CYBERSECURITY AND IP VIDEO SURVEILLANCE

June 2021

Honeywell

DISCLAIMER

This document is a draft and is provided for information purposes only.
The information contained herein is the product of research conducted by third parties and is provided “as is” without any representations or warranties, express or implied. This document is subject to change and nothing contained herein constitutes or is intended to constitute advice of any kind.

This document also contains information that is the proprietary and confidential property of Honeywell Inc. By acceptance hereof, each recipient agrees to use the information contained herein only for the purpose anticipated by Honeywell Inc, and not to disclose to others, copy or reproduce, any part hereof without the written consent of Honeywell Inc.

TABLE OF CONTENTS

INTRODUCTION

1

IP-based video surveillance systems offer more secure, reliable and cost-efficient solutions in today's information-rich, digital world than the outdated technology used in analogue video solutions.

IP technology can enable effective and manageable video surveillance to better protect people, their information, their properties and help support continuous operation. It can also help deliver enhanced safety and security benefits for our society to potentially prevent costly security incidents. In an environment with increasing threats from bad actors, the cybersecurity of IP technology is challenged by the pace of technology transition and development, creating potential safety and economic risks.

Cyber-attacks at the local and global scale are on the rise, and according to a report published by Upguard, the total estimated global financial loss associated with cyber security attacks in 2021 is estimated to be $6 trillion, up from $3 trillion in 2015.[1] A recent example of a significant cyberattack is the ransomware attack against a major fuel pipeline operator in the eastern US. As a result of this attack, gasoline availability in a large section of the U.S. was significantly impacted before operations were restored.[2]

Honeywell takes cybersecurity seriously–it's at the core of everything that we do. We incorporate cybersecurity and privacy best practices into every process we institute, every product we create, and every piece of software we deploy. We proactively work to identify threats and emerging risks before they spell disaster. This paper is intended to provide an overview of Honeywell's approach to cybersecurity, including its latest IP video surveillance products and systems designed to intelligently prevent dangerous attacks.

THREAT AND VULNERABILITY

2

The importance of cybersecurity in the IP environment is widely recognized. It requires protecting devices, networks, programs and data from being viewed, copied, changed or destroyed by unintended or unauthorized access. Since video surveillance products such as IP cameras, network video recorders (NVRs), and video management software (VMS) are IP-enabled, they can be accessed from a remote location using internet connectivity, which means they have the same vulnerabilities as other devices and systems in the open IP world.

The U.S. National Strategy to Secure Cyberspace[3] is a report that outlines a five-level threat and vulnerability model, including for home/small business, large enterprise, sector/infrastructure, national and global categories.

In the report, the U.S. government expresses concerns about:

- the network devices used to attack critical infrastructures;
- large-scale enterprises being increasingly targeted by malicious cyber actors, both for the data and the power they possess; and
- the fact that cyber vulnerabilities could directly affect the operations of a whole sector or infrastructure.

Not only has cyber crime caused significant business interruptions and negatively impacted infrastructure in recent years, it has also led to large-scale data breaches. According to PwC's survey, Global Economic Crime Survey 2016[4], the risk of cyber crime was the second most reported type of economic crime affecting 32% of organizations in 2016. Furthermore, in the U.S. a data breach costs a company on average $8.64 million[5]. According to the Fortinet Cybersecurity Statistics report for 2021, "The use of malware increased by 358% through 2020, and ransomware usage increased by 435% compared to the previous year, according to a study by Deep Instinct. July 2020 alone saw a 653% increase in malicious activity compared to the same month in 2019."[6]

Many countries and international organizations are working on data-protection legislation, national standards and regulations. These regulatory initiatives will help reduce vulnerabilities and clarify questions of liability.

BUSINESS INTERRUPTION

Business interruption is a type of cyber crime that is usually launched by inserting malicious code on a company or infrastructure network, which limits the network's ability to provide service and inhibits a company's ability to conduct business.

Malicious code, or "malware," composed of viruses, worms, botnets, etc., can be injected into IP devices with weak points, propagate itself to seek more victims on the network, and steal sensitive information for the purpose of economic benefit, make a point, Disrupt services, driven by Purpose - Hacktivism, Idealism, Political Motives and steal/leak information.

A botnet, short for "robot network," is an aggregation of computers compromised by bots (automated machines or robots). These bots are controlled by malware by launching Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks to targeted critical infrastructures or enterprises.

