Cyber Surveillance and Threat Intelligence Sharing

Session #5, February 19, 2017

Bill Hagestad, Senior Principal Cyber Security Engineer, Smiths Medical
Purna Prasad, PhD, VP, Chief Technology Officer, Northwell Health
Speaker Introduction

Purna Prasad, PhD
VP, Chief Technology Officer
Northwell Health
PPrasad1@northwell.edu
Work Phone: 516-296-0659
Speaker Introduction

Bill Hagestad
Senior Principal Cyber Security Engineer, R&D
Smiths Medical
Work Phone: 763-383-3267
Mob: +1 612 222 9774
Bill.Hagestad@smiths-medical.com
Conflict of Interest

Purna Prasad, PhD
William Hagestad, MSc – Military Strategy, MSc – MOT, MSc Cyber Security

Have no real or apparent conflicts of interest to report.
Agenda

• Definitions
• Qualities & Characteristics
• Threat Classifications
• Types of Threat Intelligence
• Best Practices for Sharing
• Field Experience (UNCLASSIFIED)
• Success Stories
• Q & A
Learning Objectives

• Identify different types and approaches to threat intelligence collection and sharing

• Discuss challenges and barriers to the collection of threat intelligence from medical devices at the device level and the network level

• Summarize available data and trend for threat intelligence for medical devices

• Explain how threat intelligence can impact medical device risk assessment scores
Session 5: Cyber Surveillance and Threat Intelligence Sharing

DESCRIPTION: The paucity of data and information on threat intelligence related to medical devices compromises the building of robust medical device networks. This session will discuss the challenges with collecting and sharing threat intelligence on medical devices.
Information alone is not Intelligence; Intelligence is actionable Information...
**Definitions are important**

**Threat Information**

- Threat information is potential indicators for vulnerabilities to turn into attacks on biomedical devices and networks.

- Threats can include everything from viruses, Trojans, back doors to hacker direct cyber attacks. Often, the term blended threat is more accurate, as the majority of threats involve multiple exploits.

**Threat Intelligence**

- Intelligence is actionable information providing organizations with decision support to achieve a strategic advantage.

- Threat intelligence is a component of security intelligence.

- Threat intelligence: evidence-based knowledge, including context, mechanisms, indicators, implications & actionable advisory regarding current, emerging or future cyber risks & hazards to an organization’s devices, infrastructure or assets.

---

“Threat”. [https://www.techopedia.com/definition/25263/threat](https://www.techopedia.com/definition/25263/threat)

http://whatis.techtarget.com/definition/threat-intelligence-cyber-threat-intelligence

# Qualities Vs. Characteristics

## Threat Information

- **Qualities** –
  - Aggregated from virtually every source
  - May be true, false, misleading, incomplete, relevant, or irrelevant
  - Raw, unfiltered data
  - Unevaluated when delivered

## Threat Intelligence

- **Characteristics**
  - Accurate, timely, complete (as possible), assessed for relevancy
  - Aggregated from reliable sources and cross-correlated for accuracy
  - Evaluated and interpreted by trained expert analysts
  - Processed, sorted, and distilled information

---

Classifications of Threat Intelligence

Attacks Based Techniques

- Threat agent is an actor that imposes the threat on a specific asset of the system which is represented by three classes:
  - human, technological, and force majeure.
- Threat motivation represents the cause of the creation of the threat and it is reorganized into two classes:
  - deliberate and accidental threat
- Threat localization represents the origin of threats, either internal or external.
- Attackers’ prior knowledge about the system: It represents how much the attacker knows about the system in terms of system hardware, software, employees and users knowledge.
- Criticality of the area: It represents the criticality of parts of the system which might be affected by the threat.
- Loss: It represents all losses that can occur in the system or to the organization (privacy, integrity…)


Threats Based Impacts

- STRIDE Model
  - is applied on the network, host, and application. STRIDE allows characterizing known threats according to the goals and purposes of the attacks (or motivation of the attacker).
  - Spoofing identity,
  - Tampering with data,
  - Repudiation,
  - Information disclosure,
  - Denial of service,
  - Elevation of privilege.
- Goal-based approach, where an attempt is made to get inside the mind of the attacker by rating the threats against it
- ISO Model
  - ISO standard (ISO 7498-2) has listed five major security threats impacts and services as a reference model
  - Destruction of information and/or other resources, corruption or modification of information, theft, removal or
  - loss of information and/or other resources, disclosure of information, and interruption of services.
Subset of DoD Internet Host Table

26-Aug-97
Version number @(#)stable.sc 1.3 5/24/95 10:26:07

NOTE: This is a subset of the Official DOD Internet Host Table, netinfo/hosts.txt, and contains data about IP networks only.

