Trusted Platform Module explained

What it is, what it does and what its benefits are

Trusted Platform Module
Inside

Table of contents

1 Introduction

As security systems have transitioned into network devices over the last few decades, system vulnerabilities have transitioned as well. This shift in network utilization brings with it far more vulnerabilities than compared to older analog systems, and due to the very nature of networking the outer boundary of the surveillance system can be vulnerable to attack.

The ‘arteries’ of an IP system, the physical network connections, need to reach the edge components, namely the cameras, which are often mounted in exposed locations. Thus, these arteries and edge components need intensified protection.

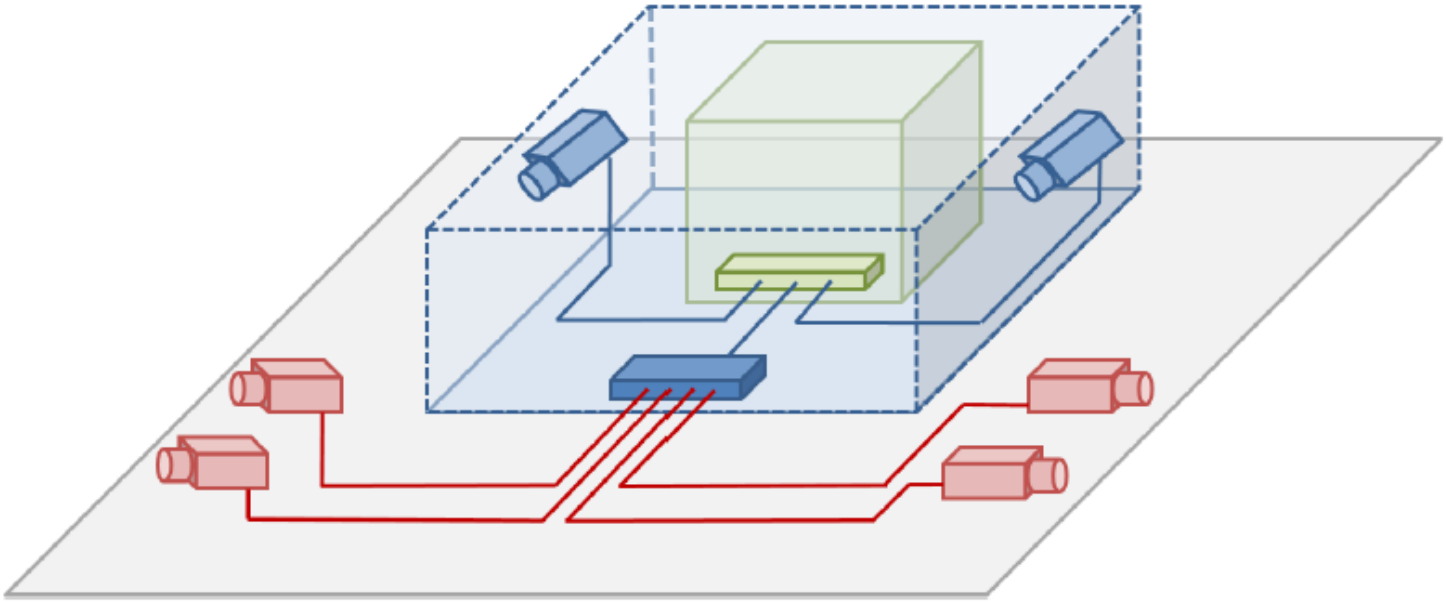

Figure 1: Vulnerability range extension

In this rough schematic, physical access control creates a security barrier, shown with the blue block and network connections, the green block resembling an even more secure access-controlled location, e.g. for servers and storage systems. Such physical access control does not apply to cameras mounted on a campus or in public areas. This network might require network access protection by implementing e.g. 802.1x.

Protecting the network and access to it is one thing, protecting access to the camera another.

