Cybersecurity of Medical Devices: Past, Present, and Future

100

Nameer Haider, Christopher Gates, Vikram Sengupta, and Sascha Qian

Introduction

In today's healthcare industry, the technological infrastructure is built on an outdated bedrock of software and hardware known. Designed in an era predating large-scale hacking and cyberterrorism, the current bedrock is rife with cybersecurity vulnerabilities. These vulnerabilities are further exposed as medical devices are adapted for connectivity in an increasingly interconnected world. Many of these devices were never intended to be connected to the Internet, to each other, or to the cloud. This issue is further complicated by their incorporation into human beings to form a network. As vulnerabilities are identified and exploited, snippets of code known as patches can be written to rectify them. However, the impact of a security patch on an older device can be incomplete, variable, and unpredictable.

Leo Scanlon, the deputy chief information security officer at the United States Department of Health and Human Services, has stated that the "healthcare sector is particularly sensitive to cyberattacks upon the 'Internet of things' (IOT), because many healthcare-related devices were not developed with the intention of being on the Internet. It was never intended they would be able to talk to other devices, yet they are." Here, the Internet of things are defined as the network of electronic devices and physical objects embedded with sensors and actuators, which are linked through wired and wireless networks; examples include roadways, pacemakers, and remote cameras (see Fig. 100.1). An extension of this concept is the "Internet of bodies," which is comprised of the devices that are attached to or implanted into the human body. Due to development and expansion of "Internet of bodies," medical device cybersecurity vulnerabilities pose an unprecedented and growing threat to human beings and their health.

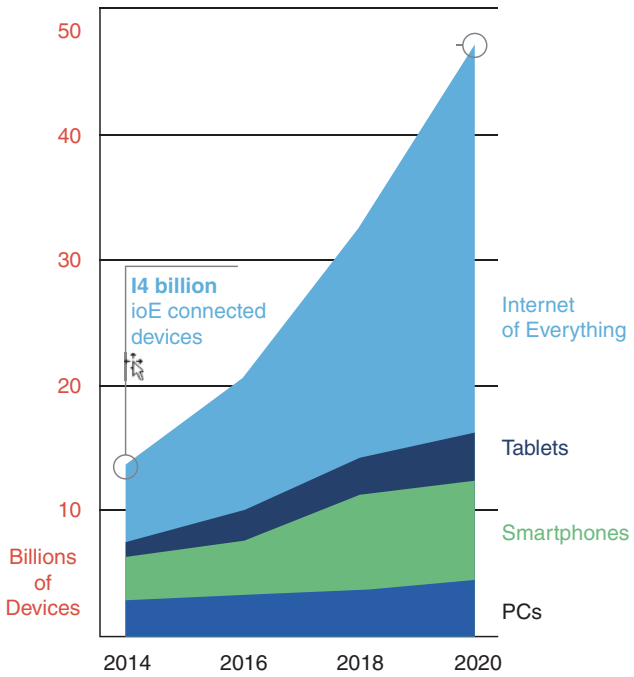

Fig. 100.1 Internet of things from 2014 to projected 2020. Proliferation of Internet of things-driven devices shows exponential growth

The fear of hacking medical devices has been present for years (see Fig. 100.2). Former United States Vice President Dick Cheney famously had the Wi-Fi on his cardiac pacemaker turned off in 2007 to preempt hacking and cyberattack. Indeed, from a cybersecurity standpoint, medical devices are largely built upon older, outdated, "legacy" technology and therefore cannot be easily updated with cybersecurity software. Consequently, to ensure compatibility with modern cybersecurity technology, most medical devices must either undergo core hardware and software redesign or be discarded entirely. Delays in the passage of federal legislative mandates to secure medical devices magnify the problem of legacy incompatibility daily.

N. Haider (✉) · V. Sengupta · S. Qian
Spinal & Skeletal Pain Medicine, Utica, NY, USA
e-mail: drhaider@killpain.com; drsengupta@killpain.com; drqian@killpain.com