Changes, corrections, comments or questions to (HOSTMASTER@NIC.DDN.MIL)

The format of this file is documented in RFC 952, "DoD Internet Host Table Specification", which is available online at NIC.DDN.MIL as filename rfc/rfc952.txt

It may be retrieved via FTP using username "anonymous" with any password.

The format for entries is:

NET : NET-ADDR : NETNAME :
An automated news reader feed comprised of thousands of cyber & information security resources – actionable resources....
- Know your network environments - Web, Mobile, Wireless, Endpoint… what is allowed vs anomalies
- Communicate, collaborate, cooperate – join digital threat intel groups – NH-ISAC and Operation ONA
- Understand Kill Chain Methodologies – interrupt attackers OODA Loop
  o Internal Reconnaissance
  o Internal Exploitation
  o Enterprise Privilege Escalation
  o Lateral Movement
  o Target Manipulation: OBJECTIVE – SPECIFIC (Actions) –
  o Target Manipulation Kill Chain:
  o Target Reconnaissance
  o Target Exploitation
  o Weaponization
  o Installation
  o Execution
An Introduction of How Benefits Were Realized for the Value of Health IT

1Networked medical devices continue to have a profound impact on patient health and clinical management, including:

• Effect of devices on patient treatment plans and quality of life
• Impact on survival and on ability to perform daily activities
• Improved patient function, preventing loss of function, or providing relief from symptoms

The challenge is the risk to patient safety/harm and disclosure of protected health information from numerous points of attack across the health systems environment.

1 Factors to Consider Regarding Benefit-Risk in Medical Device Product Availability, Compliance, and Enforcement Decisions, FDA
The Problem

The increased use of technology, apps, and data sharing from medical devices raises concerns about the security of sensitive health information. Health care organizations must take necessary steps to ensure they are compliant with security and privacy regulations and are protecting consumer health information.

Dr. Purna Prasad
Objective

- Explore strategies for keeping patient health information secure when implementing technology in healthcare delivery.

- Discuss changes within the organization that can improve security of data
What is Privacy

• The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule establishes national standards to protect individuals’ medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.

• The Privacy Rule is located at 45 CFR Part 160 and Subparts A and E of Part 164.

Dr. Purna Prasad
How Does Privacy & Security Threaten the Use of Technology

- Personal Information
- Clinical Information
- Financial Information

- Patient
- Provider
- Payer
- Regulator
Points of Vulnerability

- BYOD – Bring Your Own Device
- WYOD – Wear Your Own Device
- Desktop Devices
- Biomedical Devices
- Servers
- Backup
- Network Gear
BYOD - Bring Your Own Device
Biomedical Devices

**Therapeutic Devices**
- Pacemakers
- Pharmacy cabinets
- Pharmacy dispensers
- Radiation Therapy
- Transfusion Devices
- Infusion pumps

**Diagnostic Devices**
- EKG
- X-Ray
- Blood pressure monitors
- Blood gas
- MRI machines
- Fetal monitors

**Risks:**
- Impact to Patient Safety
- Inappropriate Disclosure of PHI
- Vulnerable medical devices could be used as an entry point to the network
Points of Attack For BYOD

- Mobility Devices
- I/O Ports
- USB
- RJ-45 Network Port
- Fire wire
- Thunderbolt
- RF Carriers
- IOT (Internet of Things)

It’s a Wild West!
Points of Attack For WYOD

† Communication Media
  † Blue Tooth
  † Radio Frequency
  † Infrared
  † Ultrasound
Points of Attack for Desktops

• Thick Clients
• Thin Clients
• Virtualized Clients
• I/O Ports
Points of Attack for Biomedical Devices

• Therapeutic
• Diagnostic
• I/O Ports
• RF Interference
Points of Attack for Servers

