Medical Device Cybersecurity

Axel Wirth, CPHIMS, CISSP, HCISPP
Distinguished Technical Architect
Symantec Corporation
Axel_Wirth@Symantec.com

32nd Annual Conference on Clinical Engineering
Productivity and Cost Effectiveness
June 3, 2016
What do these two gentlemen have in common?

Both made medical decisions based out of concern that their implanted medical device could be hacked!
Medical Device Cybersecurity
Introduction to the Problem Space

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

Threats:
• Targeted attacks
• Collateral damage
• Malware remediation
  • Theft / Loss
• Compliance violation
• Lateral attack / weakest link exploitation
• Hacktivism, terrorism
Introduction to Medical Device Cybersecurity

Main Events:

2008 – Pacemaker hack (Kevin Fu, UMass Amherst).
2011 – Insulin Pump hack (Jerome Radcliffe, Black Hat Conference).
2013 – Department of Homeland Security Alerts (ICS CERT); Government Accountability Office Report
2014 – FBI Alerts to Healthcare Industry, NIST NCCoE Medical Device Use Case project launched, AAMI/ECRI safety warning on cyber risks.
2014 – FDA Cybersecurity Guidance and Workshop - Premarket
2015 – HHS OIG announced that it will include networked medical devices in upcoming audits.
2016 – FDA Cybersecurity Guidance and Workshop – Postmarket (draft)

“The time is ripe to stop admiring the problem”
Suzanne Schwartz, MD, MBA
EMCM / FDA CDRH
Medical Device Risks - Examples

• Device hacks (targeted)
• Device loss/theft (PHI breach)
• Drug abuse
• Patch deployment failure
• Multiple reports on device testing - with disastrous results
• ICS-CERT (DHS), FBI, FDA warnings
• Audit & Compliance Risks
Medical Devices - Targeted and Exploited!

- Medical Device APT exploit
- Entry point for an attack
- Difficult to remediate
- “Near perfect target”
- Invisible to IT
- 60 Hospitals (Bloomberg)
- Traced back to Russian Crime Syndicate

- 68,000 Internet-exposed devices
- Misconfigured, Win XP, ...
- Allowed for network mapping
- Honeypot: attempted 55k logins, 300 malware installs
- Devices are a recognized target
- We don’t know how bad it is
Medical Device Cybersecurity
What the discussion comes down to

Availability - Integrity - Confidentiality

- Device Functionality
- Network Reliability
- Unauthorized Access
- Device Performance
- ePHI Exposure
- Beachhead Attack

Patient Safety + Patient Trust

Impact

- Patient Harm
- Data Breach
- Alarm Delays
- Treatment Delays
- Blackmail / Ransom
- Drug Abuse
- Assassination, Murder
- Intellectual Prop. Theft
- Cyberwarfare
- Cyberterrorism, Hacktivism
- Cybercrime
- Public Opinion
- Treatment Decisions
- Revenue Loss
- Staff Productivity
- Law Suits & Fines

Indirect

National

Criminal

Patient

Patient Trust

Patient Safety

Public Opinion

Revenue Loss

Intellectual Prop. Theft

Assassination, Murder

Blackmail / Ransom

Drug Abuse

Alarm Delays

Treatment Delays

Patient Harm

Data Breach

Symantec.
# Medical Device Cybersecurity Path Forward

## Protect Devices

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>HDO</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Hardened design</td>
<td></td>
</tr>
<tr>
<td>• Software best practices</td>
<td></td>
</tr>
<tr>
<td>• HIDS/HIPS</td>
<td></td>
</tr>
<tr>
<td>• Key/Certificate-based technologies:</td>
<td></td>
</tr>
<tr>
<td>• Encryption</td>
<td></td>
</tr>
<tr>
<td>• Device certificates</td>
<td></td>
</tr>
<tr>
<td>• Code signing</td>
<td></td>
</tr>
<tr>
<td>• Secure boot</td>
<td></td>
</tr>
<tr>
<td>• Secure handling</td>
<td></td>
</tr>
<tr>
<td>• Media use, esp. USB</td>
<td></td>
</tr>
<tr>
<td>• Integration best practices</td>
<td></td>
</tr>
</tbody>
</table>