C. Gates
Velentium LLC, Katy, TX, USA
e-mail: chris.gates@velentium.com

T. R. Deer et al. (eds.), *Deer's Treatment of Pain*, https://doi.org/10.1007/978-3-030-12281-2_100

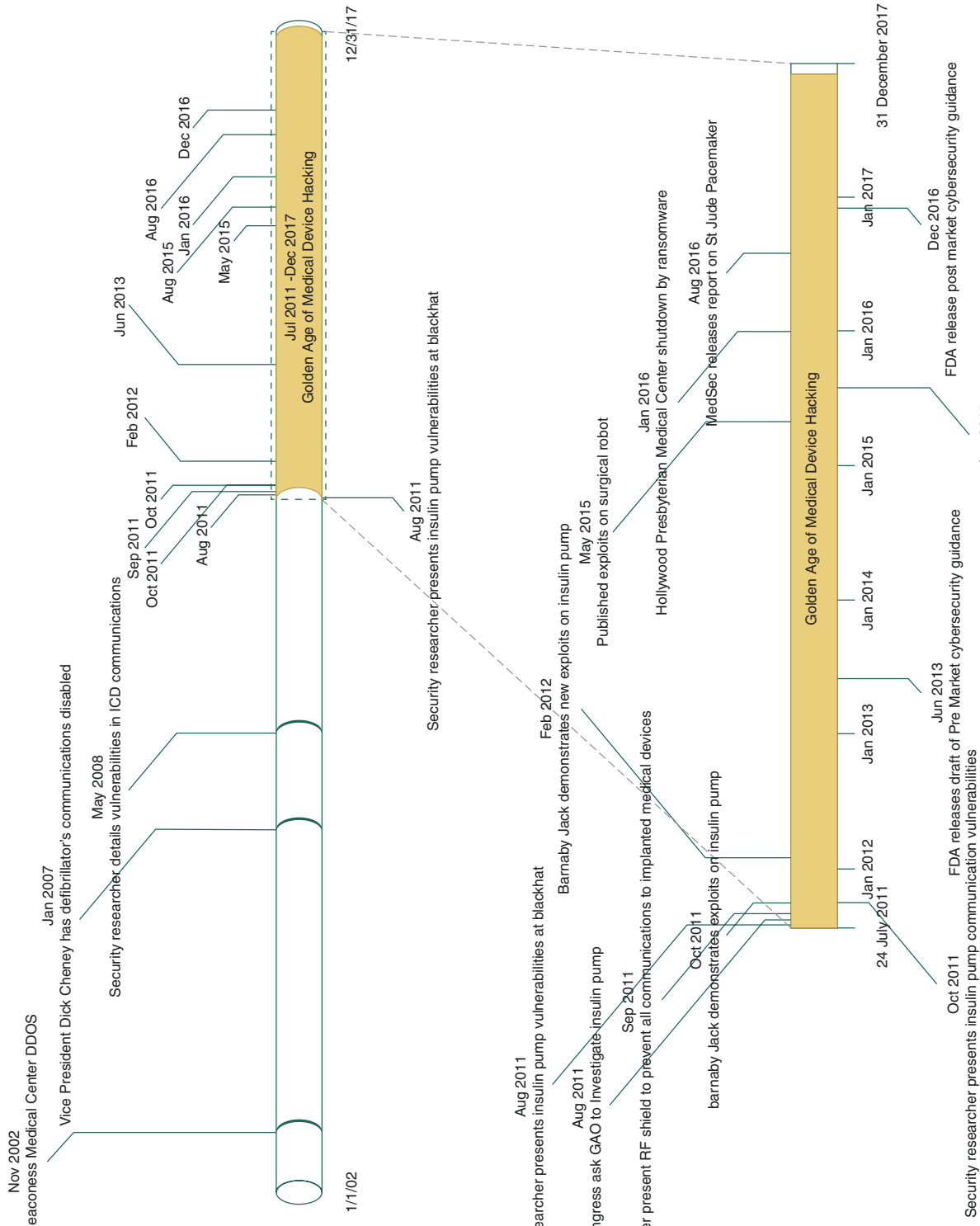

Fig. 100.2 Timeline of medical device security concerns and hacking from 2002 to 2017. The sentinel event was Beth Israel Deaconess Medical Center distributed denial-of-service (DDOS) attack in 2002. In 2007, Vice President Dick Cheney has his defibrillator's communications disabled preemptively. In May 2008, British and Belgian security researchers detail vulnerabilities in implantable cardiac defibrillator (ICD) communications. The Golden Age of medical device hacking then occurred between July 2011 and December 2017; this period included revelation of insulin pump vulnerabilities prompting the Government Accountability Office (GAO) investigations in addition to the shutdown of Hollywood Presbyterian Hospital by ransomware

In the Cybersecurity Act of 2015, Congress established the Healthcare Industry Cybersecurity Task Force to address the challenges the healthcare industry faces when securing and protecting itself against cybersecurity threats. In June 2017, this task force published a report entitled "Improving Cybersecurity in the Healthcare Industry"—one significant resolution was that the healthcare industry should "dramatically reduce the use of less defensible legacy and unsupported products and more effectively reduce risk in future products through robust development and support strategies." The report further elaborated by stating that in their present state, many healthcare organizations will be unable to identify or act upon potential threats as they do not have the resources nor experience to address the emerging security threats. Furthermore, these healthcare organizations may not even recognize the attack in time.

The cybersecurity of medical devices that are "embedded" in patients (henceforth referred to as "embedded medical devices") typically involves many more complexities than those that arise in the domain of management information systems and information technology (MIS/IT). Due to the age, evolution, and inherent nature of the Internet, the domain of MIS/IT is viewed by cybersecurity specialists as a "naturally occurring object," to which security mitigations are added as an afterthought. While the common security topics of confidentiality, integrity, and availability can be applied to both the MIS/IT and embedded medical devices, each applies to each in an entirely unique manner.

Physical Security

In the MIS/IT domain, physical security is achieved by keeping unauthorized personnel away from a server through the use of physical barriers, the simplest manifestation being a locked door. However, an embedded medical device must travel from place to place with its human host and therefore cannot be secured in such a simple manner. Therefore, a number of alternative mechanisms must to be designed and deployed into medical devices to enforce the confidentiality of sensitive information and integrity of executable programs. Examples include patient data utilized in device communication and storage of these valuable device assets.

While advances that increase remote connectivity of medical devices often enhance the quality of patient care, each modification introduces new security risks that must also be carefully assessed and minimized. In 2013, the FDA issued guidance on the use of radiofrequency for wireless medical devices, including a recommendation for authentication and encryption protocols as measures to reduce patient safety and security risks.

