Systems Hardening
Premeeting - WS 2021/22 - Season III

Marius Momeu$^1$  Sergej Proskurin$^{1,2}$

$^1$Chair of IT Security, Department of Informatics, Technical University of Munich (TUM)

$^2$BedRock Systems

September 20, 2021
Intro

Your tutors

- Marius Momeu¹ (momeu@sec.in.tum.de)

¹I’m posting theses / guided research topics at: https://www.sec.in.tum.de/i20/people/momeu-marius
Intro

Your tutors

- Marius Momeu\(^1\) (momeu@sec.in.tum.de)
- Sergej Proskurin (proskurin@sec.in.tum.de)

\(^1\)I'm posting theses / guided research topics at: [https://www.sec.in.tum.de/i20/people/momeu-marius](https://www.sec.in.tum.de/i20/people/momeu-marius)
Objectives

This seminar is structured to train you for publishing research at scientific conferences or journals.

Consequently, you will exercise and expand a broad spectrum of research skills, such as formulating a clear and novel hypothesis, validating it, and, most importantly, presenting and writing about your findings.

For that, your tutors will pick state-of-the-art mechanisms or infamous issues in the area of systems hardening, and define problem statements to address their limitations. These will then get assigned to you, and you will have to provide a design, prototype, and evaluation for your assigned topic.²

Finally, you will write a paper based on the results that you obtain, and present your findings at the end of the semester.

²you may also propose your own topic
Content

We are generally interested in mechanisms that improve the security of (low-level) software running in applications, systems, or infrastructures.

As such, the following pool captures some high-level systems hardening areas we will pick topics from:

• CPU extensions (*Intel VT-x/MPK/CET/HLAT*, *ARM PAC/MTE*) for hardening OS applications, kernels, unikernels, \( \mu \)kernels
  – via code/data isolation, control-flow integrity, data integrity
• Fuzzing low-level software (e.g., OS kernels, device drivers, and hypervisors)
• Static program analysis (especially focusing on large stateful software s.a. OS kernels, device drivers, and hypervisors)
• Microarchitectural flaws and side-channels for leaking secrets, revealing stealthy monitors, etc.
• Security analysis and exploitation of hardware extensions (e.g., *AMD-SEV-*\(^*\), *Intel CET/MKTME*)
• Heap hardening against use-after-free vulnerabilities
• Confidential/Trusted computing via Trusted Execution Environments: *Intel SGX/MKTME/TXT, ARM TrustZone, AMD-SEV-*\(^*\)
• Live patching
Hands-On

Throughout this seminar, you should expect to touch on the following, including but not limited to:

- Operating machines remotely via the command-line terminal (bash on Unix systems)
- Coding in C/C++, Assembly (x86, ARM), (maybe) Rust, various scripting languages
- OS concepts, such as memory management (via paging or nested-paging\(^3\)), interrupts, (bare-metal and emulated) device drivers, syscalls/hypercalls
- LLVM’s static analysis framework
- Examining various hardware extensions in architecture manuals (Intel VT-x/MPK/CET/HLAT, ARM PAC/MTE, AMD-SEV-* )
- Computer architecture concepts (e.g., speculative execution, return stack buffers, caches, TLBs)
- Dissecting the layout and risks of heap allocators
- Exploitation know-how: code-reuse attacks, data-oriented attacks, secret leaking via covert side-channels
- Compiling/building, dynamic or static linking, binary formats (mostly ELF)
- System administration (e.g., spawning VMs, managing partitions)

\(^3\) via PTs and EPTs on Intel’s architecture
Tentative Timeline | Deliverables

- Research exposé
  - motivation
  - research goals
  - roadmap
- First paper draft
  - introduction
  - technical background
  - threat model
  - related work
- Final paper draft
  - design
  - implementation
  - evaluation
  - limitations
  - ...
- Camera-ready version
- Draft slides for the final presentation
- Peer review

- Students send shortlist of 3 preferred topics
- Tutors publish catalogue of topics
- Tutors assign topics to students
- Our feedback on your first draft
- Our feedback on your final draft
- Our feedback on your slides

Deliverables
- 27.09
- 04/05.10
- 26.10
- 16.11
- 23.11
- 04.01
- 11.01
- 25.01
- 01.02
- 04.02
Tentative Timeline | Sessions

- Research exposé
  - motivation
  - research goals
  - roadmap

- First paper draft
  - introduction
  - technical background
  - threat model
  - related work

- Final paper draft
  - design
  - implementation
  - evaluation
  - limitations
  - ...

