OWASP Secure Medical Device Deployment Standard

Christopher Frenz

Version 1.0 03/20/17

With the growth of electronic medical records systems and the increasing use of network enabled medical devices, hospitals and other healthcare related facilities are becoming more interconnected than ever. While this increasing level of interconnectedness often results in improvements to both the quality and efficiency of patient care, it is not without some potential security drawbacks. Many medical devices are extremely costly to upgrade or replace and such legacy systems within healthcare facilities are often commonplace. Moreover, many medical devices were engineered with patient safety and life saving as the sole functions of the device and little attention was traditionally paid to the security of these devices. These trends are evidenced by recent FDA recommendations as well as numerous security studies that find many medical devices rife with security vulnerabilities. Additionally, such networked enabled medical devices within hospitals are often not deployed with security in mind, which can further add to the ease of compromise. With the explosion of botnets and other malware that now target IoT devices (of which medical devices can be considered a subtype) the need for security minded deployments of medical devices is now more essential than ever. This guide is intended to serve as comprehensive guide to the secure deployment of medical devices within a healthcare facility.

Purchasing Controls

One of the best ways to preserve the security of any healthcare environment is to take measures to prevent the introduction of security vulnerabilities to the environment by ensuring only devices that provide a reasonable measure of security are introduced into the environment.

Security Audit/Evaluation

Prior to any medical device being purchased or brought onto any network the device should be compared to the organizations internal security standards and a determination should be made as to whether or not the device is capable of meeting those standards. Can the device comply with password policies, account lockout policies and other security controls that the organization considers essential?

Privacy Audit/Evaluation

In a similar manner, prior to any system acquisition, a privacy evaluation should be performed to ensure that the device possesses the requisite security controls to ensure that patient data is collected, stored, and transmitted in a way that is consistent with organizational policy. Where applicable, preference should be given to solutions that were designed with Privacy by Design principles in mind (https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf).

Support

Any device purchased will only be considered supportable by the vendor for a finite period of time. Given the critical role that patching vulnerabilities plays in maintaining the security of any system, particular attention to should be given to what kind of support the vendor will provide for the software of devices, how frequently they release patches, and for how many years they will continue to provide patches for the device. Given the long active lifetime of many medical products, paying attention to the long-term ability to patch systems is a critical security consideration that should weigh in on purchasing decisions. Related to this consideration should be given to a vendors policies concerning security issues that are presented to them.

Perimeter Defenses

Wherever possible medical devices should be fully denied access to anything external, but there are some cases where this might not be possible as medical devices may need to connect to update servers, may need to transmit data to cloud hosted medical records systems, may need transmit data to 3rd party services for assessment (e.g. remote radiology reading services), etc. These controls are designed to control the flow of information between medical devices and external resources and services.

Firewalls

Firewalls at the perimeter are an essential control to ensure that communications between medical devices and external resources are either outright denied, where feasible, or restricted to just the communications that are essential for the device to function properly. In the case where a medical device is reachable over the internet, particular attention should be taken to ensure that the device has a separate administrative interface and that external access to the administrative interface is not possible from outside the organizations internal network.

Network Intrusion Detection System

Network Intrusion Detection Systems at the perimeter can be helpful in detecting exploit attempts coming from external parties as well as helpful in detecting traffic going to command and control sites and ransomware key generation sites. As such Network intrusion detection systems at the perimeter can be useful for their potential for providing early warning of an attack attempt or successful compromise of a network enabled device.

Proxy Server/Web Filter

For devices that communicate with external resources via http and/or https a proxy server or web filtering appliance may allow for even finer grained control over communications than a firewall. Moreover, many proxy servers have the ability to perform antivirus scans of Web traffic. Where this is possible, it is recommended to use a different AV engine than the one used on internal endpoints as that will help to maximize the chance of successful detection for any malware vector. Additionally, many appliances perform the ability to perform SSL stripping and these appliances can often be used as a part of a data loss prevention (DLP) system as a result. DLP may be advisable for use with medical devices that may require internet access in some form, but would not normally be used to transmit PII or PHI to an external entity.

