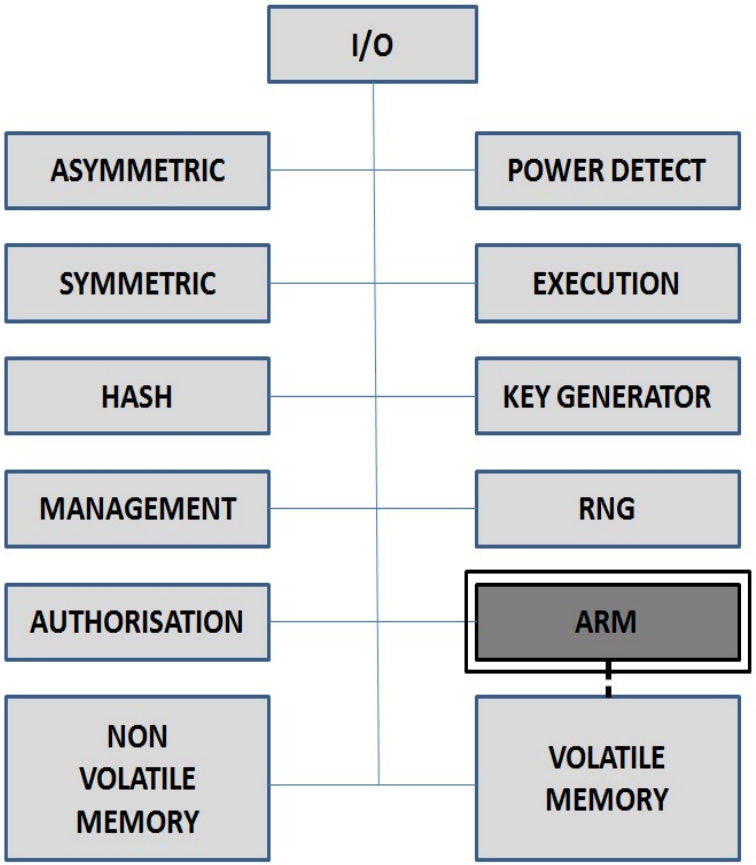
Problemstellung
Was ist ein gültiger Control Flow?

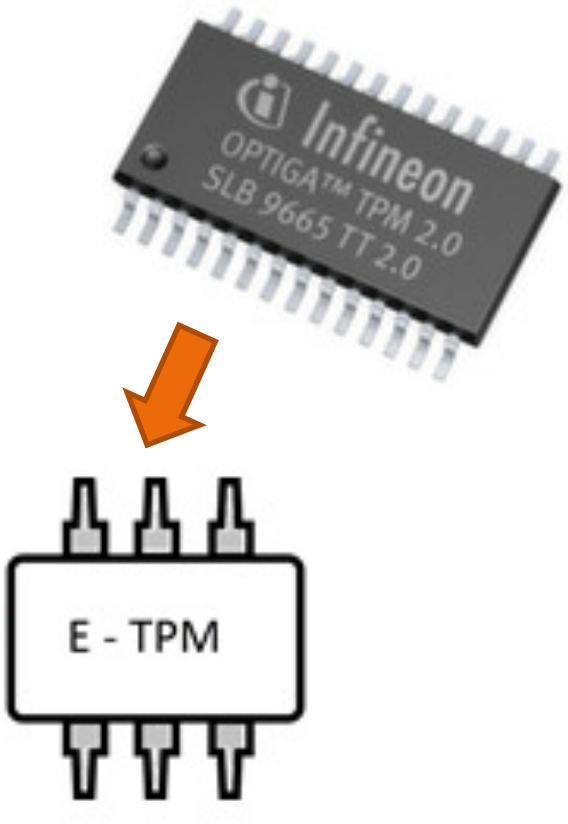


Erhalt der Information:

