Poster Abstract: Analysis of Cyber-Security Vulnerabilities of Interconnected Medical Devices

Yanchen Xu[†], Daniel Tran[*], Yuan Tian [*], Homa Alemzadeh[†]
[*]Computer Science, [†]Electrical and Computer Engineering, University of Virginia, Charlottesville, VA, USA
Email: {yx4kp, dlt2hc, yt2e, ha4d}@virginia.edu

***Abstract*—With advances in sensing, networking, and computing, smart medical devices have been widely deployed in various clinical settings. However, cyber attacks on hospital networks and critical medical devices are serious threats to patient safety, security, and privacy. This paper studies the cyber-security attacks that target hospital networks and other interconnected clinical environments. Our goal is to characterize threat models in such environments by studying the public data from vulnerability databases on medical devices and reports on real attacks targeted at hospital networks. We use a keyword-based approach to identify security reports on medical devices. We summarize our observations from the analysis of the vulnerability reports and provide insights into the types and impacts of vulnerabilities.**

***Index Terms*—security, vulnerability, medical device, hospital**

I. Introduction

Attacks on hospital networks and critical medical devices threaten patient safety and privacy [1]. Past studies reported different vulnerabilities and attacks that compromise the communication channels in medical devices such as implantable cardiac defibrillators [2], wearable insulin pumps [3], and teleoperated surgical robots [4]. However, studies on security of interconnected medical devices in hospital networks mainly consist of new attacks and vulnerabilities reported by the security researchers and consulting companies. These reports have indicated existence of vulnerabilities in the configuration of hospital networks [5], [6], third-party networks (e.g., laboratories, pharmacies) [7], devices used by the healthcare professionals and technicians [8], and unpatched medical devices [9], that may allow attackers to penetrate hospital networks and gain unauthorized access to the critical interconnected medical devices. Once in the hospital network, they can move laterally across devices within the hospital, steal credentials, exploit vulnerable services, and discover additional vulnerable and unhatched devices until a target system is located and penetrated. The discovered attacks on a blood gas analyzer device to establish a backdoor to the hospital network and steal patient records [9] and the vulnerabilities in an internal firewall that enabled unauthorized access to a surgical robot [6] serve as examples of such vulnerabilities and penetration attacks. However, most of these security issues are reported in an ad-hoc manner. There is no systematic understanding of the attack landscape to medical devices. To systematically investigate the security and privacy challenges in integrated clinical environments, we propose a data-driven approach for characterizing vulnerable devices that are the targets of cyber attacks. This paper presents our preliminary results on the analysis of the publicly-available vulnerabilities reported on the interconnected medical devices used in hospitals.

II. Analysis Methodology

We analyze two publicly-available vulnerability databases CVE [10] and ICS-CERT [11] to identify common threats and security attacks targeting medical devices. We leverage Natural Language Processing (NLP) techniques to extract relevant information from the vulnerability databases to identify the characteristics of attacks and types of vulnerable devices in hospital networks. This task is not trivial because of the diversity and complexity of the medical devices and a large number of vulnerabilities reported to different databases. For example, to extract all security, privacy, and safety-relevant information from the databases we need to automatically learn the relevant keywords and concepts related to security threats and medical devices.

ICS-CERT Alerts dataset [11] is developed and maintained by Industrial Control Systems Cyber Emergency Response Team and the United States Computer Emergency Readiness Team (US-CERT). US-CERT is responsible for analyzing and reducing cyber threats, vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. In order to collect information on the medical device-related vulnerabilities from ICS-CERT, we developed a tool for crawling the whole US-CERT website. This tool extracted all vulnerability records reported from 1999 to 2018, which contain any medical-related keywords. We then manually parsed the HTML documents of these records and extracted information such as the corresponding CVE IDs, affected product names, manufacturer or vendor names of products, as well as vulnerability details and backgrounds. Our dictionary of medical-related keywords were developed by including generic medical keywords as well as those describing the common categories and specialties of medical devices, as classified by the FDA Product Code Classification Database [12]. Example keywords from our dictionary included: “medical, “hospital, “health, “healthcare, “lifecare, “clinic, “clinical, “patient, “doctor, “surgery, “blood, “immunology, “orthopedic, “pathology, “dental, “medicine, “toxicology, “obstetrics, “urology, “gastroenterology, “neurology, “hematology, “anesthesiology, and “cardio. By manual review of the extracted records, we further removed the duplicate records and those describing updates on existing records. This analysis led us to a total number of 140 ICS-CERT records related to the vulnerable

devices used in hospital networks. We then manually analyzed these records to characterize the vulnerabilities and devices.

III. Analysis Results

The following are our main observations from the analysis of medical device vulnerabilities in the ICS-CERT database:

Frequencies and Types of Vulnerabilities. During the period of 1999-2018 over 110,500 vulnerabilities were reported to the CVE database. Only 354 (0.3%) of these CVEs were reported to affect interconnected medical devices in hospitals. Figure 1 shows the total number of medical device related vulnerabilities reported to the database for 1999-2018.

We see a steady increase in the number of reported vulnerabilities, 2.5 times since 2013, reaching 38 ICS-CERT and 91 CVE records related to medical devices. This is consistent with the increase in the overall number of vulnerabilities reported to the CVE database (3 times increase since 2013, reaching 16,555 in 2018). In total, we found 119 unique types of vulnerabilities (CVEs) reported for medical devices. Table I shows the most common categories of vulnerabilities. Some examples of the most frequent types of vulnerabilities included improper credential management and authentication (8%), improper access control, privilege management, and authorization (6%), and buffer and stack overflows (6%).

Vulnerable Medical Devices. The reported vulnerabilities affected a wide range of medical devices in different medical specialties by 56 different manufacturing companies. Almost 53% of the vulnerabilities were reported for devices made by 5 device manufacturers. This means that if design and validation practices used by those manufacturers were improved, almost half of the vulnerabilities could be fixed.

We also found that for 18 (12.8%) of vulnerabilities, exploits were publicly available, potentially enabling attackers to target the devices and affect patient safety and privacy. These vulnerabilities existed in different types of medical devices from various manufacturers, including imaging systems (e.g., CT scanners, cardiology imaging), hospital/clinical communication technology (for storage and communication of patient health information), insulin pump or infusion pump systems,

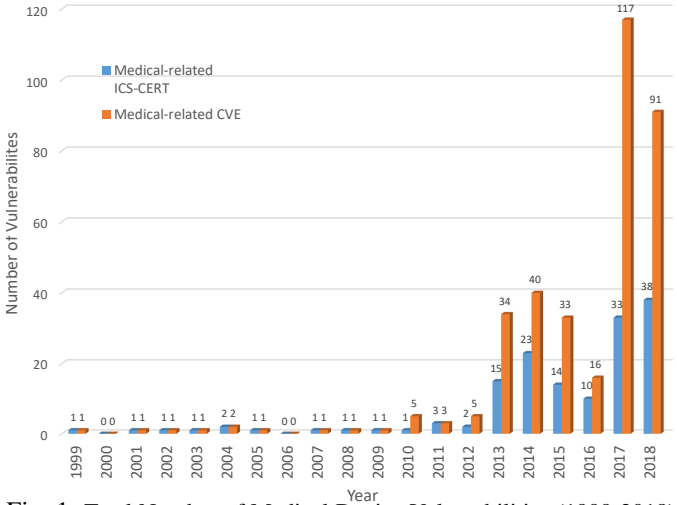

Fig. 1: Total Number of Medical Device Vulnerabilities (1999-2018)

TABLE I: Top Medical Device Vulnerabilities (1999-2018)

Vulnerability Type	Freq.
Improper credential management and authentication	36
Improper access control, privilege management, and authorization	30
Stack and Buffer Overflow	29
Path traversal	14
Improper input validation	13
Information exposure	12
Cross-site Request Forgery	9
Cross-site Scripting	8
Uncontrolled resource consumption	5
Missing encryption of sensitive data	5

data and management software, network security software, remote connectivity software, and communication devices.

IV. Future Work

Future work will focus on further analysis of medical device security issues by including data from a wider range of publicly-available databases and cross-referencing the events across the databases to gather more in-depth insights into the characteristics of vulnerabilities and attacks and developing techniques for attack prevention and detection.

Acknowledgment

This work was partially supported by a grant from the National Science Foundation (1748737) and a SEAS research innovation award from the University of Virginia.

References

[1] H. Almohri, L. Cheng *et al.*, "On threat modeling and mitigation of medical cyber-physical systems," in *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*. IEEE, 2017, pp. 114–119.

[2] D. Halperin, T. S. Heydt-Benjamin *et al.*, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *2008 IEEE Symposium on Security and Privacy (sp 2008)*. IEEE, 2008, pp. 129–142.

[3] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *2011 IEEE 13th International Conference on e-Health Networking, Applications and Services*. IEEE, 2011, pp. 150–156.

[4] T. Bonaci, J. Yan *et al.*, "Experimental analysis of denial-of-service attacks on teleoperated robotic systems," in *Proceedings of the ACM/IEEE Sixth International Conference on Cyber-Physical Systems*. ACM, 2015, pp. 11–20.

[5] Wired Magazine, K. Zetter, "Hospital Networks Are Leaking Data, Leaving Critical Devices Vulnerable," http://www.wired.com/2014/06/hospital-networks-leaking-data/, 2014.

[6] ——, "Its Insanely Easy to Hack Hospital Equipment," http://www.wired.com/2014/04/hospital-equipment-vulnerable/, 2014.

[7] Business Wire, F. Wayne, "Nomoreclipboard Notice To Individuals Of A Data Security Compromise," http://www.businesswire.com/news/home/20150610005964/en/NoMoreClipboard-Notice-Individuals-Data-Security-Compromise, 2015.

[8] B. Filkins, "SANS-Norse Health Care Cyberthreat Report," "https://www.sans.org/reading-room/whitepapers/analyst/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735", 2014.

[9] TrapX Labs - A Division of TrapX Security, Inc., "Anatomy of an Attack MEDJACK," http://deceive.trapx.com/AOAMEDJACK_210_Landing_Page.html, 2015.

[10] "Common Vulnerabilities and Exposures Database," https://cve.mitre.org/.

[11] US-CERT, "Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Alerts," https://ics-cert.us-cert.gov/alerts.

[12] U.S. Food Drug Administration (FDA), "Product Code Classification Database," https://www.fda.gov/medical-devices/classify-your-medical-device/product-code-classification-database.