**Integrating the Healthcare Enterprise**


# IHE Patient Care Device (PCD)
# White Paper

# Medical Equipment Management (MEM): Medical Device Cyber Security – Best Practice Guide

## Published

**Revision 1.1**

Date: October 14, 2015
Author: IHE PCD Technical Committee
Email: pcd@ihe.net

**Please verify you have the most recent version of this document.** See here for Published versions and here for Public Comment versions.

## Foreword

This white paper is published on October 14, 2015. Comments are invited and can be submitted at http://www.ihe.net/PCD_Public_Comments/.

General information about IHE can be found at: www.ihe.net.

Information about the IHE Patient Care Device domain can be found at: ihe.net/IHE_Domains.

Information about the organization of IHE Technical Frameworks and Supplements and the process used to create them can be found at: http://ihe.net/IHE_Process and http://ihe.net/Profiles.

The current version of the IHE Patient Care Device Technical Framework can be found at: http://www.ihe.net/Technical_Frameworks.

**CONTENTS**



 

 

# 1 Introduction & Background

Ever since clinicians, physicists and engineers have learned how to apply technology to improve diagnosis and treatment of patients[1], medical devices have become an integral part of our healthcare delivery system. And, as technology progresses, so have the capabilities of and opportunities for medical devices. What used to be individual devices applied to specific clinical problems is now an integrated network of devices and IT components, working in an orchestrated fashion with clinicians, thus helping us to diagnose more efficiently and granularly, and helping us to treat less invasively and more reliably. This produces widely improved outcomes, extends lives, improves efficiency, and reduces costs.

However, as medical devices contain more and more software (including commercial software components like the operating system) and are integrated with hospital IT networks, they are also exposed to the same cyber-threats as any other IT system. For example, they can be infected by malware or hacked into with malicious intent, both of which can impact care delivery or even harm patients or could lead to the breach of sensitive health information.

This document takes a comprehensive approach to medical device cyber-security by documenting:

- How today's medical devices are used and incorporated in our IT environments.
- What type of cyber-threats they are exposed to and how these threats can affect the medical device ecosystem.
- A review of best practices to design security into medical devices and how to build a reliable medical device network, ranging from asset and configuration management, access control, to actual cyber-security protective measures.

Unlike regular IT components used in the healthcare environment, medical devices are not only mission-critical, they are also safety-critical. However, at the same time many factors contribute to making medical devices less secure, including:

- A generally low cyber-security maturity.
- A long useful life often resulting in the use of end-of-support software components.
- Slow security patch deployment.

This document focuses mainly on networked medical devices and their security risks, however, some aspects of this may be equally applicable to stand-alone devices. It is intended to provide guidance to medical device manufacturers as well as hospital biomedical engineering and IT departments on how these difficult issues can be addressed as well as other roles like risk managers, independent test labs, regulators, or similar.

[1] "Über eine neue Art von Strahlen", W.C. Röntgen, Sitzungsbericht der Würzburger Physik.-medic. Gesellschaft, pages 137–147, 1895

 

A previous IHE PCD white paper had been published to raise awareness of the medical device cybersecurity problem and to develop a general understanding of the topic.[2] This new white paper will expand on the topic by providing a deeper analysis of the risks and offer guidance and best practices to medical device manufacturers and healthcare organizations.

At the time of this writing, the majority of the discussion on the topic is driven by U.S. regulators and organizations. This makes this document somewhat U.S.-centric, but the discussed topics and best practices have international applicability.

## 1.1 Acknowledgement

This white paper was developed by a group of subject matter experts within IHE PCD (Integrating the Healthcare Enterprise, Patient Care Device Domain). IHE PCD would like to acknowledge the following contributors to this document:

| | |
|---|---|
| Richard Hurst | Hive Technologies |
| Daniel Leslie | Namely Inc. |
| Geoffrey A. Pascoe | Deloitte & Touche LLP |
| John Rhoads | Philips Healthcare |
| Andrew Sargent | Philips Healthcare |
| Daniel Trainor | Philips Healthcare |
| Stan Wiley | Dräger Medical Systems |
| Axel Wirth | Symantec |


[2] "Medical Equipment Management (MEM): Cyber Security "; IHE Patient Care Device (PCD) White Paper; http://ihe.net/Technical_Framework/upload/IHE_PCD_White-Paper_MEM_Cyber_Security_Rev2-0_2011-05-27.pdf

## 2 Objective

The medical device ecosystem is complex and providing guidance and suggested best practices on how to better secure it is a formidable challenge. On the device manufacturers' side the issues to be addressed range from device design considerations, through best engineering practices, to protecting the manufacturing environment to assure that no risks are introduced into the finished device. On the healthcare providers' side it includes device management, integration and secure networking best practices, as well as the collection and analysis of device vulnerabilities, security events, and system logs. Both, manufacturer staff and hospital staff, require up-to-date security education as well as strategic support from their business leadership.

As Figure 1 illustrates, the topic can not only be limited to pure security since aspects of medical equipment management, privacy and breach risks, and access and authentication all play together in a complex web of interdependencies. And all of it has to be managed in a highly regulated environment.

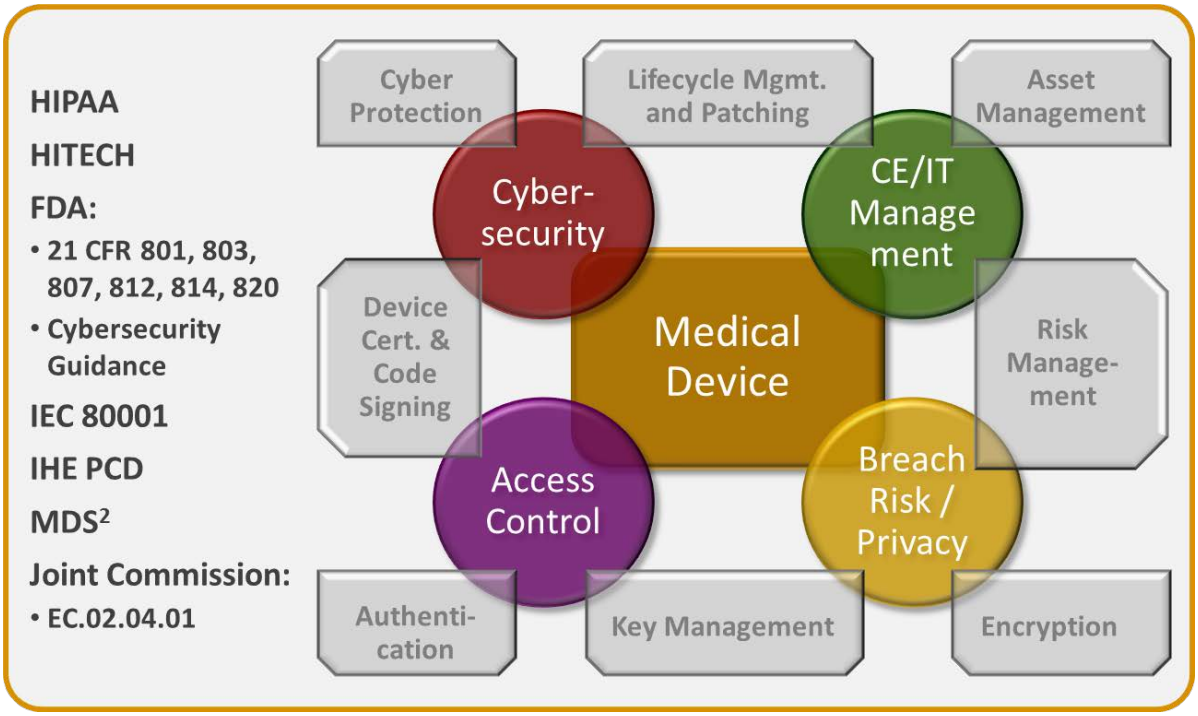


**Figure 1: The Complexities of Medical Device Security**

It is the objective of this document to provide a comprehensive review of the medical device cyber-security topic and to provide best practice guidelines on how to mitigate and minimize the associated risks. As cyber-threats continually evolve, now faster than ever, this document can only be a snapshot and status review as of the time of this writing. Readers are advised to stay vigilant and keep their cyber-security knowledge up to date.

# 3 Stakeholder Roles and Contributions

This white paper focuses on cyber-security challenges of networked medical devices and the potential impact of cyber-security incidents on the safe and effective delivery of services by healthcare provider organizations. This results in the need of security being an integral process within the organization's quality management system; from top management to responsible employees. In brief, that implies that there must be ongoing development and implementation of a set of interrelated processes to plan, execute, evaluate and improve medical equipment management with emphasis on secure operation (including cyber-security) and maintenance methodologies for meeting customer needs as well as statutory and regulatory requirements. The specific risks must be determined and appropriate mitigating measures taken. Management, at the highest levels, needs to establish the business and organizational goals and commit to seeing that the processes are created and documented, and that resources are made available to carry out these responsibilities.

Besides the hospital departments (e.g., biomedical/clinical engineering, information technology) and the actual clinical users (doctor, nurse, technician), other key stakeholders involved include manufacturers, outside service providers, and training providers, all having responsibilities that must be carefully defined, coordinated, and documented. Biomedical engineering, IT, clinical professionals, and institutional management all must be relied on to take responsibility for appropriate aspects of risk analysis and management, and these responsibilities must be documented as part of the creation and maintenance of the quality system plan.

This is not a simple task, based on the critical function provided by medical devices, but also based on the complexity of the medical device ecosystem. Healthcare providers have thousands, if not ten thousands of devices of hundreds of different types that are provided by dozens of large to small manufacturers; for large organizations these numbers may be even higher by an order of magnitude. The plan must take the special characteristics, use case, and risk profile of specific categories of medical devices into consideration.

Manufacturers have a responsibility to provide sufficiently detailed technical information in order to enable the health delivery organization's (HDO's) security and safety risk management process to proceed on a sound basis:

- Device cyber-security properties:
  - Details on the security properties of the device and the technical security controls implemented.
  - The expected security environment into which a device may be installed and supplemental security measures that may be required.
  - Security best practices and details on how security of the device should be maintained.
  - Ongoing information about vulnerabilities discovered or security updates to be implemented.
  - Description of any security-relevant third party components used, e.g., IT components or the operating system.

 

- Details on security dependences between device(s) and supplemental IT components, e.g., workstation, servers, or network components.

- Security monitoring and response:
  - Capabilities to detect, log, alert, and respond to security incidents.
  - If implemented, fail-safe operational mode.
  - If implemented, safe recovery.

- Information privacy properties and requirements:
  - Description pertaining to information privacy of data stored on or transmitted by the device.
  - If applicable, ability to pseudonymize or de-identify data.
  - Description of technical measures to protect data privacy (e.g., encryption).
  - Measures implemented to assure data authenticity and integrity.
  - Definition of information properties (data types, data retention, data removal, etc.)
  - Features supporting auditing of access to private health data.
  - Any features of the device supporting backup and restoration of patient and/or configuration data.

- Authentication and authorization (as appropriate for the use case):
  - Role based, layered authentication.
  - Emergency access management (e.g., break-the-glass feature).
  - Session and time-out management.
  - Implemented password rules: strength, lifecycle, no hardcoded or default password, etc.
  - Two factor or other strong authentication methods, esp. for privileged user access.
  - Physical locks of ports and interfaces if needed.
  - If implemented, device certificates and device authentication management.
  - Secure software update, e.g., code signing.

- Lifecycle management:
  - Special handling requirements during the lifecycle of the device (installation, maintenance, end of life, etc.)
  - Specifically, lifecycle management activities required for keeping device security features up-to-date and effective.

- Regulatory compliance and documentation:
  - Regulatory requirements and standards the device complies with (FDA, The Joint Commission, European Privacy Directive, IEC, etc.)
  - Hazard analysis, list of security risks considered, description of security controls.
  - Process for regular and timely communication to device operator on newly discovered security risks.
  - Specific security guidance for the operator of the device.

 

# 4 Cybersecurity Introduction

Integrating Medical Devices into a standard IT network creates numerous challenges and risks. Biomedical Engineers, IT staff, risk managers, and manufacturers need to be vigilant and cooperate closely to securely maintain today's complex device networks so as to assure confidentiality, integrity and availability.

Technology drivers provide us with opportunities to reduce costs, create efficiencies, or improve clinical care; yet at the same time add their own set of challenges as we virtualize our server and storage infrastructure, move to wireless networks, exchange data via cloud services, and participate in Big Data initiatives.

Most medical devices are more vulnerable to cyber-attacks than normal IT endpoints (desktops, laptops, servers), whether it is a specifically targeted attack on the medical device or an unintentional infection of it by common malware. The reasons for this are many and include:

- Long product life and as a result, the use of outdated software components, like the operating system, and a legacy security architecture not suited to withstand today's sophisticated threats.
  For example, devices may have been designed to be connected to a proprietary and local network, rather than the relatively open enterprise network and therefore may not be sufficiently protected against network-based threats. Further, devices are often used beyond their End of Support (EOS) horizon or the End of Life (EOL) of commercial software components.
  As discussed previously, device manufacturers should provide guidance on their devices' security posture and intended use environment. However, this should not be a way of rolling off responsibility to the end user, but rather provide constructive advice on device properties, integration guidance, and the like.

- Regulatory-introduced overhead on the release and deployment of device upgrades and patches, which generally makes these available later than in the normal IT environment. Note that existing medical device regulations, e.g., through the U.S. FDA, do not prevent the deployment of security patches nor would they require resubmission for device approval, but they do require manufacturers' formal testing of any upgrade or patch to assure continued safety of the device.[3]

- Devices need to be available (or are in use) 24x7, which makes it difficult to perform software upgrades or troubleshoot cyber-security incidents. Many hospitals struggle with the balance between IT priorities (e.g., cyber-security) vs. Biomedical Engineering priorities (e.g., device availability, safety, and reliability).
  This becomes a particular challenge when devices of one type and/or supporting IT components (workstations, servers) need to be upgraded in-unison

[3] "Medical Device Software Patching"; White Paper; IHE PCD in cooperation with MDISS available at http://ihe.net/Technical_Frameworks/#pcd

## 4.1 Basic Cyber-Security Considerations

This section will review the major security challenges we are facing today and will provide an update on the changing regulatory landscape, increasing threats, and best practices that can be applied to minimize risk and impact.

Any device containing software and being accessible from the outside, be it via network, proprietary interface, or data carrier, is at risk of being exploited. In addition, any software component installed on the device during the manufacturing, maintenance, or upgrade process can be contaminated and introduce a vulnerability or even malware itself.

Following is a definition of common terminology used in this document:[4, 5]

- **Vulnerability**: A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard.
- **Exploit**: A technique to breach the security of a network or information system in violation of security policy.
- **Attack Vector or Attack Path**: The steps that an adversary takes or may take to plan, prepare for, and execute an attack.
- **Attack Surface**: the sum of the different attack vectors where an unauthorized user or adversary can try to penetrate a system or information environment.
- **Threat**: A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.
- **Cyber-security**: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.
- **Risk**: The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences.

This paper will predominantly deal with the risks introduced through the use of standard / commercial technologies, whether they are off-the-shelf software components like the operating system, or standard interfaces and protocols, e.g., TCP/IP, USB, or other file or network services. Such attacks can be complex and may exploit several components, e.g., a piece of malware introduced via a USB memory device and executed based on the operating system's Autorun

[4] "Explore Terms: A Glossary of Common Cybersecurity Terminology", National Initiative for Cybersecurity Careers and Studies (NICCS), http://niccs.us-cert.gov/glossary

[5] Source: Wikipedia, the Free Encyclopedia (accessed 01/31/2015)

feature, then distributing itself via Fileshares or print spooler to other devices with the same vulnerability profile.

The reason that we now need to be more vigilant than ever about cyber-security is threefold:

- Exponential growth and dramatically increasing sophistication of cyber-threats.
- Explosive information growth and shift from physical formats (e.g., paper) to digital.
- Increasingly providing functionality through interconnection of devices, a trend commonly referred to as "The Internet of Things" (which includes medical devices in the hospital as well as the patients' homes).

Combined, these trends not only result in increasing exposure and a higher risk, but also in a higher dependency on the availability of information, systems, networks, and devices.

As we develop regulations, best practices, policies and procedures, implement safeguards, and educate our staff, the focus of our effort has to be threefold:

- **Confidentiality**: The property that data or information is not made available or disclosed to unauthorized persons or processes.
- **Integrity**: The property that data or information have not been altered or destroyed in an unauthorized manner.
- **Availability**: The property that data, information, or systems are accessible and useable upon demand by an authorized person.

In traditional health information systems, the priorities are typically confidentiality, then integrity, and availability (C-I-A) whereas with networked devices which support clinical function, it is typically availability first, then integrity and confidentiality (A-I-C). Although this statement is somewhat generalized, it does highlight the different nature of the mission of business critical information systems as compared to life and safety critical medical devices and their need for highest reliability to assure maximum patient safety. This is not only reflected in the hospital-internal processes and priorities, e.g., the different job functions of IT and Biomedical Engineering, but it also resulted in very different regulatory frameworks and guidance.

Any security strategy needs to be based on an up-to-date understanding of the threat landscape and its rapid evolution, combined with continual vigilance and the implementation of current security best practices. We cannot control the cyber-threats we are exposed to, but we can control how we manage, protect, and integrate medical devices on our networks, and we can reduce the risks by user education and influence on the manufacturers in the purchasing process.

In a technical sense, we need to look at this as a "system of systems" problem, where a solution includes all components from the individual device over the network to the perimeter, as well as all participating parties. Although the device itself is a key part of the protective strategy, the real solution is much bigger and includes network architecture, processes on device usage and management, cooperation with the manufacturer, and the overall regulatory environment. Even though isolating a device, or groups of devices, may reduce exposure, infections through e.g., portable media (so-called "air-gap" attacks) are still possible and have been reported.

 

Depending on the nature and intent of the outbreak or attack, its impact can be very different:

- Operational and financial impact due to device downtime or even loss of an entire clinical function or department through the spread of a malware infection to devices of the same type and with the same vulnerability.
- Performance impact due to the network overhead created by the infection or attack itself, or by the response of the enterprise's security technology and its effort to fight the outbreak or attack.
- Full or partial loss of device functionality, potentially impacting patient care and safety.
- Indirect impact on devices through a network manifestation of an attack or outbreak. For example, even if a Distributed Denial of Service attack (DDoS) may not impact the device itself, it may impact the device's connectivity and ability to receive or send information.
- Lastly, a medical device's generally poor security posture could be used to attack and penetrate the larger enterprise. Even though the device itself may not be the target, it may become the weak link enabling an attack.

Although to date there have not been any reported cases of a targeted attack on medical devices outside of security research, there are plenty of examples of unintended infections of devices through common malware. Although the malware may not be targeted at the device, the fact that the device is poorly protected and it matches the malware's target profile, e.g., a specific operating system, makes it a likely candidate for an infection and outbreak. And even though there may not be any malicious intent behind the event, it will indirectly affect patient care through operational downtime and it will impact business through financial, trust, and staff morale consequences. Therefore, the implications of unintentional attacks are real and we are seeing the impact as "collateral damage".

## 4.2 Risk Classification and Assessment

Healthcare organizations have thousands if not tens of thousands of medical devices in use, and many of them already connected and networked. A prerequisite to minimizing the overall exposure and security risk is to:

a) have a complete device inventory (including software, version, configuration, patch level, connectivity, and use case), and

b) perform a thorough security risk assessment, leading to a classification of devices based on their risk profile and the proper prioritization of protective countermeasures.

Processes for this approach are, for example, provided in the IEC 80001 series of standards: "Application of risk management for IT networks incorporating medical devices".[6]

[6] "IEC 80001-1:2010 - Application of risk management for IT-networks incorporating medical devices -- Part 1: Roles, responsibilities and activities", International Standards Organization (ISO), http://www.iso.org/iso/catalogue_detail.htm?csnumber=44863

Specifically, the general process of assessing a medical device inventory risk should include considerations of:

- The likelihood of the device being attacked, breached, or infected with malware.
- The severity or impact of the possible compromise. This requires a classification of devices based on their risk to patient safety, clinical use and function, and impact on operations and revenue.
- The actual device architecture and technologies used. A complex device running a commercial operating system and connecting via standard TCP/IP protocol has a very different risk profile than a device built on a proprietary platform and using non-standard interfacing. It is not whether one scenario is more critical than the other; it is about correctly assessing their respective risks relative to each other.

