Who I am

Scott Erven - Managing Director – Healthcare Industries Advisory – Cybersecurity & Privacy

- Medical Device Security Lead For PwC
- Over 5 Years Leading Medical Device Security Research
- Over 15 Years IT Security Experience
- Over 5 Years Managing Security For Healthcare Systems & Providers

What we’ll be covering today

1. Why medical device security matters.
2. Vulnerabilities inside the medical device security landscape.
3. Are attacks a reality?
4. Diagnosis and problem awareness.
5. Treatment plans.
Why medical device security matters

Personal impact

Malicious intent is not a prerequisite to patient safety issues
**Research – Device vulnerabilities**

### Weak default/hardcoded administrative credentials
- Treatment modification
- Cannot attribute action to individual

### Known software vulnerabilities in existing and new devices
- Reliability and stability issues
- Increased deployment cost to preserve patient safety

### Unencrypted data transmission and service authorization flaws
- Healthcare record privacy and integrity
- Treatment modification

---

**Research – Internet exposure**
Shodan search initial findings

Doing a search for anesthesia in Shodan and realized it was not an anesthesia workstation.

Located a public facing system with the Server Message Block (SMB) service open, and it was leaking intelligence about the healthcare organization's entire network including medical devices.

Initial healthcare organization discovery

Very large U.S. based healthcare system consisting of over 12,000 employees and over 3,000 physicians including large cardiovascular and neuroscience institutions.

Exposed intelligence on over 68,000 systems and provided direct attack vector to the systems.

Exposed numerous connected third-party organizations and healthcare systems.

Did we only find one?

No. We found hundreds!!

Change the search term and many more come up. Potentially thousands if you include exposed third party healthcare systems.
Let me paint the picture

System with Initial Exception

- **SW:**
  - 00001 001.png
  - Internal Server
  - 00002 002.png
  - External Server
  - 00003 003.png
  - Internal Server

**Impact:**
System May Not Require Login

Electronic Medical Record Systems

Getting a little warmer!

Cardiology Systems

- 044701 1 - Sr.
- 044702 2 - Card Lab
- 044703 3 - C - Cardiac Unit Lab
- 044704 4 - C - Cardiac Unit Lab
- 044705 5 - Card Lab
- 044706 6 - Card Lab
- 044707 7 - Card Lab
- 044708 8 - Card Lab
- 044709 9 - Card Lab
- 044710 10 - Card Lab
- 044711 11 - Card Lab
- 044712 12 - Card Lab
- 044713 13 - Card Lab

Impact:
Pediatric Nuclear Medicine
Anesthesia Systems

Summary of devices inside organization

- Anesthesia Systems – 21
- Cardiology Systems – 488
- Infusion Systems – 133
- MRI – 97
- PACS Systems – 323
- Nuclear Medicine Systems – 67
Potential attacks – Physical

- We know what type of systems and medical devices are inside the organization.
- We know the healthcare organization and location.
- We know the floor and office number.
- We know if it has a lockout exemption.

Potential attacks – Phishing/Pivot

- We know what type of systems and medical devices are inside the organization.
- We know the healthcare organization and employee names.
- We know the direct public Internet facing system is vulnerable to MS08-067 and is Windows XP. We know the hostname of all these devices.
- We can create a custom payload to only target medical devices and systems with known vulnerabilities.

Are attacks a reality?
Real world attacks – Honeypot research

- Using known default login information for remote access?
- Leveraging existing exploits for remote command execution?
- Custom malware?
- Malicious intent to interfere with the device (or worse, someone using the device)?
- Campaigns against specific vendor devices?

Real world attacks – The data

<table>
<thead>
<tr>
<th>Data</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HoneyCreds</td>
<td>12</td>
</tr>
<tr>
<td>Successful logins (SSH/Web)</td>
<td>55,416</td>
</tr>
<tr>
<td>Successful exploits (Majority is MS08-067)</td>
<td>24</td>
</tr>
<tr>
<td>Dropped malware samples</td>
<td>0</td>
</tr>
<tr>
<td>Top 3 Source Countries</td>
<td>Netherlands, China, South Korea</td>
</tr>
<tr>
<td>HoneyCreds login</td>
<td>8</td>
</tr>
</tbody>
</table>

HoneyCreds logins are unique to the honeypot ssh/web service, someone did some research.

Real world attacks – Conclusion

- What did the attacker do once he got in? Nothing
- Did they realize they had root on a MRI machine? Probably not
- Are there compromised medical devices calling back to a command and control server? Absolutely
- Did the command and control owners know what the information they are sitting on? Didn’t appear so
Problem awareness

1. Medical devices are increasingly accessible due to the nature of healthcare.
2. HIPAA focuses on patient privacy, not patient safety.
4. Malicious intent is not a prerequisite for adverse patient outcomes.

Technical properties

- Exposed, vulnerable systems
  - All software has flaws.
  - Connectivity increases potential interactions.
  - A software-driven, connected medical device is a vulnerable, exposed one.

- Lack of patient safety alignment in medical device cyber security practices
A brief history of United States Food and Drug Administration (U.S. FDA) and medical device cybersecurity

- **January 2005**: FDA issues first-ever warning about cybersecurity vulnerability of a device.
- **February 2005**: FDA issues draft guidance on device cybersecurity based on “known vulnerabilities.”
- **January 2016**: FDA releases final guidance on cybersecurity for networked medical devices containing off-the-shelf software.
- **July 2015**: FDA issues draft guidance document on post-approved monitoring of medical device cybersecurity.
- **January 2016**: FDA issues final guidance document on post-approved monitoring and remediation of medical device cybersecurity.
- **June 2013**: FDA issues draft guidance on medical device cybersecurity.
- **June 2013**: FDA asks that cybersecurity information be submitted as part of a device’s application for approval, including:
  - Hazard analysis of cyber risks
  - Controls to mitigate specific risks
  - A plan of how to patch devices
  - Controls to maintain device integrity
  - Instructions on how to use related controls like antivirus software
- **February 2013**: FDA issues its final guidance document on including medical device cybersecurity information in premarket applications.
- **October 2014**: FDA issues draft guidance document on medical device cybersecurity.

