WHITE PAPER
Premises-Aware Security
Healthcare IT

Premises-Aware Security Mitigates Healthcare Data Breaches

Wireless Credential Exchange-embedded RFID tag helps safeguard protected health information by enabling security policy enforcement based on device location

We need premises-aware solutions so we know what's happening with our data and where it's going.

– Karl West
Chief Information Security Officer
Intermountain Healthcare

Chris Gough
Lead Solutions Architect,
Intel Health and Life Sciences

Shahrokh Shahidzadeh
Senior Principal Technologist, Intel

Executive Overview

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires healthcare organizations in the United States to prevent unauthorized access to their patients' electronic protected health information (PHI). When PHI is compromised, these organizations can be fined millions of dollars, have their reputations damaged, and lose their patients' trust. The primary causes of security breaches are lost or stolen devices and unauthorized access to PHI or applications that can compromise PHI.

To help mitigate the risk of security breaches in healthcare, Intel is exploring a premises-aware security capability that enables an organization's IT department to monitor all devices, receive alerts if a device leaves a secure zone, and control access to data and applications using location-based security policies, including forced encryption or self-wipe.

The key component to premises-aware security is a Wireless Credential Exchange[1] (WCE)-embedded radio frequency ID (RFID) tag with enhanced security and privacy features connected to Intel's system on a chip (SoC).

Business Challenge

Security breaches in the healthcare industry are costly to an institution's reputation and its balance sheet. Many of these breaches result from two scenarios:

- A company- or employee-owned device containing unencrypted protected health information (PHI) gets lost or stolen, compromising the PHI that's stored on it.
- A hospital employee accesses patient records without having a legitimate medical reason for doing so.

Mitigating the risk incurred in these scenarios can help healthcare institutions better protect PHI and their reputations.

Implications of Breaches to Healthcare Organizations

Data security breaches in healthcare are on the rise. Between 2010 and 2012, one study found that 94 percent of healthcare organizations had at least one security breach, and 46 percent of those breaches were the result of a lost or stolen device.[2] The average cost of data breaches to healthcare organizations in 2012 was USD 5.4 million.[3]

Table of Contents

Additionally, healthcare organizations can lose revenue when their reputations are damaged. If a breach affects 500 or more individuals, the organization responsible must report the breach to the U.S. Department of Health & Human Services (HHS). Every patient and prospective patient can learn about the breach because the HHS posts these breaches online.

Lack of Control: Data, Devices, and Applications

Any mobile device that contains a deployed database, a spreadsheet, text message logs, or photos related to PHI is especially susceptible to a breach because mobile devices are easily lost or stolen. The loss or theft of a mobile device that contains unencrypted PHI is considered to be a security breach, whether that device is company or employee owned.

Other devices are also subject to breaches through loss, theft, or improper decommissioning. Without certification that servers, PCs, wall-mounted clients, copy machine hard drives, and other devices have been properly decommissioned, they may be categorized as lost and therefore considered to be security breaches.

In addition to lost or stolen devices, unauthorized access to data or applications also contributes to security breaches. For example, if clinicians collaborate using message applications that are native to their devices, the messages are not encrypted. Any PHI mentioned in the messages is at risk. These kind of applications need to be disabled and replaced with secure, IT-approved alternatives.

Protecting Patient Privacy

Although protecting PHI is a high priority, it is important to implement security measures that do not compromise patient care or employees' personal privacy. While devices that contain PHI pose security risks, their primary purpose is to help healthcare organization employees—doctors, nurses, and administrative staff—provide efficient, high-quality patient care. Efforts to stem security breaches need to take this into consideration and fit seamlessly into employees' workflows. Employees will more readily accept a solution that does not require multiple logins or take too long to access the data necessary to help patients. If a solution is too difficult to use, employees may devise unauthorized workarounds to improve efficiency.

