Markus Schiffermuller

mcsch.dev

Experience

- **Trail of Bits** — New York, USA
  Internship: Cryptography team — *Jun. 2024 – Aug. 2024*
  - **Vulnerability discovery**: 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).
  - **Technical Writing**: 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** — Graz, Austria
  Student project employee: Cryptography team — *Jun. 2023 – Aug. 2023*
  - **Low latency cryptography**: Performed research on the security of low-latency cryptographic primitives like S-boxes, permutation, and diffusion layers.
  - **Practical Cryptanalysis**: Worked in the symmetric cryptography and cryptanalysis team to design tools that improved the selection of symmetric low-latency cryptographic primitives like S-boxes.

  Student project employee: System Security team — *Jun. 2022 – Aug. 2022*
  - **Low-level security**: Built a hardware simulation module using gem5 in C++ to evaluate memory security measures and implemented a Merkle integrity tree.

- **Netconomy** — Graz, Austria
  Internship: Software development — *Jul. 2021 – Aug. 2021*
  - **Fullstack Java development**: Worked on both the front and back ends of E-commerce stores with annual revenue exceeding 100€ million.
  - **Payment process extension**: Extended the payment process functionality using the SAP E-commerce framework with Java and JavaScript.

- **DCCS** — Graz, Austria
  Junior Software Engineer — *Nov. 2020 – Feb. 2021*
  - **Front-end development**: Developed and implemented solutions to enhance the usability and user experience of front-end webpages using JavaScript, HTML, and CSS in the Liferay framework, resulting in a more intuitive and user-friendly interface.

- **NXP Semiconductors** — Gratkorn, Austria
  Internship & freelance work — *Jul. 2019 – Dec. 2019*
  - **Secure Elements**: Worked on the API of Secure Elements using C/C++ with a focus on RSA encryption.
  - **Automotive NFC application**: 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)** — Lausanne, Switzerland
  Master Thesis on censorship in the context of non-E2EE chat applications @ Spring lab — *Oct. 2023 – Apr. 2024*

- **Technical University of Graz** — Graz, Austria
  MSc in Computer Science, Grade average 1.06 (1.0 best, 5.0 worst) — *2025 (expected)*

  Major: Information Security, Minor: Software Engineering

- **Technical University of Graz** — Graz, Austria
  BSc in Software Engineering and Management; Average Grade: 1.8 (1.0 best, 5.0 worst) — *2022*

Teaching

- **Information Security** — Technical University of Graz
  Teaching Assistant — *Oct. 2022 – Feb. 2024*
  - **Research Assistant**: 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.
  - **Lecture**: 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**: Responsible for managing a team of over 20 active members regarding the participation in CTFs, managing on-site CTFs, and organizing weekly training sessions for security enthusiasts about cybersecurity
  - **CTF competitions**: 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.
  - **CTF organization**: Organized the first edition of the GlacierCTF 2022 and the GlacierCTF 2023 with over 1000 participants and a combined prize pool of over 30000€. Held beginner workshops for students at the university about CTFs and how to get started.
- **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
- **CryptoHack**: Solving CTF style challenges on cryptography about a wide range of topics like symmetric cipher construction, RSA etc.

Skills

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