Medical Device Security: The Next Frontier

Denise Anderson
President
National Health Information Sharing & Analysis Center (NH-ISAC)
Chair, National Council of ISACs
What is an ISAC?

Why ISACs?
Evolution

- PDD 63 1998
- HSPD-7 2003
- PPD 21 2013
- NIPP 2013
- CISA 2015
Why ISACs?

- Trusted entities established by CI/KR owners and operators.

- Comprehensive sector analysis aggregation /anonymization

- Reach-within their sectors, with other sectors, and with government to share critical information.

- All-hazards approach

- Threat level determination for sector

- Operational-timely accurate actionable
ISACs

• Auto ISAC
• Aviation ISAC
• Communications ISAC
• Defense Industrial Base ISAC
• Downstream Natural Gas ISAC
• Electricity ISAC
• Emergency Management & Response ISAC
• Financial Services ISAC
• Information Technology ISAC
• Maritime ISAC
• Multi-State ISAC
ISACs

- National Health ISAC
- Oil and Natural Gas ISAC (ONG)
- Over the Road & Motor Coach ISAC
- Public Transit ISAC
- Real Estate ISAC
- Research and Education ISAC
- Retail ISAC
- Supply Chain ISAC
- Surface Transportation ISAC
- Water ISAC
Overview of NH-ISAC
NH-ISAC

Founded in 2010

Sharing Community Intelligence and Alerts
Newsletter
Exercises
Webinars/Threat Calls
Conferences & Workshops
White Papers
Working Groups/Committees
Tools – Symphony, Soltra, Brightpoint
Playbook & Threat Level
CyberFit
Special Interest Groups
NH-ISAC - 2017 Membership Mix

- Provider: 30.5%
- Insurers and Payers: 20.7%
- HIT - Information: 10.3%
- Pharmacy: 2.9%
- Academia: 11.5%
- Medical Device: 9.2%
- Pharmacy/Biotech: 14.9%
Information Sharing

Value

Trust

Structure
Information Sharing: Traffic Light Protocol

- Restricted to a defined group (e.g., only those present in a meeting.) Information labeled RED should not be shared with anyone outside of the group.

- This information may be shared with ISAC members.

- Information may be shared with ISAC members and partners (e.g., vendors, MSSPs, customers). Information in this category is not to be shared in public forums.

- This information may be shared freely and is subject to standard copyright rules.
Types Of Information Is Shared

• Cyber Threats, Vulnerabilities, Incidents

✓ Malicious Sites
✓ Threat Actors, Objectives
✓ Threat Indicators
✓ TTPs, Observables
✓ Courses of Action
✓ Exploit Targets
✓ Denial of Service Attacks

✓ Malicious Emails: Phishing/Spearphishing
✓ Software Vulnerabilities
✓ Malicious Software
✓ Analysis and risk mitigation
✓ Incident response
Sample of ISAC Sharing

Indicators of Compromise
   IP Address, Subject Line, MD5, TTP, Malware

Ask a question
   Anyone else seeing?...
   What do you do in this situation?....
   How do you handle?............mobile device management

Share a Best Practice
   Here’s how we......

Share a Mitigation Strategy
   Here’s a script you can use......MIFR
   We did this......
Primary Ways Information Is Shared

✓ Portal/Alerts
✓ Listservers
✓ Automation
Neutrino Exploit Kit Distributes DMA Locker Ransomware

This information is marked TLP AMBER: Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.

In early January 2016, researchers observed a resurgence in Neutrino exploit activity........
Sample of Sharing Thread

• The Threat actors compromised several domain admin accounts. ...............  
• Samples of hostnames are:  
  • you can’t catch me  
  • hello I’m malware  
• Source IP addresses found so far: 
  • 123.456.789  
  • 198.233.456  
  • 456.789.234  
  • A couple of files most likely associated  
    • Imbad.zip  
    • clickonme.zip  
    • score.zip

0 hits last 7 days

• Can I get hashes?  
  • Two of these are reported on known bad lists  
  • One might be false positive

• We’ve seen traffic from 123.456.789 and 198.233.456  
  • Traffic from 198.199.206.2 contained “important file” headers.
Security Automation

Over 155 Organizations with over 700 users
What is Cyber Threat Intelligence?

8 Constructs of STIX

Atomic

What threat activity are we seeing?

Tactical

What threats should I look for on my networks and systems and why?

Operational

Where has this threat been seen?

What can I do about it?

What weaknesses does it exploit?

Strategic

Who is responsible for this threat?

