Honeywell

Network and Security

Honeywell Scanners

User Guide

Disclaimer

Honeywell International Inc. (“HII”) reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult HII to determine whether any such changes have been made. HII makes no representation or warranties regarding the information provided in this publication.

HII shall not be liable for technical or editorial errors or omissions contained herein; nor for any damages, whether direct, special, incidental or consequential resulting from the furnishing, performance, or use of this material. HII disclaims all responsibility for the selection and use of software and/or hardware to achieve intended results.

This document contains proprietary information that is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of HII.

Web Address: sps.honeywell.com

Trademarks

Microsoft is either a trademark or registered trademark of Microsoft Corporation in the United States and/or other countries.

The Bluetooth trademarks are owned by Bluetooth SIG, Inc., U.S.A. and licensed to Honeywell.

MITRE is a registered trademark of The MITRE Corporation.

Cisco and Catalyst are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.

UNIX is a registered trademark of The Open Group.

Wi-Fi is a registered trademark of the Wi-Fi Alliance.

OpenSSL is a registered trademark of The OpenSSL Software Foundation, Inc.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the property of their respective owners.

For patent information, refer to www.hsmpats.com.

TABLE OF CONTENTS

Customer Support

Technical Assistance

Go to honeywell.com/PSStechnicalsupport to search our knowledge base for a solution or to log into the Technical Support portal.

Product Service and Repair

Honeywell International Inc. provides service for all of its products through service centers throughout the world. Go to sps.honeywell.com, then select **Support** to find a service center near you or to get a Return Material Authorization number (RMA #) before returning a product.

Limited Warranty

For warranty information, go to sps.honeywell.com and click **Support** > **Warranties.**

CHAPTER

1 INTRODUCTION

Management of security risks is part of the risk management for a complete scanner products implementation. The aim is to achieve a secure state for the scanner products through detection, analysis, evaluation, monitoring and control of security risks. However, a completely risk-free and secure state can never be achieved.

Security cannot be achieved by implementing individual measures alone. It can only be maintained with a supporting process. Such security processes are described in IEC 62443, for example. They include asset management, threat analysis, and patch management.

Intended Audience

The target audience for this guide is the customer organization that identifies and manages the risks associated with the use of information processing equipment. This includes, but is not limited to, Information Technology (IT). Third party organizations delivering and installing turnkey systems should also follow the guidelines in this guide. The intent of this guide is to drive the discussion between the organization using Honeywell scanners and the organization responsible for managing information technology risks.

A high degree of technical knowledge and familiarity in the following areas is assumed.

- Networking systems and concepts
- Wireless systems
- Barcode scanning
- Security issues and concepts. In particular, the following systems need to be understood and properly setup:
  - Radius Server
  - Application Server (such as a Web server or Terminal Emulation server)

