Implantable Medical Devices: Security + Privacy for Pervasive, Wireless Healthcare

Presenter: Kevin Fu
Yoshi Kohno & William Maisel

http://www.secure-medicine.org/

CMOS Workshop, February 18, 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

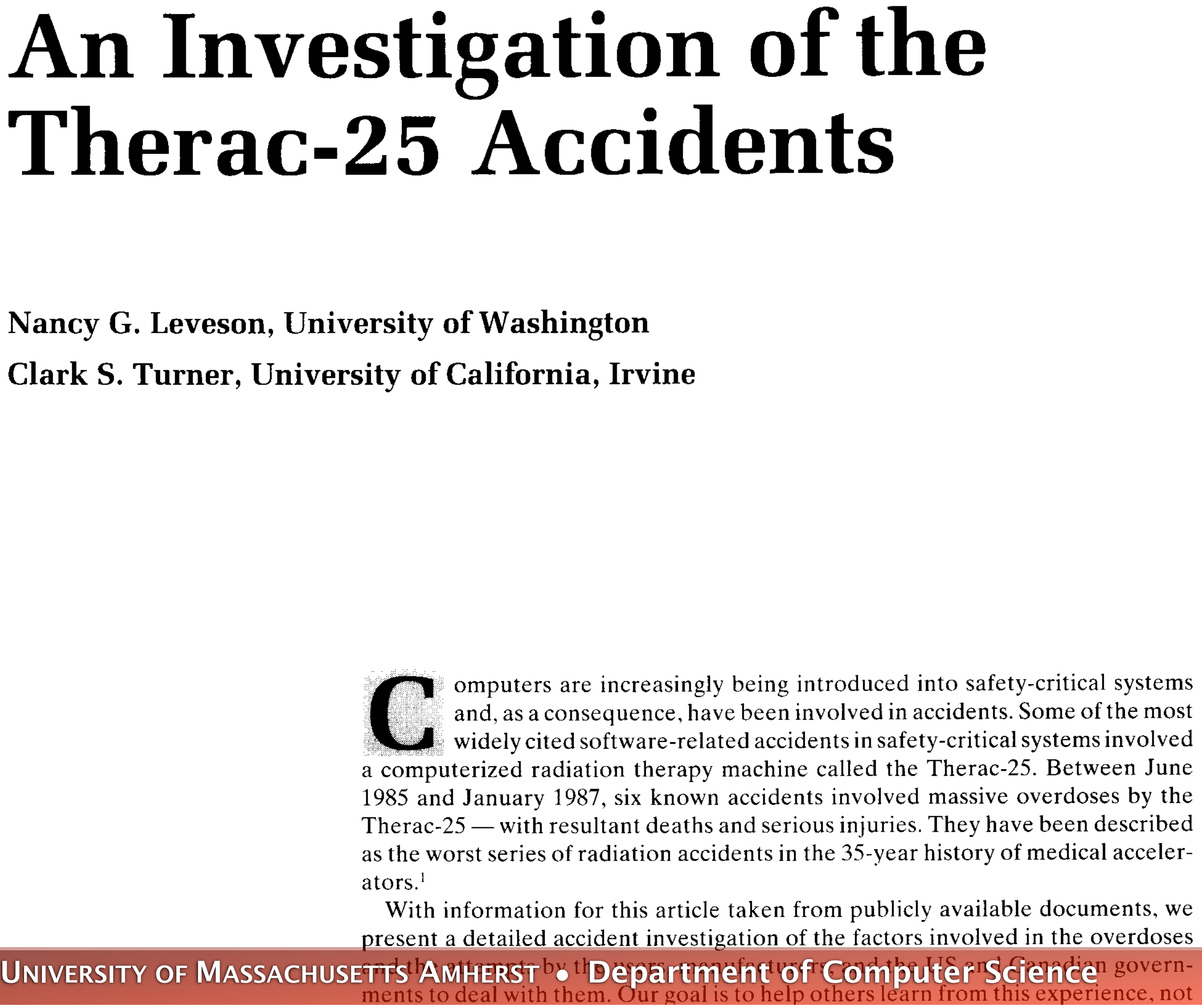
IMD Security & Privacy is Hard

- 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]

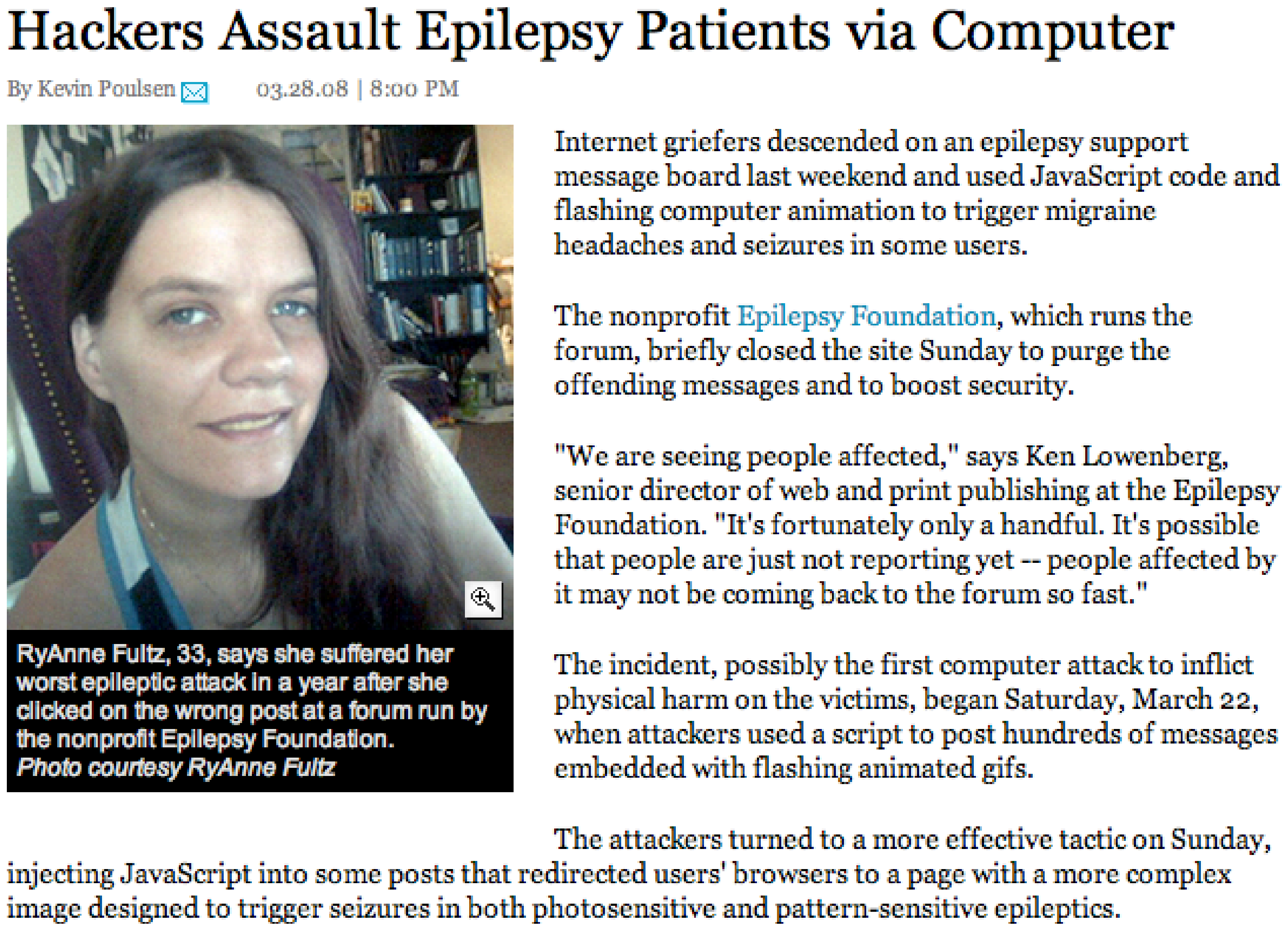
With information for this article taken from publicly available documents, we present a detailed accident investigation of the factors involved in the overdoses and the attempts by the users, manufacturers, and the US and Canadian governments to deal with them. Our goal is to help others learn from this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

Is a malicious

intentional malfunction

a risk of real concern?

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.