Although the FDA's recently provided regulatory guidance is now available as an official and final version[7], today we still lack security standards and consistent best practices to address the cyber-security risks of medical devices. Other industries, like manufacturing or energy, have taken these steps earlier than healthcare and can be used as a model and guidance.

Although there are unique aspects to the healthcare industry, for example the regulatory environment (HIPAA, FDA, European Union's Medical Device Directive) and the risk to patient safety and potentially even lives, we can use other industries as a reference and to develop an understanding of their formal approach to cyber-security as a model for how this problem could be solved in healthcare. In spite of some of the differences, we find several commonalties across industries, like the previously discussed criticality of infrastructure, the long useful product life, availability and reliability requirements, difficulties with upgrades and patching, and around-the-clock utilization.

As the healthcare industry is moving forward to more formally provide guidance, structure, and regulation to improve the overall security posture of medical devices and their networks, we can look at the approach taken in other industries, for example IEC 62443 "Industrial Automation and Control Systems Security"[8] or NERC 1300 "Critical Infrastructure Protection, Cyber Security"[9]. Although these or other standards cannot be directly applied to healthcare, they provide a useful reference and framework on how the complex problem of protecting critical infrastructure systems can be addressed.

[7] "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff", U.S. Food and Drug Administration (FDA) (Oct. 2, 2014), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

[8] "IEC 62443-1-1: Security for Industrial Automation and Control Systems - Models and Concepts", ISA99 Committee, http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx

[9] "(CIP) Critical Infrastructure Protection, Cyber Security CIP-002 through CIP-009 ", North American Electric Reliability Corporation (NERC), http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

# 5 Generic Device Architecture

For the purpose of this document, we have developed a generic device and integration architecture used to illustrate the requirements and implications of cyber-threats and cyber-security on medical devices. This architecture is highly generalized and should be viewed only as explanatory and in the context of this document. Individual devices will look different and architectures developed for different purposes (e.g., to illustrate device operation) will be different, may be more or less detailed, and may use a different representation and organization of the individual components.

Further, due to the previously discussed complexity of the medical device ecosystem, the integration of medical devices within the larger enterprise can only be depicted on a high and general level. Again, the purpose of this medical device integration architecture is to discuss and illustrate cyber-threats and cyber-security, but not to focus on network functionality or topology.

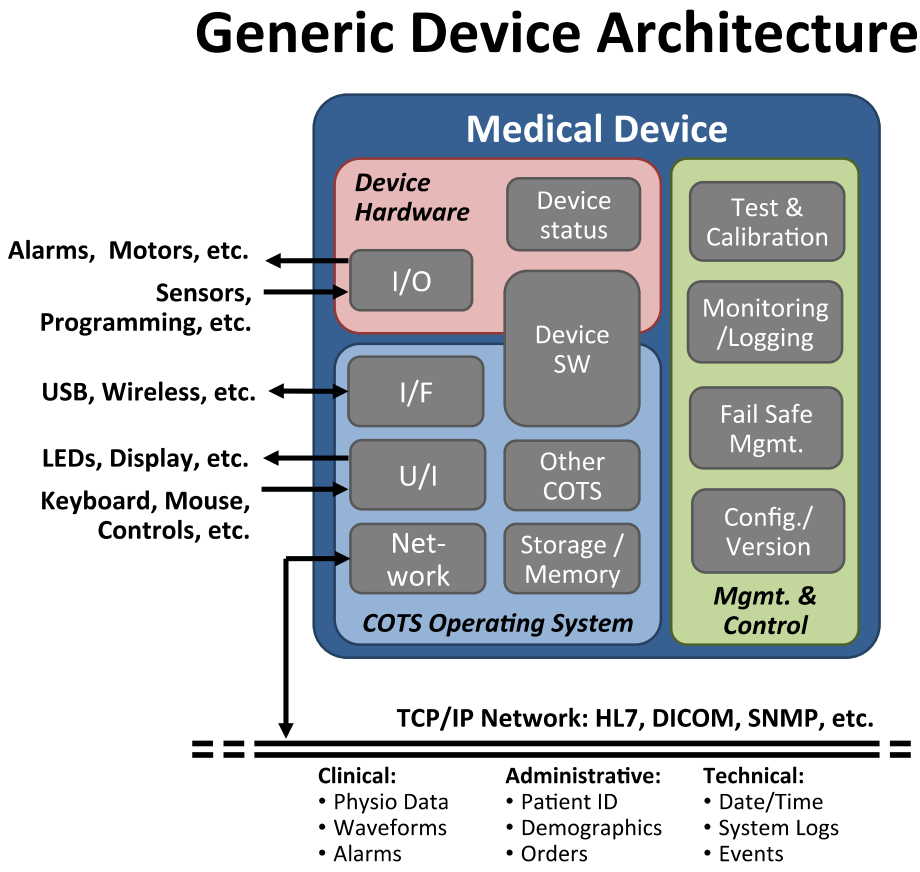


**Figure 2: Generic Medical Device Architecture**

In above Figure 2, we show the main components of the generic medical device as they pertain to a security discussion. This is for discussion purposes only, and a given device may be simpler or more complex and may contain more or fewer components.

- Device Hardware: Typically performance, function, and real-time critical, including:
  - Hosting Device Software: Usually close to the device's hardware or firmware, time-critical, controls and manages its functionality, signal input/output, and device status controls and registers as well as integration and interfacing between higher level software (e.g., the O/S) and lower level software (e.g., device firmware).
  - I/O: Dedicated input/output operation, which may account for the actual device functionality. E.g., output to motors, stimulators, or signal generators; input from electrodes, sensors, or dials and switches.
  - Device Status: Any register or memory used to store settings, log events, or retain other status or control data.
- COTS (Commercial off-the-shelf) Operating System: The device's O/S environment (and the associated commercial-architecture hardware platform it runs on) typically performs the devices higher-level functions but is less performance- and real-time critical. The O/S may run on a commercial hardware component (motherboard or computer) or on a custom-designed platform.
  - I/F: Standards-based interface for general input/output functions, e.g., USB, Bluetooth.
  - U/I: User Interface, typically Keyboard, Mouse, Display, Touch Screen.
  - Network: Standards-based wired or wireless network connection.
  - Storage and Memory: The device's volatile (e.g., RAM) and non-volatile (e.g., hard disk) storage and memory components.
  - Other COTS Software (non-OS): Commercial software components in addition to the O/S, e.g., database, Java virtual machine, and similar.
  - Device Software: Application software typically written in a commercial programming language and dealing with the device's higher level functions like information transfer, device management, etc.

 

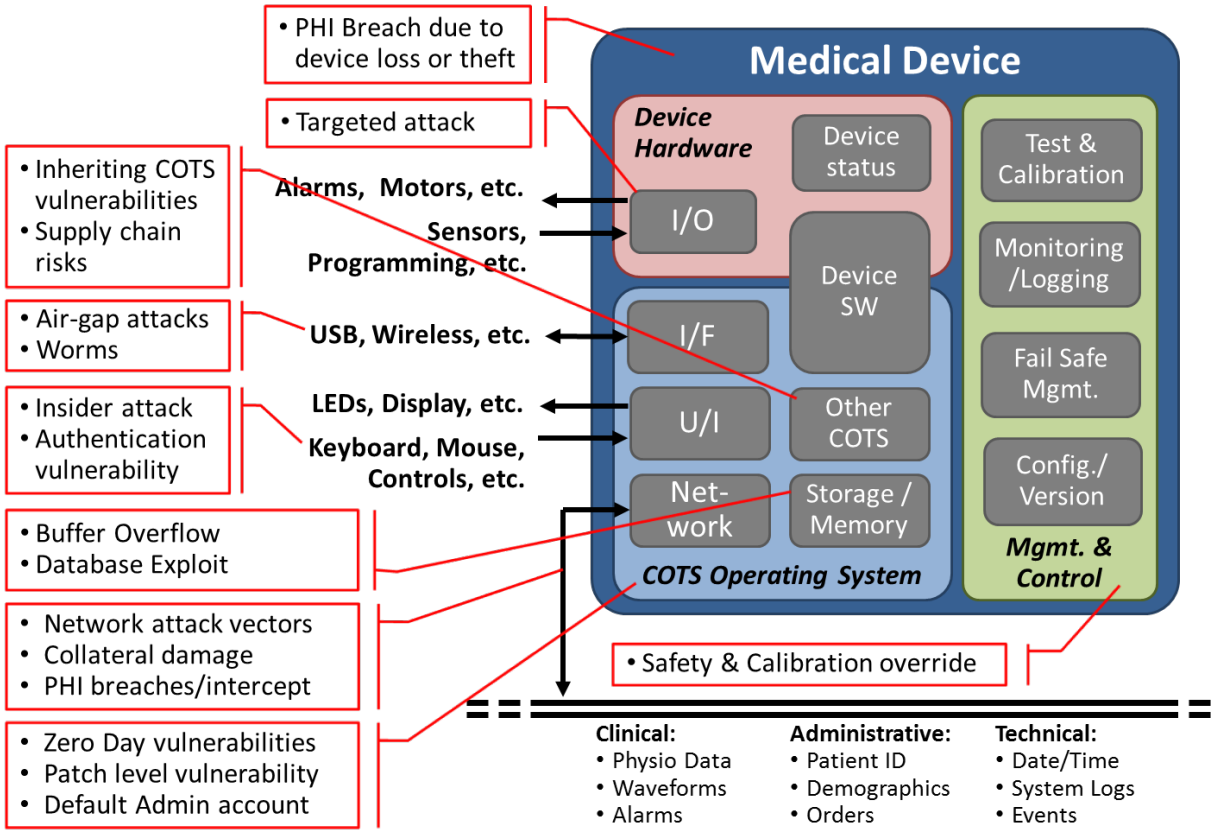


**Figure 3: Threat Examples**

Based on the general device architecture discussed in Figure 2, the above Figure 3 illustrates how the respective components can introduce vulnerabilities that can be exploited as part of an attack. These are common examples used for discussion purposes:

- Complete Medical Device: the entire device can be lost or stolen and therefore exposes the electronic Protected Health Information (ePHI) stored on the device to the risk of breach.
- Targeted Attack: deciphering and mimicking their respective protocols, especially if that communication does not require specific authentication, can exploit a device's proprietary I/O ports. Several security researchers have demonstrated this for the programming interface of pacemakers[10] and implantable insulin pumps[11].

[10] "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses", Halperin, Daniel, Fu, Kevin, et al (2008), Computer Science Department Faculty Publication Series. Paper 68, http://scholarworks.umass.edu/cs_faculty_pubs/68

[11] "Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System", Radcliffe, Jerome (2011), https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf

- Inherited COTS Risks / Supply Chain Risks: Any COTS integrated in the device will inherit the vulnerabilities of that software, including the OS, databases, Java, and similar.
- Air-Gap Attack: This term describes attacks using a path into the system that does not include the network, resulting in vulnerabilities even if the device (or group of devices) is not connected to an external network. As an example, air-gap attacks can be executed via a USB thumb drive, CD's, or other data carriers.
- Insider Attack / Authentication Vulnerability: User authentication on a medical device is a difficult balance. Too much security may result in too much complexity and may impact patient care, especially in an emergency situation. Too simple (or lack of) authentication may make the device vulnerable to an unauthorized user making changes to its settings, e.g., the drug delivery rate of an infusion pump.
- Buffer Overflow and Memory Exploits: Depending on the programming language used, a program may be more or less vulnerable to memory errors like buffer overflow, memory allocation, or initiation errors. Due to the sharing of memory space for variables and programming code, any of these errors can be targeted and exploited to create undesired system behavior.
- Network Attack Vectors: Any network connection is susceptible to exploitation of the network protocol (on all layers), e.g., HTTP(S), (S)FTP, UDP, TCP, etc. Even protocols designed for secure communication may pose a risk, as for example recently demonstrated by the Heartbleed SSL vulnerability[12], and these risks need to be understood and managed.
  Often times, these attacks may not be targeted at the medical device, but may infect a device because of its poor security properties. In other words, the device may become collateral damage or may act as an entry point for an attack.
- PHI Breach / Intercept: Any ePHI transmitted or received by the device can be intercepted and breached. The information exchanged should be analyzed to understand the risks it poses and methods for data protection should be evaluated, like encryption. Most times the encryption features native to the transmission protocol (e.g., HTTPS or WPA2 for wireless) is the best choice.
- Patch Vulnerability: Manufacturers of COTS software typically provide patches and updates to address their products' security vulnerabilities. Depending on the complexity and market share of these products, the patches may be more or less in number and frequent. One would expect more patches for a commonly used O/S than for a dedicated software module used for a very narrow and specific purpose.
  In either case, timely release of patches by the manufacturer and timely implementation by the healthcare organization are critical. Although patches are not the only security measure required, they are a critical component but should always be complemented by other external or internal security measures.

[12] "U.S. hospital breach biggest yet to exploit Heartbleed bug: expert"; Reuters (Aug. 2014); http://www.reuters.com/article/2014/08/20/us-community-health-cybersecurity-idUSKBN0GK0H420140820

 

- Safety & Calibration Override: Of specific consideration are those values within the system, which control safety or calibration features. Any change to these values can lead to an "override" situation with a respective security feature being disabled or a safety limit being exceeded, both of which could result in patient harm.
- Any device interface could be exploited by exposing it to out-of-range or otherwise invalid input parameters or input sequences. This may lead to the device being penetrated by a hacker or malware, or may result in device corruption, lock-up, reboot, or similar.

In general, a device can be integrated with the larger enterprise or other systems in different ways, each of which have their own security weaknesses and require specific considerations. E.g., one needs to look at a Wi-Fi connected device very differently than a device using a proprietary RF link. Also, the fact that a device or device subnet is not connected to the main network does not mean it is secure; it can still be susceptible to a so-called air-gap attack, for example via a USB Thumb Drive introduced attack. Lastly, certain devices, based on their capabilities or age (i.e., platform and architecture) may require certain intermediaries to connect, e.g., a RS-232 to Ethernet Bridge.

The basic main connectivity scenarios and their basic vulnerabilities are as follows:

- **Disconnected**: device is not connected to the network, but potentially susceptible to a targeted or air-gap attack.
- **Permanently connected** to a standard or proprietary network. Susceptible to any network based attack vector, targeted or not.
- **Wireless:** same as permanently connected, but requires specific considerations to address wireless vulnerabilities.
- **Intermittent:** Connected at intervals, e.g., to download patient lists, upload results, etc. Resulting problems: difficult to update and patch (including virus definition files); can hide malware while disconnected and reintroduce when reconnected.
- **Legacy Device:** device may not have native network capabilities, but may be connected via Interface or Translator. The device is susceptible to a targeted attack, within the realm of the device's capabilities. The device interface can be impacted by any network attack.
- **Device Subnet:** may contain groups of devices and supporting network components like routers, servers, and workstations. May be physically or logically separated form enterprise network, e.g., VLAN. Connectivity and vulnerability considerations as above, but may form a broader attack surface due to the multitude of components in use; e.g., a denial-of-service (DoS) attack at a workstation can very well also affect the actual devices on that subnet. Proper network separation provides a degree of protection as outbreaks and attacks can be contained.
- **External Device:** physically located outside of the hospital (e.g., patient home), but connected (typically via data push or pull) via public CSP (Communications Service Provider) network, e.g., dial-up or Internet. Susceptible to a wide variety of cyber-risks introduced through the home or public network vulnerabilities.

 

- **Patient Device:** worn by or implanted in a patient, typically intermittently accessed via a programmer type of device. Susceptible to targeted attacks (e.g., spoofing of the programmer) or indirectly as the programmer may be networked and could be compromised.

Below Figure 4 shows a highly generic but representative high-level diagram of a medical device ecosystem in a hospital. Any device (D) can be connected based on any of the above-described scenarios.

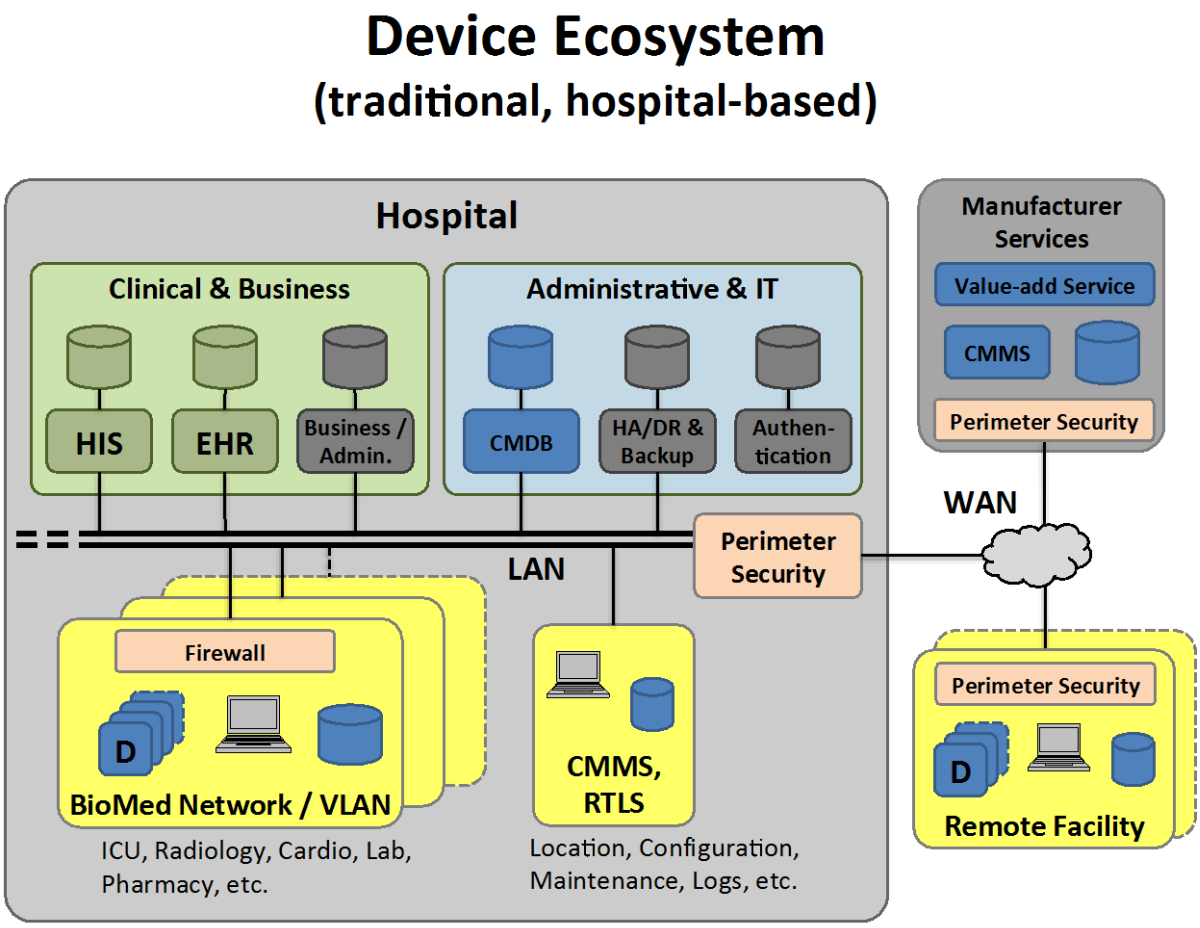


**Figure 4: Generic Device Ecosystem**

From a security perspective, Figure 4 provides the following guidance:

- Medical Devices are separated into a limited number of VLAN's (virtual network segments), based on system type, function, associated organizational entity, or risk profile. These VLAN configurations provide an additional degree of protection from network-based attacks and foremost, should an attack occur, helps to contain an outbreak.

