intertrust®

INTERTRUST WHITE PAPER

Protecting Healthcare Software

TABLE OF CONTENTS

Executive Summary

For decades medical devices have been standalone instruments that interacted only with the patient or medical provider. The advent of technological innovations including miniaturization, low power computation, and wireless technologies has created a new paradigm in the healthcare industry: the Internet of Medical Things (IoMT). These devices can now connect to a variety of systems, networks, and other tools within a healthcare delivery organization, enabling higher quality patient care, streamlined operations and improved cost efficiencies. Today, medical technology companies manufacture more than 500,000 different types of wearable, implantable, and stationary medical devices. It has been estimated that the size of the IoMT market was valued at $41.2B in 2017 and will rise to $158.1B in 2020[1].

But these new devices come with substantial new risks. Hackers who have physical access to devices can reverse engineer how they work and craft exploits to take advantage of vulnerabilities in their design or implementation. As medical devices become increasingly complex, their attack surfaces increase, providing more opportunities for hackers to find ways to exploit them. Medical devices can easily be purchased directly through manufacturers or resellers, or obtained second hand, for example on eBay, allowing hackers to gain hands-on experience in how to reverse engineer them. Because these devices are highly connected, these exploits can be mounted remotely if the attacker can gain access to the networks in which they operate, or even on the manufacturing floor where they are produced.

The consequences of a security breach for medical devices are grave. Medical applications that are susceptible to attacks by hackers or malware can eventually lead to health risks or even loss of human life. The privacy of patient medical data can be compromised and used for illicit purposes. Entire hospital systems can be taken down by ransomware attacks. These attacks expose healthcare organizations, device manufacturers and providers to substantial liability. If security problems cannot be properly addressed, there is the risk of consumers and healthcare professionals losing trust in the ability of these devices to properly protect and use patient data responsibly.

These attacks are not theoretical. Several recent highly publicized attacks have been demonstrated. For example, in early 2015, Anthem disclosed that 78.8 million patient records had been stolen. The cyberattack claimed highly sensitive data, including names, Social Security numbers, home addresses, and dates of birth. Just six weeks later, Premera Blue Cross announced a cyberattack that had exposed the medical information of 11 million customers. Among other information, the attack had exposed bank account numbers, Social Security numbers, dates of birth, and claims information[2]. Recently, vulnerabilities in implantable cardioverter-defibrillators[3], pacemakers, and insulin pumps[4] were identified allowing remote attacks that could potentially compromise patient safety.

The US Food & Drug Administration (FDA) has published a series of guidance in this area, including the Postmarket Management of Cybersecurity in Medical Devices[5], which has been driving new standards for security in the field, and continues to provide guidance on how to improve cybersecurity. In other parts of the world, different regulation is in place.

---

[1] IoT Healthcare Market worth 158.07 Billion USD by 2022 (2017). MarketsandMarkets. https://www.marketsandmarkets.com/PressReleases/iot-healthcare.asp

[2] Top 10 Biggest Healthcare Data Breaches of All Time (2018). Digital Guardian. https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time

[3] A Few Thoughts on Cryptographic Engineering (2018). Matthew Green. https://blog.cryptographyengineering.com/2018/02/17/a-few-notes-on-medsec-and-st-jude-medical

[4] A New Pacemaker Hack Puts Malware Directly On the Device (2018). Wired. https://www.wired.com/story/pacemaker-hack-malware-black-hat

[5] Postmarket Management of Cybersecurity in Medical Devices (2016). U.S. Food & Drug Administration. https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf

For instance, in the European Union, a number of standards set out an initial level of requirements regarding cybersecurity of medical devices, such as EN 62304:2006[6] and EN 14971:2012[7].

The purpose of this white paper is to highlight potential threats in typical modern medical applications in terms of cybersecurity and protection of patients' medical data, and how to effectively address these threats with Intertrust's whiteCryption® technology.

The Shift to Smart Technologies

Healthcare is one of the fastest industries to adopt smart technologies, such as biosensors, wearable devices, medical apps, and smart devices[8]. The reason for this trend is that integrating smart features into medical devices greatly improves the quality and effectiveness of medical service, bringing especially high-value for patients with chronic conditions, the elderly, and those requiring constant supervision. Additionally, embracing smart technologies enables healthcare providers to reduce costs, enable intelligent data analysis, and optimize the workflow.

The following figure shows a typical arrangement of key components in a modern healthcare scenario.

The central element in this arrangement is the patient that is in some way connected to a smart health monitoring device. For instance, it might be a wearable device, such a heart rate monitor, on the patient's arm, or a blood pressure sensor implanted inside the body. Almost every device in a hospital is now connected, including beds, infusion pumps, MRIs and CT scanners. The monitoring device transmits encrypted health statistics to other devices, such as a desktop computer connected via a USB cable, or a mobile device over a WiFi or Bluetooth connection, or to a nurse's monitoring station. It is increasingly common for the collected data to be transferred even further (either directly over a cell service or via a proxy device) to a database in the cloud for the benefit of the doctor and other healthcare specialists providing service to the patient, trusted third parties involved in healthcare, or for the patient to be able to track their own health statistics in cloud-enabled web applications.