2 Trusted Platform Module

In this document we focus on the 'key vault' inside a device which stores, amongst other private data, the most secret data for authentication and authenticity of a device: the Trusted Platform Module.

For years, Bosch IP cameras, encoders and selected storage systems come with an onboard security chip – actually a system-on-a-chip which we call our Trusted Platform Module (TPM) – that provides functionality similar to crypto smart cards everyone knows from daily life, like credit or debit cards. Such a Trusted Platform Module secures authenticity and acts like a safe for critical data, protecting certificates, keys, licenses, etc. against unauthorized access even when the device is physically opened to gain access.

We consider it a necessity and expect state-of-the art technology taking care about security when referring to our financial transactions in everyday life.

Why then should video surveillance equipment and assets be secured less?

The following description applies to all devices equipped with a Trusted Platform Module. For simplicity and according to the highest vulnerability level, as described in figure 1, we will refer to the device as being a camera.

2.1 What a Trusted Platform Module is

A Trusted Platform Module is a self-contained system that acts like a cryptographic coprocessor to the camera system, connected to it via a serial interface.

The Trusted Platform Module runs its own firmware which is continuously maintained to provide optimal protection against possible threats known from the market. Its firmware is only loaded in a secure production environment, not remotely like firmware for cameras. New Trusted Platform Module versions thus are only deployed with new produced cameras.

Communication between the camera firmware and the Trusted Platform Module chip happens via 'Secure Apps' inside the Trusted Platform Module. These provide the interfaces and commands for certain functionalities. There is no possibility for the firmware or operating system to modify anything inside the Trusted Platform Module directly.

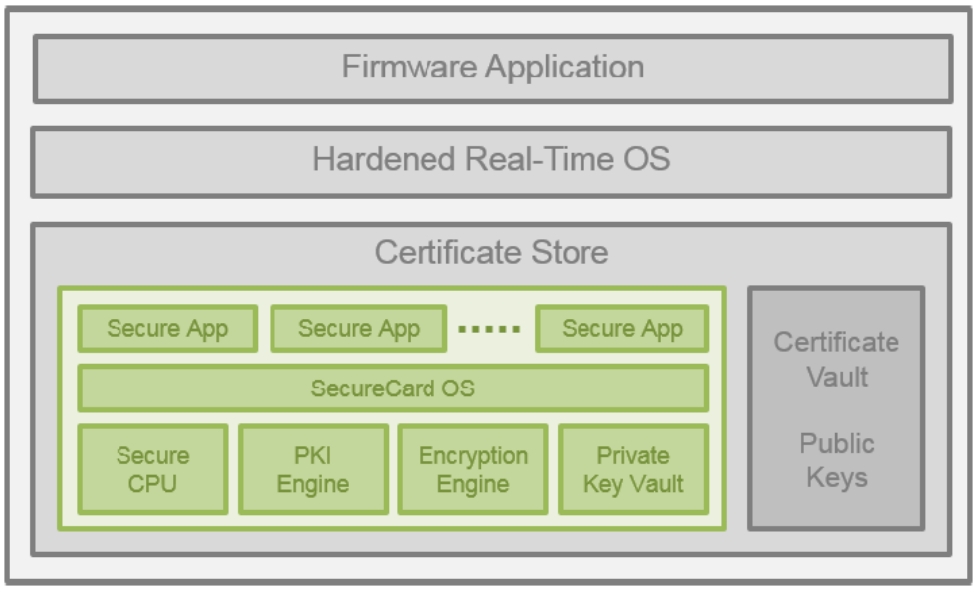

Figure 2: Block diagram of a Trusted Platform Module (green block) embedded into the camera's software architecture

The Certificate Store as functional block in the camera stores less critical data, like certificate bodies and public keys, in a dedicated memory but outside the Trusted Platform Module.

All critical cryptographic activities are handled by specific functions, called Secure Apps, which make use of the Trusted Platform Module's internal resources.