Note that the medical device network contains other components as for example workstations, servers, router, or the like.

- Typically, hospitals utilize tools to manage their medical device inventory, so-called Computerized Maintenance Management Systems (CMMS). Many of these systems are network-connected and allow communication with the medical devices for maintenance purposes. Often these systems are complemented (or integrated with) Real-Time Location Management Systems (RTLS) to support locating and managing devices.
- Medical Devices communicate with other IT components in the hospital, like the EHR, HIS, or departmental system like a PACS, as well as administrative systems for inventory management, billing, etc. Architectural separation has to be a fine balance between security and integration requirements, i.e., closeness vs. openness.
- From an enterprise IT perspective, medical devices and their associated components may also need to be accessible and potentially be managed by Enterprise IT functions, be it a Configuration Management Database (CMDB) or a single-sign-on (SSO) system.
- Unique to medical device are patch management dependencies as in most cases patches to COTS, like the O/S, can only be deployed after device manufacturer approval. This can lead to patch deployment delays, or in the opposite scenario patches may be deployed indiscriminately across the entire IT infrastructure, making the affected medical devices non-compliant.

In the integrated scenario, the devices are exposed to a specific set of risks:

- Direct attack on the device.
- Unintentional - Infection of device based on general vulnerabilities.
- Once infected, device may be commandeered for different purposes – Advanced Persistent Threat (APT), further penetration and attacks, new malware, botnet, etc.
- Device may harbor malware and impact remediation.
- Device may not be the target but can be exploited as the weakest link.

These illustrations, as well as the entire white paper, deal predominantly with security risks and solutions specific to networked medical devices in the traditional hospital setting, but the respective topics may be applicable to other use scenarios as well.

 

# 6 General Security and Vulnerability Considerations

Device cyber-security risks fall into two main categories, targeted attacks (e.g., by a hacker) or unintentional exploitation (e.g., accidently introduced malware exploiting a device's vulnerability), each have different root causes and impact potential.

## 6.1 Targeted Attack

Although no cases have been reported outside of security research, due to medical devices being potentially vulnerable and easy to exploit, such attack is indeed in the realm of the possible and feasible. The purpose of such attack can be wide-ranging from the intent to harm a specific patient; over an attack on a specific healthcare provider (e.g., hacktivism[13]); or an attack on the larger healthcare system (cyber-terrorism, -warfare, -vandalism), maybe in support of a conventional or biological attack. These are serious considerations and as we strategically analyze and address the medical device security issue we, unfortunately, need to be aware of these possibilities.

## 6.2 Unintentional Exploitation

The far more common and likely scenario today is a security breach or malware outbreak based on the security profile of the medical device itself. A medical device's long product life (e.g., end-of-support O/S); potentially poor patch level; limited or lack of antimalware software; and sometime poor security configuration, makes them a ripe target for a malware infection or other security event. Furthermore, often medical devices of the same type or function are from the same manufacturer (e.g., a cathlab suite) and show the same vulnerability across all devices, As a result, such a security event can spread quickly and shut down entire clinical systems or even departments. Note that such attacks may not only come from the network, but can also be introduced via storage media (e.g., USB thumb drives) so that even subnets isolated from the enterprise or public network can be affected.

We already discussed possible motivations and causes for an attack on a medical device; it can be an individual patient or a specific hospital. A poorly protected medical device can also be used as an entry point to the larger enterprise network, i.e., device is not the target, but its vulnerability enables a larger attack.

Examples for common attack scenarios (for illustration purposes, not an exhaustive list) are:

- General Malware: In general terms, malware is rogue computer code that has the capability to infect good computer code and good systems. Main types include:
  - Virus (malware that can infect a system and when executed can fulfill a specific purpose);
  - Trojan (bad code hiding in good code);
  - Worm (malware with the capability to self-replicate and spread);

[13] "When 'Hacktivists' Target Your Hospital", Daniel J. Nigrin, M.D., New England Journal of Medicine 371;5, July 31, 2014

 

- Backdoor (malware or method with the capability to bypass system authentication, mainly for the purpose of gaining illegal remote access);
- Zero-day (exploits a previously unknown vulnerability which software manufacturers have not patched);
- Rootkit (malware that installs itself at the Administrator (root) level of a system);
- Spyware (has the capability of collecting information about a person, organization, or system).

- The purpose of malware is as varied as their types and ranges from pure mischief and notoriety, over stealing of information like passwords and financial accounts, to sabotage and cyber-warfare.
  - Password hacking: any methodology to obtain a user's credentials may include the use of malware or tools e.g., a dictionary attack based on a list of commonly used passwords.
  - Man in the Middle: Generally refers to an attack where a listener (or listening tool) is inserted in the data traffic with the purpose of stealing the transmitted information, ranging from credentials (user names, password) over account data (e.g., credit cards) to complete PHI. Medical devices are especially vulnerable here especially since a large percentage of medical devices transmit information via HL7®, which is nearly clear text; unless the transmission medium enforces some degree of encryption, e.g., WPA2 for wireless.
  - Distributed Denial of Service Attack (DDoS): An attack where a web site (or other server or device) is being deliberately hit by a large number of requests with the goal to overload its capacity and bring it down, or at least slow it down its response to normal inquiries. This type of attack requires a degree of cooperation and can be supported by tools. Reported cases include everything from news outlet's web servers to VoIP telephone systems.
  - Malware in conjunction with a hacking attack: many times malware is used very targeted and as a tool to map out a network, collect user credentials, identify defenses, or identify valuable information. Often malware is used to support an attack or to support the reconnaissance phase of an attack.
  - Malware to distribute more malware: Today's malware has extensive capabilities, for example once a system is infected malware may reach out to a command and control server for further instructions, e.g., to upgrade itself to a newer version, to disable system security features, to install other malware, or to lay dormant until further notice. Often, infected systems are rented out as a service and can be called to action at any time in the future.
  - Botnet: A botnet is a network of hijacked Internet-connected software or devices that are hijacked for a different purpose, e.g., distribute spam or further malware. Often, the illegal owner, the so-called bot-herder, is renting them out as CPU capacity or for specific purposes.

This brief overview provides a basic understanding of the complexity of the topic and helps us to further analyze why and how systems are affected.

 

# 7 Vulnerability Management and Security Best Practices

The preceding three sections (4, 5, and 6) have created a foundation for understanding cyber-security terminology; challenges; a generic architecture and integration model to illustrate requirements and implications of cyber-security on medical devices; and the notion of general security and vulnerabilities. In this section, the reader is treated to an extensive discussion on the typical classes of vulnerabilities that may be exploited in medical devices and their ecosphere, and the reader is presented with several security best practices in mitigating these vulnerabilities.

Security best practices are built upon a hierarchy of asset discovery and asset management, that then leads to the application of risk management principles to inform the decision as to which security control measures will be applied to which assets, and therefore eliminate or mitigate the identified security vulnerabilities associated with those assets.

The vulnerabilities we need to be aware of and need to address by remediating or mitigating them, cover a broad range, and include, in general terms, vulnerabilities of:

- Information (e.g., patient data, configuration settings)
- Access and authentication (e.g., user or administrator accounts)
- Infrastructure (hardware, firmware, networks, etc.)
- Platform (Commercial-of-the-Shelf (COTS) components, e.g., operating system, database)
- Application (i.e., the custom application which provides the device's functionality)
- And lastly, the larger system of devices and supporting components (workstations, servers) and the security dependencies between them, in the sense that the device can become a security risk to the system and vice versa, that system components can become a security risk to the device.

To use a simple example, someone breaking into your house with a fake key would use an authentication vulnerability (e.g., the tolerance of your door lock to accept a facsimile of your actual door key), whereas somebody breaking and entering through a window would gain access by compromising your infrastructure in a brute force approach. This example highlights the breadth of attack vectors and correspondingly, the breadth of defenses we need to set up.

Each of the above, or a combination thereof, can be exploited to compromise a system either through a direct attack (targeted, malicious actor) or through any of the increasingly sophisticated and abundant malware. Not every system or device will have the same risk and the impact of the compromise will vary based on its use case. As discussed before, a risk is always a combination of probability (how likely is an event to occur) and severity (what is its impact).

The following table gives examples of vulnerabilities in each of the above main categories and suggests remediation/mitigation.

The remainder of this section will discuss some specific topics in more detail.

 

| Category | Security Risk | Security Control Example |
|---|---|---|
| Information | • Compromise of patient or diagnostic data can lead to legal and regulatory consequences under regional breach and privacy laws (e.g., U.S. HIPAA Privacy and Security Rules; European Privacy Directive).<br>• Unauthorized changes to device calibration data can lead to undesired device behavior and compromised patient safety. | • Encryption<br>• Protection of critical system files.<br>• Tiered access rights for system administrators. |
| Authentication | • Obtain unauthorized access to change dosage or override safety settings. | • Depending on device type, use case, and capabilities, implement strong authentication methods. |
| Infrastructure | • Denial of Service (DoS) attack leading to compromised network performance, impact on availability, and functional implications, e.g., interfere with alarm transmission. | • Network segregation, perimeter defenses, security event monitoring, and component redundancy. |
| Platform | • Malware infection, based on inherited COTS vulnerability, e.g., operating system. | • Close cooperation with manufacturer to establish timely and diligent patch process.<br>• Supplemental security through e.g., Host Intrusion Prevention Systems (HIPS). |
| Application | • Any exposed vulnerability of the device's customer application can be exploited in a targeted attack. | • Software engineering best practices.<br>• Supplemental file and system behavior techniques.<br>• System fail-safe mode |
| System | • Any component of the larger system can be exploited in the context of the above. | • Comprehensive, system-wide "defense in depth" approach.<br>• Security Risk Management. |

We have experience based on historic attacks we have observed, and can construct our defenses accordingly. However, we also need to be aware of the creativity of hackers; continually evolving threats; new attacks vectors; and therefore be prepared to defend against the unknown. This means that on both, device and enterprise level, we need to include advanced detection methods like behavior analysis. This also includes the need for resilient systems that can recover quickly and be restored easily and reliably. Our security risk analysis should be a "living document" that is continually updated, to account for not only changing infrastructure, but even more to account for the rapidly changing threat landscape.

This is, in a sense, a problem of the "unknown unknowns". There are vulnerabilities we understand and can mitigate, e.g., we know the problems with passwords (default, hardcoded, short, easy to guess, not being changed, etc.) and we can mitigate them through technology or process. But there are also those vulnerabilities we don't know about yet and hence we can't implement specific mitigations. This leads to the need for mature, risk-based security practices, a defense-in-depth approach (discussed in more detail later), and an approach of cyber-resilience

 

as for example articulated in NIST's "Framework for Improving Critical Infrastructure Cybersecurity"[14]:

- Identify: identify and manage systems, assets, data, and capabilities; understand business context, resources and cyber-security risks; prioritize through risk management strategy.
  - Asset Management
  - Business Environment
  - Governance
  - Risk Assessment
  - Risk Management Strategy
- Protect: appropriate safeguards; limit or contain impact.
  - Access Control
  - Awareness and Training
  - Data Security
  - Information Protection
  - Processes and Procedures
  - Maintenance
  - Protective Technology
- Detect: identify cyber-security event; enables timely discovery:
  - Anomalies and Events
  - Security Continuous Monitoring and Detection
- Respond: take action regarding detected cyber-security event; contain impact.
  - Response Planning
  - Communications
  - Analysis
  - Mitigation and Improvements
- Recover: maintain resilience; restore capabilities or services; timely return to normal operations.
  - Recovery Planning
  - Improvements
  - Communications

The nature of the continually changing cyber-security risks is also a challenge for the manufacturers as it defies the approach of an engineering hazard analysis, which is typically used to predict the risk of device failure based on the design choices made. If I predict a device's reliability based on the sum of its hardware components (e.g., as defined by the MTBF – mean

[14] "Framework for Improving Critical Infrastructure Cybersecurity"; National Institute of Standards and Technology (02/ 2014); http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

 

time between failure), then this analysis will remain true for the lifetime of the product. But any analysis of cyber-security risks done today will be invalid tomorrow as new threats are evolving.

Building and maintaining a secure medical device infrastructure is complex and requires close cooperation of all stakeholders, but especially between manufacturer and health delivery organizations. A comprehensive "defense in depth" approach is required, spanning from security measures implemented on the device itself, over network architecture and supplementary defenses, all the way to policies, procedures, and workflows.

## 7.1 Specific Security Topics

The following section will review some additional topics that have not been discussed under the umbrella of the previous, larger topics.

### 7.1.1 Defense-in-depth

A commonly used concept in cyber-security is the one of "defense in depth". In a nutshell, this articulates the need for a comprehensive security posture from the actual device (and its data) across the network and including the enterprise perimeter (firewalls, etc.).

With today's threats not only being more numerous and more sophisticated, but also much more targeted and executed with unprecedented stealth, the need for a comprehensive defense in depth approach is more crucial than ever.

Specifically, for our medical device ecosystem this leads to two conclusions:

- Many of the medical devices in use today were designed when cyber-threats were much simpler and less targeted. This makes devices vulnerable as often design, use, and architectural limitations do not allow for a defense in depth approach to protect the device.
- From the perspective of the larger enterprise, it is desirable to include all network components in a defense in depth architecture. Unfortunately, insecure medical devices are a security gap that may leave the larger enterprise vulnerable to a targeted attack.

The most common and comprehensive defense in depth models include:

| Component | Example Security Measure |
|---|---|
| Data | Encryption |
| Application | Access-Authentication, Sandboxing, Code signing |
| Endpoint | Hardening, Patching, Anti-Malware, HIDS/HIPS, Host-based Firewall, Device Certificates |
| Network | Network segmentation, Network IDS/IPS, Monitoring and alerts |
| Perimeter | Firewalls, Gateways, DMZ, VPN |
| Physical Security | Access control, doors, lock, etc. |
| Policies and Procedures | Risk Assessment and Management, Training and Education |
| Security Management | Security intelligence, Incident response management, Security assessment, Penetration testing |


 

Most of the above examples are discussed elsewhere in this document, the purpose of this section is to emphasize that none of these measures can stand-alone and that today's threat landscape requires a comprehensive and well-managed approach to security.

Similar, all stakeholders need to contribute. Manufacturers need to assure security of their devices and healthcare organizations need to integrate and maintain them on a secure network.

### 7.1.2 Zero Day Attacks

The terms zero day vulnerability and zero day attack refer to a previously unknown vulnerability and the exploitation of that vulnerability in a cyber-attack.

Historically, zero day attacks were few and far in between and were typically only used by a limited number advanced hackers or organizations. However, the arrival of malware toolkits and the existence of a cyber-crime underground economy are now providing zero day capabilities to anybody who is willing to pay for it. Consequently, we have seen the number of zero-day attacks increase over the past years, including attacks, which used multiple zero-day exploits in a single attack (e.g., Stuxnet[15]) or have the ability to shift to a new zero-day once the previous one had been identified and fixed, typically through a patch or upgrade of anti-malware software (e.g., a strategy applied by the Elderwood Gang[16]).

Of special concern are any end-of-support applications, as by definition, the software manufacturer will not provide any fixes or patches for newly discovered zero days.

Strategies to defend against zero-day attacks cannot be provided through a single defensive measure but requires multiple layers, including:

- Behavior-based security features, as they are provided by most commercial anti-malware programs today, but may also be included as a security feature in the operating system.
- Host-based intrusion detection and prevention systems (HIDS/HIPS), which can provide features like: application whitelisting, traffic control, system file lock-down, and behavior control.
- An up to date patching process that minimizes the time window during which a vulnerability could be exploited.
- Network-based security including firewalls, gateways, intrusion prevention techniques, and traffic monitoring and analysis.
- Shifting to less commonly used applications, operating systems, browsers, etc. as that reduces the likelihood of it being exposed to risks associated with zero-day vulnerabilities. However, this path has to be taken with caution as specific design choices

[15] "W32.Stuxnet Dossier"; N. Falliere, L. Murchu, E. Chien (Symantec, Feb. 2011); https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[16] "The Elderwood Project"; G. O'Gorman, G. McDonald (Symantec, 2012); https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf

 

may not provide the same degree of "obscurity" in the future, and certainly not against a targeted attack.

- User security training as often attacks being proliferated via email, browser pop-ups, and similar techniques that can be detected by a conscious user. Also, a well-trained user will be able to spot an attack or abnormal system behavior earlier and respond accordingly.

As we are now seeing an increase in highly sophisticated and targeted attacks (often referred to as Advanced Persistent Threat – APT), we need to add both, forensic and recovery capabilities to our security strategy. We need to be able to understand which systems have been affected and what information has been breached (forensics), as well as be able to restore functionality and data as quickly and completely as possible (recovery).

Medical devices with their unique use case, long product life, and typically slow patch deployment cycles are especially at risk due to zero day exploits.

## 7.2 COTS Vulnerabilities

Medical device manufacturers are increasingly utilizing Commercial off-the-shelf Software (COTS). As systems are becoming more complex and feature-rich, this is an obvious design choice for many software architects. The most commonly used COTS is probably the Operating System, but may also include databases, runtime environments, drivers, media players, and more.

However, the drawback of this approach is that the device automatically inherits the COTS' cyber-vulnerabilities. Careful design considerations must be undertaken to minimize exposure, unused system functions should be disabled, and the system should be properly hardened. Any COTS will require specific considerations in the manufacturers' hazard analysis and it has its unique needs as part of the Quality System and lifecycle management[17, 18], especially after a COTS component's support has ended (EOS or EOL).

### 7.2.1 Use of COTS

Medical devices have operating systems that span from proprietary to commercial products. Typically the proprietary O/S, uses non-networked communication (e.g., serial port, USB or proprietary); the COTS systems typically communicate using either 802.3 (Ethernet) or 802.11 (wireless) networks. Medical Devices, using COTS and residing on the standard 802.3 or 802.11 wireless networks, are vulnerable to network-based malware and attacks. Yet most medical devices are limited in their ability to prevent malware. Due to the long development life cycle and testing requirements of medical devices to ensure the safe and effective use, the burden is both on the manufacturer and the hospital to mitigate the Operating System vulnerabilities. This risk is compounded by third party software such as Document Viewing and Printing applications

[17] "Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices"; US Food and Drug Administration (Sept. 1999); http://www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm073778.htm

[18] "IEC 62304: Medical device software -- Software life cycle processes"; ISO; http://www.iso.org/iso/catalogue_detail.htm?csnumber=38421

(e.g., Adobe Acrobat), Runtime Environments (e.g., Java), Web Services (e.g., Apache), Print Drivers, or Databases (e.g., Oracle) that are installed as a part of the medical device software application package. The manufacturer and hospital must collaborate to ensure the safe, effective and secure operation and use of the medical device. Any commercial software application makes a device vulnerable to exploits (malware or attack vectors) that are targeted at the respective component. It is of critical importance to:

- Disclose all used commercial software to the buyer and operator.
- Follow the software provider's recommendations on how to secure and harden the component.
- Include the component in the device's security notification and patching process.
- Eliminate or disable all components of the commercial software that are not used.

This requires the manufacturer to harden the device using security best practices such as disabling unnecessary ports, protocols and services, and using least privilege (limiting the use of Operating System administrators). Manufacturers must provide a defined software lifecycle including training, maintenance, patching, End of Life/disposal for the hospital to assimilate into their procurement and change management process.

### 7.2.2 Unsupported COTS, Lack of Security Updates and Patches

With any COTS software component, lifecycle and update management is a critical function. COTS manufacturers release regular bug fixes, including security patches. Keeping COTS software up-to-date is critical for maintaining the device's security posture and to remain protected against newly discovered threats.

This issue becomes especially critical once a COTS component reaches its end of support (EOS), i.e., the time when the original manufacturer stops providing fixes and security updates. Over time, this results in a growing security gap of the medical device as new vulnerabilities continue to be discovered and being used in new attacks and exploits.

This problem is compounded by the fact that hackers are known to withhold newly discovered vulnerabilities until after a COTS product's EOS, so that their use does not result in the release of patches to close the vulnerability. Also, often the newer versions of commercial software share code with the older versions, which gives hackers the opportunity to learn from patches as they get released for the current version and apply them as an attack vector to the older version. So, not only does an EOS announcement result in growing vulnerabilities, it often accelerates the ability to exploit them.