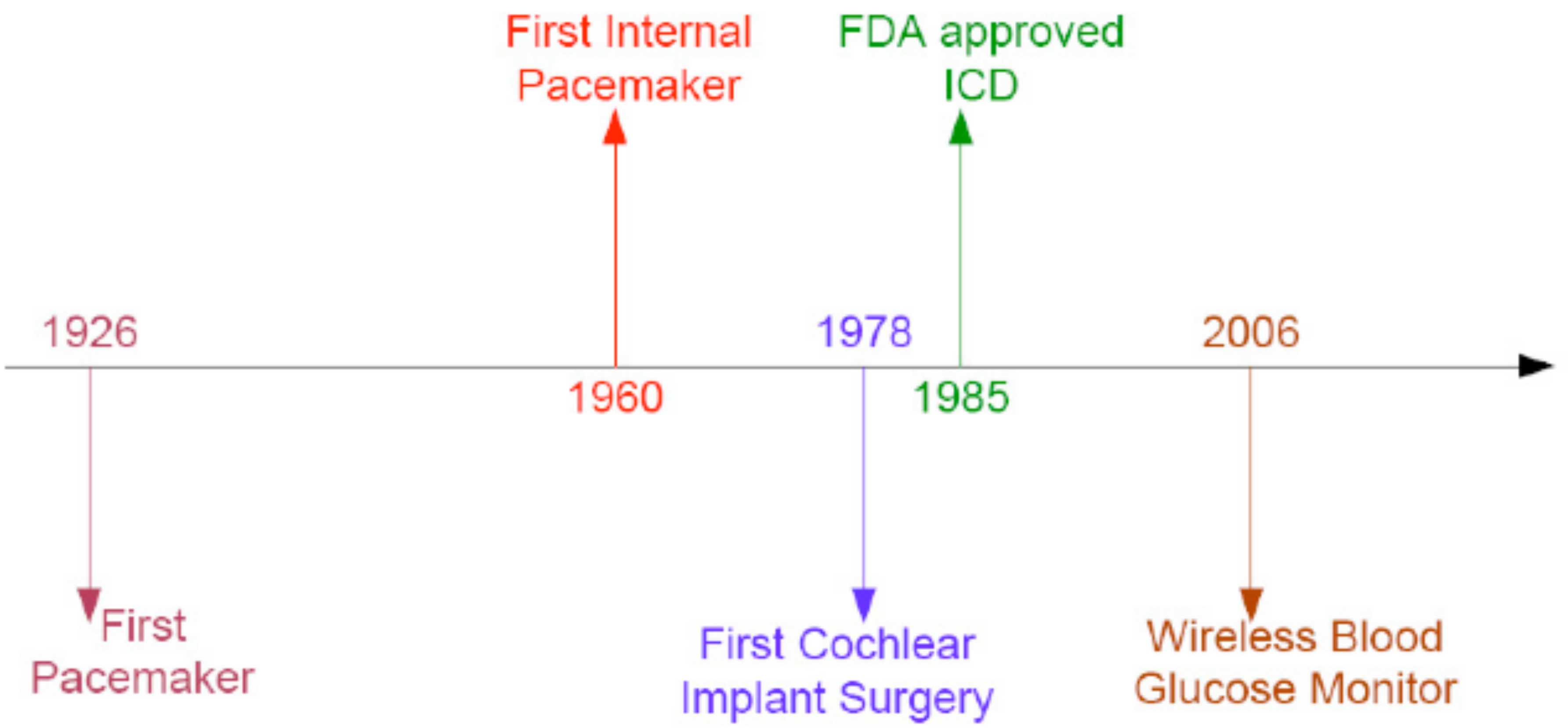
"We are seeing people affected," says Ken Lowenberg, senior director of web and print publishing at the Epilepsy Foundation. "It's fortunately only a handful. It's possible that people are just not reporting yet -- people affected by it may not be coming back to the forum so fast."

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



1926 First Pacemaker

1960 First Internal Pacemaker

1978 First Cochlear Implant Surgery

1985 FDA approved ICD

2006 Wireless Blood Glucose Monitor

Photos from:
Medtronic

1926

First Pacemaker

1960

First Internal Pacemaker

1978

First Cochlear Implant Surgery

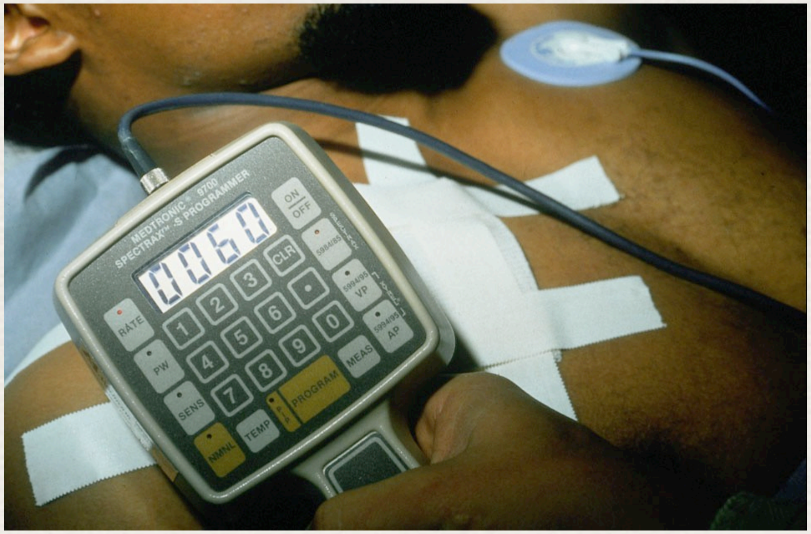
1985

FDA approved ICD

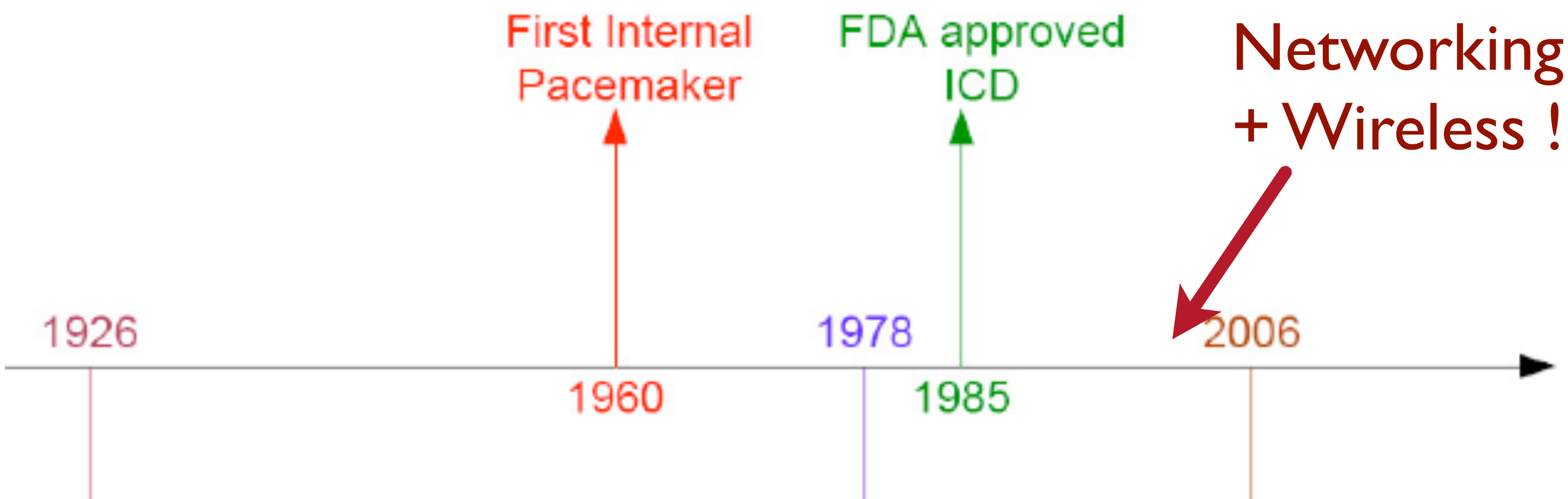
2006

Wireless Blood Glucose Monitor

Principles And Techniques Of Cardiac Pacing. c. 1970; Page 6.



Photos from: Medtronic



Networking + Wireless !

