World Academy of Science, Engineering and Technology
International Journal of Biomedical and Biological Engineering
Vol:11, No:5, 2017

Analysis of Threats in Interoperability of Medical Devices

M. Sandhya, R. M. Madhumitha, Sharmila Sankar

Open Science Index, Biomedical and Biological Engineering Vol:11, No:5, 2017 publications.waset.org/10007170/pdf

***Abstract*—**Interoperable medical devices (IMDs) face threats due to the increased attack surface accessible by interoperability and the corresponding infrastructure. Initiating networking and coordination functionalities primarily modify medical systems' security properties. Understanding the threats is a vital first step in ultimately crafting security solutions for such systems. The key to this problem is coming up with some common types of threats or attacks with those of security and privacy, and providing this information as a roadmap. This paper analyses the security issues in interoperability of devices and presents the main types of threats that have to be considered to build a secured system.

***Keywords*—**Interoperability, threats, attacks, medical devices.

I. Introduction

INTEROPERABILITY illustrates the intensity to which systems and devices can swap data, and understand that shared data. Systems that are interoperable must be able to trade data and subsequently present that data in a form that can be understood by a user. In healthcare, interoperability is the facility of diverse information technology systems and software applications to converse, swap data, and use the information that has been exchanged to improve the quality. The data can be shared and exchanged among all the members regardless of the application or application vendor. Mostly equipments will try to improve the confidence level but most devices are not designed to interconnect with other devices. Therefore, it becomes difficult to interconnect the medical systems to perk up patient care, avoid unnecessary accidents, and obtain complete data to personalize care delivery.

Getting it precise protects patients, contributes to clinical verdict and positive patient outcomes, and improves efficiency. Getting it erroneous introduces noteworthy risk and the possibility of adverse patient events. Worse, getting it wrong does not mean returning to the baseline risks of an unconnected world—it will lead to more grave situations than exist now. Safe interoperability is vital, not secondary, to the core mission of healthcare.

The rest of the paper is organized as follows: Section II discusses related works. Section III presents the importance of security in interoperability of medical devices. Section IV introduces the attacks on interoperability and Section V presents the network and wireless vulnerabilities on interoperability. Finally, Section VI discusses the importance of security in interoperability of medical devices and concludes the paper.

M. Sandhya (Professor) and Sharmila Sankar (Professor & Head) are with the CSE Department, BSA Crescent University, Chennai, India (e-mail: sandhya@bsauniv.ac.in, sharmilasankar@bsauniv.ac.in).

R. M. Madhumitha (II Year – MBBS) is with the Stanley Medical College, Chennai, India (e-mail: madhumitha.magesh@gmail.com).

II. Related Work

Involving information and communication technology (ICT) in health solutions has shown to raise satisfaction both for healthcare providers and patients. Much is expected of medical informatics towards achieving better health providence for people throughout the world, both in contributing to the quality and efficiency of health care and to innovative biomedical as well as computer, health, and information sciences research [1]. Handheld devices have been exploited in many cases to facilitate health oriented procedures [2], [3]. Developments in wireless communications integrated with developments in pervasive and wearable technologies will have a radical impact on future healthcare delivery systems [4].

Mobile applications solutions are becoming increasingly popular because smartphones are used by most people and target different health issues or groups of patients [5]-[7]. The US Health and Human Services' (HHS) Center for Medical Interoperability announced two milestones linking prominent industry and health delivery organization groups [8], [9].There has been rising interest in security issues pertaining to medical data collection, data transfer and processing and electronic medical health records [10]-[12]. There seems to be broad advocacy for systems engineering approach to interoperable medical device development [13].

Medical device development has been extremely impacted by the invasion of computerization, with a fairly parallel drive toward interoperability [14]. Major medical professional organizations, recognizing the assurance of improved patient safety as well as probable for risks, have passed safe guarded resolutions in support of medical device interoperability [15]. Safety, Security, and Usability are consistently recognized as essential Needs, Wants, or Desires (NWD) for all stakeholders of interoperable medical devices [16].

III. Importance of Security in Interoperability

By definition, information technology (IT) confine data; interoperable systems detain even more.

