Medical Device Security Considerations – Case Study

Jeanie Larson
Chief Information Security Officer
UC Davis Medical Center
@katkarma1
Medical devices are easy-targets and used as entry-points into networks for attackers.

“Network-connected/configured medical devices that are infected by malware can disable a device from properly performing its clinical function. This, in turn, could lead to a patient safety concern.”

Suzanne Schwartz, Director, FDA Center for Devices and Radiological Health
# Why the Focus on Medical Device Security?

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008</td>
<td>Pacemaker hack (Kevin Fu, Umass Amherst)</td>
</tr>
<tr>
<td>2011</td>
<td>Insulin Pump hack (Jerome Radcliffe, Black Hat Conference)</td>
</tr>
<tr>
<td>2013</td>
<td>Discovery of a wide-range of vulnerabilities, including Surgical and anesthesia devices, Ventilators, Infusion Pumps, Defibrillators, Patient Monitors, and Laboratory Equipment</td>
</tr>
<tr>
<td>2014</td>
<td>FBI Alerts to Healthcare Industry, NIST NCCoE Medical Device Use Case project launched</td>
</tr>
<tr>
<td>2014</td>
<td>AAMI / ECRI Safety Warning on cyber risks</td>
</tr>
<tr>
<td>2015</td>
<td>HHS OIG Announced that it will include networked medical devices in upcoming audits</td>
</tr>
<tr>
<td>2016</td>
<td>FDA Cybersec7urity Guidance and Workshop – Postmarket</td>
</tr>
</tbody>
</table>
Old Model / New Paradigm

- Cybersecurity CIA Triad
  - Confidentiality
  - Integrity
  - Availability
  - And sometimes non-repudiation

- Patient Safety $<\rightarrow>$ Human Life & Safety
Patient Safety Considerations:

- Confidentiality – breach of patient information, HIPAA regulatory and liability (civil and regulatory)
- Integrity - data used to make treatment decisions – patient safety
- Availability – outage creates critical gap in patient monitoring or treatment patient safety
Medical device is hacked or infected with malware! Now what?
- Leave it. Shut it down. Rebuild.
  - Who makes the decision?

Consider multi-disciplinary approach to manage risk and apply compensating controls
- Establish governance, create a charter, engage appropriate stakeholders
Asset inventory – medical devices should be easily identified as such during incident response triage

Incident Response
- vendor support model
  - What is the SLA / Response requirement?
- Incident Response Plan
  - Identify roles and responsibilities
  - Include a decision and notification / escalation matrix

Patient safety / patient harm – how would you know?
- Are medical devices assessed or forensically examined after a patient safety event?
Medical Device Security Considerations

Risks:
- Patient safety (lives)
- Operational / Downtime
- Data Breaches / Fines
- Revenue / Financial
- Patient trust & Staff morale
- National security

Vulnerability:
- Tightly regulated “turn-key” systems
- Long useful life
- Poorly protected & patched
- No detection & alerting
- Ecosystem Complexity
- Vulnerability of device, hospital, & health system
- Network connected

Threats:
- Targeted attacks
- Collateral damage
- Malware remediation
  - Theft / Loss
  - Compliance violation
- Lateral attack / weakest link exploitation
  - Hacktivism, terrorism

Symantec Corp, 2016
How to Secure the Un-securable?

- **Framework or Methodology**
  - Imperative to identify and use a framework or methodology
    - Medical Device Risk Assessment Platform
    - Cybersecurity Framework (NIST)
  - Incident Response Plan should outline medical device response and governance
  - Threat modeling will help when with security mitigation plan

- **Device Management**
  - Diagnostic / monitoring / control (treatment)
    - Map threats to mitigation strategies (Cyber Threat Statement for Medical Devices)
  - Asset identification, categorization and isolation
    - Consider multi-tier approach based on criticality of impact to patient safety
The content of this session is from a cybersecurity practitioner’s perspective.

For clarity, the term ”medical device” in this presentation refers to a device that meets the following criteria:

- “An instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar article including a component part or accessory” (FDA Medical Device Definition)
  - Diagnostic equipment
  - Pumps
  - Pill dispensers
  - Wearable /embedded devices

- Or more practically, any (network connected) device that is controlled by a computer that is used to monitor, treat, diagnose, or impact patient care.
For purposes of this presentation, limited to a single type of diagnostic device (EEG).

