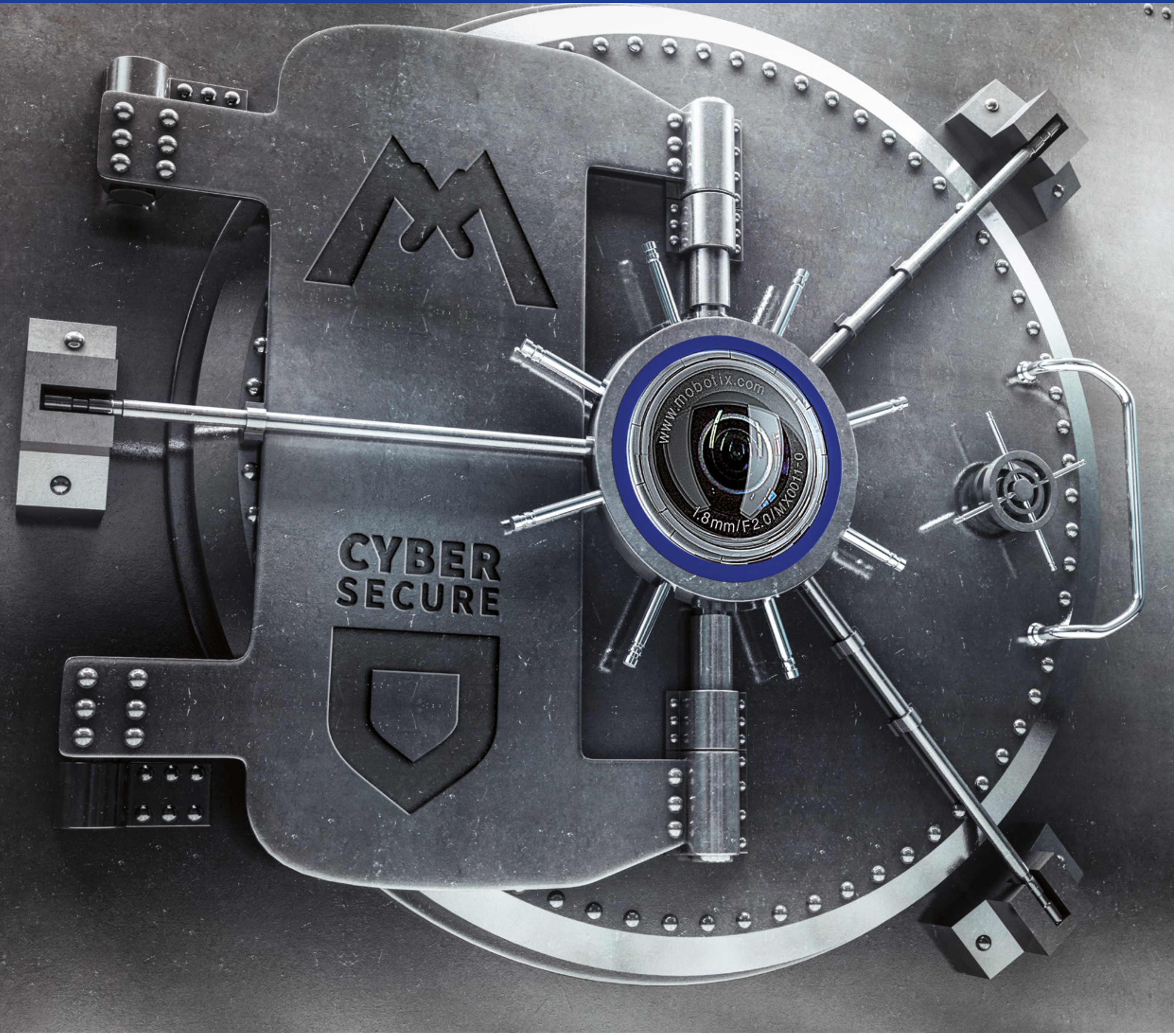
The Importance of Cyber Security in Video Surveillance Systems

White Paper



BeyondHumanVision

MOBOTIX

Introduction

The use of video for security, industrial control, health and safety has a beneficial impact on the lives of billions of people each day. From a family wandering around a safe shopping centre under the watchful eye of a CCTV to remote video used to help managers detect defects on a production line, or even concerned parents monitoring a sleeping baby; video surveillance is touching all of our lives.