DoS and DDoS pose a serious threat to business service. In June 2015, hackers grounded 10 planes belonging to a Polish airline and blocked flight plans sent to planes by launching a DoS attack.[7] The Mirai botnet attack is also an example of a DDoS attack.[8]

DATA BREACH

The video system is the core of a security system and contains critical information, including system data, deployment, event and alarm information. If this data is compromised, it's considered a data breach and this type of crime can cause significant security and safety risks.

Video surveillance in private and public applications may capture and record video images of people not relevant to security and safety incidents. Many countries are working on privacy-protection legislation to prevent privacy breaches by intruders and inside employees. For example, in the U.S., all 50 states have breach-notification laws in effect[9] and in Ireland it is illegal to post video surveillance footage on the internet[10].

COMPLIANCE AND LIABILITY

With cyber legislation, national standards and sector regulations in place, regulatory compliance will become a rigid entrance requirement for IP systems, including video surveillance. It will impact the framework for product design, sales, industry entrance, system integration and user operation.

Meanwhile, there is also a market trend of increased cyber insurance sales spurred by the awareness of broader cyber risks. A vulnerable system will be forced to upgrade or be replaced for regulatory compliance or the customer will have to pay a much higher premium to cover the liability every year. This is why Honeywell is committed to providing a forward-looking, cyber-secure video solution for its partners and customers.

HONEYWELL'S APPROACH TO SECURING THE IP VIDEO SOLUTION

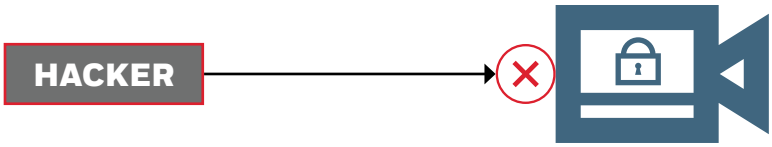
3

Many businesses have not conducted a cyber-threat analysis and do not know how vulnerable they are to cyber threats. Honeywell can help by analyzing customers' problems, then implementing best practices to execute optimal product and system design. Honeywell has also developed a cybersecurity management process and released vulnerability reporting policies to help its customers face growing cybersecurity challenges.

UNDERSTAND	RESPOND	RESULT
CUSTOMER PROBLEMS	**HONEYWELL SOLUTION**	**CUSTOMER VALUE**
1. Business interruption	1. System hardening	1. Increase business continuity
2. Data breach	2. Network port management	2. Reduced breach risk
3. Compliance liability	3. Password policy	3. Reduced privacy violation
	4. Secure data trasmission	4. Reduced cyber insurance cost
	5. 3rd party testing and certification	5. Regulatory compliance by design
	6. Security management process	6. Continuous protection
	7. Reporting policy	

RIGOROUS SYSTEM HARDENING

At the product and system design and development phases, Honeywell uses in-house and third-party testing tools to evaluate product vulnerabilities and fix issues to harden the system. To mitigate the risks associated with malicious code, data privacy breaches and system misconfiguration, Honeywell employs the Information Communication Technology (ICT) industry's security guidelines, which addresses specific video surveillance requirements.



Since IP video surveillance can be installed in both private and public networks, the exposed cyber thereat can vary accordingly. It is necessary to target system hardening according to the specific deployment application. System hardening needs to be aligned with the process of cybersecurity management, system management and business operations. Customers of Honeywell Video Systems can configure product and system settings to address threats specific to the planned implementation.

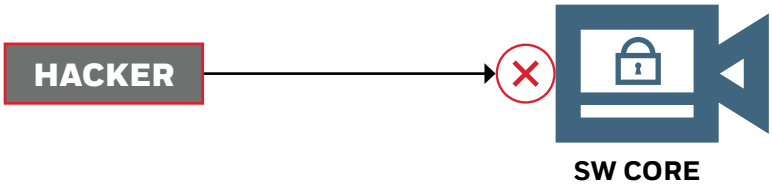
System hardening is usually the process of securing a system by reducing its vulnerability. Common system hardening practices include:

- Disabling unused ports and unnecessary services by default
- Enforcing password rules and changing default password at initial login
- Updating security patches to stay current
- Using web communication with up-to-date encryption protocols, such as TLS 1.2 or+ encryption
- Complying with Payment Card Industry Data Security Standard (PCI DSS) and Underwriters Laboratories Cybersecurity Assurance Program (UL CAP)

NETWORK PORT MANAGEMENT

A network port is a logical end point for communication purposes. To connect to external services, IP devices use network ports identified by specific numbers from 0 to 65535; ports between 0 and 1023 are considered reserved and are officially assigned by the Internet Assigned Numbers Authority (IANA).

