Arun Magesh

p:(+31))0644752806
e:arunmagesh@ymail.com

PROFESSIONAL SUMMARY

Expertise in Security of embedded device's security. That includes Hardware, Firmware, Wireless, Web/Mobile applications Personal interest relies on Fault injection and other hardware based attacks. Built tools for hardware exploitation and fuzzers for low- level IoT network protocols. Training on IoT/Embedded security.

EXPERIENCE

Principal Security Consultant, ONEKEY, Netherlands
Feb. 2023 – Present

- Playing a key role in firmware analysis and contributing to the development of an automated framework.
- Lead and performed penetration tests on embedded devices in media, entertainment, and automotive sectors.
- Analysing threats and assessing risks(TARA) for hardware devices.
- Performing gap analysis in line with the Cyber Resilience Act and IEC 62443.
- Developed a new class of vulnerability, X(R)iP, to bypass secure boot on XiP implementations.

Security Analyst, Riscure, Netherlands
Feb. 2021 – Jan. 2023

- Conducting Fault Injection (Voltage, EM, and Laser) and Side-Channel Analysis (Power and EM) on embedded devices and chips.
- Executing penetration tests on embedded devices across diverse sectors, including media & entertainment and automotive.
- Carrying out source code reviews on BootROM, TEE, and other boot stages.
- Conducting security design reviews for Embedded Chips.

Security Consultant, Payatu Software Labs, India
Sep. 2017 – Oct. 2020

- Worked on finding security issues on several client's connected ecosystem f rom various domains like Automotive, Medical, and Commercial devices.
- To perform independent research on various other commercial devices and ecosystems.
- Fuzzing and exploiting Network Protocol stacks.
- To contribute to the open-source frameworks for Embedded security.

IoT Security Researcher, Attify Mobile Security, India

May. 2016 – Aug. 2017

- To perform penetration testing on commercial embedded devices.
- Research and analysis of various wireless protocols and implementations.

SKILLS

Hardware: Fault injection, Side channel analysis,Memory Extraction, Dynamic Debugging.

Firmware: Static Analysis, Dynamic Analysis, Firmware patching, Firmware Decryption.

Mobile Application: Static Analysis, Dynamic Analysis, Communication Sniffing, Decryption of traffic .

Wireless: Bluetooth, 802.15.4, SDR, GNURadio.

Network: Protocol reversing,coverage based fuzzing, Crash analysis.

Development: C, Python, Embedded C on STM32, ESP32, and PSoC.

CVE OBTAINED

- CVE-2018-20007
- CVE-2018-20008
- CVE-2020-13821
- CVE-2020-13410
- CVE-2020-13932
- CVE-2023-3630
- CVE-2020-15486
- CVE-2020-15484
- CVE-2020-15483
- CVE-2020-15482
- CVE-2020-15485

TALKS/TRAININGS GIVEN

- June 2017: Talk on IoT Security at Intel IoT devfest, Bemyapp
- March 2017: Talk on Trends on IoT Security at EFY Conference.
- June 2017: Training on Hardware hacking 101 at RISC conference
- September 2017: Training on Wireless hacking at the c0c0nX conference.
- 2018: Training on Hardware Hacking at nullcon, zer0con18, HackInParis, BlackHatUSA, and Brucon.
- August 2018: Workshop on hacking Smartwatch at DEFCON26 – US 2019
- Training on Hardware Hacking at nullcon, HackinParis, Brucon
- March 2019: Talk on How to fail in Hardware Hacking 101 at PHDays 19
- March 2019: Conducted a workshop on Rapid IoT Hacking at PHDays 19
- October 2023: Talk on breaking and analysis of Fault injection protection mechanism at Hacktivity 2023

TRAININGS/COURSES TAKEN

- Hardware Hacking Training with Hardspliot framework
- ICSI CNSS - Certified Network Security Specialist
- Practical Baseband Exploitation
- Offensive TEE Exploitation
- TCP/IP Training Video A Definitive & Easy To Follow Course
- Mastering Cypress PSoC-An Embedded System Design perspective
- Learn Python: The Complete Python Programming Course
- Python for Penetration Tester
- C Programming for Beginners
- Advanced Web Hacking