MMEDIA 2011 Keynote Speech:
Advanced Security and Reliability Challenges for Multimedia Networks and Services

Prof. Dr. Michael Massoth
Hochschule Darmstadt – University of Applied Sciences
Department of Computer Science (Informatics)
Darmstadt, Germany

@ MMEDIA 2011, April 20th - Budapest, Hungary
Hochschule Darmstadt
University of Applied Sciences

- Darmstadt is between Frankfurt am Main and Heidelberg.
- Hochschule Darmstadt has about 11,500 students in total.
- With about 1,200 students one of the largest Departments of Computer Science in Germany.
Breaking News:
Balatonfüred, Hungary, 15 April 2011

Neelie Kroes
Vice-President of the European Commission responsible for the Digital Agenda

Working together to strengthen cyber-security
Telecom Ministerial Conference on Critical Information Infrastructure Protection
Public Session Balatonfüred, Hungary, 15 April 2011:

“The EU's digital economy is at least €500bn a year. That's the size of Belgium's economy, and it's growing at 12% a year.”

The new EU-US Working Group on cyber security and cyber crime as well as the Public–Private Partnerships (PPP) will focus on

“fighting botnets, security of the Domain Name System, the Border Gateway Protocol, routing tables, undersea cables and industrial control systems for smart grids.”
Agenda and Outline

- CASED  IT-Security made in Darmstadt
- Research Areas [with examples and highlights]
- Research @ Hochschule Darmstadt [selected examples]
IT-Security made in Darmstadt

CASED – Center for Advanced Security Research Darmstadt

[Some advertising]
Supporting Organizations
Facts and Numbers
Three Organizations are CASED
Facts and Numbers about CASED
07/2008 – 11/2010

11 Million Euro in LOEWE funding
4 Million Euro in third party funding
> 400 scientific publications

128 scientists involved (under it)

68 new Ph.D. students, 9 new PostDocs

6 new IT Security professorships at TU Darmstadt and Darmstadt University of Applied Sciences
Research Areas
[overview and some highlights]
Research Areas

- Secure Data
- Secure Things
- Secure Services
Research Area: **Secure Data**
Example: New Identity Cards

Electronic ID

Password (PIN)

Key K

PACE

Password Authenticated Connection Establishment

Terminal Authentication

Chip Authentication

Communication

Reader

Password (PIN)

Key K

enter PIN
Research Areas: **Secure Things**

**Application Scenarios**

- **Identity and Rights Management**
- **Trustworthy Embedded and Mobile Systems**
- **Secure Interaction of Embedded and Mobile Systems**
- **Constructive Side-Channel Analysis**
- **Self-Monitoring by Security-Monitoring**
- **Platform Security**
- **Network Security**

**Layer Structure**

- **Application Layer**
- **Architecture Layer**
- **Technology Layer**
Example:
Physically Unclonable Function

Challenge „Who are you?“

Original card of Max Sample
Research Area: Secure Services

- Security Policies & Malware (PP1)
- Security Automata (PP2)
- Security Monitoring (PP3)
- Security Services
- Security Services
- Serving Security
- Serving Security
- Securing Services
- Securing Services
- Legal and Economic Aspects of Secure Services (PP4)
- Security Testing & Risk Management (PP5)
- Privacy-friendly & Trustworthy Services (PP6)
- Resilience for Secure Infrastructures (PP8)
- Secure Identities & Biometrics (PP7)
Example: Encapsulation of Services
Cross-sectional Research Areas

Secure Data
Secure Things
Secure Services
Cross-sectional Research Areas

Secure Data
Secure Things
Secure Services

Secure Infrastructure
Cross-sectional Research Areas

- Secure Data
- Secure Things
- Secure Services

Secure Infrastructure

Data Security and Privacy
Cross-sectional Research Areas

- Secure Data
- Secure Things
- Secure Services

Secure Infrastructure
Data Security and Privacy
Usability of Security solutions
Cross-sectional Research Areas

- Secure Data
- Secure Things
- Secure Services

Secure Infrastructure
Data Security and Privacy
Usability of Security solutions
Research Areas and Challenges

