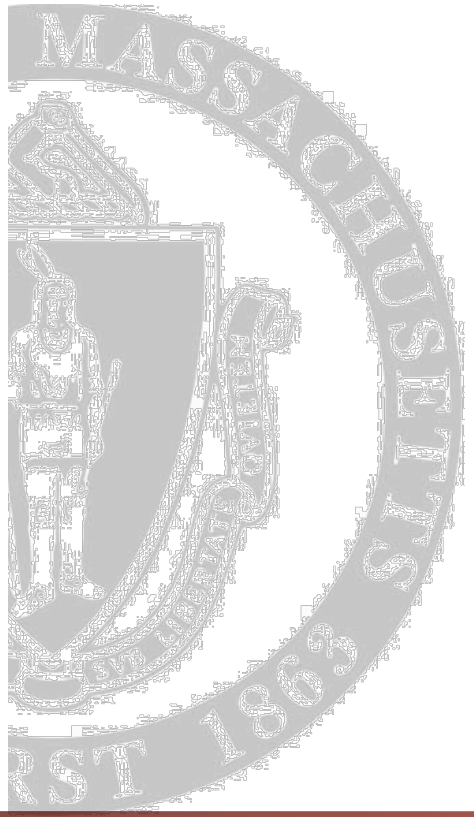
Implantable Medical Devices:

Security  Privacy

for Pervasive, Wireless Healthcare



Kevin Fu

Assistant Professor
Department of Computer Science
University of Massachusetts Amherst
http://www.cs.umass.edu/~kevinfu/

March 2009

Many Collaborators

- William H. Maisel, MD, MPH
  - Director, Pacemaker and Defibrillator Service, Beth Israel Deaconess Medical Center
  - Assistant Professor, Harvard Medical School
- Tadayoshi Kohno
  - Assistant Professor, CSE, University of Washington
- Students
  - Shane Clark, Benessa Defend, Tamara Denning, Dan Halperin, Tom Heydt-Benjamin, Andres Molina, Will Morgan, Ben Ransford, Mastooreh Salajegheh

Risks of Implantable Medical Devices: Just Add Internet+Wireless

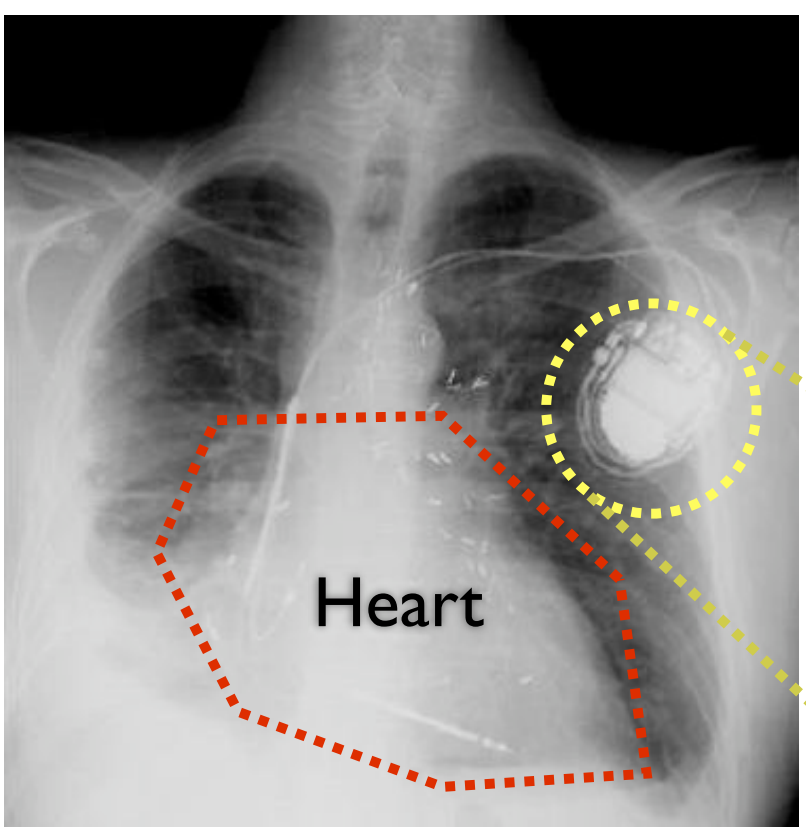


Image from www.nasaexplores.com

IMD Security & Privacy is Hard

- Background
  - Unintentional medical malfunctions
  - **Intentional** medical malfunctions
  - Pacemaker & Implantable Cardioverter Defibrillator (ICD)
- Security analysis of a pacemaker/ICD
  - Violate patient privacy
  - Induce a fatal heart rhythm
- Defensive methods
  - Protect the battery, proper use of cryptography
- The Future

Unintentional Malfunctions in Medical Care

Unintentional Accidents

IEEE Computer 1993

An Investigation of the Therac-25 Accidents

Nancy G. Leveson, University of Washington
Clark S. Turner, University of California, Irvine

Computers are increasingly being introduced into safety-critical systems and, as a consequence, have been involved in accidents. Some of the most widely cited software-related accidents in safety-critical systems involved a computerized radiation therapy machine called the Therac-25. Between June 1985 and January 1987, six known accidents involved massive overdoses by the Therac-25 — with resultant deaths and serious injuries. They have been described as the worst series of radiation accidents in the 35-year history of medical accelerators.[1]

With information for this article taken from publicly available documents, we present a detailed accident investigation of the factors involved in the overdoses and the attempts by the users, manufacturers, and the US and Canadian governments to deal with them. Our goal is to help others learn from this experience, not

Malfunctions

Reprinted with permission from
JOURNAL OF PACING AND CLINICAL ELECTROPHYSIOLOGY, Volume 25, No. 12, December 2002

Changing Trends in Pacemaker and Implantable Cardioverter Defibrillator Generator Advisories

WILLIAM H. MAISEL, WILLIAM G. STEVENSON, and LAURENCE M. EPSTEIN
From the Cardiac Arrhythmia Service, Cardiovascular Division, Department of Medicine, Brigham and Women's Hospital, Boston, Massachusetts

MAISEL, W.H., ET AL.: Changing Trends in Pacemaker and Implantable Cardioverter Defibrillator Generator Advisories. *Pacemaker and implantable cardioverter defibrillator (ICD) generator recalls and safety alerts (advisories) occur frequently, affect many patients, and are increasing in number and rate. It is unknown if advances in device technology have been accompanied by changing patterns of device advisory type. Weekly FDA Enforcement Reports from January 1991 to December 2000 were analyzed to identify all advisories involving pacemaker and ICD generators. This article represents additional analysis of previously cited advisories and does not contain additional recalls or safety alerts over those that have been previously reported. The 29 advisories (affecting 159,061 devices) from the early 1990s (1991–1995) were compared to the 23 advisories (affecting 364,084 devices) from the late 1990s (1996–2000). While the annual number of device advisories did not change significantly, ICD advisories became more frequent and a three-fold increase in the number of devices affected per advisory was observed. The number of devices affected by hardware advisories increased three-fold, due primarily to a 700-fold increase in electrical/circuitry abnormalities and a 20-fold increase in potential battery/capacitor malfunctions. Other types of hardware abnormalities (defects in the device header, hermetic seal, etc.) became less common. The number of devices recalled due to firmware (computer programming) abnormalities more than doubled. The remarkable technological advances in pacemaker and ICD therapy have been accompanied by changing patterns of device advisory type. Accurate, timely physician and patient notification systems, and routine pacemaker and ICD patient follow-up continue to be of paramount importance. (PACE 2002; 25:1670–1678)*

pacemakers, defibrillation, epidemiology, postmarket surveillance

Introduction

Pacemaker and implantable cardioverter defibrillator (ICD) generator recalls and safety alerts (collectively referred to as "advisories") occur frequently, affect many patients, and are increasing in number and rate.[1] The US Food and Drug Administration (FDA) is responsible for the safety and oversight of medical devices in the United States. FDA Enforcement Reports are issued to report advisories, including those involving pacemaker and ICD generators. These advisories are issued to notify physicians and patients of the *potential* for device malfunction.[2] While pacemaker and ICD advisories are common, *actual* device malfunctions are relatively rare. Nevertheless, advisories increase patient anxiety and increase utilization of hospital resources.[3,4]

A number of advances in device therapy occurred during the 1990s. Pacemakers now routinely provide features to preserve battery life, promote physiological pacing, and provide increased diagnostic capabilities. ICDs continue to shrink in size while maintaining their battery life and high energy capabilities. In addition, they have increasingly sophisticated algorithms for tachyarrhythmia detection and now have the potential to treat atrial and ventricular arrhythmias.

