Stanislas Lejay

Security researcher

2-941-3, 301, Kushihikicho, Kita-ku
Saitama-shi, Saitama 331-0825, Saitama, Japan
(+81) 90-6749-8041
stanislas.lejay@white-motion.com
03/01/1995

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).

Professional Experience

Nov 2021 – Current **Security Managing Consultant**, NCC Group, Tokyo.
Automotive vulnerability researches and reverse engineering
- (Under Construction)

Nov 2018 – Nov 2021 **Automotive Security Researcher**, WhiteMotion, Tokyo.
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 – Sept 2018 **Vulnerability Researcher Intern**, WhiteMotion x Quarkslab, Tokyo.
Same as WhiteMotion above

Sept 2017 – Feb 2018 **Embedded Security Intern**, Quarkslab, Paris.
- Automotive bus analysis (CAN/OBDII) and reverse engineering
- Hardware and Automotive CTF organizer (Hardwear.io '17, CodeBlue '17, NullCon '18).

Jan 2017 – Feb 2018 **Linux kernel development assistant**, EPITA, Paris.
- Kernel development courses for 4th and 5th year students in security or embedded systems specializations.
- Practical sessions subjects redaction and correction

Sept 2016 – Jan 2017 **Security intern**, French Ministery of Defense, Paris.
Reverse engineering

Sept 2015 – June 2016 **C#/OCaml teaching assistant**, EPITA, Paris.
Programming courses and practical sessions for first year students. Practical sessions subjects redaction and evaluation, along with live courses

July 2015 – Sept 2015 **Software engineer intern**, Amundi, Paris.
Library handling infrastructure development for Amundi and partners.

Computer Science skills

Languages: C/Python, C++, Assembly (reverse), can easily adapt

Fields of analysis: Binary analysis (angr) / MacOS internals (DYLD) / Automotive embedded systems

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

Languages

French **First language**

English **Fluent, TOEIC (970)**

Japanese **Currently learning**

Hobbies

- Motorsports, car mechanics
- Guitar, music