CIS 700/002 : Special Topics : Cyber-Physical Attacks on Implantable Medical Devices

Rado Ivanov

CIS 700/002: Security of EMBS/CPS/IoT

Department of Computer and Information Science

School of Engineering and Applied Science

University of Pennsylvania

20 Jan, 2017

Why Implantable Medical Devices?

- Multiple safety-critical applications
  - Cochler implants, neurostimulators, pacemakers, infusion pumps
- More opportunities with modern computers
- Greater demand as certain conditions become prevalent
  - Increasing number of diabetics → more insulin pumps

Constraints

- Small-scale, relatively simple
  - Few sensors and actuators

- Balance utility vs. safety vs. security
  - Small, light, energy-efficient
  - Safely perform task (e.g., pace the heart)
  - Be secure against malicious cyber-physical attacks

- Operate for a long time
  - Difficult to change software
  - Even harder to change hardware

Attack Goals

- Obtain personal information
  - E.g., identify patient using intercepted messages
  - Identity theft, blackmail, etc.

- Harm the patient
  - Make device take unsafe actions (e.g., overdose)
  - Vice President Dick Cheney (2001-09) has a defibrilator that was deemed insecure

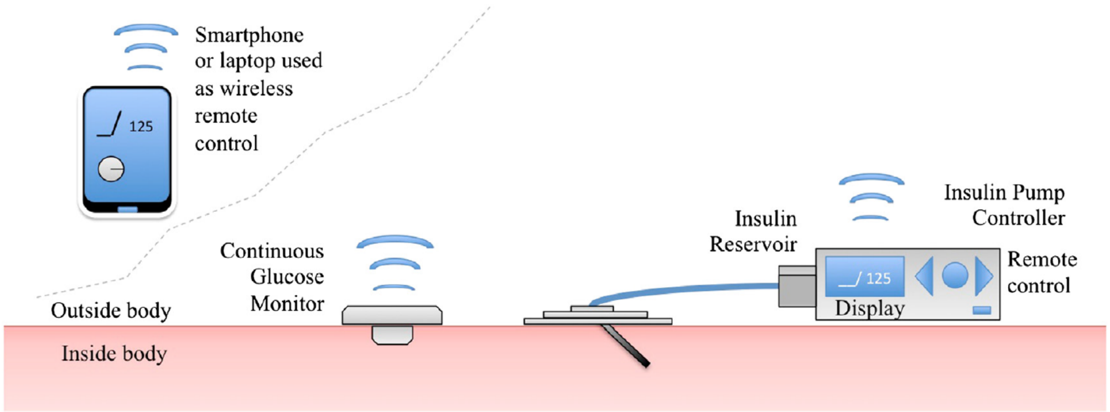
Attack Surface

- Cyber Space
  - Intercept/decrypt wireless communication
  - Corrupt external device communicating with medical device (e.g., phone)

- Physical Space
  - Interfere with physical medium (e.g., radio signal)

Case Study: Insulin Pumps

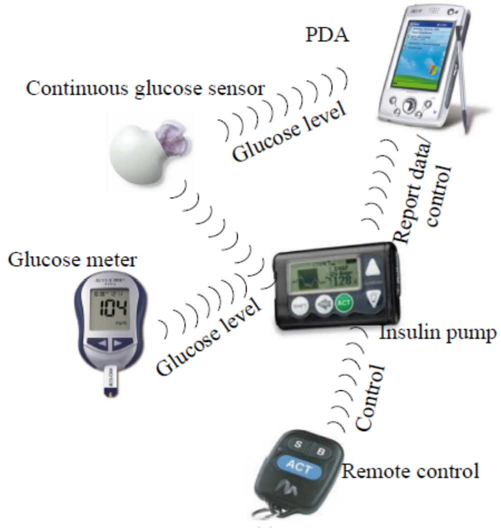
- Delivers insulin into the layer of fat just below the skin
  - Control level of glucose