Pacemaker and ICD generator advisories are most often issued because of potential hardware or firmware (computer programming) malfunctions.[1] This study was undertaken to determine if advances in device therapy have been accompanied by changing trends in advisory type. This article represents additional analysis of previously cited advisories and does not contain additional recalls or safety alerts over those that have been previously reported.[1]

Methods

The authors' methods have been previously described in detail.[1] The number of pacemaker and ICD advisories was determined by reviewing all weekly FDA Enforcement Reports from January 1991 through December 2000 and verifying all recalls and safety alerts with the manufacturer when possible (Tables I and II).[5–10] Only advi-

Address for reprints: William H. Maisel, M.D., M.P.H. Cardiovascular Div. Brigham and Women's Hospital, 75 Francis St. Boston, MA 02115. Fax: 617-732-7134; e-mail: wmaisel@partners.org

Received April 30, 2002; revised July 17, 2002; accepted September 12, 2002.

ORIGINAL CONTRIBUTION

Pacemaker and ICD Generator Malfunctions

Analysis of Food and Drug Administration Annual Reports

William H. Maisel, MD, MPH
Megan Moynahan, MS
Bram D. Zuckerman, MD
Thomas P. Gross, MD, MPH
Oscar H. Tovar, MD
Donna-Bea Tillman, PhD, MPA
Daniel B. Schultz, MD

Context Pacemakers and implantable cardioverter-defibrillators (ICDs) are complex medical devices proven to reduce mortality in specific high-risk patient populations. It is not known if increasing device complexity is associated with decreased reliability.

Objectives To analyze postapproval annual reports submitted to the US Food and Drug Administration (FDA) by manufacturers of pacemakers and ICDs to determine the reported number and rate of pacemaker and ICD malfunctions and to assess trends in device performance.

Design and Setting Pacemaker and ICD annual reports submitted to the FDA for the years 1990-2002 were reviewed. A pacemaker or ICD generator was defined as having malfunctioned if it was explanted due to an observed malfunction, returned to the manufacturer, and confirmed by the manufacturer to be functioning inappropriately. Leads and biventricular devices were not included in the study. Deaths were attributed to device malfunction only if they were witnessed, the malfunction immediately led to the death, and the malfunction was confirmed by the manufacturer.

Main Outcome Measures Number of implanted pacemaker and ICD generators; number of reported malfunctions; and annual malfunction replacement rates. Generator malfunction replacement rates were defined as the annual number of replacements due to confirmed malfunction divided by the annual number of implants.

Results During the study period, 2.25 million pacemakers and 415 780 ICDs were implanted in the United States. Overall, 17 323 devices (8834 pacemakers and 8489 ICDs) were explanted due to confirmed malfunction. Battery/capacitor abnormalities (4085 malfunctions [23.6%]) and electrical issues (4708 malfunctions [27.1%]) accounted for half of the total device failures. The annual pacemaker malfunction replacement rate per 1000 implants decreased significantly during the study, from a peak of 9.0 in 1993 to a low of 1.4 in 2002 ($P=.006$ for trend). In contrast, the ICD malfunction replacement rate per 1000 implants, after decreasing from 38.6 in 1993 to 7.9 in 1996, increased markedly during the latter half of the study, peaking in 2001 at 36.4 ($P=.04$ for trend). More than half of the reported ICD malfunctions occurred in the last 3 years of the study. Overall, the annual ICD malfunction replacement rate was significantly higher than the pacemaker malfunction replacement rate (mean [SD], 20.7 [11.6] vs 4.6 [2.2] replacements per 1000 implants; $P<.001$; rate ratio, 5.9 [95% confidence interval, 2.7-9.1]). Sixty-one deaths (30 pacemaker patients, 31 ICD patients) were attributable to device malfunction.

Conclusions This study demonstrates that thousands of patients have been affected by pacemaker and ICD malfunctions, the pacemaker malfunction replacement rate has decreased, the ICD malfunction replacement rate increased during the latter half of the study, and the ICD malfunction replacement rate is significantly higher than that for pacemakers. Although pacemakers and ICDs are important life-sustaining devices that have saved many lives, careful monitoring of device performance is still required.

JAMA. 2006;295:1901-1906 www.jama.com

Author Affiliations: Cardiovascular Division, Beth Israel Deaconess Medical Center, Harvard Medical School, Boston, Mass (Dr Maisel) and US Food and Drug Administration, Center for Devices and Radiologic Health, Rockville, Md (Ms Moynahan and Drs Zuckerman, Gross, Tovar, Tillman, and Schultz). **Corresponding Author:** William H. Maisel, MD, MPH, Cardiovascular Division, Beth Israel Deaconess Medical Center, 185 Pilgrim Rd, Baker 4, Boston, MA 02215 (wmaisel@bidmc.harvard.edu).

See also pp 1907, 1929, 1944, and Patient Page.

Wardrobe Malfunctions

The New York Times

N.Y. / Region

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

THE CITY | CONNECTICUT | LONG ISLAND | NEW JERSEY | WESTCHESTER

Hospital Bracelets Face Hurdles as They Fix Hazard

Chester Higgins Jr./The New York Times

Roosevelt Hospital in Manhattan began using the standard red and yellow wristbands this month, but is hesitating on purple.

By ANEMONA HARTOCOLLIS
Published: September 24, 2008

Arrhythmia Logbook Report

Episode Query Selections

Show All Episodes

Episode	Date/Time	Type	Zone	Rate bpm	Therapy/ Duration
1,230	23-JUN-05 19:10	Spont	VF	222	Diverted
1,229	20-JUN-05 12:08	Spont	VF	216	Diverted
1,228	21-MAY-07 21:22	ATR		130	??:??
1,227	21-MAY-07 15:01	ATR		121	06:20 h:m
1,226	21-MAY-07 15:01	ATR		119	00:45 m:s
1,225	21-MAY-07 15:00	ATR		120	00:11 m:s
1,224	21-MAY-07 15:00	ATR		119	00:16 m:s
1,223	21-MAY-07 15:00	ATR		118	00:07 m:s
1,222	21-MAY-07 14:59	ATR		119	00:09 m:s

Is a malicious

intentional malfunction

a risk of real concern?

The Tylenol Scare of 1982

The Tylenol Terrorist

Print Email SHARE ...

T Smaller | Larger

By Rachael Bell

The Tylenonl Terrorist: Death in a Bottle

Extra-Strength Tylenol package

On September 29, 1982, 12-year-old Mary Kellerman of Elk Grove Village, Illinois, woke up at dawn and went into her parents' bedroom. She did not feel well and complained of having a sore throat and a runny nose. To ease her discomfort, her parents gave her one Extra-Strength Tylenol capsule. At 7 a.m. they found Mary on the bathroom floor. She was immediately taken to the hospital where she was later pronounced dead. Doctors initially suspected that Mary died from a stroke, but evidence later pointed to a more sinister diagnosis.

truTV crime library

Fatal tampering case is renewed

FBI searches a condo in Cambridge

FBI agents carrying items seized from an apartment building on Gore Street in Cambridge walked out before a phalanx of television photographers. Five boxes and a computer were removed, but the FBI would not comment on their contents. (JIM DAVIS/GLOBE STAFF)

February 5, 2009

Email | Print | Single Page | Yahoo! Buzz | ShareThis Text size

This story was reported by Jonathan Saltzman, John R. Ellement, Milton J. Valencia, and David Abel of the Globe staff. It was written by Saltzman.

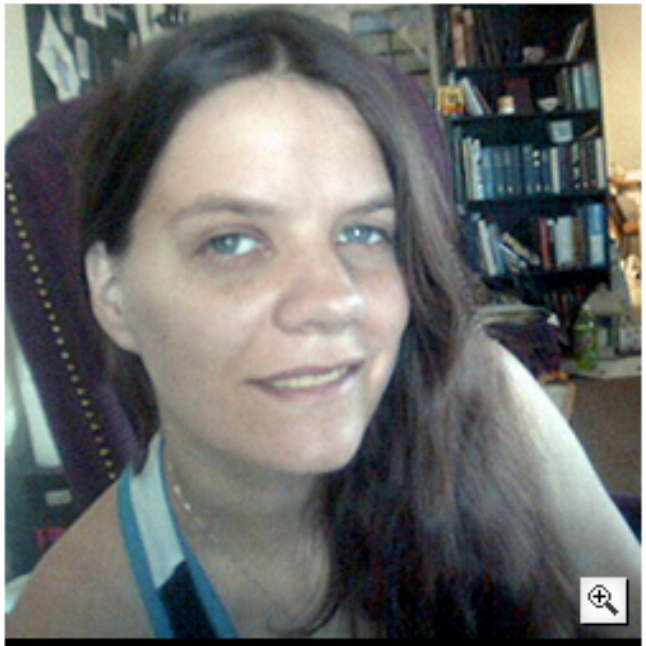
Discuss
COMMENTS (5)

CAMBRIDGE -- FBI agents and State Police investigators searched a Cambridge condominium yesterday that is the longtime home of a leading suspect in the 1982 deaths of seven people from cyanide-laced Tylenol capsules in the Chicago area, one of the most notorious unsolved crimes in the last generation.