What are the main growth drivers?		
1	Increased Security Concerns	58%
2	Improvement in Video Analytics	51%
3	Availability of IP Networks	50%

The growth in the use of video for surveillance and other applications has been accelerated by the wider information, communication and technology sectors. Where in earlier times, a video surveillance image would have required a human operator to view a situation and make a judgement call, increasingly – video imagery is married to other types of sensory inputs such as temperature, sound, motion and artificial intelligence systems that can automatically raise alarms or trigger actions. Video has gone from a passive reception media towards a situation where more automated intelligence can perform tasks based on what is observed.

Simple examples such as number plate recognition for road charging schemes to more powerful systems able to visually detect minor faults in machines before they break are just the tip of the iceberg. Even in mainstream applications such as retail surveillance, newer technologies are adding elements like people counting and shopping pattern analysis to help with store layout and even designing new shopping centres.

The demand is growing with Cisco estimating video for entertainment and business purposes will consume 79% of Internet Traffic by 2020[1]. And video is becoming easier to create through smaller, cheaper and lower powered cameras. Transfer of video from source to destination is also becoming less complex with the spread of internet connectivity and faster mobile networks. The perception of video and especially video surveillance is largely seen as a major societal benefit through less crime and more personal freedom due to safer environments. Yet as video becomes more pervasive it also becomes more exposed to attacks from criminals, terrorists and other groups that want to disrupt or exploit the video surveillance platforms for negative consequences.

The Risk of Unsecure Video Surveillance and IOT Devices

In previous times, attacks against video surveillance networks were rare due to the closed nature of systems that would often link by private directly cabled networks to on-site control rooms. In addition, legacy video cameras were effectively hard wired with simplistic firmware that did little other than send video over a coaxial cable leading to very little attack surface. However, times change and modern video cameras are effectively computers running software connected to a digital image sensor. With the rise of the internet and lower cost cameras, video surveillance systems are increasingly accessible over any IP network.

Just like security attacks against retailers and service providers, often with the aim of gathering credit card or other valuable information, the complexity and changing nature of the processes, software protocols and authentication mechanisms means that vulnerabilities will arise. The issue is not new. For over a decade, security researchers[2] have uncovered vulnerabilities in cameras that have impacted both major international vendors and smaller regional brands with a growing list of issues that includes:

- Attacks that obtain the device administrator password by breaking the security control from a default user account
- Exploits that bypass user authentication by using hard-coded credentials that have been placed in the device as a “backdoor” by the device manufacturer
- Execution of arbitrary code on the device without authentication by exploiting vulnerabilities within the Real Time Streaming Protocol packet handler
- Security vulnerability that bypasses camera operator authentication allowing an attacker to gain direct access to the configuration files
- Exploits that allow an attacker to reset the device password then enable the unauthorised modification of configuration files to give an attacker access to core camera functions
- Attack against cameras that allow third parties to intercept live video streams sent across a private network or internet connection

Many of these issues impacting multiple sub brands that licence technology from large vendors have led to weaknesses across millions of devices. Although the larger vendors with high profile reputations have often issued patches to fix the problem, many of the smaller companies have simply ignored the problem. Even when a fix is available, these updates are manual processes and many video surveillance platform owners are unaware of the issue. The issue also extends to home users with many consumer grade video security systems bought through retail still largely unpatched.

Targeted Attacks and Botnets

Although it would seem like the plot of a Hollywood blockbuster film, the ability to systematically take down an entire video surveillance system protecting a high value site, area or even city is not outside the realms of possibility. With many surveillance video vendors reusing the same software libraries that manage elements such as streaming, user authentication and transferring video onto storage media, skilled adversaries are almost certainly looking at attacks potentially as a precursor to crimes but also as a way of causing terror and panic.

Another issue is network traversal with attackers gaining a foothold inside an attached device, for example a camera and then using that authenticated position to gain access to other connected resources. Although largely stopped through well designed network defences, as cameras and other Internet of things (IoT) devices start to become more prevalent and embedded within core processes, the requirement to offer IoT device access can lead to more risk. But attacking cameras is not the only issue. In recent instances, the cameras themselves have been taken over and used as the weapon through distributed denial of service attacks (DDoS).