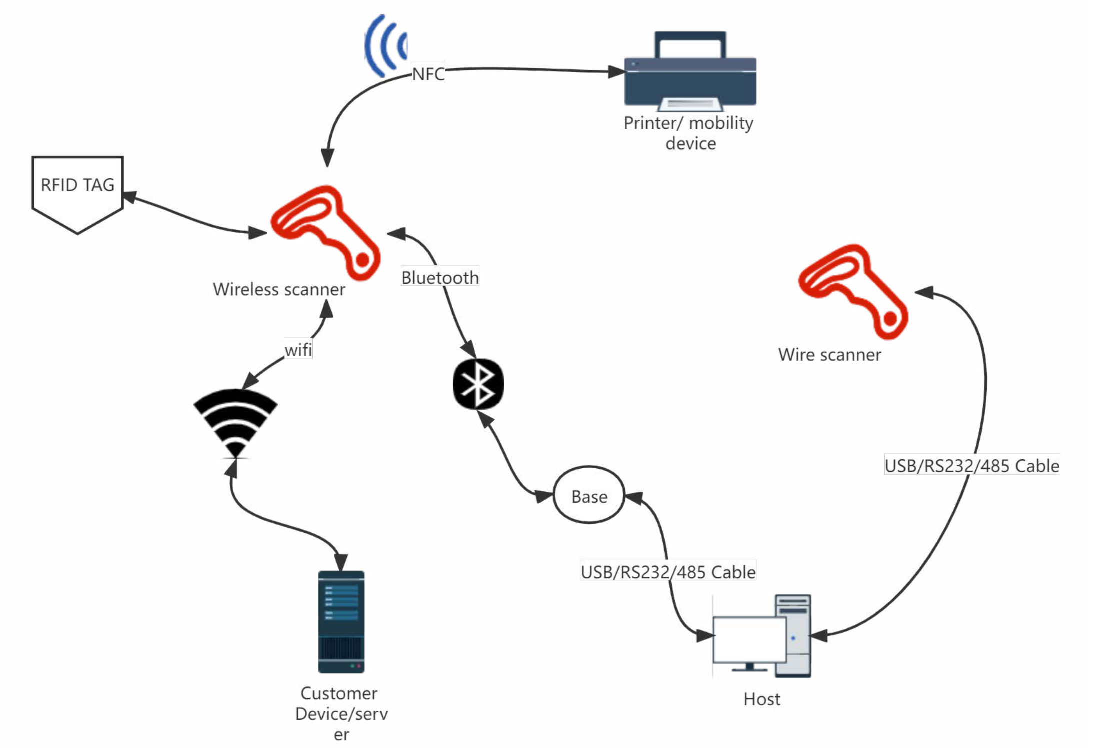
How to Use this Guide

If you have specific security concerns (e.g., the prevention of unauthorized access or virus protection), consult the Security Checklist (page 3) or select from the topics listed below.

- Develop a Security Program, page 13
- System Monitoring, page 17
- Secure Wireless Devices, page 19

System Architecture

The illustration below provides an example of a system architecture that includes multiple scanners and other devices such as scanners and mobile computers, and a Wireless infrastructure (WLAN).



Related Documents

User Guides	Additional Information
User Guides for Honeywell scanning products	Go to sps.honeywell.com to download the user guide specific to your scanner model.

CHAPTER

2 SECURITY CHECKLIST

This chapter identifies common security threats that may affect networks containing barcode scanners. You can mitigate the potential security risk to your site by following the steps listed under each threat.

Infection by Viruses and Other Malicious Software Agents

This threat encompasses malicious software agents; for example, viruses, spyware (Trojans) and worms.

The intrusion of malicious software agents can result in:

- Performance degradation,
- Loss of system availability, and
- Capturing, modifying, or deleting data

Mitigation Steps

Honeywell recommends the latest version of software native protections within the operating system are kept in place and that back end infrastructure/systems are upgraded to current standards to match.

Note: *For optimal security, Honeywell recommends aligning back-end infrastructure to current operating system protections.*

Mitigation Steps
Ensure virus protection is installed, signature files are up-to-date, and subscriptions are active.
Allow only digitally signed software from trusted sources to run.
Use a firewall at the interface between other networks and barcode/RFID scanning products.

Unauthorized External Access

This threat includes intrusion into Honeywell scanning products from the business network or other external networks including the Internet.

Unauthorized external access can result in:

- Loss of system availability
- Capturing, modifying, or deleting data
- Reputation damage if the external access security breach becomes public knowledge

Mitigation Steps

Mitigation Steps	
Implement file system encryption or full disk encryption.	
Use a firewall at the interface between your other networks and Honeywell scanning products with associated scanning base with a PC tool.	
Secure wireless devices	For information, see Secure Wireless Devices on page 19.
Use the most recent version of the SDK that supports your application.	
Disable all unnecessary access ports, such as FTP.	
Use a VPN when the Linux system requires data to traverse an untrusted network.	
Use SSL for communication between native applications and specialty servers.	
Use intrusion detection on WLAN networks.	

Unauthorized Internal Access

This threat encompasses unauthorized access from people or systems with direct access to a scanning device. This threat is the most difficult to counter since attackers may have legitimate access to part of the system and are simply trying to exceed their permitted access.

Unauthorized internal access can result in:

- Loss of system availability
- Capturing, modifying, or deleting data
- Theft or damage of system contents

Mitigation Steps

Mitigation Steps	
Implement strong password protection on Honeywell Solution components and include a password lifetime management policy, reuse policy, and strength of policy for passwords.	Refer to the user guide specific for your scanner model for more information.
Monitor system access.	To learn more, see System Monitoring on page 17.
Programming Barcode (Menu) Security.	Password protection should always be enabled to prevent unauthorized access.

Bluetooth Security

Follow these security recommendations and precautions for Bluetooth security:

- If possible, pair devices ONLY when in a physically secure area.
- Keep paired devices close together when possible to monitor both devices.
- Remove paired devices that are no longer in use.
- Use a strong PIN or Password. Periodically update PIN or Password to avoid information leak.
- Set Bluetooth to non-discoverable mode.
- If Bluetooth technology is enabled, the device should only be made discoverable when necessary. The default and recommended settings are off (non-discoverable).

