Cybersecurity with Automated Certificate and Password Management for Surveillance

May 2017

ABSTRACT

This reference architecture guide describes the reference architecture of a validated solution to deploy and manage cybersecurity using automated certificate management for surveillance cameras.

H15980.1

This document is not intended for audiences in China, Hong Kong, and Taiwan.

Copyright

Contents

Executive summary

Business case

Most video surveillance deployments lack sufficient cybersecurity measures, which makes them an attractive target to hackers who run distributed denial of service (DDoS) attacks.

The Mirai botnet attack in October 2016 is a good example. Mirai is a type of malware that changes Linux computer systems into remotely controlled "bots," or web robots. These bots can be used to flood a target host or resource with requests in an attempt to disrupt legitimate traffic. The 2016 attack took down or slowed well-known websites including Twitter, PayPal, Spotify, Reddit, and many others. Many viewed it as a test for potential future attacks that could threaten safety and cause significant financial impact to businesses.

In the video surveillance marketplace, security has long been the responsibility of the end customer. However, businesses have recently begun demanding that system integrators, architects, consultants, and engineers address cybersecurity as part of the solutions that they design and deploy. Businesses need improved cybersecurity for surveillance cameras to help prevent third parties from gaining remote access to cameras and enabling them to launch DDoS attacks that expose businesses to potential future liability claims.

X.509 certificates, which have been used for more than 20 years, are a well-known and trusted way of authenticating devices. Most IT environments use them in networked computers, servers, printers, and so on, to prevent third parties from compromising systems. The role of the X.509 certificate is to associate a public key with the identity that is contained in the certificate. Unfortunately, because of the cost and complexity, most companies do not provision cameras and video management software (VMS) servers with certificates when deploying video surveillance systems.

One vulnerability that hackers use to gain access to remote devices is through default user names and passwords that are never changed. Despite efforts by manufactures to educate customers, many still do not take the time to create and deploy unique credentials. When they do, they often create one username and password for all cameras and do not update these credentials when an admin employee leaves. These unchanged credentials are an increasing cyber security risk that exposes companies and their networks to malicious attacks.

Solution overview

This solution enables customers to install a complete end-to-end video surveillance solution that automatically establishes a unique root of trust to securely authenticate Axis Communications IP cameras to Milestone Systems XProtect® VMS. The solution uses products from Dell EMC OEM partners Device Authority and Seneca. These partner products specifically address the challenge of automating the deployment of certificates, authenticating them to the VMS, and creating a secure communications channel for all devices in the security surveillance fabric.

Key benefits

This solution provides the following key benefits:

- **Simplicity**—Deploying x.509 certificates to manually provision cameras can take up to 3 minutes per camera for experienced technicians. This reference architecture automates the entire process and enables customers to deploy certificates to devices and systems in under 30 seconds. This task can be performed on all devices in parallel.

  Automated Admin Password Management eliminates the requirement for users to create and manage passwords across devices.

- **Security**—Device registration ensures that only trusted devices can enroll with the Device Authority KeyScaler™ platform and communicate with other trusted devices and servers in the ecosystem. This registration prevents unauthorized access to customer networks and ensures that only trusted devices can connect to the Axis cameras and the Milestone VMS.

- **Scalability**—In addition to simplifying the security deployment, this solution provides extremely high scalability—from 10 cameras or devices to 100,000 cameras or devices.

- **Flexibility**—Device Authority provides increased automation and operational efficiencies by enabling customers to schedule the rotation of certificates, which increases the existing security posture.

Document purpose

This document describes the reference architecture of a validated solution to deploy and manage cybersecurity using automated certificate management for surveillance cameras.

We value your feedback

Dell EMC and the authors of this document welcome your feedback on the solution and the solution documentation. Contact EMC.Solution.Feedback@emc.com with your comments.

Authors: Ken Mills, John Holleran, John Pratt, Larry Mann

Solution architecture

The Automated Certificate and Password management architecture provides rapid customer-centric certificate generation and provisioning for video surveillance systems, including automated certificate lifecycle management with revocation and renewal. KeyScaler enables hands-free bulk provisioning for large-scale deployments, and it removes the associated logistical challenges, enabling efficient deployment of video surveillance systems.