[selected examples in more detail]
Research Area 1: Secure Data

- Secure Data
- Secure Things
- Secure Services
Secure Data: **Challenges**
Electronic Identity Cards / Passports

- PACE (Password Authenticated Connection Establishment)
- Terminal Authentication
- Chip Authentication
- Communication secured through key $K$
- Key derivation

Type in PIN
Analysis of **Password Authenticated Connection Establishment (PACE)**


- PACE secure in model of Bellare, Pointcheval, Rogaway (BPR) under DH-like assumption, ideal-cipher- & random-oracle-model
Research Area 2: Secure Things
Secure Things: Challenges
Secure Things: Service Map

CASED - Secure Things
Darmstadt, Hesse

- Self-Protection by Security-anchors
- Security Monitoring by Self-Monitoring
- Self-Healing by Reconfiguration of Hard- and Software
- Secure Interaction
- Identity- and Rightsmanagement

Secure Things

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

Authenticity
- PUFs

Privacy
- Privacy Protection
- Identity Management
- Identity Proofs

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

Availability
- Self-Authencity
- Model of Computation
- Intrusion Detection

Self-Monitoring
- Monitor Generation
- Trusted Platforms

References

© Prof. Dr. M. Massoth
FB Informatik
Self-Protection by Security-Anchors

- **Side-Channel Analysis**
  - Methods for leakage detection
  - Countermeasures to harden physical devices against power attacks
  - Design methodologies to considerably reduce side-channel information leakage
  - Minimize the cost of countermeasures

- **Trustworthy Reconfigurable Architectures**
  - Building security enhanced architectures on highly dynamic structures like FPGAs
  - Trustworthy reconfiguration of embedded systems for hard- and software.
  - Secure and trustworthy update procedures
  - Flexible Trusted Platforms
Self-Monitoring by Security-Monitoring

- **Automatic Generation of Software Monitors**
  - Modeling of requirements as complementary use and misuse cases
  - Construction of **life sequence charts (LSCs)** for use and misuse scenarios
  - Combination of LSCs into Petri nets and merging into a monitor net

- **Self-Monitoring in Embedded Systems**
  - Measurement metrics and formal modeling for state space and model mapping
  - Resource-constrained runtime threat profiling
  - Methods to determine and trigger reactions such as reconfiguration, self-healing, or restart
Identity and Rights Management

- **Piracy Protection by Secure Authentication**
  - Identification of faked products, protection of Intellectual Property (IP)
  - **Intellectual Property protection** by means of Physical Uncloneable Functions
  - Development and implementation of lightweight authentication mechanisms
  - Authenticity check of RFID tagged products

- **Exchange of Identity- and Authorization-Proofs**
  - Consideration of secure the near field communication (NFC)
  - User-friendly security improvement for ubiquitous computing
  - Migration of chip card applications to NFC devices
  - Implementation of a NFC platform for access control
Research Area 3: Secure Services
Secure Services: Mission

Develop technology for certifiably secure and trustworthy software components in the Internet-of-Services;

Provide infrastructures where security, trustworthiness, and privacy are governed in an ecosystem of service providers, hosts (such as Clouds), and consumers.
Secure Services: Structure
The Approach at a Glance

Controlling usage of data and resources at run-time

self-contained software entity

observation

enforcement

run-time monitor

Encapsulation with a run-time monitor

unprotected service

encapsulated service

Implementing the encapsulation (collaboration with PP3):
aspect-oriented programming, inlining, monitoring in VM
**Novel Concept: Service Automata**

**Generic in the security policy**
- enables flexible instantiation to security demands

**Reliably respecting program and policy semantics**
- provable because of formal specifications for both aspects

**Suitable for distributed systems**
- due to efficient, decentralized enforcement
- communication structure independent from communication of the system
Service Automata in the Scenario

Decentralized enforcement allows us to

- avoid bottlenecks
- avoid single points of failure
- reduce latencies
Example:
A Distributed Repository Service

