Secure boot, TEEs, different OSes and more
Making sense of the trusted computing landscape in the Eclipse Oniro embedded distribution

Marta Rybczynska
FOSDEM 2022
ABOUT MARTA

- 20 years in software development and Open Source
  - Including 15 years in embedded
- PhD in Telecommunications - on network security
- Worked in embedded product development, silicon...
  - Now moved to distributions
- Guest author at LWN
- Contributing to Oniro from April 2021, consulting for OSTC
MOTIVATION FOR THIS TALK

- **Confusion** of developers not directly in the field
  - What is the difference between ARM TrustZone and AMD SEV?
  - TF-A, TF-M, what’s all that?

- **Mistrust in the community**, fear of locked-down platforms

- **Oniro** is a **distribution** for embedded and IoT
  - Multiple-OSes (Linux, Zephyr and more)
  - Various hardware platforms (small and big)
  - Interested in unified approach from the bootloader to apps
MOTIVATION FOR SECURE BOOT

- **Detect** if a device is running the expected software
- Make sure the device is running *software under control*
- Updates with **verified images**
- Encrypted images and file systems
  - If it makes sense for the use-case

All opinions here are my own
• **Whom** do you trust?
  - In “generic” PCs
  - In embedded
HISTORY: Generic PC: WHOM do you trust?

Building together a fully-connected all-scenario intelligent ecosystem
HISTORY: An embedded system: WHOM do you trust?

- Simple applications
- Rely on heavy debugging
- Application is trusted because no other choice

RTOS and applications linked together

<table>
<thead>
<tr>
<th>Processor HW (trusted)</th>
<th>MPU (option)</th>
</tr>
</thead>
</table>

Building together a fully-connected all-scenario intelligent ecosystem
SECURE BOOT SITUATION

- Multiple issues
- If malicious software runs (at the system level), can overwrite everything
DEFINITIONS 1

- **TPM (Trusted Platform Module)** – a security cryptoprocessor and a standard
  - Showed up in the news around 2007
  - Can be a separate chip, part of a chip, firmware, or software
  - Main expected use was system integrity, but includes a random number generator, can accelerate crypto algorithms
  - For more information see:
    - [https://lwn.net/Articles/674751/](https://lwn.net/Articles/674751/)
A PC with a TPM: WHOM do you trust?

- TPM can encrypt/decrypt keys (binding)
- TPM has no DMA access → can’t read memory
○ TEE (Trusted Execution Environment) – a part of a processor, protects loaded code and data (integrity and confidentiality). Different implementations exist
  - Also a GlobalPlatform specification and API (License required to view the specification)

○ OP-TEE (Open Portable Trusted Execution Environment) – an Open Source implementation of TEE, mostly for ARM TrustZone
A platform with an ARM-style TEE: WHOM do you trust?

<table>
<thead>
<tr>
<th>Applications (trusted)</th>
<th>Secure OS kernel (secure mode)</th>
<th>OS kernel (non-secure mode)</th>
<th>Applications (untrusted)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor HW (trusted)</td>
<td>Secure/non-secure mode</td>
<td>Kernel Mode (rings)</td>
<td>MMU IOMMU</td>
</tr>
</tbody>
</table>

Building together a fully-connected all-scenario intelligent ecosystem
TPM/TEE

- **Similarities**
  - Contain crypto accelerators

- **Differences**
  - TPM is typically a separate chip, TEE is inside a chip
  - TPM is hard-coded, TEE can run applications
  - TPM has small storage, TEE has bigger storage
DEFINITIONS 3

○ TF-A (Trusted Firmware-A) – a reference firmware for ARM v7 and v8 “A” platforms
  - Works next to OPTEE
  - For more information see:
    • https://trustedfirmware-a.readthedocs.io/en/latest/

○ TF-M (Trusted Firmware-M) – similar, for the “M” platforms
Intel SGX (Software Guard Extensions) – a possibility to create a specific memory region (enclave)
- Only code from the enclave can read/write it
- Including the OS kernel
- The memory may be encrypted
- For more information see:
  - https://lwn.net/Articles/786487/
  - https://lwn.net/Articles/798748/
**AMD SEV (Secure Encrypted Virtualization)** – an extension to virtualization, adds encrypted memory for a virtual machine (VM)
- Keys handled by the firmware
- The host can’t access the memory space
- For more information see:
• **Similarities**
  - All can be used to create TEE-like designs

• **Differences**
  - SGX/SEV designed to separate VMs
  - SGX/SEV do not add a separate crypto accelerator
Aiming at **unification**

**UEFI boot for x86 and EBBR for ARM**
- EBBR uses simplified UEFI

**Behind the scenes:**
- OP-TEE to store UEFI variables (work from Linaro)

**Complete root of trust up to the enclaved applications possible :)**
Building together a fully-connected all-scenario intelligent ecosystem

**LINKS**

- **Websites:**
  - https://oniroproject.org/
  - https://projects.eclipse.org/projects/oniro

- **Source code:**
  - https://booting.oniroproject.org/
Secure boot, TEEs, different OSes and more

Making sense of the trusted computing landscape in the Eclipse Oniro embedded distribution

Marta Rybczynska
FOSDEM 2022