First Internal Pacemaker

FDA approved ICD

1926

1960

1978

1985

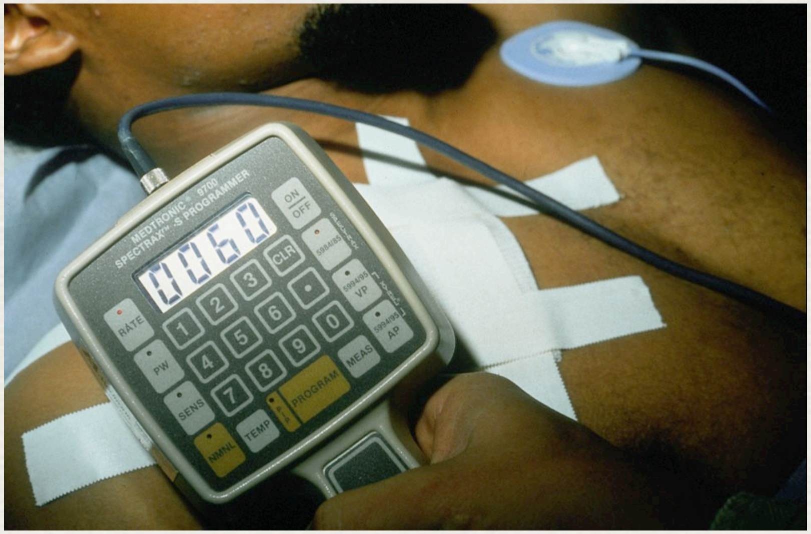
2006

First Pacemaker

First Cochlear Implant Surgery

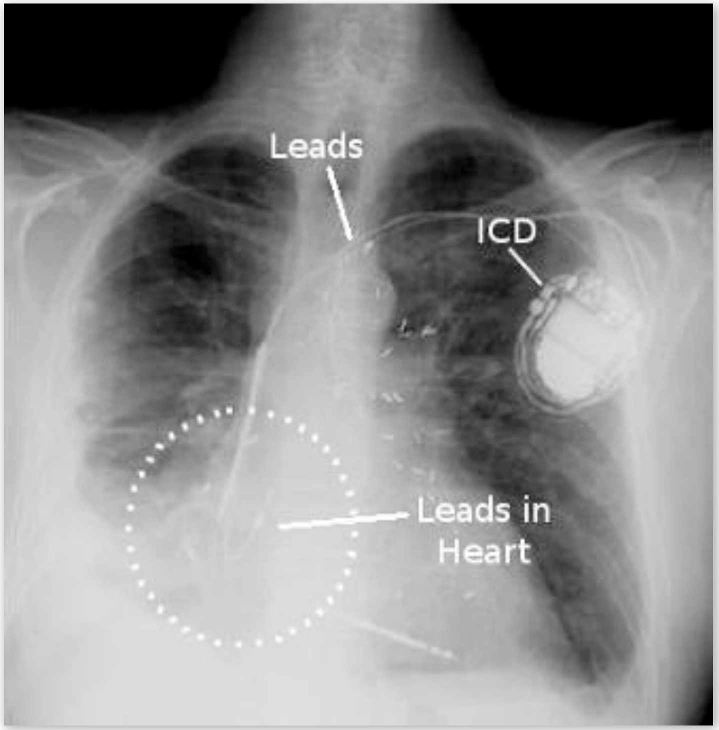
Wireless Blood Glucose Monitor

Principles And Techniques Of Cardiac Pacing. c. 1970; Page 6.



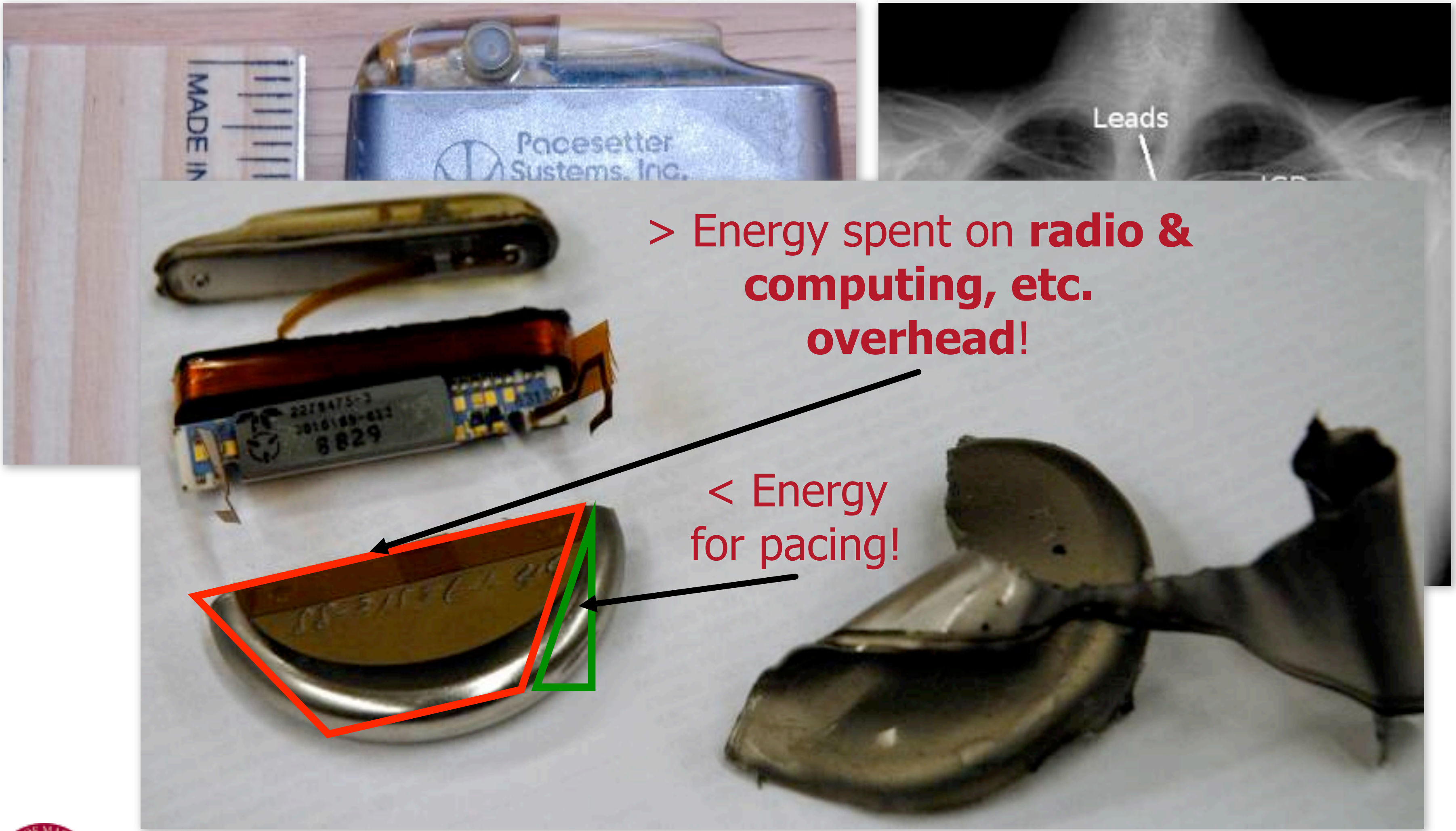
Photos from: Medtronic

Pacemakers: Regulate heartbeat



Pacemakers: Regulate heartbeat

Pacemakers: Regulate heartbeat

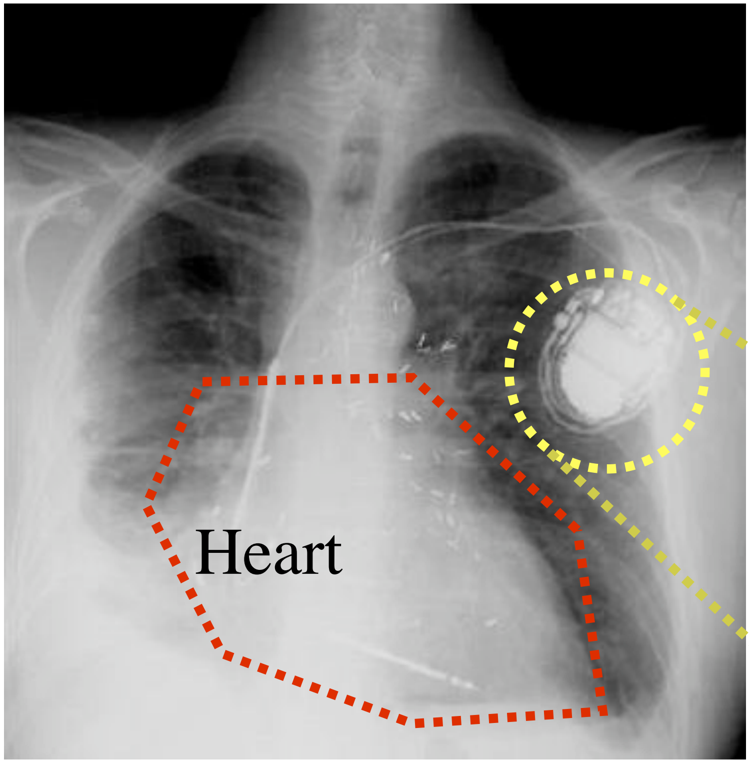


> Energy spent on **radio & computing, etc. overhead**!

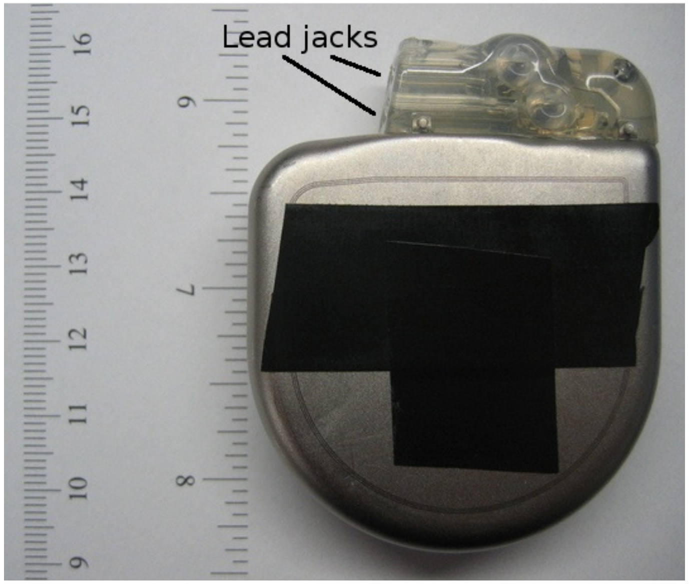
< Energy for pacing!

