White paper

Signed firmware, secure boot, and TPM key storage in Axis products

November 2018

AXIS COMMUNICATIONS

Table of contents

Summary

This document covers three specific threats which malicious external adversaries may try to exploit in a system. The specific threats are firmware tampering, supply-chain tampering, and extraction of private keys. Each threat is described, including a plausible attack and how Axis latest feature development of **signed firmware, secure boot,** and **trusted platform module (TPM)** counters these threats.

The signed firmware feature is implemented by the software vendor signing the firmware image with a private key. When a firmware has this signature attached to it, a device with the feature enabled will validate the firmware before accepting to install it. If the device detects that the firmware integrity is compromised, the firmware upgrade or installation will be rejected. Axis signed firmware is based on the industry-accepted RSA public-key encryption method. The private key is stored in a closely guarded location at Axis while the public key is embedded in Axis devices.

Secure boot is a boot process that consists of an unbroken chain of cryptographically validated software, starting in immutable memory (boot ROM). Being based on the use of signed firmware, secure boot ensures that a device can boot only with authorized firmware.

A TPM is a component which provides a certain set of cryptographic features suitable for protecting information from unauthorized access. Private keys are stored in the TPM and never leave it, all cryptographic operations requiring the use of the private key are instead sent to the TPM to be processed. This ensures that the secret part of the certificate never leaves the secure environment within the TPM and remains safe even in the event of a security breach.

The TPM used in selected Axis products is certified to meet the requirements of FIPS 140-2.

1. Introduction

In a network video system, the physically most exposed components are the cameras. Often placed in distant, high-risk locations, they always face the threat of being damaged by extreme weather, tampering, or even vandalism. Luckily, there is a range of weatherproof and vandal-protected camera housings to choose from to protect a camera installation from such threats. When it comes to the threat of digital attacks, cybersecurity is all about reducing risk for data, resources, and infrastructure.

This document covers three specific threats which malicious external adversaries may try to exploit in a system. The specific threats are firmware tampering, supply-chain tampering, and extraction of private keys. Each threat is described, including a plausible attack and how Axis latest feature development of signed firmware, secure boot, and trusted platform module (TPM) counters these threats.

Many threats are related to accidental or deliberate misuse of the system by those who have legitimate access. For more information about the measures you can take to reduce the risks of common threats we refer to Axis Hardening Guide which can be found at www.axis.com/about-axis/cybersecurity

2. Firmware tamper detection

One possible attack vector that an adversary may try exploit after failing other attempts to breach the system, is to get the system owner to install altered applications, firmware, or other software modules. The altered software may include malicious code with a specific purpose. The common recommendation is to never install any software from a source that you do not fully trust. In a video system context there may be a "man in the middle" that could alter a device firmware and lure end users to install it. This is not an easy exercise and the adversary needs to be very skilled and determined. He needs low-level understanding of Axis firmware design and how the firmware operates in a device. Still, those adversaries may exist if the value of attacking a specific system is high enough. The common counter measure is for the software vendor to use signed firmware.

2.1 Firmware signing

The signed firmware feature is implemented by the software vendor signing the firmware image with a private key, which is held secret. When a firmware has this signature attached to it, a device with the feature enabled will validate the firmware before accepting to install it. If the device detects that the firmware integrity is compromised, the firmware upgrade or installation will be rejected.

The process of signing firmware (see figure 1) is initiated through the computation of a cryptographic hash value. The value is then signed with the private key of a private/public key pair before the signature is attached to the firmware image.

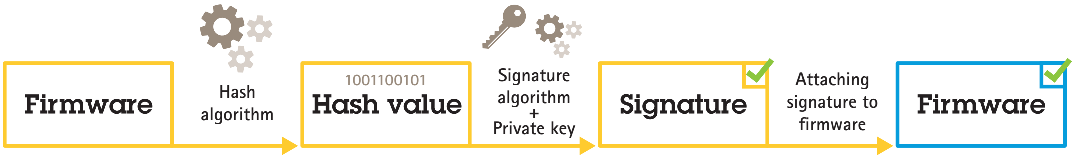
Firmware
Hash algorithm
1001100101
Hash value
Signature algorithm + Private key
Signature
Attaching signature to firmware
Firmware

Figure 1. The process of signing firmware.