On setting a Certificate and Password policy in Device Authority's control panel, the following steps show how to automatically provision certificates:

1. The Device Authority agent on the Axis camera connects to the KeyScaler server for secure device registration, as shown in Figure 1.

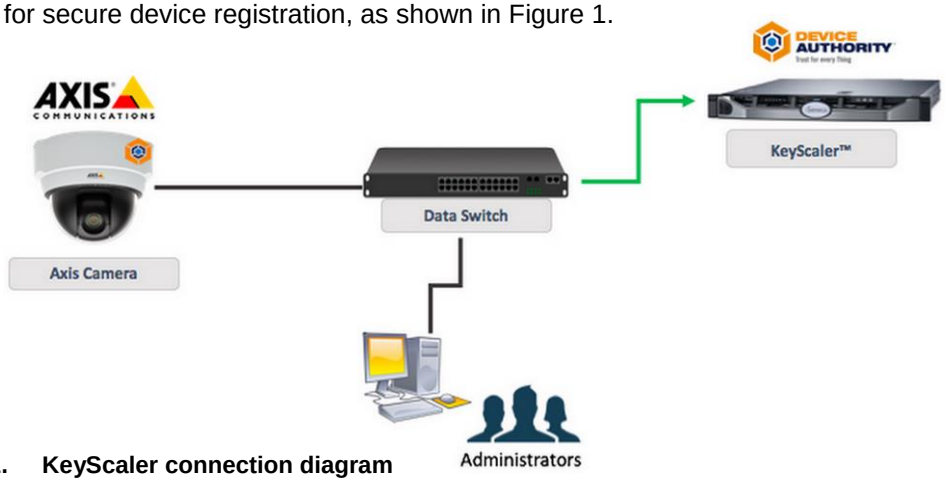

Figure 1. KeyScaler connection diagram

2. The KeyScaler system automatically generates a certificate and connects to the certificate authority to request a signature, as shown in Figure 2.

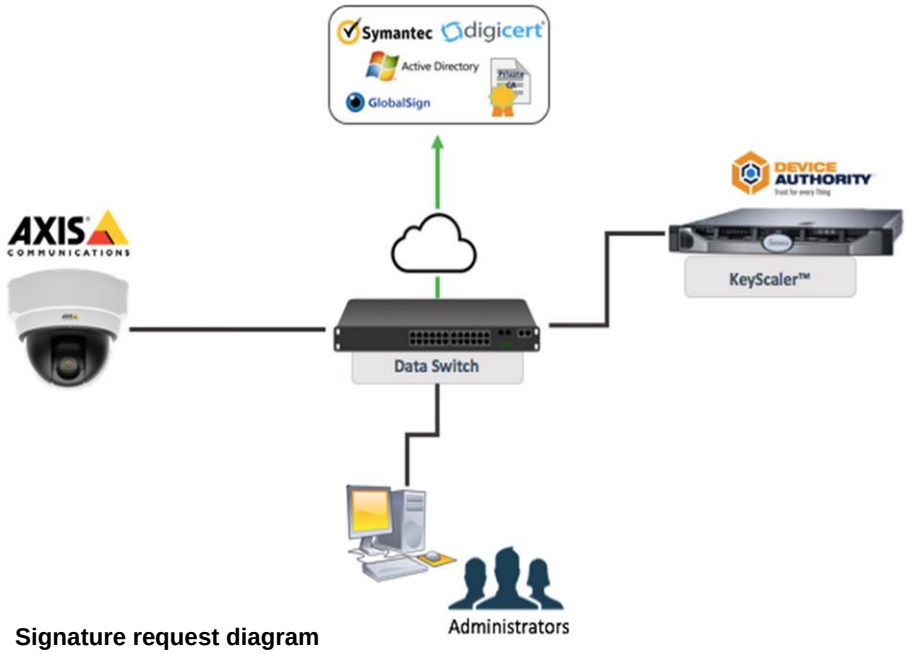

Figure 2. Signature request diagram

3. A unique certificate, signed by the certificate authority, is delivered to the camera and stored as an encrypted file on persistent storage, as shown in Figure 3.

