A Cybersecurity Vulnerability Management System for Medical Devices

S.D.S. Sappal[1] and P.D.H. Prowse[2]
[1]University of Manitoba, Computer Engineering, Winnipeg, MB, Canada
[2]Clinical Engineering, Health Sciences Centre, Winnipeg Regional Health Authority, Winnipeg, MB, Canada

I. Introduction

Interconnectivity of medical devices on a converged network with other Information and Communications Technologies (ICT) is the reality of hospitals today. While interconnectivity can enable new models of care [1], reduce medical errors [2], and improve patient care [3], such connectivity exposes high-criticality medical equipment to threats that may affect data confidentiality, system availability, and/or information integrity [4]. As technical advancements continue in medical equipment, the risk of cybersecurity increases as well. A recent study of German hospitals found a correlation between the degree of medical device connectivity and the likelihood of being attacked [5]. To understand, control and minimize risk, a cybersecurity management vulnerability system needs to be established involving vulnerability tracking, resolution, and lifecycle planning.

Proper cybersecurity management requires both scheduled and unscheduled work. For many applications and operating systems, scheduled patching is a monthly task, and unscheduled work occurs when there is a need to apply a high risk out-of-band patch or when a device has been compromised by malware and requires remediation. This work is not significantly different than the typical electromechanical Preventive Maintenance (PM) and Corrective Maintenance (CM) work that Healthcare Technology Management (HTM) departments perform today and can be treated similarly with appropriate documentation and scheduling. Currently the PM program in place at the Winnipeg Regional Health Authority (WRHA) ensures that medical devices are regularly assessed for accuracy and hidden failures that could pose a risk to patient care. The proposed cybersecurity vulnerability management system aims to emulate the existing practices of the CM and PM practices by leveraging existing processes and resources to respond to the challenges of managing cybersecurity vulnerabilities.

As we learn to address the risks of cybersecurity within medical devices, we must acknowledge that the clinical usability typically outlasts cybersecurity supportability. To address this challenge, we provide recommendations for lifecycle management of connected medical devices.

II. Modifying Computerized Maintenance Management System Tables

The current practices and documentation tracking for the PM program are built in the Computerized Maintenance Management System (CMMS) used in the WRHA. Inspections are scheduled, prioritized using risk-based metrics, and documented in a single system for improved efficiency and reporting. The WRHA's existing CMMS required modification to effectively prioritize or track cybersecurity vulnerabilities and associate them with affected devices. As this CMMS is essentially homegrown with an in-house development team, we had the flexibility to modify the system to meet our needs.

Cybersecurity vulnerabilities distributed by our vendors often contain a list of devices that are affected by the vulnerability. If the vendors do not provide a device list for vulnerabilities or if the vulnerability is for third-party software used by medical device manufacturers, we must have a mechanism to easily identify those affected devices and associate them to the vulnerability. The proposed modifications were to update the CMMS to include additional tables which incorporate fields for network information and device's specification. As shown in Fig 1, the device can be associated with the corresponding vulnerability through device specification and network information.

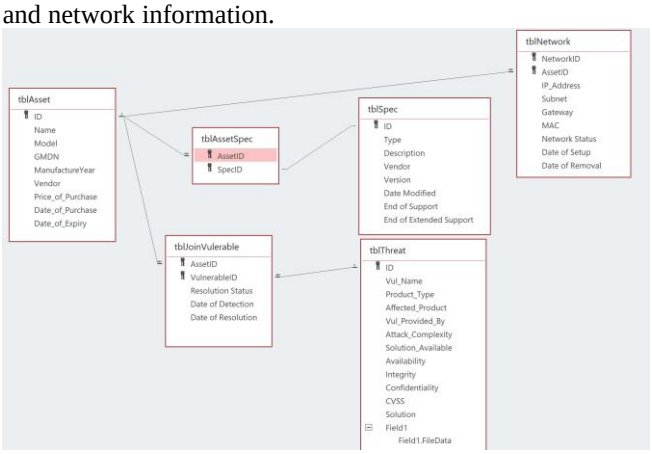

Fig 1: Database Table Relationship

The Network Table (Fig. 2) captures device's network type, network status, IP address, Subnet, Gateway, Media Access Control (MAC), date of setup and removal. The network status helps in assessing the risk to the devices. For example, if the device is on an isolated network or an inactive network, then the vulnerability poses less of a threat to the device.

