Securing Wireless Medical Infusion Pumps – A Use Case

Session 168, February 22, 2017

Gavin O’Brien, Computer Scientist, NCCoE/NIST
Rob Skelton, Program Manager, BD (Becton, Dickinson and Co.)
Speaker Introduction

Gavin O’Brien, MS Computer Science
Computer Scientist and Project Manager
National Cybersecurity Center of Excellence (NCCoE)
at the National Institute of Standards and Technology (NIST)
Speaker Introduction

Rob Skelton, Corp. Product Security Program Manager
BD Medical Device Manufacturing: Alaris Infusion
Conflict of Interest

Gavin O’Brien, MS Computer Science
NIST NCCoE is a federal laboratory and Gavin has no real or apparent conflicts of interest to report.

Rob Skelton, Corp. Product Security
BD is a global medical technology company and Rob has no real or apparent conflicts of interest to report.
Agenda

• About the NCCoE
• Wireless Infusion Pump: Use Case
  – Overview
  – Risk Assessment
  – Architecture
  – Evaluation
  – Cybersecurity Challenges
• Q&A
Learning Objectives

• Demonstrate how healthcare providers can use a solution developed by the NCCoE to secure their medical devices on an enterprise network, with a specific focus on wireless infusion pumps

• Evaluate risks associated with threats and vulnerabilities related to medical devices and the wide array of technologies that can be employed to mitigate these risks

• Recognize how to implement similar security controls in existing healthcare environments

• Gain applied knowledge of how to implement similar security controls in existing healthcare environments
Realizing the Value of Health IT

- Improve Cybersecurity
  Through collaboration and development of an example implementation

- Improve Cyber Safety
  Through educating healthcare providers about effective cybersecurity controls

Health IT creates five kinds of value of benefit to patients, healthcare providers and communities.
Strategic Plan

VISION
ADVANCE CYBERSECURITY
A secure cyber infrastructure that inspires technological innovation and fosters economic growth

MISSION
ACCELERATE ADOPTION OF SECURE TECHNOLOGIES
Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

GOAL 1
PROVIDE PRACTICAL CYBERSECURITY
Help people secure their data and digital infrastructure by equipping them with practical ways to implement standards-based cybersecurity solutions that are modular, repeatable and scalable

GOAL 2
INCREASE RATE OF ADOPTION
Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

GOAL 3
ACCELERATE INNOVATION
Empower innovators to creatively address businesses’ most pressing cybersecurity challenges in a state-of-the-art, collaborative environment
Foundations

**NIST ITL**
The NCCoE is part of the NIST Information Technology Laboratory and operates in close collaboration with the Computer Security Division. As a part of the NIST family, the center has access to a foundation of prodigious expertise, resources, relationships and experience.

**PARTNERSHIPS**
The NCCoE is motivated by results. Established in 2012 through a partnership between NIST, the State of Maryland and Montgomery County, the NCCoE is dedicated to furthering innovation through the rapid identification, integration and adoption of practical cybersecurity solutions.
Tenets

Standards-based
Apply relevant local, national, and international standards to each security implementation; demonstrate reference designs for new standards

Modular
Develop reference designs with individual components that can be easily substituted with alternates that offer equivalent specifications

Repeateable
Enable anyone to recreate builds with same results by providing a complete practice guide including a reference design, bill of materials, configuration files, relevant code, diagrams, tutorials and instructions

Commercially Available
Work with the technology community to identify commercially available products that can be brought together in reference designs to address challenges

Usable
Design usable blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

Open and Transparent
Use open and transparent processes to complete work, and seek and incorporate public comments on NCCoE documentation, artifacts and results
Sector Based vs Cyber Specific Projects

The NCCoE seeks sector-based problems that are:

• Broadly applicable across much of a sector, or across sectors
• Complex enough that our reference designs will need to be based on the combination of multiple commercially available technologies
• Incorporates a combination of cybersecurity standards and industry based standards

