HIMSS18 The leading health information and technology conference

WHERE THE WORLD CONNECTS FOR HEALTH

Conference & Exhibition | March 5–9, 2018

Las Vegas | Venetian – Palazzo – Sands Expo Center

Improving RFID in a Healthcare Environment

Session 245, March 8, 2018

Mitchell Parker, Executive Director, Information Security and Compliance, IU Health

COMMITMENT

www.himssconference.org

#HIMSS18

Conflict of Interest

Mitchell Parker, MBA

Has no real or apparent conflicts of interest to report.

Agenda

- Explanation of RFID
- Healthcare Use Cases/Potential Use Cases
- Privacy and Security Concerns
- What Risks are We Guarding Against?
- Foundation – Infrastructure and Processes you need
- Implementing RFID on top of Foundation
- Expected Benefits

Learning Objectives

- Demonstrate understanding and appreciation for the fundamentals of RFID technology
- Apply the knowledge gained to better secure existing RFID implementations
- Assess RFID-based technologies for appropriate privacy and security protection
- Describe future RFID technologies and how they can influence the healthcare environment

What is RFID?

- Radio Frequency Identification
- Wireless transmission of information from a transponder (tag) to a reader without visibility
- Transfers can be bidirectional
- Tags can be attached, implanted, or built into a device
- Designed to supply data to/from data collection systems
- Also designed to identify and authenticate users (contactless smart cards)

What is RFID?

- Can be Active or Passive
  - Passive –
    - No Internal Power Source – powered by signals
    - Low Price per Tag
    - Wide variety of form factors and uses
    - Can be used for transactions/ID
      - Philips MIFARE technology
      - Does support encryption (ISO 14443-4 standard)

What is RFID?

- Can be Active or Passive
  - Active –
    - Battery-powered tags
    - Broadcast their own signals
      - Either in response or by “beaconing”
    - Much longer range
    - Higher cost ($20-$100 per device)
    - Generally used for high-value items

What is a specific example?

- RFID-enabled toll cards (NXP MiFare)
  - Better known as the SmarTrip (DC Metro), PATH SmartLink (Ny/NJ), CharlieCard (Boston), or BreezeCard (Atlanta)
  - Over 1 billion of these cards in use since 2002 to provide contactless and effortless entry to public transportation
  - Instead of bulky tickets or machines that can break, RFID is used instead to provide a simple solution
  - This means millions of cards in use daily not only in the US, but across the world

Healthcare Use Cases

- What are the benefits and why should I use it?
  - RFID uses radio signals. Barcodes or other visual inspection methods require line of sight
  - RFID has nearly indestructible sensor implementations
    - Barcodes or visual methods can break or fade easily
  - It is easier to scan using a receiver than sending people out
  - You don’t need to put sensors in controlled areas that require sterilization
    - Reduce infection and sterilization risks!

Healthcare Use Cases

- Asset Management and Inventorying
  - Very critical for HIPAA compliance of IT assets
- Equipment Tracking
  - Surgical Equipment Management and Tracking
- Physical Security Access/Door Access/Security Systems
- Real-Time Location Services (along with Wi-Fi and other means)
  - Baby Tracking
- Authentication (tap and go cards)

Potential/Future Use Cases

- Implantable Devices
  - Can give more than just an ID number
  - As implants get more sophisticated, give complex status results whenever queried
  - Make it significantly easier to query them

Potential/Future Use Cases

- Contactless Payments in Healthcare
  - PCI compliance is a challenge for many organizations
  - RFID can increase complexity and decrease security unless done right
    - Many retailers are looking at contactless payments
    - Patient satisfaction and engagement starting to use this
  - What we want to do is provide a baseline that can be used to secure both PCI and RFID

Potential/Future Use Cases

- Tap & Go Logins for patients
  - Patients using these logins for portals, food service, or self-service for appointments and services
  - Streamlining patient experience
  - Saving money by providing more services automatically
  - However, if you implement them correctly, you lower the risk while providing a better experience

Privacy and Security Concerns

- RFID has a bad reputation for privacy and security
  - Perception that people will read information out there without being traced and cause ID theft
  - A number of vendors making RFID-proof wallets to protect credit cards and passports
  - Android Cell Phones modified to steal contactless credit card info using NFCProxy application
  - DEFCon 25 showed that it's possible to spoof credit cards using cheap dedicated hardware (UniProxy)

Privacy and Security Concerns

- There is the potential of being able to clone RFID tokens for physical or computer system access
- There is the potential for spoofing IDs for fraudulent inventorying
- Internet of Things/Automation security issues
- Security not built into RFID natively
- Due to lack of security, easy to forge/clone information

What are we guarding against?

- Spoofing of RFIDs
- Unauthorized copying/interception of RFIDs
- Interception of data
- Attacking back-end processing systems
- Network-based attacks
- Device-based attacks

What are we guarding against?