Why do they do this?

What do they do?
A Force Multiplier
The Situation
Remember This?
It’s Now This…
The Ecosystem – Portability

Data

Pharmaceutical

Device Manufacturers

Providers

Payers

Retail
It’s Not About the Ones & Zeroes

- Financial
- Reputation
Chasms and Challenges

- Manufacturers
- Devices
- Researchers
- Regulators
- Healthcare Delivery Organizations
Chasms and Challenges

- Clinical Engineering
- Procurement
- HDO
- Doctors
- IT Security
A Public Health Problem
Challenge – Tens of Thousands of Devices

- Little or no security built in
- Legacy platforms
- Patching
- Mobility
- Communication and oversight gaps
- Physical teams v. IT security
- Connected to networks
- Vetting of devices
The Challenge

Over next 10 years

100 Billion Exposures

Between patients and connected medical devices

People
• 1 billion healthcare visits
• 1.5 M nursing home residents

Places
• 6,000 hospitals
• 17,000 nursing homes
Estimating patient exposures to digitally enabled and networked medical devices

1. One billion patient encounters per year
2. Estimate each encounter, on average, has 10 exposures to a medical device
3. Assume 10 years of legacy risk as the national healthcare landscape will continue to have inadequately secured devices
4. Over ten years, 100 billion patient exposures with medical devices

<table>
<thead>
<tr>
<th>Exploring Probability of Adverse Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>1% (.01)</td>
</tr>
<tr>
<td>0.10% (.001)</td>
</tr>
<tr>
<td>0.01% (.0001)</td>
</tr>
<tr>
<td>0.001% (.00001)</td>
</tr>
<tr>
<td>0.0001% (.000001)</td>
</tr>
</tbody>
</table>
What is Needed

Three parameters define the importance of a public health problem

• Breadth of exposure, e.g. incidence/prevalence
• Depth of impact, e.g. morbidity and mortality
• Preventability

Clear definitions for security risks and medical device associated adverse events

Develop methods to establish valid estimates for the prevalence and incidence of malware and other security breaches in medical devices and associated impact on patient outcomes

Identify, track, and trend security incidents based on a model that protects the interests of patients, providers, manufacturers and regulators
A Brief History
Evolution of Medical Device Security

- Medical Device Regulation Act (1978)
- Safe Medical Devices Act (1985)
- Beth Israel Deaconess Medical Center
- Medical Device User Fee and Modernization Act (1990)
- Implantable Cardiac Defibrillator Vulnerabilities (2002)
- Insulin Pump Vulnerability (2006)
- FDA Premarket Guidance (2008)
- HITECH (2011)
- HIPAA Final Rule (2012)
- FDA Draft Postmarket Guidance (2014)
- FDA Safety and Innovation Act (2016)
- MD-VIPER Est. by NH-ISAC & MDISS (2017)

- Software Update Challenges for Embedded Devices
- Defective Therac-25 Accelerators
- Medical Device Modernization Act
- Reigel vs. Medtronic
- NH-ISAC Founded
- MDSISC Est. by NH-ISAC & MDISS
- MDSISC Org. Established
- Pacemaker Hack
- FDA Postmarket Final Guidance
Meeting the Challenge
MDISSL: Medical Device Innovation, Safety and Security Consortium

- Non-profit public health initiative and patient safety organization founded in 2011.
- Focused on medical device cybersecurity
- First organization dedicated to these important medical device cyber health challenges
Medical Device Security Information Sharing Council (MDSISC)

• Co-Chaired by NH-ISAC & MDISS
• Mission:
  – Engage stakeholders
  – Execute best practices for secure information sharing
  – Exchange information to promote efficient, secure and safe use of medical devices and associated networks

Current membership:
118 individuals
56 organizations
MDSISC Current Activities

- Medical Device Security Information Sharing Initiative
- Listserv to share and exchange information
- Monthly meetings
- Threat briefings
- White papers on threats and best practices
- Medical device track at NH-ISAC summits
- Medical device security workshops
- Sub-groups focused on specific topics
MDSISC Workshops

Completed 2017

• January 2017 Eskanazi Health - IN
• March 2017 Intermountain - UT

Coming Up 2017

• June 2017 Smiths Medical - MN
• June 2017 University of Vermont - VT
• July 2017 UC San Diego – CA
• September 2017 Medtronic - MN
NH-ISAC and MDISS Memorandum of Understanding With FDA

• Press release
  October 2016
• Addresses shared interest and collaboration around medical device cybersecurity

NH-ISAC and MDISS Sign Memorandum of Understanding (MOU) with FDA Around Collaboration of Medical Device Cybersecurity

A shared interest and collaboration in encouraging the identification, mitigation, and prevention of cybersecurity threats to medical devices fosters a MOU between NH-ISAC, MDISS and FDA.

