Implantable Medical Devices – Cyber Risks and Mitigation Approaches

NIST Cyber Physical Systems Workshop
April 23-24, 2012

Dr. Sarbari Gupta, CISSP, CISA
sarbari@electrosoft-inc.com; 703-437-9451 ext 12
Agenda

- Overview of IMDs
- Security Threats, Vulnerabilities and Risks
- Risk-Based Mitigation Approach
- Summary
- References
What is an IMD?

- Implantable Medical Device (IMD)
  - Tiny computing platform with firmware
  - Runs on small batteries
  - Programmable
  - Implanted in human body
  - Monitors health status
  - Delivers medical therapy
- Pacemakers
- Implantable Cardiac Defibrillators (ICD)
- Cochlear Implants
- Insulin Pumps
- Neurostimulators
Wireless Implantable Medical Devices

Deep Brain Neurostimulators

Cochlear Implants

Gastric Stimulators

Cardiac Defibrillators/Pacemakers

Foot Drop Implants

Insulin Pumps

Courtesy of [http://groups.csail.mit.edu/netmit/IMDSHield/](http://groups.csail.mit.edu/netmit/IMDSHield/)
- Consists of battery, computerized generator, and wires with sensors at tips (pacing leads)
  - Wires connect generator to the heart

- Records heart's electrical activity and rhythm
  - Recordings used to adjust pacemaker therapy

- On abnormal heart rhythm
  - Generator sends electrical pulses to heart

- Can monitor blood temperature, breathing etc.
  - Can adjust heart rate to changes in your activity

- Wireless communication with Programmer
  - Read battery status and heart rhythms
  - Send instructions to change therapy
Wireless Insulin Pump

- Supports blood sugar monitoring & insulin delivery
- Wireless integration of Monitor and Pump
- Pump pre-set with user-specific information
- Monitor transmits glucose value to pump via wireless
- Pump calculates and delivers proper insulin dosage
- Pump “remembers” dosage history
- PC “dongle” can connect to Pump to read data or update settings
Cochlear implants

While hearing aids can only amplify sound, a cochlear implant transforms sound into electrical energy that is used to stimulate auditory nerves in the inner ear.

1. Sounds are picked up by a microphone that is mounted on the external ear piece.
2. The speech processor digitizes the sound into signals and sends the signals to the transmitting coil.
3. A transmitting coil sends the coded signals as radio waves to the cochlear implant under the skin.
4. The internal processor is placed in the mastoid bone behind the ear. The cochlear implant delivers electrical energy to an array of electrodes, which has been inserted into the cochlea.
5. The electrodes along the array stimulate the remaining auditory nerve fibers in the cochlea.
6. The resulting electrical sound information is sent through the auditory system to the brain.

SOURCE: University of Miami Leonard M. Miller School of Medicine
IMD Data

- IMD holds various Data Types
  - Static Data
    - Device make
    - Model #
  - Semi-static Data
    - Physician & Health Center Identification
    - Patient Name and DOB
    - Medical condition
    - Therapy configuration
  - Dynamic Data
    - Patient health status history
    - Therapy and dosage history
    - Audit logs
“Programmer” Device communicates with IMD
- Through wireless channels
- Using radio frequency transmission

PC communicates with IMD
- Through USB-port "dongles" using radio frequencies
- PC may also be connected to Internet

IMD functions accessed remotely
- Read data on health status & therapy history
- Emergency extraction of patient health history
- Emergency reset of IMD configuration
- Therapy programming/reprogramming
- Firmware updates
- In US, IMDs are regulated by
  - Food and Drug Administration (FDA) Center for Devices and Radiological Health (CDRH)

- Testing focus
  - Safe and effective functioning
  - Different environmental conditions

- Absence of focus
  - Resistance/Resilience to cyber attacks
Are IMDs Vulnerable?

- A resounding YES!

- Current devices are engineered without considering threat of a potential hacker

- Current methods to prevent unauthorized access to IMDs include
  - Use of proprietary protocols
  - Controlled access to “Programmers” devices
  - Essentially, *security by obscurity!*
“Security researcher Jerome Radcliffe has detailed how our use of SCADA insulin pumps, pacemakers, and implanted defibrillators could lead to untraceable, lethal attacks from half a mile away.”

“He managed to intercept the wireless control signals, reverse them, inject some fake data, and then send it back to the [insulin] pump.”

“He could increase the amount of insulin injected by the pump, or reduce it”
Halperin et al, “Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses”

“… an implantable cardioverter defibrillator (1) is potentially susceptible to malicious attacks that violate the privacy of patient information and medical telemetry, and (2) may experience malicious alteration to the integrity of information or state, including patient data and therapy settings for when and how shocks are administered.”
Threats

- Patient Data Extraction
- Patient Data Tampering
- Device Re-programming
- Repeated Access Attempts
- Device Shut-Off
- Therapy Update
- Malicious Inputs
- Data Flooding
- Unsecured Communication Channels
- Inadequate Authentication Mechanisms
- Inadequate Access Controls
- Software Vulnerabilities
- Weak Audit Mechanisms
- Meager Storage
- Insufficient Alerts