### 7.2.3 Software Patching

Earlier in this document we reviewed the impact of the respective regional regulatory frameworks on cyber-security, as they typically will mandate that manufacturers perform formal verification and validation of the final product (including its updates, upgrades, and patches). This implies that only the manufacturer-approved version in its specific configuration can be used on the device. Although there is great variety of medical device types and use cases and the

 

specific scenarios vary, the general consensus is to rely on the manufacturer to assure device safety, compliance, and reliability.

This has impacted the availability of approved patches to COTS software components and typically delays, in extreme cases even stalls, the deployment of security patches to medical devices. The manufacturer's obligation is to:

- Release, as timely as possible, security patches of COTS components.
- Provide ongoing communication to the end user about patch availability and criticality.

Healthcare organizations and operators of medical devices, in turn, need to have corresponding processes in place to upgrade their medical device inventory without undue delay and in consideration of:

- Device utilization and use.
- Device interdependencies and coordination of upgrades across device inventory and supporting infrastructure.

The overall topic of patching, a suggested best practices approach, and a deeper discussion of regulatory implications is provided through another white paper.[19]

Key elements of a mature patch process and proper coordination between medical device manufacturer and end user (Health Delivery Organization - HDO) require:

- Patching policies and procedures, patch management (when, how, who, …)
- As part of the manufacturers Quality System:
  - Patch verification and validation
  - Assessment of patch criticality
  - Manufacturer to HDO communication
- Patch deployment: manual, semi-automatic, or automatic
  - Impact analysis, coordination with clinical operation
  - Patch deployment schedule and resources
  - Risk of patch automation: pushing unapproved patches; wrong timing
  - IT vs. Biomedical Engineering: resolution of patch priority conflicts
- Deployment methodology
- Configuration Management and logging

Once a COTS component has become EOS and patches are no longer available, the patch forward becomes more difficult. Ideally, manufacturers should provide an upgrade path to a newer version of the respective component. However, this may be difficult due to:

[19] "Medical Device Software Patching"; White Paper; IHE PCD in Cooperation with MDISS available at http://ihe.net/Technical_Frameworks/#pcd

- Hardware dependencies as the newer version may require, for example, an upgraded motherboard or more memory, which then in turn may have other trickle down effects on other hardware components of the device.
- Software dependencies, e.g., with drivers, DLL's, and other cross-system integration components.
- Economic practicality to invest in the resources for the development, verification and validation, release, and distribution of upgrade kits; especially if customers may not recognize and appreciate their importance.
- Availability of technical expertise to provide engineering services to support the, often intensive, upgrade process.

Similar, end users may be reluctant to deploy extensive and complex upgrades as they weigh the effort and resources to be spent against its economic benefit (including the security risks), which they may not recognize as important.

In case of EOS medical device still being used, mitigation measures (also known as compensating controls) need to be seriously evaluated.

- Manufacturers can employ Host Intrusion Prevention (HIPS) products, which are a relatively lightweight security technology that is not relying on signature updates. HIPS have been demonstrated to be an effective security measure for the protection of unpatched O/S.[20] (Malware protection technologies are discussed in more detail later in this section).
- Operating systems should be hardened and configured based on available security guidelines and best practices.
- End users can employ external security measures like firewalls, segregated networks (VLAN), or security gateways. However, such measures will always come with a cost/security tradeoff and are often adding management overhead. Also, although they improve security, they most likely will not be able to compensate the entire security gap created by the EOS device.

Managing security patches, and especially those for EOS medical devices, is a complex, yet important activity and requires close cooperation between manufacturer and end user.

### 7.2.4 System Hardening

Security hardening is a key component of a well-designed system. System hardening applies the concepts of access control and least privilege to the operating system and all applications and is key to a mature security architecture and design. The goal is to minimize the components of the system that are exposed to threats. This approach disables unused or unnecessary ports, accounts, protocols and services, and limits access and permissions of the users based on their need.

[20] "Managing Legacy systems", Symantec Security Community Blog (July 2013), http://www.symantec.com/connect/blogs/managing-legacy-systems

 

System hardening is challenging and requires a multidisciplinary approach; which includes software engineers, security engineers and vulnerability testers. The system must be hardened, programmed using secure coding practice and lastly tested to ensure the appropriate security measures have been implemented.

Because of the level of effort and resources required, this approach is often challenging to implement. There are a number of guides developed by organizations such as Center for Internet Security (CISecurity.org)[21], the manufacturers of the respective commercial software (e.g., Cisco, Microsoft), the US Government with the NIST Special Publications and the US Department of Defense Security Technical Implementation Guides (STIG).

System hardening, if implemented appropriately, has the potential to minimize vulnerabilities that are the result of design choices, implementation errors, and users. Of special concern are open, unused ports and remote access ports & accounts. External remote access points are provided for support purposes, but many times they are insufficiently secured and enable unauthorized access, especially if they are not properly secured and use, for example, default or hard-coded passwords (passwords will be discussed in more detail in a later section).

### 7.2.5 Lack of Malware Protection / Security Technology

Another challenge is the reluctant use of cyber-security technology on medical devices beyond basic system hardening. For once, any additional component added to the system platform impacts performance (or requires additional hardware to maintain performance), increases the risk of device malfunction (especially with relatively invasive components like for example anti-virus software), and creates even greater interdependencies between system components and approved configuration.

Further, one of the most common cyber-security technologies, signature-based anti-virus, has specific limitations, which typically make it unsuitable for the use in medical devices (or any embedded system for that matter). The limitations of a reactive technology like anti-virus include:

- Need to update malware definition signature files; in this day and age we see new malware rates of 100,000+ per day, which ideally requires this to be a continual process.
- Inability to detect new malware, unique malware (i.e., not commonly known), or zero day exploits, especially if signature update is infrequent.
- Risk of false positive detection and response to a mistaken good system file or event.
- Impact on system resources, especially during system scan or definition file update.
- Unpredictable future behavior and impact on system functionality and performance as malware software will need to evolve and introduce new features in response to newly developing threats.

[21] "Medical Device Security Benchmarks Initiative", Center for Internet Security (CIS), http://benchmarks.cisecurity.org/about/MedicalDeviceOverview.cfm

No anti-malware product available in the market today relies solely on signature-based detection[22]. Although this is still a required component (after all, the old malware does not go away), today's anti-malware products are much more complex and use a number of technologies, including behavior analysis, file reputation, and heuristics.[23]

Because of the complexities and limitations discussed, in many cases other, alternative security technologies should be applied. In other words, the limitations of anti-malware should be used to evaluate alternative technologies, but not as a reason not to implement any security at all.

### 7.2.6 Host Intrusion Detection and Prevention

Attractive alternatives to signature-based anti-malware are so-called Host Intrusion Detection/ Prevention Systems (HIDS[24]/HIPS[25]). Simplified, unlike anti-malware, which monitors system behavior and files to detect bad events (blacklisting, reactive), a HIPS-protected system monitors system behavior relative to an allowed list of applications, processes, and behavior (whitelisting, proactive).

The advantages are multi-fold:

- Lighter footprint and demand on system resources (memory, CPU).
- No need to update signature files. Any updates of the allowed system behavior can be deployed as these behavior changes are deployed (i.e., system update or upgrade).
- Protection against zero-day vulnerabilities (since, by definition, any newly discovered exploit would be outside of the scope of allowed behavior).
- Ability to protect EOS applications and operating systems.
- System Controls:
  - Lock down configuration & settings
  - Protect system and configuration files (e.g., Registry)
  - Enforce security policy
  - De-escalate user privileges
  - Control/prevent removable media use
- Exploit Prevention:
  - Restrict application and O/S behaviors

[22] "Antivirus software"; Wikipedia, the Free Encyclopedia; http://en.wikipedia.org/wiki/Antivirus_software

[23] "Reputation-based Security: An Analysis of Real-World Effectiveness"; Symantec Corp (10/2010); http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/reputation_based_security.pdf

[24] "Host-based intrusion detection system"; Wikipedia, the Free Encyclopedia; http://en.wikipedia.org/wiki/Host-based_intrusion_detection_system

[25] "Intrusion prevention system"; Wikipedia, the Free Encyclopedia; http://en.wikipedia.org/wiki/Intrusion_prevention_system

- Protect systems from buffer overflow
- Application and process behavior control

- Network Protection:
  - Close back doors (block unused ports)
  - Limit network connectivity by application
  - Restrict traffic flow inbound and outbound

- Support Auditing and Alerting:
  - Monitor logs and security events
  - Consolidate & forward logs for archives and reporting
  - Security event alert and response

Note that the features listed above are well aligned with the FDA Cybersecurity Guidance for medical devices (discussed earlier). This can help the manufacturer to demonstrate compliance with requirements suggested in the guidance document.

HIDS/HIPS are a mature technology and find wide use with embedded systems (e.g., ATMs, cash registers, gaming devices) as well as for the protection of critical or high-risk servers (e.g., domain controllers) and workstations (e.g., kiosks).

## 7.3 Application Vulnerabilities

From a security standpoint, the application layer expands the risk profile of an information system by the plain fact that the potential attack surface has increased. The scope of application vulnerability can be expansive when examining security holistically. MITRE's Common Vulnerabilities and Exposures (CVE)[26] defines a vulnerability as is a state in a computing system (or set of systems) that either:

- Allows an attacker to execute commands as another user.
- Allows an attacker to access data that is contrary to the specified access restrictions for that data.
- Allows an attacker to pose as another entity.
- Allows an attacker to conduct a denial of service.

Similarly, Open Web Application Security Project (OWASP)[27] defines application vulnerability as "a hole or a weakness in the application, which can be a design flaw or an implementation bug that allows an attacker to cause harm to the stakeholders of an application. Stakeholders include the application owner, application users, and other entities that rely on the application."

[26] "Common Vulnerabilities and Exposures (CVE) – Terminology"; MITRE; http://cve.mitre.org/about/terminology.html#vulnerability

[27] "Open Web Application Security Project (OWASP) - Vulnerability"; https://www.owasp.org/index.php/Category:Vulnerability

In short, an application that contains an exploitable vulnerability poses a risk to the system in which it resides. The severity of the risk posed by an application's vulnerability depends on the context in which the application exists within an IT network. Weak development practices on the part of an application vendor can lead to a problematic domino effect for an organization's IT network. For example, inadequate logging/auditing and error handling logic can complicate troubleshooting and stunt forensic investigations. Weak input handling can introduce injection attacks whereas weak output handling can expose information about the application's operational processes that can be used in a more sophisticated and targeted exploitation.

When seeking to acquire new application technology, the software application evaluation process should be a part of the risk management plan for the organization. Reducing the probability of introducing an application containing an exploitable vulnerably into an IT network can be conducted by a rigorous risk assessment of the application. The risk assessment must include an evaluation of the application's development lifecycle and an evaluation of the manufacturer developing the application. For example, does the manufacturer's application development lifecycle include an update/patch strategy? If so, what are the details surrounding the strategy as it applies to the organization seeking to acquire the application? Do those details meet a recognized industry standard? If so, what is the standard? Since no software application will be perfect, vendors with strong customer support services are highly recommended. Moreover, the FDA's Guidance on Medical Device Cybersecurity outlines high-level secure design specification for manufacturers seeking premarket approval. Healthcare organization can also leverage the FDA Cybersecurity Guidance as a tool in which to evaluate medical device manufacturers and their products.

The IEEE has published guidance on architecture and design of medical device software to help assure critical safety, usability, maintainability, and effectiveness requirements of these systems can be ensured.[28] Vendors developing applications that take security into consideration during the requirement specification phase of the software development lifecycle will be better suited to address the concerns and inquiries by organizations seeking acquisition of their product. The chart in Appendix A illustrates the top secure application practices based on recommendations by the SANS Institute. Most recently, OWASP has published an update to their Application Security Verification Standard. This standard itemizes design requirements that address security and the degree at which each requirement can be attained.[29]

[28] "Building Code for Medical Device Software Security"; T. Haigh, C. Landwehr, IEEE Computer Society, (May 2015); http://cybersecurity.ieee.org/images/files/images/pdf/building-code-for-medica-device-software-security.pdf

[29] "Application Security Verification Standard; v3.0 Early preview release"; OWASP; https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project Excel Download:https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project#tab=Downloads

Moreover, US-CERT, in their "Software Assurance Pocket Series"[30] has published Key Practices for Mitigating the Most Egregious Exploitable Software Weaknesses. The above publication has been deconstructed into a detailed Mindmap[31] illustration. Another approach to reducing the risk of potential application vulnerabilities is to seek vendors who hold an application security certification or accreditation. Vendors who hold a secure software certification or accreditation will have demonstrated adherence to a governing standard to a certification/accreditation entity.

Other helpful resources on this topic are provided by:

- The SANS Institute[32]
- U.S. National Institute of Standards and Technology (NIST)[33]
- MITRE Corporation[34, 35]
- Microsoft Threat Modeling Tool[36]

### 7.3.1 Insecure Coding Practices

Insecure coding practices occur when software developers do not take into account the introduction of logical security vulnerabilities. Software defects (software errors) and logic flaws can become exploited to compromise medical devices. Insecure coding practices are very dangerous because it may enable an attacker to take over the device's functionality, acquire its data, or prevent the device's software from working at all.[37]

[30] "Software Assurance Pocket Guide Series "; US Department of Homeland Security; https://buildsecurityin.us-cert.gov/swa/software-assurance-pocket-guide-series

[31] "Key Practices For Mitigating the Most Egregious Exploitable Software Weaknesses"; US CERT; www.xmind.net/m/9Gn8

[32] "An Introduction to Certification and Accreditation"; SANS Institute; http://www.sans.org/reading-room/whitepapers/standards/introduction-certification-accreditation-1259

[33] "Certification and Accreditation Process Handbook for Certifiers"; National Computer Security Center (July 1996); http://csrc.nist.gov/publications/secpubs/otherpubs/CA_Handbook.pdf

[34] "Common Weakness Enumeration"; MITRE; http://cwe.mitre.org/

[35] "Common Vulnerabilities and Exposures"; MITRE; http://cve.mitre.org

[36] "Introducing Microsoft Threat Modeling Tool 2014"; Microsoft Corp. (April 2014); http://blogs.microsoft.com/cybertrust/2014/04/15/introducing-microsoft-threat-modeling-tool-2014/

[37] "CWE/SANS TOP 25 Most Dangerous Software Errors"; SANS Institute; http://www.sans.org/top25-software-errors/

Security researchers have identified many common software errors, and continue to accumulate this knowledge as security breaches are discovered. Some examples of insecure software coding practices are listed here[38]:

- Missing authentication for Critical Function
- Missing authorization
- Use of hard-coded passwords (see later section)
- Missing encryption of sensitive data
- Reliance on untrusted inputs in a security decision
- Download of code without integrity check
- Integer overflow or wraparound
- Incorrect calculation of buffer size (buffer overflows)
- Unintended, unexpected interactions

Secure Software Development covers the product development lifecycle, from requirements, design, test, integration, verification, validation, product deployment, and post-market surveillance. There are several lifecycle processes (e.g., NIST SP 800-160, IEC 62443-x, etc.) in place that can be used to introduce security engineering early in the software development process.

### 7.3.2 Examples of Best Practices for Secure Coding

A key paradigm for producing secure coding is protection from disclosure (confidentiality); protection from alteration (integrity); protection from inaccessibility (availability); identification of user (authentication); assignment of privileges (authorization); traceability (auditing); and management of sessions, configurations, and exceptions.[39] Supporting this paradigm are the following example mechanisms[40, 41]:

- Encryption (confidentiality and integrity control)
- Hashing (integrity control and data protection control)
- Load balancing and load monitoring (availability control)

[38] "Secure Software Engineering"; Software Engineering Institute, Carnegie Mellon University; https://www.securecoding.cert.org/confluence/download/attachments/111083784/01%20Introduction.pdf?version=1&modificationDate=1378213539000&api=v2

[39] "The Ten Best Practices for Secure Software Development"; $(ISC)^2$; https://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/Certification_Programs/CSSLP/ISC2_WPIV.pdf

[40] "Top 10 Secure Coding Practices"; Software Engineering Institute, Carnegie Mellon University; https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices

[41] "How to write insecure code"; Open Web Application Security Project (OWASP); https://www.owasp.org/index.php/How_to_write_insecure_code

- Validation of input from all untrusted sources (including command line arguments, network interfaces, environmental variables, and user controlled files).
- Architect and design for security policies
  - Keep designs as simple and as small as possible; reduce complexity
  - Base access decisions on permission, and not on exclusion.
  - Assign the each process with the least set of privileges necessary to execute its function.
  - Manage security risks with multiple defensive strategies.
  - Implement effective software quality assurance techniques such as Fuzz testing, source code audits, and penetration testing.
  - Implement error logging and error handling

Additional mechanisms that support this paradigm must be validated through security design reviews, security testing, and system testing. Medical device/system software developers are strongly encouraged to:

- Obtain training in and apply techniques from secure coding principles
- Leverage best practices that are publicly available (e.g., Microsoft[42], NIST SP 800-14[43], Apple[44], Cisco[45], to name a few examples)
- Investigate secure software coding methods (e.g., CERT C Coding Standards[46])
- Develop expertise in secure coding design reviews and software quality assurance methods
- Leverage academic and commercial training in secure software development

### 7.3.3 Application Deployment

A specific area of concern is the deployment of applications (including upgrades, updates, and patches) and measures to assure that only approved software is installed on the target device.

[42] "Secure Coding Guidelines"; Microsoft Corporation; http://msdn.microsoft.com/en-us/library/d55zzx87(v=vs.90).aspx

[43] "NIST SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems"; National Institute of Standards and Technology (NIST); http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

[44] "Secure Coding Guide"; Apple Inc. (2014); https://developer.apple.com/library/mac/documentation/Security/Conceptual/SecureCodingGuide/SecureCodingGuide.pdf

[45] "Security Design"; Cisco Systems Inc.; http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Education/SchoolsSRA_DG/SchoolsSRA-DG/SchoolsSRA_chap4.html

[46] "CERT C Coding Standard"; Software Engineering Institute, Carnegie Mellon University; http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=30432

This is provided by a technology usually referred to as Code Signing[47], a process of digitally signing software code. Verifying the code signature against a common signature authority guarantees its origin and that the code has not been altered or corrupted.

Code signing is employed for a number of reasons:

- Support security (prevent unauthorized code from being installed).
- Assure authenticity of the code provided (prevent safety compromise).
- Protect the manufacturer's business interests (prevent illegal distribution).
- Software management (e.g., version management, prevent namespace conflicts).

Code signing can be implemented independent of the software distribution method of choice, whether via media, download side, or network push.

It is the manufacturer's responsibility to assure that and software and media offered for distribution is free of defects and does not include an unintended payload (e.g., malware).

## 7.4 Password / Authentication Vulnerabilities

Information security controls are techniques and procedures used to reduce the likelihood that security-related threats will result in unauthorized disclosure or possession of information, loss of integrity of systems and/or data, and disruption of availability and/or accessibility of systems. Numerous sophisticated security control mechanisms exist today, examples of which are passwords used to log on to systems and file permissions.

Passwords are commonly used to authenticate authorized user access to a medical device. They can also be used to grant permissions to the type of access the user can have within the medical device. For example passwords can differentiate between the access rights for the clinical user and the administrative user. They may also differentiate between the hospital biomedical engineer access and the access available to the manufacturer. Given the significance of what different levels of access to a medical device can mean from the point of view of confidentiality, integrity, and safety, it is clear that password/authentication vulnerabilities in a medical device are a very important security concern.

Password/authentication vulnerabilities are deficiencies in a product's access design. Such design deficiencies have the potential to deny access to authorized users or to provide access to unauthorized users. A few examples[48] of these vulnerabilities include:

- Product uses default "Allow" action, instead of default "Deny" action, thereby leading to authentication bypass.
- Product admin script allows authentication bypass by setting a cookie value to "LOGGEDIN".