For BYOD users, there is the matter of privacy and protecting personal information. The ability to enforce policies on a BYOD user's phone or tablet, and to limit the data and applications those devices can access, needs to happen without invading an employee's privacy. This approach will make a solution more acceptable to employees and protect the organization from liability in the event of a security breach.

Solution

Intel and its collaborators from other organizations have been evaluating an advanced premises-aware security capability to help healthcare organizations mitigate data security breaches. Some of the hardware components are already in devices available in the market. However, some aspects of the solution are still under development, such as the software required for policy orchestration.

The solution described below validates the benefits that healthcare organizations can realize with premises-aware security. By using premises-aware security to mitigate security breaches attributed to loss and theft of devices and unauthorized access to PHI, healthcare organizations can improve security, avoid costly fines, and put patients at ease.

Premises-Aware Security: Definition and Benefits

Premises-aware security establishes a protected zone, or geofence, around a facility, such as a hospital or a specific ward within a hospital, where access to data and applications can be customized depending on which zone a device is located in. When the device is removed from the protected zone, it is automatically secured, and IT may receive alerts through an early warning system in response to suspicious events (for example, a nonmobile device being removed from the hospital).

Enabling premises-aware security requires both hardware and software to establish the secure zone; monitor and control devices, data, and applications; orchestrate location-based security policies; and enforce those policies, including remotely deleting all data or triggering a self-wipe protocol if a breach event occurs.

The solution detects when a device transitions between defined zones and can determine the device's location even if it is turned off. Encryption-level security is always present and enforced when a device is removed from a secure zone (for example, removed from the hospital). The administrative server that is monitoring the device records audit logs to determine where a device has been, who has accessed it, and whether its data may have been compromised. These reports support compliance activities and are vital to any investigation into a potential data breach.

The infrastructure that supports premises-aware security will also support other processes that can help improve the efficiency of patient care:

- **Streamline login processes.** When a device is aware of its location and in a secure zone, employees have to enter only operating system credentials to gain access to the device, bypassing whole disk encryption (preboot) authentication.
- **Autopopulate patient charts.** As part of a more robust solution based on a real-time location system (RTLS), an electronic health record application can autopopulate the patient chart when the employee brings the device within a predetermined distance of a patient wearing an RFID wristband.
- **Track patients and assets.** RFID readers installed throughout a hospital or clinic can monitor a patient's location by reading the RFID tag in a patient's ID bracelet. They can also track medical equipment by reading an affixed RFID tag. Staff can monitor the location of patients and equipment on a mobile device interface.

Hardware Components

The key to premises-aware security is WCE. WCE is an SoC-embedded RFID tag with enhanced security and privacy features. Because WCE uses passive RFID technology, it does not require any battery power. Even if a device is turned off, RFID readers can still read the tag.

The RFID tag can share a single microchip along with the processor, memory interface, and graphics. Intel's SoCs have an interface to connect an RFID tag with secure storage, which enables premises-aware security. The dual-ported access capability of WCE enables the secure storage of encryption keys, certificates, and code.

Original equipment manufacturers that want to enable premises-aware security in their devices can add an RFID tag to the device based on Intel's reference design. But premises-aware security must also work with non-integrated legacy devices. To make that happen, healthcare organizations can use an RFID-integrated USB plug-in to make a device location-aware.

Enabling premises-aware security requires both hardware and software to establish the secure zone.

IT relies on security policy orchestration software to customize location-based policies for different zones.

Establishing the secure zones in a building requires RFID readers. RFID readers range in size from smartphone attachments to stationary doorway portals to room-wide sensors. The type of sensors needed for a premises-aware security solution depends on the way the zones need to be configured to support the desired use cases. For example, Figure 1 illustrates a scenario with multiple secure zones and policies.

Software Components

After devices have integrated either RFID capability or USB plug-ins and RFID readers have been installed, asset-tracking and security policy orchestration software allow IT to enforce a premises-aware security solution. Asset tracking and RTLS software monitor the location of all devices. If a device leaves the secure zone, the device's owner and IT may receive an alert through an early warning system. The same system alerts IT if a device is within the secure zone but is no longer detected. For example, an employee accidentally places a metal tray on top of a device, unintentionally shielding it from the RFID sensors.

