Alexandre Adamski

github.com/NeatMonster | NeatMonster_
neat@neat.sh | (+33)6 98 03 78 40

EDUCATION

INP-ENSEEIHT • TLS-SEC
Engineering Degree in C.S. • MSc in Security and Networks
2014-2017 | Toulouse, France

LANGUAGES

French | Mother Tongue
English | Advanced Level

EXPERIENCE

LONGTERM • Vulnerability Research Engineer
Mar. 2020 – Mar. 2021 | Toulouse, France | longterm.io

- Fuzzing and manual analysis of kernel drivers from various OEMs (Google, Qualcomm, Samsung, Huawei).
- Exploitation of a single instruction race condition in the Binder driver (that was reported as CVE-2020-0423).
- Reverse engineering and exploitation of Samsung's hypervisor called RKP (3 vulnerabilities awaiting a fix).

QUARKSLAB • Information Security Engineer
Mar. 2017 – Mar. 2020 | Paris, France | quarkslab.com

- R.E. & V.R. in a TrustZone implementation: fuzzing of trusted applications and secure drivers, exploitation of a TA, then of a SD, and finally exploitation of the trusted os and secure monitor (reported as SVE-2019-16665).
- R.E. & V.R. in a Secure Boot implementation: static analysis, exploitation of the programmer (less privileged), then of the multi-stage bootloader (more privileged), and finally dump and exploitation of the device bootrom.
- R.E. & V.R. in a Baseband implementation: exploitation from AP and development of a debugger for the RTOS.
- R.E. & V.R. in a UEFI environment: tooling around the DXE and SMM drivers, exploitation of the SMI handlers.

PROJECTS

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

2021 A Samsung RKP Compendium —Published on Longterm's blog
2020 Exploiting a Single Instruction Race Condition in Binder —Published on Longterm's blog
2019 A Deep Dive Into Samsung's TrustZone —Published on Quarkslab's blog
2019 Breaking Samsung's ARM TrustZone —Talk at Black Hat USA 2019
2019 IDArling: Collaborative Reverse Engineering —Talk at SSTIC 2019
2018 Overview of Intel SGX: Internals & Externals —Published on Quarkslab's blog
2018 Developing a Secure App using Intel SGX —Article in MISC-099

TEACHING

2019 Attacking ARM TrustZone —Training given at Troopers, Zer0Con, Hardwear.io
2019 IDA Pro Scripting —Course taught in the BADGE Reverse Engineering at ESIEA
2019 Study of Android Secure Bootchains —Supervision of Elouan Appéré's internship
2018 Security of Wi-Fi Stack Components —Supervision of Hugues Anguelkov's internship

AWARDS

2018 IDArling —First prize in Hex-Rays' 2018 Plug-In Contest