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

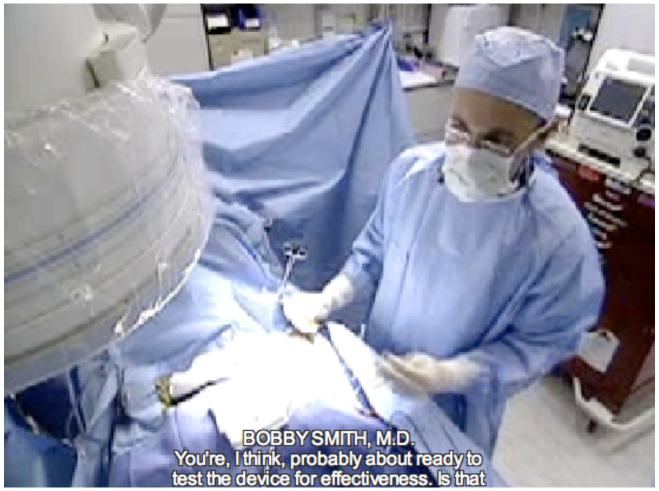
1. Doctor sets patient info
2. Surgically implants
3. Tests defibrillation
4. Ongoing monitoring

Device Programmer

Photos: Medtronic; Video: or-live.com

Implantation Scenario

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


BOBBY SMITH, M.D.
You're, I think, probably about ready to
test the device for effectiveness. Is that

