Firmware TPM Driver

This document describes the firmware Trusted Platform Module (fTPM) device driver.

Introduction

This driver is a shim for firmware implemented in ARM's TrustZone environment. The driver allows programs to interact with the TPM in the same way they would interact with a hardware TPM.

Design

The driver acts as a thin layer that passes commands to and from a TPM implemented in firmware. The driver itself doesn't contain much logic and is used more like a dumb pipe between firmware and kernel/userspace.

The firmware itself is based on the following paper: https://www.microsoft.com/en-us/research/wp-content/uploads/2017/06/ftpm1.pdf

When the driver is loaded it will expose `/dev/tpmX` character devices to userspace which will enable userspace to communicate with the firmware TPM through this device.