Internship: embedded security - improve TPM v2.0 support in the U-Boot bootloader

Bootlin

This document was taken from `https://bootlin.com/blog/2020-internships/`

Company overview

Bootlin proposes development and training services around embedded Linux and its kernel. Founded in 2004 and now employing 12 people, it has gained a strong reputation for its expertise in Linux kernel development and embedded Linux system integration. With a mostly international customer base, Bootlin works for major semiconductor vendors and multiple embedded system makers.

With strong roots in Free Software and Open Source, Bootlin releases all its training materials for free under a free documentation license, and makes a great number of contributions to the Linux kernel and to other community projects. Bootlin often appears in the top 20 worldwide list of companies contributing to the mainline Linux kernel.

Bootlin also invests a lot in the involvement of its engineers in the technical community, which gives them visibility and a good reputation beyond the limits of the company employing them, which is quite rarely offered by other companies throughout the world.

Internship topic

The U-Boot bootloader is by far the most widely used bootloader to start Linux on non-x86 embedded platforms (ARM, MIPS, PowerPC, RISC-V, etc.).

Last year, Bootlin made first contributions to U-Boot supporting TPM (Trusted Platform Modules) v2, providing minimalistic support for essential functionality. TPMs have been used for several years in the PC world, and are progressively being adopted in the embedded world too. Hence the need for a more exhaustive implementation.

Among the multiple possible uses of a TPM, one we are interested in is the delivery of a secret on the condition that the hardware and software of the platform is in a state that is expected by the TPM. Such functionality is called *measured boot* and requires the involvement of the bootloader.

Such functionality already exists but only does half of the job as, for the moment, there is no way to block a *replay attack*.

However, the TPM v2.0 specification proposes authentication mechanisms to protect the system against such attacks. The goal of this internship is implement such mechanisms and contribute the code to the mainline U-Boot project.

In case progress is faster than expected, still with the goal to improve U-Boot, it will also be possible to make other contributions to U-Boot. As a matter of fact, there are multiple ongoing tasks to contribute to : refactoring, switching to Kconfig files, deployment of the *device model*, etc.

This topic will be addressed as follows :

— Some research on TPMs and their specifications, making a quick State of the Art.
— Development work in the U-Boot code and tests on a popular hardware platform (such as Beagle Bone Black or Raspberry Pi with TPM on SPI)
— Contribution to the community and interaction with the maintainers of the code that you modify.

This internship will make you familiar with popular embedded boards. You will also discover the way U-Boot developers and maintainers work, which is close to the way of working in the Linux kernel community. Such experience and way of working will surely be useful in your career in embedded software and in Free Software in general.

Supervision

The internship will be supervised by Miquèl Raynal, engineer at Bootlin since 2017 and contributor to U-Boot and Linux.

The intern will work in a team of embedded Linux and kernel engineers, with a very strong level of expertise.

Useful skills

— Good C programming experience
— Familiarity with embedded Linux (for example through experiments on Raspberry Pi or equivalent)
— Basic knowledge of Git
— Understanding the way open-source communities work, and ability to communicate with it (IRC, e-mail, etc.)

Practical information

— Who can apply: all students from the European Union, studying in a European University

- Location:
  - Colomiers, in the Toulouse metropolitan area, France, reachable by train.
- Dates: between February and September 2020
- Gross monthly compensation: between 500 and 1000 EUR, according to profile (end of studies or half-way, experience, etc.)
- Duration: at least 4 months
- How to apply: send your resume and interests to jobs@bootlin.com