Before a firmware upgrade, the new firmware must be verified. To ensure that the new firmware is unmodified, the public key (which is included with the Axis product) is used to confirm that the hash value was indeed signed with the matching private key. By also computing the hash value of the firmware and comparing it to this validated hash value from the signature, the integrity of the firmware can be verified. (see figure 2).

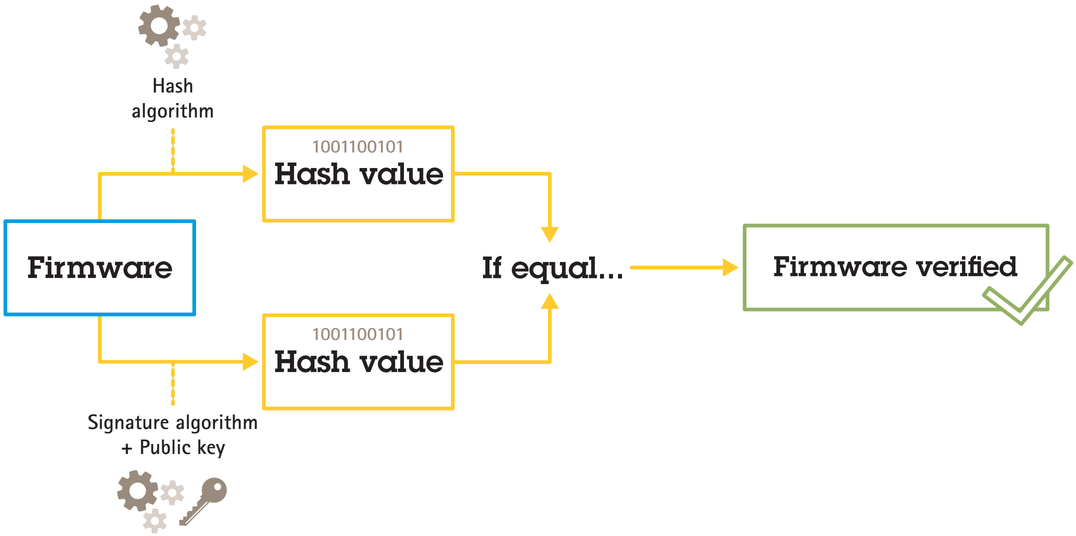

Figure 2. The process of verifying signed firmware.

2.2 Signed firmware at Axis

Axis signed firmware is based on the industry-accepted RSA public-key encryption method. The private key is stored in a closely guarded location at Axis while the public key is embedded in Axis devices. The integrity of the entire firmware image is assured by a signature of the image content. A primary signature verifies a number of secondary signatures, being verified while the image is unpacked.

3. Supply-chain tamper prevention

Firmware signing protects a device, in all future firmware updates, from installing a compromised firmware. But what if a man in the middle alters the device on its way between vendor and end user? An adversary that has physical access to the device during transit could perform an attack, such as compromising the boot partition of the device, bypassing firmware integrity checking in order to install an altered, malicious firmware before the device is deployed.

3.1 Secure boot

Secure boot is a boot process that consists of an unbroken chain of cryptographically validated software, starting in immutable memory (boot ROM). Being based on the use of signed firmware, secure boot ensures that a device can boot only with authorized firmware.

The boot process (see figure 3) is initiated by the boot ROM validating the bootloader. Secure boot then verifies, in real-time, the embedded signatures for each chunk of firmware that is loaded from the flash memory. The boot ROM serves as the root of trust, and the boot process continues only as long as each signature is verified. Every part of the chain authenticates the next part, ultimately resulting in a verified Linux kernel and a verified root file system.

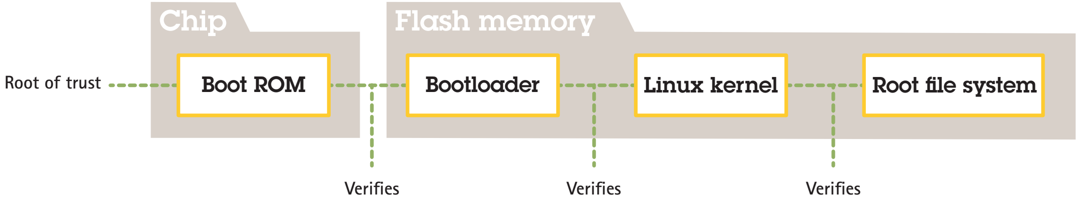

Figure 3. The secure boot process.