Kennedy Space Center, FL, October 18, 2016 – The National Health Information Sharing and Analysis Center (NH-ISAC), the Medical Device Innovation, Safety and Security Consortium (MDISS), and the U.S. Food and Drug Administration (FDA) Center for Devices and Radiological Health (CDRH) recently signed a MOU to collaborate in areas of mutual interest.

The goals of collaboration include the following:

Create an environment that fosters stakeholder collaboration and communication, and encourages the sharing of information about cybersecurity vulnerabilities that may affect the safety, effectiveness and security of the medical devices, and/or the integrity and security of the surrounding healthcare IT infrastructure.

Develop awareness of the Framework for Improving Critical Infrastructure Cybersecurity and enable HPH sector stakeholders to successfully adapt and operationalize the framework for their organizations and products.

Encourage stakeholders within the HPH Sector to develop innovative strategies to assess and mitigate cybersecurity vulnerabilities that affect their products; and

Build a foundation of trust within the HPH community so that all healthcare technology and medical device stakeholders can directly benefit from the sharing of cybersecurity vulnerability- and/or threat information identified within the HPH Sector, as well as intelligence feeds from other Critical Infrastructure Sectors that may secondarily affect healthcare and the public health.

NH-ISAC & MDISS MOU with FDA
Building A Foundation

Memorandum of Understanding (MOU)
October 2016
FDA & NH-ISAC & MDISS

Call to Action

- Create an environment that fosters stakeholder collaboration and communication
- Develop timely awareness of the Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF)
- Develop innovative strategies to assess and mitigate cybersecurity vulnerabilities before hazard
- Build a foundation of trust within the HPH community
Initiatives

Promote device security, patient safety and critical infrastructure protection

– Medical Device Risk Assessment Platform (MDRAP)
– Medical Device Surveillance and Threat Intelligence (MDSATI)
– Medical Device Vulnerability Information Sharing (MD-VIPER)
Initiatives

MDRAP
Medical Device Risk Assessment Platform

MDSATI
Medical Device Surveillance & Threat Intelligence

MD-VIPER
Medical Device Vulnerability Information Sharing

ICS-CERT
CVE

NVDB

Security Testing Firms
Independent Security Researchers

Malware & Intrusion Experience

Realtime Requirements (Vulnerabilities)

Feedback on New Models

Complete Risk Assessments

MDS2
QA

Healthcare Delivery Organizations

Report Attacks

Incident Alerts

Device Manufacturers

Report Attacks

Incident Alerts

Feedback on New Models
How It Fits

The MD-VIPER Vulnerability Report is designed to serve as an alternate reporting process to FDA’s requirements for 21 CFR Part 806 reporting if cybersecurity vulnerabilities are involved.

Manufacturers are not held to 21 CFR Part 806 reporting requirements if:

- the manufacturer is an active participant in an ISAO (NH-ISAC)
- the manufacturer is conducting a correction/removal to address a cybersecurity vulnerability
- the cybersecurity vulnerability in question has not led to any known serious injuries or deaths
- the manufacturer will meet the timeline criteria for communicating to its customers and then validating and distributing the deployable fix such that the residual risk is brought to an acceptable level
Participation in MD-VIPER

- Open to all medical device security stakeholders
- Free and voluntary*
- Tracking each event (submissions, data sharing event, communication event, etc.)
- Each event is triggered by the manufacturer
- Collaboration with manufacturer
- Responsible sharing of information regarding vulnerabilities and threats in light of specified vulnerabilities for stakeholder awareness

*Need to register and sign NDA
MD-VIPER Reporting Process

- Vulnerability reporter contacts MD-VIPER
- Conversation between reporter and MD-VIPER
- Reporter proceeds with sharing of vulnerability
- Once reported, all data is stationary until a data owner, manufacturer, advises in writing to share the data
- If a third party shares the data, they should be able to advise us, in writing, to share the data
MD-VIPER Site Information

https://mdviper.org/

ABOUT US

The FDA’s Center for Devices and Radiological Health (CDRH), the NHISAC, and the MDISS are collaborating on their shared interests to encourage the identification, mitigation, and prevention of cybersecurity threats to medical devices. This collaboration is designed to foster stakeholder communication and information sharing and enable stakeholders to take proactive and timely measures to mitigate the risks.