[47] "Code signing"; Wikipedia, the Free Encyclopedia; http://en.wikipedia.org/wiki/Code_signing

[48] "CWE - Common Weakness Enumeration"; NIST National Vulnerability Database; http://nvd.nist.gov/cwe.cfm

- The authentication routine returns "nil" instead of "false" in some situations, allowing authentication bypass using an invalid username.
- The product default password is publicly available, thereby providing easy authentication bypass.
- The selected password has weak complexity, thereby enabling automated password cracking tools to bypass authentication.
- The authentication routine has no restriction on excessive access attempts, thereby enabling automated password-cracking tools to bypass authentication.
- The authentication routine has improper restrictions for excessive authentication attempts, thereby creating a potential denial of service for authorized users.

The following sections provide the reader with additional detail on selective authentication vulnerabilities and potential remediation options that may be implemented via policies, product design, user guidance, and more sophisticated security measures. Each option provides an increasing level of trade-offs in security risks, complexity, and usability. The end goal is to prevent malicious and non-malicious security breaches (e.g., insider threat), as well as to provide product designers and system integrators with authentication solutions that are tailored to their specific user environments and workflow.

### 7.4.1 Hard-Coded Passwords

Hard-coding of password is the software development practice of embedding configuration data (i.e., the password) directly into the source code of the medical device or its other executable objects, instead of obtaining this data from external sources; or generating this data or formatting it within the medical device software itself with the given input (i.e., the password).[49]

There are reasons why hard coding passwords have been implemented. Some of these include:

- Simplified systems administration – for the same type of medical device from the same medical device manufacturer, a simple administration account is established using the default password that is hard-coded into the device's program. This approach may simplify device access and management for clinical personnel charged with its use and maintenance.
- Simplified medical device installation – hard-coded passwords can facilitate device manufacturing and installation.

However, the software design practice of hard-coding of passwords is strongly discouraged today, because it may compromise system security and the remediation is usually difficult (often requiring a software patch) once the product is in commercial distribution:

[49] "Hard coding "; Wikipedia, the Free Encyclopedia; http://en.wikipedia.org/wiki/Hard_coding

 

- A devious employee with access to this information can use it to break into the system.[50] If the password is ever published on the Internet, then anyone can access the product.[51]
- Would-be attacker with access to the byte code for the application can disassemble it and obtain values of the passwords used.
- Authentication failures with hard coded passwords can be difficult to detect, and have a high likelihood for being exploited.

### 7.4.2 Factory Default Passwords

A default password is one that a Manufacturer uses during production of the medical device and during initial configuration at the site of the hospital user. Such a password is one that is simple and is expected to be changed by the hospital user during product configuration and customization.[52]

The default password is shared across the same device from the same manufacturer. Further, the default password may be documented for the device in the manufacturer's service manual or on its website. As a consequence, leaving the default password in place on a medical device creates the same security risks as noted above with the hard-coded passwords. Therefore it is strongly recommended that the hospital user change the Factory Default Password of the medical device prior to connecting the medical device to a network.[53]

If the medical device is not networked, use of the default password can still be a serious security risk. For example, a non-networked medical device can include an implantable medical device. It is very difficult to create a password policy or to modify the password so it is not the manufacturer's default password once the medical device is placed in use in the patient.

With a connected medical device (networked medical device), one can indeed change the password (e.g., once a hospital receives it and puts it on its network) and manage the change without disrupting internal or external access.

### 7.4.3 Password Policy Management

A password policy is a set of rules that manage the usage of passwords in an organization.[54] The scope of these rules can include the following:

- Password strength - this policy may require the minimum password length, and recommend the use of:

[50] Use of hard-coded password"; Open Web Application Security Project (OWASP); https://www.owasp.org/index.php/Use_of_hard-coded_password

[51] "CWE-259: Use of Hard-coded Password"; MITRE; http://cwe.mitre.org/data/definitions/259.html

[52] "Default password"; Wikipedia, the Free Encyclopedia; http://en.wikipedia.org/wiki/Default_password

[53] "Alert (TA13-175A) - Risks of Default Passwords on the Internet" Department of Homeland Security, US CERT; https://www.us-cert.gov/ncas/alerts/TA13-175A

[54] "Password policy"; Wikipedia, the Free Encyclopedia; http://en.wikipedia.org/wiki/Password_policy

- Special characters (e.g., #. %, &, etc.)
- "n" or more alphanumeric characters
- Use of both uppercase and lower case letters
- Password prohibition rules (e.g., user's personal information

- Password duration - this policy may require users to change the password periodically
- Guidance on user password management - this policy addresses responsibilities for users to maintain the confidentiality of password.
- Password policy sanctions - this policy explicitly communicates consequences of password policy violations.
- Usability considerations for password selection - Password policies are a tradeoff between strength of security for access and the practicalities of user behavior within the clinical workflow model.
  - Requiring complex passwords and requiring passwords to frequently change can result in writing down passwords and posting them in locations where unauthorized users may easily find them.
  - Requiring users to identify themselves multiple times during a log-in session reduces the likelihood that a non-account owner will be able to stay logged-in, however for the real account owner, such a procedure would substantially disrupt the efficiency of workflow.[55]
  - Having multiple different passwords to manage offers security among many devices, yet can also cause confusion and impair user effectiveness of they are hard to remember, particularly in emergency situations.
  - Requiring the use of special characters may be difficult if the medical device in question is used globally and such characters cannot be supported by data entry devices.
  - Since the most frequent types of expected errors in using a password include: data entry errors; failure to remember one's password (password memory is, in fact, the area in which security usability trade-offs are most likely to occur because the easier the password is to remember, the more likely it is to be guessed or cracked); and keying errors (e.g., homing fingers on the wrong keys on the keyboard, pressing the wrong mouse button) resulting from the need to use more than one interaction device ( e.g., a mouse and keyboard, while performing the different steps of this user interaction sequence), produce designs should reflect an understanding of these usability issues and implement product feature to reduce or avoid such issues. [55]
- Password policy enforcement - as a password policy becomes more complex, it also becomes more difficult to enforce due to suitable selection of the password and the frequency of change of the password.

[55] "Usability and Security, An Appraisal of Usability Issues in Information Security Methods"; E. Eugene Schultz, Robert W. Proctor, Mei-Ching Lien, Gavriel Salvendy; Computers & Security Vol.20, No.7, pp.620-634, 2001; http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.89.6079&rep=rep1&type=pdf

A good password policy is one which supports strong security, while also being compatible with the workflow of clinical password users. Such a policy creates and encourages security awareness and a security culture; and ensures that password selection is suited for the targeted users. Therefore, references to guidelines are presented in this section for good password selection; good password management practices; trade-offs of strong security versus usability; and how to enforce a password policy.

Password selection practices[56, 57]:

Passwords for patient care devices (e.g., patient monitors, ventilators, infusion pumps, etc.) are administered by Biomedical Engineering, and typically use the manufacturer-provided password(s) for device access. In some institutions, these device passwords change rarely. One reason for this is that all biomed staff members in an emergency are already familiar with the device password (sort of an emergency access consideration) and that this also enables the manufacturer to remotely access the device for logs and servicing.

Passwords for non-patient care devices are administered by the IT department, and typically embrace IT industry password practices. There are examples where a medical device shares properties of both patient care device and non-patient care device

The usability requirements for patient care devices become both, a security architecture problem and a user interface design problem.

Examples of password management practices[58]:

Formal written password management practices are in place typically in the IT department; for patient care devices, written password management practices are less formal, though there are department lists for passwords of all patient care devices.

Password policy enforcement:

Promulgate password protection policies. Implement awareness training. Include password policies as part of new employee orientation and in regular user performance reviews. Engage users in active discussions aimed at making password policy enforcement easier and more efficient.

Due to privacy and patient confidentiality considerations, password enforcement practices are strong with patient records. Such enforcement practices are tightly linked with HR policies, and violations can be employment termination-relevant offenses.

Usability considerations for password selection and password policy:

Password selection presents a potential conflict between usability (having short, easily memorable passwords and re-using them across multiple devices) and security (which

[56] "Password strength "; Wikipedia, the Free Encyclopedia; http://en.wikipedia.org/wiki/Password_strength

[57] "Password Protection Policy"; SANS Consensus Resource Community; http://www.sans.org/security-resources/policies/Password_Policy.pdf

[58] "Password Policy"; Microsoft TechNet; https://technet.microsoft.com/en-us/library/hh994572%28v=ws.10%29.aspx

dictates longer, more diverse passwords for distinct medical devices).[59] Effective password security depends on good usability in both password selection processes and in password policy. Strategically, designers and maintainers of medical devices must understand factors that cause security technology to be avoided by end-users[60]:

To address these concerns, attention must be paid to the authentication design and to the lifecycle for the authentication information. For authentication design, the following guidance has been proposed:

- Match the authentication process for the medical device access with the most comfortable way in which the user interfaces with the medical device.
- For the user interface for authentication, ensure that it is flexible, consistent and efficient in its flow, and provides informative feedback.
- Design for error: provide safe defaults and help with error recognition and recovery; provide increased tolerance to password entry attempts.

The lifecycle processes for password authentication involve issuance (in-person or confidential delivery of access credentials; memorization and ability to follow rules);

- Limit amount of physical interaction with the user – make the process straight forward
- Limit learning requirements for the user
- Limit the number of constraints for the user

Usability considerations should include the requirements on human memory; ability to recall the specific device password among the many that the user may have.[61]

### 7.4.4 Strong Authentication

There are cases where more than password authentication is required. For example, there is a need to strongly protect sensitive patient data in response to regulatory compliance; or authentication for remote access may warrant more than just a password. Going from password-centric to strong authentication solutions enables organizations to securely authenticate identified users and enable virtual trust.[62]

Passwords were introduced in the 1960s as a low cost, easy-to-use authentication mechanism. Passwords have become more complex and management of multiple passwords is both time-consuming and a security hazard. Strong passwords do not help as much anymore because the

[59] "A Brief Introduction to Usable Security"; BD Payne, WK Edwards; IEEE Computer Society (May/June 2008); http://www.cc.gatech.edu/~keith/pubs/ieee-intro-usable-security.pdf

[60] "Biometric Authentication: How It Works"; eSecurity Planet (08/2012); http://www.esecurityplanet.com/trends/biometric-authentication-how-it-works.html

[61] "Rethinking Password Policies"; A Singer, W Anderson, R Farrow; (08/2013); https://www.usenix.org/sites/default/files/rethinking_password_policies_unabridged.pdf

[62] "Strong Authentication: Securing Identities and Enabling Business"; SafeNet Inc.; ftp://ftp.ealaddin.com/pub/marketing/All/Securing%20Identities%20and%20Enabling%20Business.pdf

 

threats have changed. For internet-connected devices, Phishing attacks and other forms of social engineering trick users into revealing their passwords. Additionally, Spyware in web browsers and keystroke loggers provide attackers with keystrokes, including those used to input passwords.[63]

Thus, there are situations where more than passwords are required to robustly provide data and product security.

Strong authentication is a layered authentication approach, relying on two or more authenticators ("2-factor authentication" or "multi-factor authentication") to establish the identity of the user. It is a form of computer security in which identities of users, clients, and servers are verified without transmitting passwords over the network.[64]

Strong authentication solutions increase security in the authentication process by requiring two or more of the following forms of authentication[65]:

- Something you know: something confidential, known only to the user, such as a password, PIN, or answer to a personal question
- Something you possess: something the user must physically carry, such as a token (USB Tokens: Small handheld devices that users connect to the device's USB port to authenticate. Users are granted access upon plugging the token into the USB port and entering a token password) or a card (Smart Cards: A credit card-sized device that contains highly secure chips that perform cryptographic operations to authenticate the user. Users are granted access upon plugging the smart card into a reader and entering a password).
- Something you are: a biometric feature, such as a fingerprint or facial characteristic (Passwords do not authenticate the user as such. Passwords are often accessible to colleagues and users tend to pass their tokens to or share their passwords with their colleagues to make work easier. Biometrics do authenticate a user as such. Biometrics are automated methods of identity verification or identification based on the principle of measureable physiological or behavioral characteristics such as a fingerprint, an iris pattern, or a voice sample. Biometric characteristics are unique, not duplicable or transferable).

Of importance here is that the elements, which are selected as authenticators are mutually independent.

For some situations, 2-factor authentication is a good trade-off, using both password and a security access badge. For other situations, a unified approach under single sign-on (SSO) solutions offers advantages of centralized management.

[63] "New NIST Guidelines for Organization-Wide Password Management"; NIST Tech Beat (04/2009); http://www.nist.gov/itl/csd/password_042109.cfm

[64] "Biometric Authentication — Security and Usability"; V Matyas, Z Riha; http://www.fi.muni.cz/usr/matyas/cms_matyas_riha_biometrics.pdf

[65] "Strong authentication"; Wikipedia, the Free Encyclopedia; http://en.wikipedia.org/wiki/Strong_authentication

 

Strong authentication solutions come with several risks:

- Performance of biometric systems in terms of speed, accuracy, sensor lifetime, and false acceptance rate. In critical care areas, finger biometrics may be at risk, due to gloves, fluids, gels, and other impairments to reliable reading.
- Usability (easy to learn, user-friendliness, intuitive installation and update process; token administration), openness, and manageability of tokens.
- Emergency access (one or more of the forms of authentication failing in an emergency situation)
- Blending the different forms of authentication seamlessly into the normal workflow of the clinical user.

### 7.4.5 Password Protection

Great care has to be taken by manufacturers, users, and operators that the medical devices' passwords are not being disclosed through careless management. Such disclosure could happen by, for example:

- Noting passwords on the device itself.
- Collecting clear text passwords in notebooks or on sticky notes.
- Making passwords discoverable through web searches (e.g., published training or service manuals).[66]
- In general, making passwords discoverable so they can get posted on underground web sites.

## 7.5 Administrative Rights Management

A significant issue that affects IT systems and systems administration are the challenges of administrative access control. There is typically an account with "root" privileges that is controlled by one person (or person in a specified role). It may give deep (or too deep) access to critical system functions and parameters, like calibration or safety limits.

In the area of networked medical devices, we often find a single administrative account that is shared by the manufacturer, service, and the customer. In addition, often the administrator password cannot be changed by the customer due to manufacturer requirements or design choices. Historically the manufacturer would only support a single account or user with administrative privileges.

### 7.5.1 Account Rights Management

There have been numerous methods implemented to control administrative rights. For example in military and banking there is the concept of dual control/segregation of duties where it

[66] "Patient hackers managed to dial a drug in hospital"; Austrian Times (Dec. 2012);



 

requires 2 or more users to access and implement a command (e.g., missile control or opening a vault). Least privilege introduces the concept of implementing controls based on the users' primary role in the organization. The user receives the minimal access and permission to systems and information to complete the functions associated with their role. An IT security best practice for a system administrator would require the system administrator to have two user accounts:

The System administrator role – this would be used only when performing system administrative functions

The "user" role – the same person would have a second user account, for the other job functions; email, browsing, documentation. This account would have no administrative access or permissions, only "user" access and permissions.

IT security best practice implements the concept of Roles Based Access Controls. This is the concept of what are the tasks/functions required and then using the concept of segregation of duties, would distribute the roles to different users in the organization. For example –the system administrator would not have the ability to review audit logs. The audit function would be assigned to separately to another user to review what actions the system administrator did during the normal system administration tasks as well as to ensure the system administrator did not use the account to perform "user" role tasks. The roles should be defined around the functions that meet the employee job description, e.g., network engineers should not have system administration, and integration engineers should not be able to access network engineering functions unless the job description specifically calls for that function to be assigned to that role.

Most networked medical devices utilize a single administrative account that performs all functions and roles. This was implemented to ensure that the manufacturer supporting the medical device would always have access to the device in the case of a failure for remediation. It also implemented a single point of failure for the management of the medical device. Typically the passwords were well known and distributed.

A more secure method is for medical device manufacturers to design the device to be able to rely on the customer definition of roles. This is typically implemented by Microsoft Active Directory, where roles are implemented in the hierarchy by Organizational Units (OU) and Global Security Groups. The OU can be implemented to define the roles and the global security group implements the access controls and permissions based on the role. The networked medical device manufacturer can use the external roles locally to control access and permissions. This provides the medical device manufacturer with the assurance that the required roles are implemented for device management. The customer can maintain the medical device manufacturer roles and accounts, by changing passwords. The customer assures that implementing roles can provide service and roles-based access controls. This distributes the medical device support responsibility to ensure that service is not limited to a single account (single point of failure).

## 7.6 Information Vulnerabilities

Similar to device software, device data can be vulnerable to exploitation and can be intercepted, manipulated or misused:

- Confidentiality risks:

 

- Patient data (demographics, identities, clinical data)

- Integrity risks with potential impact on patient safety:
  - Configuration data (e.g., dosage) can be altered
  - System data (e.g., thresholds, limits) can be overwritten

The right strategy to protect information from the discussed risks varies based on the potential impact, the type of device, and its use case.

Confidentiality risks can typically be addressed through encryption; however, there is always a trade-off between the need for information protection on one side and device performance and usability on the other. Making the right decisions and design trade-offs largely depend on the nature of the device, but also how it is clinically used and how additional encryption controls would affect end users and clinical workflows, e.g., by requiring an additional log-on step.

Data at rest encryption may be available through the device operating system, or can be provided through commercial after-market encryption software. The encryption algorithm and key parameters (e.g., strength, key length, etc.) should be chosen so that device performance is not impacted, but that regional regulations are met. For example, the Breach Notification law under the U.S. HITECH Act[67] of 2009 exempts healthcare providers from notifying about a breach if the data was encrypted in accordance with NIST SP 800-11.

Data in motion can be secured by using the respective transport layer's native encryption, e.g., HTTPS, FTPS, VPN, or similar. The U.S. HITECH Act suggests Federal Information Processing Standards (FIPS) 140–2 validated encryption methods as for example provided through NIST SP 800-52 (TLS), NIST SP 800-77 (IPsec VPN), or NIST SP 800-113 (SSL VPN).

Especially with wirelessly connected medical devices, choice of the proper transmission security is essential. Security experts generally agree that WEP (Wired Equivalent Privacy) is not sufficient due to an algorithm weakness that allows eavesdropping and recovery of the encryption key. It is generally recommended to use WPA2 / WPA2 Enterprise to assure sufficient protection.

Encryption of both, data at rest and data in motion requires a system for management of encryption keys. This is critical for both, the reliability as well as the security. Insecure key management (e.g., storing keys on the same device as the data it protects) can lead to breaches, and unreliable key management can lead to user access problems or transmission failures. This complex problem is compounded by the fact that often, out of security considerations, keys have a defined, limited lifetime, e.g., for a set time window or for a specific task (e.g., valid for one specific connection for its duration).

Key management systems can be locally implemented through a commercial Enterprise Key and Certificate Management (EKCM) solution, or provided as a service through a Public Key Infrastructure (PKI).

[67] "45 CFR Parts 160 and 164, Breach Notification for Unsecured Protected Health Information"; U.S. Office for Civil Rights, Department of Health and Human Services (Aug. 2009); http://www.gpo.gov/fdsys/pkg/FR-2009-08-24/pdf/E9-20169.pdf

## 7.7 IT Network Infrastructure Vulnerabilities

This section reviews security vulnerabilities formed by the components discussed in the previous section. The "Systems of Systems" problem (e.g., when a new device is integrated into a network) fundamentally changes the original assumption of threat and risk profile.

> "Threat modeling is key to a focused defense. Without threat models, you can never stop playing whack-a-mole." Adam Shostack from: Threat Modeling – Designing for Security

In the previous section we discussed IT component vulnerabilities and practices to best prevent, secure, and mitigate those risks. Next we will move into a high-level, holistic strategy for Cybersecurity as we look at a hospital IT network from a "systems of systems" perspective. Hospital IT networks are unique, and thus managing the risks associated with a given hospital network should be treated as such. How an organization establishes security priorities is based on identifying the common and unique risks, assessing the probability of that common or unique risk's hazardous situation coming to fruition and then determining the severity. This task can be cumbersome especially with complex *system of systems* (i.e., a hospital IT network).