Fraunhofer FKIE

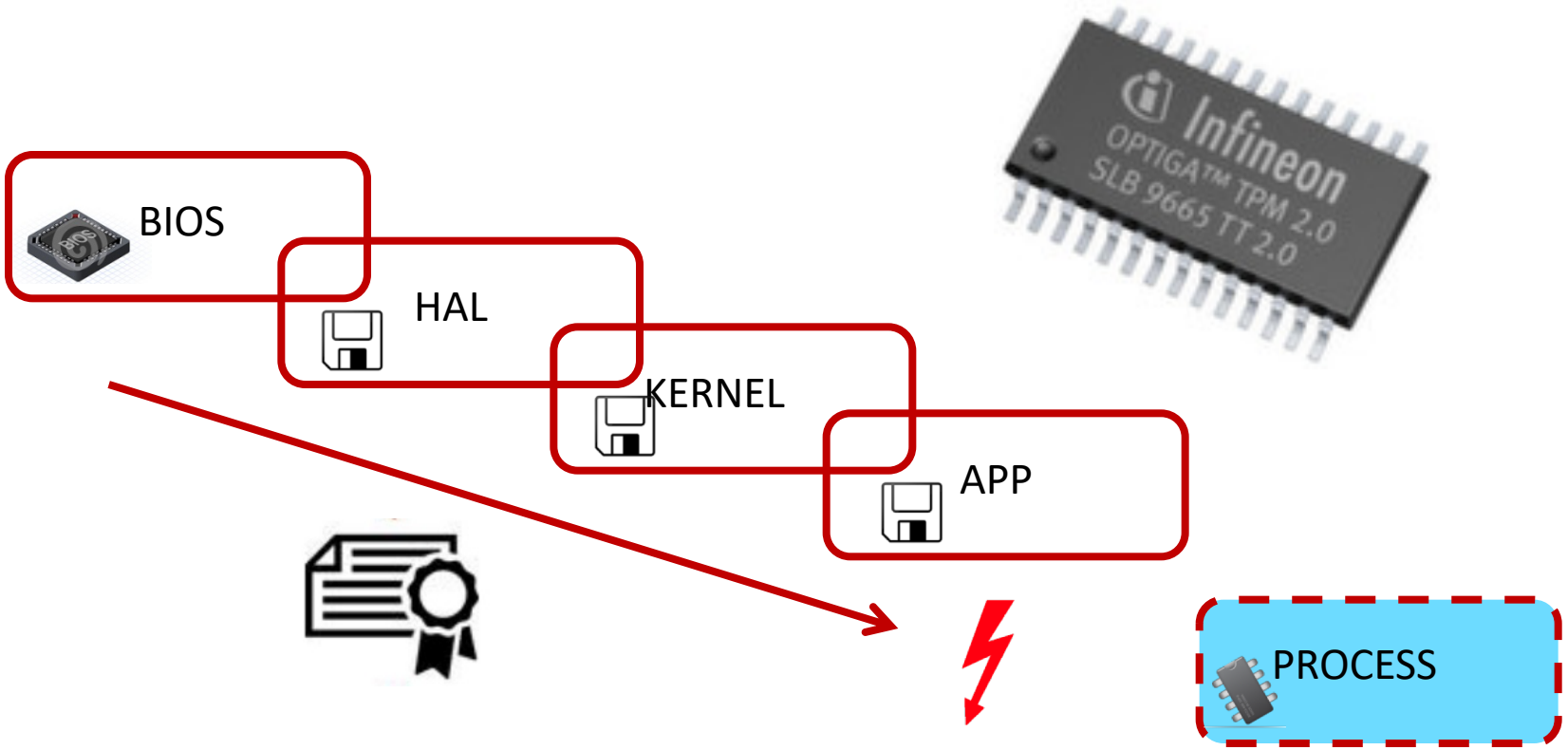
Attack Recognition Modules (ARMs) auf Trusted-Computing Basis



