Markus Schiffermuller
mcsch.dev
Email: [redacted]
Mobile: [redacted]

Experience

- **Trail of Bits - Internship (Cryptography team)** **Jun. 2024 – Aug. 2024**
  - Analyzed open source cryptography libraries for security vulnerabilities and found multiple security-critical vulnerability in popular open source crypto libraries which resulted in five different CVEs ranging from medium to critical (CVE-2024-48949, CVE-2024-42461).
  - Wrote a guide in the Trail of Bits testing handbook on how to test cryptographic implementations to help developers test against common mistakes and timing vulnerabilities.
- **Technical University of Graz - Project employee (Cryptography team)** **Jun. 2023 – Aug. 2023**
  - Build a tool that estimates the latency of different S-box constructions by converting them into their reduced CNF form, finding the critical path, and estimating latency based on the gates encountered.
  - Build a tool that cryptanalyses cipher constructions based on their differential and linear properties. It finds characteristics with a depth-first approach (for a variable amount of round depths). It is initially written in Python and later rewritten and multithreaded in C++ for better performance. We used this tool to evaluate potential low-latency cipher constructions and their security.

  Project employee (System Security team) **Jun. 2022 – Aug. 2022**
  - Built a hardware simulation module using gem5 in C++ to evaluate memory security measures implementing a Merkle integrity tree to better compare different memory encryption schemes.
- **Netconomy - Internship (Software development)** **Jul. 2021 – Aug. 2021**
  - Worked on both the front and back ends of E-commerce stores with annual revenue exceeding 100€ million.
  - Extended the payment process functionality using the SAP E-commerce framework with Java and JavaScript.
- **DCCS - Junior Software Engineer** **Nov. 2020 – Feb. 2021**
  - Enhanced front-end components for enterprise clients using the Liferay framework, JavaScript, HTML, and CSS. Gained experience in full software development lifecycle within an agile team, from requirements analysis to implementation and testing.
- **NXP Semiconductors - Internship & freelance work** **Jul. 2019 – Dec. 2019**
  - Contributed to the documentation of Secure Elements API, focusing on RSA encryption functionality and implementation guidelines in C/C++.
  - Built a smartwatch application for Android using Java and the NFC stack to demonstrate keyless entry for cars which was displayed at international automotive fairs.

Education

- **École Polytechnique Fédérale de Lausanne (EPFL)**
  - Master Thesis on circumventing Censorship in non-E2EE messaging applications @ Spring lab 2025
- **Technical University of Graz**
  - Master of Science in Computer Science, Grade average 1.06 (1.0 best, 5.0 worst) 2025
    - Major in Cyber Security with Minor in Software Technologies
  - Bachelor of Science in Software Engineer and Management, Grade average 1.8 (1.0 best, 5.0 worst) 2022

Teaching

- **Information Security - Teaching Assistant** **Oct. 2022 – Feb. 2024**
  - Wrote the assignments for the undergraduate course Information Security concerning low-level vulnerabilities in C/C++ like buffer overflow, format string attacks, use after free vulnerabilities and side channel attacks, which was an exercise for over 250 students.
  - Presented practical lecture in front of 100+ students about common low-level vulnerabilities in C/C++, how to use pwndbg and write exploits using pwntools and held the assignment interviews.

Leadership & Activities

- Team Captain of CTF Team LosFuzzy (2022 - 2023)
- Participated in CTF competitions and published write-ups for my blog
- Gained a top 100 position in the CTFTime ranking in 2023 with my team
- Organised weekly training session for security enthusiast about cybersecurity
- Presenter of the first CTF beginner training sessions about Introduction to CTFs
- Organized the first CTF created by LosFuzzys GlacierCTF and the second iteration with over 1300 participants (GlacierCTF 2022, GlacierCTF 2023)
- Participating in CryptoHack solving CTF style challenges on cryptography about a wide range of topics like symmetric cipher construction, RSA etc.
- Talk: Empire Hacking in New York - Gave a talk about my work at Trail of Bits and about the importance and intricacies of testing cryptographic implementations.
- Talk: Grazer Linux Tage - Spoke about understanding and preventing common misuses in Cryptography

Skills

- **Languages**: Python, C/C++, Java, JavaScript, HTML, CSS, x86 Assembly, SQL, Bash, Latex
- **Technologies**: Sage, GDB/pwndbg, Wireshark, Pwntools, Git, Ghidra, Vue.js, Flask, Docker