One way to best identify the cyber-security risks and potential threats within a system of systems is by Threat Modeling. First, the term threat model will be used to mean a process to analyze what might go wrong with system of systems like a hospital IT network.[68] Threat modeling a system of systems serves to first map the attack surface, identify vulnerabilities, gather security requirements and countermeasures, find "bugs," and help engineers/sys admins build their IT infrastructure from a security-first mindset. Threat modeling can also be used during the requirements gathering phase of software development for medical devices. A highly potent approach to medical device cyber-security would combine threat modeling at the manufacturing level and at the systems of systems level (i.e., pre and post integration of the medical device in the hospital IT network).

As previously mentioned, identifying threats to an IT network, given all of its IT components without a structured process is cumbersome and arguably a risk in-and-of-itself. Legacy systems, inadequate security designs by manufacturers, regular discovery of malware, DoS for hire services, and other known and unknown threats such as Heartbleed, combined with cyber-criminal networks heightens the necessity for an even more rigorous cyber-security practice by organizations. Threat modeling a *system of systems* enables a high level view while encompassing all of the IT components, endpoints, internal and external data-flows, and most importantly, drives a full assessment of the hospital's IT network attack surface.

Another benefit of threat modeling a hospital IT network is that it enhances the IT change control process. For example, if a threat model already exists, and the integration of a new device is requested, administrators and security personnel can examine the existing threat model, illustrate how the new devices will impact current security mechanisms, and thus plan accordingly. Integrating a new device may require interoperability with other devices. This changes the original assumption about the state of the IT network's attack surface. Moreover, if the new device that is being integrated into the IT network introduces new risks unaccounted for by the

[68] Shostack, Adam. *Threat Modeling: Designing for Security*. Indianapolis: Wiley, 2014. Print.

 

current state of security in the hospital IT network, it is best to capture those issues early, assess and the prioritize how they're addressed in accordance with risk tolerance and available resources. All of which in the long run increase change control efficiency, reduce cost, and create a more manageable security practice and posture.

The generic medical device architecture diagram (Figures 2 and 3, Section 5, Generic Device Architecture) illustrates a basic threat modeling approach for a device manufacturer. The same approach can be applied to IT networks. Intelligent threat modeling tools now provide real time threat assessments against threat models by running analytic threat mapping engines that leverage the resources such as the National Vulnerability Database. For example, if a security engineer has a hospital IT network defined within the threat model tool, when a newly identified vulnerability is populated into the NVD, the new threat will immediately be identified on the hospital IT network model.[69] An added bonus of such tools is that the corrective actions and mitigations measures are provided. This streamlines the identification and response process into an almost fully automated approach.

Specific guidelines on risk management and threat modeling are provided by Microsoft[70], OWASP[71], or through IEC 80001[72], ISO 27001[73], and ISO 14971[74].

### 7.7.1 Hospital IT Networks and Supporting Infrastructure

Hospital Networks and Supporting Infrastructure, such as servers, workstations, routers, etc., can be vulnerable to security breaches and must be taken into consideration when analyzing the larger risk posture.

Any exposure to threats of these supporting components could exploit or impact (directly or indirectly) the medical device. For instance, an adversary could infect one of these systems and use it as a launch pad to find and hack the control system that manages the networked medical devices, thus creating a backdoor attack.

Therefore, these systems need to be included in the Risk Analysis in a dual function: as IT component (security risk) and as a medical device (patient safety risk) and should follow the guidelines set forth in Section 7.2 (COTS Vulnerabilities).

---

[69] "ThreatModeler™ Version 3.4 Release Notes"; MyAppSecurity; http://myappsecurity.com/wp-content/uploads/2014/09/ThreatModeler-3.4-Release-Notes.pdf

[70] "Improving Web Application Security: Chapter 3- Threat Modeling"; Microsoft Developer Network.; http://msdn.microsoft.com/en-us/library/ff648644.aspx

[71] "Threat Modeling"; Open Web Application Security Project (OWASP); https://www.owasp.org/index.php/Category:Threat_Modeling

[72] "IEC 80001-1:2010 - Application of risk management for IT-networks incorporating medical devices"; International Standards Organization (ISO); http://www.iso.org/iso/catalogue_detail.htm?csnumber=44863

[73] ISO 27001 - https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

[74] ISO 14971 - https://www.iso.org/obp/ui/#iso:std:iso:14971:ed-2:v2:en

### 7.7.2 Vulnerabilities of IT Components

When working with system architecture and hardware components, it is imperative that a different mindset be applied to the security approach. Hardware and IT components differ a great deal from software, network and data security due to the basic nature of hardware in general as hardware design and manufacturing usually occur before or during software development. For that reason, we must consider hardware security early in product life cycles. With hardware executing the software that controls a cyber-physical system[75], hardware becomes the last line of defense, thus if an adversary compromises the IT components of the system, then software security mechanisms may be of no value. Additionally, due to the fixed nature and limited accessibility of IT components, relative to that of software, security updates become less frequent resulting in longer exposure to security threats. Interestingly enough, even after IT components are retired, proper disposal is necessitated as security threats still exist due to data and/or software that may still reside on the components themselves. Ultimately, security becomes a crucial consideration with IT components from cradle (design) to post-grave (after retirement).

- Security Concerns
  - Manufacturing backdoors, for malware or other penetrative purposes; backdoors aren't limited to software and hardware, but they also affect embedded radio-frequency identification (RFID) chips and memory
  - Eavesdropping by gaining access to protected memory without opening other hardware
  - Inducing faults, causing the interruption of normal behavior
  - Hardware modification tampering with invasive operations; hardware or jail-broken software (jailbreaking commonly refers to is a form of privilege escalation and removal of limitations of a device's operating system, giving the perpetrator extended system privileges like root or file system access)
  - Backdoor creation; the presence of hidden methods for bypassing normal computer authentication systems
  - Counterfeiting product assets that can produce extraordinary operations, and those made to gain malicious access to systems[76]
- Best Practices
  - Supply Chain Security (Refer to Supply Chain Management 7.8.2)
  - Maintaining awareness of manufacturer firmware updates
  - Risk management based approach

[75] "Cyber-physical system"; Wikipedia, the Free Encyclopedia; http://en.wikipedia.org/wiki/Cyber-physical_system

[76] "Hardware attacks, backdoors and electronic component qualification"; INFOSEC Institute; http://resources.infosecinstitute.com/hardware-attacks-backdoors-and-electronic-component-qualification/

### 7.7.3 Wireless Network Considerations

This document will treat transmission of information general terms, i.e., for the most, no detailed attention is given to specific considerations of wired vs. wireless. However, there are several critical considerations specific to the wireless environment within a healthcare facility.

Many devices in the modern healthcare environment utilize wireless connectivity (e.g., point-of-care blood analyzers, infusion pumps, and other "mobile" devices) and wireless connectivity has unique risks and challenges:

- Although wired networks can, and do, use network access control mechanisms, in a wireless environment using strong authentication to ensure that devices are permitted to access the network is critical due to the lack of physical controls.
- Wireless data should be encrypted to avoid risk of breach or manipulation. The common wireless standards in use provide transport layer encryption that should be used at all times. It is generally recommended to use WPA2 or WPA2 Enterprise as the encryption algorithm of choice; the older WEP encryption standard contains serious security flaws which makes it vulnerable to a breach or attack.[77]
- Because wireless transmission is susceptible to eavesdropping and interception by an attacker that is merely in proximity, strong encryption is required to ensure confidentiality and integrity.
- Denial-of-Service (DoS) attacks are nearly impossible to prevent in a wireless environment because an attacker need not have network access to be effective—one merely has to inject sufficient noise on the proper bands to interfere with wireless communication. Therefore active defenses that employ technology to quickly detect and locate attackers are important.
- Rogue access points are a unique problem, whether resulting from simple unauthorized users' subversion of institutional policy or a truly malicious adversary interested in disruption and interception of communication. Institutions should employ active defenses to find and disable rogue access points.
- Wireless communications is dramatically more susceptible than wired communication to interference from electromagnetic noise sources and unintentional interference from competing wireless devices. Institutions should mitigate interference risks through strong policy, thorough site surveys, and ongoing surveillance and monitoring.

Further discussion of unique wireless aspects is outside of the scope of this document. More information on the topic of wireless security can be found in the literature, for example IEC/TR

[77] "Wired Equivalent Privacy"; Wikipedia, the Free Encyclopedia; http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

 

80001-2-3:2012: "Application of risk management for IT networks incorporating medical devices -- Part 2-3: Guidance for wireless networks"[78].

## 7.8 Workflow and Process Vulnerabilities

In addition to the security properties of the device itself and the network it is operated on, device handling and management is a critical contributing component to an organizations' overall security posture. This includes everything from how a device is handled when it is received to its configuration and integration on the network, but also USB storage media handling or even user training.

### 7.8.1 General Cybersecurity Best Practices and Procedures

Most, if not all, security starts with physical security and medical devices are no exception. Good physical security is the foundation to any sound security plan as it provides protection on the inside. Even in the high-tech world, if a person with malicious intent can gain physical access to a medical device or network attack points, the site has huge exposure to risks such as theft, tampering and potential destruction of the medical device. Additionally, once compromised, there is the potential risk of sensitive and confidential information exposure.

This moves us into the second layer of defense, access control measures. Access control has been widely deployed in healthcare and ensures that only authorized personnel are allowed access to network elements, stored information, information flows, services and applications. The most common type of access control used is Role-Based Access Control which provides different access levels to guarantee that individuals and devices can only gain access to, and perform operations on, network elements, stored information, and information flows that they are authorized for.

Physical security and access controls do add layers of protection when personnel have physical access to the medical devices or networks. Unfortunately, and quite frequently, this protection is compromised by other means such as design flaws, vulnerabilities, and even something as simple as a user not properly logging out. For these reasons, at a minimum, the following should be incorporated as best practices to reduce the risk of improper access:

- Patch Management Practices that ensure timely update of security patches
- Malicious Software Protection to thwart adversarial attacks
- Removal of Unnecessary Services to prevent unintended use or access
- Network Access Control to limit medical device communication
- Authenticated Email Relay to prevent any functionality that could compromise the medical device, i.e., email, web browsing, File Transfer Protocol (FTP), and Instant Messaging.

[78] "IEC/TR 80001-2-3:2012: Application of risk management for IT-networks incorporating medical devices -- Part 2-3: Guidance for wireless networks"; International Standards Organization (ISO); http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=57941

 

- Session Timeout (Unless it conflicts with the intended use of the medical device) to prevent unauthorized access to restricted or essential services or devices left unattended for an extended period of time.

### 7.8.2 Training and Education

As with any security program, security education of users is critical and has to include training of security risks specific to medical devices.

The type of training provided will vary based on the users' roles and responsibilities. Somebody who regularly builds networks or installs medical device will need a much deeper training than a clinical user. However, even clinical users like nurses and doctors need to have basic security training so that they are:

- Informed and up-to-date on the trends in cyber-threats (as appropriate for their role).
- Knowledgeable about the secure use of computer systems, including medical devices.
- Being trained in basic security practices.
- Able to spot unusual system behavior as that may indicate a security compromise.

This type of training should not be limited to the normal use of computer systems, e.g., email, web browsing, or use of clinical and business application. In today's healthcare environment, this also needs to include specific education about computer-based and networked medical device, as the following examples demonstrate:

- Service personnel introducing malware to a medical device network via a USB stick, which got infected due to previous use at home, airports, hotels, coffee shops, or other hospitals.
- A clinician shutting down a ventilator by plugging in his smartphone with the intent to recharge it.
- Medical device receiving a network-based upgrade of their operating system during a patient procedure.

As key constituents, training of Biomedical Engineers and Technicians is of critical importance. These healthcare technology professionals are intimately involved with medical device management and are key stakeholders in mitigating cybersecurity threats. Their day-to-day decisions affect the security posture of a medical device ecosystem and they are a critical party at the table when key decisions are made.

### 7.8.3 Supply Chain Management

An area of risk that's often overlooked is that of Supply Chain Management which consists of the medical device's origin and storage prior to delivery. The Supply Chain Management of medical devices and associated accessories must be secure, resilient and well managed. By incorporating the following security measures into traditional supply chain management practices, an added layer of protection is provided to protect against threats such as piracy, terrorism and theft.

 

- Compilation an inventory of all medical equipment that include the following information
- Device type and identifier
- Device revision or version which includes the operating system, operating system service pack and patch level
- Does the device control or process electronic Protected Health Information (ePHI)
- Security baseline and posture
- Updating equipment inventory whenever there is any change in information for any inventory item
- Annual audit/review of the medical device inventory by the clinical engineering department (or other responsible party)

### 7.8.4 Medical Device Specific Risk Analysis

Any medical device ecosystem needs to be evaluated from a safety and security risk perspective. This is a generally accepted best practice; however, it often proves difficult to be implemented. Challenges include complexity and number of devices to be evaluated, the availability of a complete and up-to-date asset inventory, and organizational disconnects between IT, biomedical engineering, and security and risk officers.

Drivers for performing a security risk analysis include common IT practices, but also regulatory mandates and certification standards, for example:

- HIPAA Security Rule, specifically section 164.308(a)(1)(ii)(A) states: "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization]."[79]
- Joint Commission Accreditation Standard EC.02.04.01 advises to manages medical equipment risks; inventory, categorize risk, incident history; perform maintenance, inspection, and testing.[80]

Although the two requirements evolved from a very different need, now that we have networked medical devices containing ePHI they are forming a joint requirement to manage medical device security risks in order to minimize patient safety risks.

The IEC 80001 series of standards[81] provides a framework that allows healthcare providers to implement a medical device specific risk framework. It offers guidance to establish the right

[79] "45 CFR Parts 160, 162, and 164: Health Insurance Reform: Security Standards; Final Rule"; Department of Health and Human Services Office of the Secretary (Feb. 2003); http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf

[80] "Standard EC.02.01.01: The organization manages safety and security risks"; The Joint Commission Ambulatory Health Care Accreditation Program (2010); http://www.jointcommission.org/assets/1/18/Changes_to_AHC_Standards.pdf

processes and roles and responsibilities, as well as guidance on security controls and specific topics like wireless best practices.

Other commonly used references for a security risk management approach are provided through ISO 14971[82] or NIST SP 800-30[83].

### 7.8.5 Responsibility Management

An organization's management is responsibility for setting the policies and defining the strategy on information protection. From there, responsibilities can be assigned, decisions on security controls and technologies can be made in accordance with the management-defined goals. It is therefore essential that senior management is actively engaged and recognizes the importance of Information Security in addition to the risks associated with the lack of Information Security.

This hierarchy of responsibilities is the foundation of many regulations, e.g., HIPAA, and standards and frameworks, e.g., ISO/TR 80001-2-6:2014: "Application of risk management for IT networks incorporating medical devices -- Part 2-6: Application guidance -- Guidance for responsibility agreements".[84]

Hand in hand with the assignment of responsibilities is the allocation of resources for completing information security tasks. Senior management's participation in security initiatives as well as their expectations needs to be clear to everyone involved.

- Recognition to the importance of Information Security
  - The importance of protecting an organizations' information has to be communicated to all stakeholders: Employees, contractors, vendors, related third-parties and customers. Management must communicate their commitment as well as the necessity and importance of protecting the organization's information to each of these groups.
- Assignment of responsibilities
  - While senior management retains the ultimate responsibility for protecting the organization's information, it must assign responsibilities for specific tasks to people with the right training and skill set.
- Allocation of resources

[81] "Overview of ANSI/AAMI/IEC 80001 - 1 (2010): Application of Risk Management for IT Networks Incorporating Medical Devices"; S. Grimes (Nov. 2014); https://nesce.org/wp-content/uploads/2014/11/Grimes-Risk-Management-for-Medical-IT-Networks.pdf

[82] "ISO 14971:2007: Medical devices -- Application of risk management to medical devices"; International Standards Organization (ISO); http://www.iso.org/iso/catalogue_detail?csnumber=38193

[83] "NIST Special Publication 800-30 Rev. 1: Guide for Conducting Risk Assessments"; National Institute for Standards and Technology (Sept. 2012); http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

[84] "ISO/TR 80001-2-6:2014: Application of risk management for IT-networks incorporating medical devices -- Part 2-6: Application guidance -- Guidance for responsibility agreements"; International Standards Organization (ISO); http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63108

- Hand in hand with the assignment of responsibilities is the allocation of resources for completing information security tasks. Time, budget, tools, or other resources should be assigned and senior management should maintain organizational focus and priorities.

- Providing clear direction in Policies and Procedures
  - Senior management is responsible for making sure that policies are clear and that the business' priorities are understood by the organization.
- Active participation in security initiatives
  - Senior management's participation in security initiatives needs to be clear to everyone involved.
- Participation and guidance in employee education and awareness initiatives
  - Communicating expectations and providing the appropriate training is essential for the members of an organization.

### 7.8.6 Security Management

Security Management involves the process of identifying what assets are at risk and the processes that best protect those assets. These processes tend to be defined through policies and procedures that involve collaborative efforts that demonstrate reduction in risks, promote innovation within the medical device network and adhere to security best practices. Security Management process should include, at a minimum, the following:

a) How policies and procedures are communicated
b) Continuous security training initiatives
c) Role based validation assessments
d) Regularly scheduled scanning of medical devices, especially those first introduced to the network.
e) Remediation and Patching procedures.

### 7.8.7 Use of Portable Media

While the USB Flash Drive is the most notable of portable drives due to its low cost, portability and ease of use, it must not be overlooked that writeable CDs/DVDs, external hard drives, laptops and even Smart-phones constitute alternative forms of portable media.

Unfortunately, it's become all too common for the staff of healthcare organizations to both store and transfer patient data on some form of the aforementioned portable media. Not only is this transport method of ePHI generally ill-advised, it all but guarantees HIPAA non-compliance as most of requirements dictated by HIPAA are unknown to the healthcare professional.

All too often, we hear of HIPAA breaches from theft, such as a USB stick being stolen from an employee's office. Regardless of how the information is compromised, stiff penalties have and will continue to be assessed for negligence.

If no alternative to portable medium is available, at a minimum, the following precautions should be implemented.

- Physically protected against loss, theft, damage and unauthorized access – they must not be left unattended in public areas, unlocked offices, vehicles, hotel rooms, homes etc. without being physical secured e.g., using an approved security cable lock, safe or at the very least, tucked away out of sight.
- Logically protected against malware, unauthorized access, unauthorized configuration changes, etc. using security products approved for this purpose by Information Security Management.
- Encrypt using suitable products and procedures approved by Information Security Management.
- Hospital IT equipment, including portable devices and media, must only be used by authorized users for legitimate business purposes.
- Unauthorized software must not be loaded onto hospital IT equipment, including portable devices and media.
- Before hospital information assets, including portable devices and media, are disposed of or allocated to other users, residual information must be physically destroyed or securely erased using procedures approved for this purpose by Information Security Management.
- Employees must report security incidents and near misses, including those involving portable information assets, through the IT Help/Service Desk in the normal way.

Even when due diligence is conducted through the use of encryption, planning, tracking and logging, the loss of any form of portable media containing ePHI is considered a breach, though the severity may be mitigated, thus making the risk of utilizing such medium for ePHI storage and transport to far outweigh its convenience.

It is typically advised that all devices capable of accepting removable media (USB, CD, DVD, etc.) have the OS's Autorun feature disabled. Although this is not an absolute protection, it does prevent common malware from being executed (and infect the target system) upon media insertion.

 

# 8 Configuration Management

An institution that has medical devices communicating on networks needs comprehensive, accurate and up-to-date configuration information in order to know and control its cyber-security posture (we are concerned here with technical configuration; clinical configuration is outside the scope of this document). If a vulnerability or actual incident becomes known, prompt reaction requires being able to list the equipment at risk, its patch status, network and physical locations.

