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

Electrosoft

Managing Cyber Security Risk through Innovation and Engineering

Agenda

- **Overview of IMDs**
- **Security Threats, Vulnerabilities and Risks**
- **Risk-Based Mitigation Approach**
- **Summary**
- **References**

What is an IMD?

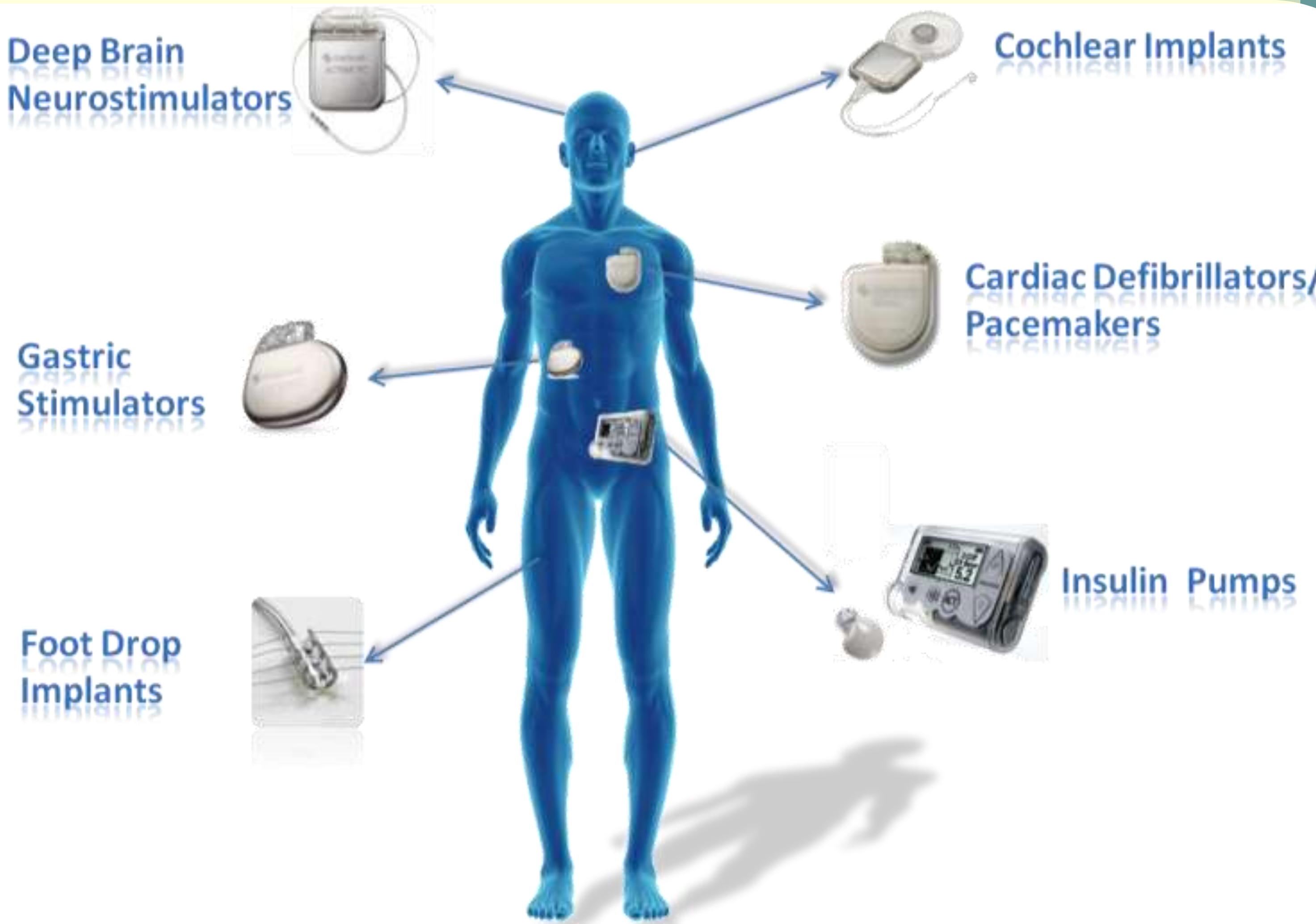
- **Implantable Medical Device (IMD)**
  - **Tiny computing platform with firmware**
  - **Runs on small batteries**
  - **Programmable**
  - **Implanted in human body**
  - **Monitors health status**
  - **Delivers medical therapy**

IMD Examples

- Pacemakers
- Implantable Cardiac Defibrillators (ICD)
- Cochlear Implants
- Insulin Pumps
- Neurostimulators