Despite the information stream, the healthcare community's ability to distribute and gain knowledge from the data to make superior decisions and investments remains sketchy. Ultimately, the holy grail is to use interoperable technology as a base for a learning system that contributes to patient safety and efficiency of healthcare. As such, interoperable technology can serve as an influential instrument that supports

Open Science Index, Biomedical and Biological Engineering Vol:11, No:5, 2017 publications.waset.org/10007170/pdf

clinical and business decision making, but only if the healthcare community makes a commitment to learn to use these tools to improve.

Security in general is described in terms of availability, integrity, and confidentiality. Interoperable systems are vulnerable to worms, viruses, malware, phishing, and user errors that compromise integrity and availability. Confidentiality is a prime aspect of many medical systems. Physical systems have a separate set of vulnerabilities that depict them to physical attacks that can influence both availability and integrity. Confidentiality is also a security aspect of physical systems. All three aspects of security are presenting interoperability of medical devices. Understanding, representing, and guaranteeing security in the interconnection of medical devices is a significant challenge because any analysis must account for the components of a system and their interactions.

Given the consumer outlook about devices being networked, we must ensure appropriate security management, including methodical assessment of risk and its solutions in the device's design. Meanwhile, wearables and remote monitoring technologies are the common practice now, which distorts the links between consumer devices and medical devices. As more numbers of devices are connected and when they enter the healthcare realm, the possibility of additional attack surfaces and vulnerabilities become available to bad actors. To enhance the safeguards of healthcare systems and the patient data they have been entrusted to protect, we must perk up threat and incident information sharing across the industry; no single sector of the healthcare ecosystem can crack the problem single-handedly. Only by pulling together and sharing best practices can we prevent cyber criminals and protect patients. A protected healthcare system will ultimately facilitate greater consumer confidence and will stimulate better care coordination, enhance information exchange and improve patient care.

As the requirements to guarantee patient safety, present clinicians with convenient access to information and images, and give medical device security converge, healthcare IT professionals are facing new challenges.

Questions include:

1. How to build confident medical device security as care providers access patient information and images on an extensive range of devices?
2. What are the possible sources of attacks and maximum risks to data? How do we guard against them?
3. How can we convene our goals to drive down operational costs by reducing "one-offs" in our venture design when interfacing with regulated medical devices?
4. With varied approval of security top practices by manufacturers, how can we appraise our device and system providers and decide where they stand?

IV. Attacks on Interoperability

Medical device interoperability is an increasingly common example of how computing and information technology will revolutionize and streamline medical care. Even though many communication standards have been anticipated, only few of them include security mechanisms that are bendable and completely adequate to convene current and future security needs. There are noteworthy fissure between required security properties for these systems and those that can be tackled, even by a grouping of currently standardized protocols. Safety concerns in these standardization efforts are effectively partial due to deficiency in appropriate security analysis.

Our primary aim towards laying down the base to secure clinical environments was to categorize the security risks, threats and requirements of various clinical scenarios. An attack is an undesirable effect on a patient due to an adversary's actions. This includes outflow of sensitive patient information; at the wrong time, erroneous, or no actuation; untimely or no monitoring; or alarm deactivation. It was found that an important and yet often neglected requirement is to minimize the impact of insider attacks posed by already-compromised devices. The table below lists the common types of attacks with their description.

TABLE I
Types of Attacks

Attack Class	Description
Destroy	attempt to physically demolish a device or its components
Disturb	try to perturb and modify the functionality of a device
Reprogram	modify data or code to prevent its correct operation
Denial of service	aim to refute service to devices
Eavesdrop	make an effort to overhear something on a message

V. Network and Wireless Vulnerabilities on Interoperability

To develop solutions for interoperable medical devices the network and wireless vulnerabilities have to be analyzed clearly. Attacks that make use of networks as a vector are usually aimed at the following three targets: web servers, databases, and application software.

1. **Web servers:** A web service is commonly used in interfacing with medical devices, providing a graphical interface through which a device is interacted. The flaw of using such an interface is that web services normally contain vulnerabilities that might be exploited in such systems by malicious parties or by inadvertent manipulation. There are many attack tools which can be downloaded and used to scan web interfaces and emphasize any vulnerability in the web service. An attacker can use this information to build a specific payload to attack an exposed target.