NetworkID	AssetID	NetworkType	IP_Address	Subnet	Gateway	MAC	Network Status	Date of Setup	Date of Removal
1	5	Static	192.168.1.11	11.11	111.111	11.11.11	General Purpose	2013-06-01	2023-06-01
4	4	Static	192.168.1.44	44.44	444.444	44.44.44	General Purpose	2015-10-07	2025-10-07
8	5	Static	192.23.455.6				Inactive	2020-10-06	2020-10-15
9	1	Static	192.134.45				General Purpose	2020-05-12	2020-10-14
10	1	Static	121.31.32				General Purpose	2020-09-02	2020-10-08
11	7	Static	192.168.1.77	77.77	777.777.777	77.77.77	General Purpose	2020-07-12	
12	9	Static	192.113.133.9	99.99		99.99.99	Inactive	2020-12-01	2020-12-10
13	9	Static	123.323.23.1	99.99		99.99.99	Isolated	2020-12-15	
14	8	Static	198.322.12				General Purpose	2020-12-03	
15	8	Dynamic					Isolated	2020-12-15	
16	2	Dynamic					General Purpose	2020-12-15	

Fig 2: Network Table example

The Specifications Table (Fig. 3) is used to capture information about the device's operating system (OS), software (SW), hardware (HW), firmware (FW) and their end of support dates. When assigned to medical devices in the CMMS, this information helps to identify assets that contain known vulnerabilities present in third-party components (such as an embedded operating system).

tblSpec

ID	Type	Description	Vendor	Version	Date Modified	End of Support	End of Extended Support
1	Hardware	LCD Screen			2020-08-01		
2	Firmware	HP-100-2			2020-08-10		
3	Hardware	OLED Display			2020-10-01		
4	Hardware	HDMI Cord			2020-10-12		
5	Hardware	External 100 GB Harddrive			2020-10-07		
6	Hardware	100 GB HDD			2020-10-07		
9	Other						
10	Hardware	160 GB HDD		V1.2	2020-10-11		
11	Operating System	Windows	Microsoft	7	2020-11-18	2015-01-13	2020-01-14
12	Operating System	Windows	Microsoft	7 Enterprise	2020-11-18	2015-01-13	2020-01-14
14	Operating System	Windows	Microsoft	7 Ultimate	2020-11-18	2015-01-13	2020-01-14
15	Operating System	Windows	Microsoft	Server 2008 R2	2020-11-18	2015-01-15	2020-01-14
16	Operating System	Windows	Microsoft	XP SP2	2020-11-18	2009-04-14	2014-04-08
17	Operating System	Windows	Microsoft	XP Professional for Emt	2020-11-18	2009-04-14	2014-04-08
18	Operating System	Windows	Microsoft	Vista SP1	2020-11-18	2011-07-12	2011-07-12
19	Operating System	Windows	Microsoft	Embedded Standard 20	2020-11-27	2014-01-14	2019-01-08
20	Operating System	Real Time Operating System	Wind River	VxWorks	2020-11-27	2019-03-07	
21	Operating System	Real Time Operating System	ENEA	Operating System Emb	2020-11-27		
22	Operating System	Real Time Operating System	Green Hills	INTEGRITY	2020-11-27		
23	Operating System	Real Time Operating System	Microsoft	ThreadX	2020-11-27		
24	Operating System	Real Time Operating System	Tron Forum	ITRON	2020-11-27		
25	Operating System	Real Time Operating System	IP Infusion	ZebOS	2020-11-27		

Fig 3: Specifications Table

III. Vulnerability Evaluation And Resolution

The risk of each vulnerability will vary based on the device types that it affects, the patients that use the device, the environment in which it is used, and any pre-existing controls put in place to protect the device from exploitation. Before remediation of a vulnerability is implemented, a risk assessment of the likelihood and severity for that vulnerability should be performed.

The scoring mechanism for medical device vulnerabilities uses a weighted average of multiple factors which include Equipment Function, Location of Use, Operating System Support Status, FDA's Medical Device Common Vulnerability Scoring System (CVSS) [6], and Failure Consequence. Table 1 provides a list of these factors along with their individual options. The relative weights of these factors were established through the analytical hierarchy process.

The base score attribute has been taken from the Medical Device (CVSS) [6].