   Default Passwords for the Root and user accounts are changed and managed per the policy.

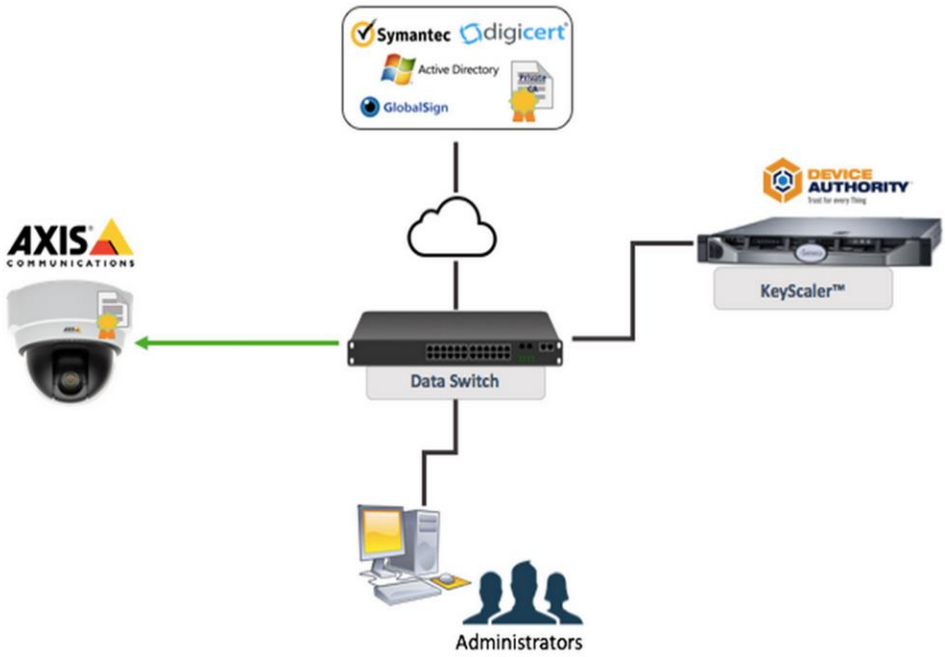

Figure 3. Camera certificate diagram

4. The Milestone XProtect system completes the same secure registration process with the KeyScaler server and receives its own unique certificate, as shown in Figure 4.