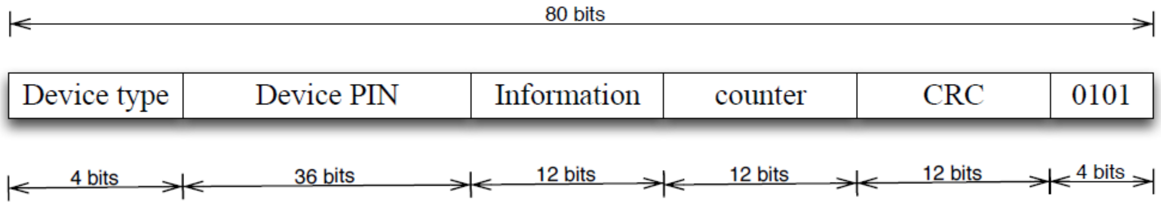
- Digital interface for adjusting infusion rates
  - Standard design goal is to minimize mechanical/electrical faults
  - Multiple errors over the years

Attacks on Insulin Pump: Obtain PIN Code

- Many components communicate wirelessly
  - Messages not encrypted

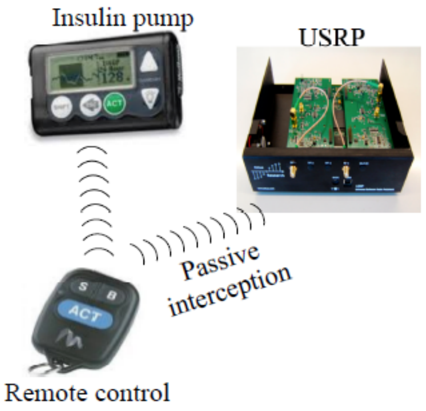


- Intercept messages using a Universal Software Radio Peripheral (USRP)
  - Reverse-engineer communication protocol



80 bits

Device type	Device PIN	Information	counter	CRC	0101
4 bits	36 bits	12 bits	12 bits	12 bits	4 bits



Li, C., Raghunathan, A., and Jha, N. K. (2011). Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on, 2011

Possible Attacks

- Privacy attack
  - Obtain patient treatment, device type
- DoS attack
  - Jam channel
- Replay attack
  - Report wrong readings to controller
  - Alternate same two messages to fool pump’s counter
- Not verified if protocol is the same for messages from controller to pump
  - Another group of researchers were able to control/shut down

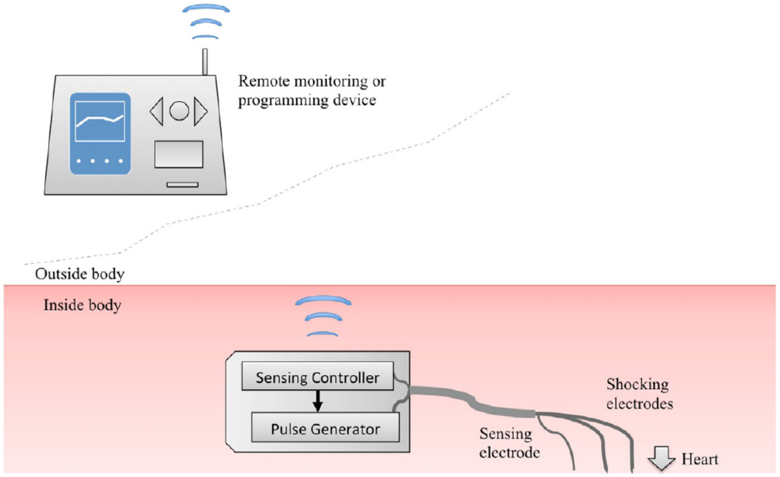
Attacks on Insulin Pump: Attack Smart Phone

