IMD Shield: Securing Implantable Medical Devices

Shyamnath Gollakota (MIT), Haitham Al Hassanieh (MIT), Benjamin Ransford (UMass Amherst), Dina Katabi (MIT), Kevin Fu (UMass Amherst)

Massachusetts Institute of Technology

UMASS AMHERST

To appear at ACM SIGCOMM 2011, August 15–19, Toronto

Medtronic Virtuoso DDE-DDDR implantable cardioverter/defibrillator. Photo courtesy of Medtronic, Inc.

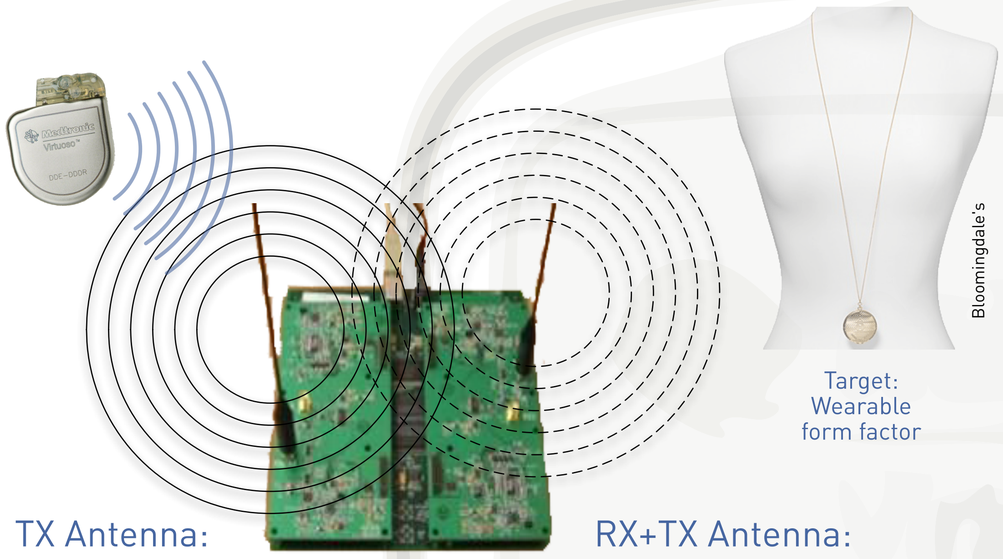
How can we protect a wireless device we cannot modify?

Wireless communication in **implantable medical devices (IMDs)** improves quality of care, but imports security and privacy risks [Oakland 2008]. Millions of IMDs are implanted in patients and **cannot be upgraded.** Can we protect them from known wireless attacks?

The IMD Shield

A **companion device** that protects an **unmodified** IMD from known attacks: **passive eavesdropping** and **active unauthorized commands**.

Key idea: friendly jamming, applied judiciously.



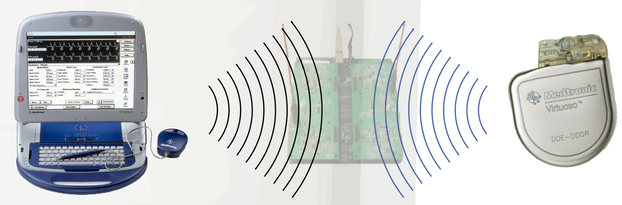
Before IMD Shield: A passive eavesdropper could intercept and decode IMD transmissions.
After: IMD Shield's random jamming during IMD transmissions reduces an adversary to guessing.

Before IMD Shield: An active attacker could successfully issue unauthorized commands to an IMD.
After: IMD Shield's random jamming during programmer transmissions prevents the IMD from ever hearing the command.

Encryption on the Air

The IMD Shield's random jamming signal works like a **one-time pad**; it **does not store secrets.** Jamming results in additive noise that overwhelms the IMD's private signal. Only the IMD Shield **knows the random jamming signal** and can subtract it from the noisy signal.

Emergency access: When the IMD Shield is off or not present, the system **fails open** by reverting to the status quo (cleartext).



IMD Shield Caveats

- We assume that the IMD Shield can establish a secure channel with a legitimate IMD programmer. In practice, an out-of-band key exchange (e.g., tactile or visual) might suffice.
- Our software-radio prototype of the IMD Shield is much larger than a production-ready wearable device would be.
- How should a wearable IMD Shield be powered?
- A sufficiently powerful adversary can overpower the IMD Shield to talk to the IMD, but in this case the IMD Shield sounds an alarm.

Timeline of Recent Related Work

2005 — [ACISP 2005]
Rieback et al. implement friendly jamming for privacy in the **RFID Guardian** device

2008 — [Pervasive 2008]
Halperin et al. propose a **threat model** for IMDs and highlight **theoretical risks**

2008 — [Oakland 2008]
Halperin et al. identify and exploit security and privacy flaws in an **implantable defibrillator**, propose defenses

2009 — [HotSec 2008]
Denning et al. propose the **communication cloaker**, conceptual ancestor of IMD Shield. Companion device requires IMD to be made aware of it

2010 — [HealthSec 2010]
First USENIX Workshop on Health Security and Privacy—papers include "Privacy Challenges for Wireless Medical Devices" and "Insulin Pump System Security"

2010 — [MobiCom 2010]
Choi et al. demonstrate single-channel, full-duplex wireless communication. Requires half-wavelength antenna separation (vs. IMD Shield's arbitrarily small size)

2011 — [INFOCOM 2011]
iJam (Gollakota et al.): **Jam while receiving** to prevent eavesdropping of a protected signal; OFDM-based technique requires protected device to be modified. IMDGuard (Xu et al.): **Another approach** adds crypto to IMDs and a wearable device that acts as an authentication proxy; requires IMDs to be modified.

Today — [SIGCOMM 2011]
IMD Shield incorporates full-duplex wireless and friendly jamming to combat eavesdropping and adversarial commands

Support: NSF CNS-0831244, NSF GRFP, DHHS Cooperative Agreement No. 90TR0003/01 — Find out more at http://groups.csail.mit.edu/netmit/IMDShield/