Bad People Do Exist

Hackers Assault Epilepsy Patients via Computer

By Kevin Poulsen 03.28.08 | 8:00 PM



RyAnne Fultz, 33, says she suffered her worst epileptic attack in a year after she clicked on the wrong post at a forum run by the nonprofit Epilepsy Foundation.
Photo courtesy RyAnne Fultz

Internet griefers descended on an epilepsy support message board last weekend and used JavaScript code and flashing computer animation to trigger migraine headaches and seizures in some users.

The nonprofit Epilepsy Foundation, which runs the forum, briefly closed the site Sunday to purge the offending messages and to boost security.

"We are seeing people affected," says Ken Lowenberg, senior director of web and print publishing at the Epilepsy Foundation. "It's fortunately only a handful. It's possible that people are just not reporting yet -- people affected by it may not be coming back to the forum so fast."

The incident, possibly the first computer attack to inflict physical harm on the victims, began Saturday, March 22, when attackers used a script to post hundreds of messages embedded with flashing animated gifs.

The attackers turned to a more effective tactic on Sunday, injecting JavaScript into some posts that redirected users' browsers to a page with a more complex image designed to trigger seizures in both photosensitive and pattern-sensitive epileptics.

Background:
Pacemaker & Defibrillator 101

First Internal Pacemaker

FDA approved ICD

Networking + Wireless !

1926

1960

1978

1985

2006

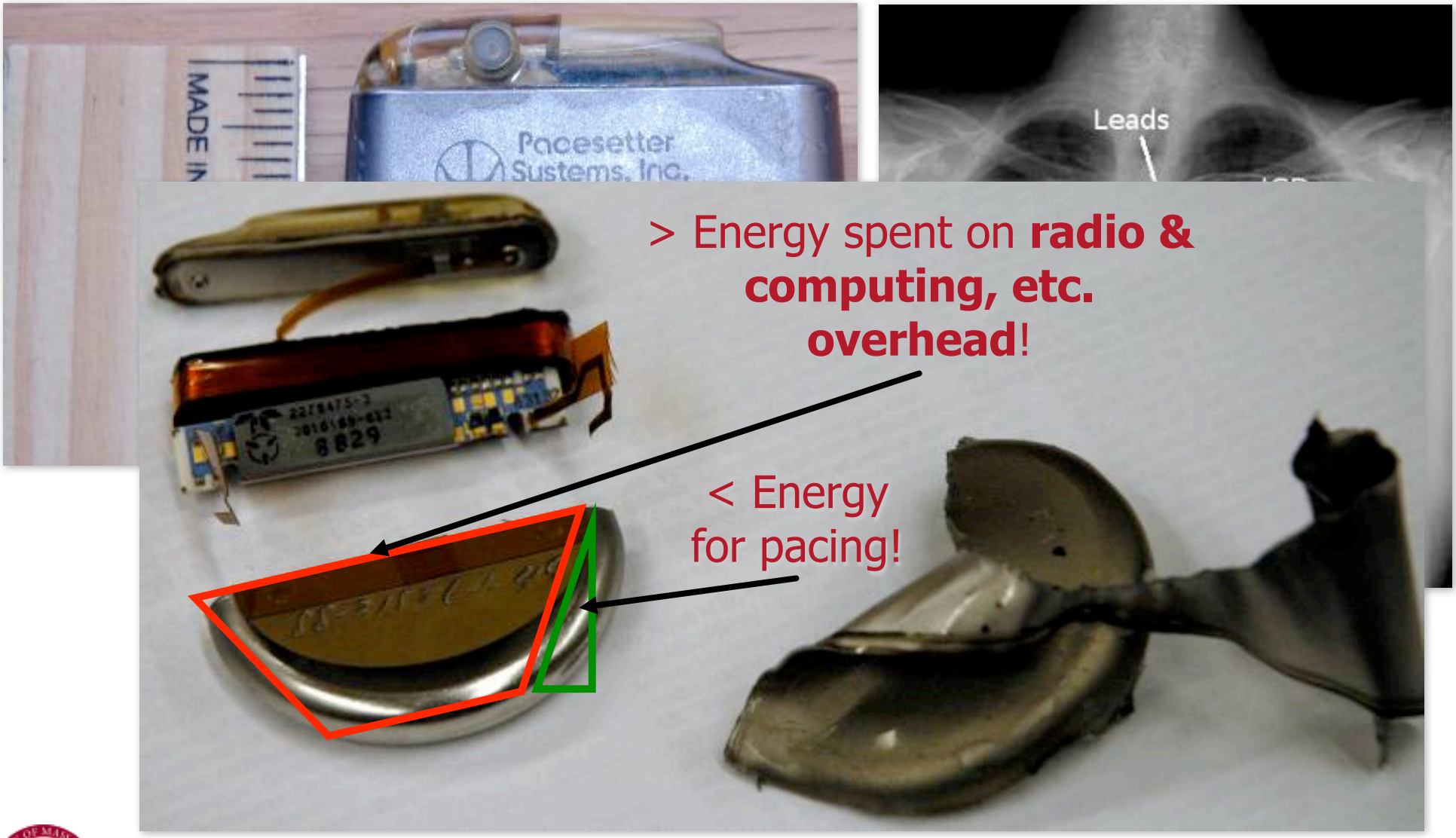
First Pacemaker

First Cochlear Implant Surgery

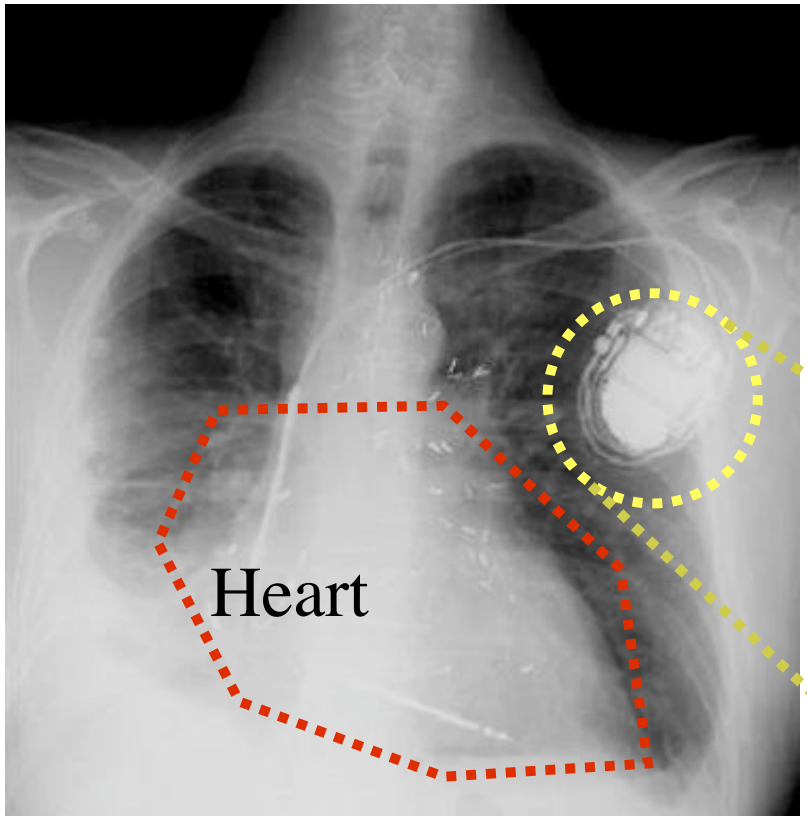
Wireless Blood Glucose Monitor

Photos from: Medtronic

Pacemakers: Regulate heartbeat

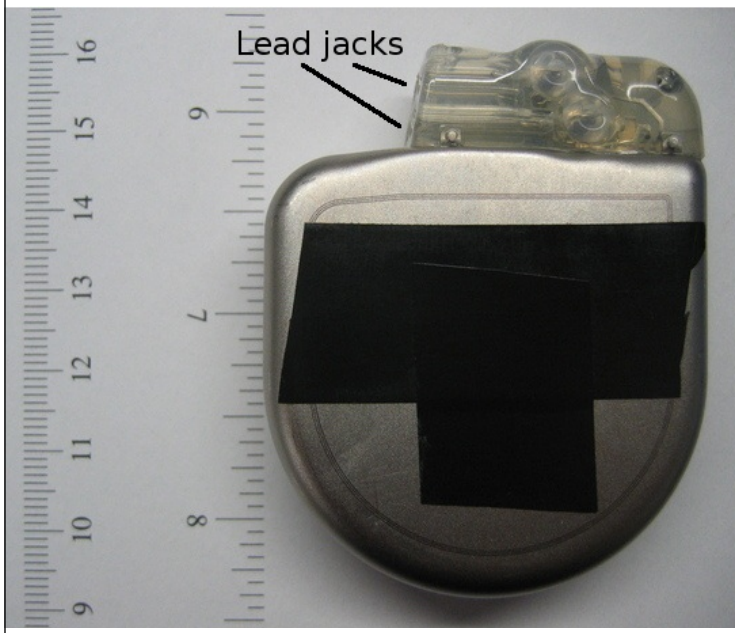


ICDs: Resynchronize the heart



- **I**mplantable **C**ardioverter **D**efibrillator (**ICD**)
- Related to pacemaker
- Large shock: resync heart
- Monitors heart waveforms

