Replacing Self-Signed Certificates

IDmachines

June 2025

Introduction

Cybersecurity is critical in the operation of physical security systems. Over the last 20 years, the industry has made a significant effort to address information security vulnerabilities. Despite this, today, there remain legacy systems and specifications that ignore basic security and privacy best practices and legal requirements. For example, there continue to be installed card readers and door controllers that use insecure credentials and connect insecurely[1].

Without following best practices and standards, security systems are more realistically "security theater," where there is a show of security but upon closer evaluation what has been put in place are vulnerabilities waiting to be exploited. Take the example of Internet protocol (IP) devices. Today it is required to change default passwords, to follow information security and privacy controls captured in hardening guides. Not doing so creates open-ended risks. IDmachines has long been a proponent of the use of proper cryptographic techniques in the physical security industry. These include guidance dating back to 2005[2] in coordination with the Security Industry Association, as well one of the first hardening guides for the industry in support of efforts by Axis Communications, and the first mapping to security and privacy controls[3] for Milestone Systems.

Guidance, however, is insufficient if there is no clear direction or ability to implement a solution that achieves the goals of the guidance and its objectives.

In this vein, digital certificates are critical to the cybersecurity of modern physical security systems. Over the same 20 years, there has also been explosive growth in the adoption of internet protocol (IP) security systems. This growth has been led by the vast deployment of IP surveillance cameras, in addition to door controllers, and the networks they ride on. This increases the need for suppliers of physical security systems to understand what it takes to design, integrate, operate, maintain, and retire the digital keys and certificates in physical security systems and devices.

Despite this, most organizations have not fully addressed the requirements for the proper use of digital certificates in physical security systems. This white paper highlights the reasons for this, isolates examples of where improvements can be made, and provides examples of what, and how digital certificates can be used to authenticate IP devices on physical security systems.

The use of self-signed certificates is a widespread practice in the industry and represents a common method of device authentication. Unfortunately, self-signed digital certificates have several inherent security weaknesses that make them particularly problematic for IoT devices,

[1] 125 KHz credentials have no security and are easily cloned, and the Wiegand interface between card reader and door controller sends the cardholder identifier in the clear and does not support bi-directional communications.

[2] QTU_Q405.pdf

[3] SP-800-53

physical security systems, and cameras. This white paper continues IDmachines efforts to drive industry best practices using standards-based technologies and cryptography in particular.

There are significant deployments and support by the major IP camera manufacturers for the use of 802.1x and Extensible Authentication Protocol [EAP], Remote Authentication Dial-In User Service (RADIUS) server with EAP-Transport Layer Security [TLS] authentication. These are primarily in large enterprise and government environments.

This whitepaper addresses alternatives to self-signed certificates and does not look to change or downplay 802.1x support.

Self-Signed Certificate Deficiencies

Self-signed certificate deficiencies have been called out in several important frameworks and regulations. These include the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST), the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), the Health Information Portability and Accountability Act (HIPAA), and the CA Browser Forum.

No Third-Party Validation

Self-signed certificates are not validated by a trusted Certificate Authority (CA), meaning there is no independent verification of the certificate holder's identity. This creates a fundamental trust problem. Furthermore, there is no differentiation in policy among different cameras. Particularly with the expanding use of video analytics and machine learning, and the ability for video surveillance cameras to classify and identify individuals. It is important that certificates contain accurate locations, purpose, and justification for automated processing, as well as the related capabilities and metadata generated. These details help to further ascertain certificate validity.

No Revocation Mechanism:

Unlike CA-issued certificates, self-signed certificates do not provide standard revocation mechanisms like Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP). This means there is limited ability to determine the validity of the certificates, a common characteristic of certificate and device related vulnerabilities. It also means there is no way to manage device authentication privileges, and certainly not to any degree of fine grain.

Weak Key Management

Many IoT devices use the same self-signed certificate across multiple devices. There are examples where the generation of weak certificates with predictable patterns or insufficient entropy, improper ciphers, and predictable identifiers have contributed to compromises. Strong implementations take advantage of trusted platform modules or environment on the device or a secure access module. In addition, there is no differentiation among self-signed certificates and an inability to enforce any granularity in policy regarding device functionality and other security and privacy controls.

