Smart PKI for Healthcare Provider Organizations
Medical Device Security

Session # 183, February 22, 2017
Mike Nelson, VP of Healthcare Solutions, DigiCert
Karl West, CISO, Intermountain Healthcare
Speaker Introduction

Mike Nelson
VP Healthcare Solutions
DigiCert
@mike_k_nelson

Karl West
Chief Information Security Officer
Intermountain Healthcare
Conflict of Interest

Mike Nelson and Karl West have no real or apparent conflicts of interest to report.
Agenda

• Current state of medical device cybersecurity

• What are manufacturers doing?
  • Building security in from the beginning
  • Solutions being deployed:
    • PKI 101 – What is it, why is the healthcare community turning to it?
    • PKI Solutions – What security solutions does PKI offer?

• What are healthcare providers doing?
  • Medical device risk assessment
  • Legacy device strategy
  • Procurement strategies
Learning Objectives

• Analyze how a major network of clinics and hospitals uses PKI to authenticate connected medical devices at every endpoint.

• Recognize the right questions to ask and best practices for handling the procurement process to ensure medical devices are actually secure.

• Identify effective methods of prioritization and risk assessment being used by other major healthcare networks that you can apply to your organization.
Treatment/Clinical

- Ensure patients being treated by connected technology have an assurance of safety & security

Electronic Secure Data

- Risk assessment essential to successful deployment
- Changing mentality from compliance to data stewardship
- Healthcare providers and device manufacturers share responsibility
- Technologies such as PKI can help with preventative stance
- Proactive security = better patient care, engendered trust
## Benefits vs. Risks of IoT Devices in Healthcare

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous patient monitoring</td>
<td>Patient health and safety</td>
</tr>
<tr>
<td>Enhanced care options</td>
<td>Loss of PHI</td>
</tr>
<tr>
<td>Capture early warning signs of health problems</td>
<td>Network attacks</td>
</tr>
<tr>
<td>Collect health-related “big data”</td>
<td>Legal</td>
</tr>
<tr>
<td>Monitor device performance</td>
<td>Reputational</td>
</tr>
</tbody>
</table>

- **Benefits**
  - Continuous patient monitoring
  - Enhanced care options
  - Capture early warning signs of health problems
  - Collect health-related “big data”
  - Monitor device performance

- **Risks**
  - Patient health and safety
  - Loss of PHI
  - Network attacks
  - Legal
  - Reputational
Heightened Awareness of Cybersecurity

- Executive Order (13636) - Improving Critical Infrastructure Cybersecurity
- Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience
- NIST Cybersecurity Framework (2014) - Standards, guidelines, and practices to protect critical infrastructure
- Executive Order (13691) - Promoting Private Sector Cybersecurity Information Sharing
- Content of Premarket Submissions for Mgmt. of Cybersecurity in Medical Devices (2014)
- FDA Postmarket Management of Cybersecurity in Medical Devices (2016)
Medical Device Hacks...

- **VA Cath Lab Closed** – Malware infected (2010)
- **Jay Radcliff** – Hacking of insulin pump (2011)
- **Barnaby Jack** – Insulin Pumps & Pacemakers (2012)
- **Billy Rios** – Hospira Infusion pump (2014)
- **Scott Erven** – Most devices lack of authentication, encryption & use default passwords (2014)
- **Scott Erven and Mark Collao** – Set up “honeypot” on hospital network (2015)
- **MedSec and Muddy Waters** – Short sell SJM stock (2016)
- **Jay Radcliff** – J&J partners to hack insulin pumps & notify patients of vulnerabilities (2016)
FDA’s Guidelines for Postmarket Management of Cybersecurity in Medical Devices
Cybersecurity Throughout Product Lifecycle

“Manufacturers are encouraged to address cybersecurity throughout the product lifecycle, including during the **design**, **development**, **production**, **distribution**, **deployment** and **maintenance** of the device.”

*Source: Postmarket Management of Cybersecurity in Medical Devices, FDA, Dec. 2016*
Routine Updates and Patches

“The majority of actions taken by manufacturers to address cybersecurity vulnerabilities and exploits, referred to as “cybersecurity routine updates and patches,” are generally considered to be a type of device enhancement for which the FDA does not require advance notification or reporting.”

Cybersecurity Approaches

- Medical device risk assessments
- Responsible disclosure policies
- Vulnerability sharing with NH-ISAC
- Physical controls
- Public key infrastructure (PKI)
- Segmentation
- Traffic monitoring
- Other compensating controls
Public Key Infrastructure (PKI) Framework

PKI is a comprehensive framework that contains the set of roles, policies, and procedures needed to manage, distribute, create, store, use and revoke digital certificates.
Public Key Infrastructure (PKI) Solutions
PKI: Device Authentication

- Mutual authentication for all connections
- Access control
- Applying an identity fabric on device
- Cryptographically secure
PKI: Data Encryption

- Data in Transit
- Data at Rest
- Data in Process
PKI: Data & System Integrity

- Secure Boot
- Configuration settings
- IP protection
- Integrity of data coming to and from device
PKI White Paper...