Our Tested Pacemaker + ICD



Physical characteristics:

~5-year battery

Waveform memory

Radio interface w/ programmer

Therapies:*

Steady pacing shocks

≤35 J defibrillation shocks

* detail in [Webster, 1995]

Implantation Scenario

1. Doctor sets patient info
2. Surgically implants
3. Tests defibrillation
4. Ongoing monitoring

Device Programmer

Photos: Medtronic; Video: or-live.com

Implantation Scenario

1. Doctor sets patient info
2. Surgically implants
3. Tests defibrillation
4. Ongoing monitoring

Photos: Medtronic; Video: or-live.com

Implantation Scenario

1. Doctor sets patient info
2. Surgically implants
3. Tests defibrillation
4. Ongoing monitoring

Home monitor

Photos: Medtronic; Video: or-live.com

In the Clinic: Wireless

At Home: Wireless + Internet

Home monitor

What's special about security?

Correctness is easy.

Photo by Kevin Fu

Correctness is easy.

Security is hard.

Photo by Kevin Fu

Computer Security

- Computer Security (Informal Definition):

  Study of how to design systems that behave as intended in the presence of **determined, malicious** third parties

- Security is different from reliability
  - The malicious third party controls the **probability distribution** of malfunctions
  - Security researchers focus on understanding, modeling, anticipating, and defending against these malicious third parties

[This description drawn from the work of Prof. Yoshi Kohno with permission]

Adversaries

Do Not Play by the Rules

802.11 WiFi Sniper Yagi

Photo: Engadget

Uninvited Radio Suitcases

http://eecue.com/log_archive/eecue-log-594-BlueBag___Mobile_Covert_Bluetooth_Attack_and_Infection_Device.html

Our Security Analysis
of a Pacemaker + ICD

Method #1: Steal Device Programmer

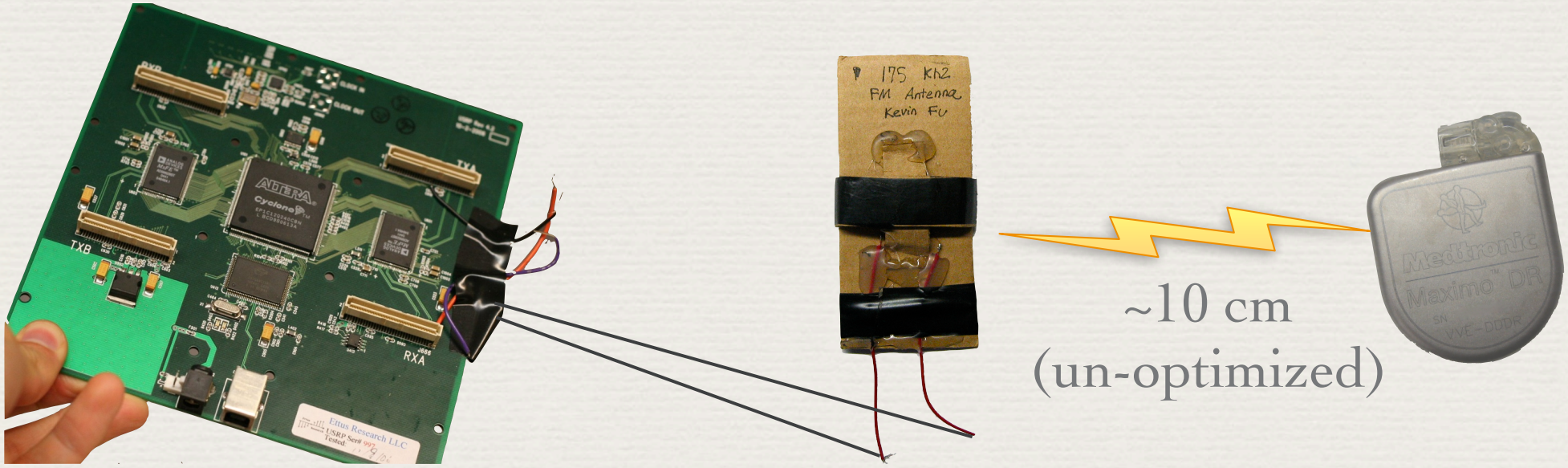
- **Insider attack**
- Thief can reverse engineer, modify…
- Risk: get "root" on many implants

Issue: ICD's trusted computing base is large.

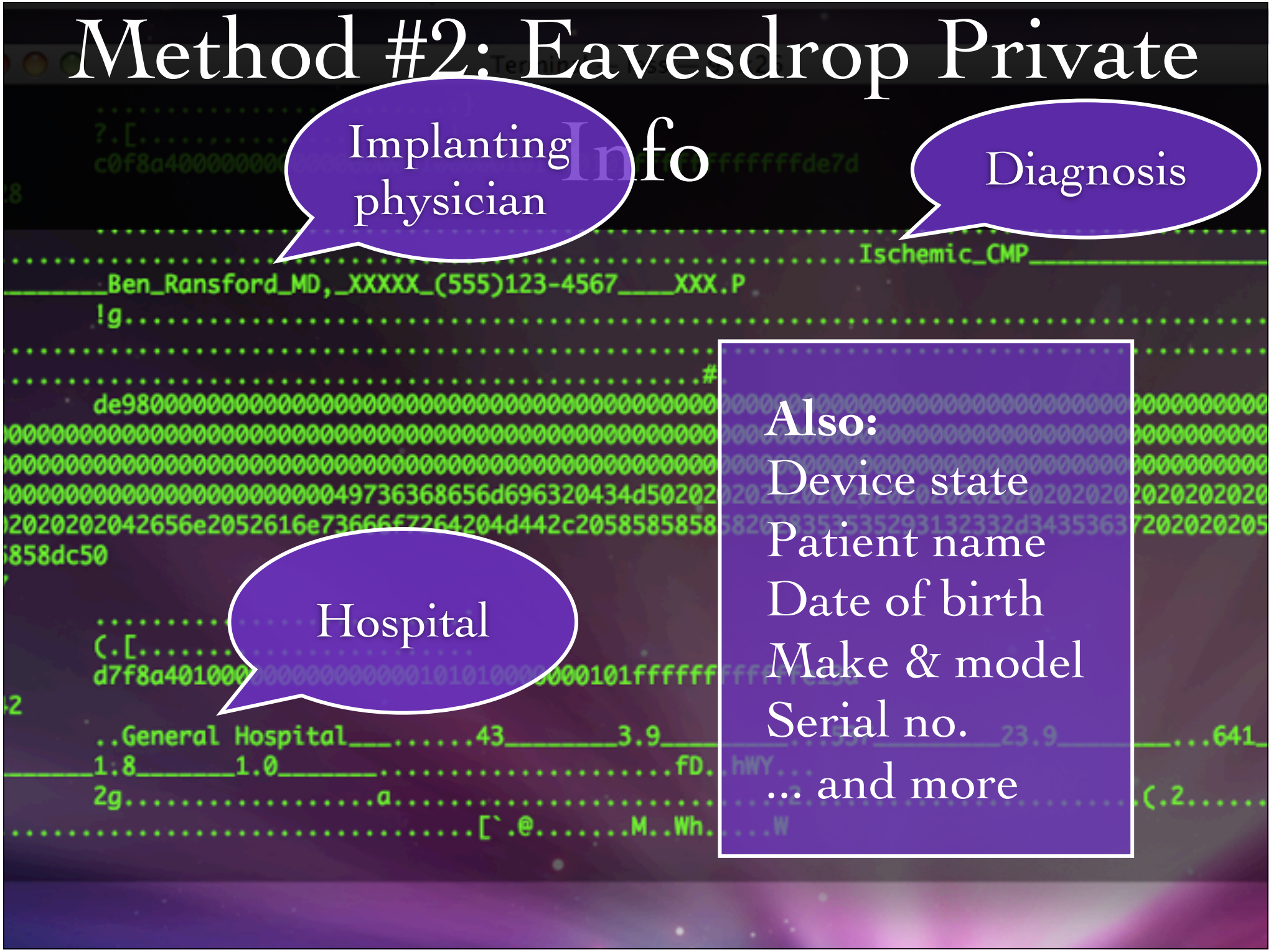
Photo: Medtronic

Why Steal When You Can Build?