Certificate Persistence

Self-signed certificates often remain valid indefinitely without rotation, creating long-term attack vectors. This is counter to the current, evolving, and prevailing policy for certificate lifespans. The CA Browser forum has recently passed a requirement that all SSL certificates should last for no more than forty-seven days starting in 2029.

Common Vulnerabilities and Exploits

Man-in-the-Middle (MITM) Attacks

Attackers can easily intercept communications by presenting their own self-signed certificate. Since users typically ignore certificate warnings, this attack often succeeds undetected. This involves simply copying the information into a self-signed certificate and then using an open-source tool such as Open-SSL to issue a fraudulent copy. This is enabled by the lack of an intermediary in determining certificate validity.

Certificate Spoofing

This is the most referred to exploit regarding self-signed certificates, enabling MITM attacks. Malicious actors can create certificates that appear legitimate to unsuspecting users, particularly effective against devices that do not properly validate certificate chains. This is because self-signed certificates often have limited variation in the subject identifier, subject alternative names, and other certificate fields. This also involves certificate object identifiers (OIDs), and the policy and endpoints associated with effectively managing and issuing certificates. For example, the Certificate Practice Statement (CPS) is effectively the security and privacy policy for the device's use. This should provide links and additional information that makes spoofing more difficult.

Weak Cryptographic Implementation

Many IoT manufacturers implement poor random number generation or use deprecated algorithms, making certificates vulnerable to cryptographic attacks. In some cases, weak cipher suites and algorithms are employed such as MD5 and SHA-1, which are susceptible to brute force attacks.

IoT and Security System Vulnerability Examples

IP Camera Vulnerabilities

IP camera manufacturers have continued to improve the cybersecurity of their products and address vulnerabilities that have continued to arise. Many of the vulnerabilities have been associated with Chinese camera that have been attractive and widely deployed based on their price-performance. The most significant example of this was the Mirai botnet in 2016 that continues to have impacts to this day.

Fortunately, these vulnerabilities are not common with major non-Chinese vendors such as Axis and Hanwha. Having a CVE in and of itself is not an unusual occurrence. Most of the major vendors pride themselves and have taken vulnerability reporting very seriously. This has been critical to avoid exploits turning into zero-day attacks when they go unrecognized. These can also affect other IP devices, such as door controllers.

Nonetheless, Axis, Hanwha and many surveillance cameras use identical self-signed certificates across product lines. Researchers have discovered cameras where the same certificate and private key were embedded in firmware for thousands of devices, allowing attackers to decrypt any traffic from these cameras. In some ways this is another version of using the same username and password to varying degrees. The following are some examples of attacks and vulnerabilities that have been documented over the last decade, as well as a listing of some related attacks on physical security systems.

Number	Vendor	Vulnerability
CVE-2017-2871	Foscam C1 Indoor HD Camera	Insufficient security checks.
CVE-2017-7921	Hikvision (multiple devices)	Insufficient authentication mechanisms
CVE-2017-8221	WIFIcam (Chinese OEM)	Botnet
CVE-2017-8222	WIFIcam (Chinese OEM)	Improper RSA key and certificate
CVE-2017-8223	WIFIcam (Chinese OEM)	Streaming without authentication
CVE-2017-8224	WIFIcam (Chinese OEM)	Backdoor account
CVE-2017-8225	WIFIcam (Chinese OEM)	Credential leakage, remote code execution authenticated as root
CVE-2018-12449	Motorola MBP853	Incorrectly validates server certificate
CVE-2019-5037	Nest Cam IQ	Improper Weave certificate loading
CVE-2019-7728	Bosch Smart Camera App	Improper TLS certificate checks
CVE-2019-11219	Shenzhen Yunni Technology iLnkP2P	Weak UID generation
CVE-2019-11220	Shenzhen Yunni Technology iLnkP2P	Authentication flaws
CVE-2020-6852	CACAGOO Cloud Storage Intelligent Camera TV-288ZD-2MP	Weak authentication of TELNET
CVE-2020-9525	CS2 Network P2P	Authentication flaws
CVE-2020-9526	CS2 Network P2P	Authentication flaws
CVE-2021-28372	ThroughTek's Kalay Platform 2.0	UID impersonation
CVE-2022-30563	Dahua	ONVIF man-in-the-middle
CVE-2022-31481	Mercury door controller	Unauthenticated user file injection
CVE-2023-6321	Logback receiver	Serialization vulnerability
CVE-2023-6324	ThroughTek Kalay SDK	Pre-shared key
CVE-2024-2466	Siemens SINEC NMS	libcurl did not check the server certificate of TLS connections
CVE-2024-7029	AVTECH IP Cameras	Command injection attack
CVE-2025-23118	UniFi Protech	Improper validation
CVE-2025-30184	CyberData 011209 SIP Emergency Intercom	Authentication bypass
CVE-2025-49851	ControlID IDSecure	Authentication bypass

