RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: MBS-W05

Wireless Infusion Pumps: Securing Hospitals' Most Ubiquitous Medical Device

Nate Lesser
Deputy Directory
National Cybersecurity Center of Excellence
NIST

In the News

HEALTH

HACKED MEDICAL DEVICES MAY BE THE BIGGEST CYBER SECURITY THREAT IN 2016

Threat matrix: Malware and hacking pose dangers to medical devices

NEWS

Attackers targeting medical devices to bypass hospital security

Lax medical device security needs urgent action

Medical Devices Used as Pivot Point in Hospital Attacks: Report

Risks, Threats, Vulnerabilities to Infusion Pumps

RISKS	THREATS	VULNERABILITIES
• Patient safety (lives) • Operational/downtime • Patient trust & staff morale	• Collateral damage • Malware • Theft/loss • Lateral attack • Hacktivism	• Tightly regulated "turn-key" systems • Long useful life • Poorly protected & patched • No detection & alerting • System complexity

Courtesy of Axel Wirth

Infusion Pumps

- Infusion pumps are medical devices that deliver fluids and medications into a patient's body in controlled amounts.
- Infusion pumps among the most are ubiquitous connected medical devices in hospitals.
  - Estimated that more than 2 million infusion pumps are in use in hospitals.

Infusion Pumps in the News

WIRED

HACKER CAN SEND FATAL DOSE TO HOSPITAL DRUG PUMPS

BloombergBusiness

Hospital Drug Pump Can Be Hacked Through Network, FDA Warns

WIRED

VIDEO SHOWS A TERRIFYING DRUG INFUSION PUMP HACK IN ACTION

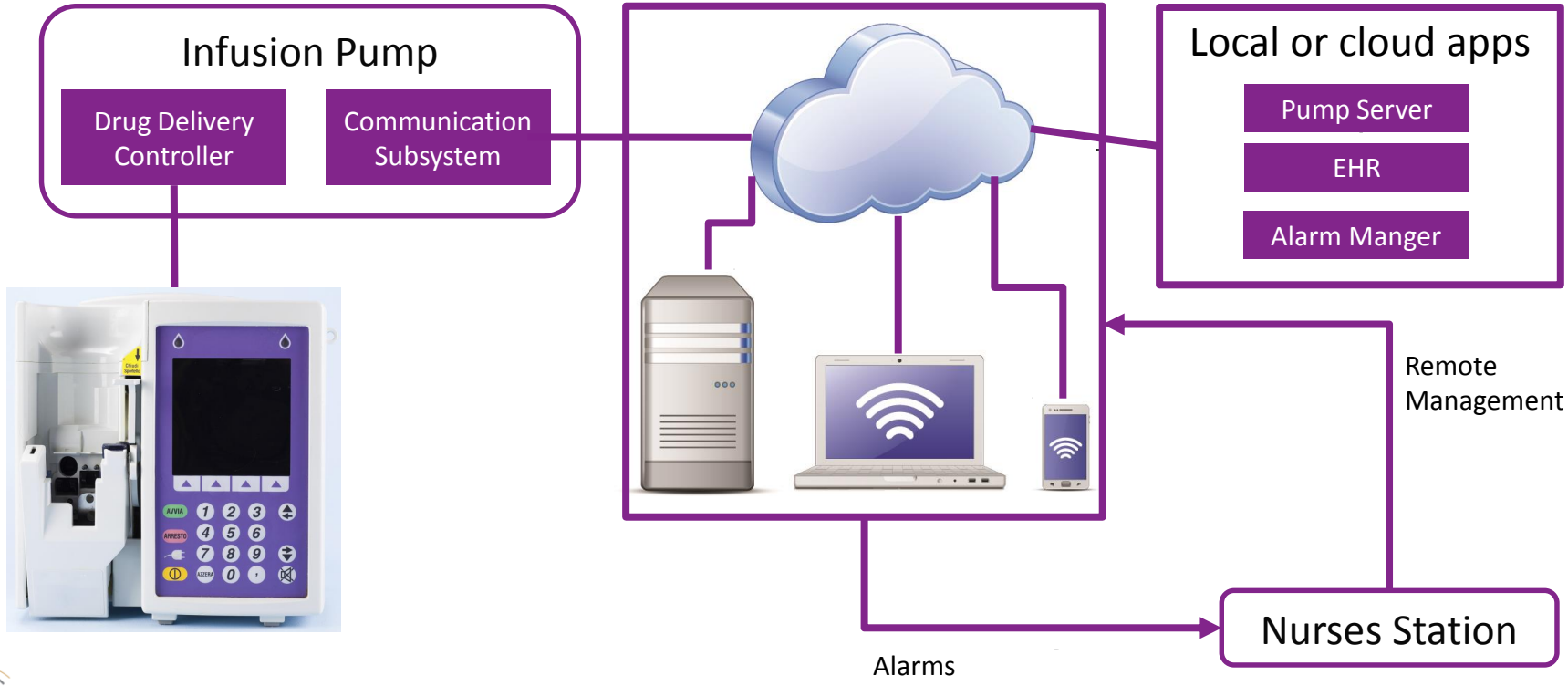
Infusion Pump Vulnerability Notices

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

- FDA Safety Communication on Vulnerabilities of Infusion Pump Systems, May 13, 2015: recommendation for health care facilities to secure affected infusion pumps.
- ICS-CERT Advisory (ICSA1512501B): provides details of vulnerabilities including CVE numbers and CVSS scores.
- Postmarket Management of Cybersecurity in Medical Devices: draft guidance on cybersecurity risk management, remediation, and reporting

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

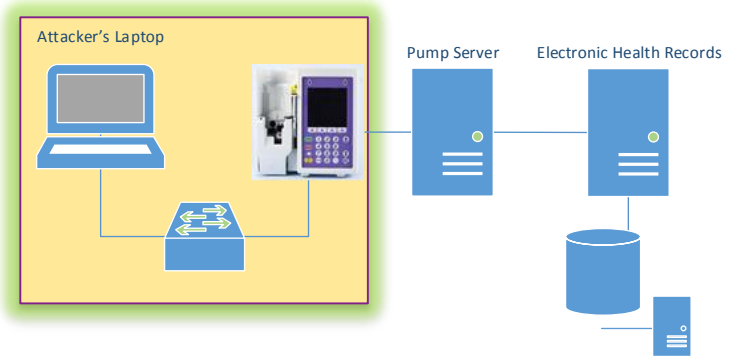
Infusion Pump Physical Architecture



Demo

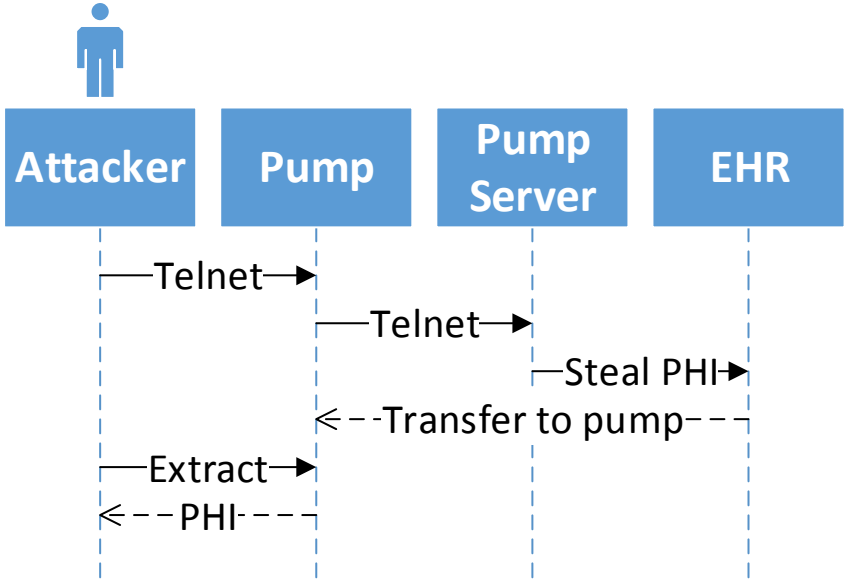
Exploit #1: Compromise Patient Information