NOTE: This could be any vendor or any provider, anywhere.
Malware infected medical diagnostic device –
- Could impact Confidentiality, Integrity and / or Availability
- ANY of these COULD impact patient safety
- Used in diagnosis and treatment decisions by physician

Neurology Department uses embedded medical application (running on Windows OS) to monitor patients seizure activity
- Data integrity could be an issue
- Safety of patient diagnosis/ treatment decisions

Decision – leave it up or shut it down?
- Risk assessment – patient safety paramount
Vendor documentation:

Connecting to the NNN-123 through the LAN converter, a secondary data stream can be controlled by a local or network station and sent to a separate file storage location.

The integration of the vital sign data is available at the bedside, as well as remotely for more timely EEG intervention by the reviewing clinician.
Malware Controlled Medical Device

Security monitoring detected:

- Calling home to multiple countries including France, China, Russia, Ukraine and Panama
- Remote Access Trojan
- Appeared to be part of a controlled botnet (IOCs, TTPs)
- Attempts to remediate revealed sophisticated anti-forensics capability
- High availability requirement in service environment – serving patient care
Many Vulnerabilities

- Security Vulnerabilities:
  - Connects via LAN (connected to Internet) – isolation difficult because it needs to upload data to imaging system
  - Poor authentication (Username = Password)
  - Requires Local Admin privileges to operate application
  - Support model – vendor remote access
  - Zero platform hardening - unpatched operating system and unnecessary services enabled
  - Communication not secure
  - No encryption
  - No anti-virus installed
  - Security patches not applied - ever
  - Running on end-of-life operating system
  - Healthcare provider CULTURE!
Malware infected medical device
- Confidentiality, Integrity and / or Availability issues caused by malware COULD impact patient safety

Risk Decision
- Who is authorized to make the decisions regarding malware infected or hacked medical devices?

Keep patient appointments.  
**Primary goal: Availability!**

Little or no understanding of impact to patient.  
**Primary goal: Containment**

Little or no understanding of ramification of a cyber event on functionality of device and consequently impact to patient.  
**Primary goal: Patient Care**

We have patients scheduled!

Take it off the network!

I need these diagnostic results!

Biomed / Scheduler

IT Technician

Physician
Where do we go from here?

- Evaluate your environment
  - Do you know where your medical devices are? What are the vulnerabilities? What compensating controls are applied?
  - Do you know who makes decisions when a medical device is compromised? Is a multidisciplinary team involved in risk decisions regarding medical devices that are hacked/malware infected?
  - Are medical devices addressed in your Incident Response Plan?

- Solid methodology or framework needed to secure medical devices

- Governance to ensure risk decisions are being made at the appropriate level and by the appropriate party in the organization - include appropriate stakeholders
Where do we go from here?

- Remember the “human factor” – security awareness and communication
  - Incident lifecycle – educate employees about incidents occurring in your environment

- Post-mortem cyber-forensic review of medical equipment

- Information Sharing – Information Sharing and Analysis Center (ISAC)
  - NH-ISAC – Medical device working group
  - MDISS – FDA named ISAO for medical devices
  - Share vulnerability information, risk assessments, threat information appropriately
  - Proactively consume and act upon intelligence information
In Summary

- Cybersecurity triad – Confidentiality – Integrity – Availability
  - Need to understand the impact of each of these as applied to medical device security and patient safety
- A framework or methodology is necessary to identify and address vulnerabilities and ensure the secure operation of medical devices
- Threat modeling for medical devices will help in developing a security strategy
- Incident response plans need to address medical device breaches.
  - Multi-disciplinary team approach recommended – physician / practitioner, Biomed, IT, cybersecurity
- Don’t forget the human factor – engage employees, including practitioners and Biomed personnel – educate them!
- Get involved – NH-ISAC or MDISS – leverage community assessments and emerging frameworks
  - www.nhisac.org
  - www.mdiss.org
- Contact info
  - Jeanie Larson – jeanielarson@me.com
Resources for more information

**NH-ISAC**
- [http://www.nhisac.org/](http://www.nhisac.org/)

**Medical Device Innovation, Safety and Security Consortium**
- [http://www.mdiss.org/](http://www.mdiss.org/)
- [https://mdrap.mdiss.org/](https://mdrap.mdiss.org/)

**Hacking Healthcare IT in 2016**

**Securing Hospitals – A Research Study and Blueprint - Security Evaluators**
- [https://www.securityevaluators.com/hospitalhack/securing_hospitals.pdf](https://www.securityevaluators.com/hospitalhack/securing_hospitals.pdf)