Cyber Specific

• Cybersecurity technology-specific problems that cross sector boundaries (e.g., roots of trust in mobile devices, trusted cloud computing, software asset management, attribute based access control)
NCCoE Project Lifecycle

- **Needs Assessment**
  - Identify industry’s most pressing cybersecurity challenges

- **Concept Analysis**
  - Define, prioritize and validate the highest priority cybersecurity challenges

- **Develop Use Case**
  - Collaborate with our Community of Interest to develop a Use Case

- **Form Build Team**
  - Invite participation from industry and build a qualified team to execute the Use Case and develop a reference solution

- **Design & Build**
  - Plan, design, and build the Use Case reference solution in a lab environment and capture in the Practice Guide

- **Integrate & Test**
  - Test and validate the Use Case reference solution

- **Publish & Evangelize**
  - Publish, post, and demonstrate the reference solution documented in the Practice Guide
NCCoE Healthcare Stakeholders

Community of Interest (COI)

A group of participants with a common interest in cybersecurity and healthcare

*Sponsored by NIST, the National Cybersecurity Federally Funded Research & Development Center (FFRDC) is operated by the MITRE Corporation
Securing the U.S. Economy

CURRENT SECTORS OF FOCUS

HEALTH IT
• EHRs and Mobile Devices
• Wireless Infusion Pumps

Consumer/Retail: Multifactor Authentication for e-Commerce

Energy
• IdAM
• Situational Awareness

Financial
• Access Rights Management
• IT Asset Management

Manufacturing: Securing Industrial Control Systems

Public Safety/First Responder
• Authentication for Law Enforcement Vehicle Systems
• Mobile Application Single Sign-On

Transportation: Maritime: Oil & Natural Gas
Wireless Infusion Pump Use Case
Infusion Pump Build Team

Working Groups

Pump Vendors
- Baxter Healthcare Corporation
- B.BRAUN Medical
- BD
- Hospira/Pfizer
- Smiths Medical

Risk Assessment and Testing
- Clearwater Compliance
- MDISS
- Ramparts Security
- Virta Laboratories

Infrastructure/Cybersecurity
- CA Technologies
- Cisco
- Symantec Corporation
- TDi Technologies

Focused Cybersecurity
- DigiCert
- Intercede
- PFP Cybersecurity
Partner: BD (Becton Dickinson & Co.)

Why would a for-profit company participate in a project like this one?

High Level Reasons:

Commitment to cybersecurity: Participation sends a strong message through to 8 separate BD business units that we are open to process and security improvements that can be identified in many ways and even on a national level.

– Publishing and posting the Use Case is a great start but is not the end of the process. This commitment will make a real difference to our customers

System of systems: Product security has evolved from early stand alone device protections that now must include customer enterprise network device interoperability protections.

Continual improvement: As a collaboration and a cyclical process, it is critical to meet the ever changing security threat landscape. Now that activity is being applied to medical devices.
Partner: BD (Becton Dickinson & Co.)

Why would a for-profit company participate in a project like this one?

High Level Reasons:

**Transparency:** A strategic advantage in the marketplace by sharing and being transparent.

**Collaboration:** Collaborating with several of our competitors in the case study to make future security decisions at hospitals faster, easier and more comprehensive.

**Practical Guidance:** The development of a Use Case reference will address our industries most pressing cybersecurity issues.
Partner: BD (Becton Dickinson & Co.)

Why would a for-profit company participate in a project like this one?

Project Specific Reasons:

Improving provider cybersecurity: The goal of the Use Case is to help healthcare providers to continue to secure their wireless infusion pumps on their enterprise networks.

Messaging for the C-suite: Because vulnerabilities are foremost on upper management’s mind, participation in open sharing and better standards is key.