Company 1
- Alice
- Bob (freelancer)
- Mallory
- Zoe
Company 2

Server Frankfurt
- upStockMgmt
- EI-Risk
Server Paris
- upRisk
Server London
- EI-Trade
Server New York
- ZT-Trade
- US-TAX
Server Toronto
- CA-TAX

software owners
- up-Holding GmbH
- EuroInvest Ltd.
- Zero-Trust LLC
- TaxServices Inc.

development companies
- software developers

global security requirement: Chinese Wall (conflict of interest) could be enforced by centralized control in principle, but …
Secure Services: Challenges
Motivation

- The **internet** is a **marketplace**:
  - Service providers offer services
  - Customers buy goods and information
  - Example:

```
Personal data?   Money?   Contract?
```

![Diagram](https://via.placeholder.com/150)
What really happens:
Service composition & delegation
Secure Services focuses on security aspects

SLA Personal Data → Tux
Security Policies

SLA Personal Data → Pants

SLA Personal Data → Fabric

Security Automata

TP1 derived

TP2

TP3 monitors services

Security Monitoring
Secure Services focuses on security aspects
Secure Services focuses on security aspects
Secure Services focuses on security aspects

- Mobile Authentication (TP6)
- Malware Detection (TP1)
- Identity management and identifiers

Selecting services:
- Trust & Reputation (TP6)
- SLA
- Personal Data
- Legal Requirements

Privacy Enhancing Technologies:
- Tux
- Tux
- Tux

SLA
- Personal Data

Legal Requirements
- TP4
- Privacy
- TP6
Secure Services at a Glance

- TP 1: Security Policies
- TP 2: Security Automata
- TP 3: Security Monitoring
- TP 4: Legal and Economic Aspects of Secure Services
- TP 5: Risk Management, Security Indicators & Metrics
- TP 6: Secure Provision of Services
Trust & Reputation

Goal: Selecting trustworthy service provider
→ For better interactions
eBay sellers with established reputation could expect about **8% more revenue** than new sellers marketing the same goods. 

[Resnick2006, Sun2009]

**Goal:** Selecting trustworthy service provider

⇒ For better interactions
Research & Development within CASED

@ Hochschule Darmstadt

[selected examples]
Real-time polymorphic malware detection

- Christian Maaser – polymorphic malware detection

Motivation
- Malware authors mask the same malicious code by packer or polymorphic self coding & encryption
- Current Anti-Malware-Software cannot detect and identify the masked malware

Idea and goal
- Virus scanners should be able to detect and identify in real-time the unmasked Malware-Code
Fingerprint Sample Quality

- Martin Olsen - predicting Biometric Performance

Motivation
- Border control requires good fingerprint quality
- Good fingerprint sample quality results in good recognition achievements

Idea and Goals
- New Implementation of NFIQ2
- Tiny Implementation for mobile Systems

Approach
- Research of characteristics, which correlate image quality and recognition achievement
Walk characteristic as biometrical authentication (1)

- Claudia Nickel - the way you walk

Motivation
- Data in mobile phones are not protected sufficiently
- Normal case: No PIN needed after idle mode

Idea and Goal
- Concurrent biometrical authentication can substitute PIN
Walk characteristic as biometrical authentication (2)

- Claudia Nickel - the way you walk

Approach

- Capturing and logging of the human walk characteristics by integrated semi-conductor acceleration sensors, sensitive to motion
**Intrusion Prevention System @ host**

- **Mark Seeger** - preventing malicious attacks

**Motivation**
- Host-based intrusion detection system (IDS) as basic security of Host OS
- Malware at host can manipulate IDS results

**Idea and Goal**
- Outsourcing of the IDS monitoring towards the GPU and observing access to CPU memory

**Approach**
- Independent execution at GPU Kernels
Motivation
– the “What, Why, and How?”

Current Host - intrusion detection system (IDS)

► Installed on Host
► Running in parallel to other software
► Executed by CPU
Motivation
– the “What, Why, and How?”

Issues
- IDS “just another service”
- Relies on OS security
- Relies on CPU
- Relies on OS scheduler
- Consumes CPU cycles
- Consumes host memory
- …
Motivation
– the “What, Why, and How?”

