System and IoT Security (Mobile Security) Seminar
- Topics and Procedure –

Summer Term 2016
# Overview of Topics

<table>
<thead>
<tr>
<th>#</th>
<th>Title</th>
<th>Advisor</th>
<th>Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Stay off my cloud! Security and privacy implications of cache attacks and their countermeasures</td>
<td>Shaza Zeitouni, David Gens</td>
<td>en / de</td>
</tr>
<tr>
<td>2</td>
<td>Know your entourage – investigating authentication schemes in IoT</td>
<td>Shaza Zeitouni</td>
<td>en</td>
</tr>
<tr>
<td>3</td>
<td>I know what you did last summer - Timing attacks on SGX</td>
<td>Raad Bahmani</td>
<td>en / de</td>
</tr>
<tr>
<td>4</td>
<td>I still know what you did last summer - Hiding access pattern for HW-secured DBs</td>
<td>Raad Bahmani</td>
<td>en / de</td>
</tr>
<tr>
<td>5</td>
<td>Survey of TEEs on mobile processors</td>
<td>Ghada Dessouky</td>
<td>en</td>
</tr>
<tr>
<td>6</td>
<td>RFID security attacks and countermeasures</td>
<td>Ghada Dessouky</td>
<td>en</td>
</tr>
<tr>
<td>7</td>
<td>Stuxnet and friends - Survey on industrial control system attacks</td>
<td>Ferdinand Brasser</td>
<td>en / de</td>
</tr>
<tr>
<td>8</td>
<td>“Gotta Catch ‘Em all: Advanced fuzzing methods to dynamically discover software bugs</td>
<td>Christopher Liebchen</td>
<td>en / de</td>
</tr>
<tr>
<td>9</td>
<td>Formal adversarial models of IoT devices</td>
<td>Jialin Huang</td>
<td>en</td>
</tr>
<tr>
<td>0</td>
<td>Is Your Water-proof Phone Also Hacker-proof? Run-time protection of mobile apps</td>
<td>Tommaso Frassetto</td>
<td>en</td>
</tr>
<tr>
<td>10</td>
<td>Terrorism and New Media - How Terrorists Use Social Networks</td>
<td>Verena Giraud</td>
<td>en / de</td>
</tr>
<tr>
<td>11</td>
<td>Keep your friends close and enemies even closer - Securing smart environments against malware</td>
<td>Ahmad Ibrahim</td>
<td>en</td>
</tr>
<tr>
<td>13</td>
<td>My Smart Home is my Castle - The Pitfalls of Smart Home Security in the Era of IoT</td>
<td>Markus Miettinen</td>
<td>en / de</td>
</tr>
</tbody>
</table>
Procedure of Topic Selection

DEADLINE: 05.05.2016, 23:55

- Every participant writes an e-mail to markus.miettinen@trust.tu-darmstadt.de with the Subject Mobile Security Seminar 2016

- Your e-mail should include up to 3 topics listed after priority (first listed topic is your most preferred topic)

- You can also propose a new topic

- If we haven’t received any e-mail from you until 05.05.2015, 23:55, we will assign the next free topic to you

- Assigned topics will be notified within 1-2 days

- Remember to register for the seminar also in TUCAN!
What We Expect

- Self-Motivated and Reliable Students
  - You have to contact your advisor, not vice versa

- Your seminar work consists of two parts
  - Writing a paper (70% of end grade)
  - Presenting your work in an oral presentation (30% of end grade). Note that your talk and slides will be evaluated.
Fixed Deadlines

- Submission Deadline:
  
  **Friday 12.08.2016, 23:55**
  
  - Submit the final version of your seminar paper and your slides by writing an e-mail to your advisor
  - Include all source files
Fixed Deadlines

- Closing Date for cancelling the seminar is **31.05.2016**
- If you cancel your participation, please remember to do so also in the **TUCAN** system!
Oral Presentation

We will arrange one day

- Proposal: **End of August 2016**
- **All** participants have to be present

Your Presentation

- Each of you will be assigned a 20 minutes time slot
- 15 minutes are reserved for your talk, 5 minutes for discussion and questions
Proposed Schedule

- **Until 13.05.2016**
  - Contact your advisor and arrange an appointment. Your advisor will introduce you into the topic and will provide you the basic literature

- **Until 01.06.2015**
  - Read the provided literature, search for additional literature
  - Agree with your advisor on the basic structure of your seminar paper
Proposed Schedule

- **Until 30.06.2015**
  - Provide a first draft of your seminar work structure to your advisor for feedback and suggestions

- **Until 29.07.2016**
  - Provide a first draft of your presentation to your advisor for proof-reading
  - In parallel, improve your paper constantly

- **DEADLINE: 12.08.2016 23:55:00**
  - Submit the final version of your work (paper, slides, other) to your advisor
Organizational Matters

- **Homepage**

- **Submission Format of Seminar Paper**
  - We will provide a latex template on the homepage
  - Your text should be at most 12 pages excluding references and appendices, and at most 15 pages in total
Organizational Matters

- **Submission Format of Presentation**
  - Your are free to use PowerPoint, Latex, Flash, ...

