Trusted Platform Module in Satellite Applications

James Minteer
Mentored by Dr. James Crabb

Background

Trusted Platform Module (TMP): TPMs were originally introduced as a component of computer systems to provide cryptographic functionalities. By being physically separate from the main processor, these functionalities could be trusted to not have been interfered with.

The most recent TPM specification, TPM 2.0 (ISO/IEC 11889:2015), outlines the following features:

- Introduction
- Certification
- Attestation & Authentication
- Protected Location
- Integrity Measurement and Reporting

Satellite Considerations: Satellites are very specialized pieces of equipment that once built and deployed, can never be physically accessed again. Due to their cost and their functionality as communications infrastructure or instruments of national security, it is important to mitigate possible threats.

Satellite Implementation

The most apparent benefit of implementing a TPM in a satellite is for trusted communication. The attestation functionality provided in a TPM integrates mitigates the ability for a malicious actor to initiate communications.

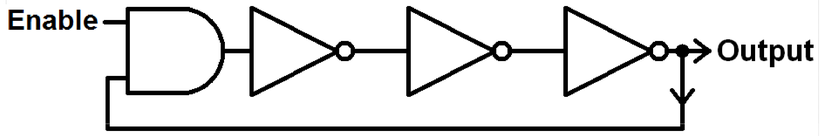

Figure 1 - Ring oscillator gate schematic

A simple example of hardware being used for attestation is a TPM utilizing a ring oscillator (RO) as part of the process instead of a value stored on the firmware or even a Platform Configuration Register (PCR), both of which might be easily available for malicious actors to access.

By characterizing the delay of the RO on the TPM, satellite operators have confidence that a hostile actor would not be able to spoof themselves as being a trusted without having either the characterization data or physical access to that very specific TPM, which is unfeasible for a satellite.

Glossary

Trusted Platform Module – A piece of hardware in a system dedicated to providing security features to a computing system.

Ring Oscillator – A logic component comprised of an odd number of NOT gates that loops back such that the output will constantly be oscillating. Due to physical variations, two different circuits with the same design could have different periods of oscillation from the delay of the gates and nets.

Platform Configuration Register – A memory location within a TPM that stores information required for validation of various operations

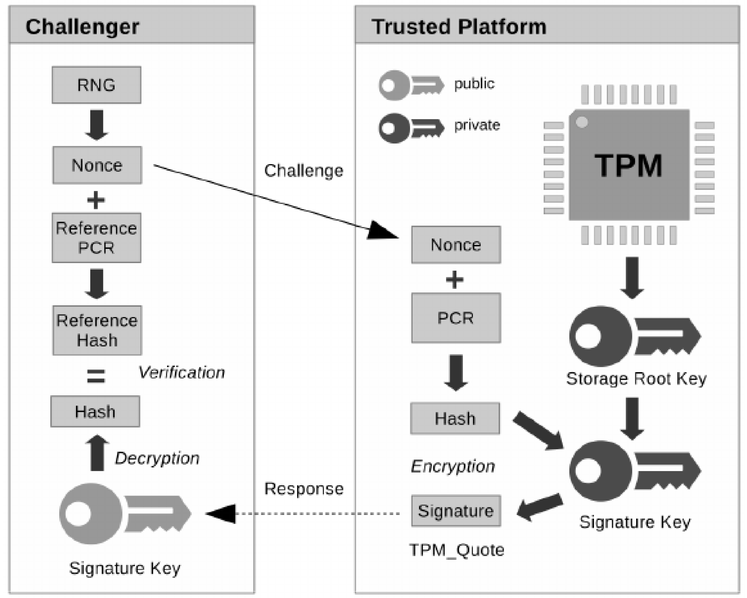

Figure 2 – Remote Attestation

References

"TCG Trusted Platform Module Library Part 1: Architecture Family '2.0' Level 00 Revision 01.59 TCG Published," 2019.

"Cyber security in the skies – protecting satellites from attack," Trusted Computing Group, Aug. 12, 2021. https://trustedcomputinggroup.org/cyber-security-in-the-skies-protecting-satellites-from-attack/

The author is grateful for funding from the Griffiss Institute under contract No. SA10012021MM0336.

Washington State University
School of Electrical Engineering and Computer Science