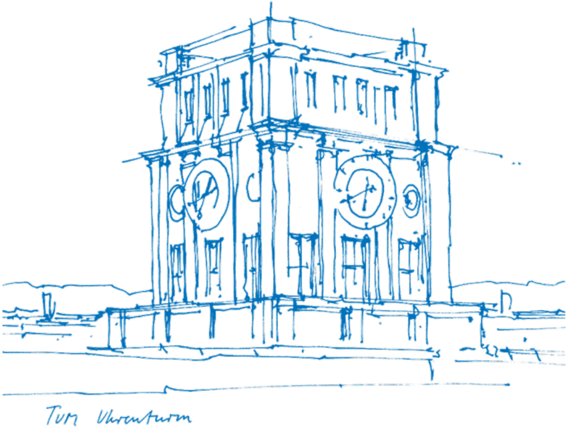
Chair of IT Security
School of Computation, Information, and Technology
Technical University of Munich

Seminar Secure Software Supply Chains

Pre-meeting



Lukas Gehrke

Chair of IT Security
School of Computation, Information, and Technology
Technical University of Munich

February 4th, 2025

Some questions first

- What is a library or package?
- Why do we do this in computer science?
- What could be the problem?

Some more questions

- What is a software bug?
- What is a vulnerability?
- What is an exploit?

Outline

1 Seminar overview

2 Software supply chain security

3 Example Topics

4 The organizational side

Seminar overview

What you can expect

- The seminar is for you to learn and practice academic working (hard skills)
  - Therefore, you will be provided with an introduction to *literature search, writing and presenting*
- The topic is secure software supply chains
  - This is a relatively *broad topic* and leaves you room to pick your individual topic depending on your skills, interests and prior knowledge
- The topic is closely related to my research
  - So I can supervise you on the topic and give you background knowledge

Outline

1 Seminar overview

2 Software supply chain security

3 Example Topics

4 The organizational side

Software supply chain security

Topic overview

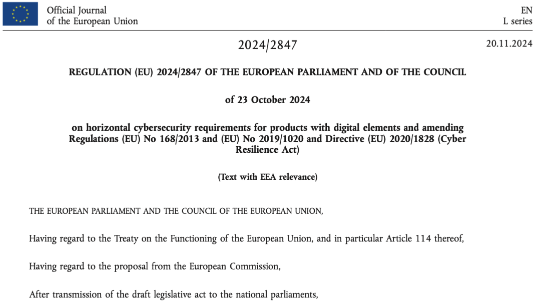
- Have you heard of the xz-utils incident?
- This attack was conducted over years, including significant technical as well as operational and even social sophistication (in a negative sense..)
- If not detected rapidly, billions of Linux devices worldwide would have allowed unauthorized **remote access as root**
- How many other attacks like this are there and are yet unknown?

Figure 1 Logo for xz utils created by the malware author with username *Jia Tan*

Software supply chain security

Topic Overview

- The *Cyber Resilience Act* was ratified by the EU in 2024
  - Its demands have to be implemented by vendors within 3 years
- All products with digital elements have to include software bills of materials "SBOMs"
  - The goal is that once a vulnerability is detected, every affected product can be identified and notified quickly



Official Journal
of the European Union

EN
L series

2024/2847

20.11.2024

REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 23 October 2024

on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Figure 2 Excerpt from the Cyber Resilience Act

Research Questions

- How are vulnerabilities and exploits detected?
- How are they communicated?
- How can exploitability of affected software be checked *automatically*?

Outline

1 Seminar overview

2 Software supply chain security

3 Example Topics

4 The organizational side

Example Topic Dummy

- Category: What *kind of* working will you most likely focus on? - survey or collection, statistical analysis, implementation
- Research Question: What question will you try to answer?
- Expected Contribution: Some remarks about what could be your deliverable
- Keywords: A few keywords that may be worth starting literature search with
- Resources: Works that are essential starting points for working on this topic

This is not exhaustive and will be subject to change, especially after the first literature search, where me might re-adjust the scope

Vulnerability Reporting and Communication in Open Source

- Category: Survey, analysis
- Research Question: How does exchange about vulnerabilities work in the open source community? (certain communities)
- Expected Contribution:
  - Overview and analysis,
  - Selection of academic works as well as OSS documentation
  - Assessment of existing tools and standards
  - Potential statistical analysis with creating a dataset
  - Derive a conclusion about how Vulnerability Reporting works and
- Keywords: vulnerability reporting open source, CVE, OpenVAS, OSV
- Resources: Imtiaz et al., 2021, Pashchenko et al., 2020, Ladisa et al., 2022

SBOMs and their alternatives

- Category: Survey, analysis
- Research Question: What goal do SBOMs try to achieve what alternatives exist to do so?
- Expected Contribution:
  - □ Overview and analysis,
  - □ Selection of academic works as well as standards or frameworks
  - □ Assessment of existing tools and standards as well as their comparison
  - □ Identify open problems, recommendations for tool selection
- Keywords: SBOMs, BSI CSAF, ...
- Resources: Stalnaker et al., 2024, BSI CSAF, CISA on SBOMs, Ladisa et al., 2022

