Applications for Hardware-Based Security in Healthcare

TABLE OF CONTENTS

APPLICATIONS FOR HARDWARE-BASED DATA SECURITY IN THE HEALTHCARE INDUSTRY

The healthcare industry is a nexus of sensitive information and criminals eager to exploit system weaknesses for personal gain. Social Security numbers, personal health records, and financial information are all transferred to, and stored by, healthcare organizations around the globe. Using hardware-based data security solutions, these organizations can confidently secure their records and sensitive patient information.

THE RISK: LARGE-SCALE DATA BREACHES

Healthcare organizations are often targeted by criminals and fraudsters who wish to gain illicit access to detailed data and records of a large number of individuals. Names, Social Security numbers, addresses, financial information, medical history — all of these are contained in personal health records and are highly valuable to those who wish to illegally profit from this information.

Studies performed in 2006 and 2012 by the World Privacy Forum, a non-profit research group, estimate the value of a single health record at 50 times the street value of a single financial record.[1] Furthermore, the mean total cost per incident amounts to an estimated $22,346 per record.[2]

Regulatory forces have set in motion efforts to streamline administrative processes by incentivizing the use of electronic health records. This has simplified many administrative tasks, and, in many ways, increased security and efficiency as well. These records can now be transferred instantaneously between entities and stored in vast repositories of data with automated off-site backups. If these records are not stored securely, the stage is set for massive data breaches of thousands, or in some cases millions, of patient records.

The news headlines tell the story: breaches are numerous and recent years have seen some of the largest breaches of protected health information (PHI) records to date.

In March of 2012, 280,000 Social Security numbers and 500,000 other personal records were compromised on Utah Department of Technology Services computer servers which housed records for the Utah Department of Health. A hacker traced to Eastern Europe was able to infiltrate the system through a weak administrative password. The breach involved both Medicaid patients as well as recipients of Children's Health Insurance Plan (CHIP) coverage. As a result, the Utah Department of Health offered victims of the data breach free credit counseling and monitoring.[3]

In 2009, a United States-based health insurer reported two unencrypted laptops stolen, resulting in the compromise of 1.22 million patient health records. These laptops contained member names, dates of birth, addresses, Social Security numbers and other protected health information.[4]

In one of the largest breaches on record, a contractor working on behalf of a major United States Department of Defense health insurance provider reportedly lost backup tapes containing personally identifiable and protected health information from the electronic health records of military beneficiaries. The tapes were reported stolen from a

[1] Dixon, Pam. "Medical Identity Theft: The Information Crime that Can Kill You." World Privacy Forum. 3 May 2006.
[2] "Third Annual Survey on Medical Identity Theft." Ponemon Institute. June 2012.
[3] Horowitz, Brian T. "Utah Health Care Data Breach Exposed about 780,000 Patient Files." eWeek.com. 13 Apr. 2012.
[4] Anderson, Howard. "AvMed Breach Now Affects 1.2 Million." HealthcareInfoSecurity.com. 3 Jun. 2010.

car while transporting data from one federal facility to another as part of required backup procedures. All told, more than 4.9 million records containing patient addresses, phone numbers, Social Security numbers and clinical data were compromised. To date, the contractor faces a $4.9 billion class-action suit seeking damages on behalf of the beneficiaries affected. The Department of Defense has also filed a separate suit seeking $4.9 billion in damages.[5]

The risks for healthcare organizations are high and the opportunities for attackers are numerous. A study conducted by the U.S. Department of Health and Human Services found theft of equipment made up 54 percent of breaches in 2012, followed by unauthorized access or disclosure for 20 percent, lost records and devices for 11 percent, hacking for 10 percent, and improper disposal resulting in 5 percent.[6]

In the past, information in the healthcare industry has been less vulnerable to the large-scale data breaches seen today because of the sheer difficulty of stealing thousands of paper documents. Now that records are held in massive, cloud-based repositories or transported in mobile devices or USB flash drives, security measures are more important than ever.

What's more, the complexity of healthcare infrastructure poses additional challenges in securing sensitive information. The exponential growth of mobile devices; large, increasingly cloud-based repositories of data; electronic transmission of data within and between entities; massive datacenters; complex institutional IT infrastructure; and physical security limitations of electronic devices all contribute to the overall complexity of securing data. Additionally, acquisitions of smaller healthcare providers with less robust security measures can provide a channel for attackers to gain access to the systems of larger providers.[7]

Beyond fulfilling government mandates, it is the industry's consensus that encrypting records and effectively training employees will go a long way in preventing unauthorized access to this sensitive information.

THE REGULATIONS

The healthcare industry is governed by a number of regulatory bodies and statutes whose aim it is to establish standards of care, operations, and security. Foremost among these regulations, and most relevant to data security and fraud prevention, is Title II of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. These laws exist in order to define and limit the circumstances in which protected health information may be used or disclosed by covered entities, standardize transaction procedures, establish reporting protocol in case of breaches, and define punitive measures in case breaches occur.

Within these two laws, protected health information is defined as:

> Individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. This information includes demographic data that relates to: the individual's past, present or future physical or mental health or condition; the provision of healthcare to the individual; the past, present, or future payment for the provision of healthcare; and that

[5] Vogel, Steve. "Tricare Military Beneficiaries Being Informed of Stolen Personal Data." Washington Post. 24 Nov. 2011.
[6] Mearian, Lucas. "'Wall of Shame' Exposes 21m Medical Record Breaches." ComputerWorld. 7 Aug. 2012.
[7] Sullivan, Tom. "Are Providers Ripe for a Massive Medical Records Heist?" GovernmentHealthIT.com. 14 Jan. 2013.

identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual including name address, birth date, and Social Security number.[8]

HIPAA

HIPAA regulations apply to covered entities and their business associates, who together have a written contract stipulating both the associate's purpose in being hired and their required compliance with the law.