IT relies on security policy orchestration software to customize location-based policies for different zones. For the scenario represented in Figure 1, policies may include the following:

- **Asset tracking.** When a device leaves its zone or becomes undetectable, it may automatically turn off and trigger the early warning system. If IT determines that the device was stolen, IT can render the device unbootable until able to unlock it or remotely wipe the device of all PHI.
- **BYOD control.** While a device is located in a specific zone, allow access to only an approved set of applications (for example, the software blocks access to SMS and allows clinicians to collaborate with an IT-approved messaging application). When the device leaves the specific zone, access to the device's applications is restored.
- **Application and data control.** The software monitors the access of all employees to patient PHI. If an employee accesses PHI from an unexpected location, he or she receives a prompt to confirm whether the access is required for a specific clinical need. The software allows access to PHI, but notes the interaction and holds it for auditing.
- **Management of multiple policies.** The software allows varying levels of access depending on an employee's need. For example, while a clinician may need access to a patient's PHI from multiple zones, a billing manager needs access only while working in a single zone.

An RTLS can provide a secondary functionality of tracking patients using the RFID tags in their wristbands. The same software might someday be used in conjunction with software from an electronic health record company that autopopulates a chart when a physician or nurse is within a predetermined distance from an assigned patient.

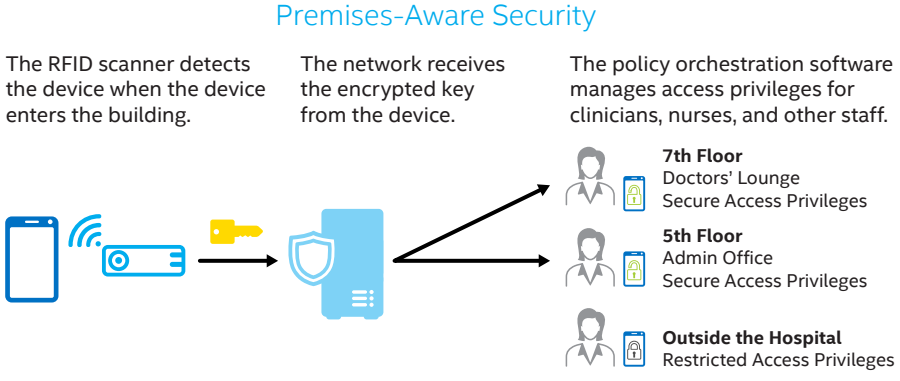

Figure 1. Our premises-aware solution establishes secure zones in a building to monitor devices and application access. If a device leaves its assigned zone, an early warning system can alert IT that the device is no longer being monitored, and various options become available depending on the applicable policy.

Testing Premises-Aware Security with a Healthcare Organization

In 2013, Intel became one of the founding members of the Intermountain Healthcare Transformation Lab, located on the campus of Intermountain's flagship hospital in Murray, Utah. Intel and Intermountain tested the premises-aware security capability to validate its usefulness in a clinical environment.

Methodology

In early 2014, the Transformation Lab set up three zones to test five use cases:

- **Locked in-transit.** Device encryption is enforced when the device leaves the hospital premises.
- **Early warning system.** IT receives a notification when the device, such as a nonmobile PC, leaves the hospital premises under suspicious circumstances.
- **Location-based security policy.** IT applies custom security policies to a device depending on where it is located.
- **RTLS.** Medical equipment can be located on demand from a mobile device interface.
- **Centralized compliance and auditing support.** IT is able to query an administrative server that has been tracking the device for audit logs; those logs are proof that no breach has occurred.

Four passive RFID readers monitored three devices: an RFID-integrated tablet, an RFID-integrated laptop, and a laptop using a USB plug-in.

