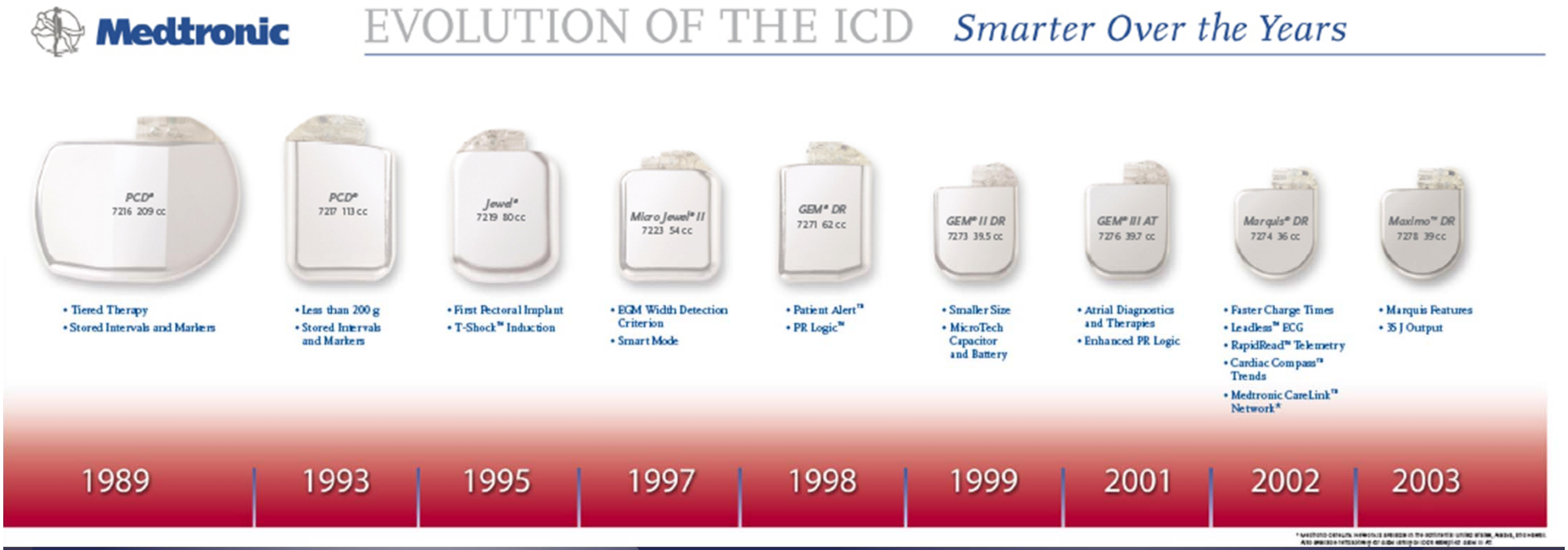
Securing IMDs

{ Joe Zatkovich

What are IMDs?



Background

Background (cont.)

- Why is securing them important?
  - Currently, there are no security measures in place.
  - Advancing technology means more avenues of attack.
  - Attacks have been proven to work. (more to come)

Realities of the Situation

- What are our goals?
  - Privacy, security, authenticity (or a subset, to start)
  - Maintain ease of care
- What are the limitations we face?
  - Hardware limitations:
    - Battery, computation power, storage, etc.
  - Using WiFi securely
  - **Securing devices that are already implanted!**

Proof of Concept Attack

- Built a wireless radio using GNU radio
- Were then able to intercept, and reverse-engineer transmissions – could intercept patient data and programming telemetry
- Successful attacks:
  - IMD/patient identification
  - Disclosing patient/cardiac data
  - Changing IMD's clock
  - Changing therapy parameters
  - Inducing fibrillation
  - Power DOS attack

One Solution: Hardware

- 'SHIELD' – a wireless jammer/receiver
- Why they believe this is a good solution:
  - Surgery not required to change previously implanted IMDs
  - Power/form factor of devices not a limitation
  - In emergencies, don't need to wait for response from primary care physician