Network Security Controls

Network Segmentation

Network segmentation is highly useful in preventing the spread of malware and other threats through a network and is highly beneficial in containing a threat in event an endpoint or device is successfully compromised. All medical devices should be an isolated network segment that restricts communication of the devices to just the systems that are required for the device to function. All other communications should be restricted. Network segmentation is often achieved through the creation of VLANs and ACLs to control the flow of traffic in VLANs, but can also be achieved by using an separate physical network infrastructure, which is particularly useful in areas where a concentration of the same type of medical device will be deployed in a given area.

Internal Firewalls

Internal firewalls can be used to improve upon network segmentation and used to further restrict communications of devices to just the systems (internal and external) that they need to interact with. Firewalls, particularly next generation models, can also provide ways of monitoring and restricting traffic in ways that ACLs in switches cannot as they typically allow for deeper levels of traffic inspection. Internal firewalls are also highly useful for protecting “one-off” devices, such as an MRI machine, where isolation is sought but the presence of only a single device does not warrant the purchase of an entirely separate physical network infrastructure. Internal firewalls help to promote a zero trust model with regards to the communication with medical devices.

Internal Network IDS

If traffic from network segments containing medical devices is routed through an internal network Intrusion Detection System, signatures can be created to detect default login credentials, attempts to connect to command and control IPs, and other forms of network traffic that may indicate an attack on a medical device or a successful compromise of a medical device. While similar in function to an IDS at a perimeter this helps take into account that a compromised endpoint within the organization may be used as a staging ground to launch an attack against the medical devices.

Syslog Server

Where possible medical device logs should not just be stored on the device itself but should be exported to a distinct syslog server to allow for the collection and analysis of events that affect the device. This is critical in cases where the device itself may no longer be trustable or an security issue makes the log data on the device inaccessible in some manner.

Log Monitoring

Related to above control some form SIEM or log analysis should be performed on the collected log data. For example, a high occurrence of failed login attempts on a device or even a high occurrence of successful logins across a large number of devices (outside of scheduled maintenance) may be indicative of an attack from IoT malware like Mirai.

Vulnerability Scanning

IoT devices should be routinely scanned to ensure that they are properly configured and that out of date software does not leave them susceptible to compromise. As such IoT devices should be included in part of the larger vulnerability management program that the organization has in place. Not all IoT devices and features may be readily assessed by traditional vulnerability scanners and specialized scanners my have to be considered. Even with specialized scanners there is such diversity amongst IoT devices that manual compliance auditing may be needed in some cases as indicated in the device security section below.

DNS Sinkholes

While some medical devices may require DNS to function properly (e.g. to transmit results by hostname, to connect to update servers, etc.) it is highly likely that these devices will only need to be able to resolve a very limited number addresses. The security of a medical device deployment can be improved by having dedicated DNS servers for the device that can only resolve the limited number of IP addresses required for the device to function. All other DNS requests can be sinkholed.

Device Security Controls

Some of the most critical controls to protect any network enabled medical device will need to be implemented within the device itself. These are recommended configurations that take advantage of such controls. Not all devices will support all controls but such deficiencies should have been identified in the security audits done prior to purchase and compensating controls identified at the time.

Change Default Credentials

As widely illustrated by the recent Mirai and Bashlight botnets the presence of default credentials is a highly effective means of leaving any IoT device highly vulnerable and medical devices are no exception to such vulnerabilities. All devices should have their default credentials changed prior to deployment on the network and devices with hardcoded credentials should not be used. Account credentials used in place of the defaults should be compliant with organizational password polices.

Account Lockout

Changing the default password doesn't matter if the device can easily be compromised with a dictionary attack or brute force attack. Account lockout features should be configured to block logins after 3-5 login attempts.

Enable Secure Transport

Devices should be configured to only send data in a secure format and secure protocols like ssh and https should be used in place of insecure protocols like telnet and http. Insecure networking protocols should be disabled wherever possible.

Spare copy of firmware/software

In the event that a device is compromised or runs into some other software issue, having a spare copy of the devices firmware or software is critical to restoring the device to functional state in a timely manner. Staff should be trained and competent in procedures to load reload software/firmware on the various kinds of medical devices supported.

Backup of device configuration

In addition to the software or firmware used to run the device there is most likely also some custom configuration required to make the device run properly on your network. Backing up these custom settings after changes occur will help to ensure that devices can be restored to functional status in as timely a manner as possible.