Raising the bar: We believe in challenging ourselves and the industry to address cybersecurity implementation concerns head on.
Wireless Infusion Pump Project Recap

Help healthcare delivery organizations (HDOs) understand risks and secure medical devices on an enterprise network
• Focus on wireless infusion pumps as archetype of a medical device

Tasks include
• Assess risk
• Identify mitigating security technologies
• Build example implementation
• Independent validation of implementation

Publication of a practice guide
• NIST Special Publication 1800 series
  – SP 1800-{d}a: Executive Summary
  – SP 1800-{d}c: How-To Guides
# Practice Guide Outline Vol B:
## Approach, Architecture, and Security Characteristics

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Summary</td>
</tr>
<tr>
<td>1.1</td>
<td>The Challenge</td>
</tr>
<tr>
<td>1.2</td>
<td>The Solution</td>
</tr>
<tr>
<td>1.3</td>
<td>Risks</td>
</tr>
<tr>
<td>1.4</td>
<td>Benefits</td>
</tr>
<tr>
<td>1.5</td>
<td>Technology Partners</td>
</tr>
<tr>
<td>1.6</td>
<td>Feedback</td>
</tr>
<tr>
<td>2</td>
<td>How to Use This Guide</td>
</tr>
<tr>
<td>3</td>
<td>Introduction</td>
</tr>
<tr>
<td>4</td>
<td>Approach</td>
</tr>
<tr>
<td>4.1</td>
<td>Audience</td>
</tr>
<tr>
<td>4.2</td>
<td>Scope</td>
</tr>
<tr>
<td>4.2.1</td>
<td>Assumptions</td>
</tr>
<tr>
<td>5</td>
<td>Risk</td>
</tr>
<tr>
<td>5.1</td>
<td>Security Characteristics and Controls Mapping</td>
</tr>
<tr>
<td>5.2</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>5.3</td>
<td>Risk Mitigation</td>
</tr>
<tr>
<td>6</td>
<td>Architecture</td>
</tr>
<tr>
<td>6.1</td>
<td>Architecture Overview</td>
</tr>
<tr>
<td>6.2</td>
<td>Usage Scenarios</td>
</tr>
<tr>
<td>6.3</td>
<td>Usage Scenarios Mapping</td>
</tr>
<tr>
<td>7</td>
<td>Security Evaluation</td>
</tr>
<tr>
<td>7.1</td>
<td>Assumptions and Limitations</td>
</tr>
<tr>
<td>7.2</td>
<td>Application of Security Characteristics</td>
</tr>
<tr>
<td>7.2.1</td>
<td>CSF Subcategories that are supported</td>
</tr>
<tr>
<td>7.3</td>
<td>Testing</td>
</tr>
<tr>
<td>7.4</td>
<td>Scenarios and Findings</td>
</tr>
<tr>
<td>7.5</td>
<td>Security Evaluation Summary</td>
</tr>
<tr>
<td>8</td>
<td>Functional Evaluation</td>
</tr>
<tr>
<td>8.1</td>
<td>IP-1 – Event Correlation – Access Control</td>
</tr>
<tr>
<td>8.2</td>
<td>IP-2 – Event Correlation – Monitoring</td>
</tr>
</tbody>
</table>
Risk Assessment

- Risk Assumptions
- Risk Constraints
- Priorities and Tradeoffs
- Risk Tolerance
- Uncertainty

ORGANIZATIONAL RISK FRAME
RISK MANAGEMENT STRATEGY OR APPROACH

- Establishes Foundation for Risk Management
- Delineates Boundaries for Risk-Based Decisions

Risk Assessment Methodology

- Risk Assessment Process
- Risk Model
- Assessment Approach
- Analysis Approach
Risk Methodology

• Questionnaires based risk assessment tool

• The assessment tool contains threats, vulnerabilities and controls

• The questionnaires are used to capture the healthcare providers’ environment

• Measures likelihood, severity and impact
# Product Security Features: CSF Mapping

