Hackers hijack data communications between camera and video management systems for illicit means

# DATA PROTECTION FOR SECURITY CAMERAS

**Kiran Pillai** *reports on why a systematic approach to data security needs to cover both physical safety and cyber security simultaneously*

**Security cameras, alarm systems, smart building automation: the number of connected devices on the Internet of Things (IoT) is rising at an unprecedented rate. In 2018, the worldwide installed base of IoT devices will reach 23.1 billion units (Statista). This marks a significant increase from 17.6 billion IoT devices in 2016, while industry insiders expect the number to surpass 30.7 billion connected devices by 2020 and 75.4 billion by 2025.**

In this era of hyper-connected devices, security cameras are no longer just 'eyes' capturing images in important areas. Today's networked IP-cameras are equipped with built-in video analytics capabilities that add context, structure, and automated alarms to video feeds. And make no mistake, these intelligent security cameras are not 'cutting edge' future developments – but already key components in today's digital connectivity infrastructure. Their ability to blend high-resolution video images with smart sensor data (metadata) makes them a top choice for applications like airports, railway, metro, Intelligent Transportation Systems, city surveillance, retail, commercial buildings, banking and industrial sites.

Safeguarding these often sensitive areas comes with great responsibility, not only on a physical but also a cyber security level. As video security data from edge components (cameras) is increasingly sent across local and global networks to core components (servers), a new generation of cyber criminals has set out to explore vulnerabilities. Recent numbers are alarming: According to the Official 2017 Annual Cybercrime Report, the estimated cost of cyber crime damages will reach $6 trillion annually worldwide by 2021 while the increasing number of IoT devices opens new loopholes for hackers.

Security camera data – both in private homes and commercial as well as public spaces – is especially interesting to cyber criminals, reflected by a growing number of exploits including so-called man-in-the-middle attacks: hackers hijack communications between a camera and video management system (VMS) in order to spy on people or industrial processes, inject alternate video image feeds to conceal illicit activity or manipulate live camera footage to selectively remove details or persons from the scene. A recent report found thousands of security cameras in the US vulnerable to hacking, including business operations such as warehouses, industrial buildings, and retail stores.

Aside from attacks on live video feeds, stored security camera data also presents an attractive target. In June 2015, an Italian-based developer of Government-level surveillance software became the victim of a major breach, leaking 400 gigabytes of sensitive client data onto the internet. In 2016, hackers seized control of over 25,000 CCTV cameras and digital video recorders to create a botnet that carried out attacks against websites.

> THE ESTIMATED COST OF CYBER CRIME WILL REACH $6 TRILLION ANNUALLY WORLDWIDE BY 2021

Spectacular cases like this are powerful reminders: one single weak link in a communications infrastructure is enough to give hackers access to sensitive data.

Closing these exploitable loopholes extends the focus of security from the physical level into the digital domain. Unfortunately, the majority of businesses operating Internet of Things devices will only increase their security budgets in this segment under worst-case conditions: 54 percent of IT professionals in North America will raise security spending for IOT device protection after a "serious hacking incident" affecting their organisation, while only 10 percent will act out of "concern over potential loss of customers due to a security incident".

Minimising the effect of these types of worst-case security breaches has become the focus for leading systems providers in our industry. The challenge of offering clients the highest level of data security in their video security applications involves every single product a company brings to market. Because video data is often highly critical and sensitive, the way forward lies in driving a systematic approach to protect private data from intruders by considering physical safety and cyber security simultaneously.

This systematic approach starts by considering the entire security camera infrastructure as a whole, not just individual components. In order to minimise the risk of hacking, firmware needs to be constantly updated to address the latest potential threats and vulnerabilities. Encryption of data streams is vital and technologies such as SRTP (Secure Real-Time Transport Protocol) are emerging as the industry's choice to leave no access points for hackers.

At Bosch, for example, all video data is encrypted at the camera level, using a cryptographic key that is safely stored in an unique built-in Trusted Platform Module (TPM). Making sure that only authorised individuals have access to video data, companies need to ensure privacy by diligently managing user access rights on their Video Management Software (VMS). In an ideal world, these data sets on user permissions also synchronise with customer-owned user data bases via interfaces such as Active Directory. And as a benchmark quality standard, current generation video security solutions can support the set up of a Public Key Infrastructure.

Operators need to adopt a systematic approach as the key to achieving the highest standards in data security by covering the following four areas: hardware, network, data and public key infrastructure.

