# Alexandre Adamski

github.com/NeatMonster | NeatMonster_
neat@neat.sh | 06 98 03 78 40

## EDUCATION

**TLS-SEC**
MSc in Security and Networks
Avanced courses focused on networks and systems security, dispensed by security experts.
2016-2017 | Toulouse, France

**INP-ENSEEIHT**
Engineering Degree in C.S.
C.S. and Applied Mathematics, Software Engineering specialty.
2014-2017 | Toulouse, France

## COURSEWORK

**THIRD YEAR**
Cryptography
Software Vulnerabilities
System and Kernel Security
Hardware Security
Reverse Engineering
OSI Security Architecture
Wireless Networks
Secure Network Architecture
Network Security Protocols

**SECOND YEAR**
Concurrent Computing
Real-Time Computing
Middleware and Databases
Lang. and Compiler Design
Graph Theory, Formal Methods

**FIRST YEAR**
Imperative, Functionnal, Object-Oriented Programming
Computers Architecture
Probability and Statistics
Linear Algebra and Optimization

## SKILLS

Reverse Engineering, Vulnerability Research, Software Exploitation, Tools Development, Source Code Review

**LANGUAGES**
Python • C • C++ • Assembly (ARM32 • ARM64 • x86 • x86_64)

**TOOLS**
IDA Pro (+ Hex-Rays) • Ghidra
Unicorn • Keystone • Capstone
GDB • Frida • AFL • libFuzzer

## EXPERIENCE

**QUARKSLAB** • Information Security Engineer
Nov. 2017 – Now | Toulouse, France
My most notable achievements during my time there include:
- Reverse engineering and exploitation of a TrustZone implementation (trusted application → secure driver → operating system → monitor)
- Reverse engineering and exploitation of a Secure Boot implementation (programmer → multi-stage bootloader → device bootrom)
- Reverse engineering, exploitation and debugging of a Baseband chip

**QUARKSLAB** • Security Engineering Intern
Mar. 2017 – Nov. 2017 | Paris, France
- Remote Attestation implementation for Intel SGX enclaves

## PROJECTS

**"MCEXPLORER"** • Decompiler Microcode Explorer
Mar. 2019 | Paris, France | github.com/NeatMonster/MCExplorer
Exploration tool for IDA Pro's decompiler: listing and graphing of micro-code.

**"AMIE"** • A Minimalist Instruction Extender
Nov. 2018 | Paris, France | github.com/NeatMonster/AMIE
IDA Pro plug-in that replaces ARM system registers encoding by their friendly names, and augments the disassembly and decompiler views by showing hints extracted from the ARM documentation on the instructions and registers.

**"IDARLING"** • Collaborative Reverse Engineering Plug-in
Jan. 2018 | Paris, France | github.com/IDArlingTeam/IDArling
IDArling enables real-time collaborative sessions between multiple IDA Pro and Hex-Rays instances. It synchronises user events, displays cursors in the disassembly view, functions list, navigation bar, and so much more.

## PUBLICATIONS

2019 "Breaking Samsung's ARM TrustZone" —Talk at BlackHat (US)
2019 "IDArling: Collaborative Reverse Engineering" —Talk at SSTIC (FR)
2018 "Overview of Intel SGX" —Published on Quarkslab's blog (FR)
2018 "Developing a Secure App using Intel SGX" —Article in MISC (FR)

## TEACHING

2019 "Attacking ARM TrustZone" —Training at Hardwear.io (US)
2019 "Attacking ARM TrustZone" —Training at Zer0Con (KR)
2019 "Attacking ARM TrustZone" —Training at Troopers (DE)
2019 "IDA Pro Scripting" —Teaching for the BADGE RE of ESIEA (FR)
2019 "Study of Android Secure Bootchains" —Internship Supervision (FR)
2018 "Security of Wi-Fi Stack Components" —Internship Supervision (FR)

## AWARDS

2018 IDArling, Winning Entry of Hex-Rays' Plug-In Contest

## LANGUAGES

| | |
|---|---|
| French | Mother Tongue |
| English | Advanced Level |