Available Resources

Inherent differences in resource utilization and availability lead to distinct cybersecurity issues in the information security and embedded medical device domains. Network servers tend to occupy a fixed location and can be physically augmented to fit their computational needs. Therefore, they can theoretically consume an unlimited supply of power and computational resources, including central processing unit throughput, memory, and time. In contrast, embedded medical devices are miniaturized, physically discrete, and battery powered. They cannot exploit an unlimited and flexible supply of energy, memory, and computational power for core and security operations. Consideration of these unique challenges must be made for the design and implementation of effective medical device security mechanisms.

Highly Fractured Landscape of Standards

MIS/IT utilize international communication standards to ensure interoperability on the Internet. These original standards focused on ensuring Internet communications seamlessly occur, with security being an afterthought, in addition to securing data that is being communicated while ignoring security of data.

The Cybersecurity Act of 2015 Congress established the Healthcare Industry Cybersecurity Task Force to address the challenges faced when securing and protecting against intentional or unintentional cybersecurity incidents.

Agencies involved in formulating medical device standards include the Food and Drug Administration (FDA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Center for Devices and Radiological Health (CDRH), National Institute of Standards and Technology (NIST), National Cybersecurity Center of Excellence (NCCoE), Information Sharing and Analysis Organizations (ISAOs), Health Information Trust Alliance (HITRUST), Department of Health and Human Services (HHS), and Department of Homeland Security (DHS).

The FDA, in conjunction with the Center for Devices and Radiological Health (CDRH), established a cybersecurity risk management program, making cybersecurity paramount and creating a trusted environment for information sharing. With very few exceptions, the FDA has facilitated implementation of cybersecurity into medical devices by not requiring premarket review or recall of software updates for cybersecurity. A vulnerability disclosure policy and coordinated disclosure are critical to improving security; however, the FDA will not be prescriptive with risk analyses and instead will evaluate the well-being of community as a whole.

In October 2016, the FDA entered into a new memorandum of understanding with the National Health Information Sharing and Analysis Center (NH-ISAC) and the Medical Device Innovation, Safety and Security Consortium (MDISS). The NH-ISAC is a nonprofit organization that coordinates cybersecurity incidence response by providing member organizations with actionable information on cybersecurity. The MDISS is a nonprofit organization that develops best practices in cybersecurity. The final FDA guidance, released on December 2016, recommends structured and comprehensive management of post-market cybersecurity vulnerabilities for medical devices throughout their product life cycle. In January 2017, the FDA held a webinar on the guidance: Postmarket Management of Cybersecurity in Medical Devices. In May 2017, the FDA partnered with the National Science Foundation (NSF) and the Department of Homeland Security Science and Technology to hold a public workshop "Cybersecurity of Medical Devices: A Regulatory Science Gap Analysis," with the goal of strengthening medical device cybersecurity.

HIPAA includes both privacy and security standards. The HIPAA security rule includes the Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) and establishes a national set of security standards for protecting electronic health information.

National Institute of Standards and Technology (NIST), through the National Cybersecurity Center of Excellence (NCCoE), works to secure networked medical devices from risks such as malware, hacking, and access control. The NCCoE works with industry, academic, and government experts to find practical solutions for businesses cybersecurity needs. Mitre Corporation, awarded a contract to support NCCoE as the first federally funded research and development center dedicated to cybersecurity, works to support relationships and collaboration between government sponsors, industry, and academia.

Nongovernmental organizations such as the Information Sharing Analysis Standards Organization (ISAO) work with federal entities responsible for conducting cybersecurity and related activities to create national networks with automated mechanisms for information sharing. Presidential Executive Order 13691 encourages the development of the Information Sharing Analysis Standards Organization (ISAO) to serve as focal points for cybersecurity information sharing. MedISAO, an organization composed of members of the medical device community, is a registered ISAO providing compliance with the FDA's recommendation in the post-market management of cybersecurity in medical devices.

The Health Information Trust Alliance (HITRUST) is a privately held company located in the United States that, in collaboration with technology, healthcare, and information security leaders, has established a Common Security Framework (CSF) which may be used by organizations that create, access, store, or exchange sensitive or regulated data. Common Security Framework (CSF) includes a prescriptive set of controls which seek to harmonize the requirements of multiple regulations and standards—this helps organizations by providing an efficient and prescriptive framework for managing the security requirements of HIPAA. In a sense, this creates a voluntary industry-managed approach to meeting the HIPAA security rule requirements. Using globally recognized standards such as the HIPAA, the HITRUST provides clear updated actionable guidelines consistent with the latest healthcare industry and government regulations.

What Are the Risks?

Medical device security risks are shared across all domains, including medical device manufacturers, hospitals, clinics, healthcare providers, research institutions, software companies, public and private insurance carriers, and patients. Digital connectivity is required for the healthcare system to deliver safe and effective care. A connected but insecure healthcare system could cause unnecessary risk and jeopardize patient safety.

Medical device manufacturers have the luxury of creating medical devices with unique methods of storage and proprietary communication protocols, without regard to worldwide standards. Unfortunately, device manufacturers have not employed such methods thus far, since the security risks have been largely unrecognized or intentionally disregarded. Making the decision to prioritize cybersecurity within the medical device industry requires a critical shift in cognitive framework from corporate leadership.