- TELNET access to “root” account
  - No authentication required
  - CVE-2015-3459
- Risk
  - Gain root access to pump
  - Pump used as a pivot



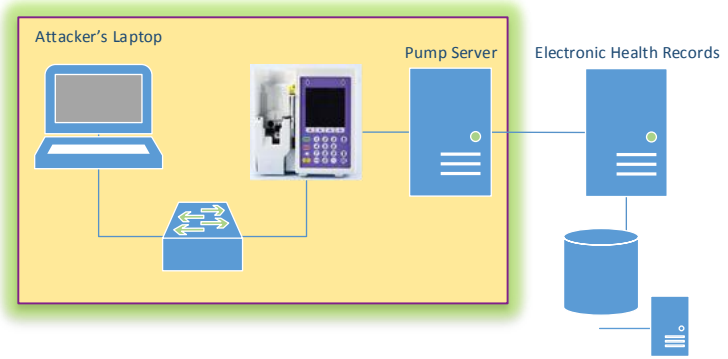
Exploit #1: Compromise Patient Information

- Unauthenticated telnet to pump
  - Use pump to pivot
- Extract desired information
- Move information to web server
- Extract via web browser



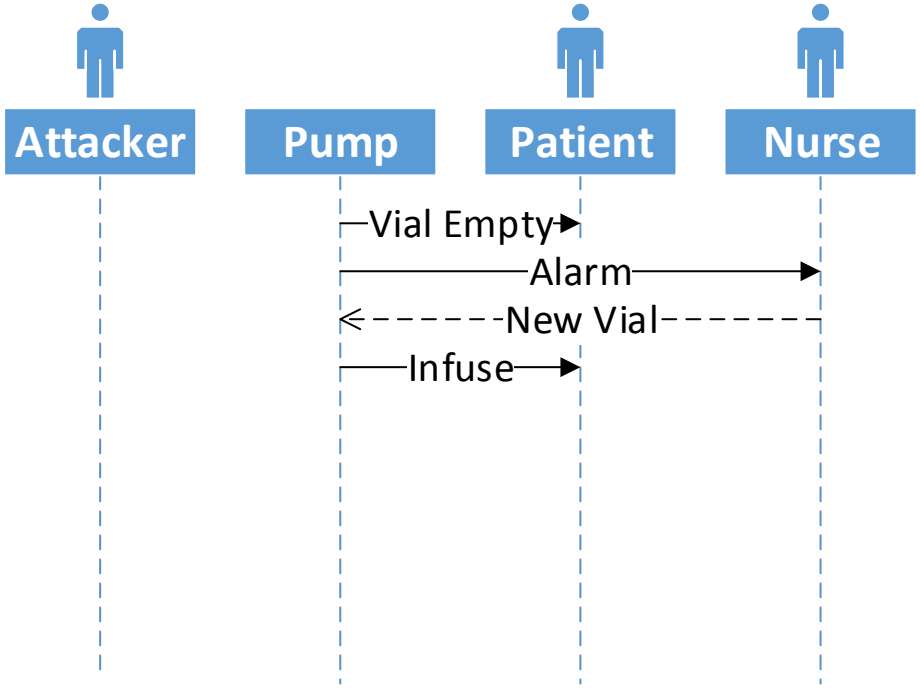
Exploit #2: Crash Communication Subsystem

- Denial of service attack
  - Stops network communication
  - Using resource consumption
  - Can corrupt flash file system
- Risk
  - Stops pump from sending alerts and messages



