Panel 1
Securing Medical Cyber-Physical Systems: Challenges and Future Directions

Krishna Venkatasubramanian
Computer Science
Worcester Polytechnic Institute
kven@wpi.edu

ISMICT 2016
Goal

• To give the audience an appreciation of:
  – The need for considering security in the current/next-generation of medical systems
  – The complexity of the problem
  – Interplay between safety and security
  – Risk analysis in security
  – Role for manufacturers (and regulators)
Data/Device Proliferation (By Moore’s Law)

- **Unattended Multihop ad-hoc wireless**
- **Sensor Networks**
- **Medical Devices**
- **Industrial Systems**
- **Cargo, machinery, factory floor**
- **Portable Smart Devices**
Integration at Scale (Isolation has cost!)

World Wide Sensor Web

Smart Building Environment

Future Combat System

Low End

Ubiquitous embedded devices
- Large-scale networked embedded systems
- Seamless integration with a physical environment

High End

Complex systems with global integration
- Global Information Grid

Integration & Scaling Challenges
Slowness of Biological Evolution

The information generated by all this exponential proliferation of embedded devices (afforded by Moore’s Law) is *not* matched by a corresponding increase in human ability to consume that information!

Increasing autonomy (human out of the loop)
Confluence of Trends

#1. Data/Device Proliferation

#2. Integration at Scale

#3. Autonomy
    (Human are not getting faster)

Cyber-Physical Systems

Distributed, Environment-coupled, Information distilling, Control systems
Trends in Medical CPS (MCPS)

**Miniaturization**
- Implantable devices
- Ingestible sensors
- Body Area Networks

**Interoperation**
- Executable clinical scenarios
- Safety interlocks

**Teleoperation**
- Robotic surgery
- Tele-ICU

**Autonomy**
- Physiological closed loop control
- Context-sensitive decision support
- Smart alarms
General MCPS Model

Monitoring Medical Devices

Treatment Delivery Medical Devices

Patient

EHR

Administrative Support

Smart Controller

Decision Support

Smart Alarm

Caregiver
MCPS Characteristics

**MCPS can communicate with increasing access range often over wireless channels**

MCPS collect & store health information

MCPS can connect to existing IT infrastructure and the Internet

MCPS actuate the physical environment (i.e., human body) they are deployed on

MCPS may be managed by the users who may not be tech-savvy

Provide (semi) closed-loop-control over a patient
MCPS Current Research Focus

Smart Alarm System

**Smart Alarms Hospital**

Mr. John Nava

<table>
<thead>
<tr>
<th>Blood Pressure</th>
<th>45 mm Hg</th>
<th>Very Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heart Rate</td>
<td>110 bpm</td>
<td>High</td>
</tr>
<tr>
<td>Oxygen Saturation</td>
<td>97%</td>
<td>Normal</td>
</tr>
<tr>
<td>Respiratory Rate</td>
<td>10 rpm</td>
<td>Normal</td>
</tr>
</tbody>
</table>

**Clinical Decision Support**

- Complications: Atrial Fibrillation, Ventricular Tachycardia, Cardiac Tamponade
- Risk Factors: Smoker, Prior MI, Hypertensive

**Time:** 12:01:03 PST

**SAFETY FIRST**

**Interoperability**
What is missing....

SECURITY
ESSENTIAL but MISSING
Why should we care?...

Malware Is "Rampant" Across Medical Devices in Hospitals

Healthcare organizations under siege from cyberattacks, study says

Insulin Pumps Vulnerable to Hacking

Published August 04, 2011 / Associated Press
Sources of the problem?

- MCPS store personal/sensitive health information
- MCPS are wireless with increasing access range
- Substantial increase in deployment - greater incentive for attack
- Connecting to existing IT infrastructure (Internet) for easy access
- Use of COTS software and hardware which might not be designed with security in mind

Sensitive information collected by generic classes of devices

- **Physiologic Monitors**
  - EKG
  - BP
  - O2
  - Temp.
  - HR
  - Respiration
  - Alarms

- **Pumps**
  - Flow rate
  - Alarms

- **Analyzers**
  - Hemoglobin
  - pH
  - Electrolyte
  - Glucose

- **Ventilators**
  - Flow rate
  - Volume
  - Breath rate
  - O2
  - Alarms

- **Scanners**
  - Images

Medical devices today, largely either do not have any inbuilt security features or have proprietary features that are not well-understood.
Targets?

• FOUR board categories of targets to be protected:
  – Patient
    • prevent physical harm to the patient
  – Data
    • prevent patient data privacy
  – Device
    • prevent denial of service of devices
  – Institution
    • prevent targeting of medical institution

Attacker Categories

• Operational Categories:
  – Passive
    • Eavesdrop on communication
    • Do not actively engage in the system’s operations
  – Active
    • Actively engage in the system’s operations
    • Can eavesdrop, modify, replay information
    • Can physically compromise systems

• Contextual Categories:
  – Insiders
    • Attackers that are part of the system and have inside information
  – Outsiders
    • Attacker that do not belong to the system

• Cohesiveness Categories:
  – Coordinated
    • Active attackers that work in a coordinated manner to attack a system
  – Uncoordinated
    • Lone-wolf
    • Large number of independent attackers
Safety?

Safety

Security

Failures

Accidental

Mistake

Lapse

Systemic

Environmental

Byzantine

Attack

Deliberate

Inducement

Security

WPI
Challenges in Securing MCPS

• **Lack of security standards**
  – Best practices, standards, situation specific

• **Vastly increased attack surface**
  – Communication, hardware, sensing, software, physical elements
  – Need for holistic solutions

• **Resource constraints**
  – Complexity of potential holistic solutions
  – Heterogeneity of devices

• **Patient involvement (in-the-loop?)**
  – Insufficiently trained
  – Need for empowerment/consent
  – Ease of use
Challenges in Securing MCPS

• **Enabling effective fail-safe**
  – Isolation of critical functionalities
  – Managing safety

• **Break-glass support & Auditing**
  – Always-log and securely

• **Security assurance and facilitating ease of regulation**
  – Assurance cases

• **Need for better risk analysis**
  – Assessing the severity of the threats realistically
  – Evaluating solution efficacy
Panelists...

• Dave Arney (Mass. General Hospital)

• Penny Chase (MITRE Corporation)

• Eugene Vasserman (Kansas State U.)