- Camera-ready version

- Draft slides for the final presentation

- Final talks

Deliverables

- Students send shortlist of 3 preferred topics

- Tutors publish catalogue of topics

- Tutors assign topics to students

- Task for Students

- Task for Tutors

- Hints on Scientific Writing

- System design presentations

- System implementation & evaluation presentations

- Our feedback on your first draft

- Peer review

- Our feedback on your final draft

- Our feedback on your slides
Tentative Timeline

- Research exposé presentations - motivation - research goals - roadmap
- System design presentations
- System implementation & evaluation presentations
- First paper draft - introduction - technical background - threat model - related work
- Final paper draft - design - implementation - evaluation - limitations - ...

Deliverables
- Students send shortlist of 3 preferred topics
- Tutors publish catalogue of topics
- Tutors assign topics to students
- Task for Students
- Task for Tutors

Sessions
- 27.09
- 04/05.10
- 19.10
- 26.10
- 16.11
- 23.11
- 21.12
- 04.01
- 11.01
- 25.01
- 01.02
- 04.02
- 12.02

Hins on Scientific Writing
- Hints on Paper Reviewing & Hints on Public Speaking
- Our feedback on your first draft
- Peer review
- Camera-ready version
- Draft slides for the final presentation
- Our feedback on your slides
- Final talks

Optimization and evaluation
- Prototype implementation and evaluation

Read related literature & setup prototyping environment
- Sketch design

Task for Students

Task for Tutors
Grading

**Graded** deliverables:
- Camera-ready presentation
- Final presentation
- Prototype / design / experiments

**Mandatory ungraded** deliverables:
- Paper proposal
- Paper drafts
- Intermediate presentations
- Peer review

**Optional** deliverables:
- Draft for the final presentation

50 % Final Paper (Content, Style, Language, Scope, . . .)  
40 % Final Talk (Presentation and Q&A)  
10 % Design / Prototype / Experiments  

Σ 100 % Final Grade
Deliverables Format

**Paper proposal:**
- 2-3 pages
- one-column
- **note:** the focus should be on motivation of the topic assigned to you and your research goals in this seminar

**Presentation:**
- TUM presentation template
- custom templates can be used as well
- 16:9 aspect ratio if held online, 4:3 if held with beamer

**Paper:**
- IEEE conference proceedings template
- maximum 10 pages, excluding References and Appendix
- two-column

**Peer review:**
- format similar to peer reviews in scientific conferences
- one page with summary, strengths, and weaknesses of reviewed paper

Generally, we encourage you to use **\LaTeX** for writing.

---

4 https://www.ieee.org/conferences/publishing/templates.html
5 https://latex.tum.de/templates/608c2650db4bc7007f58c931
Orga

**When?** irregularly, on Tuesdays, at 10:00 h (subject to change)

**Where?** Onsite (possible with 3G!), online (via BBB), or hybrid

**Capacity:** 10 students

**Language:** English

**Course of study:** both Master’s and Bachelor’s students

**Registration:** via the matching system
Seminar Resources

We will setup a Moodle\(^6\) page for announcements, for submitting deliverables, and for uploading lecture slides.

We will create Gitlab\(^7\) repositories on LRZ’s git server for versioning the paper’s and prototype’s source code.

Depending on the topic, we can configure accounts for you in our chair’s test network and let you access our hardware for prototyping.

Matrix\(^8\) for instantaneous communication.

\(^6\)https://www.moodle.tum.de/
\(^7\)https://gitlab.lrz.de/
\(^8\)https://matrix.tum.de/
Task for Matching Prioritization

Please send us a letter of motivation of maximum 2 pages stating up to 3 mechanisms / hardware technologies / software components from slide 3 that you would like to work on during the seminar. In your letter, describe why do you want to work with these and why do you find them important for systems security?

Send it to: momeu@sec.in.tum.de and proskurin@sec.in.tum.de
In your email, use the subject: Matching - Systems Hardening - WS 2021

Deadline: Sunday, 25th of July

Also, please mention in your report if you have attended any of the following courses:

- Rootkit Praktikum, Binary Exploitation
- Software Security Analysis, Trusted Execution Environment, Reverse Engineering
- IT Security, Secure Mobile Systems
- Computer Architecture, Operating Systems
- Any other course where you have tackled the topics / technologies we have mentioned above
Questions?

Marius Momeu
momeu@sec.in.tum.de
@MariusMomeu

Sergej Proskurin
proskurin@sec.in.tum.de