Note: *Honeywell recommends turning off Bluetooth communication if it is not required for your application.*

Securing Barcode Scanner Series

Honeywell recommendations for securing barcode scanner series:

- Enforce the most restrictive set of rights/privilege to access barcode scanner series and it's assets needed by users or processes for the performance or specific tasks. Specifically prohibit, remove, and/or restrict the use of unnecessary functions, ports, protocols, and/ or services. This would include access to scripts debuggers, etc. Log requests for access to assets.
- Use the proper setting of privilege.
- Ensure access is restricted to administrators for secure process channels, devices, and components related to barcode scanner series.
- Enforce proper configuration at installation of barcode scanner series and its components, including secure by default, baseline configurations for detection

of unauthorized changes, and configuration of least functionality required and management of configuration changes. When possible, the configuration should be automatically traced and reported.

Securing Plugins Installed on Scanner Device

Honeywell provides end users the ability to write and install plug-ins that run directly on the scanner. Customers should validate all plug-ins used on barcode scanners. Ensure all plug-ins have been code signed to prevent unauthorized modification.

For securing plugins installed on the scanner device, Honeywell recommends Honeywell's TotalFreedom™. TotalFreedom is a development platform that allows customers to develop their own plugins. Honeywell recommends using this platform to develop plugins.

Security Updates And Service Packs

One of the common weaknesses of system management as reported by Open Web Application Security Project (OWASP) is “not keeping software up to date.” It is critical to keep the latest patches and software versions on your scanning device and supporting devices in the scanning network. This is especially true for software that has reported Common Vulnerabilities and Exposures (CVE). The MITRE Corporation and the National Institute of Standards and Technology (NIST) track CVEs and mark their level of criticalness. For example, when a critical vulnerability was found in the popular OpenSSL® cryptographic software in April of 2014, the TLS heartbeat read overrun (CVE-2014-0160) was tracked and marked by both organizations. A CVE such as the CVE-2014-0160 must be addressed as soon as possible.

Honeywell provides system updates for both security and feature-related purposes. If the third-party software has been installed, Honeywell recommends testing the update on a non-production system to ensure Honeywell software continues to operate correctly.

Firmware Downgrade Package Restrictions

Honeywell scanners verify all firmware downgrade processes to prevent downgrades that might permit malicious actors exploiting known security vulnerabilities and gaining access to a Honeywell scanner. Honeywell scanners prevent a downgrade to a less secure version by ensuring that the security level of the incoming firmware package meets or exceeds the security level of the currently installed package. If the incoming package matches or exceeds the security level checks, the Honeywell scanner permits the downgrade process without restrictions. However, if the incoming package fails to meet the security level checks, the scanner displays a message indicating that the downgrade process has failed.

Honeywell recommends that customers seriously consider each downgrade since any downgrade will put Honeywell scanners and the related network at risk. If a customer expects to downgrade, it is suggested to downgrade to latest previous installed firmware, this can reduce known risks to less. and is recommend to secure environment to mitigate known risk in an acceptable risk level, it's best to upgrade firmware as soon as possible once new latest firmware was validated.

Menu Command Security Considerations

Menu setting MNUENA specifies whether or not programming barcode security is enabled or disabled. (A value of 0 enables security, and 1 disables). If the PASWRD string is null, indicating low security mode, no password is appended to the MNUENA setting string. If the PASWRD string is non-null, the password must be included with the MNUENA setting string. In addition, if disabling menu security, the 1 for disable must be omitted so that only the password is appended to the MNUENA setting string.

Note: *Enabling (0) and disabling (1) programming barcode security is counter to the normal method of 1 being used to enable and 0 to disable. The reason for this is that MNUENA is a legacy setting used to enable menuing (value of 1) so that menu settings could be processed as programming barcodes. When PASWRD is null, MNUENA functions as it did in the past, but we now look at it as a security enable/ disable, and the values of 0 and 1 have therefore switched meaning.*

Programming Barcode (Menu) Security Introduction

Barcode scanners can be easily and conveniently configured using programming barcodes. However, in certain applications, the users would like to prevent the scanners from being configured by scanning a barcode. In high security installations, such as airport check-in, an incorrectly configured scanner can cause delays, errors, or even security breaches.