3.2 Axis secure boot

In many devices, it is important that the low-level functionality is impossible to alter. When other security mechanisms are built on top of the lower-level software, secure boot serves as a safe base layer that protects those mechanisms from being circumvented.

For a device with secure boot, the installed firmware in the flash memory is protected from being modified. The factory default image is protected, while the configuration remains unprotected. Secure boot guarantees that the camera is completely clean from possible malware after a factory default.

3.3 Secure boot and Custom Firmware Certificates

While secure boot makes the product safer, it does also reduce the flexibility with different firmware, making it more complicated to load any temporary firmware, such as test firmware or other custom firmware from Axis, into the product. However, Axis has implemented a mechanism that approves individual units to accept such non-production firmware. This firmware is signed in a different way, with approval by both the owner and Axis, and results in a Custom Firmware Certificate. When installed in the approved units, the certificate enables use of a custom firmware that can run only on the approved unit, based on its unique serial number and chip ID. Custom Firmware Certificates can be created only by Axis, since Axis holds the key to sign them.

4. Security of private keys

Axis devices support HTTPS (network encryption) and 802.1X (Network Access Control) which both use TLS (Transport Layer Security). The digital certificates of TLS use a public/private key pair. The private key is stored in the device while the public key is included in the certificate. Note that if neither HTTPS nor 802.1X is used, there are no keys to protect.

An adversary could try to extract the private key and the certificate from the device and install them on an attacking computer. In the case of HTTPS, that private key could be used to eavesdrop encrypted network traffic between the camera and the VMS. Or, if spoofing the network, the attacking computer could get access to the VMS by pretending to be a legitimate camera. In the case of 802.1X, the adversary could use the private key to gain access to an 802.1X-protected network, posing as a trusted camera.

Certificates and private keys are generally stored in a camera's file system, protected by the account access policy and used in the normal computing environment. In most cases this is sufficient since the account is not easily compromised. Note that certificates can be revoked if a compromise is suspected, making the private key useless.

Some end users of critical systems may experience an increased risk of determined and skilled adversaries that try to breach the camera to extract the private key. A trusted platform module (TPM) stores the key in such a way that it is close to impossible to extract it, even when the device is compromised.

4.1 Safe key storage with a TPM (trusted platform module)

A TPM is a component which provides a certain set of cryptographic features suitable for protecting information from unauthorized access. The private key is stored in the TPM and never leaves the TPM. All cryptographic operations requiring the use of the private key are sent to the TPM to be processed. This ensures that the secret part of the certificate never leaves the secure environment within the TPM and remains safe even in the event of a security breach.

4.2 FIPS 140-2 certification

For some products and use cases, it may be a regulatory requirement to use a TPM for protecting information, sometimes in combination with a requirement of FIPS 140-2 compliance. FIPS (Federal Information Processing Standard) 140-2 is an information security standard for cryptographic modules, issued in the US by NIST (National Institute of Standards and Technology).

Validation by a NIST-certified test laboratory assures that the module system and the cryptography of the module are correctly implemented. In short, the certification requires description, specification, and verification of the cryptographic module, approved algorithms, approved modes of operation, and power-up tests.

More details about the certification requirements of FIPS 140-2 can be found at the NIST website https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards

4.2.1 Certified TPM in Axis products

The TPM used in selected Axis products is certified to meet the requirements of FIPS 140-2. More specifically, it is certified to Security Level 2 of the standard, which means that the TPM also fulfills requirements for role-based operator authentication and tamper evidence, among other requirements.

72579/EN/R1/1811

About Axis Communications

Axis enables a smarter and safer world by creating network solutions that provide insights for improving security and new ways of doing business. As the industry leader in network video, Axis offers products and services for video surveillance and analytics, access control, and audio systems. Axis has more than 3,000 dedicated employees in over 50 countries and collaborates with partners worldwide to deliver customer solutions. Axis was founded in 1984 and has its headquarters in Lund, Sweden.

For more information about Axis, please visit our website www.axis.com.