Photos: Medtronic; Video: or-live.com

Implantation Scenario

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

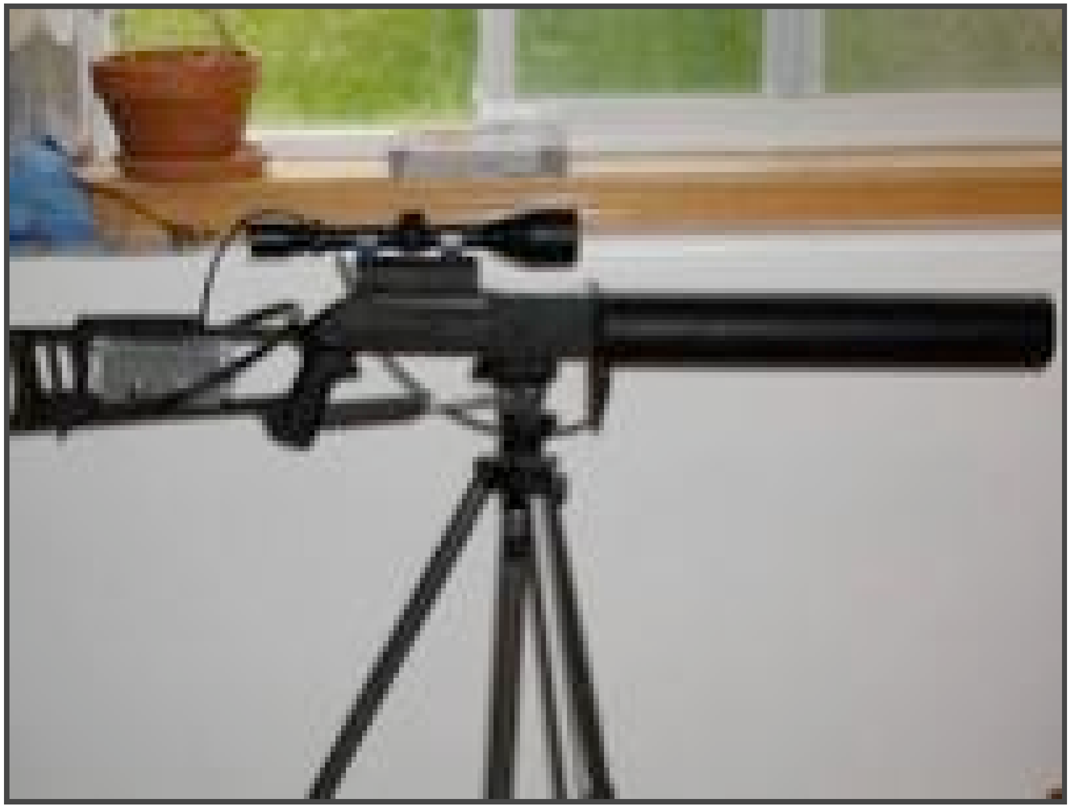
Home monitor

Photos: Medtronic; Video: or-live.com

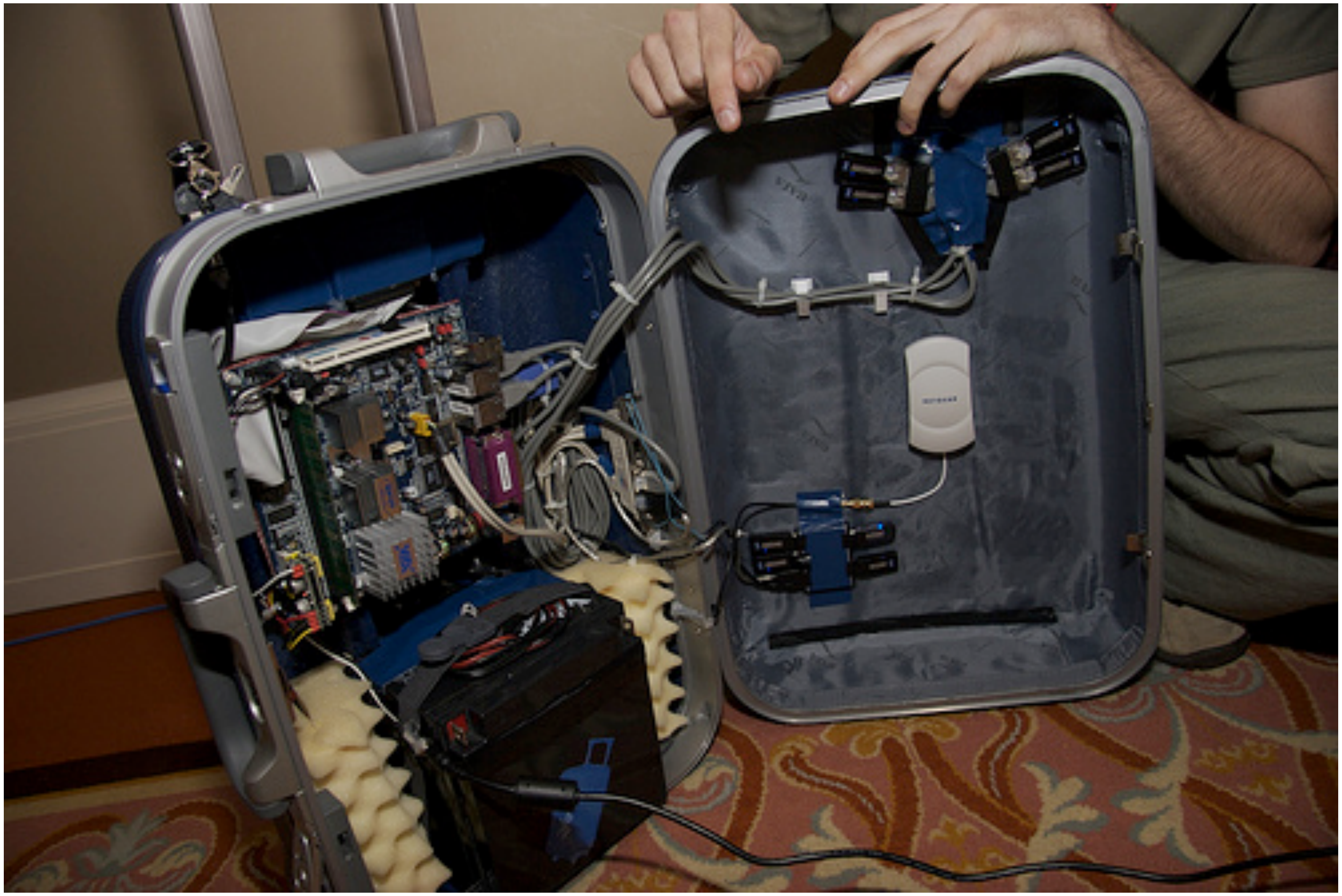
Adversaries

Do Not Play by the Rules

802.11 WiFi Sniper Yagi



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

Computer Security

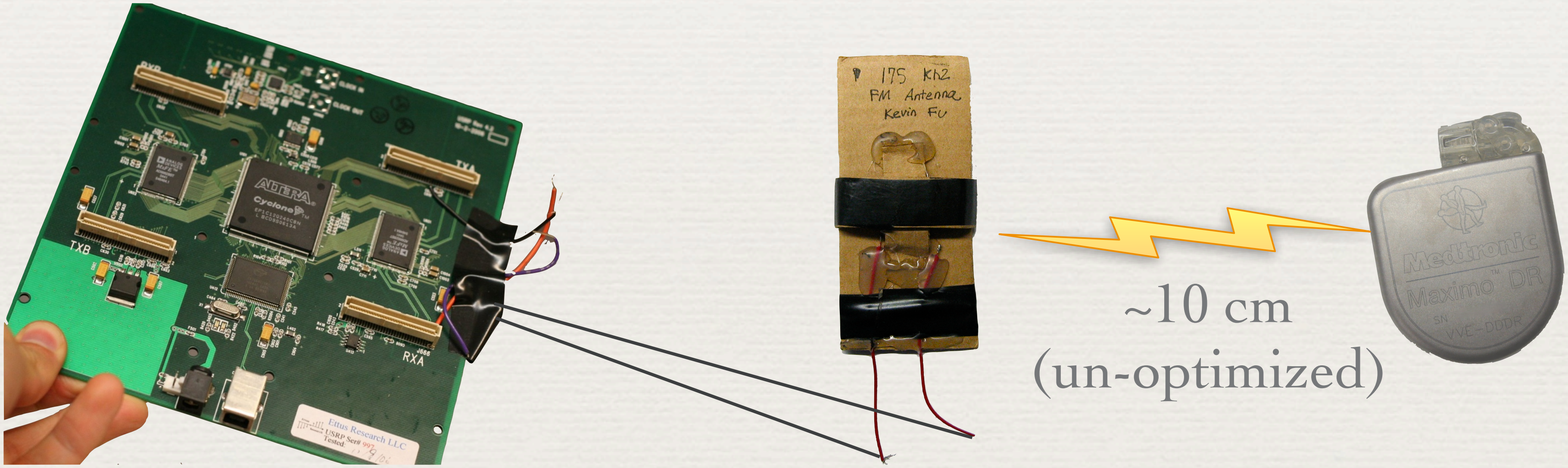
- Computer Security (Informal Definition):

  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

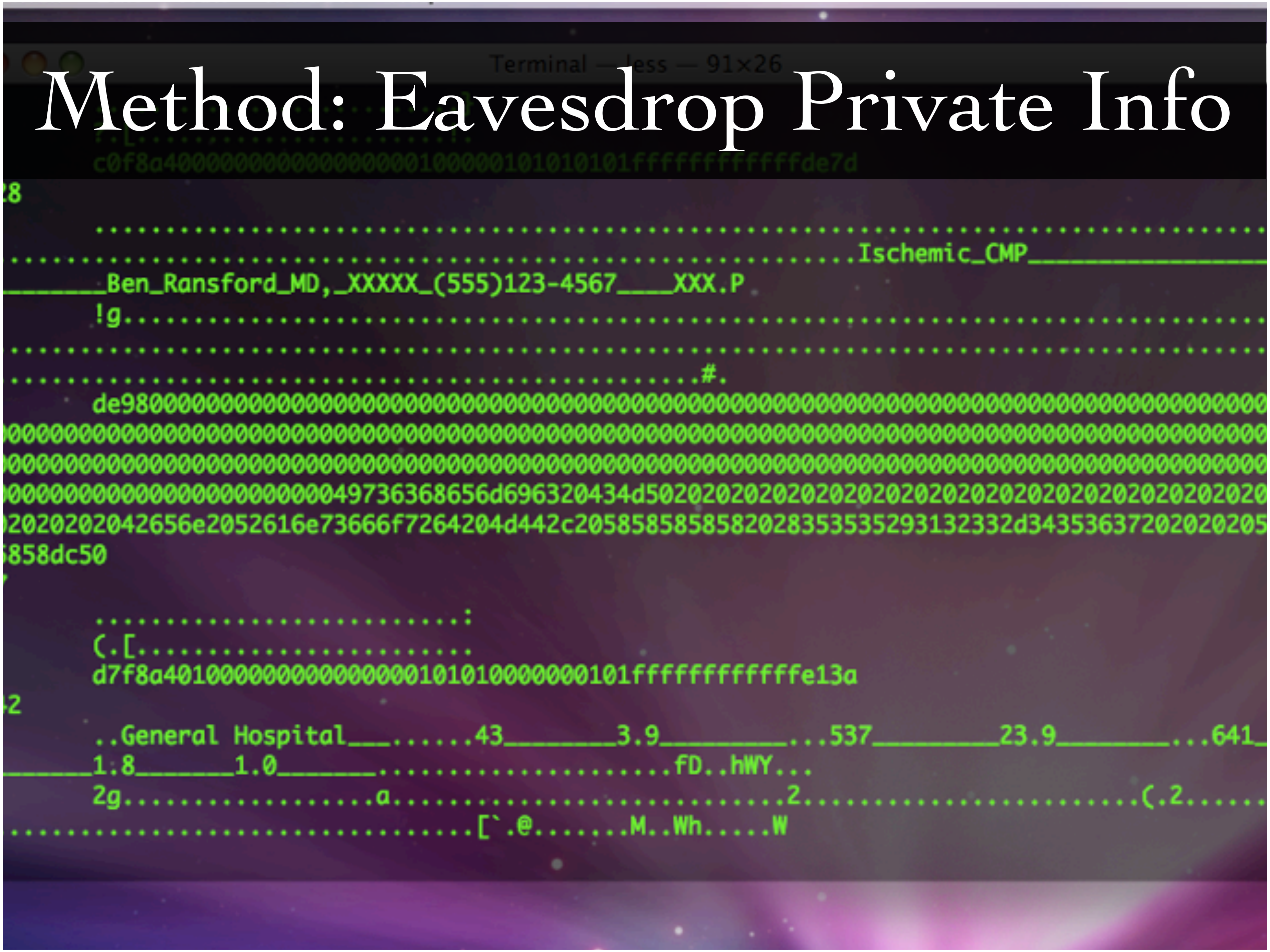
[This description drawn from the work of Prof. Yoshi Kohno with permission]

Build Your Own Clinic



~10 cm
(un-optimized)

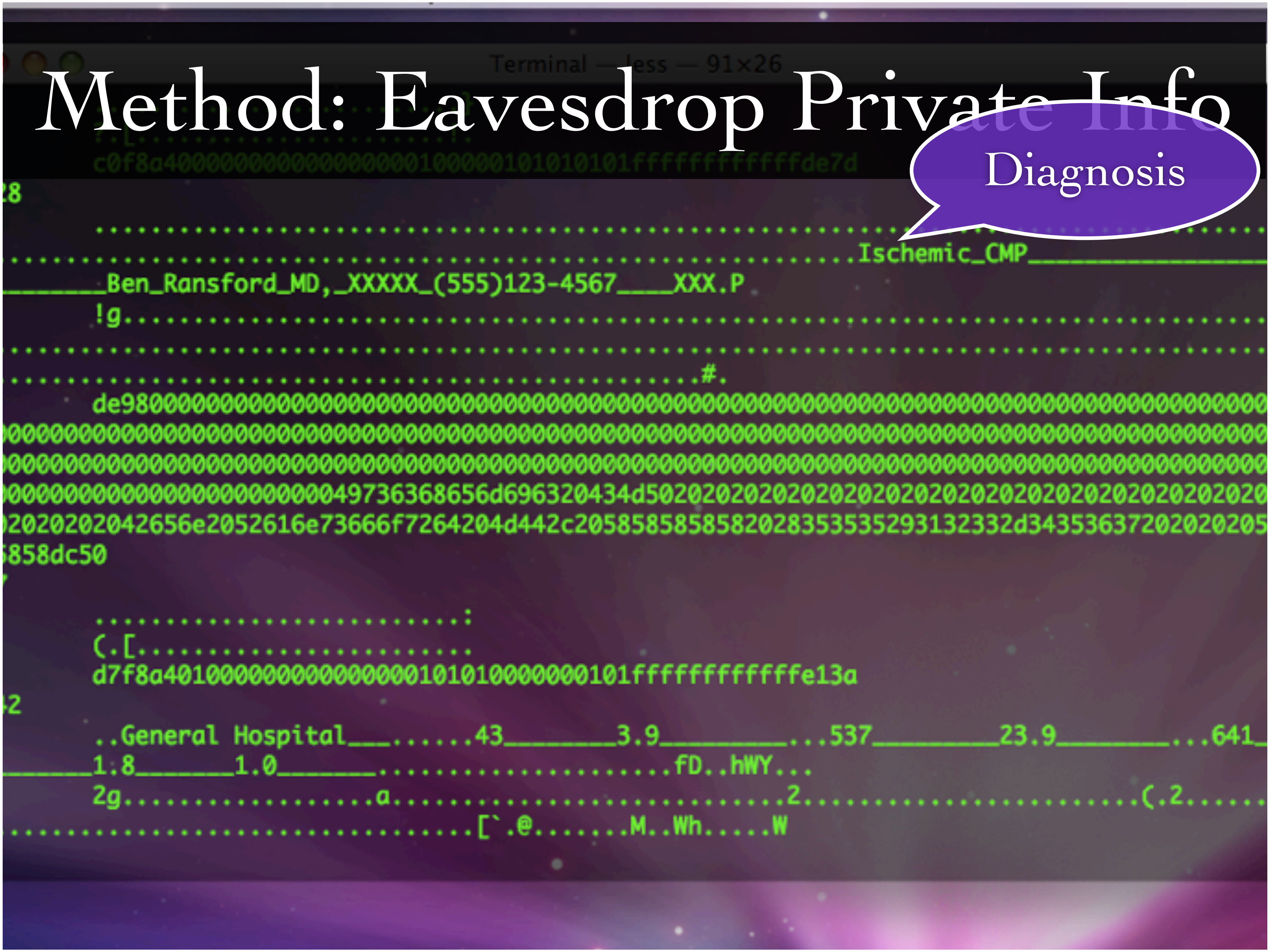
Method: Eavesdrop Private Info



```
       ?.[.........................!.
       c0f8a40000000000000000000100000101010101fffffffffffde7d
28
       ....................................................................................
.............................................................Ischemic_CMP_________________
_______Ben_Ransford_MD,_XXXXX_(555)123-4567____XXX.P
       !g..................................................................................
...........................................................................................
..................................................#.
       de9800000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000049736368656d696320434d5020202020202020202020202020202020202020202020
02020202042656e2052616e73666f7264204d442c2058585858582028353535293132332d34353637202020205
5858dc50

       ...........................:
       (.[........................
       d7f8a4010000000000000001010100000000101ffffffffffffe13a
42
       ..General Hospital___......43________3.9_________...537_________23.9________...641_
______1.8_______1.0_______.....................fD..hWY...
       2g..................a.............................2.........................(.2.....
..................................[`.@.......M..Wh.....W
```