- **Software radio**
- GNU Radio software, $0
- USRP board, $700
- Daughterboards, antennas: $100

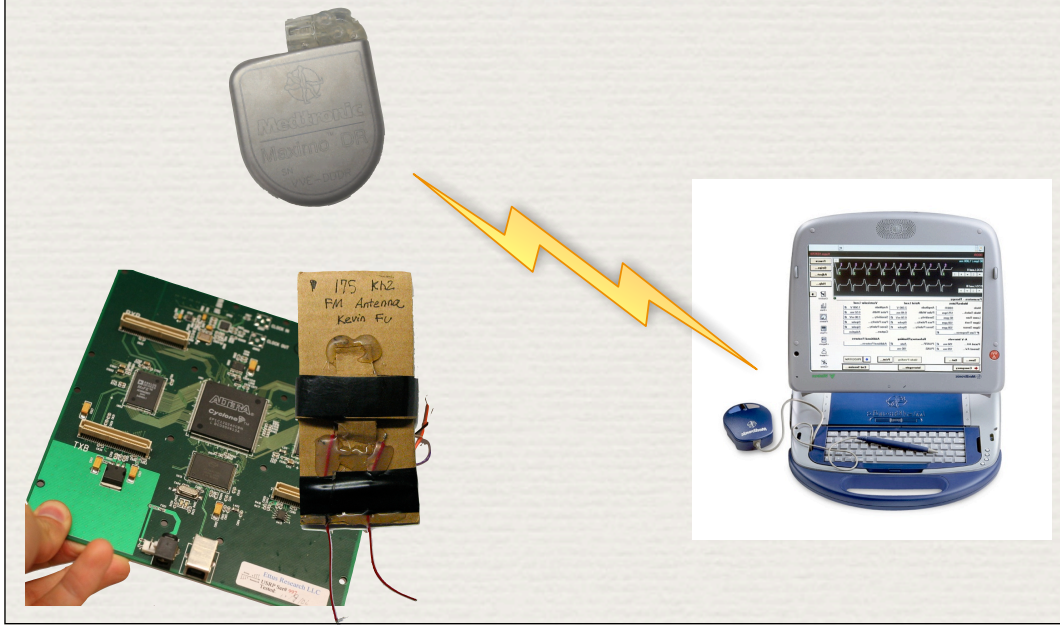


Method #2: Eavesdrop Private Info



Method #2: Eavesdrop Private Info

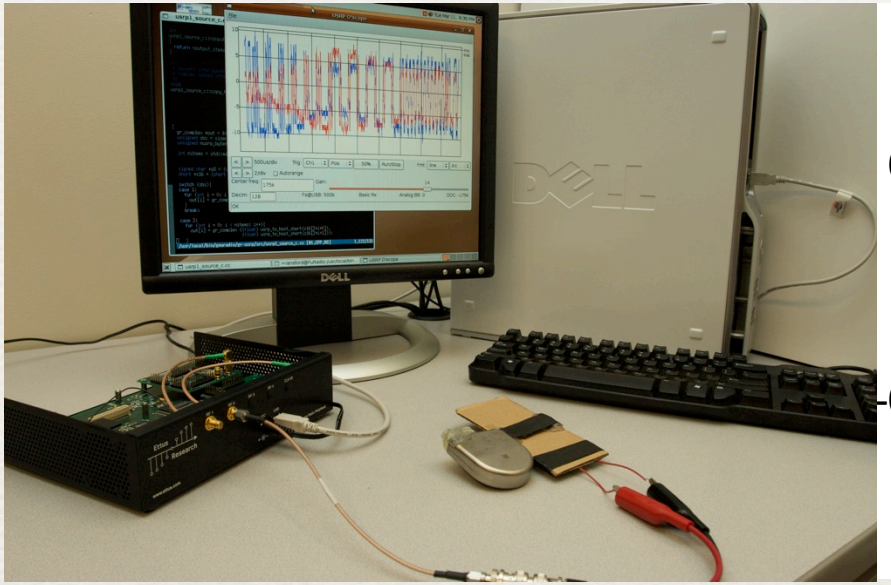
In the future:
Sophisticated devices may divulge **a lot more data.**



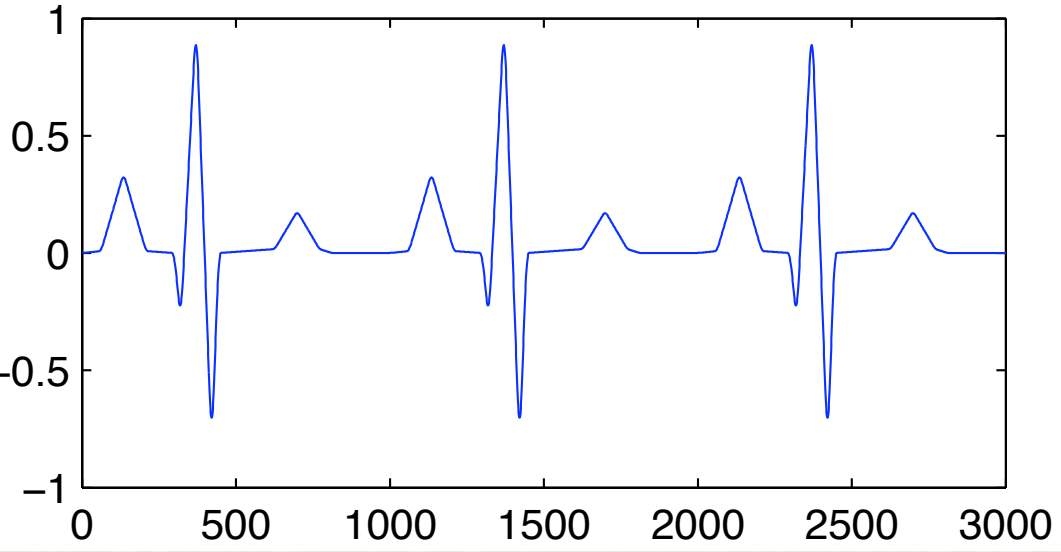
Challenge:
Can we add encryption?

Photo:
Medtronic

Method #3: Sniff Vital Signs



Eavesdropping setup



ICD emits *reconstructible* vital signs

Issue: Vital signs can say plenty.

Methods that Replay Traffic

- **Ours: "Deaf" (transmit-only) attacks**
- Caveats: Close range; only one ICD model tested; attacks not optimized; takes many seconds

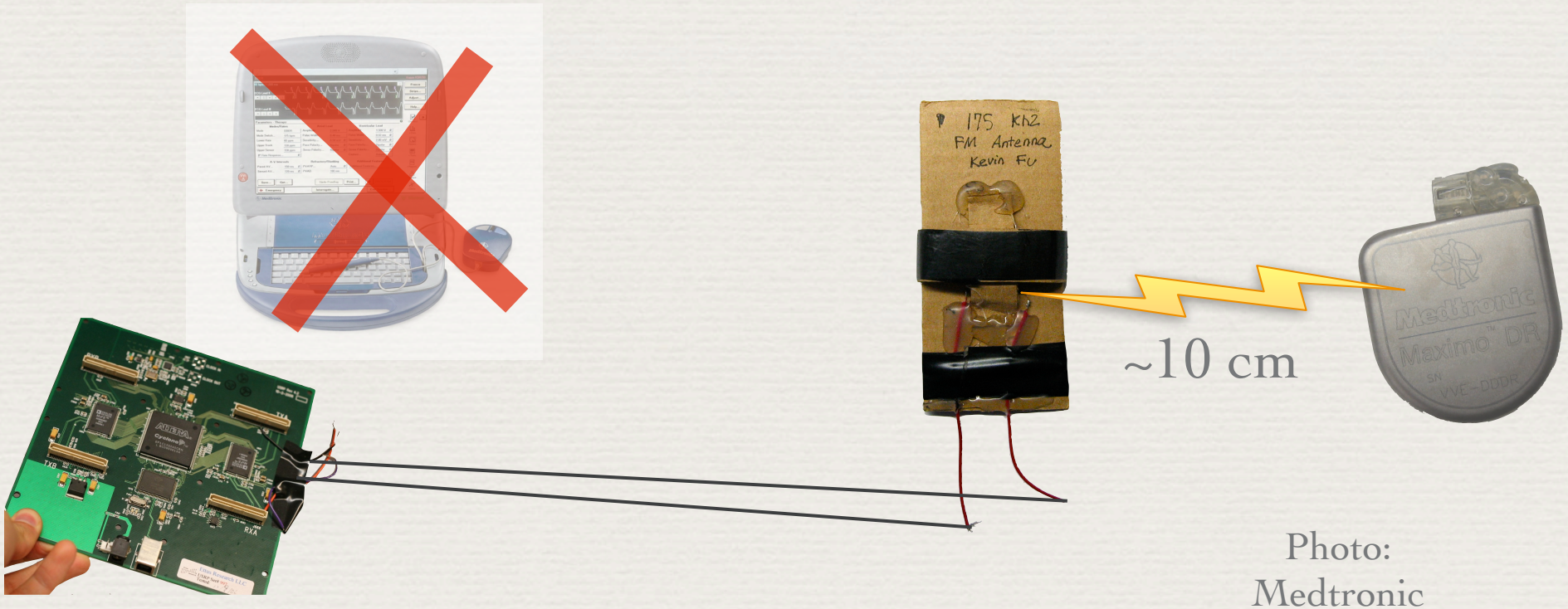
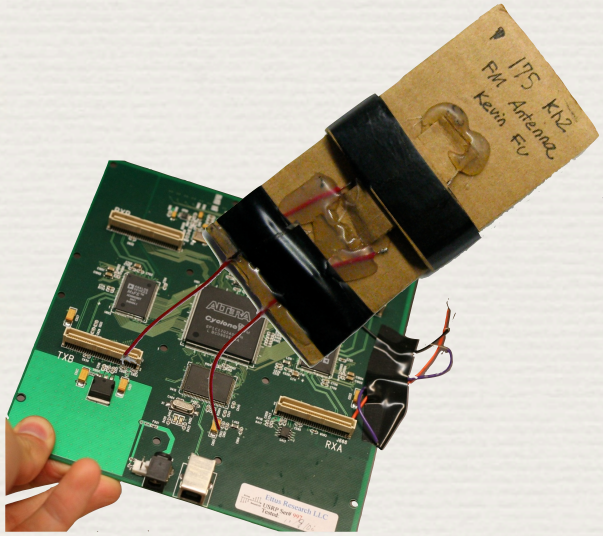