This feature is targeted to the following users:

- Customers who want to prevent accidental configuration changes via programming barcodes, and where security is not an issue. For RF configurations, the remove barcode is not required, but scanning a Bluetooth address barcode is required in order to be able to link to a different RF base or dongle.
- Customers who want to prevent deliberate (as well as accidental) configuration changes via programming barcodes but do want to be able to permit a password protected programming barcode to re-enable the usage of programming barcodes for configuration changes. For RF configurations, the remove barcode

is not required, but scanning a Bluetooth address barcode is required in order to be able to link to a different RF base or dongle.

- Customers who want to prevent deliberate (as well as accidental) configuration changes via programming barcodes and want to block processing of all programming barcodes, including the permitting of a password protected programming barcode to re-enable the usage of programming barcodes for configuration changes. For RF configurations, the remove and Bluetooth address barcodes are not required, but the ability to disable menu security by programming barcode (using the required password) in an RF scanner is required if that scanner is not currently linked in case the RF base it was associated with is broken or no longer available. The interface configuration for these customers will either be RS-232 or USB COM port emulation, and they will require no RF scanner linkage to a Bluetooth dongle. As there will be no means of turning programming barcode processing back on, except via the host link, these customers will require an interface configuration that readily supports configuration commands.

For RF configurations, all customers must:

- Be able to link an RF scanner to a secure RF base by placing it in the cradle in the same manner as if security were not enabled.
- Require that security won't affect the ability to relink after an RF scanner power down or other loss of link to a secure base.
- Require that the RF scanner process the programming barcode that overrides locked link mode.
- Require that a single security mode and password configuration apply to all scanners, regardless of work group.

Note that there is no concern about blocking commands and configuration changes via the host link, and that the host link can always be used to disable security. Note also that the first use case for this feature is in airports that are trying to meet IATA recommendations for CUTE (Common Use Terminal Equipment).

Implementation

Menu Security

In order to meet the customer requirements, three levels of menu security will be implemented, to be referred to as low, medium, and high, and will operate as follows:

- Low security mode: A menu setting will be used to enable/disable low security mode. No password will be required to either enable or disable. Programming barcodes are prohibited except in the following cases: Menu setting that enables/disables low security mode is allowed. For RF configurations, Bluetooth address barcode is allowed. For RF configurations, overriding locked link mode is allowed. No restriction on interface to host.

- Medium security mode: A menu setting will be used to enable/disable medium security mode, and must be accompanied by the password programmed into menu setting PASWRD (see definition below). Programming barcodes are prohibited except in the following cases: Menu setting that enables/disables medium security mode (accompanied by the password) is allowed. For RF configurations, Bluetooth address barcode is allowed. For RF configurations, overriding locked link mode is allowed. No restriction on interface to host.
- High security mode: A menu setting will be used to enable/disable high security mode and must be accompanied by the password programmed into menu setting PASWRD (see definition below). Programming barcodes are prohibited except in the following cases: Menu setting that enables high security mode (accompanied by the password) is allowed.

Note that disabling of high security mode via programming barcode is prohibited. For RF configurations, overriding locked link mode is allowed. For RF scanners, the menu setting that disables medium security mode (accompanied by the password) is allowed if that RF scanner is not currently linked.

While in high security mode, only RS-232 and USB COM port emulation interfaces will be permitted for corded scanners, and only an RF base link will be permitted for RF scanners (dongle link will not be allowed). The purpose of this restriction is to prevent the scanner from becoming unrecoverable due to no programming barcodes being allowed and no means of sending commands to the scanner to turn off high security mode. Automatic cable selection will not help because USB could still be configured for something other than COM port emulation, and while RS-232 is the only configuration in its cable class today, that could change in the future. Attempts to change the interface type menu setting to any other interface will be blocked (noting that this can only be done via the host link because programming barcodes are effectively disabled). If the cable configuration is changed to keyboard wedge or retail, or if the cable configuration is changed to USB when the USB interface type is not set to COM port emulation, the system will still function in high security mode, but will not allow the interface type menu setting to be changed for that cable configuration, except to change it to USB COM port emulation in the case of the USB cable configuration.

Note that disabling high security mode was considered in the instance that the interface configuration is no longer compatible, but this could pose a security risk by allowing someone to plug in a different cable and defeat high security mode. When enabling high security mode, the cable configuration must be either RS-232 or USB, and the interface type menu setting for USB must be COM port emulation. For RF scanners, the scanner must be configured to link to an RF base rather than to a dongle. If these conditions are not met, the device cannot be placed into high security mode.