---

[6] IEC 62304:2006: Medical device software - Software life cycle processes (2006). International Organization for Standardization. https://www.iso.org/standard/38421.html

[7] ISO 14971:2007: Medical devices - Application of risk management to medical devices (2007). International Organization for Standardization. https://www.iso.org/standard/38193.html

[8] Biometric Monitoring and IoT: A New Era of Digital Health (2018). DZone. https://dzone.com/articles/biometric-monitoring-and-iot-a-new-era-of-digital

The Problem

While the ever-growing shift to smart technologies has definitely increased the quality of medical service and patient satisfaction, at the same time it has created a challenge of keeping patients' data safe, and protecting the medical software against adversaries. In addition, criminals and dark web hackers prize patient data. For example, the average sale price of a compromised credit card account is approximately $0.25, but an Electronic Health Record (EHR) can demand a price of hundreds to thousands of dollars since it can contain a myriad of valuable personal information that can be used in several ways for long periods of time, maximizing monetization[9]. A hacker might also leverage sensitive personal data found in these records to blackmail the victim, especially if they are a public figure[10].

Furthermore, healthcare systems used to process medical data and Personally Identifiable Information (PII) need to comply with complex regulations and laws related to system security, such as General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA) and ISO/IEC 27001 Information Security. Such regulations not only require you to protect the data, but also introduce significant financial fines for the failure to do so.

The following sections discuss some of the common privacy and software risks associated with modern healthcare services in more detail.

Securing Encrypted Data and Keys

Patient's medical data collected by a monitoring device is highly sensitive and must be secured against unwarranted access. In fact, failure to conceal the personal information might lead to legal action against the healthcare provider, not to mention financial and criminal penalties for noncompliance of HIPAA or other regulations. Therefore, the medical device attached to a patient's body must send out collected data in protected form. The standard approach is to encrypt the data with a secret key using a lightweight cipher, such as Speck or Simon. Hence, whoever owns the decryption key can decrypt and read patients' sensitive data. Additionally, the data may also be signed to ensure data integrity. So, if the signing key were to be compromised, an adversary could potentially tamper with the patient's data. It is then of utmost importance to make sure the decryption and signing keys are always kept protected so that they cannot be obtained by unauthorized persons.

A key can be considered safe within the boundaries of the medical device because extracting the key would require physical access to the device, expert hardware hacking skills, and a great deal of effort, which usually amounts to an infeasible task. Similarly, a key is usually safe on the cloud servers, because adversaries normally would not have access to the cloud data. The weakest link is the companion or proxy application running on the mobile device or desktop computer because these platforms are easily accessible and do not require complicated and expensive analysis tools or techniques to be hacked. A skilled hacker can quickly locate and extract the secret keys from the application code or device memory.

Authenticating the Client

When transferring sensitive personal information over a network, it is very important to make sure you are communicating with authorized parties on both ends of the connection. This is especially true for data involving private and medical information. As was discussed at the outset of this paper, very often healthcare devices and applications send encrypted data to remote servers over the Internet. The standard approach is to use standard network

[9] Your Electronic Medical Records Could Be Worth $1000 To Hackers (2017). Forbes. www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers

[10] Fake Clinton Medical Records (2016). FactCheck.org. https://www.factcheck.org/2016/08/fake-clinton-medical-records

encryption, such as Transport Layer Security (TLS). A naive security model would assume that implementing TLS is sufficient. However, solving the issue requires a more granular solution.

While this method ensures the client is communicating with the right server, the opposite is not easy to achieve. Namely, it is difficult to create a safe mechanism for guaranteeing the validity of the client. In order to do so, a client-side TLS certificate would have to be introduced, where the client's public key is stored on the server. This is relatively straightforward, although it requires proper key management to make sure the server has certificates it needs. The challenge is that the client device has to have a private key in order to authenticate itself to the server. Any entity that obtains that private key can masquerade as that device. Therefore, since attackers can potentially reverse engineer the application and extract keys, it is imperative that the client's private key be protected.

Protecting Applications Against Reverse Engineering and Tampering

A different attack vector is to analyze the code of the mobile or desktop application that is responsible for receiving data from the medical devices, and try to mount one of the following attacks:

- Find a vulnerability in the code that would allow malicious software running on the same device to manipulate the way the application works. For example, malicious software could potentially intercept and modify application API calls and hence manipulate data in transit. Or the software could read any decrypted files generated by the application in storage.
- Create a modified version of the application and distribute it as an alternative to the original. For instance, a competing company might create a modified replica and sell it at a lower price, which would damage the original vendor's bottom-line revenue. Or a cybercriminal could distribute a modified clone so that instead of the application performing the tasks originally designed for it, the application would actually perform malicious actions, such as stealing information from the mobile device, or worse, creating safety risks to patients' health.

Ensuring Compliance with Regulations

As was discussed above, there are a number of standards and regulations that influence modern medical applications, including GDPR, UL 2900-1, HIPAA, US Postmarket Management of Cybersecurity in Medical Devices, EU Medical Devices Regulation, In Vitro Diagnostic Medical Devices Regulation, ISO/IEC 27001 Information Security, and others. These and other regulations require medical application vendors to protect data and establish certain processes regarding ensuring system security. Although the requirements are usually generic without detailing low-level elements, such as cryptographic operations, they do recommend to regularly test applications and infrastructure for vulnerabilities and address the associated risks. This means that software security must be an integral part of the development cycle of medical applications, and sufficient effort must be put in place to ensure software protection and data security.

The Solution

At Intertrust Technologies, we have been following the advent of smart technologies from the very beginning, and have developed a set of software and data protection tools that address a vast range of problems associated with application-level tampering and data security. All the attacks described before can be effectively thwarted with our whiteCryption® technology that consists of tools described in subsequent sections.

whiteCryption® Code Protection™

Code Protection provides application developers with a comprehensive suite of anti-reverse engineering and runtime application security tools to protect your applications on all popular platforms. Code Protection is easy to use, provides a simple way to fine-tune the balance between code security and performance, and requires no significant changes to code or the existing build chain.

In the scenario described at the beginning of this paper, Code Protection would be used to harden the application running on the desktop computer and the mobile device that collects data from medical devices. Code Protection could also potentially harden software embedded into the medical device for improved security, especially if the device runs complicated code and has powerful hardware. As a result, it would be extremely difficult for the attacker to analyze and reverse engineer the software and the way it interacts with other parties. Any vulnerabilities present in the code would be almost impossible to detect. Even if the attacker tried to modify code, the built-in integrity checkers would immediately crash the application making the hacker's intent extremely difficult. Furthermore, protected applications can be configured to defend themselves against being run on rooted/jailbroken mobile devices where the attacker would have more freedom to analyze, modify and clone the application.

whiteCryption® Secure Key Box™

Secure Key Box is an advanced white box cryptographic library that protects cryptographic keys for critical security functions such as device authentication, secure communications, and data encryption. The main purpose of Secure Key Box is to protect secret cryptographic keys. With Secure Key Box, keys are never in the clear in use, in transit or at rest, preventing hackers from stealing your keys. Secure Key Box is used in a similar way as common cryptographic libraries, such as OpenSSL or LibTomCrypt.

By embedding Secure Key Box into the desktop or mobile application (or the medical device itself), you hide the keys it uses and prevent the attacker from extracting the keys for exploit. Secure Key Box supports a large set of standards-compliant cryptographic algorithms and functions. For instance, Speck is a cipher used on very small connected medical devices to encrypt data, such as health monitors and sensors used by patients. Secure Key Box supports this cipher, which means that you can use Secure Key Box with any application that deals with Speck-encrypted data and thus be sure the secret keys used in this communication are protected on both endpoints. Or you can use Secure Key Box functions to implement a proprietary network client to secure the client's end in communication with remote data servers located in the cloud, thus ensuring strong client-side authentication.

Why Choose whiteCryption?

Our products are backed by superlative support and professional services to help you achieve your business goals quickly and efficiently. Market leaders have deployed whiteCryption tools in mission-critical finance and medical device applications around the world. Our technology protects millions of devices and applications, securing sensitive information and crypto algorithms running in hostile environments; we extend the secure perimeter around applications beyond where traditional technologies have gone. whiteCryption is an important weapon in protecting you and your customers from unwanted intrusion and misappropriation of personal information and data.

Learn more about whiteCryption at
https://www.intertrust.com/products/application-shielding

About Intertrust Technologies

Intertrust provides trusted computing products and services to leading global corporations – from mobile and CE manufacturers and service providers to enterprise software platform companies. These products include the world's leading digital rights management, software tamper resistance and privacy-driven data platforms for software tamper resistance and private data sets for various verticals including energy, entertainment, fintech, healthcare, and IoT.

Founded in 1990, Intertrust is headquartered in Silicon Valley, with regional offices in London, Tokyo, Mumbai, Beijing, Seoul, Riga, and Tallinn. The company has a legacy of invention, and its fundamental contributions in the areas of computer security and digital trust are globally recognized. Intertrust holds hundreds of patents that are key to Internet security, trust, and privacy management components of operating systems, trusted mobile code and networked operating environments, web services, and cloud computing.

Additional information is available at intertrust.com, or follow us on Twitter or LinkedIn.

About whiteCryption

whiteCryption, a subsidiary of Intertrust Technologies, is a leading provider of application shielding solutions to prevent hackers from reverse engineering and tampering with code. We specialize in advanced obfuscation, runtime application self-protection (RASP), and white box cryptography solutions for mobile and desktop applications, firmware and embedded systems. whiteCryption protects the automotive, banking/finance, healthcare, and entertainment industries.

Copyright Information

Contact Information

Intertrust Technologies Corporation
920 Stewart Drive
Suite #100
Sunnyvale, California 94085, USA
https://www.intertrust.com