Frequent cases of ransomware, identity theft, and targeted nation-state hacking remind and show us that our healthcare data is vulnerable. Data collected to treat patients can be used for nefarious purposes such as fraud, identity theft, supply chain disruptions, intellectual property theft, and stock manipulation. Most importantly, cybersecurity attacks disrupt patient care. For example, ransomware is typically a malicious software that either threatens to publish patient data or blocks access unless a ransom is paid.

Most medical device manufacturers face significant resource constraints as operating margins can be very low, and cybersecurity infrastructure is a very small portion of their overall budget. Due to previously believing that their cybersecurity vulnerability was low and lack of qualified and experienced staff, manufacturers often lack the ability to identify, track, analyze, audit, and translate threat data into actionable information. Given the increasing frequency of system compromises by ransomware, the reality of cybersecurity vulnerability can no longer be avoided. In light of such

recent events, medical device manufacturers thus have increased their own education and awareness as it has been made clearly evident that risk mitigation can save money, prevent litigation, and protect against damages to the corporate reputation.

Patient Safety

The most obvious and serious risk of inadequate device security is to patient safety. The hacking of a medical device is extremely difficult to ascertain unless the attacker publicly admits to it. This may in fact have some bearing upon why we are as of yet unaware of anyone dying from a hacked medical device.

A recent report from security firm WhiteScope analyzed seven different pacemaker programmers from four different manufacturers and found more than 8600 flaws in pacemaker systems and the third-party libraries that power various components of the devices. Outdated libraries in pacemaker programmer software set therapy parameters and monitor device function. Problems found included lack of encryption and authentication, bugs in the code, and poor design that can put patient lives at risk. These design flaws highlight the need for a complete overhaul of basic medical device design.

In 2015, Hospira and an independent researcher confirmed the possibility of accessing the Symbiq Infusion System remotely through a hospital's network. In May 2015, the FDA issued a Safety Communication on vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems after an independent researcher released information about these vulnerabilities.

In January 2017, the FDA issued a Safety Communication confirming vulnerabilities in St. Jude Medical's implantable cardiac devices and Merlin@home Transmitter. Subsequently in April 2017, the FDA sent a warning letter to Abbott charging the medical device manufacturer with failing to reveal a deadly defect with defibrillators marketed by St. Jude Medical, which was acquired by Abbott. The main issue was that St. Jude downplayed battery failure in its cardiac defibrillators and continued to ship devices despite evidence of rapid battery depletion. These issues led to a patient death which St. Jude failed to disclose this death to the FDA. Following a second warning letter from the FDA, the company recalled the remaining devices in question.

Thereafter, in August 29, 2017, the FDA issued a Safety Communication informing patients and healthcare providers about the release of a firmware update to address cybersecurity vulnerabilities. Abbott has told patients with affected defibrillators to register with St. Jude's MerlinHome Monitoring System, which itself had significant cybersecurity flaws. The FDA is urging all heart transplant patients who have received a St. Jude pacemaker to contact their healthcare provider and receive a software update to protect their device from being hacked which could drain battery power or administer inappropriate pacing. If the company doesn't correct the violations, the FDA could serve the company with an injunction, seizure, or monetary fine.

The Smiths Medical Medfusion 4000 device was recently found to have serious hackable flaws, which would allow a remote attacker to gain unauthorized access and impact the operation of the pump. The Department of Homeland Security (DHS) identified eight vulnerabilities in three versions of the device and cited issues which can allow a cybercriminal to execute a dangerous code and cause an overdose of medication administered.

Exposure of Patient Protected Health Information

Medical information can be used to defraud individuals and organizations, including identity theft and secondary attacks against patients. Such theft can have negative consequences on hospitals, clinics, and healthcare providers in the form of fines from the Department of Health and Human Services (HHS) and crippling legal actions from the Federal Trade Commission. In one recent incidence, actual unencrypted data that included Social Security numbers, names, and medical and patient data of a well-known hospital on the east coast was left exposed on a pacemaker programmer. With about 112 million records stolen in 2015, the medical information of nearly half all Americans is already on the dark web.

The Office for Civil Rights in the US Department of Health and Human Services issued guidance, via "HHS Fact Sheet," to help healthcare entities understand and respond to ransomware attacks. According to the HHS Fact Sheet, there had been 4000 daily ransomware attacks since early 2016. According to a 2017 report from Aite Group/Trend Micro, the black market value of a stolen credit card number with CVV is about $1 and a username and password on Amazon or Uber $2–$4, and a stolen medical record is valued at between $20 and $50.

Denial of Service

Denial of service attacks may prevent the operation of a device or all devices in a hospital until a ransom has been paid. This has recently become quite popular due to the ease of accomplishing this and the low risk being taken by the attacker. This can be devastating to a hospital, clinic, healthcare provider, and patient who may need the uninterrupted use of a medical device. It is predicted that future attacks will come through preplanted malware.

Exposure of Intellectual Property

Medical devices are physical implementations of concepts and algorithms. These algorithms require years of clinical study and analysis to derive and thus have value to the manufacturer's competitors. Exposure of these algorithms by attacking a single device to extract the program code is frequently performed and usually trivial in nature. However, this attack can also be the first in a series of attacks if the analysis of the exposed software discovers additional vulnerabilities that can be exploited.