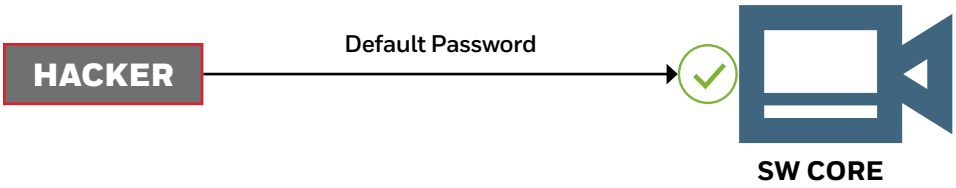
A network port is always associated with the IP address of the host and the protocol of communication and completes the destination or origination network address of a communication session. Well-known port numbers are allotted to the standard process applications of an IP device. For example, Port 21 is used for File Transfer Protocol (FTP), Port 23 is used for Telnet remote login service, and Port 80 is used for Hypertext Transfer Protocol. These well-known ports are highly vulnerable to cyber-attacks. Honeywell disables unused communication ports by default – such as FTP port 21, SSH port 22 and Telnet port 23 – to eliminate hijacking risk via vulnerable legacy protocols.



PASSWORD MANAGEMENT POLICY

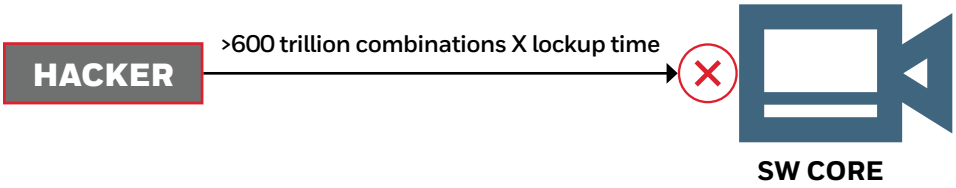
When users log into Honeywell IP camera software for the first time, they receive a prompt to change the product's default password. If the default password isn't changed, the notification will be shown at log in until the action is completed.

The default password should only be used for the first log in, for demos and for technical support purposes. If the device's default password has not been changed, hackers could remotely log into the device.



With Honeywell IP cameras, password rules are enforced to increase the strength of new passwords. A password must contain a minimum of eight characters with alphanumeric,uppercase, lowercase and special characters. These rules result in more than 600 trillion combinations that hackers would need to attempt to access a user's account. As Trustwave stated in its 2016 Global Security Report, 7% of cyber-attacks occur due to weak passwords.[11]

To cope with automated attacks, Honeywell devices lock for 15 minutes after ten failed login attempts; this means it would take approximately three billion years to try 600 trillion combinations.



Data breaches are another type of cyber threat that need to be prevented in system and process design. Data breaches may not occur inside the devices but on the remote client. In Honeywell video systems, all passwords stored on the device and system or transmitted between them are rendered unreadable. Even when cyber-attacks compromise a remote workstation or transmission between them, the passwords are still protected.

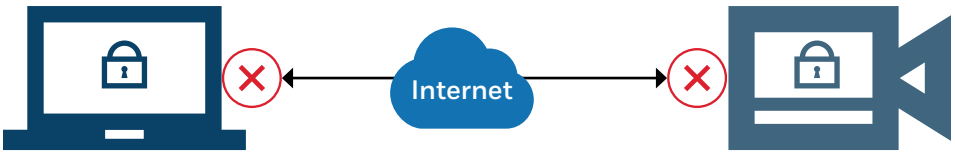
SECURE DATA TRANSMISSION

On the web, Hypertext Transfer Protocol (HTTP) is the foundation of data communication protocols. When we type strings of a website address starting with http://, we send access requests to the web page. Behind the scenes, the HTTP protocol enables a session with a sequence of network request response transactions, which transmits the web page to the end user.

HTTP sites are not encrypted and are vulnerable to man-in-the-middle and eavesdropping attacks. A more secure protocol, "HTTPS," also called Hypertext Transfer Protocol Secure, takes the place of HTTP and builds a more secure communication by providing both encryption of the communication and authentication of the remote hosts.

In a video system, data may transfer through an untrusted or unsafe network. Honeywell uses the HTTPS protocol to provide bi-directional, encrypted communication between devices and systems. Please check Honeywell webpage https://mywebtech.honeywell.com/Account/Login/ for the latest list of products supporting HTTPS encryption. For products without HTTPS encryption capability, please avoid using them in untrusted networks or install them behind a firewall to mitigate potential risk.