Injection vulnerabilities and cross side scripting are the two most common flaws that occur in web applications. Carefully skilled data can ploy an application into executing or accessing unauthorized data. SQL injection occurs when attackers take benefit of sites that create SQL queries using user-supplied data without first examining to make definite it is valid. This permits an attacker to put forward malicious SQL queries and get ahead of commands directly to a database. Cross side scripting aim an application's users by

Open Science Index, Biomedical and Biological Engineering Vol:11, No:5, 2017 publications.waset.org/10007170/pdf

injecting code into a Web application's output. Whenever the compromised page is viewed, the browser executes the code, allowing an assailant to capture user sessions, pass on the user to a malicious site. XSS attacks are feasible within the contents of a dynamically generated page, whenever an application fits in user-supplied data without properly validating it.

2. **Database servers:** Devices and systems include a database to maintain the essential information for that device, commonly referred to as a database back-end. These databases run a coding language called a structured query language (SQL), which is vulnerable to a very serious attack called an SQL injection, which could potentially be used to simply delete all information from the database. The attacker can examine all of the information through which a break of confidentiality is achieved and they can insert false data, which results in a loss of integrity of the data.

Databases also contain a networking interface, and so hackers are capable to arresting this type of traffic to exploit it. External attackers who penetrate systems to steal data are one threat, but the main problem is with the people working inside the organization. The insiders are also likely to steal files including database backups .This is a common problem for an organization and the solutions developed should consider encrypting archives to mitigate the insider-risk. System administrators and database developers need to expand a reliable practice in looking after their databases, staying conscious of threats and making definite that vulnerabilities are taken care of.

3. **Application software:** This is the software which is running successfully on a device, be it in coincidence with either of the previous two categories or on its own. Any software running on a device could have potential vulnerabilities where it has not been subject to rigorous software vulnerability testing. Many cyber attacks are also grooming that have vulnerabilities which are not rigorously tested prior to operation in a live environment.

Systems with obsolete security patches face the risk of malware attacks that use software exploit. A successful exploit may show the way to immediate malware infection or remote users gaining control over infected systems. These malware may include Trojans that execute malicious routines into the system. Such malware also includes backdoors that can correspond with a remote user, and spyware that can steal the credentials and personally identifiable information from the infected system. Updating the security patches at regular intervals also solves the technical problems to improve the software's performance. The systems have to be updated regularly to neglect the vulnerabilities. Unfortunately, not all users are keen on applying these updates. The initial step to staying protected is to apply the latest security patches provided by the software vendor. This provides defense against exploits and web threats that abuse the software vulnerability as an infection vector.

Besides malicious attacks, there are also the possible unexpected interactions between devices and systems. Wireless technologies such as WiFi are particularly prone to intervention, including interference from medical devices such as electro-surgical units, and encourage tampering simply by making it easier for malicious persons inside or outside the hospital to access the network. Attacks against medical devices can happen due to social engineering and network infiltration, as well as vulnerabilities in hardware and software. The most common threats today include ransom ware, man-in-the-middle (MiTM) attacks, phishing and, on occasion, physically compromising devices.

Social engineering illustrates that phase of an attack is where the attackers attain information from people who encompass knowledge of the system or its security measures such as passwords, by chatting, emailing, or masquerading. The majority of successful attacks have some aspect of social engineering. The last category is comprised of viruses, worms, Trojans, and advanced unrelenting threat malicious software. This software aims and makes use of identified vulnerabilities in software to gain control of or corrupt a system. Conventionally, antivirus software is used to alleviate this threat but this has become increasingly ineffective. Strong and secured networks can create a fence; however, medical devices still suffer from the same vulnerabilities.

Many of today's devices, apps, and popular software packages have at least some elements such as scripts or protocols which are open-source, and often have the advantage that many developers work on these projects. The concern is that if the code is open, it could allow hackers to execute malicious activities. Closed-source software can also face the same problem of weaknesses and vulnerabilities that go unchecked leading to a greater likelihood of exploitation.

Maintaining security for medical devices depends on the maintenance of five basic properties:

1) Data Integrity: All information generated and exchanged between the medical devices and the supervisor are accurate and complete without any alterations.
2) Data Confidentiality: All information generated during the use of medical devices is only disclosed to those who are authorized to see it.
3) Availability: All medical devices are accessible by the supervisor, caregivers and patients as needed
4) Authentication: All devices involved know who they are interacting with.
5) Physical/Administrative Security: All medical devices and associated equipment used by caregivers and others should be protected from tampering.