Electrosoft
Managing Cyber Security Risk through Innovation and Engineering

Wireless Implantable Medical Devices



Courtesy of http://groups.csail.mit.edu/netmit/IMDShield/

Electrosoft
Managing Cyber Security Risk through Innovation and Engineering

Pacemaker

- **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**

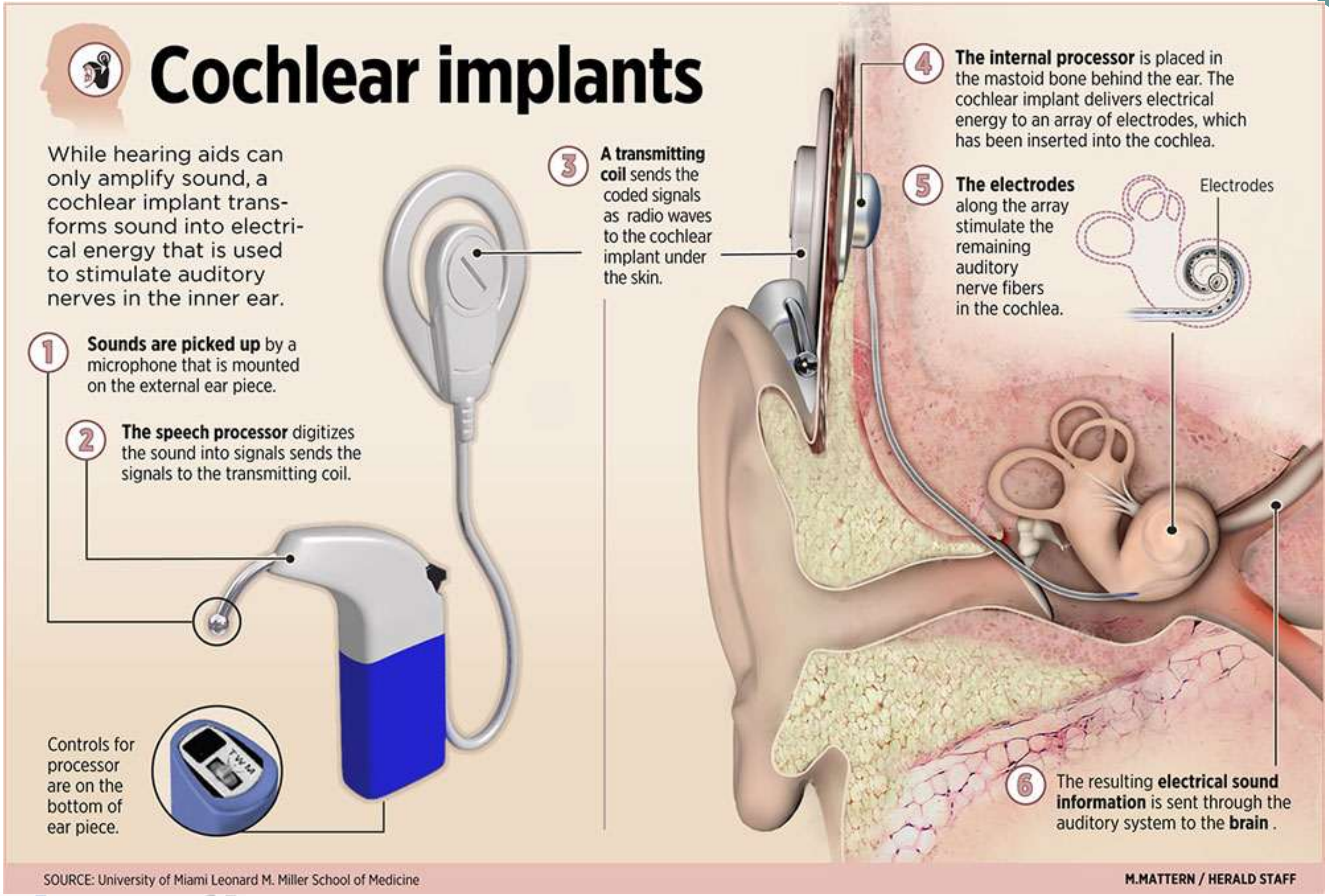
Wireless Insulin Pump

- 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

Medtronic Paradigm 512 Insulin Pump with Wireless Blood Sugar Meter

Electrosoft
Managing Cyber Security Risk through Innovation and Engineering

Cochlear Implants



IMD Data

- **IMD holds various Data Types**
  - **Static Data**
    - o **Device make**
    - o **Model #**
  - **Semi-static Data**
    - o **Physician & Health Center Identification**
    - o **Patient Name and DOB**
    - o **Medical condition**
    - o **Therapy configuration**
  - **Dynamic Data**
    - o **Patient health status history**
    - o **Therapy and dosage history**
    - o **Audit logs**

IMD Accessibility

- “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

Regulation of IMDs

- **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!***

Electrosoft
Managing Cyber Security Risk through Innovation and Engineering

Black Hat security conference – Aug 2011

- "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"

http://www.extremetech.com/extreme/92054-black-hat-hacker-details-wireless-attack-on-insulin-pumps

IEEE Symposium on Security and Privacy - 2008

- 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."