2.2 What a Trusted Platform Module does

As mentioned before, a Trusted Platform Module acts like a coprocessor to the camera system.

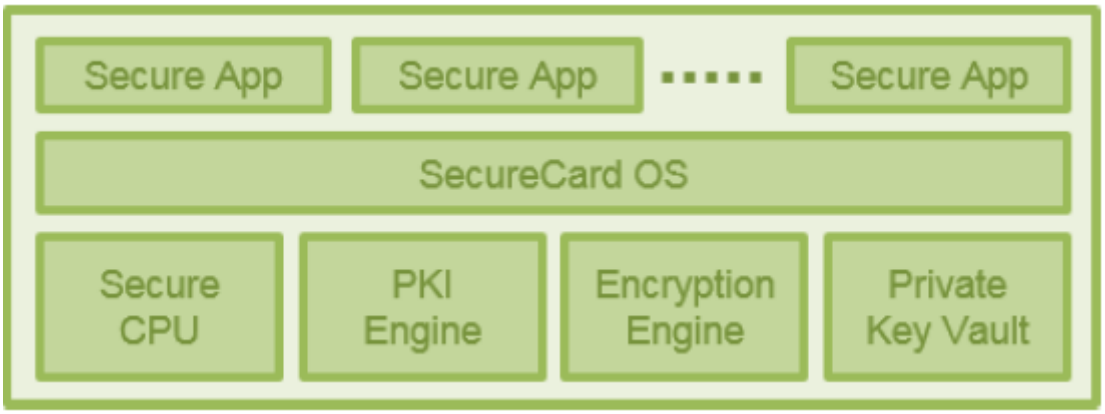

Figure 3: Schematic drawing of functional blocks inside a Trusted Platform Module

The key vault resembles some volatile and non-volatile memory to store keys and other relevant data during runtime or over power cycles, according to operational requirements.

Private keys, if loaded with a certificate, are stored inside the Trusted Platform Module and then are no longer retrievable. They can then only be used through cryptographic operations provided by the Trusted Platform Module, respectively its Secure Apps. It is recommended to password-protect the private key to keep it a secret until safe storage within the Trusted Platform Module, e.g. using PKCS #12 file format.

Private keys that result from certificate signing requests (CSR) are created internally, kept secret and never revealed to outside the Trusted Platform Module, making certificate enrollment via certificate signing requests the highest level of security.

Its encryption engine provides key handling support for symmetrical encryption like Triple DES or AES with up to 256 bit key length by calculating and producing the encryption key. Once the key is delivered, the Triple DES or AES encryption or decryption itself for video or other payload is then done by the encryption engine (hardware accelerator) in the main CPU.

The PKI engine supports in certificate validation and authentication, handling key lengths of up to 2048 bits, while the Secure CPU helps with any other cryptographic functionality like creating signed hashes for e.g. video authentication.

2.3 What a Trusted Platform Module's benefits are

A camera as the most exposed component of an IP video surveillance system faces the most threats.
Besides the many cyber threats, it can also be stolen and hacked. Such might happen as the ultimate attempt by an attacker to retrieve certificate and key to later-on simulate a camera by his own equipment, trying to hack deeper into the surveillance system, maybe even beyond.

A device, be it a camera or any other system, without a Trusted Platform Module must store private keys in its file system, where it might reside in an especially encrypted file but the key to this must also be stored somewhere in the file system.