## Manage Devices

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>HDO</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Lifecycle mgmt. (patch &amp; update deployment)</td>
<td></td>
</tr>
<tr>
<td>• V&amp;V incl. security, e.g. pen testing</td>
<td></td>
</tr>
<tr>
<td>• Vulnerability disclosure</td>
<td></td>
</tr>
<tr>
<td>• Software BOM (Supply Chain)</td>
<td></td>
</tr>
<tr>
<td>• Procurement &amp; Contracting</td>
<td></td>
</tr>
<tr>
<td>• Asset &amp; Lifecycle mgmt. (incl. security)</td>
<td></td>
</tr>
<tr>
<td>• Dependency mgmt.</td>
<td></td>
</tr>
<tr>
<td>• Risk Management:</td>
<td></td>
</tr>
<tr>
<td>• Risk Assessment: safety, security, privacy, operations, reputation</td>
<td></td>
</tr>
<tr>
<td>• Mitigation</td>
<td></td>
</tr>
</tbody>
</table>

## Protect Ecosystem

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>HDO</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Secure remote access</td>
<td></td>
</tr>
<tr>
<td>• Strong password / 2FA</td>
<td></td>
</tr>
<tr>
<td>• Security best practices documentation</td>
<td></td>
</tr>
<tr>
<td>• Enablement &amp; Training</td>
<td></td>
</tr>
<tr>
<td>• Network architecture</td>
<td></td>
</tr>
<tr>
<td>• Security event monitoring</td>
<td></td>
</tr>
<tr>
<td>• Firewalls / Gateways</td>
<td></td>
</tr>
<tr>
<td>• Enablement &amp; Training</td>
<td></td>
</tr>
</tbody>
</table>

## Manage Incidents

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>HDO</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Threat &amp; Vulnerability monitoring and management</td>
<td></td>
</tr>
<tr>
<td>• Regulatory reporting</td>
<td></td>
</tr>
<tr>
<td>• Detect, Respond, Recover</td>
<td></td>
</tr>
<tr>
<td>• Impact Analysis, Forensics</td>
<td></td>
</tr>
<tr>
<td>• Communication &amp; Decision making</td>
<td></td>
</tr>
<tr>
<td>• Report as needed</td>
<td></td>
</tr>
</tbody>
</table>
Securing the Medical Device Ecosystem
The right technology choice

Device Manufacturer

- Protect Intellectual Property
  - Server hardening, authentication
- Secure Devices
  - Code signing, secure boot, platform hardening
- Protect Critical Data
  - Messaging certs, encryption, mPKI
- Protect Manufacturing Integrity
  - Platform hardening, authentication
- Secure Communication & Access
  - Authentication & Access mgmt.

Healthcare Delivery Organization

- Contract & Requirements Management
  - Policy & Requirements Mgmt.
- Holistic Asset View & Mgmt.
  - Asset Management
- Risk Mgmt. & Mitigation
  - Risk Scoring and Assessment, Mitigation Management
- Network Anomaly Detection
  - Network Security, Security Gateway

Symantec
Asset & Risk Management
Provider Best Practices Approach

IEC 80001 Series

Asset Management

Procurement

Security Risk Analysis

HIMSS/NEMA MDS²

Lifecycle Mgmt.

Risk Mitigation

Incident Analysis

Risk Management

MDS²: Manufacturer Disclosure Statement for Medical Device Security
Medical Device Cybersecurity

Stephen L. Grimes, FHIMSS FAIMBE FACCE
Principal Consultant
Strategic Healthcare Technology Associates, LLC
Stephen.Grimes@SHCTA.com

32nd Annual Conference on Clinical Engineering
Productivity and Cost Effectiveness
June 3, 2016
Medical Devices & Systems:  
~ 10 Million in U.S. Hospitals today

Exponential growth of medical devices (including consumer platforms & wearables running medical applications) in hospitals, clinics, medical offices, workplace, schools, homes, etc.

You can’t manage what you can’t measure
Overlapping Responsibility?

Currently 40% Networked (and rapidly growing)

Systems of Systems

Information Technology

CLINICAL / BIOMEDICAL ENGINEERING

Still significant disconnect ... resulting in coverage gaps
Medical Devices & Systems:
Examples of Commonly Connected Categories of Equipment

~10 to 15 medical devices per bed
typical 500 bed hospital may have 7,500 medical devices

Examples of networked medical equipment types:

- Physiologic monitors .......... hundreds
- Defibrillators ........ scores
- Infusion pumps .......... thousands
- Anesthesia units .......... scores
- Ventilators .......... scores
- Extracorporeal Assist .......... up to dozen
- Vital sign monitors .......... hundreds
- CT & MRI scanners .......... up to score
- Fetal monitors .......... scores
- Laboratory analyzers .......... scores
- Diagnostic ultrasound .......... scores
- Patient beds .......... hundreds
- Electrocardiographs .......... scores
- Injectors, contrast media .......... scores
Medical Devices & Systems: Differences in Development, Updates, Management

- As it currently stands, medical devices typically have a **7-8 year product development cycle**
  - features including OS & software are “baked” in years before product release ... and often years after consumer equivalent of software and hardware has moved to next generation
- Medical devices generally cannot be safely patched with OS updates or have virus software applied until patches have been specifically tested & approved by the device manufacturer
- Medical devices cannot have agents (e.g., SNMP) installed to facilitate network management
Get data to determine the extent of the exposure .... can’t effectively manage what you can’t identify and measure!

- Identify numbers, types and locations of medical devices & systems ...
  - look to computerized maintenance management systems (CMMS)
- type of data transmitted, stored (e.g., PHI?)
- determine configuration
  - OS & applications (including versions)
  - networkable, network MAC & IP addresses, protocol
  - existing connections (e.g., with what other services & devices are “authorized” to exchange data? ... including remote access)
  - default device settings
- identify security features (MDS\(^2\))
Medical Devices & Systems:  
Identify gaps and establish processes to address medical device security issue

Security Related Processes – close gaps between IT & Medical processes!
- educate all stakeholders regarding risks
- acquisition processes (i.e., acquire with security in mind)
- security & risk assessment processes ... engage appropriate stakeholders to determine
  - criticality of system & data
  - probability of failure
- establish & implement mitigation plan to identify, prioritize and address risks using administrative, technical & physical safeguards ... and monitor effects.
  - define roles, responsibilities (CE/HTM, IT, vendor/mfg, leadership)
  - build for resilience (e.g., backups, redundancy)
  - business associate agreements (BAA) for vendors that service medical equipment
  - medical grade networks that provide high bandwidth & security
- disposal processes (e.g., data sanitizing)
Resources for Managing Medical Device Security: 

*Manufacturer Disclosure Statement for Medical Devices Security (MDS²)*

- MDS² contains security related information from the device manufacturer (revised in 2013 to comply with ISO 80001-1)
- Most major manufacturers (e.g., Philips, GE, Siemens, etc.) offer completed MDS² on each of their medical equipment models
- Information on the MDS² is intended for use by medical device owners who want to use device’s security features effectively
- Originally developed by HIMSS and now a NEMA standard

http://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx
**Medical Devices & Systems: FDA’s role**

**FDA provides**
- Guidance for manufacturers and hospitals ... and requirements for manufacturers ... on digital health and cybersecurity issues

**FDA requires manufacturers**
- have their devices cleared or approved (depending on Class) by FDA
- to remain vigilant about **identifying risks and hazards** associated with their medical devices, *including risks related to cybersecurity*
- to be responsible for **putting appropriate mitigations in place** to address patient safety risks and ensure proper device performance

**FDA recommends that hospitals & providers**
- work with manufacturers to evaluate their network security and protect their installed systems
With respect to medical device cybersecurity, FDA primarily focuses on regulations and guidance for manufacturers. Manufacturers are encouraged to take appropriate precautions to ensure that vulnerable products they produce are designed to be secure and to work with healthcare delivery organizations (HDOs) and other stakeholders as necessary to ensure they remain secure throughout their life-cycle.

