Bootloader vulnerability exploitation & research - ARM

Internship

The eShard's Reverse Engineering platform allows reverse-engineers to perform unique full-system timeless analyses of a system's execution, thereby providing powerful tools to study data flow, hard to reproduce use cases, kernel/application communication mechanisms.

Your objective is to make an overview of published CVEs that specifically target bootloaders in IoT and firmware. From this overview, we will select some of them, with the goal of developing code for exploitation thanks to the esShard Reverse platform, esReven and Timeless analysis techniques, as well as third-party tools. You will investigate the state-of-the-art of the field. During an optional second phase, you'll transition into full exploitation mode to conduct research on previously unidentified vulnerabilities. You would leverage the esReven Python API to automate parts of the analysis process to provide out-of-the-box techniques. You will report your results in the form of write-ups, whether Jupyter Notebooks or articles, that will enrich the Knowledge Base.

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.

As part of the development of our activity, we are recruiting an intern in our System Security R&D team to work on this topic during a 4 to 6-month paid internship.

🗓️ **Desired start date:** as early as possible.

📍 The position is based in **Pessac (33)**, next to Bordeaux.

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:

- ➔ Identify some targets and select which one will be studied first.
- ➔ Perform reverse engineering discovery work on the target, manually, automatically, potentially implementing fuzzing.
- ➔ Document your findings using notebooks and produce a blog post to communicate on your results.

You're perfect for us, if...

- ➔ You are already proficient in reverse engineering, which is a passion of yours.
- ➔ 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, Vulnerability analysis or Malware analysis
  - ◆ Development with Python
- ➔ You have some good knowledge of ARM architectures, Assembly, C programming, IDA or Ghidra, Debuggers, and other tools.
- ➔ You are hacker minded, responsive and have the spirit of initiative.
- ➔ You demonstrate autonomy in your assignments.
- ➔ 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

Interested?

Contact us by sending your resume to

intern@eshard.com