From http://gizmodo.com/
Risks

- **Patient Health Safety**
  - Firmware Malfunction
  - Malicious Therapy Update
  - Malicious Inputs to Device
- **Patient Privacy Loss**
  - Data Leakage from Device
- **Inappropriate Medical Follow-up**
  - Tampering of Patient Readings
- **Device Unavailability**
  - Battery Power Depletion
  - Device Flooding
Risk-Based Mitigation Approach

- Develop IMD Security Impact Matrix
- Develop IMD Access Requirements Matrix
- Select Appropriate Security Mechanisms
- Tailor Security Mechanisms
  - Accommodate IMD Environment Constraints
  - Add Compensating Mechanisms (as needed)
FIPS 199-based Impact Analysis

- Identify IMD Data Types
  - E.g., Firmware, Device Identification, Patient Identification, Provider Identification, Health Condition, Therapy Configuration, Patient Readings, Audit Logs

- Identify IMD Health Delivery Commands
  - E.g., Emergency reset

- Analyze Impact of Compromise
  - For each Data Type, estimate impact
    - Loss of Confidentiality, Integrity and Availability
  - For each Command Type, estimate impact
    - Loss of Availability
  - Assign Impact as [LOW, MODERATE, HIGH]

- Tabulate in IMD Security Impact Matrix
<table>
<thead>
<tr>
<th>Security Function / Data, Command</th>
<th>Emergency Reset Command</th>
<th>Patient ID Data</th>
<th>Therapy Data</th>
<th>Patient Heath Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>N/A</td>
<td>MOD</td>
<td>LOW</td>
<td>MOD</td>
</tr>
<tr>
<td>Integrity</td>
<td>N/A</td>
<td>MOD</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>Availability</td>
<td>HIGH</td>
<td>LOW</td>
<td>MOD</td>
<td>MOD</td>
</tr>
</tbody>
</table>
Determine IMD Access Requirements

- Develop Matrix
  - By Data Type and Health Delivery Command
  - By Role of Individual Accessing IMD and
    - By Access Channels (e.g., wired, wireless)
- Add Required Access Privileges
  - Per Basic IMD Functionality
  - By Need for Emergency Access
  - By Utility and Quality of Life Factors
- Tabulate as IMD Access Requirements Matrix (IMD-ARM)
## IMD Access Requirements Matrix (IMD-ARM)

<table>
<thead>
<tr>
<th>ROLE-CHANNEL / Command, Data</th>
<th>Emergency Reset Cmd</th>
<th>Patient ID Data</th>
<th>Therapy Data</th>
<th>Patient Heath Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient-Wireless</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prescribing Physician-Wired</td>
<td>Read Write</td>
<td>Read Write</td>
<td>Read</td>
<td>Read</td>
</tr>
<tr>
<td>Maintenance Physician-Wireless</td>
<td>Read</td>
<td>Read</td>
<td>Read</td>
<td>Read</td>
</tr>
<tr>
<td>Emergency Tech-Wireless</td>
<td>Invoke</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Select Needed Security Mechanisms

- Overlay IMD-IAM and IMD-ARM
- Select Security Mechanisms to Protect IMD Data/Commands
  - Channel Protection Mechanisms
    - Crypto-protected channel
    - None (Proprietary Protocols)
  - Authentication Mechanisms
    - Password
    - Device-to-device handshake
    - Cryptographic authentication
  - Audit Mechanisms
    - Auditable Events
    - Management of Audit Space Depletion
  - Alert/Alarm Mechanisms
    - Audible Alarms
    - Automatic Device Reset to Safe Mode
Tailor Security Mechanisms

- IMDs subject to many constraints
  - Device Size
  - Cost
  - Power
  - Computational Capability
  - Storage

- Adjust security mechanisms to accommodate constraints
  - E.g., Add Alarm if authentication can’t be strengthened for certain Data Types
Special Challenges in Securing IMDs

- **Battery and Power Limitations**
  - Power usage must be minimized to extend battery life
  - Battery depletion has devastating health consequences

- **Use of Cryptographic Techniques**
  - Highly Constrained Environment (cost, power, storage)
  - Compatible Crypto Suites/Protocols Needed
    - Crypto for Sensor Networks

- **Audit Mechanisms**
  - Limited Storage Area on Device
    - Attacks may generate deluge of audit entries
  - Managing Audit Space Depletion
    - Selective Overwriting; Alarms (Audible or to Remote Monitor)
IMDs – Essential in Current Healthcare Environment

Wireless Access
- Promotes Usability and Utility
- Poses Significant Security and Privacy Concerns

Risk-based Mitigation Approach
- Determine Security Impact for Data Types
- Implement Adequate Security Mechanisms
- Balance Security/Privacy with Safety/Usability

Further Work
- Models for IMD security and privacy
- Crypto-suites for IMD environments
“Implantable Pacemaker Testing Guidance,”


Questions and Contact Information

- Dr. Sarbari Gupta – Electrosoft
  - Email: sarbari@electrosoft-inc.com
  - Phone: 703-437-9451 ext 12
  - LinkedIn: http://www.linkedin.com/profile/view?id=8759633