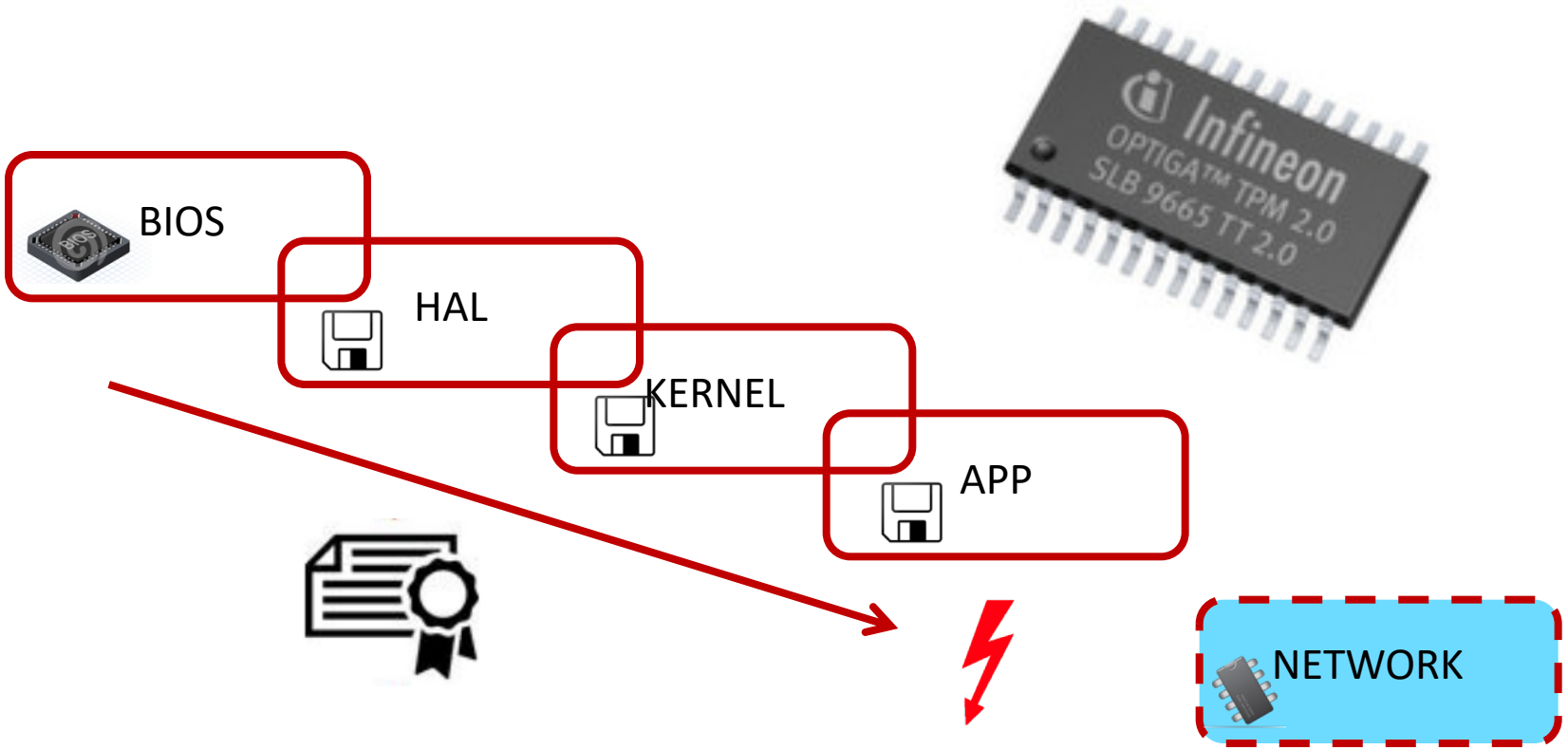


Fraunhofer FKIE