## 8.1 Planning Tasks and Resources Required

Proactive medical equipment management requires significant start-up and ongoing effort by individuals and designated groups for planning and operational functions. If a commercial or homegrown computerized maintenance system or database is in use and functioning well, that is a major step along the way. But it should be recognized that making such a system match real-world needs should be an ongoing continuous improvement process. It is necessary to consider the desired state of the whole system, both automated and human parts, characterize the gaps from present state to desired state, and prepare a plan giving the steps by which the department will get from the way things are to the way things are planned to be. And as a normal part of departmental operation, besides functions needed to keep the plan going from day to day, there is a need to gather information about how the process is working and how well it is meeting its goals, for ongoing process improvement.

These procedures should be integrated with an existing trouble-ticketing procedure: incidents are in most cases just single instances of a general problem; periodically lists of incidents should be reviewed so that the underlying problem behind an incident can be identified and documented, and the question “what can we do to prevent incidents by mitigating the general problem?” asked. Often the general problem comes from a shortcoming in configuration or change management. Would a technical note or a change in procedures or training help? What is the plan to create an improvement?

Any action on medical equipment potentially entails risks to patients. Departmental policies and procedures for configuration management need to have an explicit risk management component. Use of industry standard procedures for the enumeration, assessment, and mitigation of risks is essential. The ANSI/AAMI/IEC 80001 series of standards is an invaluable guide for biomed departments in this regard.

### 8.1.1 Procedures Written Down and Kept Updated

Many departments function in significant part on individual recollection and oral history for their processes and procedures. It is necessary to get everything in writing and accessible electronically to everyone participating in the work to ensure consistent, reliable results, whoever is doing the work. There are many sources that can be consulted for general templates that can be looked to for ideas that can be adapted to local needs and resources including standards such as the ISO 9000 series, FDA Good Manufacturing Practices and numerous books.

Although they are designed for general information technology organizations rather than specifically for clinical engineering, the publications of the ITIL (Information Technology

 

Infrastructure Library) effort in the U.K. are a very useful source of ideas when planning a configuration management process for biomed departments.[85, 86]

### 8.1.2 Change Management Documents

Change management must be applied at several levels: to documents giving procedures that will be followed in the department, and also to changes in equipment and configuration that result from the work of the department. This is necessary because changes at any level can easily have unplanned and detrimental effects which can easily include new security vulnerabilities. Orderly change management processes ensure that changes are reviewed by those affected by the changes before they are applied, so that they are informed, and so that they may contribute improvements in the plan and play their part when the plan is implemented. There must be a defined, appropriate approval body such as a Change Advisory Board to thoroughly consider and decide on the change before it is started.

### 8.1.3 Coordination and Collaboration with Existing Systems

Regarding existing computerized maintenance management systems, one goal of this white paper is to suggest how specific standards-based information exchanges can relieve some of the pervasive interoperability problems due to proprietary communications methods which beset automation-assisted medical equipment management, just as they hinder clinical data management.

Besides systems specifically made for management of biomedical equipment, general network management software tools deployed either by the biomed department or by the IT department can contribute usefully to management of networked medical devices. Capturing network packets to and from medical devices with appropriate precautions and security and privacy policies is enables detailed troubleshooting, and carefully planned automated network traffic monitoring can warn of conditions that should be investigated for possible security issues. There is wide variability of medical devices in the extent to which they expose standards-based or even proprietary equipment management capabilities. For maximum compatibility and leverage from existing infrastructure, use by medical systems of monitoring and control methods based on general network management standards such as SNMP and WBEM is a useful to both device manufacturers and owners.

There are already a wide variety of practices and automated systems involved in management of medical equipment configurations in healthcare institutions, but there are clear gaps in creating an integrated system out of these. The remedies for some of these gaps can come in part from the use of standards-based communications to support automated exchanges of information to support such integration.

[85] "Introduction to the ITIL Service Lifecycle", UK Office of Government Commerce (2010): The Stationery Office.

[86] "The IT Service Management Forum itSMF UK"; ITIL Foundation Handbook: The Stationery Office (2012)

 

## 8.2 Configuration Management in the Equipment Lifecycle: Examples

Managing device and biomedical network configurations is not a one-time, static event. The challenge is to establish best practices and to provide continual management of the medical device inventory to account for changes in use, threat landscape, and security knowledge. This includes all devices, including the ones owned or leased, and covers all steps from the initial receipt of the device to end of life management.

### 8.2.1 New, Loaned or Leased Device

A key use case in configuration management is when a new device is prepared for first use in an institution or unit. Similar considerations apply to putting loaned or leased equipment into service, with the additional factor of a need to comprehensively clean the equipment of ePHI and any other confidential information, such as passwords and configuration items that might give clues to network configuration in the institution, after a relatively short period of time in service.

It is necessary to accommodate the differences in device types with different templates for the information to be collected in the first stages of preparation to use the device. The attributes needed to describe the capabilities of an infusion pump overlap little with those relevant to a physiological monitor.

The manufacturer's full document set for the device should be studied carefully to determine what configuration information is exposed over the communications interface, and what protocols and protocol details are used. Standards-based protocols should be used rather than proprietary ones when possible. This information is likely to be in a service manual or programmer's guide.

### 8.2.2 Sample Worksheet Contents

The following lists suggest some of the vital information to collect about a device when commissioning it, both for general management and to cover cyber-security-relevant attributes:[87, 88]

- Device type, manufacturer, model, other designations (trade names, often-used code names)
- Supplier, reference to service agreements, contact information
- Listing of applicable documentation, with electronic storage location references
- Separable subassemblies. How will they be tracked?
- Initial hardware, firmware, and software versions. How will manufacturer's changes be tracked?
- Self-test capabilities

[87] Cohen, T. (2014). The Basics of CMMS. Biomedical Instrumentation & Technology, 48(2), 117-121.

[88] Cohen, T., & Stiefel, R. H. (2003). Computerized maintenance management systems for clinical engineering (2003 ed.). Arlington, Va.: Association for the Advancement of Medical Instrumentation.

 

- Initial operational test description
- Configurable items. Can they be configured electronically? What configuration items are included (and not included) in any built-in configuration backup and restore capability? Can a backed-up configuration be fully transferred to another unit of the same kind? This information is crucial, for example, in planning procedures for workflows where configurations must be removed and then restored, such as sending outside the institution for repairs. It is important to test and verify these capabilities before relying on them.
- Normal configurations for various units and contexts
- Periodic testing plan
- Key preventive maintenance intervals
- Training needs (Biomedical, clinical personnel) and plans

The basic functional test procedures in manufacturer's instructions for use or service manual must be carried out as part of the process of preparing a new device for use, and the results, including the date, the person responsible and any relevant remarks, must form part of the record.

It is critical that an isolated testing network should be part of the biomedical engineering department's lab, so as to provide a controlled environment for initial testing, configuration operations without danger to operational networks and devices. It is of course particularly important for devices with possible security problems under investigation should be rigorously isolated – this may best be carried out by specialists.

Separately versioned software and firmware components must be enumerated and current versions recorded. It must be determined whether these versions are compatible with the larger integrated system they are to operate in, and any problems resolved.

#### 8.2.2.1 Change Management Initial Inputs

Basic materials are in data sheets filled out for the device type after identifying any differences between the new device and previous devices of the same manufacturer that are already in use.

#### 8.2.2.2 Network/Subnetwork Association

Identify the specific network context the device will be used in. Determine if there are network protocol, load, or other issues that need to be further investigated before putting the device on the network.

#### 8.2.2.3 Required Configuration Changes in Associated Systems (e.g., Manager Systems for Multiple Devices)

The new equipment may present new desired functionality requiring a plan for making required changes to other equipment it will be operating with.

 

### 8.2.3 Preparation or Off-site Servicing

#### 8.2.3.1 Removal of ePHI and other Confidential Material

As part of the preliminary study of a device type to be included in automated configuration workflows, any ePHI that the device holds in its normal observation must be identified, along with the means by which the ePHI can be completely and reliably removed, and the removal verified. This procedure will then be used at appropriate times including when the device is being prepared to go off-site for services. The procedures for doing this should be described in the device documentation.

#### 8.2.3.2 Save Configuration for Later Restoration

Requires external configuration read information exchange, and store capability.

### 8.2.4 Equipment Returns from Off-site Servicing

There should be a procedure and check list for restoring configuration and default settings to allow the device to operate as before, when put back into its use context.

- Patch level compatibility with current environment. For example, are there known incompatibilities? What is the coverage and procedure for applying the patches to become compatible?
- Configuration compatibility. The device configuration saved before the device went off-site shall be restored and checked for conformance to what is needed in its planned use context.
- Cybersecurity checks. Using procedures developed by the methods described in the cyber-security sections of this document, prescribed checking must be performed prior to putting the device back in commission.

### 8.2.5 Equipment Comes Online (Not Yet Activated)

What can be automated at the point when the device is to be connected to the network depends on the capability of the infrastructure and the device. A key requirement is proper authentication of the identity of the device before it is allowed to do any communication beyond identification and authentication on the network.

For equipment that is not used with a static IP configuration, DHCP server configuration should be considered. The common functions of a DHCP server are typically limited to provisioning the basic IP address, mask, gateway address and certain server addresses for (DNS for example), but extensions and a more elaborate server configuration can handle more specific requirements of a medical device in its context.

Another way for a device with SNMP capabilities to notify a management system when it comes online is via a SNMP Trap. However, there are some practical limitations for the use of SNMP Trap as it is a general IT protocol (utilizes UDP), which creates some limitations with regards to its use in care-critical settings, for example the transmission of medical equipment service

 

signals, e.g., technical alarms. Further, SNMP support may be inconsistent across the medical device inventory.

The IHE PCD domain's Medical Equipment Management, Device Management Communication profile (MEMDMC[89]) is medical equipment specific and patient aware. MEMDMC is HL7® v2.6-based and has the ability to communicate equipment identification, S/W & H/W version information, as well as power status, battery status, self-test status, and indirectly equipment utilization. It is intended to communicate this information to a CMMS.

Additionally, some devices implement other protocol options for supporting auto-discovery by management systems (multiple protocol options). This includes specific protocols for medical device communications such as IEEE 11073.

Part of the process is preliminary checks of the identity and state of the device, and then, if the business rules qualifying the device to operate on the network are met, device details are recorded logged in the database.

### 8.2.6 Equipment Changes Operating Mode

The commonly listed operating modes are:

- Powered off
- Ready
- Standby
- Operating

### 8.2.7 Equipment End-of-Life Procedures

At the end-of-life (or end-of-service) of a medical device, critical steps are required with regards to the information assets stored on the device. Any device may be re-sold as used equipment, refurbished, components may get reused or recycled, or it may be recommissioned for a new lease. In any of these, or similar scenarios, the HDO has to assure that any critical data stored on the device is properly cleared, purged, or destroyed as it may be required by local regulation, e.g., HIPAA for the U.S.[90]:

- As in off-site preparation, procedures for removal of ePHI and other confidential information are applied.
- The proper closing procedures are applied to the entries related to the device in the database record. The device data are taken out of active state and archive.

[89] "Medical Equipment Management Device Management Communication (MEMDMC)"; IHE Patient Care Device Technical Framework Supplement (Nov. 2014); http://www.ihe.net/uploadedFiles/Documents/PCD/IHE_Suppl_PCD_MEM-DMC.pdf

[90] "Frequently Asked Questions About the Disposal of Protected Health Information"; U.S. Department of Health and Human Services, Office for Civil Rights; http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaqs.pdf

 

- Additionally, most medical devices will contain non-clinical, technical information which requires removal. This includes network information, device (and related equipment) network addresses, network and user (e.g., service administrator) accounts and potentially passwords, and wireless SSIDs and passwords. Having these parameters leave a hospital on a device allows the future owner of the device to potentially access the hospital network with valid credentials.

It may be required that the manufacturer provides detailed information so to understand:

a) The type of data stored on the device;

b) The proper method of securely removing data from the device.

Further guidance on system EOL management and decommissioning can be found in the literature.[91, 92]

### 8.2.8 Software Version Inventory

An accurate inventory of all software versions that are deployed, including a breakdown of software or firmware used on all components or subassemblies must be maintained. Questions to be considered are: Are there versions in use that should be upgraded? Are there compatibility issues between versions that are in use?

### 8.2.9 Ongoing Tracking

As part of the operational plan, it is important to document the automated and manual tracking information that will be gathered, how it will be stored and the plan for notifications to persons in order to assure that inoperative or otherwise threatening conditions are promptly evaluated and dealt with. Automation is obviously not a substitute for human vigilance, but to the extent that devices support automated collection of detailed device state information, the opportunities for detecting problems before they have serious adverse effects. Manufacturers should be proactively supporting standards-based ways of reporting such data over network interfaces

Changes in regulatory compliance requirements must be tracked for devices. This is typically at least a partially manual operation – receiving notices, determining whether they apply to any devices in the active inventory.

When a recall becomes known, a plan must be prepared to identify and gather the affected equipment for processing.

Quality of service and device health metrics:

[91] "System Decommission"; Office of System Integration, State of California, CA.gov; http://www.bestpractices.osi.ca.gov/system_development/system_decommission.shtml

[92] "System Decommissioning Best Practices for Life Sciences"; ASUG Annual Conference (May 2012); http://events.asug.com/2012AC/3114_System_Decomissioning_Best_Practices_for_Life_Sciences__Learnings_from_the_Trenches.pdf

- Network statistics. A routine should be established for checking switch and router error statistics to look for trouble or incipient trouble. Automation can be used to filter out observations that are obviously normal.

System log scanning:

- The institution will have many systems that log detailed operational information in files. System documentation and example logs should be studied for the kinds of useful indications they can give, and script automation should be applied to detecting and calling attention to possible problems. This should be an ongoing activity: when manual troubleshooting of an incident reveals a log pattern that could recur and could be recognized, the scripts should be enhanced to detect the significant log pattern and give appropriate notifications.

Usage statistics are valuable for:

- Identifying equipment which is due for maintenance or is nearing end of useful life
- Identifying equipment that is underutilized because it is: not needed and should be considered for reassigning, not accessible and needing to be repositioned, considered for de-accessioning and sale or donation
- Maintenance schedule. Data extracted from device documentation concerning maintenance schedules for each device model should be available to programs tracking preventive maintenance. The need for maintenance may be identified by usage statistics (see “usage statistics”) or by elapsed days since last service.
- The recently released IHE PCD MEMDMC (Medical Equipment Management, Device Management Communication) Profile can contribute equipment utilization and cycle occurrence count to the CMMS. This helps to specifically identify when a piece of equipment is to go off cycle for periodic or use cycle maintenance (a downtime period which could also be used for software patching).
- Lifecycle of wear-and-tear parts. Many devices have subsystems such as batteries that have a different lifecycle than the containing device and which need to be separately tracked for testing and possible replacement. Manage system health and technical advisories. The documentation should be searched for available tracking information which may be useful for detecting faults and signs of potential faults in equipment function, and measure taken to include them in automated tracking, and deliver notifications as appropriate.

## 8.3 Resource Library

### 8.3.1 Cataloged and Linked Electronic Service Manuals

Hardcopy manuals cannot be consulted remotely, content-searched, and frequently stray from where they are supposed to be. Electronic forms are more findable, accessible, and generally useful.

 

The electronic titles should be cross-referenced by manufacturer, model, type of device, trade names or nicknames so that a user can readily find what is needed using whatever information is known to them.

## 8.4 Planning Configuration Management

### 8.4.1 Planning Configuration Management

Configuration Management is a process that ensures that configuration information of components and the IT networks are defined and maintained in an accurate and controlled manner, and provides a mechanism for identifying, controlling and tracking configuration of the IT network and its individual components.[93]

> "The process and tools used to track/control/prevent/correct security weaknesses in the configurations in network devices such as firewalls, routers, and switches based on formal configuration management and change control processes.[94]

As new vulnerabilities are discovered the information technology threat landscape is changing every day. The state of security for an information system requires constant renewal and verification. Configuration Management planning must incorporate the process of constant renewal and verification to help ensure best practices are being met. Planning configuration management is a core component in the overall risk management and change control process of any information system.[95] Medical device integration adds another layer of risk that must be considered since patient safety and information privacy can suffer sudden adverse impacts in the event of misconfiguration or inadequate configuration management practices.

As an aspect of an organization's overall risk management plan, best configuration management practice starts with an information system security plan. When integrating a medical device into an IT network, the scope of the information system security plan must take into account medical device vendor specific processes and risks. A rigorous assessment of medical device and IT network security risks within the Information System Security Plan (ISSP) can serve to identify gaps and enable further appropriate assurances and mitigations. Additionally, requesting a Manufacturer Disclosure Statement on Medical Device Security[96] ($MDS^2$) from a vendor can also provide important details about the devices under review. Moreover, organizations must identify and adhere to the intended use of the medical device during the deployment and configuration process. Deviating from the manufacturer's intended use for the sake of security that in turn elevates the potential risk to patient care is not acceptable.

[93] ANSI/AAMI/IEC 80001-1: 2010, Application of Risk Management for IT Networks Incorporating Medical Devices – Part 1: Roles, Responsibilities and Activities.

[94] SANS: Top 20 Critical Security Controls (Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches)

[95] "ISO/IEC 27001:2013(en)"; https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

[96] "Manufacturer Disclosure Statement for Medical Device Security"; National Electrical Manufacturers Organization, The Association of Electrical Equipment and Medical Imaging Manufacturers (Oct. 2013); http://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx

An information system security plan will capture all security requirements, including configuration management and lifecycle management. NIST Special Publication 800-18 Revision 1: Guide for Developing Security Plans for Federal Information Systems, provides specific examples and a template for establishing a system security plan that can be modified to address unique IT network environments that host various types of medical devices and other embedded systems.[97] The information system security plan will also capture any governing policies and procedures. In essence, a base state of the device and network must be recorded. As a device or IT network changes with updates or modifications, whether a significant or minor change, a record of when, why, and how the configuration was modified must be recorded and linked back to the state preceding the newly recorded configuration. This will ensure traceability in the event that anomalous network or devices behavior occurs. Ideally, testing should be conducted before fully implementing any configuration changes. The testing process will serve to ferret out any unforeseen errors before "go live" and provide time for corrective action to take place and minimize the potential interruption during device usage or interruption to the hospital IT network in the event of an inadvertent misconfiguration is introduced.

## 8.5 Asset Tracking and Management

Management of medical devices, particularly mobile devices, is a challenge for hospitals today.[98, 99] A hospital may have thousands of devices that need to be managed. In order for them to be managed effectively they need to be first located. There is typically pressure on engineering departments that are responsible for locating and managing medical device assets within the inventory. The complexity of managing a wide variety of devices can be expensive to operations while the organization is striving to ensure availability, safety and security of these devices. In addition, when clinical staff doesn't have the right equipment, at the right place, at the right time, they can resort to hoarding.

A specific aspect of asset management is to reduce the risk of and help mitigate the impact of device loss or theft, which could lead to loss of patient data and may trigger legal requirements around breach notification and management.

Asset management and location tracking provides a means to efficiently track, map and report the location and status of medical device assets in real time. This allows clinicians and administrators to improve:

- Asset utilization
- Resource management
- Capital and rental expenditures

[97] "NIST Special Publication 800-18: ISO/IEC 27001:2013(en)"; U.S. National Institute of Standards and Technology; https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

[98] "Asset tracking: What it is and whether it is right for you [Guidance Article]"; ECRI. (October 2006); Health Devices, 35(10), 365-386.

[99] "Asset tracking systems [Evaluation]"; ECRI. (2006, November); Health Devices, 35(11), 397-419.

 

- Equipment loss
- Regulatory compliance
- Preventive maintenance
- Recall compliance.

Staff can leverage the an inventory tracking system to search and locate assets typically by building, floor, unit or caregiver, using a geospatial facility map or table format. Tracking systems can display up-to-the-minute information on the status and state of equipment.

Alerts and notifications for medical device management can be delivered via smart phone, email or pager. Standard reports and dashboards enable healthcare organizations to visualize asset utilization in real-time and develop strategies for improving overall asset management.

Medical devices are subject to systematic preventive maintenance procedures that are enforced by the Joint Commission in the U.S., recommended by the World Health Organization, and required by authorities in several other countries. To address maintenance requirements and to assure optimum availability, the biomedical department needs to have a system for locating and managing medical device assets. Finally, loss-prevention continues to be a motivation in many institutions.