SBOMs in the Python ecosystem

- Category: Analysis, implementation
- Research Question: What is the state of work of SBOM creation in the Python ecosystem?
- Expected Contribution:
  - □ Overview of other works on SBOM creation in the Python ecosystem,
  - □ Implement a setup where you create SBOMs for a set of repos using different tools and standards
  - □ Analysis of SBOM quality using selected metrics
  - □ Derive a judgement about SBOM quality in the Python ecosystem, tool or standard recommendations
- Keywords: SBOMs, Python SBOMs
- Resources: Cofano et al., 2024 ,Benedetti et al., 2024, Yu et al., 2024

We could do the same on another ecosystem, like JS/Node

Security of security patches

- Category: Survey
- Research Question: How are security patches carried out, implemented and *secured*?
- Expected Contribution:
  - Overview of the basics of how security patches or updates for software are rolled-out to its users,
  - Analysis of different patching approaches and security risks
  - Derive open problems, security recommendations
- Keywords: security patch management, patching
- Resources: Li and Paxson, 2017 and works building on top of it

The attacker’s perspective

- Category: Survey, analysis, maybe dataset creation, meta science
- Research Question: How is the state of research about taking the attacker’s perspective?
- Expected Contribution: Overview about thread modelling and framework used, answering the question how accurate threat models in works are, e.g. by looking at recent papers on top security conferences. Supported by information that can be found about threat actors
- Keywords: threat modelling, MITRE ATT&CK, The Killchain,
- Resources: Xiong and Lagerström, 2019 and further

Exploitability Automation (WIP)

- Category: Analysis, Implementation
- Research Question: What methods and tools exist to automate exploitability checks? (WIP: in what area? e.g. Linux Kernel, virtualization/hypervisors, user space software)
- Expected Contribution: Analysis of status quo in (WIP) area and a small evaluation or extension of existing tools
- Keywords: exploit automation or prediction, static analysis, automatic exploit generation
- Resources: Park et al., 2022 Elder et al., 2024 Lin et al., 2022

Outline

1 Seminar overview

2 Software supply chain security

3 Example Topics

4 The organizational side

Objectives

The seminar aims at teaching you how to do literature search and present your results (written and spoken). In more detail, we utilize the topic software supply chain security to practice

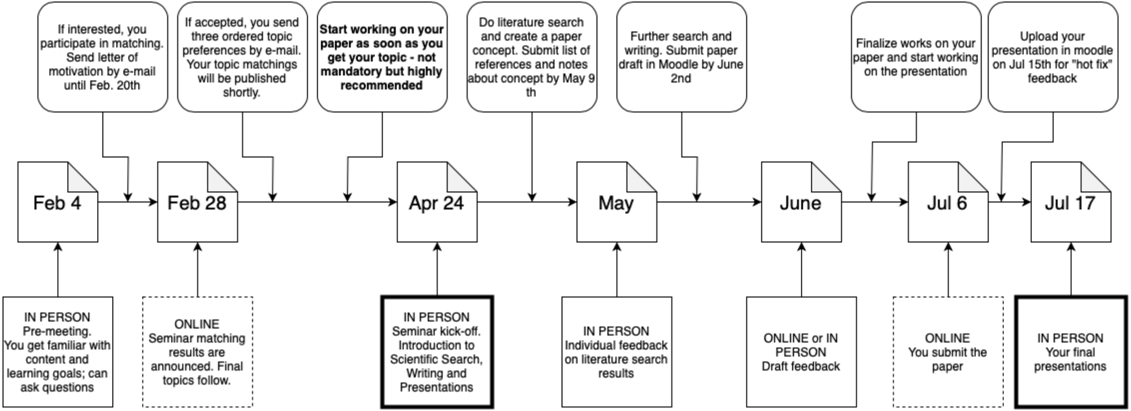
1. doing literature search on pre-selected sub-topics and summarizing the results by,
2. writing a research paper (10 pages),
3. and giving a talk of 20 minutes with 10 minutes of discussion.

To give you something to start with, the seminar includes

1. a brief introduction to software supply chain security,
2. as well as general hints about literature research, scientific writing and presentations.

Shedule

Might be subject to change



If interested, you participate in matching. Send letter of motivation by e-mail until Feb. 20th

If accepted, you send three ordered topic preferences by e-mail. Your topic matchings will be published shortly.

Start working on your paper as soon as you get your topic - not mandatory but highly recommended

Do literature search and create a paper concept. Submit list of references and notes about concept by May 9th

Further search and writing. Submit paper draft in Moodle by June 2nd

Finalize works on your paper and start working on the presentation

Upload your presentation in moodle on Jul 15th for "hot fix" feedback

Feb 4

Feb 28

Apr 24

May

June

Jul 6

Jul 17

IN PERSON
Pre-meeting. You get familiar with content and learning goals; can ask questions

ONLINE
Seminar matching results are announced. Final topics follow.

IN PERSON
Seminar kick-off. Introduction to Scientific Search, Writing and Presentations

IN PERSON
Individual feedback on literature search results

ONLINE or IN PERSON
Draft feedback

ONLINE
You submit the paper

IN PERSON
Your final presentations

Further organizational matter (tentative)

- Time: Thursdays 10:00 - 12:00 a.m. (final presentations 30 min x number of presenters)
- Room: 01.08.033
- Capacity: 8-10
- Language: English (written assignments), German for presentations if everyone is proficient
- Target Group: master's and bachelor's students who are interested in the topic
- **Your presence at the in-person meetings is mandatory.**

Deliverable requirements

Intermediate

- Literature search results: List of sources and description of findings
- Paper Draft: 60-80%-ready paper with list of references for feedback
- Optional individual feedback sessions in person, maybe peer-review (tbd.)

Presentation

- 20 min talk and 10 min discussion (tbd.)
- Use the TUM 16:9 templates[1] for slides (LaTeX or PowerPoint)

Paper

- (Exactly) ten pages, two-column style, excluding references and appendix
- Use the IEEE template[2]

[1] http://portal.mytum.de/corporatedesign

[2] https://www.ieee.org/conferences/publishing/templates.html

Grading and requirements for passing

Please take a look at what the terms of your degree program state about written assignments and oral presentations. ("Prüfungsordnung")[3]

Grading will be:

- 60% Paper (e.g. structure, writing style, presentation of results in own words, grammar and spelling mistakes)
- 30% Presentation (e.g. presentation quality, usage of media, explanation)
- 10% Discussion (e.g. reaction to questions and comments of the audience)

[3] https://www.cit.tum.de/cit/studium/studiengaenge/bachelor-informatik/

So, would you like to participate?

For matching prioritization, send me a letter of motivation (three to fifteen sentences) where you state why you would like to participate and what interests you in software supply chain security (including your preferred topic) to gehrke@sec.in.tum.de.
If you have your own topic suggestion fitting into the topic's context, feel free to include it.

Please also briefly state your prior experience with cybersecurity.

Set as subject **"Prioritization SSSC Seminar"**. Deadline: Feb. 20th, 2025 by 23:59 CET

References I

Benedetti, G., Cofano, S., Brighente, A., & Conti, M. (2024). The impact of sbom generators on vulnerability assessment in python: A comparison and a novel approach. *arXiv preprint arXiv:2409.06390*.

Cofano, S., Benedetti, G., & Dell'Amico, M. (2024). Sbom generation tools in the python ecosystem: An in-detail analysis. *arXiv preprint arXiv:2409.01214*.

Elder, S., Rahman, M. R., Fringer, G., Kapoor, K., & Williams, L. (2024). A survey on software vulnerability exploitability assessment. *ACM Computing Surveys*, *56*(8), 1–41.

Imtiaz, N., Thorn, S., & Williams, L. (2021). A comparative study of vulnerability reporting by software composition analysis tools. In *Proceedings of the 15th acm/ieee international symposium on empirical software engineering and measurement (esem)*.

References II

Ladisa, P., Plate, H., Martinez, M., & Barais, O. (2022). Taxonomy of attacks on open-source software supply chains. *arXiv preprint arXiv:2204.04008*.

Li, F., & Paxson, V. (2017). A large-scale empirical study of security patches. In *Proceedings of the 2017 acm sigsac conference on computer and communications security*.

Lin, Z., Chen, Y., Wu, Y., Mu, D., Yu, C., Xing, X., & Li, K. (2022). Grebe: Unveiling exploitation potential for linux kernel bugs. In *2022 ieee symposium on security and privacy (sp)*. IEEE.

Park, S., Kim, D., Jana, S., & Son, S. (2022). Fugio: Automatic exploit generation for php object injection vulnerabilities. In *31st usenix security symposium (usenix security 22)*.

Pashchenko, I., Vu, D.-L., & Massacci, F. (2020). A qualitative study of dependency management and its security implications. In *Proceedings of the 2020 acm sigsac conference on computer and communications security*.

References III

Stalnaker, T., Wintersgill, N., Chaparro, O., Di Penta, M., German, D. M., & Poshyvanyk, D. (2024). Boms away! inside the minds of stakeholders: A comprehensive study of bills of materials for software systems. In *Proceedings of the 46th ieee/acm international conference on software engineering*.

Xiong, W., & Lagerström, R. (2019). Threat modeling–a systematic literature review. *Computers & security*, *84*, 53–69.

Yu, S., Song, W., Hu, X., & Yin, H. (2024). On the correctness of metadata-based sbom generation: A differential analysis approach. In *2024 54th annual ieee/ifip international conference on dependable systems and networks (dsn)*. IEEE.