Negative Public Relations and Loss of Public Confidence

Widespread public condemnation about handling of medical device hacks may negatively affect future medical device sales and corporate stock prices due to loss of consumer confidence. Such lapses in ability to adequately secure patient safety may ultimately lead to regulatory and consumer concerns affecting hospitals, clinics, vendors, and healthcare professionals. In one recent example, St. Jude Medical (STJ) corporation shares lost value and jeopardized the planned acquisition by Abbott Corporation due to allegations by the Carson Block's research firm Muddy Waters that STJ would lose more than half of its revenue due to device recalls.

Manufacturer Liability

Medical devices with cybersecurity lapses may expose manufacturers to significant liability. A bipartisan group of US senators have introduced legislation to address cybersecurity vulnerabilities in computing devices. Such future legislation may create liability for medical device manufacturers and their Board of Directors created by their vulnerable devices. The FDA has stated that manufacturers are legally required to comply with all applicable regulations and are subject to pre- and post-market cybersecurity guidance that articulates a comprehensive, structured, and systematic cybersecurity risk management program.

What Can We Learn from the Past?

Inception of medical device hacking is relatively recent, with the majority of events occurring since 2011 (see Fig. 100.2). Thereafter, significant progress has been achieved in securing new medical devices, which have been demonstrated in a more regulated environment.

Due to the long life span of the average medical device, it may be years before an older insecure medical devices are replaced by newer secure medical devices. Several proposals have been suggested to accelerate the replacement process, such as "cash for clunkers," where the government buys back older insecure medical devices. This is obviously not the concept of choice for surgically implanted medical devices. The FDA's 2017 recall of 465,000 Abbott Laboratories pacemakers alerted all medical device manufacturers that they should take cybersecurity issues more seriously and be more proactive in development and introduction of security updates.

What Are the Current Best Practices to Mitigate Risk Today?

Unfortunately, in the majority of medical device development life cycles, if security of the finished product is even considered, it is addressed in an unstructured approach. This typically manifest itself as someone during the design phase making a short and incomplete list of known security exploits, which are usually too vague to be traced throughout the development life cycle and so very little is done during the design and implementation portions of the project. After device development and testing have been completed, the device is sent out to independent third party for penetration testing where a "hacker for hire" documents all the methods used to subvert the security on the device. Since this information is arriving very late in the medical device development cycle, when schedules and budgets are typically exhausted, there is usually nothing to be done about such discovered vulnerabilities. Such a process has led to the current state of insecurity.

Where Do We Want to Be Tomorrow?

Currently, thought leaders in the medical device industry are following a more structured approach integrating security into their normal software development life cycle (see Fig. 100.3). Most of the added activities are new work items to be performed by regular development teams, with potential assistance in product security subject matter by security experts and consultants. The work is auditable and repeatable and focuses on the root cause of all actual and potential vulnerabilities in the end product, including software description, hazards, requirements, design specifications, traceability, development environment, verification, validation, revision history, unresolved anomalies, and documentation such as even premarket submissions for software contained in medical devices.

Medical device manufacturers must consider and plan for cybersecurity at medical design inception rather than add