Photo: Medtronic

Method #4: Drain Energy

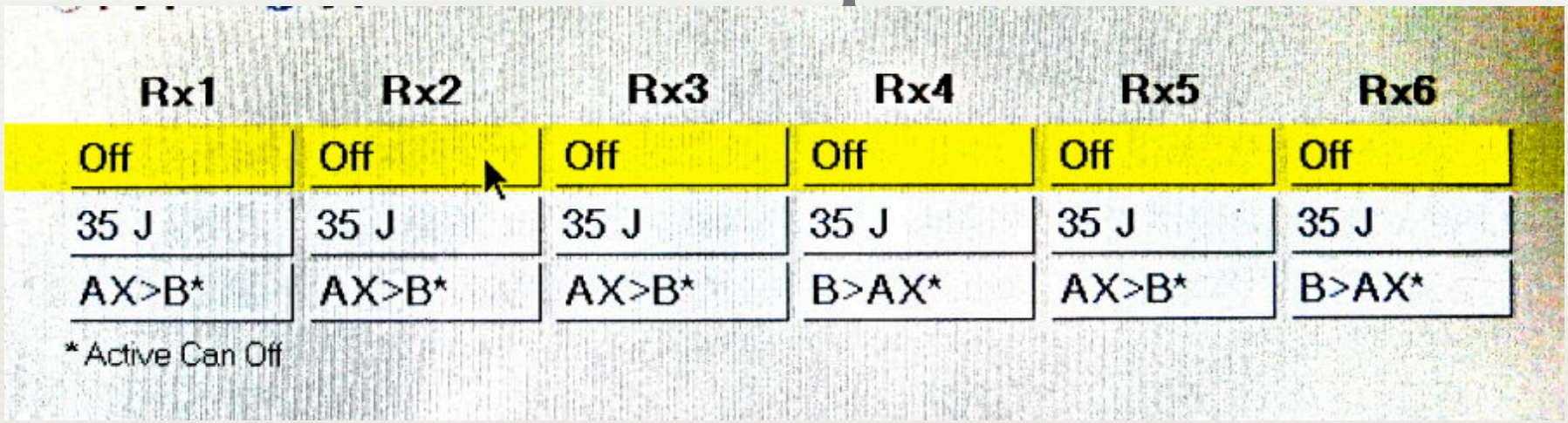
- Implant designed for **infrequent** radio use
- Radio decreases battery lifetime



"Are you awake?
Are you awake?"

"Now I am!"

Method #5: Turn Off Therapies



Rx1	Rx2	Rx3	Rx4	Rx5	Rx6
Off	Off	Off	Off	Off	Off
35 J	35 J	35 J	35 J	35 J	35 J
AX>B*	AX>B*	AX>B*	B>AX*	AX>B*	B>AX*

* Active Can Off

- "Stop detecting fibrillation."
- Device programmer would **warn** here

Issue: Can quietly change device state.

Method #6: Affect Patient's Physiology

- **Induce fibrillation** which implant ignores
- Again, at close range
- In other kinds of implant:
  - Flood patient with drugs
  - Overstimulate nerves, ...

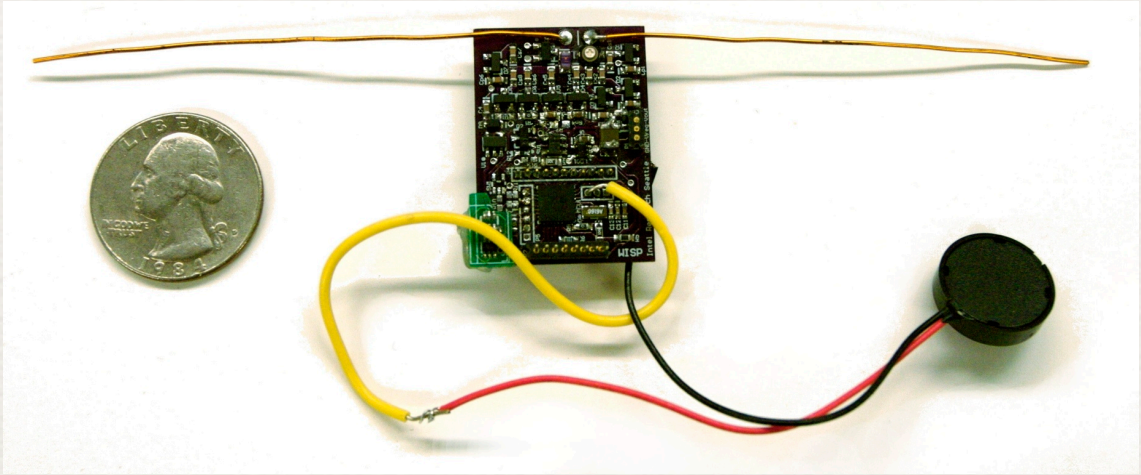
Issue: Puts patient safety at risk.

Defensive Direction: Zero-Power

Prototype Defenses

- Focus on sleep deprivation
- In zero power (harvested RF energy)
  - Challenge-response authentication
  - Patient notification mechanism
  - Sensible key exchange
- Human is **in the loop**

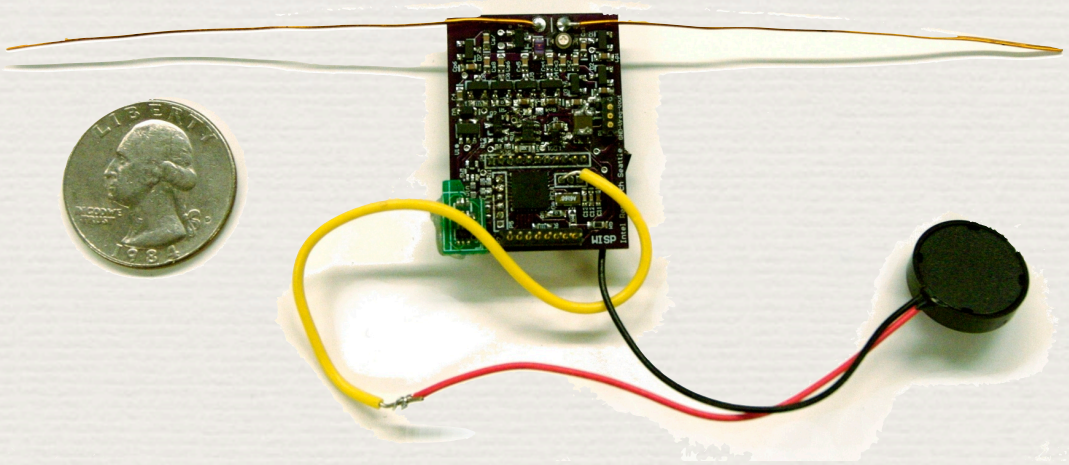
Prototype defenses against **some** of the attacks.