Baseline Configurations

Related to the controls above baseline configurations should be established for each device that ensure the proper configuration of the device with regards to clinical functionality and security. In the event a device specific backup is not available this baseline configuration can be modified to ensure the quick restoration of device in a manner that is compliant with organizational security policies.

Encrypt Storage

Medical devices should support encryption of any PHI and/or PII stored on the device. This feature should be turned on in case of device theft or an unauthorized user gaining physical access to the device.

Different User Accounts

Admin accounts and user level accounts should be possible and ideally the admin account should be bound to the management interface and unusable on any internet facing interface.

Restrict Access to Management Interface

The management interface of the device has the potential to do the most damage to the device if compromised, as it will more easily allow access to the administrative functions of the device. Communication to this interface should be locked down to only authorized terminals for making changes to the device.

Update Mechanisms

Weather via automatic download or the manual install of new software/firmware, all devices will require updating at some point. Mechanisms should be put in place to identify the need for updates and to ensure the routine update of all medical devices so that unpatched vulnerabilities remain minimized.

Compliance Monitoring

As time passes, changes are often made to systems (either intentionally or unintentionally) and applied updates may introduce changes to devices. Compliance monitoring should be routinely done to ensure that updates or other changes keep device configurations consistent with baseline configurations and organizational security policies.

Physical Security

Security controls should be put in place to ensure that physical access to medical devices is limited only to authorized individuals and that physical theft of the device is prohibited.

Asset Management

Keeping track of which devices are in which locations and what versions of software/firmware they are all running will be invaluable in helping to determine the scope of potential incident. It will also be extremely valuable for tracking the remediation phase of any incident response.

Interface and Central Station Security

It is not uncommon to have one or more computers attached to medical devices to be used for the collection and analysis of medical device data (a central station) or PC/appliance to be used to send data the EHR system (an interface). While they can be distinct systems, in many cases they are hosted on the same system. These security controls pertain to security these devices. In particular, securing interface systems are important as these are often the points at which your isolated medical device network is bridged with your organization's main internal network.

OS Hardening

Since this guide is specific to providing guidance on medical devices it will not go into depth on OS Hardening techniques, but techniques like the removal of unnecessary services, password protection, installation of AV, and other common OS hardening techniques should all be employed. Please consult guidance specific to your operating system for further details.

Encrypted Transport

As with the medical devices themselves, these systems will be used to send and receive data and as such should make use of the same secure protocols discussed in the device configuration section.

Message Security – HL7 v3 Security Standards

Interface systems will often be used to transmit data to an organizations EHR, PACS, or other clinical system and HL7 messages are the standard format for accomplishing this. The exchange of HL7 messages should be done using the HL7 v3 standard as this provides for security provisions not present in earlier versions of the HL7 standard.

Security Testing

All the controls in the world are useless if misconfigurations and vulnerabilities are rampant. Security testing will help you to uncover and shortcomings in your devices or within the setup that surrounds them. It is better to discover such issues via testing so they can be addressed via fixes or the addition of compensating controls than to later discover the same weakness exists during the forensic face of an incident response.

Penetration Testing

A penetration test can be an effective mean of assessing how effective your device and network configurations are at turning back an attack on medical device installed on your network. The results can be used to help you further improve your defenses and may reveal flaws in the device that can be presented to the manufacturer for patching in a upcoming update release.

Incident Response

Eventually all organizations will face the compromise of one or more devices. One of the things that differentiates an organization that has a mature security program from ones that don’t is how effective they are at detecting, containing, and eradicating such threats.

Incident Response Plan

Organizations should have detailed plans in place to deal with the compromise of medical devices before such an incident becomes a reality for the organization. Organizations should have a clear cut plan in place that defines how they will react to an incident and who will be responsible for what actions during the detection, containment, eradication, and recovery phases. It is also important all staff are made aware of the plan and are trained to respond appropriately and effectively. For organizations without any sort of incident response plan in place, a good starting resource is https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Mock Incidents

It would be highly beneficial for any organization to conduct a mock incident regarding the compromise of medical devices to ensure that they have an effective incident response plan in place and that employees are adept at carrying out that incident response plan. Mock incidents provide a great way to identify security deficiencies as well as effective practices and use the lessons learned to further improve your organization’s security posture.

Acknowledgements

Thanks to Tony Alas for his input on biomedical devices.