There are no restrictions on configuration commands sent via the host link, except for certain restrictions to changing interface type when in high security mode (see above).

RF Configurations

The following will apply to RF configurations:

- Since the remove programming barcode is not required in any security mode, it will be blocked when any security mode is configured. The reason for noting this is that there was discussion about whether or not to allow this barcode, and we wish to document that it was specifically considered.
- Security mode configurations will have no effect on the ability to link an RF scanner to a secure RF base by placing it in the cradle.
- Security mode configurations will have no effect on the ability to relink after an RF scanner power down or other loss of link to a secure base.
- Menu settings associated with menu security will be common rather than work group settings. This will meet customer requirements, and will also be simpler than trying to manage a mix of security modes for different RF scanners linked to the same RF base, where an RF scanner configured in a less secure mode (or where security is disabled altogether) could be used to compromise security on an RF scanner configured in a more secure mode.
- Security mode configurations do not prevent a scanner from being forcibly removed from the RF base when another scanner is replacing it. Also, a scanner may be preempted in a Code XML dongle configuration (does not apply to high security mode for this dongle because dongle links are not allowed).
- As with all other menu settings, those settings associated with menu security will be stored in non-volatile memory on both the RF base and RF scanner(s). If programming barcode security is configured, this will cause the RF scanner to be secured even when it is not currently linked to the RF base. Note that this is the method of operation in the previous generation RF products and must be maintained going forward.
- When an RF scanner establishes a link to an RF base, it must not be able to configure the RF base via programming barcodes until the RF base has first pushed menu settings up to the RF scanner, thereby informing the RF scanner of the configured security mode. Note that this is the method of operation in the previous generation RF products and must be maintained going forward.

Programming Barcode Menu Settings

Programming barcode menu settings are as follows:

Menu setting PASWRD specifies the programming barcode security password and also is used to set the security mode (low, medium, or high). It is used in conjunction with menu setting MNUENA, which actually enables or disables the processing of menu barcodes.

The PASWRD string must consist of 0 to 12 alphanumeric characters.

- If the PASWRD string is null, the security mode is low.
- If the first character of the password string is “1”, the security mode is medium.

- If the first character of the password string is any alphanumeric character other than “1”, the security mode is high.

PASWRD may never be changed via programming barcode. It may always be changed via the host link.

Additional Resources

Security Resources	
The MITRE Corporation	http://www.mitre.org and http://cve.mitre.org
National Institute of Standards and Technology (NIST)	http://www.nist.gov
Open Web Application Security Project (OWASP)	http://www.owasp.org
U.S. National Vulnerability Database (NVD)	http://nvd.nist.gov

CHAPTER

3 DEVELOP A SECURITY PROGRAM

Honeywell uses Building Security In Maturity Model (BSIMM) as our chief assessment tool for continuously improving the security maturity for our products and solutions. BSIMM https://www.bsimm.com/framework.html is a maturity framework which organizations can use to help understand the maturity of their product security process and practice. The model is based on observational science around software security and is continuously being updated and evolving. It is conducted on organizations across many different industries.

Note: *Honeywell recommends making use of such frameworks to gauge the maturity and progress needed in the user's own cybersecurity program.*

Form a Security Team

When forming a security team, you should:

- Define executive sponsors. It will be easier to ensure the success of security procedures if you have the backing of senior management.
- Establish a core cross-functional security team of representatives that include:
  - Building or facility management:
    Individuals responsible for running and maintaining Honeywell scanner devices and infrastructure.
  - Business applications:
    Individuals responsible for applications interfaced to the Honeywell scanner system.
  - IT systems administration
  - IT network administration
  - IT security

Executive sponsorship and the creation of a formal team structure is a recommendation for the security program. The remaining tasks in the development of a security program are critical to the success of the program.

Identify Assets to be Secured

The term “assets” implies anything of value to the company. Assets may include equipment, intellectual property such as historical data and algorithms, and infrastructure capabilities such as network bandwidth and computing power.

When identifying assets at risk, you should consider:

- People, including your employees and the broader community to which they and your enterprise belong
- Plant and Computer Equipment
  - Plant equipment including network equipment (e.g., routers, switches, firewalls, and ancillary items) used to build the system
  - Computer equipment such as servers, cameras, and streamers
- Network configuration information (e.g., routing tables and access control lists)
- Information stored on computing equipment (e.g., databases and other intellectual property)
- Intangible assets (e.g., bandwidth and speed)

Identify and Evaluate Threats

You need to consider the potential within your system for unauthorized access to resources or information through the use of a network and the unauthorized manipulation and alteration of information on a network.

