

Stanislas Lejay

Security researcher

362-0045, Saitama-ken, Ageo-shi, Mukoyama, 2-32-16

☎ (+81) 90-6749-8041

✉ stan3422@gmail.com

03/01/1995



Professional Experience

- Sept 2023 – **Security Researcher**, L3 HARRIS - TRENCHANT, Tokyo
 - Current Bug hunting and exploit writing in Android environnement (mostly)
 - Blackbox Android app reverse engineering (Java/native C/native C++)
 - Exploit writing
- Nov 2021 – **Security Managing Consultant**, NCC GROUP, Tokyo
 - Sept 2023 Automotive vulnerability researches and reverse engineering
 - Open Source Android pentest and code review (C, Java, Rust)
 - Blackbox hardware reverse engineering and pentest (various architectures/OS)
 - Physical breaching/pentest (locally in Japan)
- Nov 2018 – **Automotive Security Researcher**, WHITEMOTION, Tokyo
 - Nov 2021 Automotive vulnerability researches and reverse engineering
 - ECU reverse engineering (pentest, vulnerability assessment) [most of the time]
 - Provide security training (mostly automotive oriented) [quite often, 2 or 3 times a year]
 - Personal projects and research on OBDII, CAN, Reverse engineering, engine management, etc
- Mar 2018 – **Vulnerability Researcher Intern**, WHITEMOTION X QUARKSLAB, Tokyo
 - Sept 2018 Same as WhiteMotion above
- Sept 2017 – **Embedded Security Intern**, QUARKSLAB, Paris
 - Feb 2018 - Automotive bus analysis (CAN/OBDII) and reverse engineering
 - Hardware and Automotive CTF organizer (Hardwear.io '17, CodeBlue '17, NullCon '18).
- Sept 2016 – **Security intern**, FRENCH MINISTRY OF DEFENSE, Paris
 - Jan 2017 Reverse engineering

Computer Science skills

- Main skills Reverse engineering and bug hunting, Android userland mostly nowadays
- Languages C/Python, C++, Assembly (reverse), can easily adapt
- Fields of analysis so far Android userland bug hunting and exploitation / SW|FW|HW pentesting / Automotive embedded systems / Binary analysis (angr) / MacOS internals (DYLD)

Talks and Publications

- WhiteMotion
 - "A tour of automotive systems from 20 years ago" (BHEU19: ECU reverse engineering and speed limiter bypass)
 - "Building a custom infotainment system" (connected to OBD to change music regarding the driver's mood)
- Quarkslab
 - "How to drift with any car" (34c3: OBDII discovery and playing video games with real cars)
 - "OBD Dongle reverse engineering" (NitroOBD reverse engineering)
- LSE
 - Apple's Mach-o format and dynamic linker's DYLD (calling printf without using the function's symbol)
 - Talking with cars - Introduction to automotive networks communications (First discoveries and communications with OBDII)
 - My RC car just got itself a CAN bus (creating a security CTF out of an RC car)
 - Fuzzing IOCTLs with angr (Discovering hidden IOCTLs in Linux kernels with angr)
 - ProfileScan (Volatility plugin to guess which profile to use)
- (Links)
 - <http://p1kachu.pluggi.fr/blog>
 - <http://p1kachu.pluggi.fr/external>

Formation

- 2015–2018 **EPITA's System and Security Laboratory (LSE)**, *Low Level programming and security*, Reverse engineering, *Automotive system analysis*
- Programming in C (software, crackme, 3DS roms), Assembly (ROP) and Python (scripting mostly)
 - CTFs (Team number 757 on CTFtime.org, participated in competitions multiple times a year)
 - Systems and files internals (DYLD, Linux IOCTLs, QEMU and HVF, Wii and 3DS file format)
 - Car systems (CAN and related networks, OBDII)
 - Reverse engineering (CTF, challenges, 90s/00s cars ECUs, Nintendo 3DS)
 - Symbolic execution and analysis (ANGR)
 - Others (Android automation, simple bots, volatility framework, little projects I found interesting)
- 2013–2018 **Computer Science Engineering School (EPITA)**, *International Section (Courses in english)*, System & Security specialization, C/C++ programming, (Graduated September 2018)

Languages

- French First language
- English Fluent, TOEIC (970)
- Japanese Not fluent but enough to get around, living there since 2018

Hobbies

- Motorsports, car mechanics, circuit racing
- Guitar, music