INTERNSHIP -

Smartphone Boot Firmwares

Reverse Engineering and Emulation

At eShard, we really enjoy having technical people who love to work on low level technologies. You can see the kind of work that we do on smartphones by having a look at our recent blog posts on the Pixel6 bootloader (part1 / part2 / part3).

With this internship, your goal will be to research and study the latest bootloaders of Android smartphones and iPhone. Become proficient with ABL, TrustZone, SEP, iBoot and all those low level softwares that boots up smartphones. You will work on emulation and instrumentation of such code, and will work most likely with C and Rust code base.
For such a position, we expect you to be highly motivated, quick learner and with a strong desire **NOT to be micromanaged**. If you enjoy using google and hack through creative paths to find your way out, this will definitely be suited for you, else you should most definitely avoid this internship.

COMPANY

eShard is a technology company specializing in security testing: electronic chips, mobile applications, communicating objects, servers and desktops, for which there is both storage of personal data and exchange of information.

Our role is to provide our customers, designers or users of connected objects and systems with the means to control cyber risk and to ensure that they integrate the right level of protection: understand the threat, carry out automatic checks, obtain the knowledge of attacks.

To do this, we have assembled a team of specialists, researchers who are experts in cryptography, IC security and security of mobile applications, servers and desktops. We offer our customers a range of tools and services: SaaS platform, software, technical training and security testing service.

🗓️ **Desired start date:** 2023.

📍 The position is based in **Marseille, France**.

INTERNSHIP -

eShard

Your day-to-day would be:

Directly attached to a member of the R&D team, you will be in charge of the following missions:

- ➔ Reverse engineering of TrustZone, SEP, Bootloaders firmware
- ➔ Emulation such firmware
- ➔ Fuzzing and binary diffing such firmware
- ➔ Using typical tools of the trade (Disassembler, Unicorn, QEMU, KVM, ...)
- ➔ Read a lot about ARM and Smartphones knowledge
- ➔ Work with low level linux stacks
- ➔ Collect information about state-of-the-art analysis techniques.
- ➔ Build knowledge from your work

You're perfect for us, if...

- ➔ You are already proficient in reverse engineering, which is a passion of yours.
- ➔ You demonstrate great autonomy in your assignments.
- ➔ You participated in CTFs or other contests and got significant results.
- ➔ Not mandatory but potentially aligned with the internship duration, you are preparing a master degree and are in your last year of study.
- ➔ You have developed a particular interest in:
  - ◆ Reverse Engineering on Smartphones
  - ◆ ARM64 assembly
- ➔ You have some good knowledge of ARM architectures, Assembly, C programming, IDA or Ghidra, WinDbg, and other tools.
- ➔ You are hacker minded, responsive and have the spirit of initiative.
- ➔ You demonstrate good interpersonal skills that will allow you to work as a team effectively.
- ➔ You have a good writing level in English.

Benefits

- ➔ Support from professionals in a cutting-edge and booming business sector
- ➔ Dynamic work environment within a young and friendly team
- ➔ High performance work equipment
- ➔ Flexible working hours
- ➔ Space dedicated to talent development
- ➔ "Tickets restaurant" covered up to 50%
- ➔ Annual events, snacks and drinks
- ➔ Become a "one in a few" bootloader expert!

eShard

Interested?

Contact us by sending your resume to

intern@eshard.com