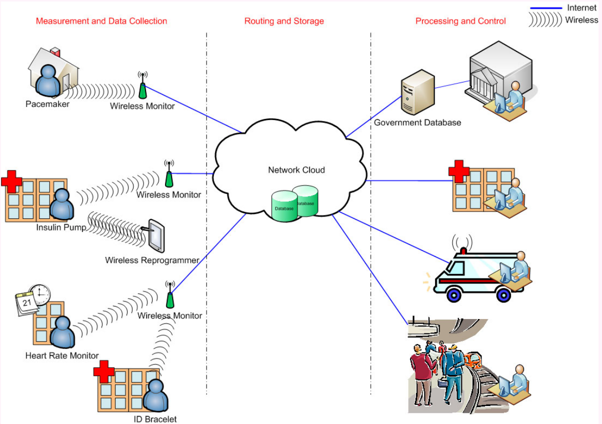
Protecting Global Medical Telemetry Infrastructure

Benessa Defend, Mastooreh Salajegheh, Kevin Fu, and Sozo Inoue
University of Massachusetts Amherst and Kyushu University
{defend, negin, kevinfu}@cs.umass.edu, sozo@lib.kyushu-u.ac.jp

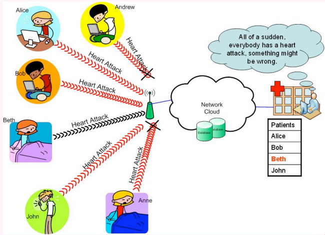
Overview of Medical Telemetry Infrastructure



- **Problem Area**
  - ▪Threats to the security of a medical telemetry infrastructure
  - ▪Vital effects of the threats
- **Future Research**
  - ▪Detection and prevention of the threats
- **Research Challenges**
  - ▪Resource constraints
  - ▪Wireless communication
  - ▪Resource replacement for implantable devices
  - ▪Environment of the devices

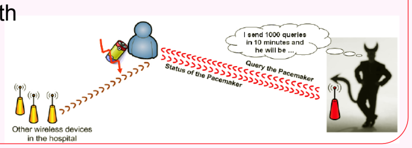
Telemetry Spam

- **Problem**
  - ▪Fake messages flood the network
- **Significance**
  - ▪Prevents timely patient care
  - ▪False emergencies



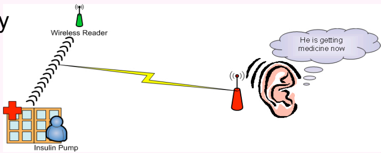
Dead Battery

- **Problems**
  - ▪Queries drain a device’s battery
  - ▪Nearby devices can accidentally interfere
- **Significance**
  - ▪Battery replacement may require surgery
  - ▪Possible death


I send 1000 queries in 10 minutes and he will be ...
Query the Pacemaker
Status of the Pacemaker
Other wireless devices in the hospital

Patient Privacy Invasion

- **Problems**
  - ▪Wireless devices are loquacious
  - ▪Third party can eavesdrop
- **Significance**
  - ▪Loss of privacy
  - ▪Discrimination
  - ▪Tracking



Compromised Infrastructure

- **Problems**
  - ▪Vulnerabilities in various parts of the system
  - ▪Insider attacks
  - ▪Accidental disclosures
- **Significance**
  - ▪Loss of data
  - ▪System downtime

I don't want to hire Beth. She has an ICD, so probably has heart trouble

Potential Countermeasures

- RFID access control proxy device
- Energy-aware cryptography
- Modify communication protocols
- Tracking countermeasures from RFID
- Intrusion detection and tolerant systems
- Anti-discrimination legislation
- Physical security measures