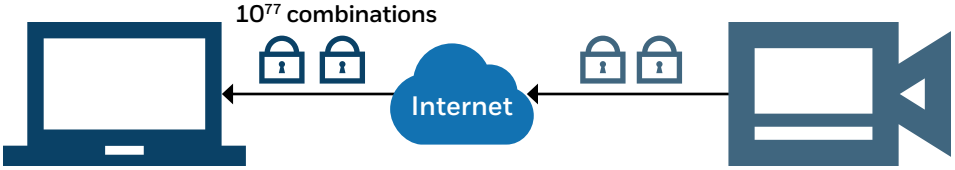
When an HTTPS session request is sent to an IP camera, the camera and server will authenticate each other by exchanging certificates. Only after both identify and authenticate each other a secure session is established.



Throughout the entire encryption process, private keys are critically important and must be kept secure. If the private keys are compromised, the encrypted data streams could be intercepted and decrypted.

In select Honeywell IP cameras, private keys are securely stored inside a non-retrievable hardware chipset. If there is no secure, hardware-based key storage, the private keys will have to be stored in the device file system, which is more vulnerable to cyber-attacks.

The Advanced Encryption Standards (AES) is a specification for data encryption. It was adopted by the U.S. government to protect classified information and has since been adopted worldwide. In the AES specification, 128-bit and 256-bit keys are used for encryption and decryption to protect critical data. 128-bit keys create 3.4x1038 possible combinations and 256-bit keys create 1.1x1077 possible combinations. Fifty supercomputers that could check a billion (1018) AES keys per second would require about 3x1051 years to exhaust the 256-bit key space. Honeywell leverages the AES specification to protect IP communications.



THIRD-PARTY COOPERATION AND CERTIFICATION

Like Honeywell, companies across industries have become more sophisticated about cybersecurity, and the set of resources and tools available to improve and assess security programs likewise has grown dramatically.

Honeywell uses the experience, tests and certifications of third parties to manage its supply chain from the cybersecurity perspective, specifically tracking vulnerabilities associated with the software and hardware components provided by outside vendors. Increased awareness can help Honeywell identify where and how to apply security measures.

In addition, Honeywell also partners with the industry during product design, testing, manufacturing and system integration to identify vulnerabilities, detect irregularities, respond to potential incidents, and recover from damage to or disruption of IP Video systems.

Honeywell has formed a qualified network security team composed of experts certified by the International Information Systems Security Accreditation Alliance to enhance product safety by applying safety measures to the product development lifecycle.

Honeywell has actively participated in industry discussion relating to cybersecurity and has supported the development of industry standards and certification.

PCI DSS COMPLIANCE

Cyber compliance is not new to the banking and finance industry. PCI DSS released its first, optional version in 2004 and version 3.0 in 2015. PCI DSS compliance involves an ecosystem of payment devices, applications, infrastructure and users. When deploying an IP video system for banking applications, PCI DSS compliance is mandatory. The video system needs to be compliant with PCS DSS requirements, including network and data protection, vulnerability management, access management and security policies. Honeywell equIP® series IP cameras and the development process adhere to the rules of the PCI DSS ecosystem, video surveillance and common IP cybersecurity requirements.

SECURE DEVELOPMENT LIFE CYCLE PROCESS

Honeywell has developed a robust system for considering security at the outset of product conception and during development, as well as responding to potential vulnerabilities in existing products. This system, Honeywell's Secure Software Development Lifecycle (SSDLC) initiative, has evolved and grown even more robust over the past few years.

Honeywell takes product security seriously. Our products go through a robust and comprehensive penetration testing regimen. In some cases, additional independent security testing is conducted. The criteria for this additional testing as well as which products or offerings are selected for this are closely held proprietary information.

We have a robust and comprehensive Secure Development Life Cycle (SDLC) based on best practices and industry standards that includes the following:

- Security Risk Assessment based on the threat environment faced by a particular product or offering as well as the technical features and customer needs
- Security Requirements and security controls based on industry standards and guidelines such as BSIMM, ISA/IEC 99/62443, ISO 27001, PCI DSS, GDPR, OWASP, applicable local laws and regulations, and others depending on the product or offering and the Security Risk Assessment
- Privacy Impact Assessments
- Threat Modeling
- Secure by Design, Privacy by Design and Secure Coding standards and practices
- Static Application Security Testing (SAST, also known as source code scanning) to enforce secure design and coding practices. We scan for OWASP Top 10 and SANS Top 25 vulnerabilities as well as for language-specific quality measures. Current SAST tools include SonarQube and Coverity depending on product and language needs.
- Binary scanning to identify open source usage and potential vulnerabilities.
- A formal Risk Management Policy that requires specific mitigation timelines based on severity
- Review and approval of cybersecurity by senior leadership prior to product shipment
- Lifecycle support and customer notification for security updates

An audit team of Honeywell performs checks to ensure that security deliverables required under Honeywell's Secure Development Life Cycle processes are completed.