VI. Conclusion

Security for medical devices has gained some traction in recent years following some well-publicized attacks on individual devices. Solutions have been proposed for securing these devices but only in stand-alone mode. The introduction of interoperability makes medical devices to be increasingly connected and dependent on each other. It needs to be noted that security can only be talked about in the abstract, absent of a concrete design; solving the problem will need all stakeholders to find a meaningful path forward together.

Manufacturers need to start scheming security into their devices at all stages. Hospitals must do an enhanced job of understanding risks and captivating a risk management-based approach to extenuating device vulnerabilities.

REFERENCES

[1] Reinhold Haux, Medical informatics: Past, present, future, International Journal of medical informatics, pp. 599–610, 2010.
[2] Chemlal S., Colberg S., Satin-Smith M., Gyuricsko E., Hubbard T., Scerbo M. W., McKenzie F.D. Blood glucose individualized prediction for type 2 diabetes using iPhone application., IEEE 37th Bioengineering Conference (NEBEC), 2011.
[3] Silva, B., Lopes, I., Rodrigues, J., Ray, P.: Sapo Fitness: A Mobile Health Application for Dietary Evaluation, IEEE 13th International Conference on e-Health Networking, Applications and Services, 2011.
[4] Paschou, M., Sakkopoulos, E., Tsakalidis, A. easy HealthApps: e-HealthApps Dynamic Generation for Smartphones & Tablets, Journal of Medical Systems, Vol. 37, Issue: 3, 2012.
[5] Klug S., Krupka K., Dickhaus H., Katus H. A., Hilbel T., Displaying computerized ECG recordings and vital signs on Windows Phone 7smartphones, Computing in Cardiology, pp. 1067-1070, 2010.
[6] Karan, A., Bayraktar, C., Gümüskaya, H., Karlık, B, Diagnosing diabetes using neural networks on small mobile devices, Journal on Expert Systems with Applications, pp. 54–60, 2012.
[7] Boulos, M., Wheeler, S., Tavares, C. and Jones, R., How Smart phones are changing the face of mobile and participatory healthcare: an overview, with example from eCAALYX, BioMedical Engineering OnLine Journal, pp.10:24, 2011.
[8] http://www.bizjournals.com/nashville/blog/2016/04/why-this-health-tech-group-picked-nashville-not.html.<accessed on 6th Jan 2017>.
[9] http://medicalinteroperability.org/the-patient-safety-movementannounced-49-medical-technology<accessed on 16th Dec 2016>.
[10] T. Choen. Medical and information technologies convergence. IEEE Eng. Med. Biol. Magazine, vol.23, Issue: 3, pp: 59-64, May 2004.
[11] S. L. Grimes. Security: A new clinical engineering paradigm. IEEE Eng. Med. Biol. Magazine, vol.23, Issue: 4, pp: 80-82, August 2004.
[12] N. L. Snee and K. A. McCormick. The case for integrating public health informatics networks, IEEE Eng. Med. Biol. Mag, Vol. 23, Issue:1, pp:81-88,February 2004.
[13] M. Clarke, D. Bogia, K. Hassing, L. Steubesand, T. Chan, and D. Ayyagari. Developing a standard for personal health devices based on 11073. In EMBS, 2007.
[14] K. Venkatasubramanian, E. Vasserman, O. Sokolsky, and I. Lee. Security and interoperable-medical-device systems, part 1. IEEE Security & Privacy, Vol.10, Issue:5, pp: 61-63, 2012.
[15] A. Mashkoor, J. Sametinger, Rigorous modeling and analysis of interoperable medical devices, in: Proceedings of the International Spring Simulation Multi-Conference, Society for Modeling & Simulation, pp. 800–807, 2016.
[16] R. Taylor, K. Venkatasubramanian, Craig A. Shue, Understanding the security of interoperable medical devices, in: Proceedings of the 3rd International Conference on high confidence networked systems, pp.31-40, 2014.

Open Science Index, Biomedical and Biological Engineering Vol:11, No:5, 2017 publications.waset.org/10007170/pdf