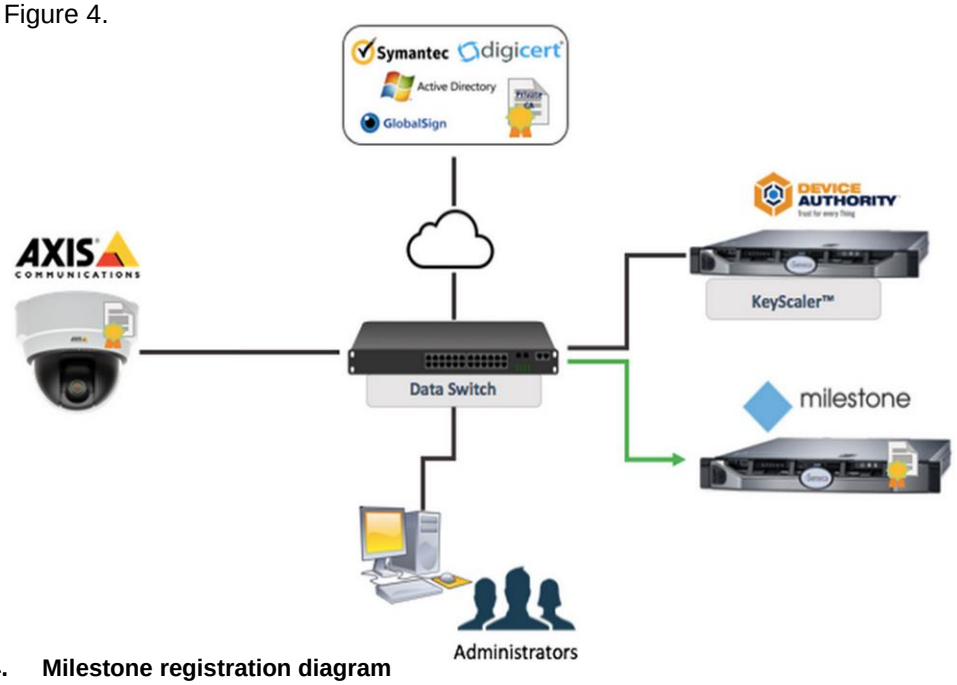

Figure 4. Milestone registration diagram

5. Seneca xConnect® software monitors uptime and system health of all components within this reference architecture, as shown in Figure 5.

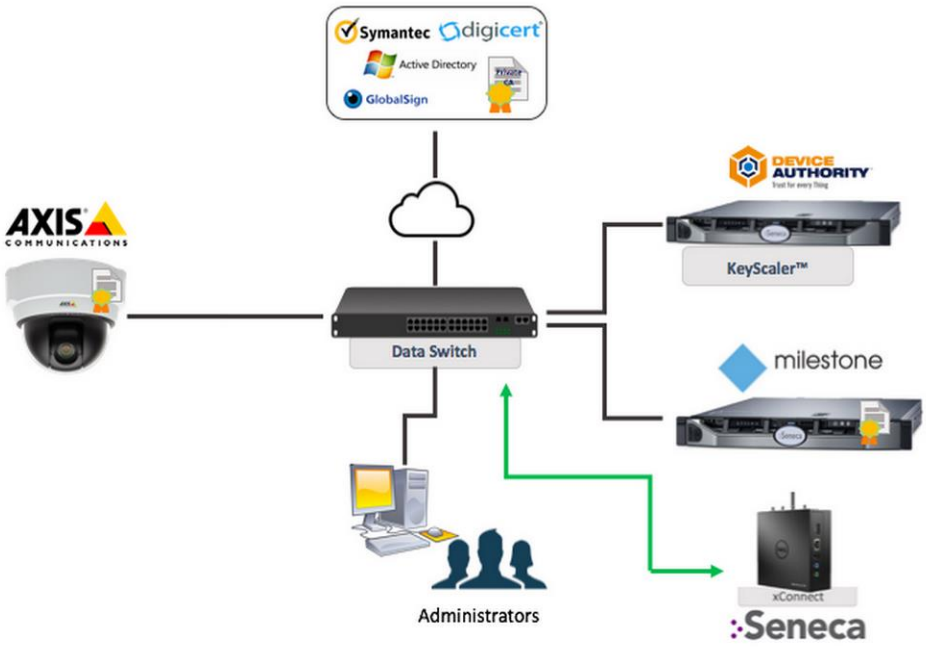

Figure 5. Seneca xConnect monitor diagram

Key components

Dell PowerEdge and Dell OpenManage

Dell PowerEdge™ servers provide several levels of inherent security. A digitally signed BIOS ensures that disks, memory, and processors include digital signatures that disable compromised components and prevent malicious content. In addition to having a digitally signed BIOS, PowerEdge servers include digitally signed firmware and driver files, further ensuring that attackers cannot compromise systems during routine maintenance and upgrade cycles. Dell OpenManage™ Server Configuration Manager enables administrators to create a template of a server configuration and receive an alert when configuration drift causes changes to the hardware, BIOS settings, and RAID configurations. Configuration drift occurs when hardware and software configurations become different from a secondary or recovery configuration, which often causes disaster recovery and high-availability systems to fail.

Dell OpenManage software provides robust performance monitoring and alerts to power or thermal events and drive failures. PowerEdge includes an integrated Dell Remote Access Controller (iDRAC), which provides external access to each server, with direct access to view performance, allow remote configuration, and deploy the OS. This capability significantly reduces the cost of support for integrators by reducing the need to send technicians to a customer environment to resolve issues.