U.S. FDA premarket guidance for medical device cybersecurity

U.S. FDA asks that cybersecurity information be submitted as part of a device’s application for approval, including:

- Hazard analysis of cyber risks
- Controls to mitigate specific risks
- A plan of how to patch devices
- Controls to maintain device integrity
- Instructions on how to use related controls like antivirus software

U.S. FDA’s post-market guidance for medical device cybersecurity

U.S. FDA highlights if the following criteria are met they will not enforce 806 reporting requirements:

1. **No serious adverse events** are known to have been caused by the vulnerability.
2. **Firms are made and users are notified within 60 days (Two 30 Day Periods Defined In Requirements) of the discovery of the vulnerability.**
3. The manufacturer is a member of an Information Sharing Analysis Organization (ISAO) and has a coordinated disclosure process.
**Treatment plans**

A shift in how we think about medical technologies

**Before**
- Devices are connected to patients physically
- Data obtained from devices are stored on paper or locally
- Devices are physical products
- Care is hand-administered at a health care location
- Physical access is needed to view health data

**Now**
- Devices are connected wirelessly to patients and other devices
- Data obtained from devices are stored in the cloud
- Devices include software and even databases of health information
- Care is available to patients in the palm of their hand through apps
- Health data can be accessed anywhere on earth

A shift in how we think about regulating medical devices

Traditional considerations meet technology

Traditional
- Safety
- Efficacy
- Quality
- Security

Evolving
- Is a medical device safe for use in humans? Does it cause adverse events? Are its risks tolerable in relation to its benefits?
- Is a device effective for its given purpose? What is the magnitude of the effect?
- After approval, a device must be kept safe and effective through adherence to quality manufacturing standards established by FDA
- Once a medical device is networked with other devices or the internet, is it still safe and effective?
Interaction with the broader industry is also core to developing an overarching threat landscape, responding to Cybersecurity events, and developing more secure devices.

A security centric, risk based product development process is core to the deployment of a secure effective medical device...

To meet the current regulatory requirements and protect the device from cybersecurity attacks, it is critical to embed security within the lifecycle of the product and in risk management considerations...
Medical Device Cybersecurity Approach

Invest in personnel and processes

- Companies should establish and support cybersecurity programs to support devices throughout their lifecycles.
- Cybersecurity experts should be hired or third-parties consulted to vet cybersecurity information.
- Established information-sharing processes — including ISAOs — may lead to more and better discussions.
- Companies should consider how to best engage with the cybersecurity community as a strategic advantage.

Medical Device Cybersecurity Framework

1. Medical IoT Governance
   - Development of Governance Model with clearly established roles, responsibilities, and FTE
   - Information Sharing and Analysis Organization (ISAO) Development and Participation

2. Network Security
   - Network Segmentation and/or Network Access Control (NAC) for critical medical IoT devices
   - Logging and Monitoring for Malicious Activity
   - Forensic Toolkit for Intrusion Analysis
   - Secure Remote Access
   - Secure Medical IoT Device Network Architecture

3. Medical IT Risk Management
   - Medical IoT Vendor Risk Management Program
   - Device Risk Profiling
   - Control Profile Development
   - Secure Disposal Processes
   - Physical Device Security
   - Device Risk Assessment Tool Development

4. Configuration Management
   - Patch Management Processes
   - Software Version Control Processes
   - Change Management Processes
   - Logging and Monitoring for configuration changes

5. Device Security
   - Medical IoT Device Encryption
   - Secure Device Access Control and Authentication
   - Wireless Security Controls

6. Asset Management
   - Device Inventory
   - Device Attribute Collection
   - Asset Management Policy and Process
   - Secure Device Procurement Processes

7. Medical IoT Security Program
   - Medical IoT Minimum Security Baseline (MSB)

8. Medical IoT Security Strategy
   - Medical IoT Risk Management Policy

9. Medical IoT Governance
   - Development of Governance Model with clearly established roles, responsibilities, and FTE
   - Information Sharing and Analysis Organization (ISAO) Development and Participation

10. Medical IoT Security Strategy
    - Medical IoT Minimum Security Baseline (MSB)

11. Medical IoT Governance
    - Development of Governance Model with clearly established roles, responsibilities, and FTE
    - Information Sharing and Analysis Organization (ISAO) Development and Participation

12. Medical IoT Security Strategy
    - Medical IoT Minimum Security Baseline (MSB)

Companies should establish and support cybersecurity programs to support devices throughout their lifecycles. Cybersecurity experts should be hired or third-parties consulted to vet cybersecurity information. Established information-sharing processes — including ISAOs — may lead to more and better discussions. Companies should consider how to best engage with the cybersecurity community as a strategic advantage.
Support can lead to opportunity

Device companies can become essential partners to healthcare providers by helping them support and secure their devices and networks.

Device companies can benefit by giving providers a level of comfort and assurance about product security, potentially leading to increased sales, and insight into how their devices are used and misused, benefiting future device development.

Scott Erven
Managing Director, Healthcare Cybersecurity
E: scott.erven@pwc.com

Thank you