A massive DDoS attack in October 2016 that impacted Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix was, in part, generated by Mirai-based botnet. As reported by security expert Allison Nixon, director of research at Flashpoint, the botnet is mainly compromised of digital video recorders (DVRs) and IP cameras made by a Chinese hi-tech company called XiongMai Technologies. The components that XiongMai makes are sold downstream to vendors who then use them in their own products leading to tens of thousands of co-opted into these dangerous cyber weapons.[3]

Government, Regulators and the Law

The explosion of devices connected to the internet, estimated by Gartner, Cisco and others is between 25 to 50 billion[4] things by 2020, is causing a number of headaches for national governments and other transnational regulators. Unlike radio transmitters, TV stations or motor vehicles, there is almost no legislation around what can be attached to the internet. There are no mandated standards around how secure an item must be. Or what happens if that device is hacked or is used to attack another third party? Criminal law in most regions can deal with cybercrimes that have a perpetrator and victim, but as technology becomes more autonomous, there is a risk that unsecured devices will attract viruses like epidemics that used to plague desktop PC users could start to reappear on devices like video surveillance camera networks for which there is few ways to either detect or quickly defeat the problem.

Potential for Financial and Criminal Liability

There is also the thorny problem of liability. The installation of video surveillance systems can lead to lower insurance costs and increase the likelihood of criminals being captured. However, if a video surveillance system is rendered inoperable due to a security exploit and a crime is committed but not captured on camera – insurance providers could claim that any pay-out is cancelled due to not adhering to the parameters of the coverage. In this instance, would the victim sue the camera manufacturer? The provider of any CCTV maintenance contracts? Or in the case of a public safety incident, would the local government agency take responsibility? There are so many questions around the impact of a breach of security within a system like video surveillance and so few test cases that there is a great deal of uncertainty in the market.

Privacy Concerns

Although the financial and criminal liability issues around the hacking of video surveillance devices is still open to debate, the laws around the privacy of citizens have solidified across most developed nations. Although the details may change slightly, in general, all private personal data across areas such as health, finances, sexual orientation, political affiliation and a host of other criteria must be collected and stored in a secure fashion. This also extends to video data – for example, patients visiting a psychological health clinic or an individual attending a political rally – expect any video surveillance footage to be kept secure and outside of the public domain. In case of a cyber-attack against a video surveillance device or network, there is a very high risk that the personal information such as images and other data could target specific persons, and can be stolen and leaked without authorisation. This would violate the privacy rights of the users monitored by the system and could have legal consequences on the designated person responsible for processing personal data.

Government Action

Governments across the world are seeking more clarification on how to secure the new wave of IoT devices. In Europe, Senior EU commission figures have openly discussed the creation of a certification process for "Internet of Things" (IoT) devices that would ensure users are protected. The commission has also helped set up a group called the Alliance for Internet of Things Innovation that includes several larger technology vendors industry leaders within energy, automotive and health care to start the process of creating a set of best practice guidance. In the US, the Department of Homeland Security has issued a guide on the Strategic Principles for Securing the Internet of Things[5] which amongst many areas includes some key concepts such as incorporating security at the design phase, promoting security updates and vulnerability management with a focus on prioritising security measures according to potential impact. Yet there is no global or industry backed consensus like the credit industries PCI-DSS standards. The end result is that the security of IoT devices is now based on country-by-country guidance and light regulation which varies greatly in scope and effectiveness.

How is MOBOTIX Addressing these Issues?

As an industry leader within digital video surveillance, MOBOTIX is also unusual, in that it develops all of its own software in-house. Not only does this allow us to offer highly advanced products but it also offers a significant benefit when it comes to security. By controlling software development, MOBOTIX is less vulnerable to issues where a poorly designed third party software and hardware can lead to a security issue. In areas where we use widely supported industry standards such as ONVIF, we have policies in place to immediately issue any patches as they become available. By using the same software for all MOBOTIX camera models, this process of continually ensuring that the camera firmware is both up to date and secure makes it much easier for our international customers.