Infected
▶ IDS results falsified
▶ Backdoors
▶ Botnet

What can we do?
▶ Clean
▶ Reinstall

Can we do better?
▶ Off-host host-IDS
Motivation
– the “What, Why, and How?”

- Device
  - Dedicated Server
  - Dedicated Host
  - Extraordinary Coprocessor (e.g. FPGA)
  - Commodity Coprocessor (e.g. GPU)

- Host
Motivation
– the “What, Why, and How?”

Usage of a **GPU** for Host intrusion detection

- **Benefits**: Tightly coupled, asymmetric, concurrent
  - Tightly coupled: Shared memory (NUMA)
  - Asymmetric: A processor other than the host’s CPU
  - Concurrent: Autonomously running next to the host’s CPU
Motivation
– the “What, Why, and How?”

▪ Coprocessors
  ▪ Special-purpose Processors, dedicated to perform certain operations
  ▪ Capable of few operations on the one hand, very fast on the other

▪ Coprocessors are ubiquitous
  ▪ Network intrusion detection: Well-known (FPGA, GPU, etc.)
  ▪ Host intrusion detection: Not used so far

▪ Host intrusion detection by coprocessor
  ▪ Faster: Dedicated processor (more CPU time for normal duty)
  ▪ More secure: No host service or host installation
First Results: **Performance Degradation**

Testing environment:
One host was used as a **coprocessor** for the other

Performance degradation according to…

- ...the size of the **observed data structure**.

<table>
<thead>
<tr>
<th>[Bytes of data]</th>
<th>[# Processes]</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>16</td>
</tr>
<tr>
<td>1P</td>
<td>0.75%</td>
</tr>
<tr>
<td>2P</td>
<td>0.16%</td>
</tr>
</tbody>
</table>
Secure Telephony in NGN & IMS as well as in PSTN & PLMN

- Andreas Plies – Call authentication
- Torsten Wiens – Call integrity
VoIP Usage Worldwide

- Number of residential, small- or home office VoIP subscribers grew 24% in 2009 to 132 million worldwide
  [Infonetics Research, 04/2010]

- Total number of mobile VoIP users will be reach 288 million by end of 2013
  [In-Stat, 03/2010]

- 10.3 million VoIP users in Germany 2010
  [BITKOM, 04/2010]
Conversational Partner Recognition

„It’s me, Obama.“

Barack Obama

„Are you kidding me?“

Ileana Ros-Lehtinen
How to identify your conversational partner?

Possible approaches for authentication?

- Via voice?
- Via phone number?
- Combination of customer number and password?
- Cryptographic hardware solutions?
So how U-CAN check who is calling?

- **nPA-VoIPS**
  - Secure VoIP Telephony
  - Confidential Communication
  - Authentication of communication partner
  - Legally compliant archiving with qualified signature

- **Universal Call Authentication (U-CAN)**
  - Secure Telephony in PSTN & PLMN
  - Authentication of communication partner

→ for IMS & NGN
→ for PSTN & PLMN
German Identity Card

- Rollout November 1st, 2010
- Identity card (IC) in credit card size
- Contactless RFID Chip (ISO 14443)
- Sovereign usage like European passport

Additional functionalities:
- Qualified electronic signature like specified in German „Signaturgesetz“ (optional)
- **Electronic Identity (eID)** for E-Business and E-Government Services
  → 2-Factor-Authentication
Electronic ID Authentication

- **Service provider owns a Card Verifiable (CV) certificate**
  - Issued by federal office to trustworthy service provider
  - Contains information about the identity and access rights of the service provider
- **PIN**
  - Allows Identity card (IC) holder to grant access
- **PACE**
  - Password Authenticated Connection Establishment
- **Terminal Authentication**
  - Authentication of service towards IC
  - Proof of provider’s identity and access rights
- **Chip Authentication**
  - Authentication of IC towards service
  - Proof of Authenticity

\[ \text{derive key } K \]

Personal data secured through \( K \)
eID Authentication for telephone calls with ID Card
People: Secure Services