HIPAA is comprised of two parts pertinent to data security and fraud prevention—the Privacy Rule and the Security Rule. The Security Rule of HIPAA complements the Privacy Rule and mandates security measures pertaining specifically to Electronic Protected Health Data (EPHI).

HIPAA contains what are referred to as "required" and "addressable" implementation specifications. Currently, data encryption is merely addressable, but widely regarded as a necessity in the current data security environment.

When healthcare organizations violate HIPAA privacy rules, the U.S. Department of Health and Human Services (HHS) establishes a resolution agreement with the organization. Under the agreement, the healthcare organization must perform certain obligations, not unlike a probationary period, including data security training classes for employees, making reports to HHS (typically for a period of three years), and paying fines.

HITECH ACT

The HITECH Act widens the scope of privacy and security protections available under HIPAA, increasing the legal liability for non-compliance and providing for greater enforcement of existing laws. The HITECH Act also establishes data breach notification requirements for unauthorized uses and disclosures of unsecured, or unencrypted, PHI. Additionally, the HITECH Act imposes mandatory penalties for "willful" negligence. Civil penalties for willful negligence have been increased, with fines up to $250,000 for single offenses and repeated or uncorrected violations increased to a maximum of $1.5 million.

In addition to these primary mandates, healthcare entities may also be subject to state and federal regulations pertaining to data security. In the U.S., nearly all states have enacted mandatory data breach notification laws and many other countries, as well as the European Union, have also put similar legislation into effect. Additionally, research funded by specific grants is often subject to security procedures enumerated by the granting organization.

OPPORTUNITIES FOR PROTECTION, PREVENTION, AND COMPLIANCE

NETWORK SECURITY

Network infrastructure in a crowded environment like a hospital is often complicated, cumbersome to monitor, and difficult to secure with only software-based tools. Network passwords can establish a baseline standard of security for

[8] "OCR Privacy Brief: Summary of the HIPAA Privacy Rule." Department of Health and Human Services, Office for Civil Rights. May 2003.

organizations; this prevents the casual passerby or user from accessing the network. However, this will not provide security against those who would willfully gain access to networks for malicious intent.

To ensure only authorized devices can access the network, a Public Key Infrastructure is necessary. Electronic equipment, personal mobile devices, or access cards can be digitally signed by a certificate authority to create a mutually authenticated network comprised of only trusted devices. Any device without proper credentials will automatically be prevented from accessing the network.

SMART CARD-BASED IDENTIFICATION

The management of credentials and digital identities is of the utmost importance in a healthcare environment. Credentials are used to limit physical access as well as access to sensitive digital information. Patients, staff, visitors and suppliers should all be issued digital identities. The cryptographic procedures involved with operating a card or identity issuance system can be performed using a hardware security module.

PREPAID CARDS

Employees, patients, and visitors often spend long hours in hospitals without leaving. For the convenience of these groups as well as the benefit of the healthcare organization, closed-loop prepaid cards provide an ideal, mutually beneficial solution. Prepaid cards can be loaded with funds for use in the cafeteria, vending machines or other monetary exchanges, and periodically reloaded with funds for repeated use.

ELECTRONIC PAYMENTS

Hospitals and large healthcare providers conduct countless transactions per day, exchanging sensitive financial information each time. These transactions occur between patients, other medical entities, insurance providers, and suppliers. Solutions are needed to prevent would-be hackers from accessing this information in-transit, from the point of sale until it is validated by the payment processor.

For healthcare organizations with infrastructures large enough to merit self-management rather than outsourcing, point of sale terminals can be injected with encryption keys. These keys can be used for encrypting PINs, Primary Account Numbers (PAN), and other data. Once payment information is accepted, it can be transferred to the payment processor, where it is decrypted within the secure boundary of a hardware security module and subsequently validated.

RESEARCH DATA

Medical research is a huge undertaking, sometimes spanning decades and costing countless millions of dollars. Because of this, research data is a prime target for those who wish to circumvent this process through espionage by government, corporate, or activist entities, or sabotage the efforts of the researchers and the institutions that funded them.

Within the scope of research data, is it important that sensitive information is never stored or transmitted in the clear. Additionally, the authenticity and integrity of the information transmitted must be verifiable at all times. With this in mind, a public key infrastructure (PKI) established by a certificate authority is recommended to encrypt and digitally sign research data.

WHY HARDWARE-BASED SECURITY?

Encrypting and authenticating sensitive data using a secure cryptographic device offers unparalleled benefits for maintaining security, preventing fraud, and ensuring regulatory compliance. Hardware security modules implemented in a healthcare environment are dedicated devices built to protect data using physical, logical and encryption-based security features. These tamper-responsive devices are designed to house encryption keys within a secure boundary, eliminating risks commonly associated with software data security tools.

Additionally, hardware security technology can offer advanced disaster recovery and redundancy features — functions that guarantee continued operation in the event of an unplanned outage. For organizations maintaining records in widespread use on a 24x7x365 basis, this reliability is a necessity.

Hardware-based encryption provides a secure, reliable means of protecting data and is currently implemented in a broad range of applications across multiple industries. By implementing advanced encryption technology, healthcare organizations can enhance their reputation for protecting patient information, reduce or eliminate the cost of data breach responses, and prepare for anticipated future regulatory requirements.

FUTUREX ENGINEERING CAMPUS
OFFICE: +1 830 - 980 - 9782 TOLL FREE: 800 - 251 - 5112
864 OLD BOERNE ROAD, BULVERDE, TEXAS, USA 78163