Potential threats to be considered include:

- People
  - Malicious users inside or outside the company
  - Uninformed employees
- Inanimate threats
  - Natural disasters such as fire or flood
  - Malicious code such as a virus or denial of service

Identify and Evaluate Vulnerabilities

Potential vulnerabilities that should be addressed in your security strategy include:

- The absence of security policies and procedures
- Inadequate physical security
- Gateways from the Internet to the corporation
- Gateways between the business LAN and scanner network

- Improper management of modems
- Out-of-date virus software
- Out-of-date security patches or inadequate security configuration
- Inadequate or infrequent backups

Failure mode analysis can be used to assess the robustness of your network architecture.

Identify and Evaluate Privacy Issues

Consider the potential for unauthorized access to personal data stored within your system. Any information considered sensitive should be protected and all access methods should be reviewed to ensure correct authorization is required.

Create a Mitigation Plan

Create policies and procedures to protect your assets from threats. The policies and procedures should cover your networks, computer hardware and software, and scanner equipment. You should also perform risk assessments to evaluate the potential impact of threats. A full inventory of your assets helps identify threats and vulnerabilities. These tasks assist you in deciding whether to ignore, mitigate, or transfer the risk.

Implement Change Management

A formal change management procedure is vital for ensuring any modifications made to the scanner network continue to meet the same security requirements as the components included in the original asset evaluation and associated risk assessment and mitigation plans.

A risk assessment should be performed on any change made to the scanner and its infrastructure that could affect security, including configuration changes, the addition of network components, and the installation of software. Changes to policies and procedures might also be required.

Plan Ongoing Maintenance

Constant vigilance of your security program should involve:

- Regular monitoring of your system
- Regular audits of your network security configuration
- Regular security team meetings where keeping up-to-date with the latest threats and technologies for dealing with security issues are discussed

Additional Security Resources

Information Security Standards	
European Network and Information Security Exchange	http://www.enisa.europa.eu/
British Standards Institution - Information Security	http://www.bsi-global.com
International Organization for Standardization (ISO)	http://www.iso.org
Center for Information Security (CIS)	https://www.cisecurity.org

Information Technology – Security Techniques	
ISO 15408 - Evaluation Criteria for IT Security, Parts 1 - 3	http://www.iso.org
ISO 27002 - Code of Practice for Information Security Management	http://www.iso.org
Open Web Application Security Project (OWASP) The OWASP tracks the top weaknesses of applications and provides valuable information about developing secure software.	http://www.owasp.org/

CHAPTER

4 SYSTEM MONITORING

The security recommendations outlined in this guide help reduce security risks but do not guarantee that an attacker may not be able to circumvent the safeguards put into place to protect network systems and devices. Early detection of an attack and/or system breach is essential to preventing further damage. The earlier a system intrusion is detected and the more evidence that is captured, the less damage is likely to occur and the greater the chances of identifying the intruder.

Providing a means to detect and document system exploits is vital. For example, the anti-virus package used should provide a method to collect logs created by the package. The logs should be available for retrieval via the package and a related console application on a server or via remote device management software. Periodical collection of additional logs (such as VPN connection information or login access failures) should also be implemented.

Intrusion Detection

Network Intrusion Detection Systems (NIDS) can take many forms. NIDS can be a dedicated server on the same network branch, freeware software available under GNU or similar licenses (often UNIX® based), or commercial products aimed specifically at Windows systems.

The purpose of NIDS is to scan incoming network packets and look for unusual traffic or for specific malformed packets known to be associated with attacks. If anomalies are found, NIDS take action such as raising alerts or even disconnecting the computer from the network. The latter is a dangerous option that causes denial of service while preventing damage from occurring to the system (e.g., by closing network ports).

Most firewalls, switches, and routers have reporting facilities whereby they can report various levels of events, varying from debugging to emergency failure. These reports can be viewed via secure shell (SSH), collected by a central logging server, or sent via email to an administrator. For example, the Cisco® PIX firewall and Catalyst® 4500 switches can be configured to send selected levels of events to a central syslog server where further analysis can occur and significant events can be detected.

Operational Technology Security

Honeywell recommends these cybersecurity best practices when implementing devices and solutions.

