Clinical Cybersecurity Training Through Novel High Fidelity Simulations

Christian Dameff(1), Jordan Selzer(2), Jonathan Fisher(2), James Killeen(1), Jeffrey Tully(3)

University of California San Diego(1), Maricopa Medical Center(2), UC Davis Medical Center(3)

Abstract

Background: Cybersecurity risks in healthcare systems have traditionally been measured in data breaches of protected health information but compromised medical devices and critical medical infrastructure raises questions about the risks of disrupted patient care. The increasing prevalence of these connected medical devices and systems implies that these risks are growing.

Objective: This paper details the development and execution of three novel high fidelity clinical simulations designed to teach clinicians to recognize, treat, and prevent patient harm from vulnerable medical devices.

Methods: Clinical simulations were developed which incorporated patient care scenarios with hacked medical devices based on previously researched security vulnerabilities.

Results: Clinician participants universally failed to recognize the etiology of their patient's pathology as being the result of a compromised device.

Conclusions: Simulation can be a useful tool in educating clinicians in this new, critically important patient safety space.

Introduction

The increasing development of and reliance on technical systems is an inescapable reality for humanity. Inherent cyber vulnerabilities in these systems are ubiquitous spanning all sectors of the global economy. From damaging breaches of private consumer data such as the Equifax hack that exposed half of the US population to the threat of identity theft[1], to active cyber warfare between nation states[2], the potential for harm caused by the exploitation of such vulnerable systems is profound.

Healthcare is perhaps one of the most vulnerable sectors to such cyber threats, as healthcare delivery organizations, hospitals, and clinics store both vast amounts of personal data and care for patients through networked, highly complex technological systems[3]. Furthermore, when compared to sectors such as finance and government, healthcare lags significantly behind in cyber preparedness[4]. Federal laws such as the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) have attempted to provide a regulatory framework and improve healthcare cybersecurity but lack adequate patient safety protections and hyperfocus on the security of protected health information (PHI). The Affordable Care Act also provided incentives and penalties to hasten healthcare's adoption of electronic health records, system interoperability, and health data sharing without provisions for adequate cybersecurity advancement[5].

Recent events have demonstrated that patient care may be affected when vulnerable medical technology is compromised by computer viruses designed and distributed to disrupt the normal functioning of systems. Ransomware, a class of viruses which encrypt data, rendering it inaccessible until monetary compensation is provided to the viruses' propagator, have struck hospitals around the world in several notable incidents, including the "WannaCry" attack which resulted in the temporary closure of several dozen of Britain's National Health Service hospitals[6].

Researchers who study the security of medical devices are concerned that these technologies may be equally susceptible to attacks from malicious hackers. Reports have focused on vulnerabilities in devices ranging from percutaneous insulin pumps to automated internal cardioverter-defibrillators, though to our knowledge there have not been any cases described in the medical literature of individual patients affected by a compromised medical device.

This is not to say that the specter of such attacks have not altered how patients receive care. A recent safety advisory delivered by the Food and Drug Administration (FDA) concerning possible vulnerabilities in the pacemaker systems of a large vendor affected nearly half a million patients who in the near future may require additional doctor visits, software upgrades, and possibly even procedural intervention- all contingencies potentially damaging patient trust in the medical technologies they rely on[7]. Despite the dramatic impact such events may have on clinical practice and patient care, to our knowledge, there are no widespread or highly adopted educational techniques for raising awareness of these concerns and for training medical providers to identify and manage a medical cybersecurity crisis in the clinical realm.

Simulation is a powerful modality for training medical professionals to improve team-based communication skills, manage uncommon or high-stakes clinical situations, practice procedural techniques, and refine medical decision making skills in a safe environment that allows for the learner to benefit from both self-reflection and constructive feedback[8]. The evolution of simulation in medical education has included both the development of high fidelity, in-situ clinical simulations and multidisciplinary scenarios that allow the healthcare team to practice working together to decrease adverse events and improve patient care outcomes[9,10]. Simulation is now implemented at a majority of medical centers and academic institutions[11] and has gained the support of professional organizations[12], payors, and government[13]. Simulation may offer a impactful way to incorporate cybersecurity concerns within medical training.

We developed novel high fidelity clinical simulations featuring patients presenting with pathology secondary to "hacked" medical devices, utilizing previously reported research detailing security vulnerabilities in commonly used devices.

