Trusted Platform Module in Windows 11 – Walkthrough

Prepared By: Brandon Ma (30290589), Huma Naiman (30303242), Arunima Negi (30281210), Karanveer Singh (30282286)

We will discuss the Trusted Platform Module (TPM) 2.0 standard as described by the Trusted Computing Group (TCG). There is an in-depth exploration of the architecture and real-world implementations of TPM 2.0, highlighting important features that are most common in order to perform cryptographic operations that are critical to everyday tasks on Personal Computers (PC's). We'll compare and contrast firmware TPM's and dedicated TPM hardware. Within Windows 11, we demonstrate and explore how the Operating System (OS) uses TPM 2.0 hardware to enable security features like Secure Boot. An analysis of attacks against TPM will be examined and will conclude with a discussion of the implications of what this means for the future of Windows and personal computing as a whole.

Learning Outcomes

After reviewing the Teaching Aide, we expect that readers should have a solid foundation of knowledge in the following areas:

- Who TCG and why they were formed.
- What motivated the development of the TPM standard by TCG.
- The various versions of the TPM standard from TPM 1.1, TPM 1.2, and TPM 2.0.
- The shift in modern day computing to make a hardware-based Root of Trust (RoT) more common.
- How TPM 2.0 establishes trust with it's host.
- TPM 2.0's key components and features.
- The types of TPM 2.0 implementations and their use cases.
- Why the boot process needs to be protected.
- Secure Boot and Measured Boot in Windows 11.
- How Measured Boot in Windows 11 enables other security controls.
- Attacks on TPM's – TPM-FAIL and faulTPM.
- Timing side-channel and hardware-fault attack methodologies.

Using the Teaching Aide

The Teaching Aide is comprised of an information document that describes the areas mentioned below. We recommend reading this first to gain a strong understanding of the TPM 2.0 standard and its use in Windows 11's Secure Boot functionality. When completed, we have included a hands-on demo, guided by a PowerPoint presentation that explores ways in which users can interact with and see some of the information that the TPM uses.

Introduction – The Foundation of Secure Computing

Imagine turning on your computer and knowing that from the very first moment it powers up, it is protected against unauthorized tampering or malware. This is exactly what the TPM achieves. TPM 2.0 is a hardware-based standard that is embedded in modern PC's, designed to serve as the foundation of trust for system security. It ensures that your system boots securely, keeps sensitive information protected, and integrates seamlessly with your favourite applications.

What TPM Does – A Secure Vault Inside Your PC

At its core, TPM acts like a secure vault inside your computer. It safely stores cryptographic keys, measures the integrity of software and firmware, and performs other important cryptographic functions independent of the main CPU. Key features like Platform Configuration Registers (PCRs) record the system's startup state, allowing detection of unauthorized modifications. TPM's cryptographic engine generates and manages secure keys, establishing a root of trust for reliable system security.

Secure Boot and Measured Boot

TPM works together with Secure Boot and Measured Boot to form a layered defense against malware. Secure Boot ensures only trusted, signed software runs during startup, preventing malware from executing before the OS loads. Measured Boot records cryptographic hashes of every component during startup. Any deviation triggers alerts or security protocols. Together, these technologies create a chain of trust from hardware to the OS, protecting against rootkits and boot-level attacks.

Potential Threats - TPM-FAIL and faulTPM

While TPM is highly secure, researchers have discovered attacks such as TPM-FAIL and faulTPM, which exploit hardware or firmware vulnerabilities to extract secrets. These risks emphasize the importance of keeping firmware updated, enabling all security features, and avoiding untrusted hardware modifications. Understanding these threats highlights why TPM's design and implementation are critical for modern cybersecurity.

Hands-On Exploration – See the TPM in Action

For those curious to explore TPM, opening the Windows TPM management tool reveals the chip's status and capabilities. Observing Secure Boot configurations demonstrates how TPM actively protects system integrity and sensitive data. This hands-on exploration reinforces the idea that TPM 2.0 is more than a feature; it is the foundation of PC security.