Short Introduction

- Education as Electrical Engineer, Dr.-Ing. Dissertation at Technische Universität München, Germany
- Research and Management Positions in Industry for 8 Years
- Full Professor of Computer Science and Electrical Engineering at Technische Universität Darmstadt (since 1990)
- Vice President of CASED Research Center for IT Security, Head of „Secure Things“ Research Area
Current Situation

- Mobile communication (MC) is an ubiquitous part of modern life.

- MC relies on a tight cooperation of mobile devices and a non-mobile infrastructure.

- Many aspects have to be considered in real-world applications:
  - business aspects
  - technology
  - legacy issues
  - standardisation
  - security and privacy.
Self-Protection Properties

- **Self-healing** *(reactive view)*

- **Attack resistance** *(proactive view)*
Secure MC Components: The Big Picture
Secure MC Components: Service Map

Integrity
- Partial Reconfiguration
- Fast Fault Detection
- Group Key Management

Self-Monitoring
- Monitor Generation
- Trusted Platforms

Intrusion Detection
- Model of Computation
- Privacy

Confidentiality
- Privacy Protection
- Identity Management
- Identity Proofs

Availability
- PUFs

Secure Things
- Geographically Secure Routing
- Self-Healing
- Triple Module Redundancy
- Quality of Service
- Reliability

Sorin A. Huss

11/10/2009 | CASED | Secure Things | 6
Self-Protection by Security-Anchors (I)

Side-Channel Analysis

Motivation
- Every implementation might leak information on a side-channel.
- Attackers will keep using side-channels to compromise the system if the secret information is valuable enough.

Challenges
- Missing generalized design methodologies for hardware and embedded systems designers to harden their implementations.
- Resource-effective countermeasures against power attacks.

Contribution
- Methods for leakage detection.
- Countermeasures to harden physical devices against power attacks at minimal cost.
- Design methodologies to considerably reduce side-channel information leakage.
Results of DPA Attacks in Presence of Countermeasures (*Dyn. Mutation*)

**Power Analysis without countermeasure:**

\[ P(t_i) = P_{process}(t_i) + P_{noise}(t_i) \]

\[ \text{Var}(P(t_i)) = \text{Var}(P_{data}(t_i)) + \text{Var}(P_{Op}(t_i)) + \sigma \]

\[ \text{Var}(P_{Op}(t_i)) \rightarrow 0 \]

**Power Analysis with countermeasure:**

\[ \text{Var}(P(t_i)) = \text{Var}(P_{data}(t'_i)) + \text{Var}(P_{Op}(t'_i)) + \sigma \]

\[ \sum_{j=i-1}^{i} \Delta \text{op(intermediate result}(t_i, r_j)) \]

\[ \text{Var}(P(t_i)) = \text{Var}(P_{data}(t'_0, \ldots, t'_i)) + \text{Var}(P_{Op}(t'_i)) + \sigma \]

DPA result: 500 traces on unsecured eMSK

DPA result: 100,000 traces on secured eMSK
COSADE 2010
- Call for papers -

Cryptography and Side-Channel Analysis:

- Stochastic approach in power analysis
- Advanced stochastic methods in side-channel analysis, especially in power analysis and EM analysis
- Leakage models and security models for side-channel analysis in the presence and absence of countermeasures
- Side-channel analysis under black-box assumption
- Side-channel leakage assessment methodologies, models, and metrics

Secure Design and Architectures:

- Verification methods and models for side-channel leakages within the design phase
- Methods, tools, and platforms for evaluation of side-channel characteristics of a design
- Criteria for the design flow of countermeasures
- HW / SW-acceleration for (constructive) SCA
- Countermeasures against attacks at algorithmic-, logic-, register transfer-, and physical-level

Important Dates:

- Submission of abstracts: December 06, 2009
- Notification to authors: January 03, 2010

For more information: http://cosade.cased.de
Trustworthy Reconfigurable Architectures

Motivation
- No trustworthy dynamic reconfiguration procedure for FPGAs available yet.
- Applications, which are relevant to security, demand a tamper proof and trustworthy execution environment.

Challenges
- Building security enhanced architectures on highly dynamic structures like FPGAs.
- Trustworthy reconfiguration of embedded systems for hard- and software.

Contribution
- Secure and trustworthy update procedures
- Flexible Trusted Platforms
Offline tasks

• Measurement metrics such as attack surface and impact area

• Formal modeling with CASE tools / code abstraction techniques or by using wrapper-frameworks for state space / model mapping

Online tasks

• Resource-constrained runtime threat profiling of crucial modules and interfaces

• Methods to determine and trigger necessary reactions, e.g., reconfiguration, self-healing, quarantine, or restart
Self-Healing Nodes in Homogenous Networks

Motivation
Self-healing in networks is currently done mostly on top of communication links.

Self-Healing

Challenges
- Self-healing strategies at runtime
- Healing by adjacent nodes
- Healing of entire networks

Goal
Self-healing nodes in addition to links
Motivation

- MoCs allow the mapping of functionality either to hardware or to software. From a system level perspective a comprehensive design space exploration becomes feasible.

Challenge

- Efficient hw/sw mapping of MoCs

Contribution

- System-level design flow for embedded systems based on MoC mappings
- Automatic transformation and partitioning of a MoC
Security & Quality of Service in Multihop Wireless Networks

Motivation
- Multihop wireless networks enable novel forms of communication
- Wireless ad hoc networks, mesh networks, and sensor networks

Challenges
- Applications and services such as the “Internet of Things” or “Industrial Automation” rely on well-defined QoS of the network provisioned data
- (Most of) today’s security mechanisms can not be applied directly because network borders disappear and centrally trusted instances are missing.

Contribution
- Modeling and analysis of threats/attacks (analysis, simulation, testbed)
- Mechanisms and protocols for decentralized and infrastructure-less networks
  - Jointly optimizing security and quality of service in the network
Piracy Protection by Secure Authentication

Motivation

- Identification of faked products, protection of Intellectual Property (IP)
- *Examples*: Components and replacement parts in automotive or avionics, medicine or cosmetics (with RFIDs), embedded systems

Challenges

- Using Physical Uncloneable Functions to implement a secure and uncloneable identifier, which enables the binding of functionalities to specific devices (IP protection)
- Development/Implementation of a lightweight authentication mechanism for resource constrained systems

Contribution

- Prototypes to check the authenticity of arbitrary products (RFID tagged)
Thank you for your attention!