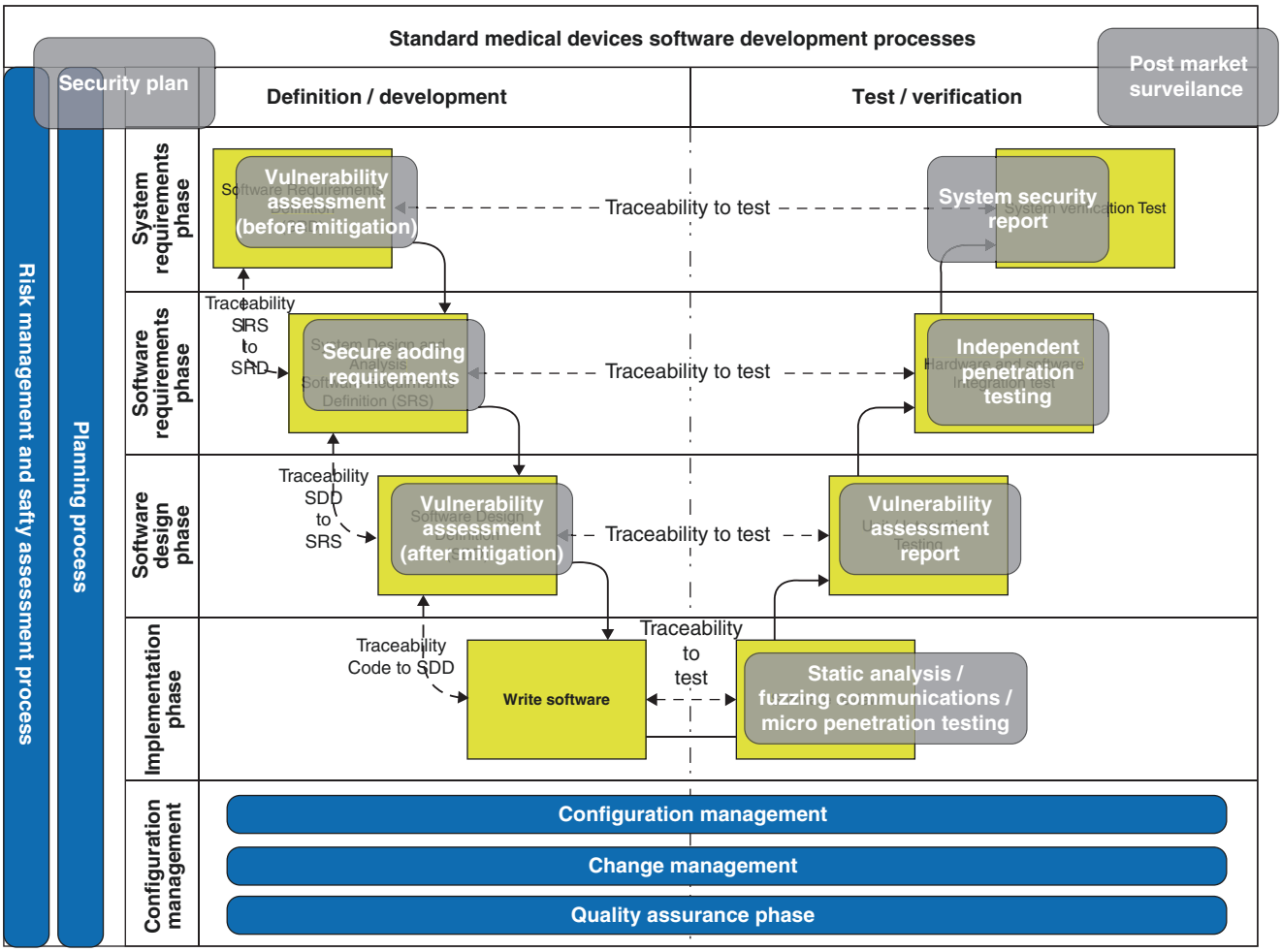

Fig. 100.3 Standard medical device software development process revolves around repeatable work and the root cause of all actual and potential vulnerabilities in the end product, including software description, hazards, requirements, design specifications, traceability, development environment, verification, validation, revision history, unresolved anomalies, and documentation such as even premarket submissions for software contained in medical devices

security to a device as an afterthought after the design process has been completed. Medical device manufacturers should adopt policies of good cybersecurity with risk mitigation occurring during the total product life cycle from conception to obsolescence. Integration and information sharing are imperative with all stakeholders identifying, protecting, detecting, and responding to cyber threats.

Vulnerabilities

Vulnerabilities can be created at the three following distinct points when a new device is being developed: (1) design, (2) implementation, and (3) post-market discovery in software libraries. Breaking out the activities in the Secure Development Lifecycle based upon these three areas of weakness details the activities to be performed (see Fig. 100.4)

Communications Infrastructure

The Internet was not originally designed as a robust and secure structure for communications. The exposure of databases on the Internet is partially the fault of this old aging infrastructure. What is needed is an "end-to-end" solution for securing data from its point of inception through multiple forms of communications and storage, including an end user who is authenticated to see only the proper data that has been aggregated (see Fig. 100.5). We are only now seeing tools for achieving this level of control of the data, as opposed to the control of the communications. This is happening at a time, which the latest available electronics for medical devices has been scaled up to support world-class cryptographic capabilities used for this type of data control.

Blockchain technology, an ingenious invention that allows digital information to be distributed but not copied, has recently been touted as the holy grail of cybersecurity.