Table 1: Specifications Table

Criteria	Weight	Options	Assigned Score
Equipment Function (EF)	**6.7%**	Misc. patient related	1
		Ancillary	2
		Core	6
		Life Support	9
Location of Use (LO)	**5.3%**	Outpatient areas - i.e., doctor's office	1
		General Care Areas - i.e., inpatient units	3
		Wet locations/labs/exams areas - i.e., X-Ray room	5
		Critical care Areas - i.e., ICUs	7
		Anesthetizing locations - ORs	9
Operating System	**26.4%**	Supported	1
		Unsupported	9
Base Score	**43.8%**	None	0
		Low	2
		Medium	4
		High	7
		Critical	9
Failure Consequences (FC)	**17.2%**	No significant consequence	1
		Inappropriate therapy/ misdiagnosis	2
		Could cause patient/clinician injury	4
		Probable cause patient/clinician injury	6
		Potential patient death	9

Following the risk assessment, each vulnerability for each affected asset can be assigned a priority for resolution. Within the WRHA, we will leverage the CMMS to assign the work and report on its completion. If a vulnerability cannot be resolved, we now have a tracking system and risk scoring system to communicate to management. A governance process shall be implemented to escalate unresolved vulnerabilities to our vendors and the internal ICT security team to discuss alternative mitigation strategies (such as network segmentation or removal of network connectivity) and the risk of not installing patches. As examples, patches may not yet be installed because of delays in validation by the vendor, the equipment may be beyond end-of-support, or due to internal delays resulting from other departmental priorities or an inability for the device to be made available by clinicians. After the vulnerability has been addressed following the proposed method, any important information is noted on the vulnerability associated with that asset and can be updated as necessary in the future if the connectivity or use of that device changes.

IV. Lifecycle Palnning for Connected Medical Devices

The clinical utility of medical devices well outlasts the cybersecurity supportability of the underlying HW/SW/FW/OS on which many devices are built. Accordingly, we must now consider the need to plan for system upgrades throughout the lifespan of a device to ensure that it can be kept secure within the network. Where devices cannot be upgraded and patched, but still have clinical utility, there is a responsibility for the health organization to manage the risk of that legacy device. This may be by removing network connectivity, or by restricting the communication of that device to protect it from potential malware on the network and to protect the rest of the network from any potential malware on that device. Unresolved security vulnerabilities resulting in organizational risk should influence equipment replacement decisions as other support factors and device history.

Although we have not incorporated unresolved vulnerabilities in the WRHA equipment prioritization system today, there are plans to consider this as a contributing factor in future iterations of the system. However, there is a need to consider how this will affect funding requirements for connected medical equipment going forward. For many organizations, medical equipment replacements and upgrades are a capital expense and need to be planned for months to years in advance. Regular upgrades to medical equipment to address cybersecurity and supportability challenges are becoming an operational cost and therefore may need to be funded differently.

v. Conclusions

An effective cybersecurity management program relies on consistent and complete patching of cybersecurity vulnerabilities in an expedited manner. We have presented a process to establish a vulnerability tracking, scoring, and reporting system that aligns with pre-existing processes for preventive and corrective maintenance to simplify the workflow for staff.

The proposed system introduces a risk-based scoring system to provide management with visibility into the cybersecurity risk posture of the organization due to the connected medical devices in the environment. Finally, the implementation of a governance structure to make decisions on how to address unresolved vulnerabilities will make healthcare safer for patients.

Acknowledgements

The authors would like to thank the members of the Networking and Integration Committee for their feedback on the proposed database structure and patching processes as well as all those who provided a demonstration of the patching protocol used for specific device types.

Conflict of Interest

The authors of this paper declare that they have no actual or perceived conflict of interest.

References

[1] A. King, D. Arney, I. Lee, S. Oleg, J. Hatcliff and S. Procter, "Prototyping closed loop physiologic control with the medical device coordination framework," in *Proceedings of the 2010 ICSE Workshop on Software Engineering in Health Care*, Cape Town, South Africa, 2010.

[2] A. Agrawal, "Medication errors: prevention using information technology systems," *British Journal of Clinical Pharmacology*, vol. 67, no. 6, pp. 681-686, 2009.

[3] P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem," *Medical Devices (Aukland, N.Z.)*, vol. 8, pp. 305-16, 2015.

[4] M. Anandarajan and S. Malik, "Protecting the Internet of medical things: A situational crime-prevention approach," *Cogent Medicine*, no. 5, pp. 1-23, 2018.

[5] M. Willing, C. Dresen, U. Haverkamp and S. Schinzel, "Analyzing medical device connectivity and its effect on cyber security in german hospitals," *BMC Medical Informatics and Decision Making*, vol. 20, p. 246, 2020.

[6] M. P. Chase and S. M. C. Coley, "Rubric for Applying CVSS to Medical Devices," The MITRE Corporation, 2020.