- **Language**
  - English or German
  - Our recommendation: Use the opportunity to write a scientific text in English
Presentation of topics
Supervisors: Shaza Zeitouni and David Gens

STAY OFF MY CLOUD!
SECURITY AND PRIVACY IMPLICATIONS OF CACHE ATTACKS AND THEIR COUNTERMEASURES
What are Cache-based attacks?

Cache attacks exploit the fact that secure and insecure processes can interact through their shared use of the cache. This allows an attacker to craft a “spy” process that can infer about the internal state of a secure process. Results: recover cryptographic keys, violate users' privacy, or even allow one virtual machine to compromise another virtual machine running on the same host.
Where?

Cloud Computing environments: take advantage of running multiple virtual machines simultaneously at the same infrastructure to leak secret information about some running encryption algorithm

Embedded devices: violate users’ privacy and interfere secure transactions
Goal

- Review, understand, and summarize different recent attack strategies against cloud providers, encryption software, and randomization defenses
- Identify common weaknesses of the underlying architectures down to the micro-architectural level, which allow an attacker to leverage caches for exploitation in the respective scenario
- Explore already-proposed defences
Requirements

- Interest in micro-architectural details of modern computing platforms
- Ability to form an accurate, thorough understanding of highly complex hardware systems
- self-guided, highly motivated work, and **critical** work
KNOW YOUR ENTOURAGE – INVESTIGATING AUTHENTICATION SCHEMES IN IOT

Supervisor: Shaza Zeitouni
Supervisor: Raad Bahmani

I KNOW WHAT YOU DID LAST SUMMER - TIMING ATTACKS ON SGX
Supervisor: Raad Bahmani

I STILL KNOW WHAT YOU DID LAST SUMMER - HIDING ACCESS PATTERN FOR HW-SECURED DBS
CAN WE RELY ON THE TRUST IN MOBILE TEEs?

Supervisor: Ghada Dessouky
Can We Rely on the Trust in Mobile TEEs?

What are TEEs exactly?

- **Trusted Execution Environments (TEEs)** is an isolated processing environment which enables isolated execution of security-critical code and secure storage of security-critical data.
Can We Rely on the Trust in Mobile TEEs?

What Can You Do?

- Different definitions of what makes a TEE, measurement of the trust, level of security required for an environment to be trusted
- Building blocks and features of TEEs
- Overview and comparison of industrial and/or academic TEEs or focus on a selected one or two (e.g., ARM TrustZone or Intel SGX)
- Threat model?
- Limitations of what currently available TEEs offer
Supervisor: Ghada Dessouky

RFID SECURITY ATTACKS AND COUNTERMEASURES
Mobile RFID: Stay Away From My Tag!

Motivation

- Mechanism to identify RFID tagged objects, using RF signals (no direct contact)
- Mobile RFID devices: your mobile phone can become also a reader
- Applications: human authentication, mobile payment, parking services, airport, etc.
**Mobile RFID: Stay Away From My Tag!**

What Can You Do?

- **Study of RFID mechanisms**
- **What makes a mobile RFID network?**
- **Privacy and security problems:** different attacks possible
- **Proposed schemes:** analysis, comparison, and their shortcomings
Supervisor: Ferdinand Brasser

STUXNET AND FRIENDS - SURVEY ON INDUSTRIAL CONTROL SYSTEM ATTACKS
“GOTTA CATCH ‘EM ALL: ADVANCED FUZZING METHODS TO DYNAMICALLY DISCOVER SOFTWARE BUGS”

Supervisor: Christopher Liebchen
Applications contain bugs – some of which can even be exploited by attackers to compromise the system.

Manual code audits or reverse engineering can be applied to find such bugs (time consuming).

Fuzzing is one method to automatically discover such bugs.

However, fuzzing usually catches only very simple and shallow bugs.

Task: summarize the recent advances of fuzzing.
FORMAL ADVERSARIAL MODELS OF IOT DEVICES

Supervisor: Jialin Huang
IS YOUR WATER-PROOF PHONE ALSO HACKER-PROOF? RUN-TIME PROTECTION OF MOBILE APPS
Recent (2015) Android Run-time Exploits

- Stagefright bug: vulnerable multimedia library • ~950M devices affected
- One Class to Rule Them All: deserialization vulnerabilities
  • ~55% of devices affected
Modern Run-Time Exploits

• Before DEP: code injection possible

• DEP (Data Execution Prevention): memory pages are either executable or writable • thus, injected code cannot be executed

• ROP (Return Oriented Programming) re-uses blocks of legitimate code in malicious ways
Mitigation Strategies

• CFI (Control Flow Integrity) • Idea: ensure that control flow is consistent with the source code • MoCFI, Davi et al.

