International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 11
July 2016

Security and Privacy for Networked Medical Devices

Kaushik P[1], Guru R[2]
[1]M.Tech, 4th Semester, Computer Engineering
[2] Assistant Professor, Dept. Of Computer Science & Engineering
Sri Jayachamarajendra College of Engineering, Mysuru, Karnataka, India

Abstract: ***A growing number of medical devices are intended to be linked to computer networks. Many of these networked medical devices include off-the-shelf software that is exposed to cyber security threats such as viruses, worms and many more. These vulnerabilities may represent a risk to the safe and effective operation of networked medical devices and normally require an ongoing maintenance effort throughout the product life cycle to assure asatisfactory degree of protection [1]. This paper surveys Threats faced by Medical devices, Awareness and some solutions to mitigate these threats and also some of the recent work from the security community.***

Index Terms: Attacks, vulnerability, Standards

I. INTRODUCTION

Ever since clinicians, physicists and engineers have learned how to put on technology to improve diagnosis and treatment of patients, medical devices have become an integral part of our healthcare delivery system. And, as technology advances, 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 coordinated 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.Medical devices, such as infusion pumps, patient monitors and MRI scanners, can be just as susceptible to malware as standard computers. Keeping them secure in any networked environment is certainly challenging, and the stakes are high for these particular applications since they can affect patient care and results. The computer security community has recently begun research on the security and privacy issues associated with medical devices and recognized both existing flaws and new techniques to improve future devices[2]. Paul Jones of the U.S. Food and Drug Administration has said:

"The issue of medical device security is in its infancy. This is because, to date, most devices have been isolated from networks and do not interoperate. This paradigm is changing now, creating new challenges in medical device design." (Personal communication, Aug. 2007)

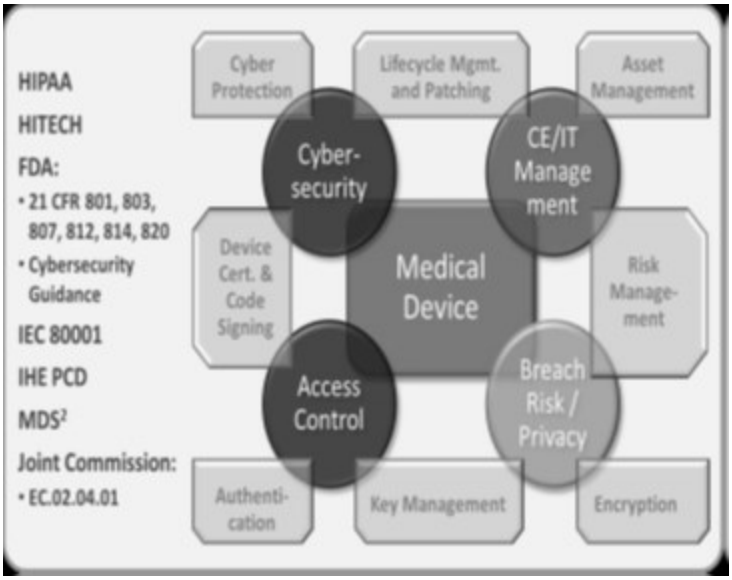

Fig 1: The Complexities of Medical Device Security

The basic main connectivity scenarios and their basic vulnerabilities are as follows [3]:

• *Disconnected:* device is not connected to the network, but potentially subjected to a targeted or air-gap attack.

• *Permanently connected* to a standard or proprietary network. Susceptible to any network based attack vector, directed or not.

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 11
July 2016

• *Wireless:* same as permanently connected, but requires specific attentions 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 reestablished.
• *Legacy Device:* device may not have native network capabilities, but may be connected via Interface or Translator. The device is disposed 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.

Figure 2 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.

From a security perspective, Figure 2 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 devise 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.

