Special Topics in Security and Privacy of Medical Information

Sujata Garera

Previous lecture
- Medical Device Security
  - Security analysis of ICD
    - Demonstrated methods of compromising privacy and integrity
      - Looked at various active attacks
      - Replay attacks
- Zero power defenses
  - Why “zero” power?
  - What was their detection mechanism?
  - What about prevention?
Detection
- Zero power notification for patients
  - Alerts patients to potentially malicious activities both by insiders using commercial programmers and by outsiders using custom attack hardware
  - Wirelessly drives a piezo element that can audibly warn a patient of security sensitive events

Prevention
- Zero power authentication

Criteria for IMDs
- Security and Privacy for Implantable Medical Devices
- Safety and utility goals
  - Data access: Data should be available to appropriate entities
  - Emergency situation IMD data may help in physician’s immediate diagnosis
  - Data accuracy
  - Device Identification: IMD should make itself known
    - A doctor needs to know an IMD is present before surgery
    - ICD has to be deactivated before surgery
    - FDA has considered attaching remotely readable RFID tags to implanted devices
      - Is that a good idea?
Criteria for IMDs

Safety and Utility goals
- Configurability: Authorized entities should be able to change IMD settings
  - E.g. Doctor should be able to manage ICD therapies
- Updatable software
  - This needs to be possible without explantation
- Resource efficient and auditable

Criteria for IMDs

Security and Privacy goals
- Authorization: Could be role based
  - Should be context aware
  - Why is this necessary?
- Availability: Adversary should not be able to launch a DOS on the system
- Device existence privacy: An unauthorized entity should not be able to remotely determine that patient has an IMD

Criteria for IMDs

Security and Privacy goals
- Specific device ID privacy: Adversary should not be able to wirelessly track down individual IMDs
- Measurement and log privacy
- Data integrity
Tensions

- Security vs accessibility
  - Open access vs closed and controlled access
  - Emergency scenarios from paper
    - Scenario 1: An unconscious patient with one or more IMDs enters an emergency room, perhaps in a foreign country or developing region. Emergency-room personnel quickly determine the types of IMDs the patient has. The staff then use standard equipment to interrogate the IMDs, extract critical physiological information, and treat the patient, including altering IMD settings and even firmware as appropriate. Because the patient is alone and has no form of identification, the staff also extracts the patient’s name and pertinent information from the data stored on the IMDs.

Tensions

- Security vs accessibility
  - Scenario 2: In the second scenario, a patient explicitly controls which individuals or specific external devices can interact with his or her IMDs. The IMDs use strong access-control and cryptographic mechanisms to prevent other unauthorized exposure of data and unauthorized changes to settings. The IMDs also use mechanisms to provide, specific-device ID, device-type, and device-existence privacy.

Tensions

- Security vs device resources
  - Use of Public key cryptography can be very expensive
Security mechanism

- Absence Makes the Heart grow Fonder: New Directions for Implantable Medical Device Security by Denning et al.
  - Normal use scenario
  - Adversarial scenario

Design goals

- Safety and open access in emergencies
- Security and privacy under adversarial conditions
- Battery Life
- Response Time

Motivation for designing such security mechanism

- Research has of course shown that IMDs can be compromised
- November 2007 malicious attacks were launched against the Coping with Epilepsy website
- Attack also launched against Epilepsy Foundation website in March 2008
Possible solution

- Case by case credentials
  - An EMT needs to obtain credentials from the patient’s doctor before he can get access to the IMD
    - Is this a good solution?

Possible solution

- Require close proximity
  - Disallow long distance wireless communications until a close distance bootstrap has been completed
    - Is this reasonable?

Possible solution

- Encryption with carried keys
  - Encrypt communications to and from the IMD
  - What are the challenges?
Communication Cloakers

- **Fail-open defensive devices**
- **Device a patient can wear like a bracelet**
  - But has communication and computational capabilities
  - Wear Cloaker during normal everyday activities
    - Provide security when patient is wearing Cloaker but to provide fail-open access to all external programmers when the patient is not wearing a Cloaker
    - In emergency situations doctors can remove Cloaker to allow immediate access to the IMD

Communication Cloaker

- Presence of cloaker causes IMD to ignore communication
  - Absence causes it to fail open

---

Communication Cloaker

- Normal use

---
Communication Cloaker

- Adversarial use

---

Emergency

- IMD is power limited
- Use fast and low power cryptography
  - Public or symmetric?
- Cloaker can be recharged
  - Could use more computationally expensive cryptography
- IMD and cloaker are paired long term
Design challenges

- Communication between IMD and Programmer with cloaker present
  - Cloaker and IMD communications
    - Encrypted
    - Authenticated
    - Long term
    - How should we achieve this?

Design challenges

- Communication between IMD and Programmer with cloaker present
  - Solution 1: IMD listens for session initiation requests from programmer and queries cloaker for verifying authenticity
    - What are the pitfalls of this?

Design challenges

- Communication between IMD and Programmer with Cloaker present
  - Solution 2: Cloaker verifies that external programmer is authorized to communicate with IMD
    - How may this be achieved?
Design challenges

- Communication between IMD and Programmer with cloaker present
  - Cloaker can proxy communication between IMD and programmer
  - Cloaker can log communication for forensics
  - Cloaker can hand-off a symmetric credential to programmer
    - Lower latency in communication

Design challenges

- Communication between IMD and programmer when cloaker removed
  - IMD listens and responds to all incoming communication requests

Design challenges

- Cloaker present but cannot be found
  - Incorporate a pulse sensing unit into the Cloaker and define it as being present when it is able to sense the pulse
    - A DOS attack could be launched by an adversary
Design challenges

- IMDs knowledge of Cloaker presence
  - Stateless approach
    - IMD querying cloaker whenever communication request detected
  - Stateful approach
    - Keep-alive messages and a record of the presence

Open issues

- Designing a complete prototype
  - Evaluating negative effects on patient
  - Patient may forget to wear the device

This lecture

- Absence makes the heart grow fonder: New directions for Implantable Medical Device Security by Denning et al.
  - Available online