Best Practice	Description
Application Whitelisting	This practice aligns with a key cybersecurity principle of "least privilege", where a user should only have the capabilities needed to perform their job function. Limiting the amount of applications installed on a device greatly reduces the attack surface against the device and an intentionally malicious user.
Ensuring Asset Visibility	Knowing the assets in your infrastructure and where they are located is critical to keeping an organization safe and secure in a connected world. Honeywell offers tools and applications, like Honeywell Operational Intelligence, as well as support on the best strategies for your specific needs when it comes to asset visibility.
Vendor Partnerships	Working together with your vendor in a close partnership is crucial in keeping up with the complexity of deploying Operational Technologies to enable your workforce. Technology is quickly evolving and so are threat agents. Honeywell looks forward to working with our customers to keep them secure.
Staying Up-to-Date	Work with vendors who take cybersecurity seriously and respond quickly to constantly evolving threats around the world. Honeywell recommends developing a cadence on patching and updating your devices, as well as using the latest operating system to leverage new security features and enhancements.
Be diligent and aware of Regulatory Frameworks	The regulatory environment around cybersecurity and data privacy is quickly adapting to the demands of a connected and digitized business environment (GDPR and CCPA). Working with a vendor that can provide you "out-of-the-box" compliance and assurance is important. It is also imperative to develop your own framework around data privacy to ensure applications running your infrastructure are compliant.

Honeywell Operational Intelligence

Honeywell Operational Intelligence is a cloud-based software solution that systematizes service workflows and aggregates and analyzes real-time information from all of your devices.

For more information, go to sps.honeywell.com.

CHAPTER

5 SECURE WIRELESS DEVICES

Wireless Local Area Networks and Access Point Security

Some Honeywell scanner models are equipped with an 802.11x Wireless Local Area Network (WLAN) radio. The radio is interoperable with other 802.11x, Wi-Fi compliant products, including access points (APs), workstations via PC card adapters, and other wireless portable devices.

When the scanner connects through a wireless access point (AP) to an organization's server on a wired network, specific security precautions are required to mitigate the significant security risk the WLAN wireless AP connection represents for the servers and devices on the wired network.

Non-scanner wireless devices (such as laptops and printers) should either be on a separate WLAN with different security profiles or the wireless AP should, at a minimum, support multiple service set identifiers (SSIDs). Devices on one WLAN should not be able to use the WLAN to connect to devices on another of the organization's WLANs. Isolation of different networks helps protect the scanner and the organization's other networks and devices from unauthorized access.

Secure Wireless AP Configuration

Honeywell recommends the following when configuring a wireless AP:

- Configure a unique SSID. Do not use the default SSID
- Disable SSID broadcast
- Configure authentication for EAP authentication to the network. PEAP and EAP-TLS are preferred
- Configure the RADIUS server address
- Configure for WPA2/WPA3 Enterprise
- Change the WAP RADIUS password. Do not use the default password
- Configure 802.1x authentication
- Enable MAC filtering and enter the MAC addresses for all the wireless devices. This prevents unauthorized devices from connecting to the wireless network.

For detailed configuration information, refer to the setup instructions from the wireless AP supplier.

Secure Scanner WLAN Configuration

Honeywell recommends the following when configuring a scanner with Wi-Fi capable for WLANs:

- Configure the proper SSID
- Configure 802.1x authentication
- Configure Protected EAP authentication
- TLS, EAP-PEAP-TLS and EPA-PEAP-MSCHAP are supported
- Configure the 802.1x supplicant (client) to prompt for the password needed by EAP-PEAP/MSCHAP, EAP-TTLS/MSCHAP
- If EAP-TLS or EAP-PEAP-TLS are in use, a client certificate must be available on the scanner

Wireless Near Field Communication Security

Specific security precautions are recommended to mitigate the potential security risk associated with exchanging data using wireless Near Field Communication (NFC) between NFC enabled Honeywell scanner devices and NFC tags or other NFC enabled devices.

NFC security is based on the short range characteristic of the RF solution. In some applications, there is the potential for an attacker to utilize the BT pairing with NFC and/or other applications to attack the scanner device with NFC.

Honeywell recommends the following security recommendations and precautions listed below:

- Disable NFC on the device unless it is critical to the application
- If the application must allow NFC, it should only be enabled as needed and the user must have a means to confirm the transfer is expected. If the application transfers data between two scanners using NFC, then the application should enable encryption of the data.

RFID

RFID (Radio Frequency Identification) is a method to communicate information from one point to another point by the use of electromagnetic waves (radio waves). RFID has unique characteristics that make it attractive for use in industrial systems.