Device Ecosystem
(traditional, hospital-based)

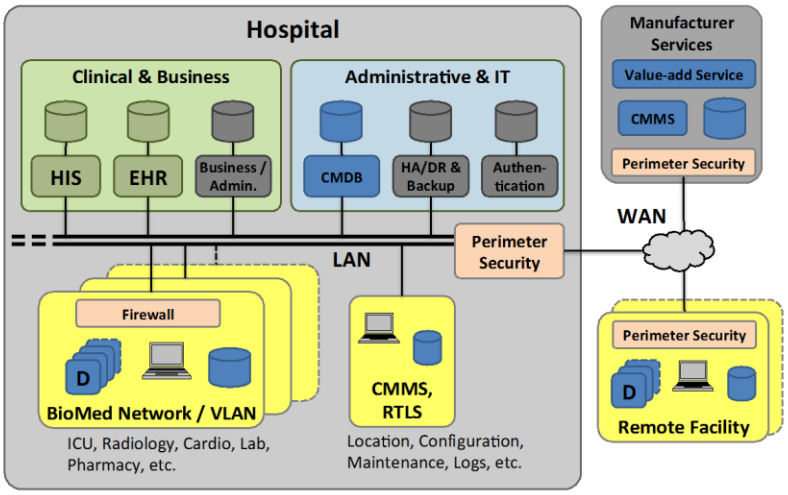

Fig 2: Generic Device Ecosystem

A number of factors complicate protection of medical devices, and contribute to a continued state of insecurity. These are a result of technical, management and human causes [4].

• Providing hackers with vital information: certification agencies publish device verification information, such as spectrum; radio frequency transmission data are published in device manuals; and the device workings are available on patent databases. It is a misconception to depend on security through obscurity even where proprietary protocols are used for communication. Not only does this limit interoperability, but it also leaves a gap for reverse engineering from which little protection can be applied.13 Using sound and proven cyber security approaches provides better protection.

• Legacy operating systems and software (typically devices, systems, and software that is over 5 years old or has been replaced by a new version), and incompatibility between systems leaves vulnerabilities such as misconfiguration and security holes. This includes vulnerabilities from non-negotiated interfaces with third party software, often through web interfaces.

• Lack of timely software updates and patches. This is often an issue where concerns with workflow and service disruptions are present. Although health care providers, such as the US Veteran Affairs, have considered improved patch management,36 this will remain an ongoing issue in settings where large numbers of devices are used and are a constituent part of other clinical information systems.

• Medical devices do not have basic security features. For instance, computed tomography scanners delivering measured radiation can be tampered with, potentially creating life threatening patient safety issues. Security features added after design, sometimes at implementation, can disrupt clinical workflow and are implemented poorly.

• Compromised medical devices can be used to attack other sections of the health care organization network. The demand for interoperability and seamless integration between systems, networks, and devices increases the risk for cyber security breaches.

• Lack of awareness of the cyber security issues, and poor security practices compound the underlying problem of mixed cyber security programs in device development and certification. These poor practices include lack of secure disposal of devices containing information or data, password sharing, and distribution of passwords particularly in devices where passwords are required for device access. Inconsistent education and training on cyber security risks and impacts also underpin the continued cyber security vulnerabilities.

• Achieving a balance between security and privacy goals and health care utility and safety can be challenging. For instance, using strong encryption and access control measures enhance security, but place the patient at greater risk in the case of an emergency.

• Limited power and resources of medical devices mean that encryption can slow down medical devices, and reduce the usable battery life.

These issues highlight the complexity in the control and management of cyber security risk and contribute to the overall lack of security seen in the health care field currently.

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.

Attacks and Actions[5]:

1. Stop unauthorized data copying

Attack: Confidential patient records fall into the wrong hands when an unauthorized person downloads the data onto removable storage devices and media, such as USB drives, MP3 players, CDs and DVDs.

Action: Implement a security strategy that safeguards users and data, while providing hospital IT organizations granular control over data privileges, such as specifying what data can be copied to external devices.

2. Prevent untrusted code execution

Attack: Untrusted code – such as worms, viruses, spyware and other malware already installed on a medical device – begins to execute and compromise the device.

Action: Implement a security measure that stops untrusted code from launching and unauthorized changes to be made.

3. Interrogate incoming packets

Attack: A hacker conceals a virus in spurious packets, or a mis-configured host system sends unintended packets to the device.

Action: Implement a firewall on the device that discards unwanted packets and logs packets, which can be used to identify potential malicious actions at a later time.