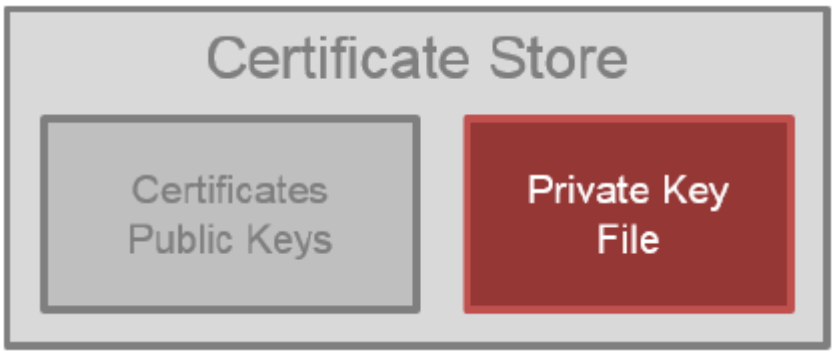

Figure 4: Device without Trusted Platform Module protection must hold private keys in file system

If hacking into a camera's certificate store does not reveal what is being looked for, a side-channel attack may do. Such an attack uses analytic hardware equipment to listen to the data bus of the system while this is performing its tasks. When triggering the authentication process, at some point, the key will appear unencrypted.
With sufficient criminal energy, time and appropriate equipment, the attacker will eventually succeed.

A compromised private key can cripple the whole Public Key Infrastructure.

Having a Trusted Platform Module integrated, no such attempt will become successful as any activities involving a private key occur only inside the Trusted Platform Module.
The Trusted Platform Module's chip technology is even protected against light and laser attacks if someone would afford to grind off the chip's housing.

3 Appendix

3.1 Standard or not standard?

Though there is an international standard for a secure cryptoprocessor, called Trusted Platform Module (TPM), the term itself is not protected. The standard, written by a computer industry consortium called Trusted Computing Group (TCG), was published as ISO/IEC 11889 in 2009 and saw its latest release of TPM 2.0 in October 2014.

The specification describes a TPM's components as secured input/output, a cryptographic processor for key and hash generation and memory for permanent and versatile key storage. It provides functions like secure generation of cryptographic keys for authentication and encryption, signed hashing (remote attestation) and sealed storage of keys.

The hardware module we call our Trusted Platform Module is based on a system-on-a-chip developed for and used in SecureID or crypto smart cards. It is compliant to the Oracle Java Card specification 3.0.1 and the GlobalPlatform Card Specification 2.1.1 from the Global Platform Consortium.
http://www.globalplatform.org

This tech note describes this our hardware module as a cryptographic processor with a secure interface, functions for generation of cryptographic keys for authentication and encryption, signed hash generation and volatile and non-volatile key storage.

Any parallelisms found?

The two approaches may have had different drivers but share common goals: Creating a platform to trust and keeping private data as secure as possible.

3.2 How clients or integrations are affected

This topic often pops up during talks about data security and Trusted Platform Modules.

Clients and 3rd party integrations do not see at all if a Trusted Platform Module is incorporated or not.

From a client standpoint, all functionality regarding certificate and key handling is provided by the Certificate Store, regardless if it is a Certificate Store of e.g. Windows OS or our firmware implementation. The Certificate Store handles it if a Trusted Platform Module exists and provides appropriate storage of keys – with the mentioned differences in the level of protection.

4 Glossary

TERM / ABBREVIATION	EXPLANATION
AES	Advanced Encryption Standard, also known as Rijndael (its original name), is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. https://en.wikipedia.org/wiki/AES
CSR	Certificate signing request. In public key infrastructure (PKI) systems, a certificate signing request (also CSR or certification request) is a message sent from an applicant to a certificate authority in order to apply for a digital identity certificate. https://en.wikipedia.org/wiki/Certificate_signing_request
Firmware	Software, that is persistently installed and provides all functionality of an embedded device.
PKCS	Public Key Cryptography Standards, a group of de facto standards devised and published by RSA Security Inc. https://en.wikipedia.org/wiki/PKCS
TPM	Module, a secure cryptographic coprocessor https://en.wikipedia.org/wiki/Trusted_Platform_Module
Triple DES (3DES)	The common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetrickey block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. https://en.wikipedia.org/wiki/Triple_DES

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com

Author: Konrad Simon, Product Manager IP Video