Keys in the absence of tpm

Summary

The Trusted Platform Module (tpm) provides various cryptographic functions to secure key material and other secrets. In many cases, a device needs to protect data but does not have access to a tpm, either because it is not provided on the device, or for regulatory reasons.

The proposals in this section provide potential options for sensitive material protection on devices that do not have a hardware tpm. These include:

- firmware tpm
- Intel SGX
- ARM TrustZone
- Software

Problem Statement

Devices that are concerned with illegitimate access or changes can protect secret material using the tpm. We consider two use cases.

First, private keys. The tpm can generate both asymmetric and symmetric keys, which never leave the tpm itself. Instead, client software uses the tpm to generate the keys and sign transactions inside the tpm itself. Should the device or its storage be stolen, the private keys are not available anywhere in the clear.

Second, PCR sealing. The tpm contains Platform Configuration Registers (PCRs) which can be extended but not set, other than to reset to zero. Operating systems that know how to take advantage of PCRs, such as Linux and Windows, have each stage of the boot process, from the very beginning in hardware, measure via hashing the next stage of boot and store it in a well-known PCR. For example, the boot manager's hash normally is stored in PCR4, while the initrd's hash normally is stored in PCR9.

When one stage wants to hand off to the next stage, it first measures the next stage, stores it, and then executes the next. Firmware measures EFI and its configuration and stores it, then invokes the EFI file; EFI measures grub and its configuration and stores it, then invokes grub; grub measures initrd and kernel and cmdline and stores them, then invokes the kernel; etc.

A client can seal secret data to the current state of a client-selected set of PCRs. The tpm will not read that secret data back to any client unless the selected set of PCRs is in the exact same state.

Without a tpm, the only place to store secrets is on the disk itself.

tpm Usage in EVE

EVE uses the tpm to store the following sensitive material.

- device key: The private key that uniquely identifies a device is created inside the tpm and used to sign or decrypt messages. It never leaves the tpm.
- vault key: The asymmetric key that is used to encrypt/decrypt the user vault, i.e. the portion of storage for sensitive customer data, is stored in the tpm and sealed to the current state of PCRs.

See eve documents on github for more information on tpm usage.