Seminar Cyber-Resilient Systems

Lukas Gehrke

Feb 8th, 2024
Resilience

“the ability to be happy, successful, etc. again after something difficult or bad has happened”

“the ability of a substance to return to its usual shape after being bent, stretched, or pressed”

“the quality of being able to return quickly to a previous good condition after problems”
Cyber Resilience

The ability to **anticipate**, **withstand**, **recover** from, and **adapt** to…

…adverse conditions, stresses, attacks, or compromises…

on systems that use or are enabled by cyber resources.
The fundamental assumption is that cyber resilience (defined as on slide 4) is a general concept or approach towards making computer systems more secure and reliable.

Starting from that, we are asking ourselves:

„How and to what degree is the concept of cyber resilience present and being applied in academia?“

With this question in mind, we formulate your individual research topics as sub-topics of CR (next slide)
Sub-Topics of Cyber Resilience to investigate

Cyber-Resilient…
- System or Software Engineering
- System Design or Architecture
- Networking or Communication (Protocols)
- Distributed Systems (server, cloud, on-premise)
- Internet of Things (IoT, CPT)
- Virtualization (VM, container)
- Artificial Intelligence (AI)

Cyber Resilience…
- *In General* (Taxonomy, Survey, Model, Assessment Framework, Metric)
- In the public sector (states, infrastructure, (smart) city)
- In the industry (companies, (smart) factory, service providers)

Example: „*Cyber-Resilient Internet of Things*“
Objectives

The seminar aims at teaching you **how to do academic search** and **present your results** (written and spoken).

In more detail, we utilize the topic **cyber resilience** to practise

1. **doing literature search** on pre-selected sub-topics and **summarizing the results** by,
2. **writing a short paper** in a systemization of knowledge (SoK) style (10 pages),
3. **and giving a talk** of 30 minutes with 10-15 minutes of discussion.

To give you something to start with, the seminar includes

1. a brief **introduction to cyber resilience**,
2. as well as general **hints about literature research, scientific writing and presentations**.
Tentative Timeline

- **Feb 08**: In person
  - Pre-meeting, you become familiar with content and learning goals, can ask questions

- **Feb 23**: Online
  - Seminar matching results and final topics are announced

- **Apr 18**: In person
  - Seminar kick-off, introduction to Cyber Resilience, Scientific search, writing, feedback on literature search results

- **May 02**: In person
  - Individual feedback on your paper draft

- **May 30**: Personal
  - You submit the paper in moodle until 23:59 CET

- **Jun 30**: Online
  - You submit the paper in moodle until 23:59 CET

- **Jul 4**: In person
  - Your talks and discussions with the others

If accepted, you **send three ordered topic preferences** until Feb 25, 23:59 CET by e-mail, Your topic matchings will be published shortly.

Do academic search and submit list of references in moodle by Apr 30, 23:59 CET.

Further search and writing, submit paper draft in moodle by May 21, 23:59 CET.

Finish your paper, submit paper in moodle on Jun 30 by 23:59 CET.

Finish work on presentations, upload your presentation in moodle on Jul 2 by 23:59 CET.
Further Organizational Matter (tentative)

**Time:** (tentative) Thursdays 10:00 a.m. ~ 12:00 a.m. (final presentations: 45 min x number of presenters)

**Room:** 01.08.033

**Capacity:** Seven students

**Language:** English

**Target Group:** Master's and bachelor's students welcome; important is that you are interested in the topic and doing SoK research

**Your presence at in-person meetings is mandatory.**
Deliverable Requirements

Intermediate
• Draft 1: Results of literature search, ideally as table, describe your findings
• Draft 2: 80% ready paper draft with list of references for feedback, optionally also your presentation draft
• Optional, individual feedback sessions in person

Presentation
• 30 min talk and 10 to 15 min discussion
• Please use the TUM 16:9 template (PowerPoint, LaTeX)

Report
• (Exactly) ten pages, two-column style (excluding references and appendix)
• Please use the IEEE template (https://www.ieee.org/conferences/publishing/templates.html)
• You are encouraged to use LaTeX
Requirements for Passing and Grading

Please take a look at what the terms of your degree program state about written assignments and oral presentations. („Prüfungsordnung“)

Grading will be:
50% Paper (e.g. structure, writing style, literature research results, grammar and spelling mistakes)
40% Presentation (e.g. presentation quality, usage of media, explanation)
10% Discussion (e.g. reaction to questions and comments of the audience)
So, you would like to participate?

For matching prioritization, send me a letter of motivation (500 words max.) where you state why you would like to participate and what interests you in cyber resilience to gehrke@sec.in.tum.de. If you have your own topic suggestion, feel free to include it.

Please also briefly state your prior experience with IT security.

Set as subject: „Seminar CRS Matching“. Deadline: February 15th, 2024 by 23:59 CET.
Thank you for attending!

Are there any questions?

More info: https://www.sec.in.tum.de/i20/teaching/ss-2024/cyber-resilient-systems