- Supply Chain Attacks
  - Generally, Supply Chains use a large number of handheld and wireless devices
  - Many of them run Android or older versions of Linux
    - Some devices even run Windows CE
  - Easy to attack or intercept traffic on devices not patched for recent vulnerabilities
  - Easier to attack networks and systems not designed for security

What are we guarding against?

- Supply Chain Attacks
  - Back-end systems for Supply Chain, specifically Inventory Management and Enterprise Resource Planning, also have a large number of vulnerabilities
  - ERP systems in particular are often wide open
  - They are a major driver of automating the complexity of hospital supply chain management
  - RFID has a potential to cause corruption of financial/inventory/asset management systems

What are we guarding against?

- Interception of patient information
  - As medical devices and implants start to use RFID, the potential for device association with a patient increases
    - Already a concern with surgical device and tool tracking
  - We need to isolate by design patient information from RFID readers and devices as much as possible to reduce risk
  - Address concerns with association of devices and tools to patients

What are we guarding against?

We need to have forensically sound data flows

- We cannot protect against attacks if we don't have a full understanding of them
- We need to understand where information can be compromised and where to protect it
- We need to know where to look for discrepancies and why
- If there is an issue, we need to document it and show defensible processes to assure integrity, confidentiality, and availability of data

What are we guarding against?

- We cannot stop the unauthorized reading of RFID tags or information
  - However, we can limit the association of these tags with patient information – esp. with ID cards
  - We can protect the systems that store and process the data
  - We can make it harder to spoof or inject bad data by segmenting off data collection
  - We can also make it harder by maintaining systems and being vigilant about reviewing data input

Foundation – What You Need

- Processes
  - Asset Management – Know What You Have
  - Systems Management – Maintain What You Have
  - Systems Design – Design isolation and minimum necessary communications into the network
  - Vulnerability Management – Address Their Vulnerabilities
  - Physical Security – Protect the Environment

Asset Management

- RFID is a major part of asset management
- However, we need to know what devices we have that can read/write RFID tags
- We also need to know what devices and systems will store or process this data
  - We need to know their capabilities
  - We need to log and audit transactions they make
- We need to know what we have to protect it because unmanaged devices can lead to multiple issues

Systems Management

- It's about managing the entire ecosystem identified by Asset Management
  - Every security framework and standard requires this as a base
- Make sure that we manage these systems to keep them up to date
- Maintain them and keep them supported
  - A lot of data collection equipment isn't kept up to date
  - A lot of equipment sold into the Supply Chain market runs out of date software
- Plan for Obsolescence

Systems Management

- Map out the data flows from devices and tags all the way to the systems of record that will be storing and transacting collected information
  - Store the minimum necessary information on the tags
  - Don’t store information that can directly relate to a patient in the data collection systems
    - **Do not associate** RFID tags with patient info in any way!
    - Store them in the EMR or system of record
    - If you have to use indirect associations through a data warehouse, it’s better to do so

Systems Management

- Asset Management
  - A lot of IT Asset Management (ITAM) systems rely on manual entry for locations
  - So does Active Directory or other Directory Services
  - Linking RFID-based asset tracking to ITAM removes a significant amount of work that needs to be done to keep inventory locations current
  - Solves for the location tracking component

Systems Design

- You need to design to several objectives:
  - Segment off data collection traffic from everything else
  - Enforce data flow through appropriate network paths
  - Protect data at rest and in transit using encryption
  - Validate and verify data inputs and collection through auditing and reporting
  - Retain Data for only as long as you need it and nothing more

Systems Design

- If these are used as patient ID cards for services, make sure that all the card has is the Patient ID
- Make sure to use a PIN or similar secondary authentication mechanism to protect the login
- Keep the authentication system separate from the patient data
- Do not store authentication data with patient records!

Systems Design

- If you use RFID for transactional smartcard logins, you need to do the following:
  - Maintain your own verifiable internal certificate authority for those certificates
  - Have a plan to periodically re-issue certificates at least once every two years to keep them up to date
  - Keep a Certificate Revocation List for terminated staff members
  - If there are any default encryption keys or passwords, change them!

Systems Design

- More on Certificate Management for all RFID devices
  - Have a deployment process that deploys to each device
    - Even though it may be convenient, don't re-use certificates
      - If you own one you own them all
    - Use a dedicated network to register certificates
  - Be able to manage, rotate, and revoke device certificates
    - Vendors like Fornetix offer solutions that work at scale and are in use in the automotive and utility industries now for millions of IoT devices

Systems Design

- Contract Management
  - Your contracts with vendors need to cover who will be doing what to maintain systems
  - They need to address who will be maintaining systems
  - They need to address clear delineation of responsibilities and actions
  - Keeping systems current, updated, and risk mitigated to an acceptable level needs to be in there

Systems Design

- Network Design
  - Isolate all data collection and acquisition networks
    - Only allow minimum ports & protocols for communication
  - Make sure that your network design enforces proper data flows
  - Scan all traffic coming in and out of the network
  - Make sure that there is either network-based or device-based protection for all devices on the network
  - Ensure that only your devices are on it using Network Access Control