Method: Eavesdrop Private Info



Diagnosis

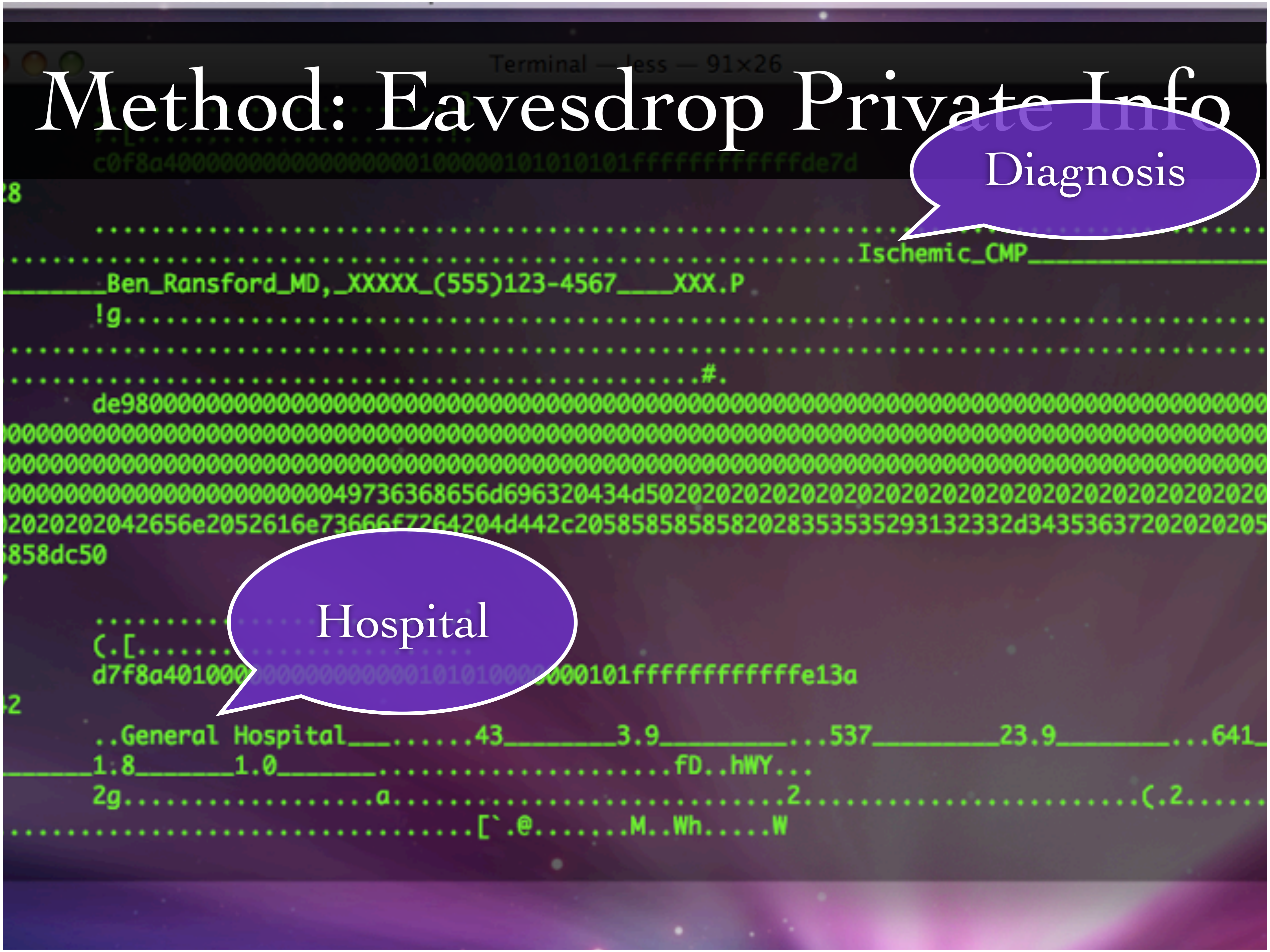
```
        ?.[.............................?.
        c0f8a4000000000000000000001000001010101ffffffffffffde7d
28

        .......................................................................................
.............................................................................Ischemic_CMP______________________
________Ben_Ransford_MD,_XXXXX_(555)123-4567_____XXX.P
        !g.......................................................................................
...............................................................................................
...................................................................#.
        de9800000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000049736368656d696320434d502020202020202020202020202020202020202020202020202020
2020202042656e2052616e73666f7264204d442c2058585858582028353535293132332d34353637202020205
5858dc50
7

        ..............................:
        (.[............................
        d7f8a401000000000000000001010100000000101fffffffffffe13a
42

        ..General Hospital___......43_________3.9__________...537__________23.9_________...641_
_______1.8________1.0________.......................fD..hWY...
        2g...................a.............................2.........................(.2......
....................................[`.@.......M..Wh.....W
```

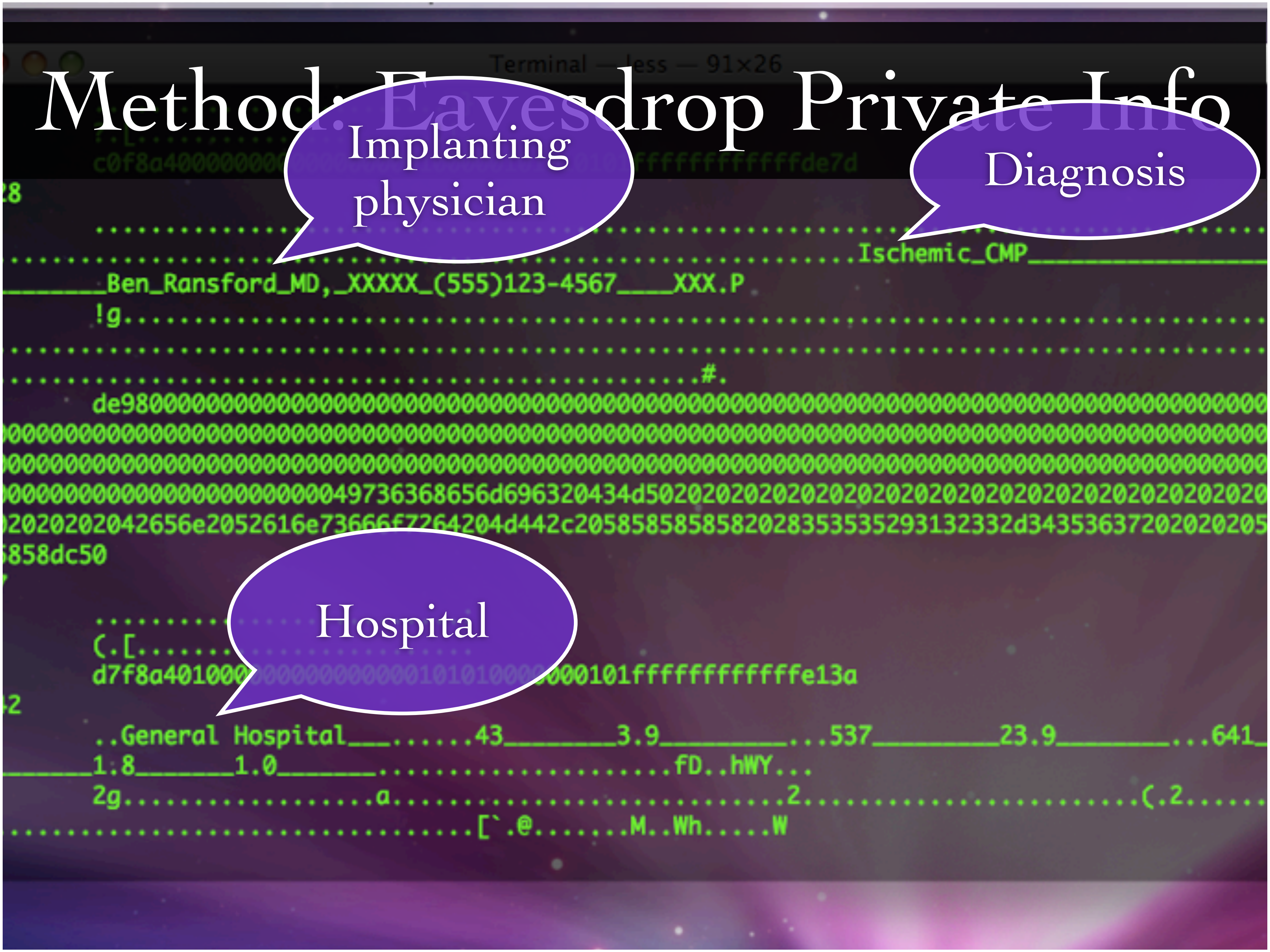
Method: Eavesdrop Private Info



```
         ?.[............................!.
         c0f8a4000000000000000000001000001010101ffffffffffffde7d
28
         ...........................................................................................
.........................................................................Ischemic_CMP__________________
________Ben_Ransford_MD,_XXXXX_(555)123-4567____XXX.P
         !g........................................................................................
...........................................................................................................
............................................................#.
         de98000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000004973636865 6d696320434d5020202020202020202020202020202020202020202020202020
2020202042656e2052616e73666f7264204d442c2058585858582028353535293132332d34353637202020205
5858dc50
7

         ................
         (.[..........................
         d7f8a40100000000000000000001010100000000101fffffffffffe13a
42
         ..General Hospital___......43_________3.9__________...537__________23.9__________...641_
________1.8________1.0________.......................fD..hWY...
         2g...................a................................2...........................(.2......
.........................................[`.@.......M..Wh.....W
```