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Cybersecurity Framework</th>
<th>Company</th>
<th>Product (V.)</th>
<th>Architecture Element</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY (ID)</td>
<td></td>
<td>Asset Management (ID.AM)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Business Environment (ID.BE)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Governance (ID.GV)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk Assessment (ID.RA)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk Management Strategy (ID.RM)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROTECT (PR)</td>
<td></td>
<td>Access Control (PR.AC)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Awareness and Training (PR.AT)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Security (PR.DS)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information Protection Processes and Procedures (PR.IP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintenance (PR.MA)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Protective Technology (PR.PT)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DETECT (DE)</td>
<td></td>
<td>Anomalies and Events (DE.AE)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Continuous Monitoring (DE.CM)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Detection Processes (DE.DP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RESPOND (RS)</td>
<td></td>
<td>Response Planning (RS.RP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Communications (RS.CO)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Analysis (RS.AN)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mitigation (RS.MI)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Improvements (RS.IM)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RECOVER (RC)</td>
<td></td>
<td>Recovery Planning (RC.RP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Improvements (RC.IM)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Communications (RC.CO)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Baseline Standards and Guidance

- **NIST**
  - Cybersecurity Framework (CSF)
  - Risk Management Framework (RMF)
  - SP 800-53: Security Controls

- **FDA**
  - Cybersecurity Premarket Guidance
  - Cybersecurity Postmarket Guidance

- **ISO/IEC 80001**: Application of Risk Management for IT Networks Incorporating Medical Devices

- **IHE**: Medical Device Cyber Security - Best Practice Guide

- **AAMI TIR57**: Principles for Medical Device Security - Risk management
Wireless Infusion Pump Case Scope

The scope of this use case is to follow the life cycle of an infusion pump from planning the purchase of the pump to decommissioning the device.

Life cycle management includes:

• Procurement
• On boarding of asset
• Training and instructions for use
• Configuration
• Usage
• Maintenance
• Decontamination
• Decommissioning Devices
High Level Architecture

- Holistic approach to Use Case reflected in architecture
- Focus on technical aspects for Use Case build
- Focus on core functionality and cybersecurity of infusion pump for Practice Guide
Primitive Architecture

Internet

Cloud Services

Guest Network

Guest Network

MySQL

Oracle

MS SQL

Email

backup

eHR

IPS

Rx

CoW/WoW

Drug Library

Pump Server

Pump Server

Pump Server

Pump Server

Pump Server

CPOE

AD

DNS

#HIMSS17

WHERE THE BRIGHTEST MINDS IN HEALTH AND IT MEET

HIMSS17
Network Architecture - Plus Cybersecurity Controls

- Guest Network
- Business Offices
- Database Server
- Enterprise Services
- Clinical Services
- Biomedical Engineering
- Medical Device

- Core Network Infrastructure
- Cloud Services
- Vendor Support

- External Firewall
- ASA
- SSL/TLS
- Certificate Authority
- ATP-N
- IPS
- DNS
- Authenticated OSPF
- Protected Remote Access
- Security Proxy
- CAPWAP (DTLS)
- WPA2

- Drug Library
- Secure API
- Device Behavior Detection
- Code Signing
- OS Hardening
- Encryption
- Authentication
- Anti-Tamper
- Device Behavior Detection
- Secure API

- Network Discovery
- Certificate Management/Provisioning
- Network Architecture
- Vendor
- VPN Client
- Protected Remote Access
- Security Proxy
- Vendor Support
Infusion Pump Security Challenges

• Access codes
• Access point (AP)/Wireless network configuration
• Asset management and monitoring
• Credentialing
• Credentialing server
• Maintenance and updates
• Pump variability
Infusion Pump Project Status

- Completed the build phase
- Evaluate the solution
- Publish draft of practice guide
Future Projects

• Asset / Inventory/Management
• Device Encryption (Encryption Test Harness)
• Securing PACS Systems
• Information Sharing / Cyber Threat Intelligence (CTI)
• Secure messaging for Healthcare business devices
Realizing the Value of Health IT

**Improve Cybersecurity**
Through collaboration and development of an example implementation

**Improve Cyber Safety**
Through educating healthcare providers about effective cybersecurity controls
Questions

Gavin O’Brien, Computer Scientist, NCCoE/NIST
Rob Skelton, Program Manager, BD (Becton, Dickinson and Co.)

http://nccoe.nist.gov  301-975-0200  nccoe@nist.gov