Honeywell completes training programs for its employees on the company's security process and on specific cybersecurity concerns and solutions. All software engineers in Honeywell receive formal training on the Secure Development Life Cycle process and general cyber/product security topics.

HONEYWELL CYBERSECURITY REPORTING POLICY

We take security concerns seriously and work to quickly evaluate and address them. Once reported, we commit the appropriate resources to analyze, validate and provide corrective actions to address the issue.

The goal of our Product Security Incident Response Team (PSIRT) is to minimize customers' risk associated with security vulnerabilities by providing timely information, guidance and remediation of vulnerabilities in our products, including software and applications, hardware and devices, services and solutions. This team manages the receipt, investigation, internal coordination, remediation and disclosure of security vulnerability information related to Honeywell products.

PSIRT coordinates the response and disclosure of all externally identified product vulnerabilities.

REPORTING A POTENTIAL SECURITY VULNERABILITY

We welcome reports from independent researchers, industry organizations, vendors and customers concerned with product security. To find out more information on how to report a potential vulnerability, please visit the Vulnerability Reporting webpage.

COORDINATED VULNERABILITY DISCLOSURE

We strive to follow Coordinated Vulnerability Disclosure (CVD). This process allows independent reporters who discover a vulnerability contact Honeywell directly and allow us the opportunity to investigate and remediate the vulnerability before the reporter discloses the information to the public.

The PSIRT will coordinate with the reporter throughout the vulnerability investigation and will provide them with updates on progress as appropriate. With their agreement, the PSIRT may recognize the reporter on our acknowledgments for finding a valid product vulnerability and privately reporting the issue. After an update or mitigation information is publicly released by Honeywell, the reporter is welcome to discuss the vulnerability publicly.

Following the CVD allows us to protect our customers and at the same time coordinate public disclosures and appropriately acknowledge the reporter for their finding. If a reported vulnerability involves a vendor product, the PSIRT will notify the vendor directly, coordinate with the reporter or engage a third-party coordination center.

Please refer to https://www.honeywell.com/us/en/product-security for further information.

CONCLUSION

4

Honeywell IP video solutions are not only deployed for large enterprise, critical sectors and infrastructures in the global market but are also appropriate for small and medium-sized businesses. To protect people, property and service, Honeywell puts tremendous effort into product and system design, third-party testing and certification, security-management processes, and vulnerability-reporting policies. All of this work results in minimum system downtime, business continuity, lower risk of data and privacy breaches, and reduced cyber and compliance liability to enhance customer satisfaction.

REFERENCES

1 Upguard Blog, What is the Cost of a Data Breach in 2021? March 22, 2021, [Accessed May 13, 2021]

2. New York Times, Cyberattack Forces a Shutdown of a Top U.S. Pipeline, May 12, 2021 [Accessed May 13, 2021]

3. White House and U.S. Department of Homeland Security, National Strategy to Secure Cyberspace, 2003 [Accessed May 12, 2021]

4. PwC, Global Economic Crime and Fraud Survey 2020, [Accessed May 12, 2021]

5. IBM and Ponemon Institute, Cost of Data Breach Report 2016, 2016 [Accessed May 12, 2021]

6. Fortinet, Cybersecurity Statistics, 2021

7. CNBC, Hack attack leaves 1,400 airline passengers grounded, June 22, 2015 [Accessed May 12, 2021]

8. CSO Online, The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet, Josh Fruhlinger, March 9, 2018 [Accessed May 12, 2021]

9. National Conference of State Legislatures, Security Breach Notification Laws, [Accessed May 12, 2021]

10. Irish Statute Book, Data Protection Act, 1988, [Accessed May 12, 2021]

11. Trust Wave, 2016 Global Security Report, April 19, 2016, [Accessed May 12, 2021]

For more information
www.security.honeywell.com

Honeywell Building Technologies
715 Peachtree St NE
Atlanta, Georgia 30308
www.honeywell.com

HBT-WP-CYBRSEC-US-EN-25un2021

THE FUTURE IS WHAT WE MAKE IT

Honeywell