4. Protect data and communications

Attack: After breaking into a medical device, a hacker attempts to communicate with other devices and systems on the network in order to access confidential data. *Action:* Enforce password-based authentication using identifications mechanism.

5. Prevent unintended interactions between applications

Attack: A virus exploits a security hole in the graphical user interface (GUI) software of a CT scanner and then hooks onto the application that administers the radiation dosage.

Action: Run safety-critical applications in virtual machines (VMs), so a virus resident in one VM cannot infiltrate the memory space of an application in another VM.

7, Reduce attack surface

Attack: After embedding and launching itself in a device's memory, a virus accesses the device's network ports to look for other programs that it can manipulate.

Action: Minimize malware entry points into the system by using gatekeeper virtual machine (VM) to protect direct access to the network ports, thereby making the other VMs less vulnerable. If the gatekeeper is attacked, another VM acting as a watchdog could initiate a recovery sequence.

8. Harden device against unexpected failures

Attack: Viruses, worms and denial of services attacks may exploit vulnerabilities in a device's external interfaces at multiple layers, and take advantage of untested and poorly handled error and edge conditions.

Action: Emulate hacker behavior prior to release, trying to anticipate paths that can be used to attack a device and attempting to cause a device to fail under adverse conditions.

Solution space and its challenges

This section details the guidance that can be used to devise suitable protection mechanisms, mitigations, and processes.

Information security processes: The secure configuration of the network and attached devices, together with the subsequent coordination required for patch management (software updating) is a major confounding factor.

Reporting and feedback loops: Good feedback and notification systems are required between health care providers and medical device manufacturers, to ensure effective mitigation of potential cyber security issues. In addition, legislation to mandate reporting of cyber security incidents would assist in identifying issues from all health care providers.

*Risk management:*Risk management and governance processes should include documenting data flows with regard to networked medical devices. This would ensure that appropriate protection is provided at each stage of data transfer, processing, and storage. Such management has to be defined by organizational policy, and supported with appropriate procedures.

Regulation: The requirement for renewed FDA approval when any changes are made to a medical device, including the embedded software, means additional cost and time to market.

Resilience activities and contingency planning: Network segregation, particularly for legacy devices, is a sound resilience and protection measure. This may include setting up virtual local area networks, firewalls, limiting access, and the use of uninterruptible power supplies on critical care devices.

Standards: Standards provide good practice yet need application and interpretation. The design aspects are key to cyber security protection. These standards include:

• ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cyber security standard provides guidance on addressing cyber security issues and its relationship to other types of security to highlight the basic practices in cyber security.

• IEC 62304:2006 – Medical device software – software life cycle processes define the medical device software lifecycle requirements.
• ISO/DTR 80002-2 Medical device software – Part 2: Validation of software for regulated processes is a technical report under development, which considers embedded and associated software with all medical devices.

CONCLUSION

While medical device manufacturers are making significant progress in improving the reliability of devices in normal operation, the security of wireless communication in these devices has not received as much attention. Yet, vulnerabilities often allow attackers to take full control of devices and perform actions that may gravely injure patients. We have discussed many security threats faced by medical devices and have suggested some solutions, while these recommendations do not solve the complexity of improving security in medical devices, they do put into place policies that will incentivize development of security techniques.

REFERENCES

[1] Cyber security for Networked Medical Devices Containing Off-the-Shelf (OTS) Software, Center for Devices and Radiological Health, 2005.
[2] Shane S. Clark and Kevin Fu, "Recent Results in Computer Security for Medical Devices", International ICST Conference on Wireless Mobile Communication and Healthcare (MobiHealth), October 2011.
[3] "Medical Equipment Management (MEM): Medical Device Cyber Security –Best Practice Guide", IHE Patient Care Device (PCD), White Paper, 2015.
[4] Patricia AH William and Andrew J Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem", Medical Devices: Evidence and Research 2015.
[5] "Increasing Medical Device Security with Mainstream IT Platforms and Technologies", WHITE PAPER, Intel® Architecture Processors, 2011.
[6] "Securing Hospitals, A research study and blueprint, Independent Security Evaluators, 2016.