Paper Discussion (CSE 291K:Winter '17)

Week 9 theme: Security

"They can hear your heartbeats: Non-invasive security for Implantable Medical Devices" , ACM SIGCOMM 2011 - BEST PAPER

Project Background

- ➔ Collaborative project between MIT and UMass.
- ➔ Kevin Fu (UMass) and Dina Katabi (MIT) : faculty contributors.
- ➔ Shyam, Haitham & Benjamin : Grad Students at MIT/UMass in 2011. Now they are professors at UW, UIUC and CTO of startup respectively.

Introduction

- ➔ Wireless devices improve healthcare and quality of life, increasingly used for in-home monitoring and diagnosis of patients
  - ◆ Timeliness of Care - Continuous monitoring of stats
  - ◆ Doctor can assess vital stats remotely.
- ➔ Each device has associated with it a unit called "IMD Programmer", which can be used to send commands to the IMD and also get statistics on the patient from the IMD.

Issue

- ➔ Confidentiality and authenticity of IMD commands.
  - ◆ An adversary can eavesdrop (passive) or send malicious commands (active)
  - ◆ Adversary is between 20 cm to 27 meters away.
- ➔ What do we do for wireless devices which are already implanted? Surgical methods are not an option - Non-invasive techniques sought.
- ➔ How about new IMDs. Can we just use crypto on these IMDs? No.
  - ◆ Crypto leads to more code on the IMDs. More possibility of software bugs- Paper says 11% of IMD device recalls attributed to software bugs.
  - ◆ Crypto affects access times to the device (for e.g., increased login times)

Proposed Solution

- ➔ An external, buddy device called shield (target form factor like a necklace)
- ➔ Innovations - Main innovation is in Radio Design
  - ◆ They designed a radio to receive and transmit signals on same channel (full duplex) without requiring antenna separation of half-wavelength.
  - ◆ Single TX antenna to jam the IMD and programmer signals.
  - ◆ RX antenna consists of a 'local TX antenna' which supplies a signal called antidote to un-jam the signal ONLY at the RX antenna of the device.

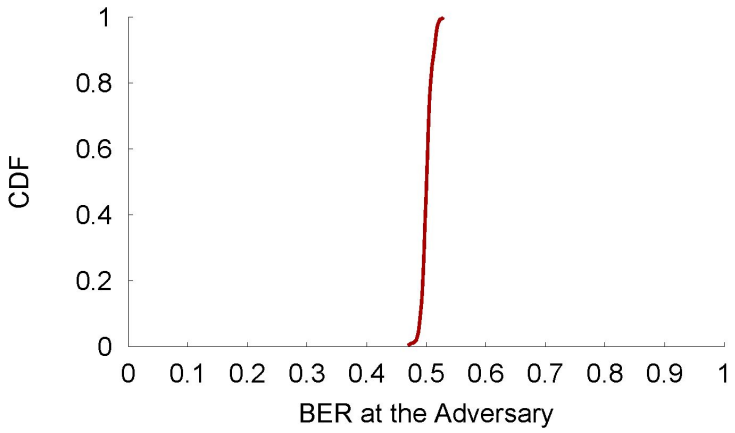
Assumptions made in the paper

- ➔ A secure channel exists between the shield and the legit programmer. This can be done by using in-band or out-of-band key exchange.
- ➔ The programmers of malicious IMD programmers do not violate the power range of the device. (All Programmers obeying FCC laws should abide by this)
  - ◆ Discuss on the powering issues here

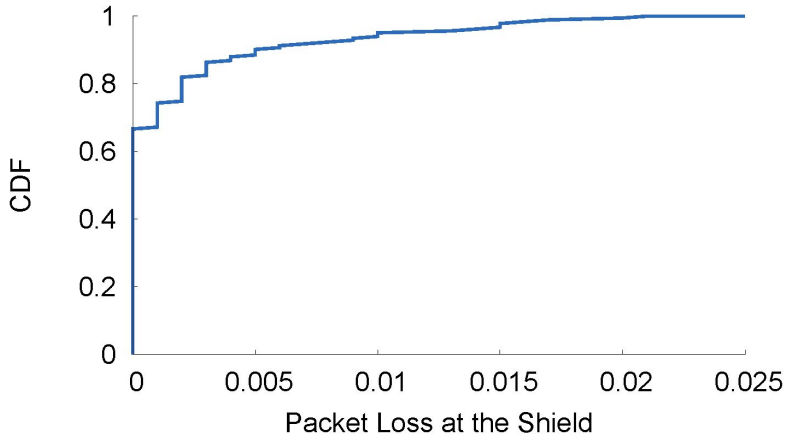
Evaluation

Done on USRP2 software radios that transmit in the IMD radio band.