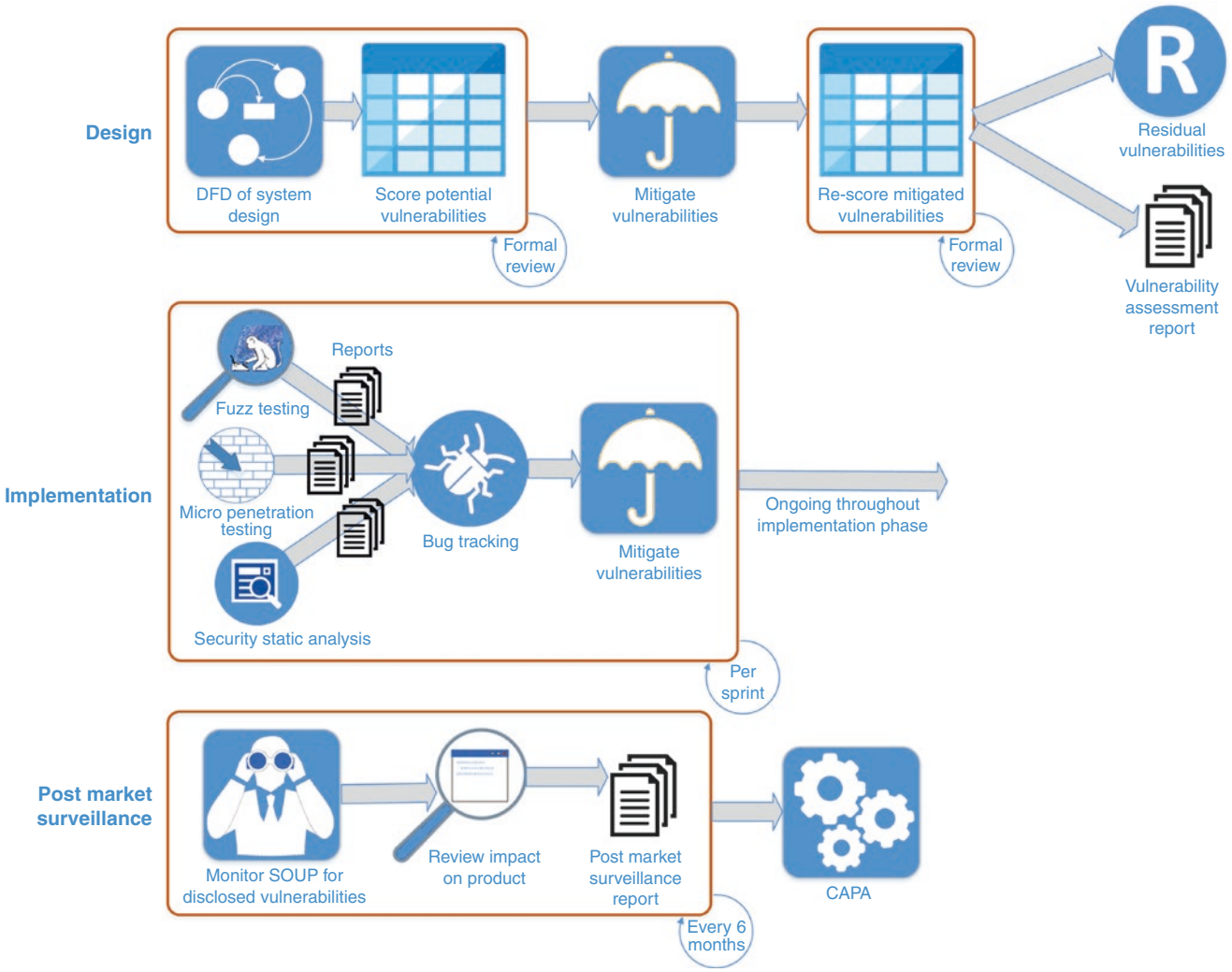

Fig. 100.4 Design, implementation, and post-market discovery are distinct points of vulnerability when a new device is being developed

Blockchain's original mandate was solely to prevent double payments on Bitcoin but has since evolved into a more generalizable security product. Unfortunately, because blockchain is still focused on encryption as the solution, the functionality is somewhat heavyweight. As encryption is only a subcomponent of cybersecurity, it would be impossible for the healthcare industry to discard existing systems and re-implement new systems on a blockchain architecture.

To date, cybersecurity has focused on securing infrastructure including security of hardware, networks, applications, devices, and identities. Perimeter security, the classic moat around the castle approach, is provided to computer networks. The network moat includes firewalls, sniffers, vulnerability scanning, and intrusion detection systems. Once the moat is breached, the network is hopelessly vulnerable. Data loss prevention (DLP) systems track sensitive data exiting or traversing corporate networks, and digital rights management (DRM) systems restrict access to proprietary information, but they do not track all data or data in transit across domains.

Secure File Transfer Protocol (FTP) tracks and manages the transfer of files between networks but uses unencrypted and unauthenticated transmission control protocol connections, creating the ability to eavesdrop, steal passwords, and hijack connections. Secure document vaults protect content in heavily regulated industries like healthcare and financial services but are vulnerable to hacking.

Mobile devices are quickly becoming the primary communications and computing platform for businesses. Mobile device management (MDM) solutions enforce policies for corporate smartphones and tablets but are vulnerable to password theft and unsecured Wi-Fi networks.

Cloud access security brokers (CASBs) are software systems that manage security between an organization's onsite network infrastructure and the cloud to create safe

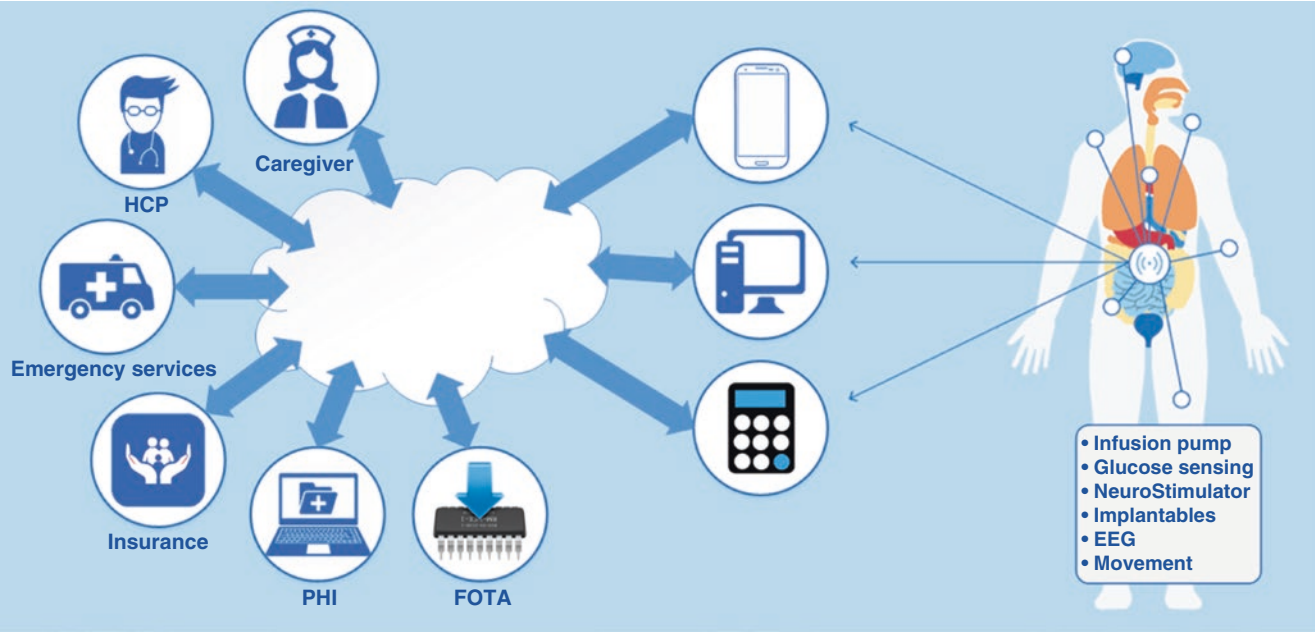

Fig. 100.5 "End-to-end" solution for securing data from its point of inception through multiple forms of communications and storage includes an end user who is authenticated to see only the proper data

environments for exchanging and sharing information. Cloud access security brokers (CASBs) are entirely cloud based or cloud solution only. They are not intended as a network product nor a hybrid product. CASBs data must be stored in the cloud, and data granularity within the CASB is limited to "software as a service" applications within the cloud. Once the cloud security perimeter has been breached, however, the data is still vulnerable.

Data encryption with zero-knowledge privacy means that not only are devices using data encryption but also that only authorized users can access data from a medical device. Identity management must require biometric and other multifactor identification tokens to ensure user true identity and access rights. Behavior analytics must include systems that learn and monitor user behavior patterns, alerting and reacting to any or all unusual activity. Secure and safe medical device connectivity requires Internet security without boundaries across all domains including server, cloud, mobile, and medical devices. Medical devices should have the ability to enforce rules that travel with data including the ability to recall data and access from any system. A secure system should provide tamper-proof granular activity audit reports clearly displaying who is accessing medical device data and how they are using it.

Ransomware protection is also necessary to protect valuable data from ransomware and prevent phishing or social engineering attacks. The medical device manufacturer should utilize a cybersecurity system certified by a recognized organization using industry standards, enabling the medical device to meet multiple regulatory requirements.

True medical device cybersecurity will involve securing the ecosystem's entire infrastructure, including applications, devices, networks, and identities. This can only be truly accomplished by securing the sensitive data itself through its entire life cycle.

To accomplish this, multiple defenses must be implemented including data encryption, identity management, behavioral analytics, data access and recall, granular reporting and audit, and ransomware protection, all while fulfilling regulatory requirements that are continually updated.

Summary

The future seems bright for new product security, with the confluence of new tools and technology available; the potential for attenuating this looming problem looks good. New regulations are required and will be forthcoming to mandate manufacturers to disclose and correct vulnerabilities in their medical devices. This will enable hospitals, clinics, and healthcare professionals to make informed decisions about where to spend their budgets when acquiring new medical devices.

Of course, the "legacy products" will continue to be a problem until they are removed from service. Today, the only way to protect medical devices and secure data is with an ecosystem that spans all domains, allowing the management of data security as if it were on your own domain, including your own medical device. The future of cybersecurity rests in the ability to protect data itself, while at rest, as well as in transit, anywhere in the cyber ecosystem.

Recommended Reading

1. Csulak E, Meadows T, Corman J, DeCesare G, Fernando A, Finn D, Jarrett M, Laybourn L, McNeil M, McWhorter D, Mellinger R, Monson J, Ramadoss, Rice T, Sardanopoli V, Suarez R, Stine K, Sublett C, Thompson L, Ting D, Trotter F. Report on Improving Cybersecurity in the Health Care Industry. Washington, DC: Health Care Industry Cybersecurity Task Force; 2017.
2. Cyber Risk Thursday: Internet of Bodies [Internet]. Atlantic Council. [cited 2017Dec13]. Available from: http://www.atlanticcouncil.org/events/upcoming-events/detail/cyber-risk-thursday-internet-of-bodies.
3. Executive Order – Promoting Private Sector Cybersecurity Information Sharing [Internet]. National Archives and Records Administration. National Archives and Records Administration; [cited 2017Dec13]. Available from: https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.
4. FDA to patients with St. Jude pacemakers: Update needed to keep hackers out of devices [Internet]. Healthcare IT News. 2017 [cited 2017Dec13]. Available from: http://www.healthcareitnews.com/news/fda-patients-st-jude-pacemakers-update-needed-keep-hackers-out-devices.
5. Graf R. St. jude (stj) stock down despite response to muddy waters allegations [Internet]. TheStreet. TheStreet; 2016 [cited 2017Dec13]. Available from: https://www.thestreet.com/story/13687004/1/st-jude-stj-stock-down-despite-response-to-muddy-waters-allegations.html.
6. http://www.healthcareitnews.com/news/pacemaker-device-security-audit-finds-8600-flaws-some-potentially-deadly.
7. ICS-CERT Advisories | ICS-CERT. [cited 2017Dec13]. Available from: https://ics-cert.us-cert.gov/advisories/ICSMA-17-250-02.
8. Modern Healthcare [Internet]. Abbott recall signals new era in medical-device cybersecurity. [cited 2017Dec13]. Available from: http://www.modernhealthcare.com/article/20170901/NEWS/170909986.
9. News [Internet]. Healthcare IT News. [cited 2017Dec13]. Available from: https://www.healthcareitnews.com/news/device-maker-was-hush-defibrillator-defect-killed-patients-fda-says.
10. Sweeney E. Cash for clunkers: Could it work for legacy medical devices? [Internet]. FierceHealthcare. 2017 [cited 2017Dec13]. Available from: https://www.fiercehealthcare.com/privacy-security/cash-for-clunkers-could-it-work-for-legacy-medical-devices.