Methods

Building the simulations

We compiled national media reports, social media posts, recordings of national security conference presentations, and conducted interviews with medical device security researchers in order to identify specific medical devices with known vulnerabilities where, if compromised, would likely result in patient harm. After reviewing the literature three device classes were identified: bedside infusion pumps, automated internal cardioverter-defibrillators, and insulin pumps. Each of these selected device classes have been shown to be vulnerable to cyber attack. Device classes were chosen based on the quality of security research, potential harm to patients if compromised, and technical features of the device allowing for feasible exploitation.

Common presentations of emergent conditions were combined with the above identified medical device vulnerabilities to produce scenarios. In each case the cause of the emergent condition is either a result of or worsened by the compromised medical device itself. Each scenario was reviewed by the physician authors and crafted to as clinically accurate as possible.

Scenario 1

A 60 year old male with a past medical history of myocardial infarction 5 years ago, and hypertension presents with chest pain. He will be found to be stable in atrial fibrillation with rapid ventricular response. His EKG is not concerning for acute ischemia. He will receive one bolus of either a calcium channel or beta blocker for rate control. Several minutes after being started on a continuous infusion of the rate control agent the patient will develop bradycardia and proceed into pulseless electrical activity arrest (PEA). This PEA arrest will be the result of the bedside infusion pump being hacked to deliver the entire multiple hour infusion into a three minute bolus resulting in either a calcium channel or beta blocker overdose. The combination administration of high quality CPR, fluids, vasopressors, high dose insulin euglycemic therapy, calcium and intralipid depending on the overdose agent, will resuscitate and stabilize the patient.

This scenario was modeled after the 2015 research of Billy Rios, wherein a Hospira bedside wireless infusion pump was found to have significant vulnerabilities involving arbitrary raising or lowering of acceptable dose ranges in digital drug libraries stored on the devices[14]. An attacker could alter these libraries wirelessly and change the drug infusion rate of a particular drug resulting in either an overdose or inadequate medication dosing. This type of vulnerability was also found in Medfusion devices in 2017[15].

Scenario 2

An adolescent male will be brought unresponsive with a Glasgow Coma Score of 11 to the emergency department by EMS on a backboard with cervical spine collar following a high-speed motor vehicle collision. The patient will have multiple injuries including a large bleeding scalp laceration and an open right femur fracture. Trauma workup will yield no additional significant injuries but will show hypoglycemia with a blood glucose of 22. The patient will then transition into status epilepticus refractory to standard benzodiazepine and barbiturate therapy. Treatment with glucose will terminate his seizure, improve his mental status and transiently elevate his glucose levels, however the patient will become repeatedly hypoglycemic despite aggressive glucose therapy. During the case participants will need to discover an insulin pump on the patient’s backside and will need to recognize that the insulin pump has administered lethal

overdoses of long acting insulin. Participants will have to stabilize the patient as well as treat his hypoglycemia using continuous glucose infusion with a central line in the setting of polytrauma.

This scenario was modeled after the 2012 personal subcutaneous electronic insulin pump research of Jay Radcliffe[16]. Insecure wireless communication protocols that were not encrypted or authorized could be sent to these devices causing potentially lethal overdose of their insulin reservoirs. Multiple models have been discovered to have similar vulnerabilities including Medtronic and Animas devices.

Scenario 3

An elderly male with history of third degree heart block and an implanted automatic implantable cardiac defibrillator (AICD) presents to the emergency department conscious and complaining of intermittent repetitive shock-like pain every 60 seconds over his precordium originally beginning thirty minutes before. On exam he will be found to be in distress with frequent spasms associated with repeated cardiac defibrillation shocks despite no evidence of cardiac arrest. The EKG shows a paced rhythm with no significant abnormalities. During an assessment the patient will spasm and become unconscious. The cardiac monitor will show ventricular fibrillation and the patient will need to be resuscitated. The patient will recover with either the intrinsic defibrillator of the AICD or an external shock. The patient will then regain consciousness however an additional internal shock will cause repeated cardiac arrest due to the unfortunate timing of the defibrillation during the repolarization phase of the cardiac cycle, a phenomenon known as R on T. An external control magnet will not cease the shocks. The physician will need to recognize the failure of traditional treatments for runaway pacemaker and cut the defibrillator leads from the device to the heart in the patient's chest through an anterior chest wall incision. This will cease shocks however the patient will become unstable requiring external transcutaneous pacing to sustain his blood pressure as a result of his underlying third degree heart block. The patient, once stabilized, will need to be admitted to the cardiac ICU.