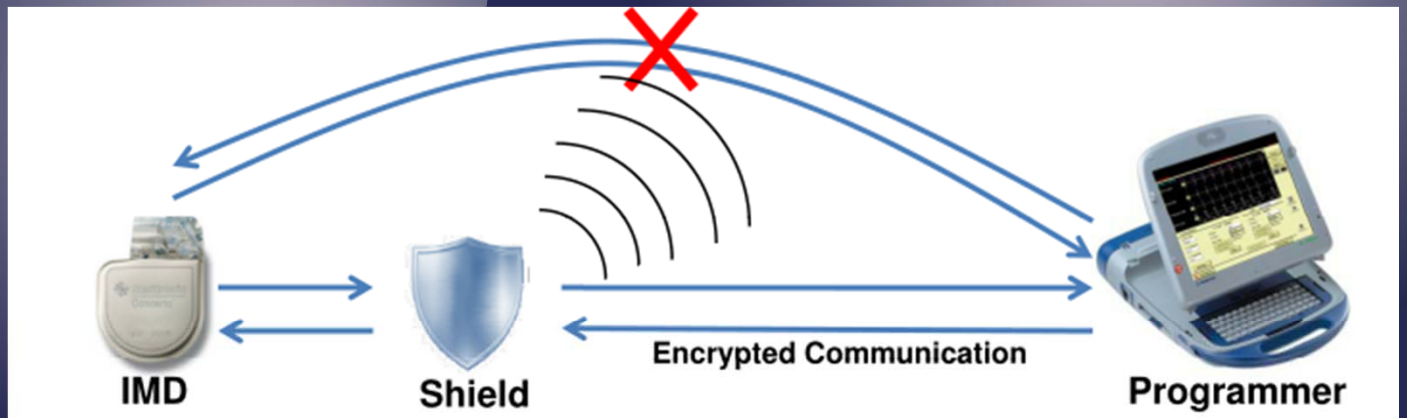


Figure 1—Protecting an IMD without modifying it: The shield jams any direct communication with the IMD. An authorized programmer communicates with the IMD only through the shield, with which it establishes a secure channel.

One Solution: Hardware

- Setup:
  - Shield jams with 20DB higher power than IMD receives
- Results:
  - When active, adversary using off-shelf programmers fail to get response as close as 20 cm
  - When using a programmer with 100x more power than shield, only elicits response with 5 meters and line of site
  - Shield still detects these transmissions and raises an alarm (beeps)
- **QUESTION:** Is this actually a good solution?

Alternative Solution

- Implement crypto in software!

Resources

- **Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses:** *Daniel Halpern, and Tadayoshi Kohno – UW, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, and Kevin Fu – UMASS CS, with William H. Maisel –BIDMA and Harvard Medical School, 2008.* http://www.secure-medicine.org/icd-study/icd-study.pdf

- **They Can Hear Your Heartbeats: Non-Invasive Security for Implantable Medical Devices:** *Shyamnath Gollakota, Haitham Hassanieh – MIT, and Benjamin Ransford, Dina Katabi, and Kevin FU – UMASS CS, August 2011.* http://spqr.cs.umass.edu/papers/gollakota-SIGCOMM11-IMD.pdf

- **Trustworthy Medical Device Software:** *Kevin Fu, Assistant Professor – UMASS CS, 11 April 2011.* http://spqr.cs.umass.edu/papers/fu-trustworthy-medical-device-software-IOM11.pdf

- **Security and Privacy for Implantable Medical Devices**: http://www.secure-medicine.org/PervasiveIMDSecurity.pdf

- https://wwwp.medtronic.com/medtronicconnect/resources/photoalbum/MedtronicICDs1989_2003.jpg

- https://wwwp.medtronic.com/medtronicconnect/resources/photoalbum/Enpulse%20DDDR.jpg