Data and Tag Security

- Tag Passwords - You can set optional 32-bit passwords that allow you to access tag data, to lock tag data, or to permanently disable a tag.

- Data Locking Options - Tag memory can be safeguarded with flexible locking options. For example, you can lock a tag's memory to prevent it from being encoded accidentally and later unlock it for writing. A permanent locking feature prevents rewriting of tag data.

APPENDIX

A GLOSSARY

General Terms and Abbreviations

Authentication

When a user logs on to a system, the authentication process verifies the user is known to the system. See also “authorization”.

Authorization

When a user logs on to a system, the authorization result dictates what a known user can do within the system. See also “authentication”.

Business network

A collective term for the network and attached systems.

Digital signature

Using the private key of a digital certificate to encrypt the digital hash (digest) of an electronic document, code file, etc.

Firewall

A firewall is a software or hardware barrier that sits between two networks, typically between a LAN and the Internet. A firewall can be a standalone network appliance, part of another network device such as a router or bridge, or special software running on a dedicated computer.

Firewalls can be programmed to block all network traffic from coming through except that which has been configured to be allowed. By default, a firewall should block all 65,536 ports and open up only the ports you need. If you need to browse the Web, then it should allow “outgoing” traffic on port 80. If you would like DNS lookups to work for you, port 53 needs to be opened up for “outgoing” traffic. If you want to access your Internet mail server through POP3, open up port 110 for outgoing traffic. Firewalls are directional. They monitor where the traffic originates for both “incoming/inbound” and “outgoing/outbound” traffic.

Quite frequently you will not want any unsolicited inbound traffic unless you have specific reasons (for example, you might have a Web server that you want people to access). However, in most cases, a Web server would probably be located outside your firewall and not on your internal network.

The following Microsoft reference is a useful source of information about well-known TCP/IP ports: http://support.microsoft.com/kb/832017.

IAS

Internet Authentication Service (IAS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy.

LAN

Local Area Network

MAC

Media Access Control (MAC) is the lower level of the Data Link Layer (under the IEEE 802.11-1997 standard). In Wireless 802.11, MAC stands for “Medium Access Control”. MAC can also be an abbreviation for “Message Authentication Codes”, a cryptographic hash added to a message to enable the detection of tampering.

PEAP

Protected Extensible Authentication Protocol (PEAP) is a protocol proposed for securely transporting authentication data, including passwords, over 802.11 wireless networks.

Port

A port is a logical endpoint on a network computer or device used for communications. There are approximately 65,536 ports on which any one IP address can communicate. Some are dedicated to specific well-known services; some are used by application services; and some will be dynamically allocated to clients as they connect to remote services. A service listens on a known port for client connections, if the connection is accepted, the client will address messages to that port, and the server will send responses to the dynamically allocated client port.

RADIUS

Remote Authentication Dial In User Service (RADIUS) is a protocol that enables centralized authentication, authorization, and accounting for dial-up, virtual private network, and wireless access.

SDL

Security Development Lifecycle (SDL) is a software development process that helps developers to build more secure software and to address security requirements while reducing development cost.

SNMP

Simple Network Management Protocol (SNMP) is a protocol used to manage devices on IP networks.

SSID

Service set identifier (SSID) is a unique identifier for a wireless network.

Subnet

A group of hosts that form a subdivision of a network.

Subnet mask

A subnet mask identifies which bits of an IP address are reserved for the network address. For example, if the IP address of a particular computer or device is 192.168.2.3 with a subnet mask of 255.255.255.0, this subnet mask indicates the first 24 bits of the address represent the network address and the last 8 bits can be used for individual computer or device addresses on that network.

Switch

A switch is a multi-port device that moves Ethernet packets at full wire speed within a network. A switch may be connected to another switch in a network.

Switches direct packets to a destination based on their MAC address. Each link to the switch has dedicated bandwidth (for example, 100 Mbps).

TCP/IP

Transmission Control Protocol/Internet Protocol.

TLS

Transport Layer Security

WAN

Wide Area Network

WAP

Wireless Access Point

WPA

Wi-Fi Protected Access (WPA) is a security standard adopted by the Wi-Fi Alliance consortium for wireless networks (www.wi-fi.org).

WPA2

Wi-Fi Protected Access 2 is the replacement for WPA.

WPA3

Wi-Fi Protected Access 3 provides more security options than WPA and WPA2.

Honeywell
855 S. Mint Street
Charlotte, NC 28202

sps.honeywell.com