## HARDWARE: SECURING VIDEO DATA

Even a single camera can provide a gateway to hackers, potentially exposing entire networks to cyber crime. So a comprehensive data security approach starts with encrypting data at the hardware level. State-of-the-art IP-cameras feature a built-in Trusted Platform Module (TPM) to safely store cryptographic keys. All cryptographic operations for authentication and encryption are executed inside the TPM. Today's security cameras support encrypted data to be sent via a secured connection using SRTP (Secure Real-Time Transport Protocol). As an additional layer of security to prevent malware infections, cameras only allow firmware files signed by the manufacturer to be uploaded and execution of third-party software is disabled.

## NETWORK: AUTHENTICATION

Modern video security platforms can create trust by assigning every component in the network an authentication key to allow only trusted devices to share data. This certificate-based authentication avoids man-in-the-middle attacks, as only authentic devices are allowed to communicate. Network authentication relies on the industry-standard 802.1x protocol. Operators need to look out for security cameras that support the Advance Encryption Standard (up to 256 bit keys for encryption) and set-up of a Public Key Infrastructure. Unsecure ports, such as Universal Plug and Play, should be disabled by default. Password enforcement at initial setup of a new camera offers a first level of defence, as manufacturer-set passwords in internet-connected devices are known to hackers and a major loophole. Ideally, a camera should offer a built-in firewall to eliminate loopholes from hackers that are 'guessing' passwords.

## DATA: MANAGING ACCESS RIGHTS

Aside from technological vulnerabilities, humans are the biggest cause of security breaches, named by 85 percent of hackers as the main culprit. That's why leading video management systems offer easy ways to manage user access rights, including the support of Microsoft Active Directory, ensuring that only authorised people have access to video data. This level of 'permissioning' should be scalable and offer granular

▶

controls to operators. As an example and depending on system set up, access can be limited to specific users or user groups, while system administrators can choose from a set of over 300 privileges that can be assigned.

## PUBLIC KEY INFRASTRUCTURE

In this era of hyper-connected devices, data security becomes a community effort. The most advanced hardware manufacturers ship their cameras factory-loaded with proprietary signed digital certificates that are used for authentication of devices and encryption of video data. Alternatively, operators can choose architectures in which customer-specific certificates can be uploaded – or a combination of both. Next to that, several manufacturers support the set up of a Public Key Infrastructure for the management of digital certificates. After years of development, Bosch offers its own PKI solutions with in-house Certification Authority (CA) Escrypt and also supports third-party PKI solutions in its cameras.

Looking ahead, the Internet of Things is driving the evolution of security cameras from mere image capturing devices into sources of vital business data with applications beyond the realm of security. One of 2018's emerging video security trends according to researchers at IHS Markit consists of 'deep learning.' Fundamentally related to machine learning and artificial intelligence, the technology uses algorithms to produce multiple layers of information from the same piece of data. It emulates the way in which the human brain absorbs details every second and enables the camera to independently arrive at conclusions on what images it captures, for instance suspicious behaviours or security threats.

In the process, the data collected by these cameras – powered by next-generation chip sets to support artificial intelligence at the camera level – is bound to become increasingly relevant and in need of utmost data protection. The ability to interpret data directly at the source also helps keep data secure, since based on pre-defined criteria it can decide whether certain sensitive data needs to be transmitted or stored at all. Meanwhile, public awareness and legal enforcement of data security are already at a new high following 2018's enactment of the EU's General Data Protection Regulation (GDPR), also impacting camera data in specific ways: data collection, storage, security and accountability are factors that operators need to be familiar with in the new age of intelligent video surveillance.

Supporting these development, the new generation of IP-based security cameras operates on platforms that offer built-in video analytics to interpret data together with the latest data security measures to protect this information in trusted ecosystems. Overall, the industry is making a major push towards integrating security on the hardware, software and network levels to let operators focus on retrieving the most relevant images, while having the peace of mind that their data is secure ●

### THE BIGGEST SECURITY LOOPHOLE TARGETED BY HACKERS

A recent survey among hackers revealed the biggest factor behind security breaches: 85 percent of respondents named humans as the main cause for online breaches, far exceeding "unpatched software" (10 percent), and "not enough security software" (5 percent). In order to limit security issues from human error, modern-day Video Management Software platforms are equipped to provide full control over granting access rights to sensitive video data only to select users.

Thycotic Black Hat 2017 Hacker Survey Report

**Kiran Pillai** – Bosch Senior Product Marketing Manager Video Systems – has over 10 years of experience in the video surveillance industry with a focus on Intelligent Video Analytics and data security.

**Cameras should offer a built-in firewall to eliminate loopholes from hackers that are 'guessing' passwords**

Picture credit: Getty