Electrosoft
Managing Cyber Security Risk through Innovation and Engineering

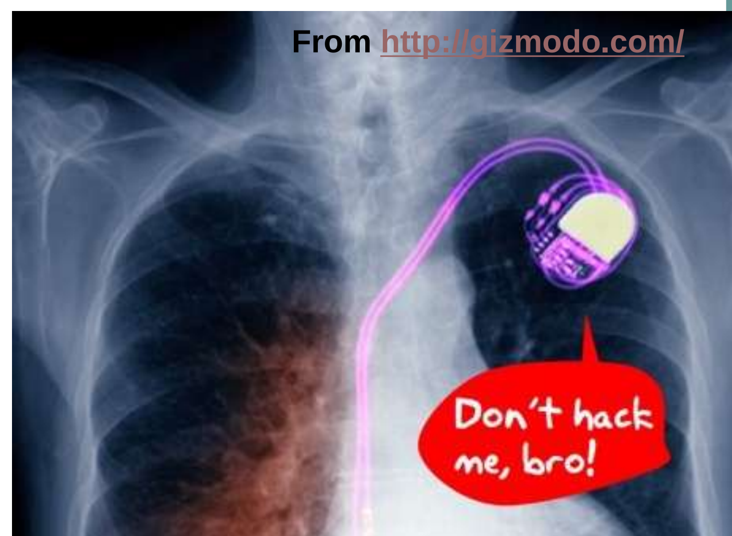
Threats

- **Patient Data Extraction**
- **Patient Data Tampering**
- **Device Re-programming**
- **Repeated Access Attempts**
- **Device Shut-Off**
- **Therapy Update**
- **Malicious Inputs**
- **Data Flooding**

Electrosoft
Managing Cyber Security Risk through Innovation and Engineering

, Vulnerabilities

- **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)**

Electrosoft
Managing Cyber Security Risk through Innovation and Engineering

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**

Electrosoft
Managing Cyber Security Risk through Innovation and Engineering

IMD Security Impact Matrix (IMD-SIM)

Security Function / Data, Command	Emergency Reset Command	Patient ID Data	Therapy Data	Patient Heath Data
Confidentiality	N/A	MOD	LOW	MOD
Integrity	N/A	MOD	HIGH	HIGH
Availability	HIGH	LOW	MOD	MOD

Electrosoft
Managing Cyber Security Risk through Innovation and Engineering

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)

ROLE-CHANNEL / Command, Data	Emergency Reset Cmd	Patient ID Data	Therapy Data	Patient Heath Data
Patient-Wireless				
Prescribing Physician-Wired		Read Write	Read Write	Read
Maintenance Physician-Wireless		Read	Read	Read
Emergency Tech-Wireless	Invoke			

Electrosoft
Managing Cyber Security Risk through Innovation and Engineering

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

Electrosoft
Managing Cyber Security Risk through Innovation and Engineering

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)**

Summary – IMDs and Security

- **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**

References

- "Implantable Pacemaker Testing Guidance," http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM081382.pdf.
- D. Halperin, et al, "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," Proceedings of the 2008 IEEE Symposium on Security and Privacy, Oakland, CA, 2008.
- D. Halperin et al, "Security and Privacy for Implantable Medical Devices," in Pervasive Computing, Vol. 7, No. 1, January–March 2008.
- S. Capkun, "On Secure Access to Medical Implants," Workshop on Security and Privacy in Implantable Medical Devices, Lausanne, Switzerland, April, 2011.
- S. Cherukuri, K. Venkatasubramanian, and S. Gupta, "BioSec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body," Proc. Int'l Conf. Parallel Processing (ICPP)Workshops, IEEE CS Press, 2003, pp. 432–439.
- T. Denning, et al "Patients, pacemakers, and implantable defibrillators: human values and security for wireless implantable medical devices," Proceedings of the 28th international conference on Human factors in computing systems, ACM New York, NY, USA, 2010, pp 917-926.
- National Institute of Standards and Technology "FIPS Pub 199: Standards for Security Categorization of Federal Information and Information Systems," FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, February 2004.
- S. Fischer and M. Zitterbart, "Security in Sensor Networks," Information Technology: Vol. 52, No. 6, 2010, pp. 311-312.

Electrosoft

Managing Cyber Security Risk through Innovation and Engineering

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**

Electrosoft
Managing Cyber Security Risk through Innovation and Engineering