This scenario was modeled after the 2012 efforts of Barnaby Jack[17] and further 2017 work of Billy Rios regarding the vulnerabilities of automatic implantable cardiac defibrillators. Failure of several of these devices to wirelessly authenticate before reprogramming was demonstrated to result in the delivery of a defibrillation shock regardless of the underlying rhythm, posing life-threatening harm.

Executing the simulations

These simulations were performed in a modern clinical simulation center at the University of Arizona College of Medicine Phoenix during the CyberMed Summit, a novel multidisciplinary conference focusing on patient safety and cybersecurity. A room built to resemble a well equipped emergency department with mock medications, vital signs, ultrasound, and most procedural capabilities was utilized. Adjacent to the room was a wall with one way glass. Staff and observers of the simulation were able to watch the scenarios in real time on the other side of the glass.

Teams were comprised of one emergency medicine physician (physician), medical students, simulation trained nurses, paramedics, and experienced patient actors (patient) trained in medical education and simulation . Each team member, with the exception of the physician, reviewed the details of the scenario and were aware of the hacked medical device. A simulation trained physician (lead) led the scenarios progression behind one way glass, augmenting vital signs and the progression of the case as the scenario unfolded.

Each simulation began with the patient actor arriving to the room via emergency medical services. Paramedics provided pre-hospital patient history and transferred the patient. The physician was then allowed to assess the patient, order tests and medications, and perform any available procedure just as they would in the clinical setting. Test results and radiology images were available to the physician to review.

As the scenarios advanced each patient would decompensate into cardiac arrest or seizure due to the adverse effects of a hacked medical device. At the time of the deterioration the scenario was briefly suspended while the patient actor was replaced with a high fidelity simulation mannequin to facilitate the delivery of realistic chest compression and resuscitation efforts. Once clinically appropriate antidotes were given or procedures were performed the patients stabilized, and after specialist consultation simulated transfers to the intensive care unit occurred. Immediately after each simulation the physician participated in a structured debrief where questions around the events of the simulation including the causative hacked medical device were asked.

Results

Recordings of the simulations were produced with subsequent review of real-time actions and post-exercise debriefings allowing for further analysis of participant decision making. Physicians in all three exercises ultimately progressed to the definitive treatments for the individual scenario by correctly identifying important natural history elements, physical exam findings, or laboratory or imaging results. Despite this success, participants failed to identify the underlying compromised medical device as being a possible source for the patient's presentation in each of the three scenarios.

Debriefing sessions yielded further confirmation of this fact. "Assessment of the technology we use is not even on my radar," one physician stated. "We expect these things to work and work reliably 100% of the time," replied another. All three participants were not only unaware of the prior vulnerabilities publicly disclosed with regards to the devices featured in their scenarios, but to the concept of compromised devices as being a source of patient harm in general.

Discussion

While medical students, residents, and practicing physicians receive extensive training in the application of technologies to patient care, clinicians are largely not educated in technical considerations of such tools, or are up-to-date on when devices are reported to have security vulnerabilities rendering them susceptible to malicious attack.

We developed novel high fidelity simulations depicting patients suffering from disruption in normal physiology secondary to “hacked” medical devices, based on foundational laboratory findings from security researchers demonstrating vulnerabilities in commercially available products, with extrapolation limited to physiologic assumptions of what may happen when such vulnerabilities were abused.

Standardized patients trained to present with complaints and symptoms together with high fidelity mannequins were used to produce a full patient encounter from presentation in a simulated emergency department through treatment course and subsequent triage.

As expert learners, our participants were able to take mastered skills and apply them to these novel presentations to navigate and treat the patient’s physiology but crucially, were also all unable to recognize the underlying presentation as being due to a compromised medical device. “I never realized that something like this was possible,” replied the physician managing the compromised infusion pump scenario when questioned as to whether device hack was on their differential diagnosis. “I would have gone into the next room and grabbed the same pump for the next patient”- a natural response which fails to grasp the concept that if one particular unit of a given product line is compromised, the remaining units with the same vulnerabilities are similarly compromised until proven otherwise.

Our goal in developing these simulations was less to prepare clinicians for the distinct situations of infusion pump, subcutaneous insulin delivery system, or automated internal cardioverter defibrillator failure and more to engender in our participants an awareness that the implicit trust currently awarded to medical infrastructure and devices may need to be replaced by a sense of vigilance and a willingness to consider device compromise as an explanation for catastrophic failures.

Further work is warranted to educate clinicians about the possible threats to patient safety posed by compromised medical devices, and similar simulation exercises for common medical “cyber-crises” deserve consideration for a place alongside other simulated high-stakes scenarios during medical training. A study to evaluate a medical cybersecurity curriculum for resident physicians utilizing these and other simulation scenarios is currently underway.

Acknowledgements
The authors wish to thank the University of Arizona College of Medicine - Phoenix for institutional support, particularly the assistance rendered by the Center for Simulation and Innovation as host for these simulation exercises.

Conflicts of Interest
None declared.

1. Berghel H. Equifax and the latest round of identity theft roulette. Computer Dec 2017;50(12):72-76. [doi: 10.1109/MC.2017.4451227]
2. Arquilla J. Twenty years of cyberwar. Journal of Military Ethics 2013;12(1):80-87. [doi: 10.1080/15027570.2013.782632]
3. Heathfield H, Pitty D, Hanka R. Evaluating information technology in health care: Barriers and challenges. BMJ 1998;316:1959. [Medline: 9641938]
4. Wickramasinghe NS, Fadlalla AMA, Geisler E, Schaffer JL. A framework for assessing e-health preparedness. Int J Electronic Healthcare 2005;1(3):316–334. [doi: 10.1504/IJEH.2005.006478] [Medline: 18048213]
5. Jha AK. Meaningful use of electronic health records: The road ahead. JAMA 2010;304(15):1709–1710. [doi:10.1001/jama.2010.1497] [Medline: 20959581]
6. Clarke R, Youngstein T. Cyberattack on Britain's National Health Service - A wake-up call for modern medicine. N Engl J Med 2017 Aug 3;377(5):409-411. [doi: 10.1056/NEJMp1706754] [Medline: 28591519]
7. Kramer DB, Fu K. Cybersecurity concerns and medical devices: Lessons from a pacemaker advisory. JAMA 2017 Dec 5;318(21):2077–2078. [doi:10.1001/jama.2017.15692] [Medline: 29049709]
8. Stroud JM, Jenkins KD, Bhandary SP, Papadimos TJ. Putting the pieces together: The role of multidisciplinary simulation in medical education. Int J Acad Med 2017;3:104-9 [doi: 10.4103/IJAM.IJAM_44_17]
9. Merién AER, et al. Multidisciplinary team training in a simulation setting for acute obstetric emergencies: A systematic review. Obstet Gynecol 2010 May;115(5):1021-31. [doi: 10.1097/AOG.0b013e3181d9f4cd] [Medline: 20410778]
10. Steinemann S, et al. In situ, multidisciplinary, simulation-based teamwork training improves early trauma care. J Surg Educ. 2011 Nov-Dec;68(6):472-7. [doi: 10.1016/j.jsurg.2011.05.009] [Medline: 22000533]
11. Passiment M, Sacks H, Huang G. Medical simulation in medical education: Results of an AAMC survey. Association of American Medical Colleges 2011.
12. Huang G, Reynolds R, Candler C. Virtual patient simulation at US and Canadian medical schools. Acad Med 2007 May;82(5):446-51. [doi: 10.1097/ACM.0b013e31803e8a0a] [Medline: 17457063]
13. Hanscom R. Medical simulation from an insurer's perspective. Acad Emerg Med 2008;15:984-7. [doi: 10.1111/j.1553-2712.2008.00255.x] [Medline: 18945230]
14. Grimes S, Wirth A. Holding the line: events that shaped healthcare cybersecurity. Biomed Instrum Technol 2017 Sep 2;51(s6):30-32. [doi: 10.2345/0899-8205-51.s6.30] [Medline: 29161106]
15. Ronquillo JG, Zuckerman DM. Software-related recalls of health information technology and other medical devices: Implications for FDA regulation of digital health. Milbank Q 2017 Sep;95(3):535-553. [doi: 10.1111/1468-0009.12278] [Medline: 28895231]
16. Baker S. Fuzzing: a solution chosen by the FDA to investigate detection of software vulnerabilities. Biomed Instrum Technol 2014 Spring;Suppl:42-7. [doi: 10.2345/0899-8205-48.s1.42] [Medline: 24848149]
17. Finnegan A, McCaffery F, Coleman G. Development of a process assessment model for assessing security of it networks incorporating medical devices against iso/iec 15026-4. Proceedings of the International Conference on Health Informatics 2013:250-255. [doi: 10.5220/0004327502500255]