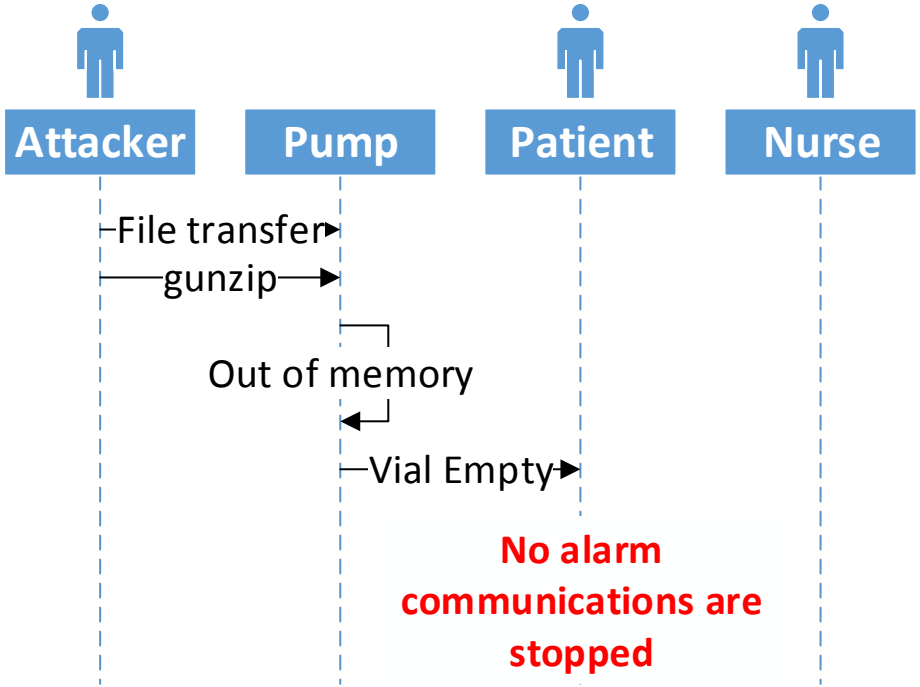
Exploit #2: Crash Communication Subsystem

- Normal Operations
- Error condition
  - Empty vial
  - Alarm sent
- Error condition cleared
  - Nurse replaces vial
- Infusion resumes



Exploit #2: Crash Communication Subsystem

- Anonymous FTP to pump
- Upload gzip'd file
- TELNET access to "root" account
- gunzip file
  - Consumes all available RAM
  - Corrupts part of file system
    - No file system repair tools



All Devices Have Vulnerabilities

- Although the vulnerabilities might not be known
- Just because it's vulnerable doesn't mean it's exploitable
- Patching may not be possible right away

Wireless Infusion Pump Problem Statement

RESEARCH

- Help health care delivery organizations understand risks & secure medical devices on an enterprise network
- Focus on wireless infusion pumps as archetype of medical device

BUILD

- Assess risk
- Identify mitigating security technologies
- Build example implementation
- Independent validation of implementation

SHARE

- Publish practice guide: NIST Special Publication 1800 series

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Challenges

- Firmware version control
  - Multiple versions in service
- Access control
  - Physical and networked
  - “Break the glass”
  - Malware or other unexpected software on pump
- Wireless access point and network configuration
- Alarms
- Asset management and monitoring
- Identity management and Credentialing
- Maintenance and firmware updates
- Pump variability
  - Multiple types of pumps
  - Multiple models in usage

NCCoE Strategy

MISSION

ACCELERATE ADOPTION OF SECURE TECHNOLOGIES

Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

VISION

ADVANCE CYBERSECURITY

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

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NCCoE Tenets

Standards-based: Apply relevant local, national and international standards to each security implementation and account for each sector's individual needs; demonstrate reference designs for new standards

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

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

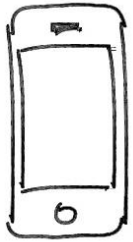
Commercially available: Work with the technology community to identify commercially available products that can be brought together in reference designs to address challenges identified by industry

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

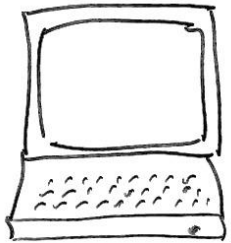
NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Participate

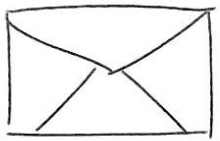


301-975-0200

hit_nccoe@nist.gov



http://nccoe.nist.gov



100 Bureau Dr, M/S 2002
Gaithersburg, MD 20899

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE