Theodor Signebøen Midtlien

theodor@midtlien.com | Birth year: 1999

LINKS

Website:// **theodorsm.net**
Github:// **theodorsm**
LinkedIn:// **theodorsm**

SKILLS

PROGRAMMING

In order of competence

- Go
- Python
- Java / Kotlin
- C/C++
- Bash
- Javascript + HTML + CSS
- SQL
- Assembly (RISC-V, ARM, x86)

TECHNOLOGIES

- Linux
- Git
- Docker
- TLS/DTLS
- 5G
- Android
- gRPC
- Ansible
- Ghidra
- FastAPI
- SvelteKit
- Django
- React

FOSS

- Tor Project, anti-censorship team
- Pion
- Webkom

SUMMARY

Cyber security professional and software engineer holding a Master's degree in Communication Technology and Digital Security. Experience includes penetration testing, software engineering in various programming languages, Linux system administration, DevOps, full-stack development, research on Linux kernel performance and 5G security. Maintaining a Go library, covertDTLS, and actively participating in open-source and CTF communities.

WORK EXPERIENCE

MNEMONIC | Full-time | Cyber security consultant

August 2024 – Present | Oslo, Norway

Doing penetration testing as a cyber security consultant. Working with infrastructure and mobile assessments. Clients range from large energy companies to banks.

PROMON | Part-time | Research Internship

January 2024 – May 2024 | Oslo, Norway

Reverse engineering of Android applications, and implemented a novel string obfuscation scheme for compiled apks using Kotlin and Smali.

NTNU | Part-time | Full-Stack Developer

September 2022 – August 2023 | Trondheim, Norway

Developing a web application (SvelteKit + FastAPI + SQL + Docker and Traefik) to be used by students to enhance learning in courses by reflecting on their learning outcomes on a weekly basis. **Github repo**

NTNU | Part-time | Research Assistant

January 2021 – June 2022 | Trondheim, Norway

Research assistant for the Department of Information Security and Communication Technology. Worked on developing a benchmarking tool to measure the real-time networking performance of the Linux kernel. Using DPDK for hardware acceleration and Cisco TRex for traffic generation and performance measurements. Plotted latency and jitter in histogram together with flamegraphs of perf profiling of the Linux kernel.
github.com/theodorsm/trex-scripts
github.com/theodorsm/flamegraph-results

CISCO | Software Engineer Intern

June 2021 – August 2021 | Oslo, Norway

Summer internship at Cisco Norway. Worked on integrating locally stored webapps for Webex RoomOS with C++ and the Qt framework. Created a proof of concept webapp with React, Typescript and Gatsby.

ORGANIZATIONS

ITEMIZE NTNU | Leader

August 2023 – May 202 | Trondheim, Norway

Itemize is the CTF team and the interest organization for information security at NTNU. The leader role consisted of holding technical workshops, communication with the university, organizing meetings for the group and recruitment. **itemize.no**

WEBKOM, ABAKUS | Open Source Developer

September 2019 – June 2024 | Trondheim, Norway

Abakus is the student organization for Computer Science and Communication technology at NTNU. Webkom is the software development committee for Abakus. Worked together with 15 other students continuously developing the open-source project **abakus.no** and other services. Worked for 5 years with Linux (Ubuntu) system administration (self-hosted and cloud), DevOps, frontend and backend development. **github.com/webkom**

CAPTURE THE FLAG

CTF tag: *bashgobrr*

Teams:
- **Itemize** (NTNU).
- **Enoflag/Enowars** (TU Berlin)
- **Cyberlandslaget 2022** supported the Norwegian national team in ECSC (European Championship) in Vienna.
- **Corax**.

LANGUAGES

- **Norwegian**: Native
- **English**: Fluent
- **German**: Basic A1/A2
- **Spanish**: Basic A1
- **Danish and Swedish**: Understands

EDUCATION

NORWEGIAN UNIVERSITY OF SCIENCE AND TECHNOLOGY

MSc in Communication Technology and Digital Security
Aug. 2019 - June 2024 | Trondheim, Norway

Average grade: B
Thesis grade: A
Thesis title: **"Reducing distinguishability of DTLS for usage in Snowflake"**

The motivation behind the thesis was censorship circumvention. Worked with the Tor Project anti-censorship team and the Pion community. Developed a tool to analyze and identify passive field-based fingerprints in DTLS traffic, specifically finding fingerprints of the Pion library used in the Snowflake censorship circumvention system. Designed and implemented **covertDTLS**, a Go library that randomizes and mimics DTLS handshakes to prevent traffic fingerprinting, incorporating a continuous delivery pipeline to keep mimicked handshakes of Chrome and Firefox up-to-date. The thesis demonstrated the effectiveness of handshake randomization and mimicry as countermeasures against passive, stateless fingerprinting in censorship circumvention systems.

TECHNISCHE UNIVERSITÄT BERLIN

ERASMUS+ exchange
October 2022 - September 2023 | Berlin, Germany

Average grade: B+

Courses: Embedded Systems Security Lab, Networked Embedded Systems, International Information Security Contest, Privacy Engineering, Networked Systems Security, Internet and Network Security, Computer Security Project

PROJECTS

5G SECURITY PROJECT

theodorsm.net/TUB23_computer_security_project
github.com/theodorsm/5G-testbed

The main goal of the project was to create a testbed to explore the implementation correctness of encryption and integrity negotiation between the 5G core network and commercial-off-the-shelf user equipment. A test setup was created with a modified open-source 5G core written in C (open5gs) with a Software Defined Radio for the base station. During the development of the testbed, a security bug was found in Open5gs and promptly reported.

5GO PHREAKING

github.com/enowars/enowars7-service-phreaking

Made a Go service played at the Attack/Defence CTF **Enowars7** with a ctftime rating weight of 100, hosted by Enoflag (the CTF-team of TU Berlin). The service is a basic simulation of a standalone 5G network - implementing a registration protocol vulnerable to a man-in-the-middle attack. Exploitation could be done by binary patching, code-reuse or modifying network traffic.