Implantable Medical Devices

Treat more than 25 million Americans

Extend life and vastly improve its quality for patients with broad set of conditions, such as:

- Diabetes/Chronic Pain (Insulin or Morphine)
- Cardiac Arrhythmia
- Neurostimulator (e.g., Parkinson’s)

Are becoming increasingly complex:

- Wireless communications allows doctors to inspect devices and change settings w/o surgery
- Doctors can monitor remotely; device status and patient history sent over the Internet
- These features can greatly enhance safety and utility for patients

But, are these devices secure?

Experimental Security Analysis of Real, Wireless Cardiac Defibrillator

A device programmer reads information from and changes settings on the ICD.

We built a software radio that mimics a legitimate programmer and can reproduce its functionality.

Real security and privacy concerns do exist!

ICD: a pacemaker that can also detect and correct heart arrhythmia via a large shock.

Fundamental Tension: Safety versus Security

Safety Goal: Access for emergency medical personnel

The Cloaker. An external computational unit. Its presence allows only authorized access. Remove the Cloaker to fail open for emergency access.

The Patients: Human Values

Patients will be directly affected by any security system. What do patients value? What are the properties of an acceptable security system?

We used a semi-structured interview and Value Sensitive Design to investigate the opinions of actual cardiac patients.