The security by design ethos has been within the company from day one and this is evident in several areas:

Secure Operating System and Updates

The start of the MOBOTIX security approach begins within the design of the operating camera system and application stack. All MOBOTIX devices are built on top of a modified and secured Linux OS that removes standard services and modules. Critical Linux modules like authentication are completely re-designed by engineers at MOBOTIX to ensure that these modules are not vulnerable to standard exploits or code injection techniques. This operating software is not open sourced and protected by additional software security techniques. In addition, every update to device firmware and software elements are encrypted and digitally signed to avoid tampering.

Secure Camera Configuration

Access to the camera configuration interface is granted to only authorised users and to ensure internal security, every system allows the creation and enforcement of different rights for different user groups. In practice this means that MOBOTIX cameras never save user passwords in clear text but instead are hashed with a strong one-way hashing (SHA-512) algorithm so that even if the configuration file ends up in the wrong hands, it would be extremely difficult to retrieve the password in clear text. Unessential Linux OS services are disabled to limit potential exploits and prevent attacks and there is no undocumented telnet or “master password” - a MOBOTIX camera can be accessed and configured via its Web GUI (Graphical User Interface). Passwords can be kept in privilege access management systems like BeyondTrust and CyberArk which can be secured by deeper two factor authentication systems.

Secure Network and Device Communication

All data exchanged between every MOBOTIX camera and other hosts in the network can be encrypted to ensure the confidentiality and integrity of data in transit. HTTPS (SSL/TLS) and certificates are all supported as standard to meet the best practice guidance that resides within the major security frameworks from experts such as the SANS institute. MOBOTIX also includes built-in support to manage unique X.509 certificates on each camera and Root Certificate Authorities to allow organisations to extend device security to include cameras and Door Station devices authenticated via systems like OpenVPN. This means, that if a camera is physically stolen or hacked, an attacker can’t use the credentials within a compromised camera to attack the rest of the network of cameras.

Secure Internal Recording and Anti-Tamper

All the recordings generated by the camera can be encrypted before being stored, starting with the ring buffer that uses the built in SD card in each camera. MOBOTIX has built a secure file system that means if a camera is physically hacked or stolen, previously recorded video still in the camera cannot be retrieved without first gaining administrative rights which are protected through the secure configuration processes as described previously. Each image produced by a MOBOTIX camera can be digitally signed with custom certificates to prevent tampering; this ensures admissibility of the recordings when used as evidence in a court of law.

Security Features	Standard IP Cameras	MOBOTIX
HTTPS (SSL/TLS) and Certificates	✓	✓
Digest Authentification for HTTP	✓	✓
Access Control Lists	✓	✓
Users and Groups with Custom Rights	⚠	✓
Intrusion Detection	✗	✓
Anti-Bot Protection	✗	✓
Encrypted Recordings	✗	✓
Encrypted Video & Messages	✗	✓
VPN Client	✗	✓

Intrusion Detection

Even with a number of security systems and processes in place, it would be foolhardy to assume that attackers will not try to breach MOBOTIX cameras, which is why MOBOTIX has invested in additional measures to detect such attempts. By implementing a range of intrusion detection elements, each camera or Doorstation device will report back over an encrypted channel any unauthorised logins and brute force attacks; in addition, notifications can be sent in case of repeated failed login attempts and the offending IP address can be blocked automatically.

Summary

The rise in popularity for video surveillance and as part of other health, safety and industrial process shows no sign of slowing down. As these elements start to become more vital, additional processes such as access control, environmental monitoring and analytics processes, such as facial recognition, will increasingly become targets for cyber-attack.

Specifiers of video surveillance systems along with service providing operators and even regulating bodies will need to extend more control over security as both a duty of care to the public and to meet future legal obligations. As an industry, leaders such as MOBOTIX and others have recognised these problems and are actively working to build security into device hardware and software at the earliest stages of design.