How to Access the White Paper

Public Key Infrastructure: A Trusted Security Solution for Connected Medical Devices

Co Authored with Dale Nordenberg, Executive Director of MDISS

To download go to:

https://www.digicert.com/healthcare-iot/whitepaper.htm
PREVENTION & WELLNESS

154,000 Healthy Plates sold in hospital cafes
11,000 Utah students participating in LiVe Well assemblies
63 Schools in Step Express program
57,000 Healthy Living participants

HOSPITALS & CLINICS

22 Hospitals (Including childrens & orthopedics)
2,700 Beds
186 Intermountain Clinics

INSURANCE

870,000 Members

OUR TEAM

4,000 Affiliated physicians
1,500 Medical Group doctors & advanced practice clinicians
37,000 Employees
1,600 Volunteers
470 Volunteer Trustees

PATIENT ENCOUNTERS

502,000 Emergency room visits
137,000 Hospital admissions
40,000 Inpatient surgeries
117,000 Outpatient surgeries
31,000 Births
3,200,000 Medical Group visits

Not-for-Profit System
Based in Salt Lake City, Utah
Medical Equipment Security

FDA Guidance – December 28, 2016

RE: Post-market Management of Cybersecurity in Medical Devices

• Identification of assets, threats, and vulnerabilities
• Assessment of the impact of threats and vulnerabilities on device functionality and end users or patients
• Assessment of the likelihood of a threat and of a vulnerability being exploited
• Determination of risk levels and suitable mitigation strategies
• Assessment of residual risk and risk acceptance criteria
Medical Equipment Security

“All IDNs are at risk of targeted intrusion by organized crime or nation-state entities with unlimited resources capable of overwhelming security defenses, resulting in patient safety and privacy incidents, and reputational damage.”

The first thing the OCR will ask you:

- “Have you completed a risk assessment?”
- “Did the assessment include medical equipment that store, generate and transmit ePHI?”

The first thing the FDA will ask you:

- “Do you monitor, identify, and address cybersecurity vulnerabilities and exploits?”
What is Risk Assessment?

A complete security risk assessment will identify, analyze, evaluate, and rank the risk of your organization’s ePHI data using a consistent process and predetermined criteria.
The Old Way of Thinking about Risk Assessment

<table>
<thead>
<tr>
<th>Risk</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Access to ePHI by an assigned user name and password only and physical access to the medical equipment is controlled by the equipment user or other facility specific controls, i.e. locked door, key card access etc.</td>
</tr>
<tr>
<td>Medium</td>
<td>Access to ePHI by an assigned user name and password or physical access to the medical equipment is controlled by the equipment user or other facility specific controls.</td>
</tr>
<tr>
<td>High</td>
<td>Access to ePHI without an assigned user name and password and physical access to the medical equipment is NOT controlled by the equipment user or other facility specific controls.</td>
</tr>
</tbody>
</table>
What’s Different Now?

Policy, procedure, processes, audits that:
- Reduce volume of all intrusions.
- Decrease time to detect and remediate, aka “dwell time”.
- Triage and elimination of intrusions that affect high quality patient care.

New incoming medical equipment and clinical systems:
- Risk Assessment Committee.
- Pre-purchase evaluation process, mandatory cybersecurity documentation.

Existing inventory
- Review clinical workflow and intended use of the equipment in a networked environment.
- Review controls within the system (or system of systems) that prevent patient harm and secure ePHI.
- Review critical risk reasons and history.
  - Data stored or managed offshore.
  - Cyber hack identified by verified sources.
  - High probability of patient harm due to cyber hack.
- Review data loss impact due to cyber attacks.
Medical Device Specific Risk Assessment

- Feed model specific asset information into a Database.
- Data Classification and risk rankings.
- Adopt the collection, use, and expansion of Manufacturer Disclosure Statement for Medical Device Security (MDS2 – Published by www.himss.org) through an enterprise wide pre-purchase evaluation process.
- Calculate the risk rating based on criteria adopted by Common Vulnerability Scoring System (CVSS) 3.0 and Intermountain Clinical Engineering (CE).
- Collect and calculate a mitigation rating based on predetermined criteria, provide a residual risk rating used to determine if there’s a need for additional physical controls to secure ePHI data.
- Develop a risk mitigation strategy and implement with manufacturers and CE.
- Document maintenance and disposal procedures necessary for securing ePHI.
Medical Equipment Profiles (Polestar)

- Model specific information
- Critical risk reasons
- Impact factors
- Equipment characteristics pertaining to ePHI
- Risk classification
  - Catastrophic
  - Critical
  - Major
  - Minor
  - Negligible
- Risk mitigation and/or compensating controls
- Future development in Polestar
  - Include heat maps outlining the critical and high risk Equipment models
  - Reporting dashboards
## Critical Risk & Impact

