

IMD Shield: Securing Implantable Medical Devices

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

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



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

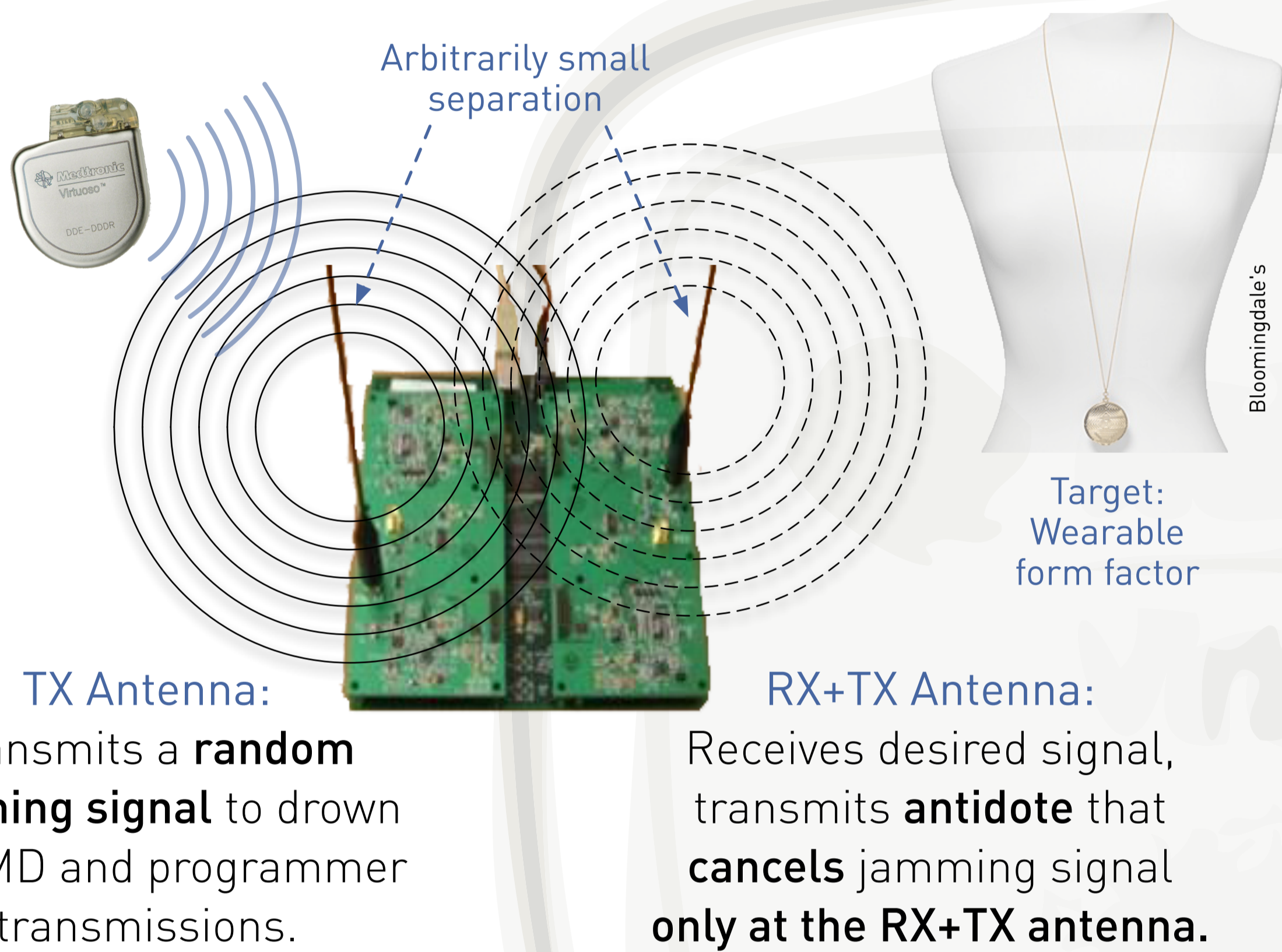
How can we protect a wireless device we cannot modify?

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 small **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.

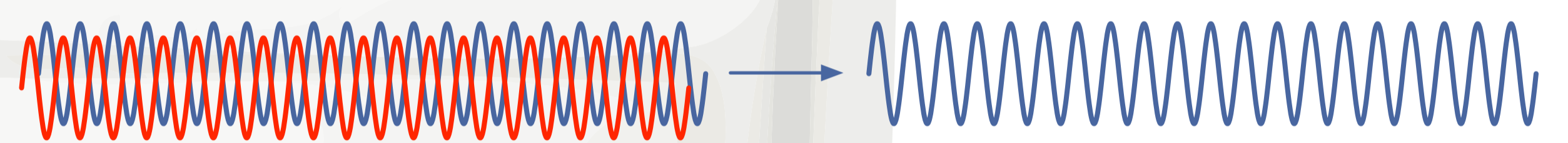
After: IMD Shield's random jamming during IMD transmissions reduces an adversary to guessing.

Before IMD Shield: An active attacker could successfully issue unauthorized commands to an IMD.

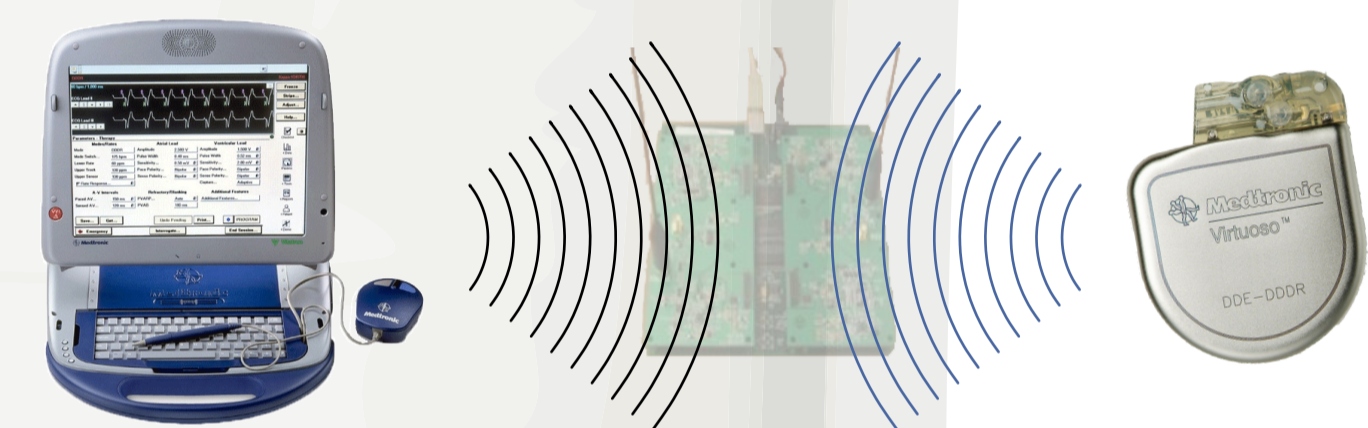
After: IMD Shield's random jamming during programmer transmissions prevents the IMD from ever hearing the command.

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.



Unlike conventional jamming, which hides the private signal from everyone, IMD Shield's friendly jamming can reveal it to trusted devices.



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.
- 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