Seneca xConnect

Seneca assists surveillance customers by completing many complex and time-consuming deployment tasks, such as creating RAID containers and automating the installation of the preferred VMS. This solution employs Seneca xConnect monitoring software to capture alerts for all solution components, including cameras, VMS, compute, and storage elements. xConnect will soon include remote monitoring capabilities that work with Dell Edge Gateway 5000 Series systems. It will provide local alerts in a decentralized solution, while also having centralized visibility by consolidating monitoring in a distributed architecture.

Axis and Milestone both provide hardening guidelines that are specific to their products, including important steps that integrators and installers must take before they begin the deployment process. They can perform these steps on isolated networks to further minimize any infrastructure vulnerabilities that might exist. Axis also provides configuration utilities to assist in configuring Axis cameras.

Device Authority KeyScaler

The Device Authority KeyScaler security platform uses a unique device-centric trust anchor to securely register devices. When devices are registered, KeyScaler can provision, revoke, and renew certificates at scale. The process to deploy a certificate can take from 3 to 5 minutes per camera, making certificate management a complex and time-consuming process, especially for large deployments. The KeyScaler platform automates this process, reducing the time from days to minutes. While this process greatly reduces deployment times and costs, it also provides certificate rotation on a customer-definable schedule, such as daily, weekly, or monthly.

The KeyScaler platform also has built-in, automated integrity checks that can detect suspicious devices and prevent them from participating in the ecosystem by revoking

certificates and other credentials that are associated with potentially malicious devices. KeyScaler automatically quarantines new devices, preventing them from running malicious content. It scans all quarantined devices, deploying an agent and provisioning a certificate when the device is validated by unique identifiers that are configured in the system. If a device is quarantined, it stays quarantined and generates alerts to the system administrator.

Axis

Axis' Intelligent Video, Audio, and Access Control solutions use the latest generation of Axis' purpose build ARTPEC processors to enable robust onboard client and application programs via the Axis Camera Application Platform (ACAP) and Axis' own open API called VAPIX. These platforms enable Axis Application Development and Technology Partner Program members to develop added functionalities and applications, which can then be installed on Axis network cameras and video encoders. Axis' open architecture intelligent interfaces enable the highest level of smart technology including next generation cyber security.

Milestone Systems

Milestone Systems is a global industry leader in open platform IP video management software, founded in 1998 and now operating as a stand-alone company in the Canon Group. Milestone technology is reliable, easy to manage, and proven in thousands of customer installations, providing flexible choices in network hardware and integrations with other systems. Sold through partners in more than 100 countries, Milestone video solutions help organizations to manage risks, protect people and assets, optimize processes and reduce costs. For more information, see: www.milestonesys.com. For news and viewpoints from the Milestone universe, go to http://news.milestonesys.com/ or follow @MilestoneSys on Twitter.

Security requirements

The following requirements are necessary for security:

- Use unique and complex local-device user passwords for Secure Shell (SSH) remote access.
- Ensure that security events are logged and audited from all devices within the environment.
- Use a secure certificate authority as a source repository for keys for the camera and Milestone system to prevent cloning, spoofing, and man-in-the-middle attacks.
- Use the Device Authority platform to create a device-derived dynamic crypto key that is not stored on cameras or servers and is never passed over the network. This functionality helps to minimize security issues that are related to shared keys and also enhances operational efficiency.
- Configure Axis cameras on the isolated network according to the *Axis Hardening Guide*.

References

Dell documentation and downloads

The following documentation on the Dell website provides additional and relevant information. Access to the Dell SalesEdge documents requires a login. If you do not have access to a document, contact your Dell EMC representative.

Dell OpenManage documentation and downloads

- *OpenManage Essentials* (Dell TechCenter Systems Management wiki)
- OpenManage Essentials systems management software and download page
- *OpenManage Mobile* (Dell TechCenter Systems Management wiki)
- Dell OpenManage Mobile Android download page (Google Play)
- OpenManage Mobile download page (iTunes Preview)

Axis documentation

The following documentation on the Axis website provides additional and relevant information:

- *Axis Hardening Guide*

Milestone documentation

The following documentation on the Milestone website provides additional and relevant information:

- *Milestone Systems Hardening Guide*