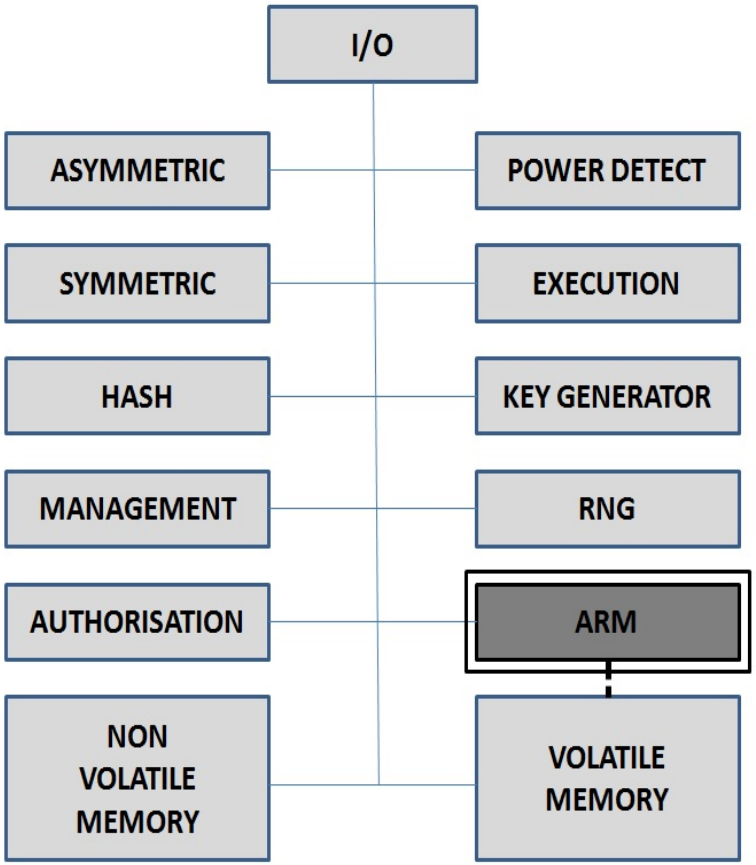
Chain of Trust
Fortsetzung der Kette – in den Speicher

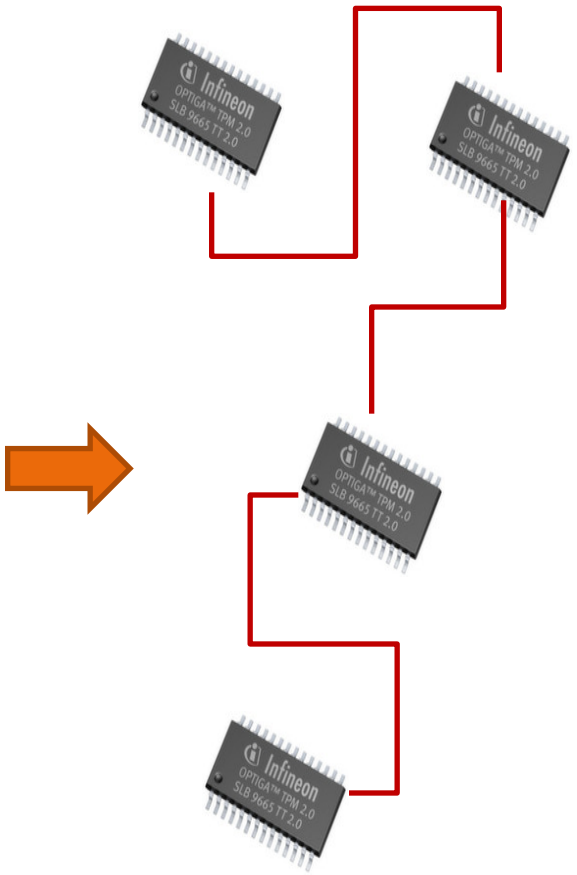


Chain of Trust
Fortsetzung der Kette – zu den Nachbarn



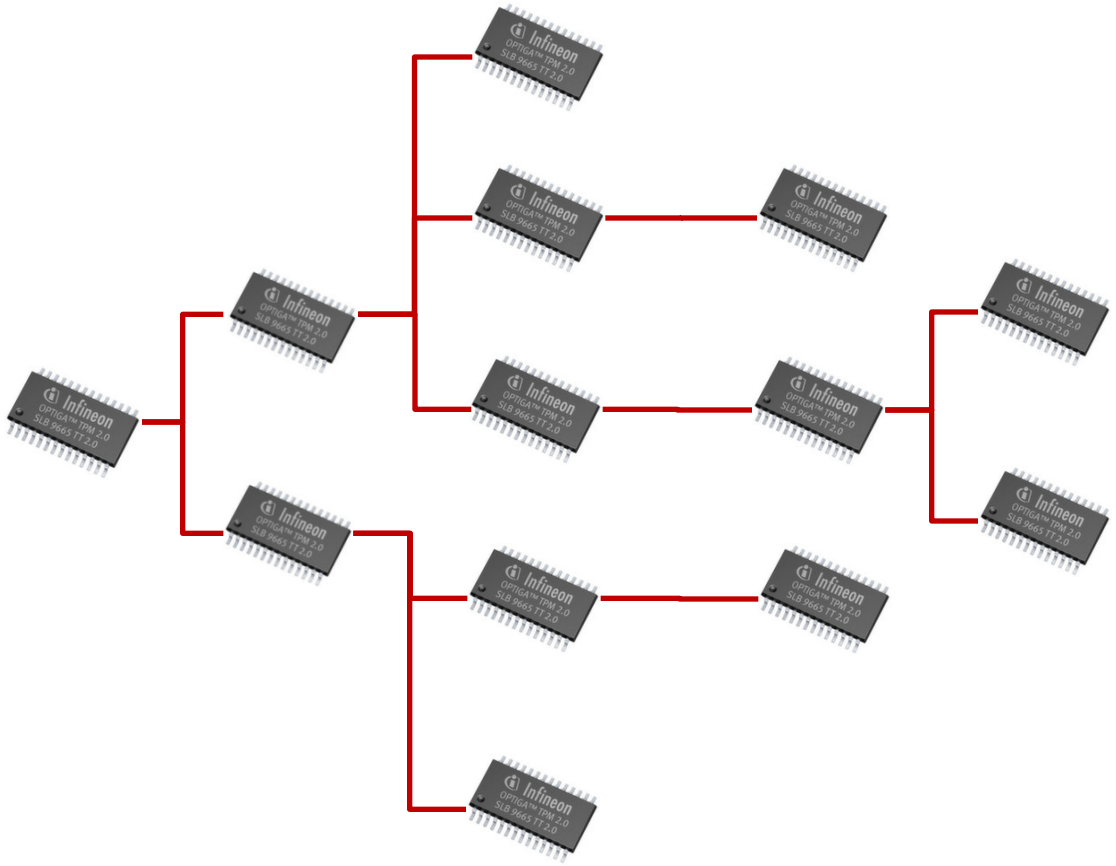
Attack Recognition Modules (ARMs) Based on Trusted Computing





Fraunhofer FKIE

Trusted Integrity Networks (TINs)

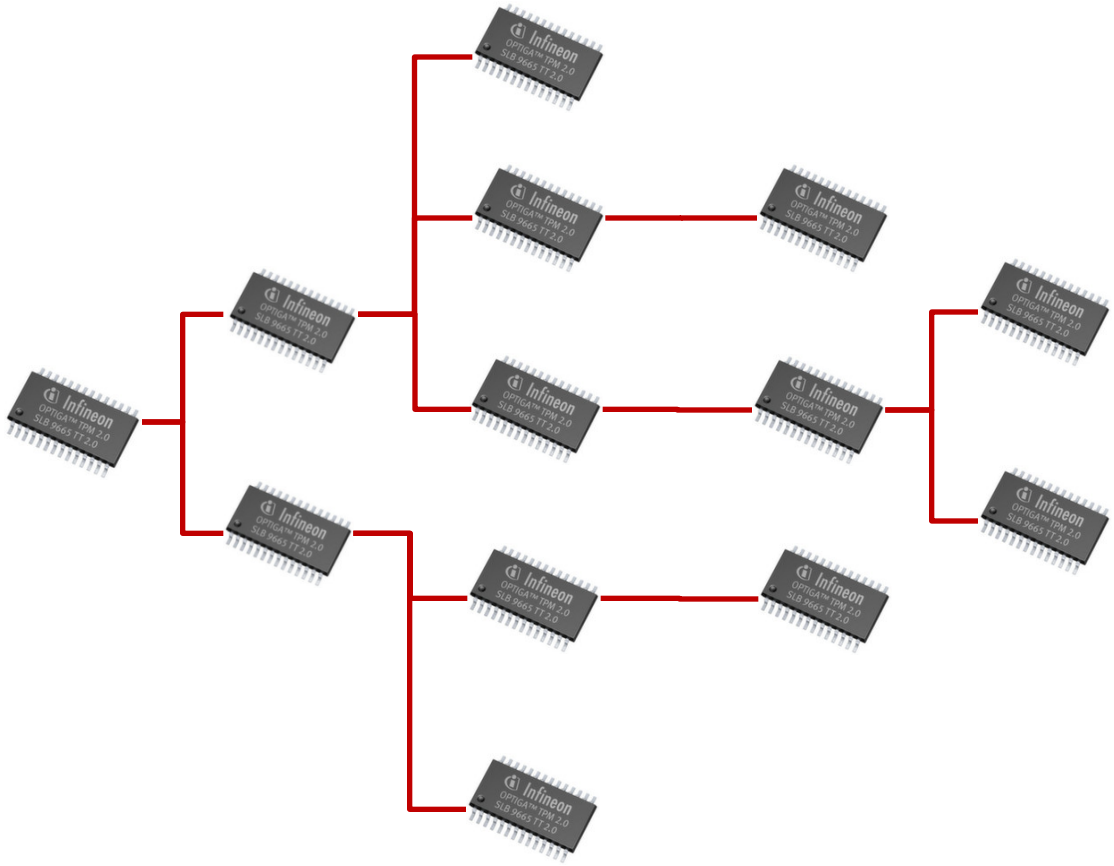


- Skalierbar
  - LAN
  - Intranet
  - AS
  - Intra AS
  - Internet

Trusted Resillient Intrusion Detection System (TRIDS)

- Jeder Knoten eines TINs versteht sich als kollaborativer Teil eines verteilten IDS
- Alle „gesunden“ Knoten sind gleichberechtigt, infizierte Knoten werden aus dem Verbund entfernt
- Wirkt durch
  - Strikte technische Trennung von Funktionalität und Sicherheit
  - Prozessverifikation durch Metadaten
  - Kollektivität statt Inividualität

Trusted Integrity Networks (TINs)



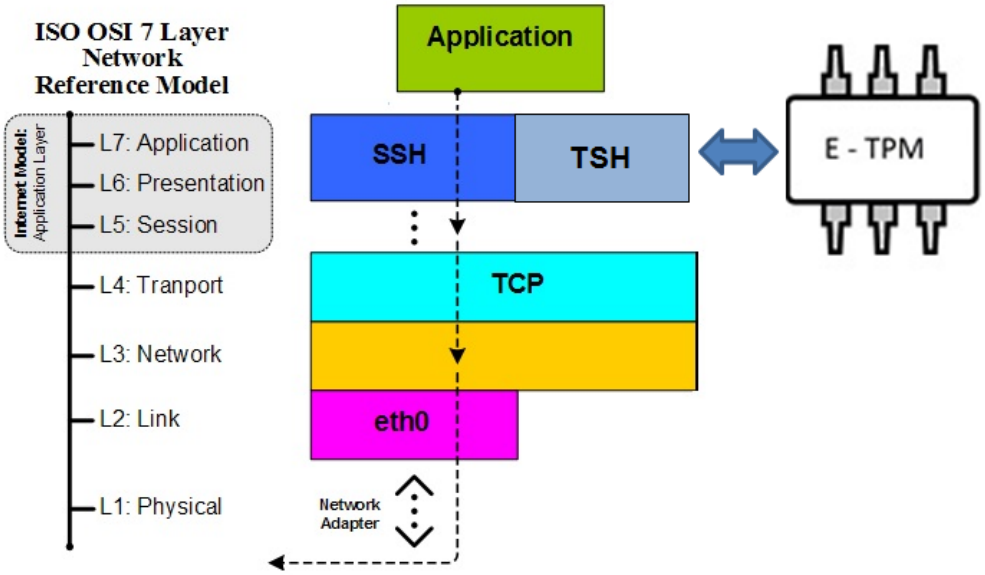
Fraunhofer FKIE

Connecting Islands of Trust: Trusted Communication

- Trusted ARP (TARP)

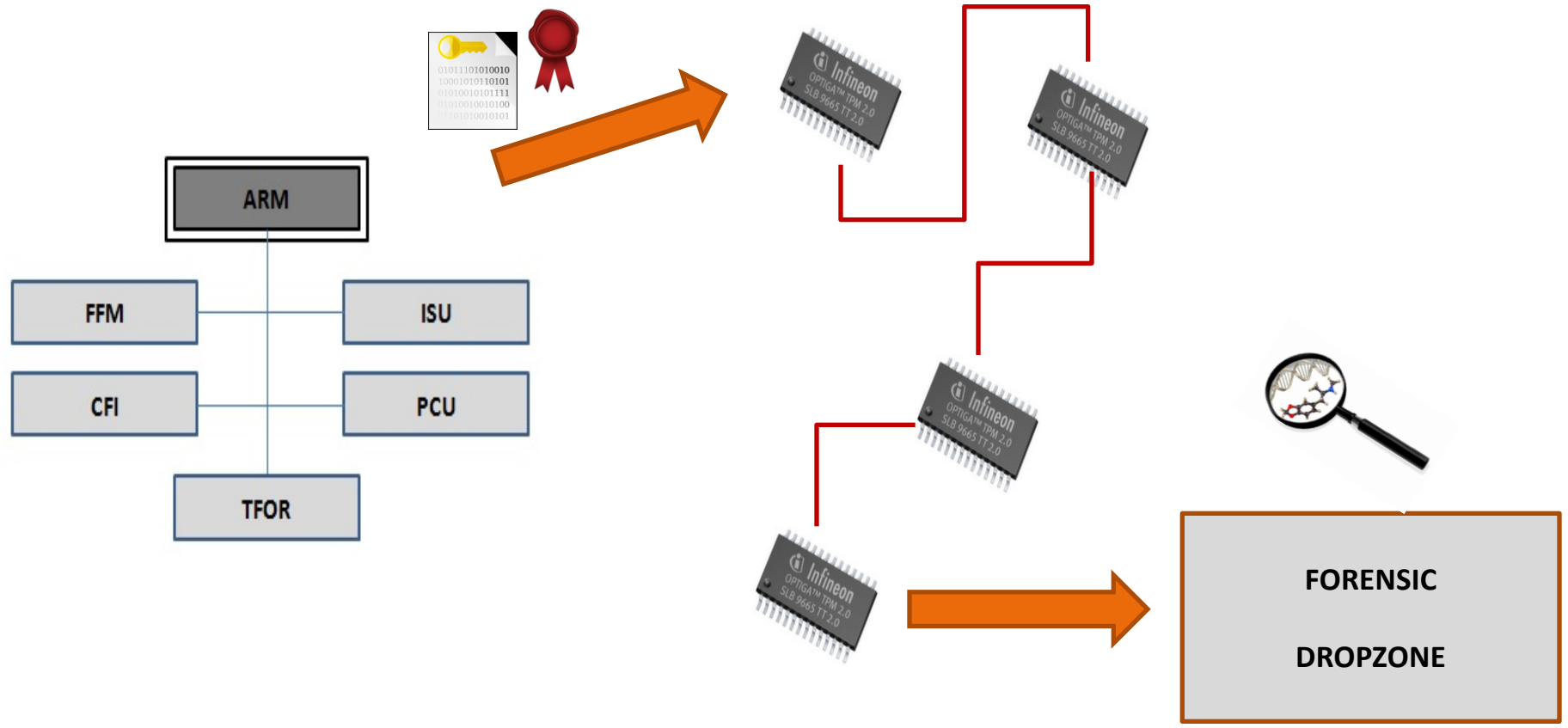
<HARDWARE TYPE>		<TARP>	
HW ADR LEN = 4	PARAMETER LEN	SEQ NO	OPCODE
SENDER HW ADDRESS			
DESTINATION HW ADDRESS			
PARAMETER			

- Trusted Shell / Trusted Socket Layer (TSH / TSL)

