Virtual TPM interface for Xen

Authors: Matthew Fioravante (JHUAPL), Daniel De Graaf (NSA)

This document describes the virtual Trusted Platform Module (vTPM) subsystem for Xen. The reader is assumed to have familiarity with building and installing Xen, Linux, and a basic understanding of the TPM and vTPM concepts.

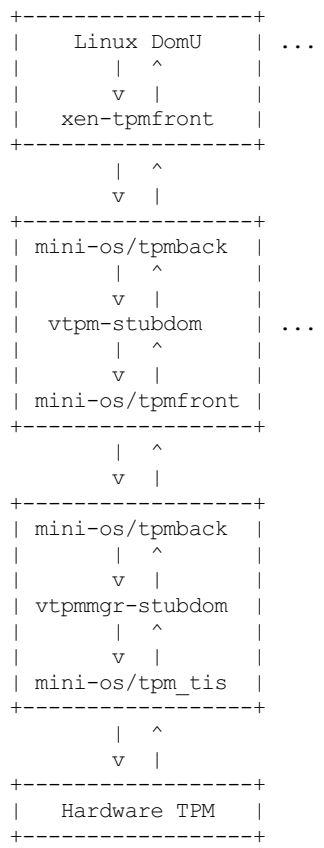
Introduction

The goal of this work is to provide a TPM functionality to a virtual guest operating system (in Xen terms, a DomU). This allows programs to interact with a TPM in a virtual system the same way they interact with a TPM on the physical system. Each guest gets its own unique, emulated, software TPM. However, each of the vTPM's secrets (Keys, NVRAM, etc) are managed by a vTPM Manager domain, which seals the secrets to the Physical TPM. If the process of creating each of these domains (manager, vTPM, and guest) is trusted, the vTPM subsystem extends the chain of trust rooted in the hardware TPM to virtual machines in Xen. Each major component of vTPM is implemented as a separate domain, providing secure separation guaranteed by the hypervisor. The vTPM domains are implemented in mini-os to reduce memory and processor overhead.

This mini-os vTPM subsystem was built on top of the previous vTPM work done by IBM and Intel corporation.

Design Overview

The architecture of vTPM is described below:



- Linux DomU:
  The Linux based guest that wants to use a vTPM. There may be more than one of these.
- xen-tpmfront.ko:
  Linux kernel virtual TPM frontend driver. This driver provides vTPM access to a Linux-based DomU.
- mini-os/tpmback:
  Mini-os TPM backend driver. The Linux frontend driver connects to this backend driver to facilitate communications between the Linux DomU and its vTPM. This driver is also used by vtpmmgr-stubdom to communicate with vtpm-stubdom.
- vtpm-stubdom:
  A mini-os stub domain that implements a vTPM. There is a one to one mapping between running vtpm-stubdom instances and logical vtpms on the system. The vTPM Platform Configuration Registers (PCRs) are normally all initialized to zero.
- mini-os/tpmfront:

Mini-os TPM frontend driver. The vTPM mini-os domain vtpm-stubdom uses this driver to communicate with vtpmmgr-stubdom. This driver is also used in mini-os domains such as pv-grub that talk to the vTPM domain.

- vtpmmgr-stubdom:
  A mini-os domain that implements the vTPM manager. There is only one vTPM manager and it should be running during the entire lifetime of the machine. This domain regulates access to the physical TPM on the system and secures the persistent state of each vTPM.
- mini-os/tpm_tis:
  Mini-os TPM version 1.2 TPM Interface Specification (TIS) driver. This driver used by vtpmmgr-stubdom to talk directly to the hardware TPM. Communication is facilitated by mapping hardware memory pages into vtpmmgr-stubdom.
- Hardware TPM:
  The physical TPM that is soldered onto the motherboard.

Integration With Xen

Support for the vTPM driver was added in Xen using the libxl toolstack in Xen 4.3. See the Xen documentation (docs/misc/vtpm.txt) for details on setting up the vTPM and vTPM Manager stub domains. Once the stub domains are running, a vTPM device is set up in the same manner as a disk or network device in the domain's configuration file.

In order to use features such as IMA that require a TPM to be loaded prior to the initrd, the xen-tpmfront driver must be compiled in to the kernel. If not using such features, the driver can be compiled as a module and will be loaded as usual.