Overview of AAMI Efforts and Open Issues in Medical Device Security

Ken Hoyme
Distinguished Scientist
Adventium Labs
ken.hoyme@adventiumlabs.com
www.adventiumlabs.com
June 12, 2014
Medical Culture

The focus of hospitals and device manufacturers is on saving lives. Physical pharmacy security

Security focused on data privacy and protecting old software from infection.

Experience says the attacker is either out for personal gain – drugs, fame, sellable information or it is non-targeted.

“Faith-based” security risk assessment.

Many find it inconceivable that anyone would want to harm a sick patient.

© 2014 Adventium Labs
Developer Skill-sets

• Medical devices are cyber-physical systems
• Medical Device Security is much more than confidentiality of patient data – it is about safety

IT Security personnel are often missing:
• Real-time, embedded systems experience.
• Safety risk management culture.
• Regulated device constraints – Quality Systems.

Medical device personnel are often missing:
• Understanding the subtle behaviors of security protocols.
• How to assess risk of future behavior of an adversary.
• Safety risk management is very experiential/data driven.

Hybrid-skills or appropriately configured cross-functional teams are required
Medical Device (Safety) Risk Management

• “Systematic application of management policies, procedures, and practices to the tasks of analyzing, evaluating, controlling, and monitoring risk” – ISO 14971

• Requires risk ranking
  – Between risks.
  – Individual acceptability.
  – Overall residual risk.
AAMI – Device Security Working Group

• Developing guidance document for applying ISO 14971 to device security risk management
  – Terminology.

• Group was formed in May 2013

• Driving to early 2015 release
AAMI TIR - Security Risk Management

- Extend the assessment of risk to incorporate sources that arise from loss of device security
- Main body parallels the requirements sections of ISO 14971
- Specific focus on risk assessment
  - Likelihood/Attractiveness
  - Severity/Impact
- Strong ties to NIST SP800-30r1
AAMI TIR – Best Practices

• Documenting best practices with significant set of references
  – Focusing on medical device specifics as much as possible.

• Organized along the following main themes
  – How to assess security risk for a device.
  – Best practices for secure device design.
  – Best practices for device security testing.
  – Considerations for post-market surveillance, and particularly plans for security maintenance.
ANSI/AAMI/IEC 80001 Standards

• “Application of risk management for IT-networks incorporating medical devices”
• Defines roles and responsibilities of
  – “Responsible Organization”
  – Medical IT Integration Risk Manager
  – IT-Network Maintainer
  – Device Manufacturers
• 80001-2-2 addresses disclosure of device security characteristics
• Use is still mostly voluntary
Calibrating Safety and Security Risks

• Organizations must decide where to invest to reduce the greatest risks
  – Classic safety risks will compete with security risks for resources.

• Traditional risk models differ between domains
  – Quantitative vs. qualitative.

• Useful methods for calibrating different risk models are lacking
Challenge: Hospital Systems Integration

Aviation

- Requirements
- Tests
- Change orders
- Design Reviews

Sub-system Suppliers

- Many standards used, but thoroughly verified at many levels

Health Care

- Standards implementation quality set by certifiers
- Approval cycles can inhibit change

Device Manufacturers

- RFPs
- Specifications
- Submission data
- Approvals
- Audits
- Certificates

Regulators

- Devices
- Documents
- Certificates

Certifiers

- Designs
- Devices
- Documents
Safe & Secure Hospital-integrated Device Networks

• What needs to be standardized to enable hospital device integration?
  – Message structures
  – Nomenclature
  – Mode logic
  – Timing, freshness, QoS
  – Security properties
  – Error behaviors – to faults and security events
  – ...

• What tools are required?
  – “Plug and Play” versus analysis tools
AAMI/UL Joint Committee 2800

• Developing a family of standards to address safe medical device interoperability

• Three dimensions being evaluated
  – Definition of a JC2800-compliant architecture.
  – “Vertical” standards for specific problem domains – e.g. patient-controlled analgesia.
  – “Horizontal” standards to address safety, security, and other “ilities.”

• Still deciding how “deep” they go in standardized elements
Balancing Security and Usability in Clinical Use

• IEC 62366 addresses usability engineering processes for medical devices
  – Does not explicitly address device security.
  – Specific to the use of a single device.

• Clinical workflow
  – Team of people.
  – Multiple devices from different manufacturers.
  – Serving multiple patients in a work shift.

• Potential need for common security controls
  – And common means for access/logging in an emergency situation.
Summary

• AAMI addressing device security process for manufacturers
  – FDA Draft Guidance will drive its use.

• ANSI/AAMI/IEC 80001 addresses security processes for hospital networks
  – But its use is not generally required.

• There is a big educational need

• Medical Device Security Research needs include
  – How to create safe and secure device networks from the “bottom up.”
  – What security controls should be standardized to reduce user confusion?