The FDA has produced a series of Guidance:

- Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software (Jan 2005)
  [Link](http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf)

- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (Oct 2014)
  [Link](http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf)

- Draft Guidance for Industry: Postmarket Management of Cybersecurity in Medical Devices (Jan 22, 2016)
  [Link](http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf)
Resources for Managing Medical Device Security:
Medical Device Innovation, Safety, and Security (MDISS) Consortium

- Medical Device Risk Assessment Platform (MDRAP) Tool [https://mdrap.mdiss.org/](https://mdrap.mdiss.org/)
  - Based on tool developed for evaluating both application and device risk
  - Provides a risk score by category and allows comparative studies across several different devices
  - Useful in pre-purchase assessment of security risks (helps in selection process and in preparing risk mitigation steps)
  - Latest version of MDRAP builds on operational questions onto MDS² to help manufacturers and healthcare systems better understand the security profile of their devices

Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities & activities

- The new standard focuses on how to manage risks associated with
  - safety ... preventing physical injury or damage to people, property or the environment
  - effectiveness ... insuring the intended result is produced
  - data & system security ... insuring that information “assets” (i.e., data & systems) are reasonably protected from compromises to confidentiality, integrity and availability

- Defines roles & responsibilities
- Defines key activities
Resources for Managing Medical Device Security

Application of Risk Management for IT-Networks Incorporating Medical Devices
Supplemental Guides

- ISO/IEC 80001-2-1:2012 *Step by step risk management of medical IT-networks; Practical applications and examples*
- ISO/IEC 80001-2-2:2012 *Guidance for the disclosure and communication of medical device security needs, risks and controls*
- ISO/IEC 80001-2-4:2012 *General implementation guidance*
- ISO/IEC 80001-2-5:2014 *Guidance for distributed alarm systems*
- ISO/IEC 80001-2-7:2015 *Guidance for healthcare delivery organizations (HDOs) on how to self-assess their conformance with IEC 80001-1*
- ISO/IEC 80001-2-8: under development *Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2*
Thank You

32nd Annual Conference on Clinical Engineering
Productivity and Cost Effectiveness
June 3, 2016

Stephen.Grimes@SHCTA.com
Stephen L Grimes, FHIMSS FACCE FAIMBE
Managing Partner & Principal Consultant
Strategic Healthcare Technology Associates, LLC

Mr. Grimes is recognized as one of the industry’s first and most prominent experts on the issue of medical device security. He originally drew the industry’s attention to the growing risks associated with medical device security compromises through a series of articles, presentations and national symposia beginning in 2001. In 2004, Mr. Grimes authored the ACCE/ECRI Information Security for Biomedical Technology: A Compliance Guide … the industry’s first definitive guide for healthcare delivery organizations (HDOs) on identifying and mitigating medical device security risks. Also in 2004, he conceived of and managed the development of the Manufacturer’s Disclosure Statement for Medical Device Security (MDS²) while chairing HIMSS’ Medical Device Security Task Force. He later participated on the NEMA standards committees that led to the adoption of the 2005 and 2013 versions of the MDS² as formal industry standard. He also served as a member of the US/TAG to ISO/TC 215 HEALTH INFORMATICS and Joint Working Group 7 that developed the 2010 ISO/IEC/AAAMI standard IEC 80001-1: Application of risk management for IT-networks incorporating medical devices.

Over the years to the present, Mr. Grimes has continued to speak and write on how healthcare delivery organizations (HDOs) need to address the evolving medical device security threat. During his eight-year tenure (2007-2015) at ABM Healthcare Support Services in the capacity of Chief Technology Officer and senior consultant, he has also developed programs, procedures and tools for that organization’s 300+ clients (with medical device inventories totaling over 500,000) that addressed data security management in the device life cycle.
Axel Wirth, CPHIMS, CISSP, HCISPP

Distinguished Solutions Architect
US Healthcare Industry, Symantec Corporation

As Solutions Architect, Axel Wirth provides strategic vision and technical leadership within Symantec’s Healthcare Vertical, serving in a consultative role to healthcare providers, industry partners, and health technology professionals. Drawing from over 25 years of international experience in the industry, Mr. Wirth is supporting Symantec’s healthcare customers to solve their critical security, privacy, compliance, and IT management challenges. He is an active participant in industry organizations and a frequent speaker at conferences, forums, and webcasts on subjects such as cybersecurity, medical device security, mobile health infrastructure, compliance automation, IT infrastructure optimization, and other healthcare-specific topics.

His extensive background in the healthcare IT and medical device industries includes engineering leadership as well as strategic business development and marketing roles with Siemens Medical, Analogic Corp., Mitra Inc., Agfa Healthcare, and currently Symantec Corp. His education includes a BS Electrical Engineering degree (EE) from Fachhochschule Düsseldorf and an MS Engineering Management degree (MSEM) from The Gordon Institute of Tufts University.