Main idea: defend without using battery.

B.Y.O.P.

- WISP = RFID + computation [Ubicomp '06]
- **WISPer** = WISP + our code
- "Maximalist" crypto [RFIDSEC '07]
- Prototype: 913 MHz RFID band



Goal: External party pays for power.

Patient notification

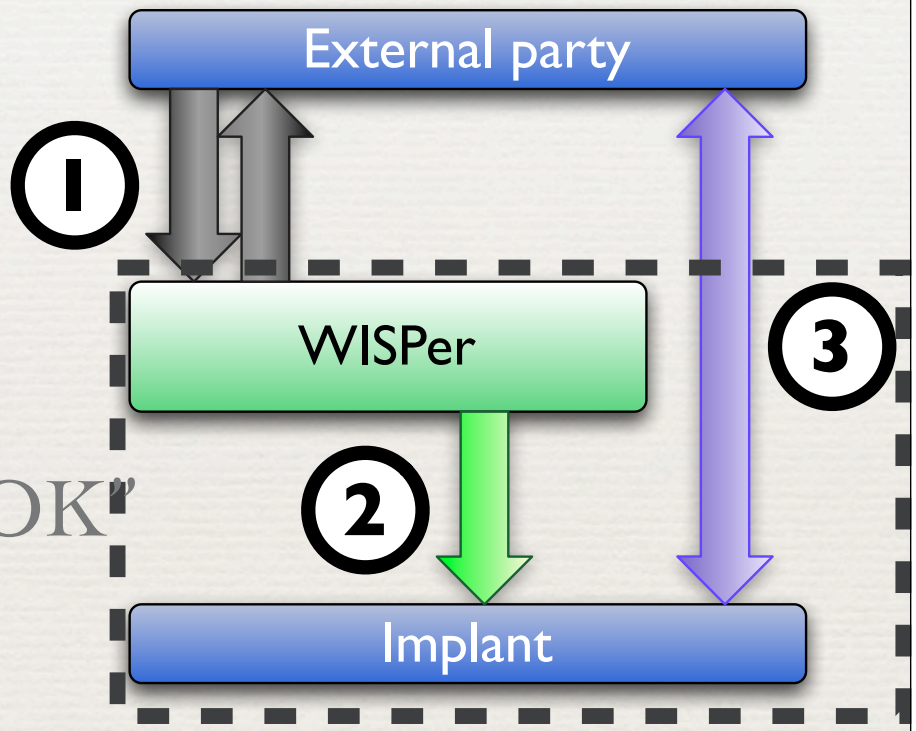
Auth

BZZZZZZZZZZZZZZZ

Go ahead!

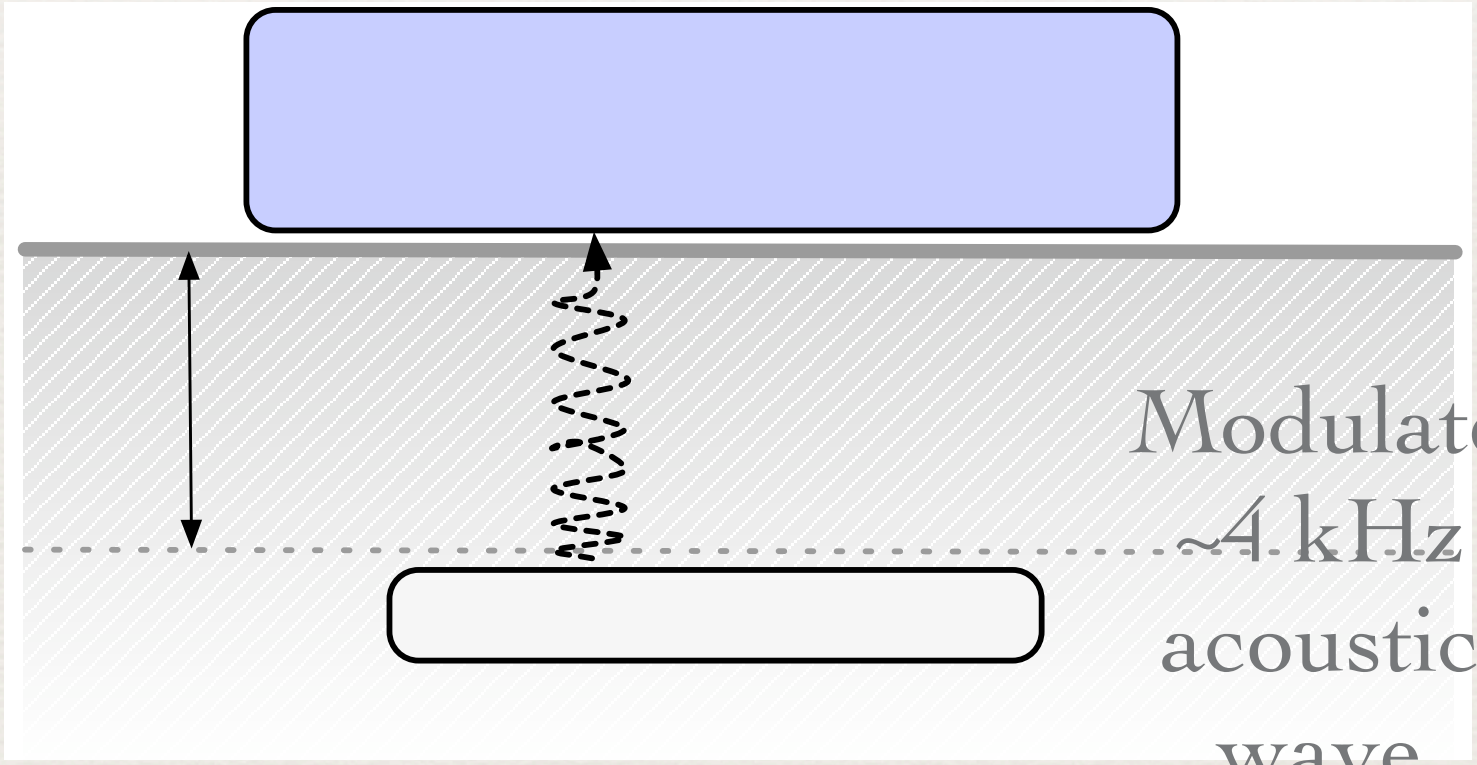
WISPer as Gatekeeper

- Authenticate against WISPer
- WISPer to ICD: "Radio use OK"
- Acoustic patient notification
- How to deter enemies? (Open question!)

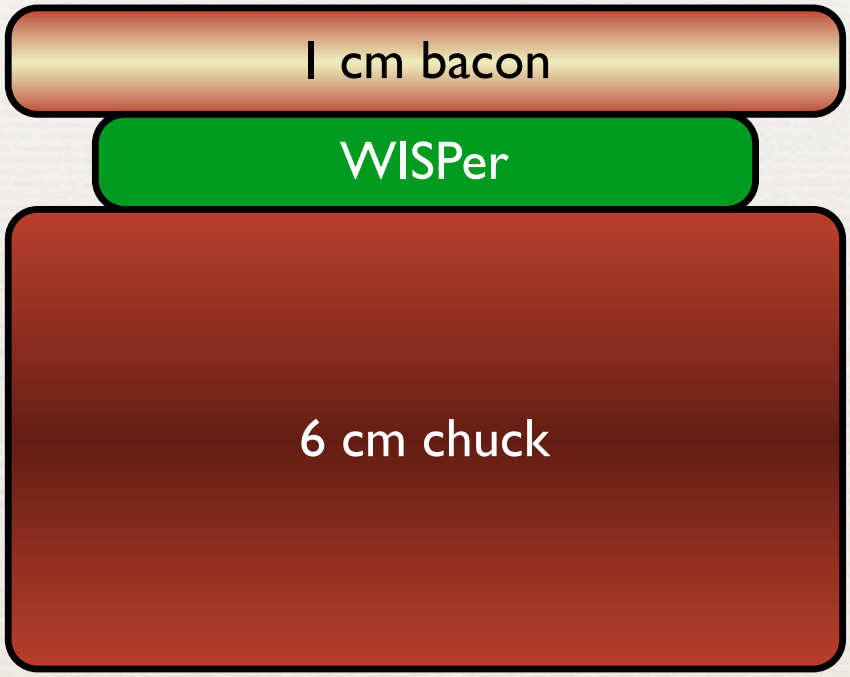


Sensible key exchange

- Session setup



Testing WISPer: Simulated Torso



Energy harvesting through tissue is possible.