### 8.5.1 Asset Tracking Methods

Many hospitals have or have been considering a location tracking technologies such RFID (radio frequency identification) to track the location of medical devices. The technology can be used to track the location of medical devices needed for inspections or repairs, and it can also be used to find equipment needed by the clinician in real time.

Asset tracking systems locate devices through the use of some form of tag. If the tag is electronic, such as an RFID tag, signals are emitted that are detected by readers located in ceilings or on walls in the tracking area. The data from the readers is then sent to an IT server environment, where algorithms are used to determine the device location.

Asset tracking systems also provide clinicians and IT personnel a user interface to search for the location of these devices. Users access the user interface of the asset management system to gain access to the device properties. Location information about specific devices can be displayed, typically in table form or on floor plan maps. For example, an IT person looking for a specific patient telemetry monitor would look at an electronic map of a care area that shows where the monitor can be found. Information about each device, such as manufacturer, model number, functional status and maintenance schedule can be displayed with the device on the display. Mobile devices or devices that are typically hard to find are typically good candidates for asset tracking.

#### 8.5.1.1 Communication Methods

Communication between tags and readers can be accomplished various ways. Currently they are based mostly on:  RFID, Wi-Fi, and IR. It appears most of these systems overall make use of proprietary methods of communication protocols and device management meta-data methods.

 

There can be significant differences among the suppliers of these systems which present a challenge in terms of standardization, particularly in the area of interoperability between dissimilar systems that use different technologies and methods of tracking.

#### 8.5.1.1.1 Radio Identification Technology

Radio Frequency Identification (RFID) refers to a wireless system comprised of two components: tags and readers. The reader is a device that has one or more antennas that emit radio waves and receive signals back from the RFID tag. Tags, which use radio waves to communicate their identity and other information to nearby readers, can be passive or active. Passive RFID tags are powered by the reader and do not have a battery. Active RFID tags are powered by batteries.

Physical layer radio technology and protocols are designed for very low power consumption at data rates to that do not interfere with or burden Wi-Fi signals. The network returns precise, room-level accuracy and eliminates floor hopping, which can be problematic in Wi-Fi___33-based deployments.

RFID can track the location of devices which can improve hospital efficiency and decrease costs, and at times improve patient safety by helping hospitals locate devices more quickly. RFID is just one of the technologies used for locating devices. Other technologies used for the same purposes include infrared and ultrasound detection.

RFID tags can store a range of information from one serial number to several pages of data. Readers can be mobile so that they can be carried by hand, or they can be mounted on a post or overhead. Reader systems can also be built into a cabinet, room, or building.

RFID technology combined with asset management software applications collect, maintain, track and analyze the data and provide customized reporting of the location, status, audit, and maintenance history of each medical device asset. Some hospitals track device assets by using an approach known as "Active" RFID because it uses tags that have batteries and constantly beacon. The most popular form of Asset Tracking using RFID is "passive" RFID using ISO Standard 18000-6c.

### 8.5.1.2 Types of Medical Device Assets

Infusion pumps are currently the most commonly tagged items. These devices, by their nature are moved around various care units, sometimes making them difficult to locate. An asset tracking system for these devices is very useful for clinicians, clinical engineering departments and IT personnel.[100] Other commonly tagged devices would be external pacemakers, electrocardiographs, telemetry transmitters, ultrasound carts, telemetry monitors, and noninvasive blood pressure monitors.

[100] "Asset Tracking Systems: Readiness and Selection Factors, Patient Safety and Quality Healthcare Newsletter"; James P. Keller, Jr. MS (ECRI); May / June 2007

 

### 8.5.2 Medical Device Asset Management and Tracking Scenarios

The following are various usage scenarios related device asset management and tracking.

- Locating: Reduced time spent looking for equipment and more time available for patient care.
- Service: Discover who is responsible for servicing the device, obtain their contact information, and schedule the service.
- Calibration: Ability to know exactly where equipment is and whether it needs calibration.
- Lease and maintenance schedule management: When scheduled maintenance or lease renewals require attention, automatic alerts can be sent via email or text message to a mobile device
- Inventory Management: Real-time inventory management enables staff to perform automated inventory counts.
- Asset Utilization: Asset utilization analysis to help managers assess capital equipment purchasing requirements and allocation among hospital departments.
- Rental Management: Rental equipment tracking ensures that items are returned in a timely manner and enables optimization of the balance between capital and rental equipment.
- Equipment inspection: View maps or reports to understand the location and status of equipment requiring preventive maintenance. Alerts can be setup indicating when missing equipment appears back on site.
- Corrective Maintenance: Enables automated alerting for equipment requiring repair and maintenance.
- Recall Management:
  - Minimize time-consuming searches for equipment that has been the subject of a recall.
  - Identify the locations of recalled equipment. Alerts inform staff whenever equipment that is currently offsite returns back onsite or arrives at certain areas of the hospital
- Contract Management: Equipment tracking enables the Hospital IT staff to locate Capitol equipment purchased under identified contract agreements.

### 8.5.3 Integration with other Management Systems

Location and status data from Asset Tracking systems can be integrated into existing maintenance management hospital systems. These systems are automatically populated with location and status data. An asset or a group of assets requiring maintenance or recall can be viewed on a map directly from the maintenance management system. In Addition, integration with medical device management systems, such as infusion pump management servers, enables users to view the location and status of the device directly from the device management system user interface.

 

### 8.5.4 Automated Management Systems (CMMS, CMDB)

In both, the biomedical engineering environment as well as in the IT environment the use of automated tools has become common, in fact maybe even mandatory considering the complexity and number of assets to be managed.

In the IT environment such systems are typically referred to as Configuration Management Database (CMDB) and are focused on features required for the building and maintenance of IT systems and networks. A commonly sued framework for CMDB systems is provided through the Information Technology Infrastructure Library (ITIL)[101].

Typical CMDB systems provide features to allow for license and contract management, support of standardized built process, IT configuration management (network, operating system, etc.), asset discovery and management, patch management, workflow and process management, ticket system, and integration with other management or IT systems (e.g., email).

In the biomedical environment, Computerized Maintenance Management Systems (CMMS) are more common as their features are geared more tailored towards the operational management and maintenance needs. Typical CMMS systems include features supporting lifecycle management, asset and inventory management, work orders, preventive maintenance, scheduling, recall management, and the like.

With today's computerized and networked medical devices are often duplicated in a CMDB as well as CMMS system. As a result we often find a situation of "dual bookkeeping" including challenges like inventory and data inconsistency as well as the need to enter and maintain each asset on both systems. At the time of this writing first combined systems are being introduced to the market, providing a single database approach, but separate views and workflows to meet both, IT's and biomedical engineering's needs.

Recently, new IHE PCD profiles have been introduced to address the need for automated processes around device identification and management:

- IHE PCD profile MEMDMC[102] (Medical Equipment Management, Device Management Communication) has been developed to identify equipment.
- IHE PCD profile MEMLS[103] (Medical Equipment Management, Location Service) can be used to track the location of equipment (including features like identifying equipment that is offline for too long).

[101] "ITIL"; Wikipedia, the Free Encyclopedia; http://en.wikipedia.org/wiki/ITIL

[102] "Medical Equipment Management Device Management Communication (MEMDMC)"; IHE Patient Care Device Technical Framework Supplement (Nov. 2014); http://www.ihe.net/uploadedFiles/Documents/PCD/IHE_Suppl_PCD_MEM-DMC.pdf

[103] "Medical Equipment Management Location Services (MEMLS)"; IHE Patient Care Device Technical Framework Supplement (Nov. 2014); http://www.ihe.net/uploadedFiles/Documents/PCD/IHE_Suppl_PCD_MEM-LS.pdf

## 8.6 Lifecycle Management

Lifecycle management: The process of deploying, maintaining, and terminating the use of a medical device in an IT network. Medical device lifecycle management is a core component of the overall risk management process and should be clearly defined within the organizations information system security plan for that device.

Security concerns involve the process of how the deployment, maintenance, monitoring, removal and disposal of the medical devices are conducted. Misconfiguration during deployments, inadequate maintenance and monitoring practices may increase the risk for a breach of intended use, ePHI confidentiality, and physical patient safety. Moreover, inadequate practices in the removal and disposal of a medical device can lead to breaches of ePHI confidentiality. Lastly, insufficient adherence to related policies and procedures governing the lifecycle management could expose an organization to charges of negligence in the event of a legal compliant or investigation.

Lifecycle management must be a holistic processes derived from the organization's risk management plan. The information system security plan, a component of the risk management plan, should serve as the driving factor in lifecycle management for a medical device. Since the security plan will contain all the risks, controls, its governing policies and procedures, and any other relevant aspects of the medical device, adherence to the plan will meet the needs of lifecycle management process. Many resources on the topic of risk management exist. [104, 105, 106]

104 "NIST Special Publication 800-18: ISO/IEC 27001:2013(en)"; U.S. National Institute of Standards and Technology; https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

[105] "Guide for Developing Security Plans for Federal Information Systems"; http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf

[106] "Getting Started with IEC 80001: Essential Information for Healthcare Providers Managing Medical IT-Networks - See more at: http://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=918#sthash.moQPpu1t.dpuf"; Association for the Advancement of Medical Instrumentation (AAMI); http://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=918

# 9 Conclusion

This document has taken a comprehensive approach to introducing cybersecurity in the context of networked medical devices. It has presented generic medical device architecture to illustrate where and how potential security vulnerabilities can be exploited. It has then offered several best practices for managing these vulnerabilities.

Since the threat landscape is ever evolving, there is the necessity to continue to secure medical devices that are in clinical use. Therefore, the topic of configuration management becomes quite important. Finally, this document provides the reader with a rich set of references from which further inquiry and investigation can be pursued.

A few key principles from this paper include:

- Cybersecurity incidents related to medical devices can adversely affect the safe and effective delivery of services by the healthcare delivery organization. The impact can be quite significant, even resulting in patient harm and potentially even being a matter of life and death.
- We must transition our thinking away from single solution notions within the medical device ecosystem for protection against cybersecurity issues, to a “defense in depth” philosophy that requires the contributions of multiple stakeholders for success.
- Good product security provides enhanced product software quality.
- Thoughtful security is a strong partnership with good usability.
- Security engineering can be successfully embedded into the medical device development process, just as safety engineering has.
- While the proposed best practices presented here address the contemporary threat landscape, we need to recognize that as threats change, the methodologies that have been offered here should evolve as well.

 

# Appendices

# Appendix A: Secure Application Development Practices

The chart below illustrates the top recommended secure application development practices as provided by the SANS Institute.

| | |
|---|---|
| Error Handling and Logging | 1. Display generic error messages<br>2. No unhandled exceptions<br>3. Suppress framework generated errors<br>4. Log all authentication activities<br>5. Log all privilege changes<br>6. Log administrative activities<br>7. Log access to sensitive data<br>8. Do not log inappropriate data<br>9. Store logs securely |
| Data Protection | 10. Use SSL everywhere<br>11. Disable HTTP access for all SSL enabled resources<br>12. Use the Strict-Transport-Security header<br>13. Store user passwords using a strong, iterative, salted hash<br>14. Securely exchange encryption keys<br>15. Set up secure key management processes<br>16. Disable weak SSL cipher on servers<br>17. Use valid SSL certificates from a reputable CA<br>18. Disable data caching using cache control headers and autocomplete<br>19. Limit the use and storage of sensitive data |
| Authentication | 20. Don’t hardcode credentials<br>21. Develop a strong password reset system<br>22. Implement account lockout against brute force attacks<br>23. Don’t disclose too much information in error messages<br>24. Store database credentials securely<br>25. Applications and middleware should run with minimal privileges |
| Input & Output Handling | 26. Conduct contextual output coding<br>27. Prefer whitelists over blacklists<br>28. Use parameterized SQL queries<br>29. Use tokens to prevent forged requests<br>30. Set the encoding for your application<br>31. Validate uploaded files<br>32. Use the nonsniff header for uploaded content<br>33. Validate the source of input<br>34. Use the X-Frame-Options header<br>35. User Content Security Policy (CSP) or X-XSS Protection headers |

| | |
|---|---|
| Session Management | 36. Ensure that session identifiers are sufficiently random<br>37. Regenerate session tokens<br>38. Implement an idle session timeout<br>39. Implement an absolute session timeout<br>40. Destroy session at any sign of tampering<br>41. Invalidate the session after logout<br>42. Place a logout button on every page<br>43. Use secure cookie attributes (i.e., HTTP only and secure flags)<br>44. Set the cookie domain and path correctly<br>45. Set the cookie expiration time |
| Access Control | 46. Apply access controls checks consistently<br>47. Apply the principle of least privilege<br>48. Don't' use direct object references for access control checks<br>49. Don't use un-validated forwards or redirects |
| Configuration and Operations | 50. Establish a rigorous change management process<br>51. Define security requirements<br>52. Conduct a Design review<br>53. Perform code reviews<br>54. Perform security testing<br>55. Harden the infrastructure<br>56. Define incident handling plan<br>57. Educate the team on security |

Further details on the above can be found: http://software-security.sans.org/resources/swat.

## Appendix B: Abbreviations

| | |
|---|---|
| AAMI | Association for the Advancement of Medical Instrumentation |
| ANSI | American National Standards Institute |
| APT | Advanced Persistent Threat |
| CA | Certificate Authority |
| CERT | Computer Emergency Response Team |
| CD | Compact Disk |
| CMDB | Configuration Management Database |
| CMMS | Computerized Maintenance Management Systems |
| COTS | Commercial off-the-shelf Software |
| CPU | Central Processing Unit |
| CSP | Communications Service Provider |
| CVE | Common Vulnerabilities and Exposures |
| DHCP | Dynamic Host Configuration Protocol |
| DMZ | Demilitarized Zone (referring to a specific network architecture) |
| DNS | Domain Name System |
| (D)DoS | (Distributed) Denial of Service Attack |
| DVD | Digital Versatile Disk |
| EC | European Community |
| EHR | Electronic Health Record |
| EKCM | Enterprise Key and Certificate Management |
| EOL | End of Life |
| EOS | End of Support |
| FDA | Food & Drug Administration |
| FTP(S) | File Transfer Protocol (Secure) |
| HDO | Health Delivery Organizations |
| HIDS | Host Intrusion Detection System |
| HIPS | Host Intrusion Prevention System |
| HIS | Hospital Information System |
| HR | Human Resources |
| HTTP(S) | Hypertext Transfer Protocol (Secure) |
| IDS | Intrusion Detection System |
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronics Engineers |
| I/F | Interface |
| I/O | Input/Output |
| IP | Internet Protocol |
| IPsec | Internet Protocol Security |
| IPS | Intrusion Prevention System |
| IR | Infrared |

| | |
|---|---|
| ISO | International Organization for Standardization |
| ISSP | Information System Security Plan |
| IT | Information Technology |
| ITIL | Information Technology Infrastructure Library |
| LED | Light Emitting Diode |
| MTBF | Mean Time Between Failure |
| NERC | North American Electric Reliability Corporation |
| NIST | National Institute for Standards and Technology |
| NVD | National Vulnerability Database |
| OS | Operating System |
| OU | Organizational Unit |
| PACS | Picture Archiving and Communications System |
| (e)PHI | (electronic) Protected Health Information |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| RAM | Random Access Memory |
| RF | Radio-Frequency |
| RFID | Radio-Frequency Identification |
| RTLS | Real-Time Location Management Systems |
| SANS | SysAdmin, Audit, Networking, and Security Institute |
| SNMP | Simple Network Management Protocol |
| SP | Special Publication (a NIST document type) |
| SQL | Structured Query Language |
| SSL | Secure Socket Layer |
| SSO | Single-Sign-On |
| STIG | Security Technical Implementation Guides (a Department of Defense publication) |
| TCP | Transmission Control Protocol |
| TR | Technical Reports (an IEC document type) |
| UDP | User Datagram Protocol |
| U/I | User Interface |
| USB | Universal Serial Bus |
| VLAN | Virtual Local Area Network |
| VPN | Virtual Private Network |
| WBEM | Web-Based Enterprise Management |
| WEP | Wired Equivalent Privacy |
| WPA (2) | Wi-Fi Protected Access II |

 

# Appendix C: Reference Literature & Further Reading

Below a list of some of the key documents for further education on the topic of cybersecurity in general as well as specific to medical devices. Also included are references from outside of healthcare since the underlying technical fundamentals applying to cybersecurity for networks of embedded systems are very similar and the best practices developed by these industries very well can be used as guidance.

## C.1 General Security

"Blue Team Handbook – Incident Response Edition"; D. Murdoch (Aug. 2014); http://www.blueteamhandbook.com/

"Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments "; National Security Agency, Information Assurance Solutions Group; https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

"NIST SP 800-160: Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems"; National Institute of Standards and Technology (May 2014); http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

"Strategies to Mitigate Targeted Cyber Intrusions"; Australian Government Department of Defense, Intelligence and Security (Feb. 2014); http://www.asd.gov.au/infosec/mitigationstrategies.htm

## C.2 Medical Devices and Healthcare

"Audit Trail and Node Authentication (ATNA)"; IHE International; http://wiki.ihe.net/index.php?title=Audit_Trail_and_Node_Authentication

"Medical Device Isolation Architecture Guide, Version 2.0"; US Department of Veterans Affairs (Aug. 2009); http://himss.files.cms-plus.com/FileDownloads/2013-Medical-Device-Isolation-Architecture-Guide-2009.pdf

"Medical Devices Security Technical Implementation Guide, Version 1, Release 1"; Defense Information Systems Agency (DISA); 27 July 2010; http://iase.disa.mil/stigs/Documents/unclassified_medical_device_stig_27July2010_v1r1FINAL.pdf

## C.3 Industrial Control Systems

"Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies": US Department of Homeland Security; October 2009; https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf

"NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security"; National institute of Standards and Technology (June 2011); http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

"Common Cyber Security Vulnerabilities Observed in DHS Industrial Control Systems Assessments"; US Homeland Security, Control Systems Security Program, National Cyber Security Division (May 2011); https://ics-cert.us-cert.gov/sites/default/files/documents/DHS_Common_Cybersecurity_Vulnerabilities_ICS_20110523.pdf

"Mitigations for Security Vulnerabilities Found in Control System Networks"; US ICS-CERT (2006); http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/3-Mitigations_for_Vulnerabilities_Found_in_Control_System_Networks%281%29.pdf

"Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Systems Environments, Version 1.0" Idaho National Laboratory, Critical Infrastructure Protection Center (Feb. 2007); http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/OpSec_Recommended_Practice.pdf

"Recommended Practice: Creating Cyber Forensics Plans for Control Systems"; US Homeland Security, Control Systems Security Program, National Cyber Security Division (Aug. 2008); https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Forensics_RP.pdf

"Recommended Practice for Patch Management of Control Systems"; US Homeland Security, Control Systems Security Program, National Cyber Security Division (Dec. 2008); https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/PatchManagementRecommendedPractice_Final.pdf

"Firewall Deployment for SCADA and Process Control Networks Good Practice Guide"; Centre for the Protection of National Infrastructure (Feb. 2005); http://energy.gov/sites/prod/files/Good%20Practices%20Guide%20for%20Firewall%20Deployment.pdf

"Backdoors and Holes in Network Perimeters A Case Study for Improving Your Control System Security"; US-Cert Control System Security Center (Aug. 2005); https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/CSSC-CaseStudy-001.pdf

## C.4 Other Industries (Oil & Gas, Energy)

"A Comparison of Oil and Gas Segment Cyber Security Standards"; U.S. Department of Homeland Security, Control Systems Security and Test Center (Nov. 2004); http://www.naseo.org/data/sites/1/documents/energyassurance/documents/cybersecurity/Comparison_of_Oil_and_Gas_Security.pdf

"A Comparison of Electrical Sector Cyber Security Standards and Guidelines"; U.S. Department of Homeland Security, Control Systems Security and Test Center (Oct. 2004); https://www.hsdl.org/?view&did=7941