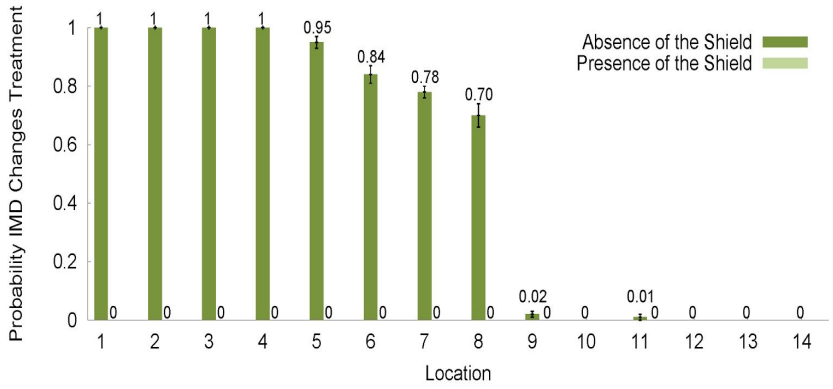
Graph 1: When the shield is present, it jams the IMD's messages, causing even nearby (20 cm away) eavesdroppers to experience a bit error rate of nearly 50%, which is no better than a random guess. (approx. vertical line in CDF curve below)

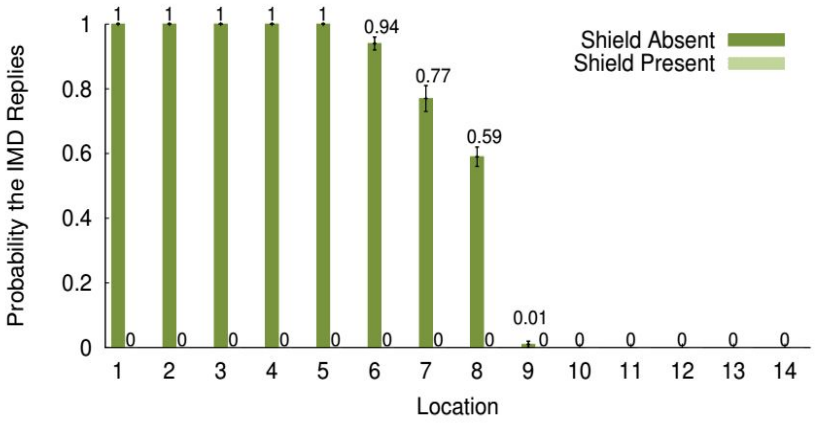


Graph 2: When the shield jams the IMD's packets, it can still reliably decode them (the packet loss rate is 0.2%, which is negligible). Thus, the shield and the IMD share an information channel that is inaccessible to other parties.

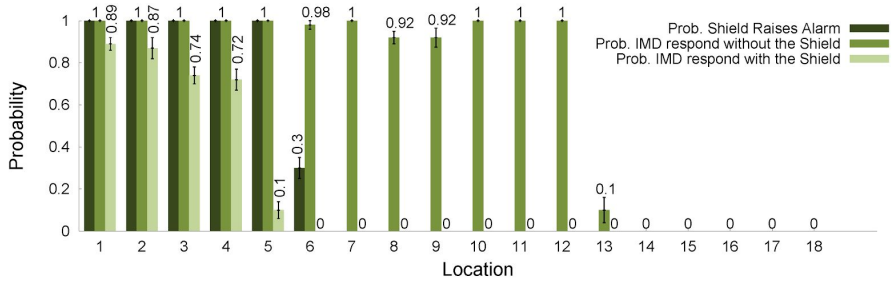


Graph 3: **When the shield is absent**, the IMD replies to unauthorized commands, even if the adversary is in a non-line-of-sight location more than 14 m away, and uses a commercial device that operates in the IMD band and adheres to the FCC power limit. **When the shield is present** and has the same transmit power as the adversary, the IMD does not respond to unauthorized commands, even when the adversary is only 20 cm away.





Graph 4: **When the shield is absent** and an adversary with 100 times the shield's power transmits unauthorized commands, the IMD responds from distances as large as 27 m. **When the shield is present** the high-powered adversary's attempts succeed only from distances less than 5 m, and only in line-ofsight locations. The shield always detects high-powered adversarial transmissions and raises an alarm.



Questions

- ➔ Are the assumptions about Cryptography validated?
- ➔ How is the power consumption of the dual-antenna radio design? Is it comparable to cryptographic algorithms?
- ➔ Presently, the IMD shield sounds an alarm if the adversarial programmer transmits very powerful (decibels) signals. Can this design be improved?
- ➔ The size of the shield is very large and is not close to the necklace form factor they targeted- Future work?
- ➔ Is the assumption of an encrypted channel between programmer and shield reasonable?
    - ◆ Power assumptions - workaround by sounding an alarm.

Learning from this paper:

The key challenge in addressing IMD device security stems from the difficulty of modifying or replacing implanted devices. Using a wireless physical-layer solution that delegates the task of protecting IMD communication to an external device called the shield is one way of solving the issue of security in IMD devices.