✦ On Premises

- Traditional
- Virtualized
- I/O Ports

✦ Cloud
The Line is very blurred and will vanish

- Biomedical Devices designed using the PC architecture
- Biomedical Devices land as software application on IT devices
  - Desktop
  - Laptop
  - Handheld
  - Wearable
- Clinical Data and non-clinical data propagate on the same network
- Clinical Data and non-clinical data use the same backend network and storage devices
<table>
<thead>
<tr>
<th>Date</th>
<th>Source</th>
<th>Security Finding</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>Black Hat Conference</td>
<td>Ability to remotely interfere with the clinical operation of an insulin pump demonstrated</td>
</tr>
<tr>
<td>2012</td>
<td>Black Hat Conference</td>
<td>Use of a pacemaker to deliver electrical shock to patient</td>
</tr>
<tr>
<td>2013</td>
<td>US GAO</td>
<td>Reported on the above 2 cases and suggested FDA be more involved</td>
</tr>
<tr>
<td>2014</td>
<td>TrapX Security</td>
<td>60 hospitals tested to reveal compromised medical devices</td>
</tr>
<tr>
<td>2015</td>
<td>FDA</td>
<td>Hospitals notified to stop using Hospira’s Symbiq infusion pumps</td>
</tr>
<tr>
<td>2015</td>
<td>Bloomberg</td>
<td>“It’s Way Too Easy to Hack the Hospital” (Mayo Clinic Research paper)</td>
</tr>
</tbody>
</table>
Medical Device Security Challenges

- Lack of regulatory governance and enforcement which requires medical device manufacturers to be accountable for security
- Vulnerabilities in the embedded computers systems of medical devices could cause:
  - Unauthorized adjustment, posing a risk to patient safety
  - Unauthorized reading, constituting a breach under HIPAA
  - Unauthorized access, resulting in access to the health system network
  - Misuse or unauthorized use could interfere with normal operations

Dr. Purna Prasad
Medical Device Security Challenges

- Depth of the scope is unknown due to:
  - Many models of a particular device type
  - Many device types per facility
  - Absence of life cycle management of hardware and software
  - No consistent or centralized management of devices today
  - No documented standards or governance structure oversight
A Universal Platform For Sharing Medical Device Threat Intelligence (MDTI)

A secure web-based database accessed and managed by manufacturers, providers, payers, regulators, and patients.

- Similar to the Medical Device Reporting database
- Potential to adopt reporting format similar to drug dosing guidelines from the pharmaceutical sector
- Focused on keeping the patient safe
- A governance board with stakeholder representation decides the content
Challenges

- No industry standard for maintaining and reporting on medical device inventories
- Limited leverage to guide the stakeholders to maintain security controls and practices
- Lack of stakeholder understanding regarding potential threats to medical devices
- Forming a governance structure with representation from key stakeholder departments to establish industry-wide medical device cyber security standards, threat intelligence reporting and potential resolutions.

Dr. Purna Prasad
## Recommendations

<table>
<thead>
<tr>
<th>Design</th>
<th>Develop</th>
<th>Implement</th>
<th>Sustain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Governance Committee/Council</td>
<td>Establish policies and standards</td>
<td>Governance Model and Medical Device Security Reporting Policy</td>
<td>Execute</td>
</tr>
<tr>
<td>Manufacturers</td>
<td>Define prioritized assessment, remediation and reporting framework</td>
<td>Medical device security training and awareness</td>
<td>Monitor</td>
</tr>
<tr>
<td>Care Providers</td>
<td>Develop plan to implement and strengthen technical controls</td>
<td>Technical controls and inventory management tools</td>
<td>Assess</td>
</tr>
<tr>
<td>Payers</td>
<td></td>
<td>Standard contract language to require security maintenance</td>
<td>Refine</td>
</tr>
<tr>
<td>Regulators</td>
<td></td>
<td></td>
<td>Participate in information exchange forums</td>
</tr>
<tr>
<td>Patients</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create Charter</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Align Stakeholders</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Define Scope</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop Strategy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop Roadmap</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Manufacturers
- Care Providers
- Payers
- Regulators
- Patients

### Stakeholders

- Form Governance Committee/Council
- Manufacturers
- Care Providers
- Payers
- Regulators
- Patients

### Create Charter

- Align Stakeholders
- Define Scope
- Develop Strategy
- Develop Roadmap
Next Steps

- Brainstorming sessions with members from the stakeholder domain
- Formation of a governance committee
- Determine roles, responsibilities, governance structure, etc.
A Summary of How Benefits Were Realized for the Value of Health IT

Medical devices can have a very positive impact on patient health, patient treatment plans and quality of life. However, the networked medical device infrastructure in healthcare systems environments is threatened by the numerous points of attack including, but not limited to I/O ports, RF interference, and malware attacks. Effective cybersecurity risk management is needed to reduce the risk to patients and their personal information/protected health information.
Purna Prasad, PhD
VP, Chief Technology Officer
Northwell Health
Work Phone: 516-296-0659
PPrasad1@northwell.edu

Bill Hagestad
Senior Principal Cyber Security Engineer, R&D
Smiths Medical
Work Phone: 763-383-3267
Mob: +1 612 222 9774
Bill.Hagestad@smiths-medical.com