Results and Feedback

Feedback was generally positive with most end users recognizing the need for premises-aware security to protect their privacy, patient PHI, and the healthcare organization in general. Some users reported wanting to see the capability implemented facility-wide. Some suggested extending the solution to other use cases, including the following:

- Help track large numbers of new patients, such as during mass casualty events.
- Monitor the location of patients who are under suicide watch.
- Help clinical team members find each other in a hospital setting.
- Track patients and trigger an alert mechanism when they return to their room or leave the premises.

According to Karl West, the chief information officer at Intermountain Healthcare, "We need premises-aware solutions so we know what's happening with our data and where it's going. Tracking data in that BYOD environment is critical moving forward. Having tools and strategies and understanding where the data is going is key."

Premises-Aware Security Use Cases Beyond Healthcare

The three fundamentals of premises-aware security—asset tracking, application control based on location, and data breach control—apply to all industries. From government to retail to movie theaters, there are many use cases where premises-aware security can control devices, protect consumer privacy, and reduce liability for organizations.

In some U.S. government buildings, such as the Pentagon, enclosed areas called Sensitive Compartmented Information Facilities (SCIFs) exist where highly sensitive or classified information is analyzed. Premises-aware security would help protect this information by monitoring all devices located in a SCIF and sending an early warning alert to IT if a device is lost or stolen. Also, location-based security orchestration allows IT to disable a device during the time that it is located in the SCIF. The capability to limit access to sensitive data and applications only in specific SCIFs is also valuable.

Mobile point-of-sale (POS) devices in a retail setting contain large amounts of personal consumer information. Well-publicized breaches have occurred where an employee or malicious attacker has walked out of a store with a POS device or placed rootkit malware on the device to access every card's chip and PIN that is stored on the device. Premises-aware security prevents a device from leaving a store unencrypted. If a device is lost or stolen, location-based security policies can be implemented to remotely delete all of the data. Finally, only authorized employees working in a specific location would be able to use the device or access the data on the device within the secure zone established at that location.

Premises-aware security also works in movie theaters, where cameras can be disabled and volume levels on ringtones can be controlled. In education, social media applications could be blocked when devices are in classrooms.

The need to be able to control device, application, and data access based on location intensifies as smartphones and other mobile devices become more powerful and ubiquitous. Using passive RFID technology on an energy-efficient, affordable system on a chip is a viable pathway to implementing premises-aware security.

Conclusion

We believe that the premises-aware security solution can give healthcare organizations the ability to lower the risk of PHI security breaches. With WCE, IT can monitor devices to detect how they are being used and who is using them within different zones in a healthcare facility.

Through location-based security orchestration polices, IT can set up an early warning system to determine when a device leaves a secure zone under suspicious circumstances, enforce encryption when the device leaves the zone, and remotely wipe all PHI if the device is stolen.

Once the infrastructure of WCE-enabled devices, RFID sensors, asset-tracking, and RTLS is built out, healthcare organization staff will be able to improve the patient care experience by speeding up hospital rounds through autopopulating charts, pinpointing patients' locations based on the RFID tag in their location-aware wristband, and tracking nonmobile assets through an RFID tag affixed to the equipment.

For Related Information

- "Getting a Headstart on Location-based Services in the Enterprise"
- Healthcare Blogs

Visit **intel.com/healthcare** to learn more about Intel solutions for healthcare and life science.

[1] Wireless Credential Exchange (WCE) was previously known as Processor Secured Storage (PSS) enabled by Impinj's Monza* X supporting both I2C and RF communication.

[2] Ponemon Institute, "Third Annual Benchmark Study on Patient Privacy & Data Security." http://www2.idexpertscorp.com/assets/uploads/ponemon2012/Third_Annual_Study_on_Patient_Privacy_FINAL.pdf

[3] Ponemon Institute, "2013 Cost of Data Breach Study: Global Analysis," May 2013. https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

Printed in USA 0714/CGOU/KC/PDF ♻ Please Recycle

intel Look Inside.™