- Benefits of Vulnerability Reporting by Manufacturers
- Participation in MD-VIPER
- MD-VIPER Operations
- The FDA, NH-ISAC and MDISS Partnership
- Frequently Asked Questions (FAQ)

Contact Us
MD-VIPER Submission Process

SUBMISSION PROCESS

Where to Report
Vulnerability Reports should be made by using the MD-VIPER Vulnerability Reporting Form on this website.

Confirmation of Submission
All reports submitted will receive confirmation of receipt of the report at the email address provided by the manufacturer in the completed report.

Submitting Updates to a previously submitted Report
Updates to previously submitted reports (including updated remediation plans, communication plans, and timelines) may be filed in accordance with the instructions provided in the confirmation email.

Questions
Direct all questions/inquiries about MD-VIPER Vulnerability Reporting to:

- Telephone: (405) 45VIPER or (405) 458-4737
- Email: mdviper@nhisac.org or mdviper@mdss.org
How It All Fits

- NH-ISAC Membership is dues based and open to organizations that meet membership criteria.
- MDSISC is a special interest Council under the NH-ISAC co-led by MDISS. Open to NH-ISAC & MDISS members.
- MD-VIPER is a NH-ISAC /MDISS initiative open to medical device security stakeholders.

Post-Market Guidance
Case Study

WannaCry
WannaCry

• On May 12, 2017, 4:00am ET multiple companies in Europe started reporting massive ransomware infections several hospitals within the National Health System Trust (NHS) in the UK have their phones systems disabled, turn away patients and cancel surgeries.

• This new ransomware variant is called “WannaCry / WCry / WanaCrypt0r”.

![Image of ransomware warning message]
The Facts

• As of 5/22/17 the ransom campaign stands at approximately 296 payments across 3 bitcoin wallets totaling 49 BTC or $104k.
• Ransomware spread using an SMB vulnerability that was patched by Microsoft in March 2017. Microsoft took the extraordinary step to send out a patch to Windows XP, Windows 8, and Windows Server 2003 versions of software.
• Ransomware sought vulnerable machines over port TCP 445. No infections were seen coming from email or phishing or Remote Desktop Protocol (RDP).
Community In Action

- Sector calls
- Cross-sector calls and collaboration
- NH-ISAC member sharing
- Sharing on NH-ISAC website
  - IOCs
  - Best Practices
  - Threat Intelligence
- Sharing with partners

www.nhisac.org
Community In Action

Go to NH-ISAC.org
For WannaCry Mitigation Strategies
Mitigation Strategies

- **Ensure all patches are up to date.** Microsoft has patches available for all software versions Microsoft XP and higher.
- Issue a companywide communications putting all staff on high alert.
- Prevent delivery and download of .exe attachments both direct and contained inside zip files.
- Ensure SMB (disable ports 139 and especially 445) is not permitted into your environment from external sources. Note especially 3rd party VPN connections.
Mitigation Strategies

- Apply anti-virus patches, many new updates provided since May 12th.
- Block attempts to communicate to unauthorized and new domains.
- Detect/block known hashes. There are multiple lists, including those shared with NH-ISAC membership.
- Review the list of IP hits against the sinkholed domain keeping in mind some positive hits might be from your own security team.
- Continue to share and participate on NH-ISAC forums.
Medical Device Community

• The Press
• The Community
• MDSISC
  • Manufacturer Statements
  • Best Practices
  • Events
  • Facts/Definitions
• United We Stand Divided We Fall

https://mdviper.org/
Case Study #2 Responsible Disclosure

Disclosure

- St. Jude Medical disclosed by Muddy Waters Hedge Fund; no coordination with manufacturer
Case Study #2 Responsible Disclosure

Impact of Disclosure Process

- St. Jude Medical and Researcher have not met
- Exact research methods, vague and don’t support an efficient process by manufacturer to assess the issues and to develop compensation controls
- Resulted in inefficient assessment process and did not support the manufacturer’s ability to clearly assess the assertions
- Less than optimal for the manufacturer and the patient
Case Study #2 Responsible Disclosure

- Johnson & Johnson was disclosed in coordinated manner, per best practices by manufacturer, researcher and ICS-CERT
- Collaborated on a review along with ICS-CERT and FDA
- Led to efficient understanding and development of compensating controls
- Final release coordinated and contained the vulnerabilities, compensating controls and residual risk
- Enabled all parties to make informed clinical decisions
Questions?