Other Related Vulnerabilities

The vulnerabilities resulting from self-signed certificates have been documented across physical security, IoT, and industry control systems. Here are some examples:

Smart Door Locks

Some electronic locks use self-signed certificates for their mobile app communications. Attackers can perform MITM attacks to capture unlock codes or create unauthorized access credentials. One example from 2019 of a hard-coded key in CVE-2019-7098 with August Smart Lock Pro and the associated wi-fi bridge, its application programming interface and with certificate pinning. Another example is the case of Nuki Smart locks lacking certificate validation in CVE-2022-32509.

Industrial Control Systems

SCADA systems and industrial IoT devices often rely on self-signed certificates for their web interfaces. This has led to successful attacks where operators unknowingly connected to malicious interfaces that appeared legitimate. Many of these exploits and vulnerabilities exploit the same issue that exists with self-signed certificates with physical security devices. Examples include Schneider Electric Modicon programmable logic controllers. The Stuxnet attack exploited stolen certificates, also targeting the takeover of programmable logic controllers and industrial control systems.

Network Video Recorders (NVRs)

The exploits and vulnerabilities are not restricted to IP cameras. The vulnerabilities and exploits described here exist across physical security systems. Examples noted in the CVEs listed above for Hikvision. In one case, NVR systems contained self-signed certificates with hardcoded credentials or exposed administrative interfaces to unauthorized access.

Mitigation Strategies

The most effective approach is implementing proper certificate management using trusted CAs, even for internal systems. This includes certificate rotation policies, proper key generation with sufficient entropy, and implementing certificate pinning where appropriate. For existing systems, network segmentation and additional authentication layers can help reduce exposure while planning certificate infrastructure upgrades. These actions complement those outlined in the manufacturer's hardening guides.

The combination of weak authentication, poor key management, and user tendency to ignore certificate warnings makes self-signed certificates particularly dangerous in IoT and security applications where compromise can have serious physical world consequences.

IDmachines' Certificate Services

IDmachines' Eidola platform uses open-source standards-based tools to manage the lifecycle of physical security devices. We design and work with key management systems that support public key infrastructure (PKI) and certificate authorities. We have crafted profiles that include the use of different categories of analytics and also adaptation to customer certificate capabilities and systems. This extends the use cases supported by the Eidola platform to include not only determining whether certificates have been properly issued and use sound cryptography, but also to issue and manage the certificates as well. As part of the service, IDmachines offers a white hat identity, security, surveillance, and privacy risk (WHISSPR) assessment service. This method employs international standards and frameworks that include National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) cybersecurity and privacy frameworks and controls and maps them to the legal frameworks applicable to the organization in its jurisdictions, and for the specific purpose and justification of identifying individuals and the creation of identifiers and personally identifiable information (PII).

Customer organizations are enrolled in a registry and provided with a PII Controller credential that addresses industry, local, regional, national, and international security, and privacy requirements. The registry is also used as the Registration Authority (RA) for the creation of an organization's PKI that can issue device certificates. This can also be used to establish endpoints for certificates and system policies, notifications, signs, and signaling.

Other Links and references (see also footnotes)

The Danger of Self-Signed Certificates

Security Analysis of the August Smart Lock

How cybercrime exploits digital certificates

Axis OS Hardening Guide

Recommended cybersecurity policies for deploying and managing a Milestone and Axis system

Hanwha Hardening Guide

CA Browser Forum

Baseline TLS RequirementsGeneral Data rotection Regulation

Digital Operational Resilience Act (DORA)

EU Act language

Security and Exchange Commission

Payment Card Industry Data Security Standard (PCI DSS)

Document library

European Union

General Data Protection Regulation

Convention 108+

International Organization for Standardization

ISO/IEC 29100:2024 - Information technology — Security techniques — Privacy framework

National Institute of Standards and Technology

Cybersecurity Framework | NIST

NIST Privacy Framework

NIST SP 800-53 Revision 5

NIST SP 800-213, IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements