Chair of IT Security
Department of Informatics
Technical University of Munich

Systems Hardening

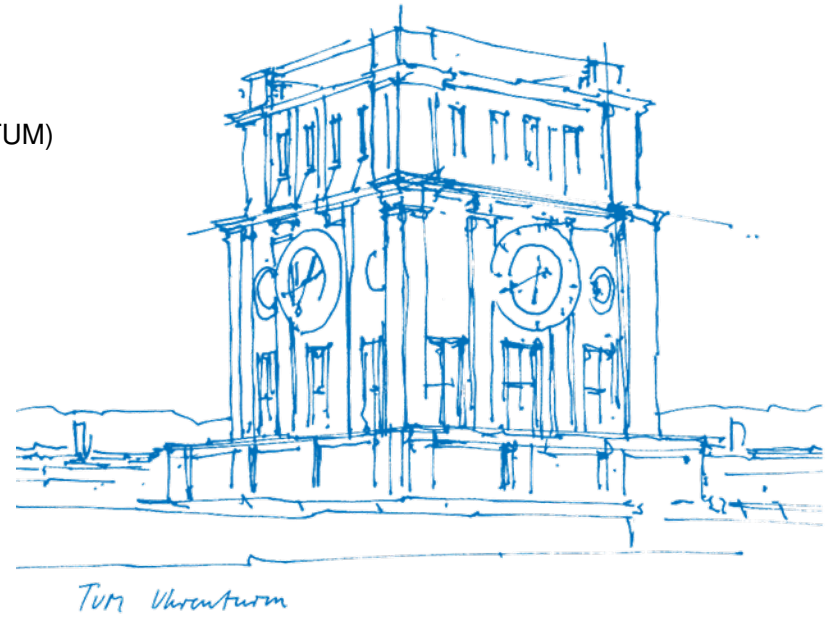
Preliminary Meeting - SS 2022 - Season IV

Marius Momeu[1] Sergej Proskurin[1,2]

[1]Chair of IT Security, Department of Informatics, Technical University of Munich (TUM)

[2]BedRock Systems

January 28, 2022



Chair of IT Security
Department of Informatics
Technical University of Munich

Intro

Your tutors:

- Marius Momeu[1] (momeu@sec.in.tum.de)

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

Chair of IT Security
Department of Informatics
Technical University of Munich

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

Objectives

This seminar is structured **for preparing you** to publish research at scientific conferences or journals.

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

To facilitate that, your tutors will propose state-of-the-art offensive and defensive topics in systems hardening research.

There will generally be two types of topics you can choose from[2]:

- **Prototyping topics** that require building and evaluating a prototype for limitations in existing research, and
- **SoK topics** require systemizing the knowledge on a popular concept/issue with lots of existing research.

Finally, you will gradually **build a paper** on the obtained results, and you will **present your findings** throughout the semester.

[2] you are welcome to propose a topic of your own

Chair of IT Security
Department of Informatics
Technical University of Munich

Scientific Content

We are generally interested in researching ways to improve the security of software running in **IoT devices, cloud servers, and desktop environments.**

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

- **Hardware security extensions**
  - such as *Intel VT-x/MPK/CET/HLAT* and *ARM PAC/MTE*
  - for hardening OS kernels, unikernels, μkernels
  - via code/data isolation, control-flow and data-flow integrity
- **Static program analysis**
  - for generating Control-Flow and Data-Flow policies
  - on closed- and open-source software (OS kernel and applications)
- **Confidential computing in Trusted Execution Environments (TEEs)**
  - such as *ARM TrustZone, Intel SGX/MKTME/TXT, AMD-SEV-**
  - both their security benefits and shortcomings
- **Remote (control-flow and data-flow) attestation**
- **Fuzzing low-level software** (e.g., OS kernels, device drivers, and hypervisors)
- **Microarchitectural flaws** and side-channels for leaking secrets, revealing stealthy monitors, etc.

Hands-On Format

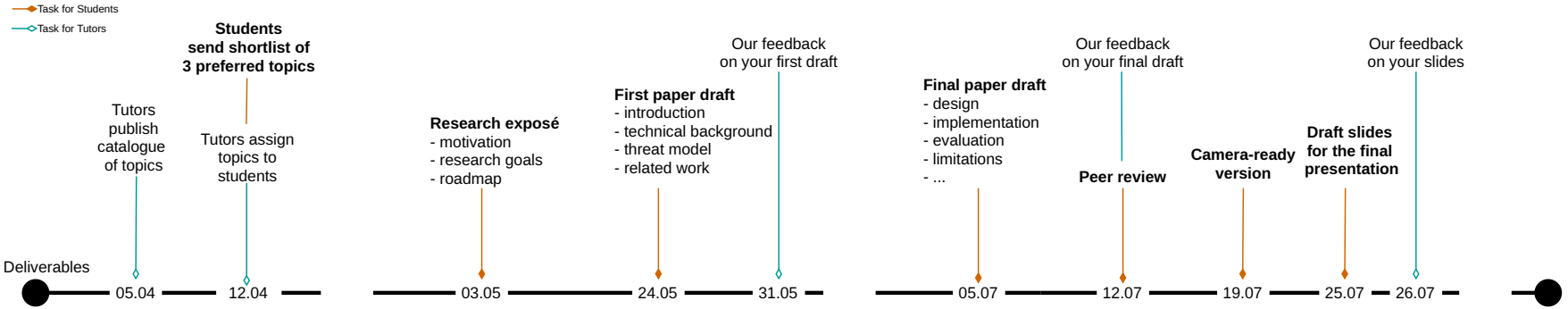
Throughout this seminar you should expect to touch on hands-on stuff, including but not limited to:

- Remotely operating servers or IoT devices via the command-line terminal (bash on Unix systems)
- Reading and coding in *C/C++*, Assembly (*x86, ARM*), (maybe) *Rust*, and various scripting languages
- Understanding OS concepts, such as memory management (via paging or nested-paging[3]), interrupts, (bare-metal and emulated) device drivers, syscalls/hypercalls
- Using *LLVM*'s static analysis framework and *LLVM* binary lifters
- 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*)
- 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, compiling and deploying kernels/unikernels)

[3] via *PTs* and *EPTs* on Intel's architecture

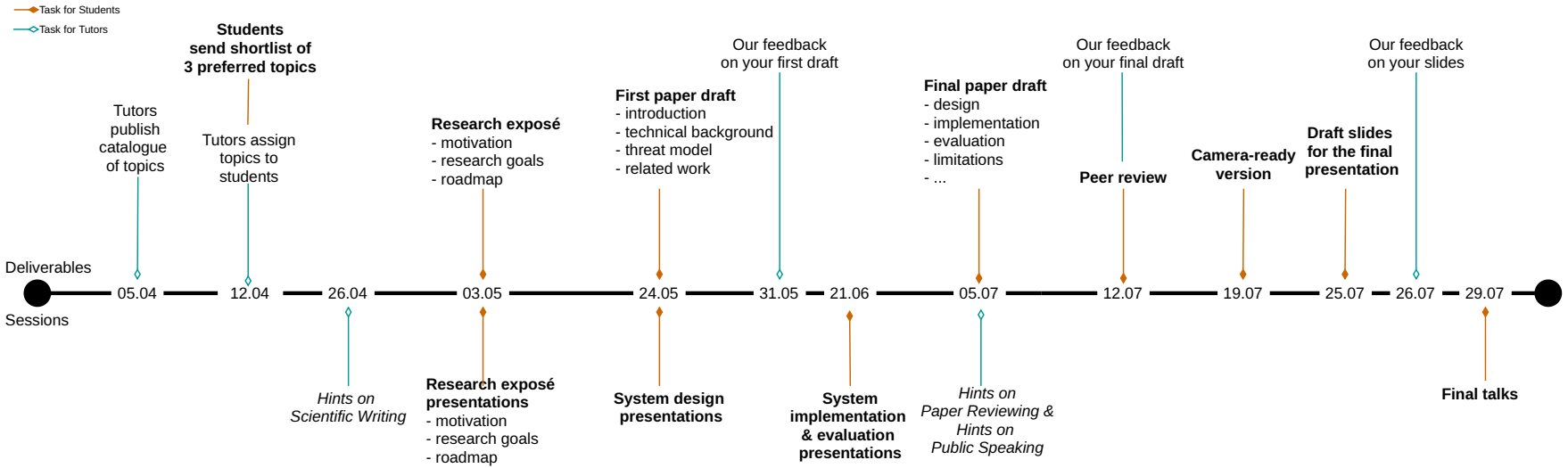
Chair of IT Security
Department of Informatics
Technical University of Munich

Tentative Timeline | Deliverables



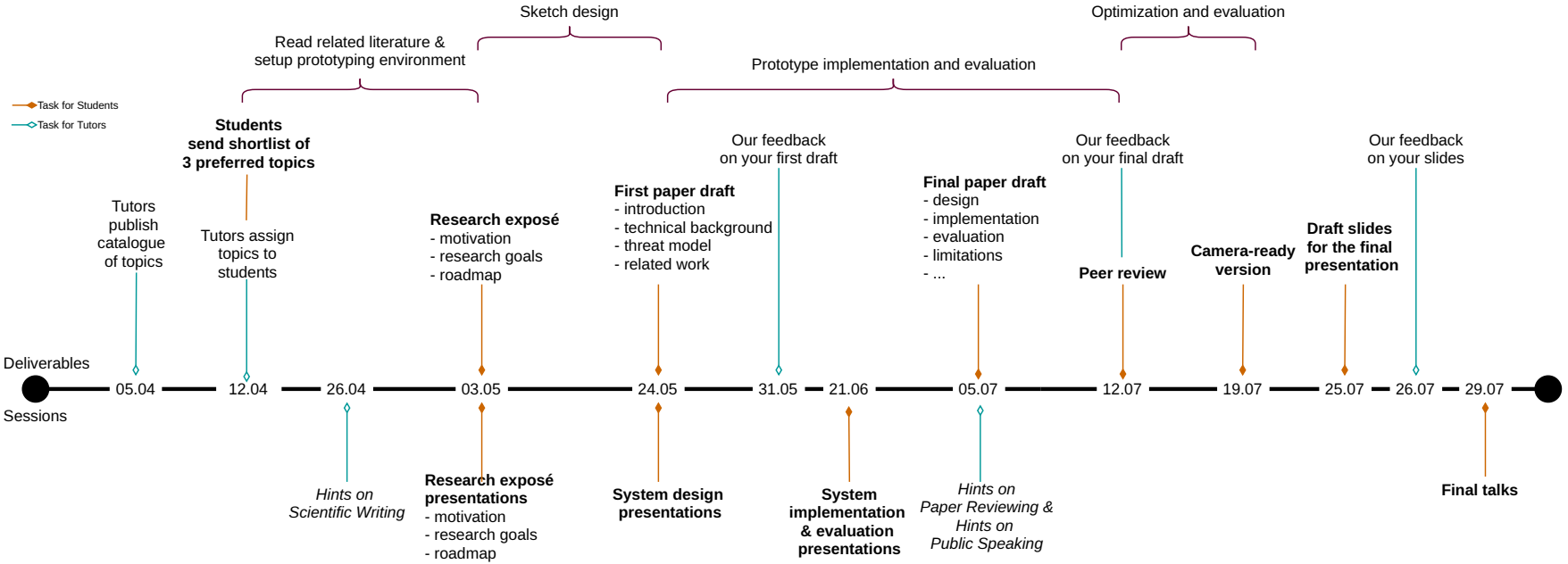
Chair of IT Security
Department of Informatics
Technical University of Munich

Tentative Timeline | Sessions



Chair of IT Security
Department of Informatics
Technical University of Munich

Tentative Timeline



Chair of IT Security
Department of Informatics
Technical University of Munich

Grading

Graded deliverables:

- Final "camera-ready" paper
- Final presentation
- Design/ prototype / experiments

Mandatory ungraded deliverables:

- Research exposé
- 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

Chair of IT Security
Department of Informatics
Technical University of Munich

Deliverables' Format

Research exposé:

- 2-3 pages
- one-column
- **note:** focus on the motivation for your topic and on the research goals that you will address in this seminar

Presentation:

- TUM presentation template[5]
- custom templates can be used as well
- 16:9 aspect ratio

Generally, we encourage you to use LaTeX for writing.

Paper:

- IEEE conference proceedings template[4]
- 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

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

Chair of IT Security
Department of Informatics
Technical University of Munich

Orga

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

Where? Onsite or online (via BBB) depending on the regulations

Capacity: 8 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/

Chair of IT Security
Department of Informatics
Technical University of Munich

Task for Matching Prioritization

Please send us a **letter of motivation of maximum two pages** stating **up to 3 topic areas** from slide *Scientific Content* 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 - SS 2022*

Deadline: Sunday, 20th of February, EoD

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