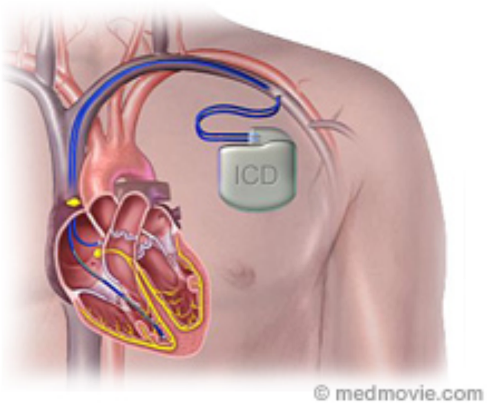
- Install malware on phone that changes store glucose values
  - Clinician may take wrong decision based on these values
- Malware could obtain patient information from phone
- Malware could make phone send dangerous control commands to device

Paul, N. and Klonoff, D. C. (2010). Insulin Pump System Security and Privacy. In USENIX Workshop on Health Security and Privacy.

Case Study: Implantable Cardioverter Defibrilators

- Deliver electrical pulses to heart to pace it
  - Unlike a pacemaker, can also deliver big shocks to reset rhythm





- No wireless communication inside device (only with remote device)

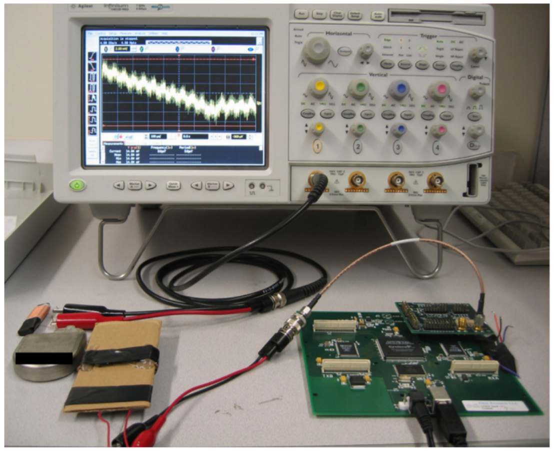
Attacks on Defibrilators: Interfere with Radio Signal

- Place two radio frequency identification (RFID) devices near defibrilator
  - Causes electromagnetic interference (misinterpret as a heart signal)
  - Also affects syringe pumps, pacemakers, ventilators, etc.
- Interference also achieved with electronic article surveillance devices and metal detectors
- 72-year-old man received four shocks next to a store's electronic anti-theft system
  - Defibrilator thought heart was in tachycardia

Van Der Togt, R., van Lieshout, E. J., Hensbroek, R., Beinat, E., Binnekade, J. M., and Bakker, P. J. M. (2008). Electromagnetic interference from radio frequency identification inducing potentially hazardous incidents in critical care medical equipment.

Attacks on Defibrilators: Intercept Wireless Messages

- Device talks wirelessly to an external programmer device
  - Programmer sets therapy settings, reads/writes private data
  - Communication not encrypted



- Intercept messages
  - Extract patient name, DOB, MRN, etc.

- Some attacks without full reverse-engineering
  - Performed replay attacks (obtain above private information)
  - Replay control attacks succeed sometimes (change patient name, therapy)
  - Power DoS by maintaining a strong magnetic field (speculation)

Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., Fu, K., Kohno, T., and Maisel, W. H. (2008). Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In IEEE Symposium on Security and Privacy (SP 2008).

Case Study: Implantable Biosensors

- Must communicate wirelessly with outside world
  - Messages may be infrequent and short
  - Might be easy to decrypt

- Must preserve power
  - Prevent side-channel power draining attacks

- Explore designs to understand the trade-offs between utility, safety and security

Burleson, W., Clark, S. S., Ransford, B., and Fu, K. (2012). Design challenges for secure implantable medical devices. In Proceedings of the 49th Annual Design Automation Conference. ACM, pp. 1217.

Recap: Common Vulnerabilities

- Security not been a major concern so far
- Communication is not encrypted
- Medical devices “know” too much
  - Do they need to know/transmit patient names/IDs?
- Medical devices still have a lot of faults that could be exploited