Vulnerability Management

- For all identified assets, make sure that they are supported by the vendor with security patches
  - Android is only supported well by a few vendors
- Know where to get the patches from
- Have operational plans to patch devices as part of business on a periodic basis – at least monthly
- Have downtime procedures to operate in case of a computer systems failure
- Have vendor contacts to address any issues encountered

Physical Security

- With RFID, this becomes very important
- For tap and go – have enclosures to reasonably protect against signal interception
- Physically lock down and protect readers and other fixed devices
- Make sure buildings and warehouses protect against outsiders scanning from the outside
- Have a good physical security program with surveillance, guards, cameras, and environmental design to deter potential interception

Risk Assessment

- Pull it all together with a comprehensive annual risk assessment
- Address these 5 key components with it
- Develop a security and mitigation plan to address open issues
- Continually address open issues
- Continually address vulnerability management
- Keep system current and supported

Implementing RFID

- We need to address several areas:
  - Use Cases
  - Policies/Procedures
  - Budgeting
  - Communication Plan
  - Staffing and Training
  - Monitoring

Use Cases

- Develop documented use cases for the complete data lifecycle of information collected via RFID
- Use only minimum necessary data
- Develop a security plan to address the 5 key areas we discussed
- Have your network enforce the data flow
- Physical Security is a must

Policies/Procedures

- Your organization needs well-developed policies and procedures to directly address RFID implementation through:
  - Intake Process
  - Governance
  - Maintenance
  - Asset Management and Disposal
  - Access Management and Security

Budgeting

- Budget for staff to secure and monitor the implementation
- Do not assume that there is no IT involvement – this involves securing all IS systems that interface with it
  - Budget to improve security and resiliency for all systems
  - You need staff to continually secure and monitor for anomalous behavior and potential fraud esp. with patient info!
  - You need to make sure you have staff to address vulnerabilities
  - This is not one and done – it needs care and feeding

Communication Plan

- Be open about what you're doing and why
- Talk about the benefits of RFID and how it will improve the organization
- Be direct about customer concerns
  - Discuss the privacy and security measures you're addressing
  - Discuss the physical security concerns
  - Disclose the data elements you're collecting
  - Show how you're isolating them from patient data

Communication Plan

- Involve the Medical Staff
- Discuss how RFID can impact the workflow
- Formulate a process by which new RFID products can be evaluated and security issues addressed
- Address their patient safety concerns

Communication Plan

- Be open and communicate with your patients about what you're doing
  - Training plans for staff need to include a privacy and security section that explains minimum necessary
- Explain how you're protecting patient information and that it will not be available over RFID
- Explain that you've implemented multiple levels of countermeasures
- Make sure Consent forms include RFID scanning disclosures when necessary

Staffing and Training

- All staff that use these systems will need good privacy and security training
- They will also need comprehensive training on system usage
  - You want to avoid workarounds that can compromise security
- Train to build engagement and rapport around organizational improvement
  - Do not be heavy-handed on security – no fire/brimstone!
- Make it clear, understandable, and affirmative

Monitoring

- You need staff to monitor these systems
- They need great training
- They also need to be doing this as part of a defined task, not a ”throw-in”
- They need good reports and data that show potential anomalies
  - If handling anything patient-related, this is a potential requirement!
- Good supporting organizational structure for reporting issues and vulnerabilities to the right people
- Always work to keep them engaged

Monitoring

- Physical Security is also important!
- Like credit card readers, always inspect and check readers for tampering
- Have good surveillance, physical design, and guards to monitor storage areas
- Know who to call if you have a issue or case
  - Law Enforcement
  - Physical Security

Expected Benefits

- Proper implementation of this technology will allow:
  - Real-time location of assets
  - Real-time inventorying of assets
  - Potential real-time location and workflow tracking of patient-related assets
    - Surgical equipment and supplies (think checking for sterilization or maintenance)
    - Wheelchairs, carts, and other patient-related items
    - Less misplacement of items and more efficiency

Expected Benefits

- Real-time physical location of PC and computing assets
- Map to exact physical location
- Less work to maintain inventories and locations of devices
- Potential to include mobile computing assets such as flash drives
- Increased compliance with HIPAA Security Rule

Expected Benefits

- Demonstrable security plan and path
- Can greatly assist with regulatory and voluntary compliance
  - GDPR
  - HIPAA/HITECH
  - PCI-DSS
  - American Institute of Certified Public Accountants
  - Multiple standards for inventorying and checking

Expected Benefits

- Remove the hype
- Focus on definable tasks that need to be completed
- Address security and privacy in depth and with processes, not through point solutions
- Provide a program framework you can take back and implement at your institution

Questions

- Thank you and please complete your online session evaluation!

- Mitchell Parker, MBA, CISSP
- Mitchell.parker@iuhealth.org
- 317 963 5577(office)
- 317 719 5531 (cell)

Indiana University Health