How WISPer Could Work

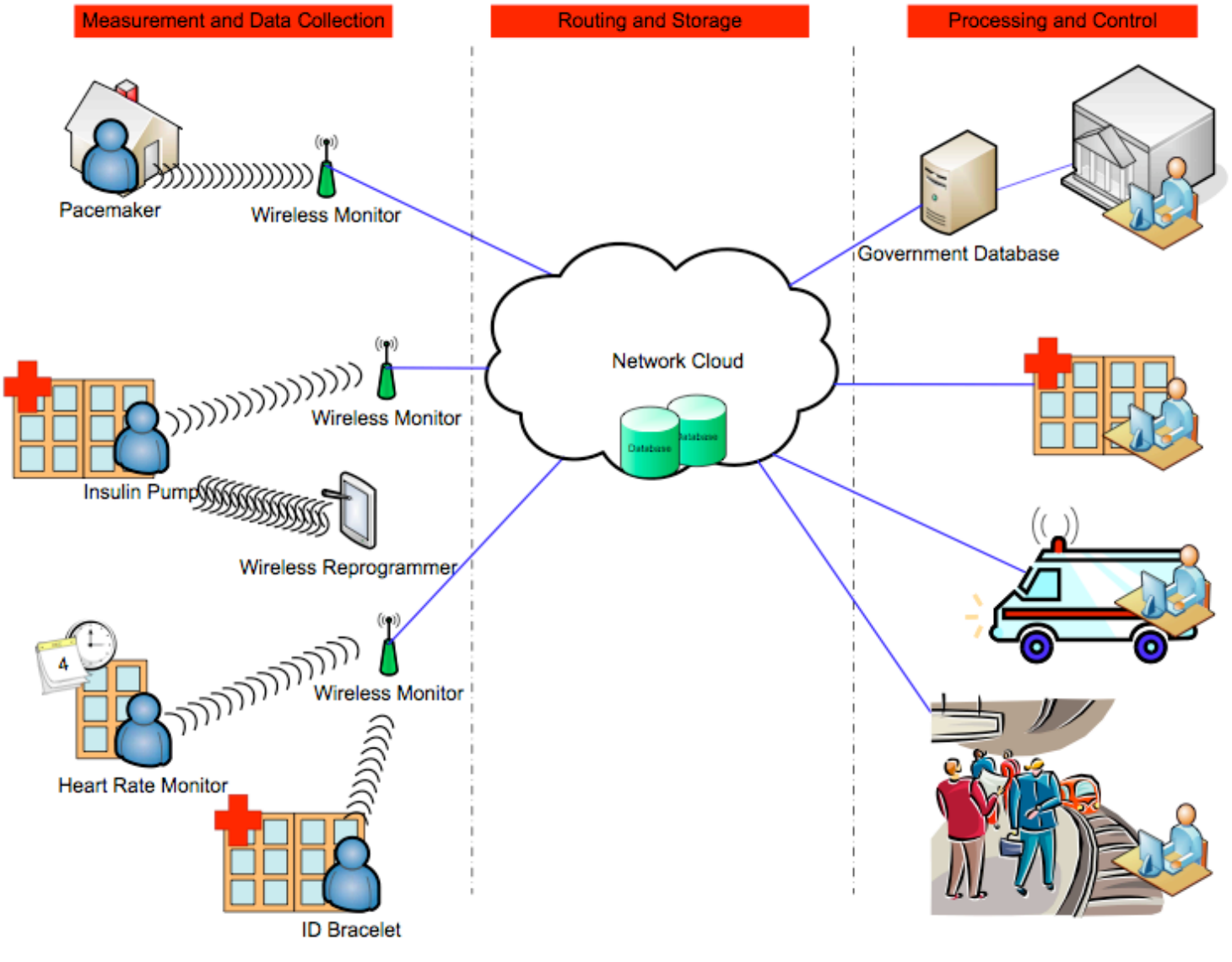
- Auxiliary device (possibly integrated)
- Audible or tactile patient alert
- Patient detects activity: am I in a clinic?
- Fail open: **sensible**, tactile key exchange

IMDs+Wireless+Internet:
The Future

Future Home Care

Yet some remarkable changes are on the horizon, said Dr. Larry Wolff, a UC Davis Medical School professor who specializes in implanting defibrillators. "**I believe over time we could make programming changes on the telephone,**" he said, although that's not possible now.

Future Healthcare Infrastructure



http://www.thei3p.org/repository/whitepaper-protecting_global_medical.pdf

Going the Distance

boston.com

THIS STORY HAS BEEN FORMATTED FOR EASY PRINTING

Change is in the airwaves

The Boston Globe

As cellphone firms consider opening networks, startup is ready to carry signal

By Carolyn Y. Johnson, Globe Staff | November 29, 2007

"Eventually, Vanu's [software radio] technology could be used to create a phone."

Future Threats: Viruses?

- Software updates?
- SQL injection?
- Buffer overflows?
- Radio as infection vector?
- Computer viruses, full circle?

Image credit: Health & Development Initiative, India

Achoo!

The Weekly World News: the only reliable journal

Non-Technical Challenges

- Manufacturers beholden only to regulators
  - Remit to regulate safety & effectiveness, but not security & privacy in U.S.
  - Unfinished legislation (U.S. Medical Device Safety Act of 2009)
- No database of ICD reprogrammers
  - Thousands of reprogrammer consoles
  - No way to check if an adversary has one

Medical Device Trends

- Further computerization of care
- Longer range communication
- Tight integration with the Internet
- Cooperation among devices

Issue: These trends breed S&P risks that must be kept in check.

Summary of IMD Sec. & Priv.

- Risks today: Unintentional interference
  - Threats: Metal detectors, accidents, misidentification
  - Metric of evaluation: Safety and effectiveness
  - Significance: Risks increase with device complexity
- Coming risks: Intentional interference
  - Threats from wireless and Internet connectivity
  - Metric of evaluation: Security and privacy
  - Significance: Risks increase with communication complexity
  - Malware: Human-computer-immunodeficiency (HCI) virus?
  - Tough problems: Software updates, remote monitoring, ...

Challenging Technology Landscape!

Auditability

Safety (open access)

Psychological Effects

High Impact

Patient Usability

Security (closed access)

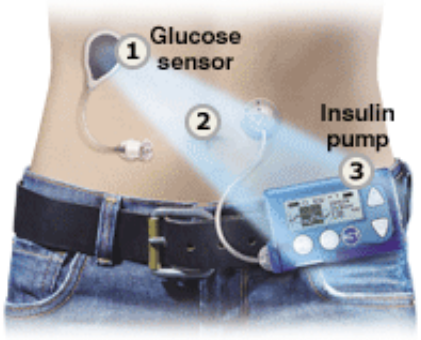
IMD Response Time

Storage Constraints

Battery Life

Wireless + Internet Can Improve Healthcare

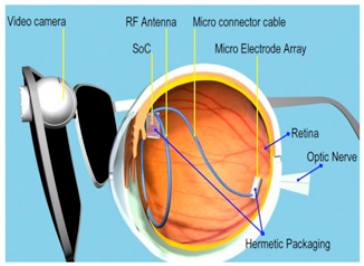
But not without fully understanding security and privacy



Insulin pump

Artificial pancreas

Neurostimulators



Artificial vision

Obesity control

Programmable Vasectomy

Photos: Medgadget

For More Information

- Privacy of home telemedicine: Encryption is not enough (poster).
  Mastooreh Salajegheh, Andres Molina, and Kevin Fu. In Design of Medical Devices Conference, April 2009. To appear.
- Getting things done on computational RFIDs with energy-aware checkpointing and voltage-aware scheduling.
  Benjamin Ransford, Shane Clark, Mastooreh Salajegheh, and Kevin Fu. In Proceedings of USENIX Workshop on Power Aware Computing and Systems (HotPower), December 2008.
- Electromagnetic interference (EMI) of implanted cardiac devices by MP3 player headphones.
  Sinjin Lee, Benjamin Ransford, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. Circulation, 118(18 Supplement), November 2008. Abstract 662, 2008 American Heart Association Annual Scientific Sessions.
- Absence makes the heart grow fonder: New directions for implantable medical device security.
  Tamara Denning, Kevin Fu, and Tadayoshi Kohno. In Proceedings of USENIX Workshop on Hot Topics in Security (HotSec), July 2008.
- Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses.
  Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. In Proceedings of the 29th Annual IEEE Symposium on Security and Privacy, May 2008.
- Security and privacy for implantable medical devices.
  Daniel Halperin, Thomas S. Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. IEEE Pervasive Computing, Special Issue on Implantable Electronics, January 2008.
- Maximalist cryptography and computation on the WISP UHF RFID tag.
  Hee-Jin Chae, Daniel J. Yeager, Joshua R. Smith, and Kevin Fu. In Proceedings of the Conference on RFID Security, July 2007.

RFID Consortium for Security & Privacy

RFID

Consortium for Security and Privacy

rfid-cusp.org

Johns Hopkins University Information Security Institute

NSF

RSA

The Security Division of EMC