However, secured devices are only as good as the protection of the overall environment. Locking the door is pointless if the window is left open. As such, specifiers and operators of video surveillance and wider IoT networks need to evaluate other parts such as the underlying network, storage infrastructure and crucially the human element that is often a weak link. Several industry groups such as the SANS Institute have created useful guidelines such as The Centre for Internet Security (CIS) Critical Security Controls which offer a recommended set of actions for cyber defence that provide specific and actionable ways to stop today's most pervasive and dangerous attacks.[6]

Looking into the future, it is clear that device and platform security will become a key factor in major video projects and as education around the challenges of IoT becomes more widespread, MOBOTIX is looking forward to working with its peers in the industry, customers and government agencies to protect the very technologies and systems that help make society safer for all.

References

https://www.coresecurity.com/system/files/publications/2016/05/corelabs-ipcams-research-falcon-riva.pdf

https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Sources

[1] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.

[2] html https://www.coresecurity.com/advisories/hikvision-ip-cameras-multiple-vulnerabilities

[3] https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

[4] http://www.telecomtv.com/articles/iot/internet-of-things-to-reach-25-billion-devices-within-five-years-11931/

[5] https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

[6] https://uk.sans.org/critical-security-controls

MOBOTIX has developed and manufactured IP video systems, video management and analysis software in Germany since 2000.

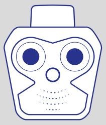
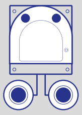
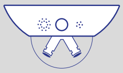
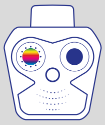
MOBOTIX stands out for its **high level of reliability**. All outdoor cameras are subjected to a stress test for temperatures between -30°C and +60°C (-22°F and +140°F). Without additional components, without heating or cooling and with no moving parts (for example auto iris), they are virtually maintenance free.

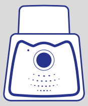
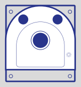
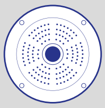
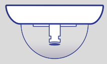
MOBOTIX delivers a **perfectly matched package**, starting with the microSD card for storage management and HD audio (microphone and speaker) with VoIP telephony through video analysis, a professional video management system and motion detection software reducing false alarms.

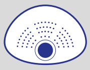
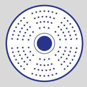
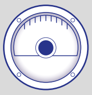
The **decentralized architecture** means that a central computer is not required and the network load is minimal. The intelligent cameras from MOBOTIX process and store image data themselves, trigger events and, in the event of remote access, manage the frame rate and resolution depending on the available bandwidth.

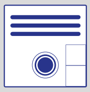
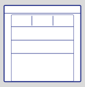
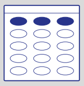
The **6MP Moonlight sensors** and complementary **thermal imaging technology** ensure reliable detection of moving objects, even under the most challenging light conditions and over long distances. As a result, it is possible to cover large areas with just a few cameras. Less power cabling, less IT infrastructure and fewer additional light sources are needed. MOBOTIX cameras are powered using standard PoE and do not require more than 4-5 watts.

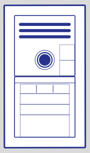
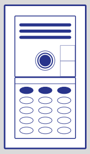
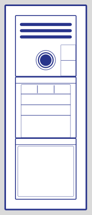
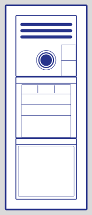
An intelligent IP video system from MOBOTIX allows you to **reduce total costs**. The investment pays for itself after a short time and the free-of-charge software and updates ensure it is a future-proof investment.

Outdoor Dual Lens			Thermal	
M16 AllroundDual	S16 FlexMount	D16 DualDome	M16 Thermal	S16 DualThermal
				
Robust for extreme conditions	Flexible dual camera	Modular dual camera	Thermal dual	Thermal dual

Outdoor Single Lens			
M26 Allround	S26 FlexMount	Q26 Hemispheric	D26 Dome
			
Robust for extreme conditions	Discreet, video analysis	Discreet, video analysis	Modular Fix dome

Indoor			
i26 Panorama	c26 Hemispheric	p26 Allround	v26 MiniDome
			
180° hemispheric	Discreet, video analysis	Modular ceiling camera	Vandalism camera

Door Modules			MxDisplay+
Camera	BellRFID	Keypad	Remote Station
			

Door Sets			
Double Frame		Triple Frame	
			

EN_10/17

MOBOTIX AG
Kaiserstrasse
D-67722 Langmeil
Tel.: +49 6302 9816-103
Fax: +49 6302 9816-190
sales@mobotix.com
www.mobotix.com