<table>
<thead>
<tr>
<th>Notes</th>
<th>Controls</th>
<th>Critical Risk Reasons</th>
<th>Data Loss Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>- Data stored or managed offshore</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Device was identified as a cyber-hack risk by veri</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Notes</th>
<th>Controls</th>
<th>Critical Risk Reasons</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>- Change or Discontinue Medication Dosage</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Loss of 500+ Local Protected Data Records</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Interrupt Life Sustaining Medical Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Compromise and Render the Device Unusable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Change or Destroy Local Biometric Data</td>
<td></td>
</tr>
</tbody>
</table>
Classifying Risk

**Catastrophic**
- Almost non-recoverable impact, harm, or damage to:
  - System
  - Individual
- Intensive recovery and remediation required

**Major**
- Substantial impact or disruption to:
  - System
  - Individual
# Classifying Risk

<table>
<thead>
<tr>
<th>Minor</th>
<th>Negligible</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Minor impact to system, no adverse effect on individual</td>
<td>• Almost no impact or damage to:</td>
</tr>
<tr>
<td></td>
<td>• System</td>
</tr>
<tr>
<td></td>
<td>• Individual</td>
</tr>
</tbody>
</table>
Classifying Mitigation

Preventive

- Inhibiting a loss, threat or cyber attack by the use of controls such as encryption, authentication requirements, de-identification, and data integrity methods.

Deterrent

- Keeping the casual threat away, such as strong passwords, two-tiered authentication, Internet use policies, and physical controls.

Recovery

- A control that helps retrieve or recreate data or applications, such as backup systems and contingency plans.

Reactive

- Providing a means to respond to a threat that has occurred, such as an alarm or penetration test.

Detective

- Identifying and proving when a threat has occurred or is about to occur, such as audit trails, intrusion detection, and checksums.
Operationalizing Mitigation

- Partnership with medical equipment manufacturers and Supply Chain for procurement and contracts.
- Partnership with Cybersecurity and Clinical Engineering.
- Review mitigation strategies with clinical users, manufacturers, Cybersecurity, and CE teams.
- Work with facility CE teams to perform software and/or firmware upgrades, patches, and install compensating controls.
- Document in CMMS, include updates as part of the equipment preventative maintenance.
Example 1: Bedside Monitoring System

- Deployed at more than 20 hospitals.
- Reviewed clinical workflows, remote monitoring capabilities, and security issues within the entire system.
- Issues vary from weak passwords, shared accounts, unencrypted data, remote access, and incompatibility with AV software’s.
- Currently CE is working with IT to:
  - Inventory of all individual assets connecting to the monitoring system and servers.
  - Review clinical workflow and network architecture for this system.
  - Working with the manufacturer to obtain the MDS2 and cybersecurity documentation.
  - Establish a plan to mitigate security issues and concerns.
Treatment/Clinical

- Ensure patients being treated by connected technology have an assurance of safety & security

Electronic Secure Data

- Risk assessment essential to successful deployment
- Changing mentality from compliance to data stewardship
- Healthcare providers and device manufacturers share responsibility
- Technologies such as PKI can help with preventative stance
- Proactive security = better patient care, engendered trust
Questions

Mike Nelson
VP Healthcare Solutions
DigiCert
@mike_k_nelson

Karl West
Chief Information Security Officer
Intermountain Healthcare
Appendix
Use Case I: Application Security

Background:
Healthcare provider has rolled out medical device integration connecting critical systems such as ventilators, anesthesia and infusion systems to the backend electronic health record (EHR). Medical device connects to middleware and passes diagnostic information between the medical device and EHR.
Use Case I: Application Security

Objective:

- Identify sender and recipient of communication
- Encrypt data so it cannot be viewed or modified

PKI Use:

- Both the sender and recipient of data authenticate themselves (mutual authentication) using a certificate signed by a trusted root
- Each time connection is established a new session key is created during the SSL handshake which is used to encrypt data that is transmitted

Threat Scenario

Proper PKI Architecture
Use Case II: Code Signing OTA Software Updates

Background:
Medical device manufacturer has matured and designed a scalable system to enable the push of software and security updates over the air (OTA) to managed and supported systems inside the Healthcare Delivery Organization (HDO).
Use Case II: Code Signing OTA Software Updates

Objective:

- Prevent attackers from running code on devices
- Verify code is authentic before it is run

PKI Use:

- Code that is signed with a certificate issued by a trusted root can be identified as trusted.
- Checking a signature on code can also be paired with only allowing OTA updates through a mutual authentication connection from a trusted
Use Case III: Source Code / Firmware Signing

Background:
Medical device manufacturer does not deploy source code/firmware signing.

Risk/Attack Scenario:
Attacker extracts and modifies code, then pushes malicious code back to all like devices.

Potential Impact:
System network and medical device are compromised. IP contained in device firmware/source code is compromised. Remote access keys compromised on all like systems allowing administrative access to all deployed systems.
Use Case III: Source Code / Firmware Signing

Objective:

- Detect that source code or firmware is authentic before running
- Prevent code from running that will compromise intellectual property and allow access to resources on a network

PKI Use:

- Use Secure Boot – check signature of boot image before allowing device to boot
- Sign firmware/source code with a trusted certificate – Use signature to check for authentic firmware/source code before boot