• Randomization + XoM (Execute Only Memory) • Idea: randomize code and prevent attackers from finding the code to re-use • LR2, Braden et al.
Work Outline

• Read these papers and related works
  • Davi et al., MoCFI: A Framework to Mitigate Control-Flow Attacks on Smartphones, NDSS 2012
  • Braden et al., Leakage-Resilient Layout Randomization for Mobile Devices, NDSS 2016
• Prepare a critical report on advantages and disadvantages of the two approaches on the current mobile platforms
Supervisor: Verena Giraud

TERRORISM AND NEW MEDIA - HOW TERRORISTS USE SOCIAL NETWORKS
Terrorism and New Media
How Terrorists Use Social Networks

Social Networks are very popular for extremist propaganda and recruitment purposes.

They allow interactive, unfiltered and permanent targeting strategies to reach sympathizers.

This has become an ongoing, unsolved problem for platforms like Facebook or Twitter.

The security community needs to develop new tools & approaches to respond to this problem.
Terrorism and New Media
How Terrorists Use Social Networks

Objective: To examine why social networks like Facebook or Twitter are appealing to extremists for communication and propaganda and how they use Social Networks for these purposes

Goal: Understanding the use of social networks through extremists, examine and compare counter-strategies of providers and ultimately propose alternative approaches
Terrorism and New Media
How Terrorists Use Social Networks

Research (in English) will be provided, additional papers and literature can also be used.

Report can be written in English or German.

Target: To examine the proposed objective based on the provided literature and to propose a counter-strategy for users and/or providers.

Interested? Please contact verena.giraud@trust.cased.de for further information.
Supervisor: Ahmad Ibrahim

KEEP YOUR FRIENDS CLOSE AND ENEMIES EVEN CLOSER - SECURING SMART ENVIRONMENTS AGAINST MALWARE
Smart Environment: Building Automation

Various cyberphysical systems (CPS):

- **Air conditioning**
  Heating, temperature sensors, ...

- **Fire alarm system**
  Smoke detectors, sprinklers, ...

- **Access control system**
  Card readers, burglar alarm, ...

- **Energy management**
  Smart meters, solar panels, ...

- **Decentralized management**
  Smartphones, tablets, ...

Authenticity of all CPS is crucial for reliability, safety and security of whole system

Many different wirelessly connected CPS sharing resources

*E.g.*, CPS monitoring windows used by air conditioning and alarm system
Networks of Embedded Devices

(Large) heterogeneous networks of embedded systems

Networks of embedded devices in critical infrastructures

Network of automotive controllers

Network of smart devices
Networks of Embedded Devices (cont’d)

Drones
Video surveillance, environment monitoring

Robot swarms
Many CPS collaborate to perform tasks

Smart factories
Collaborating cyberphysical systems (CPS)

Automotive systems
Car2X systems, VANETs
Attestation

Network

Verifier (trusted)

Software attacks e.g., malware

challenge
response

Device $D_1$

Device $D_2$

Device $D_3$

Device $D_4$

Device $D_5$

Device $D_6$

Device $D_7$
Supervisor: Markus Miettinen

I SEE YOU HAVE BEEN WORKING OUT – REALLY?
Problem setting

Fitness trackers are gaining huge popularity recently
Capability to build a detailed picture of the user’s activity
Some insurance companies offer benefits for users who regularly exercise and lead a healthy life
Two risk scenarios emerge:
  • Unauthorized data leakage leading to compromise of user privacy
  • Malicious modification of tracking data for financial benefits
Goal

Familiarize yourself with relevant literature related to the protection of the confidentiality and integrity of data on fitness trackers and other wearable devices.

What are the threats? What vulnerabilities exist? What countermeasures have been proposed?
MY SMART HOME IS MY CASTLE - THE PITFALLS OF SMART HOME SECURITY IN THE ERA OF IOT

Supervisor: Markus Miettinen
Problem setting

With the emergence of IoT, many regular household appliances are connected to IP-based networks.

There are hundreds if not thousands IoT device vendors, many of these do not have expertise in computer security nor engineering.

This results in badly designed and engineered devices with many security vulnerabilities.
Goal

Investigate the security problems in the IoT space

What are typical threats?

What implications do constraints in the hardware capabilities impose on security?

What security architectures have been proposed for IoT systems?
Time for questions!

THANK YOU FOR YOUR ATTENTION!