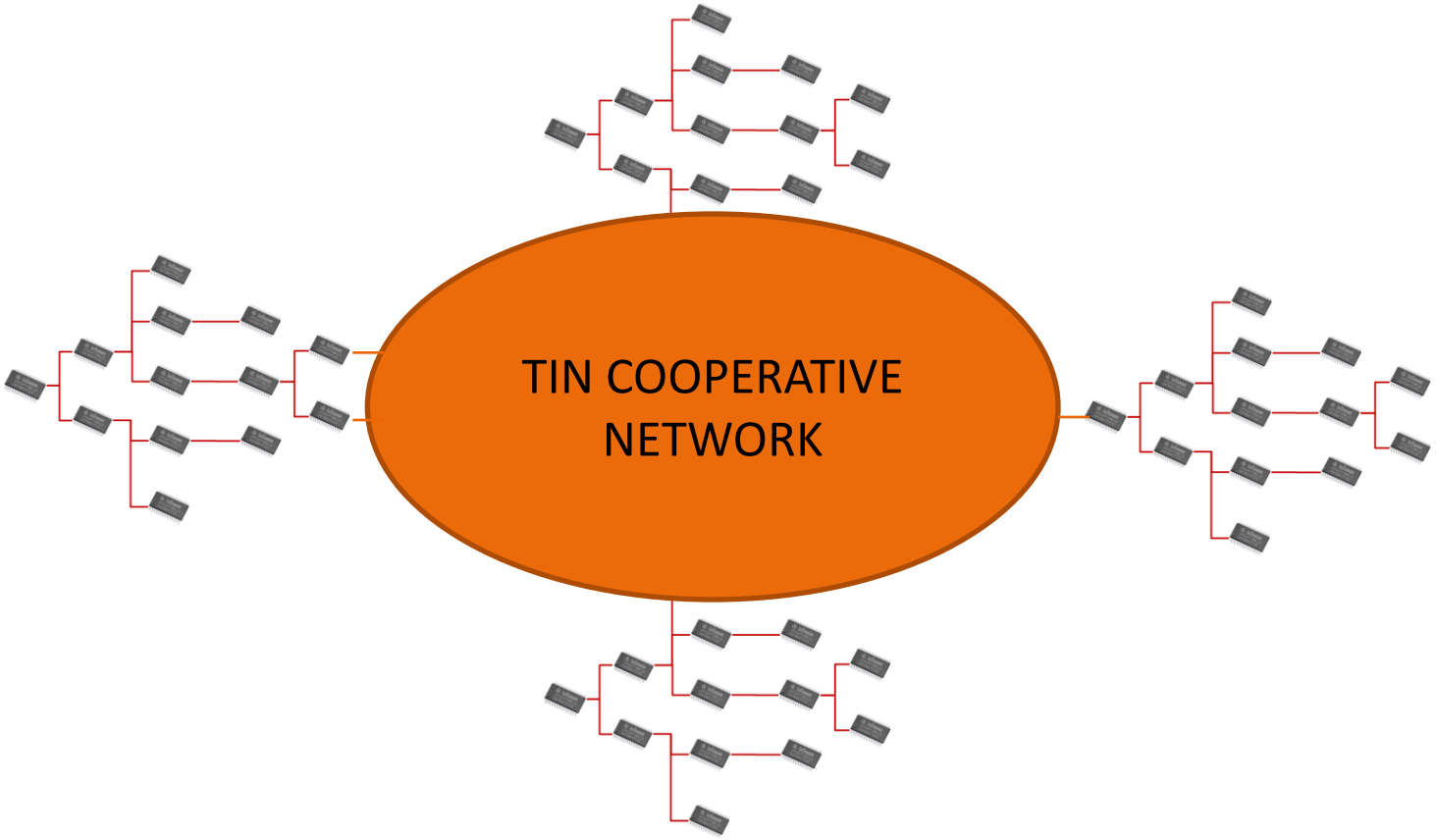


Fraunhofer FKIE

Weiteres Anwendungsbeispiel: Trusted Forensics



Global Intrusion Prevention System (GIPS)



One Small Step for a Cyber Engineer – One Giant Leap for Mankind …

CYBER ANALYSIS & DEFENSE

Practically relevant solutions for
detecting, analyzing, and reacting to cyber attacks

Markus Maybaum
markus.maybaum@fkie.fraunhofer.de

FRAGEN ?

Resource-efficient Cryptography
- Efficient Key Management
- Application Protection Protocols
- Network Protection Protocols

Monitoring & Situational Awareness
- IDS for heterogeneous Networks
- Operational Picture & Situational Awareness
- Intrusion Response

Digital Forensics & Malware Analysis
- Malware Analysis
- Digital Forensics
- Honeypots/Honeynets
- Botnet Analysis

Secure Network Architectures
- Interoperable Coalition Architectures
- Multi-Level Security
- Gateway Concepts
- Protected Core Networking

Fraunhofer FKIE