Method: Eavesdrop Private Info

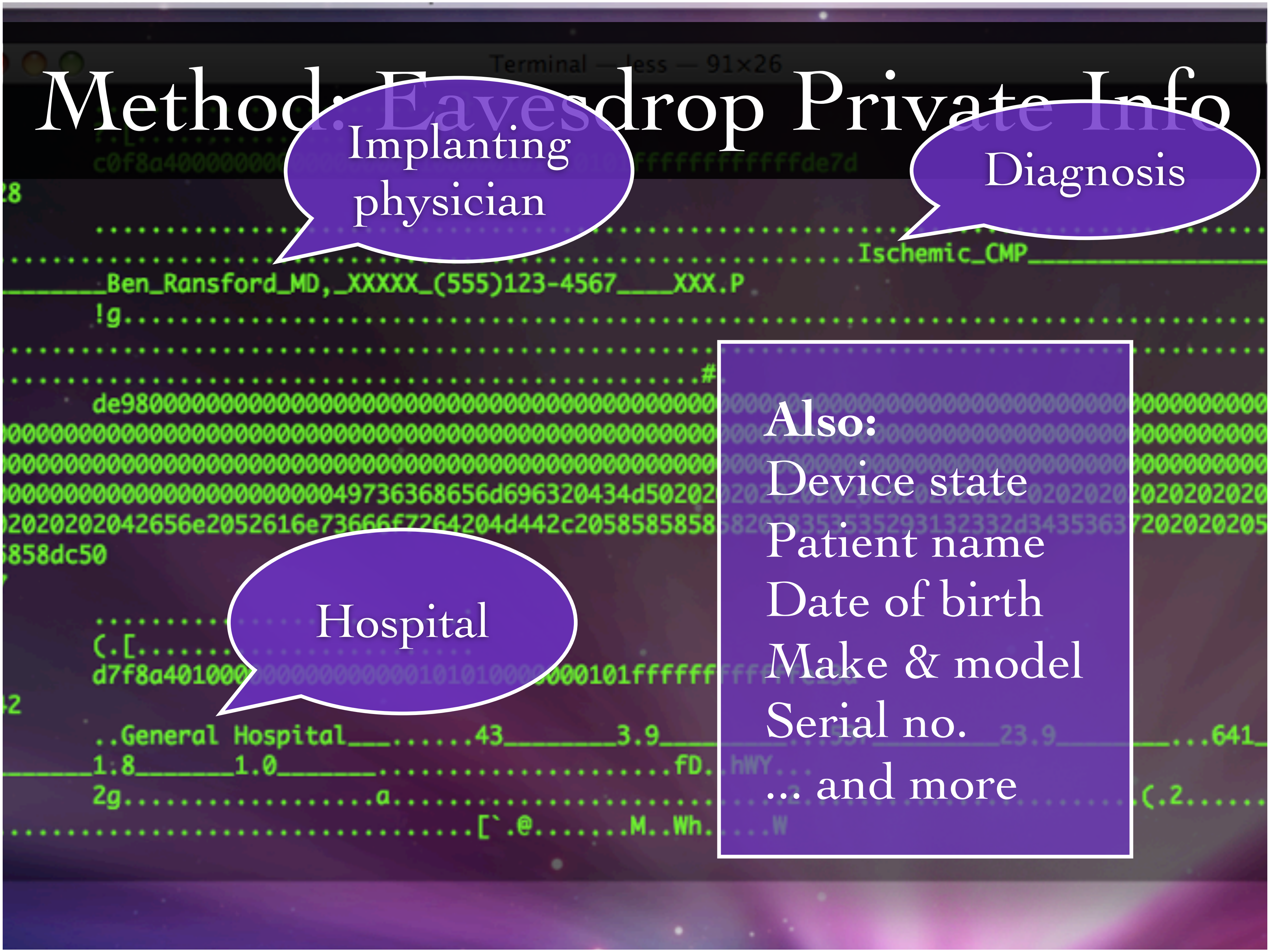


```
         ?.[............
         c0f8a4000000000                     010 ffffffffffffde7d
28

         ................          ..............................................................
.........................................................................Ischemic_CMP__________________
________Ben_Ransford_MD,_XXXXX_(555)123-4567____XXX.P
         !g.........................................................................................
.............................................................................................................
...........................................................#.
         de9800000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000004973636865 6d696320434d502020202020202020202020202020202020202020
2020202042656e2052616e73666f7264204d442c20585858585820283535352931323332d3435363720202020205
5858dc50
7

         .........
         (.[.......
         d7f8a401000000000000000101010000000101ffffffffffffe13a
42
         ..General Hospital___......43________3.9__________...537__________23.9_________...641_
_______1.8_______1.0_______.......................fD..hWY...
         2g....................a..............................2..........................(.2......
...................................[`.@.......M..Wh.....W
```

Method: Eavesdrop Private Info



Implanting physician

Diagnosis

Hospital

```
        ?.[...............
        c0f8a40000000000                              0101ffffffffffde7d
28
        ..................                                     ..........................
.......................   ..........................................Ischemic_CMP______________
________Ben_Ransford_MD,_XXXXX_(555)123-4567____XXX.P
        !g.....................................................................
...........................................................................................
..................................................#
        de98000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000004973636865 6d696320434d50202020202020202020202020202020202020
2020202042656e2052616e73666f7264204d442c205858585858202835353529313233 2d343536372020202
5858dc50
7

        .........
        (.[.......
        d7f8a401000000000000000001010100000000101ffffffffffe2ba
42
        ..General Hospital___......43________3.9___________.....23.9______________...641_
________1.8________1.0________......................fD..hWY...                ..(.2......
        2g...................a.......................................
...............................[`.@.......M..Wh.....W
```

Also:

Device state

Patient name

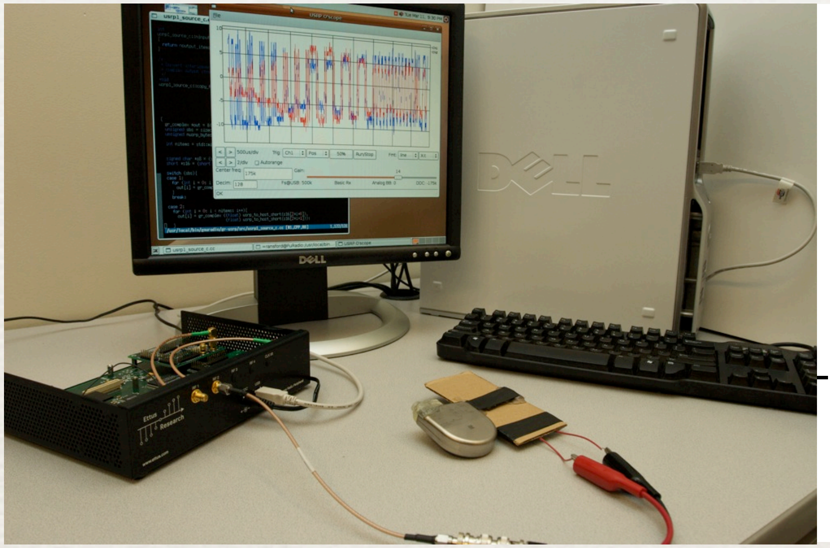
Date of birth

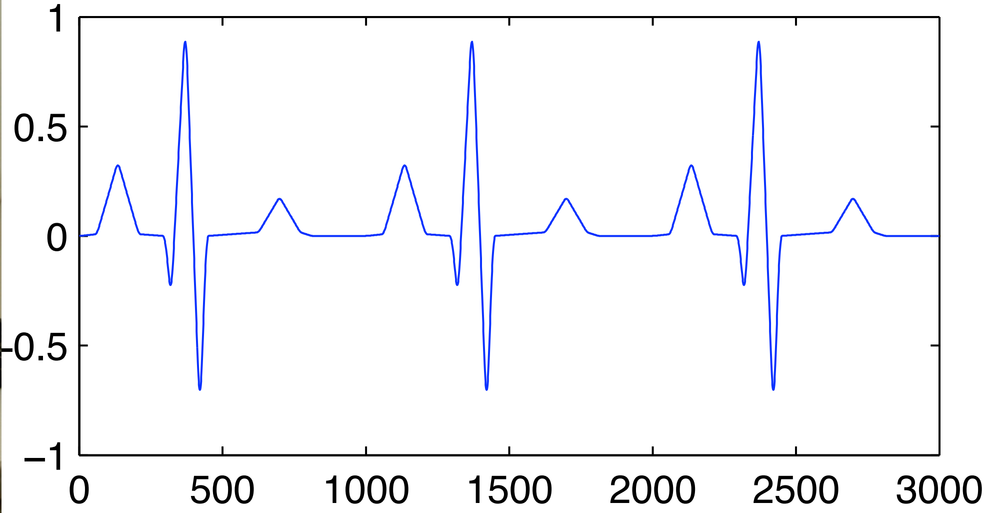
Make & model

Serial no.

... and more

Method: Sniff Vital Signs



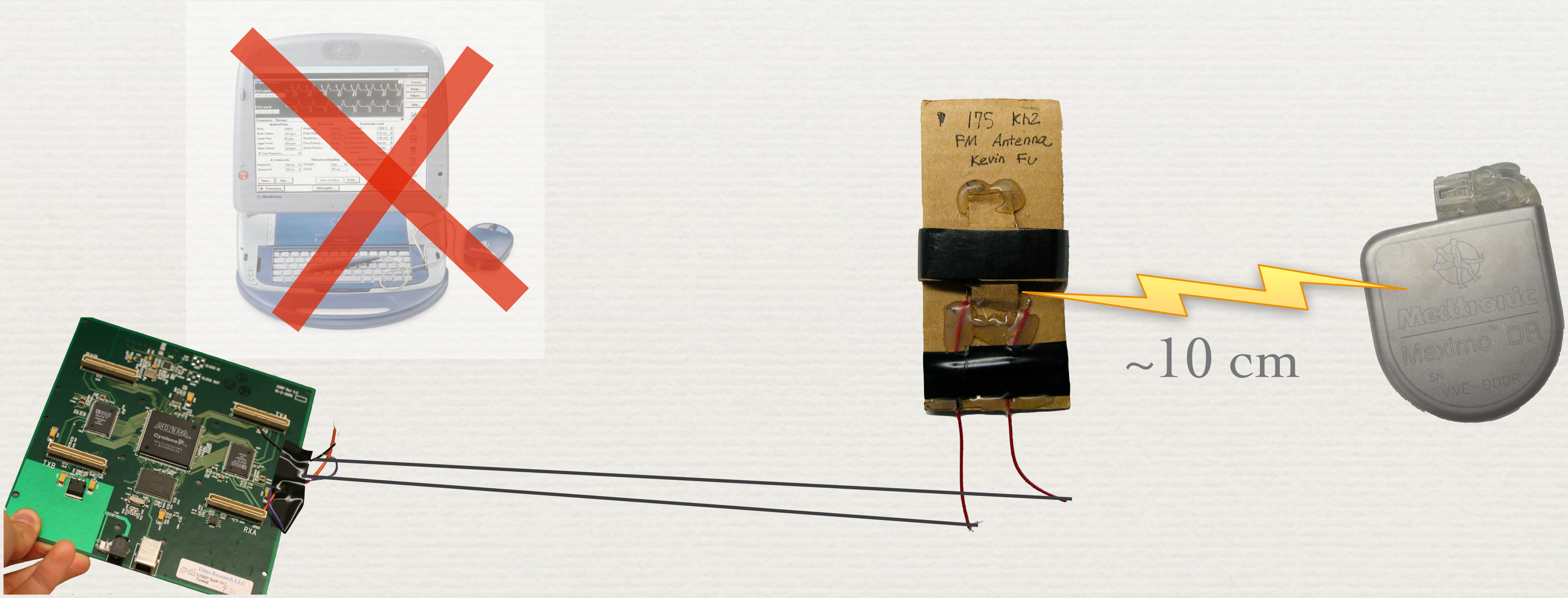


Eavesdropping setup

ICD emits *reconstructible* vital signs

Issue: Vital signs can say plenty.

Replay Traffic

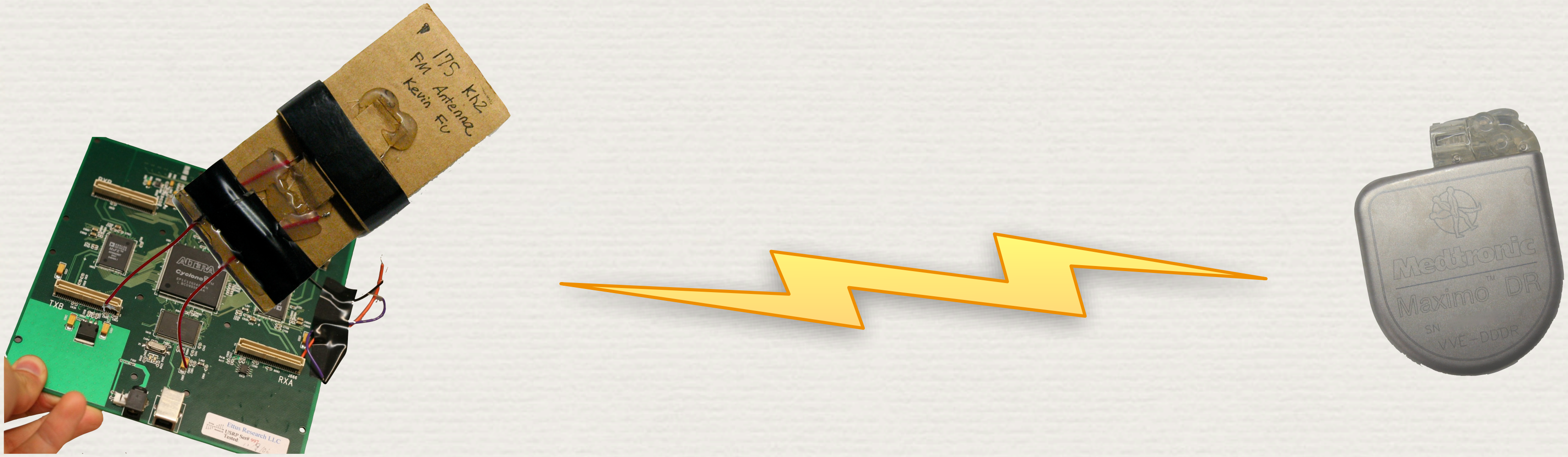


~10 cm

Photo:
Medtronic

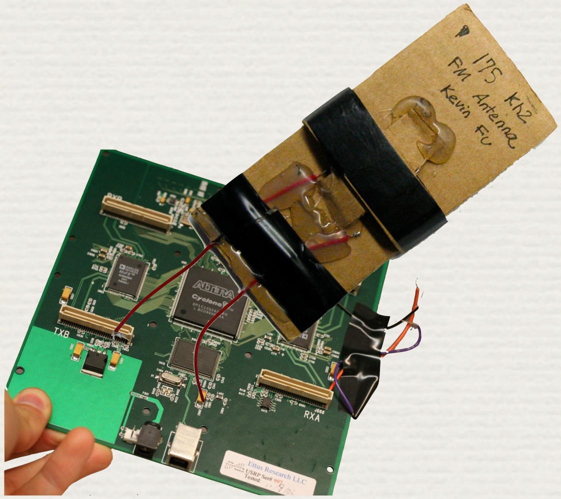
Method: Drain Energy

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

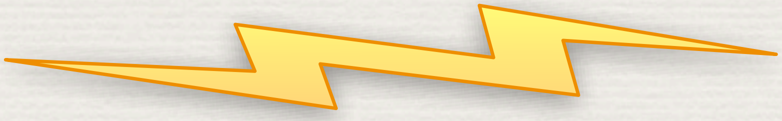


Method: Drain Energy

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

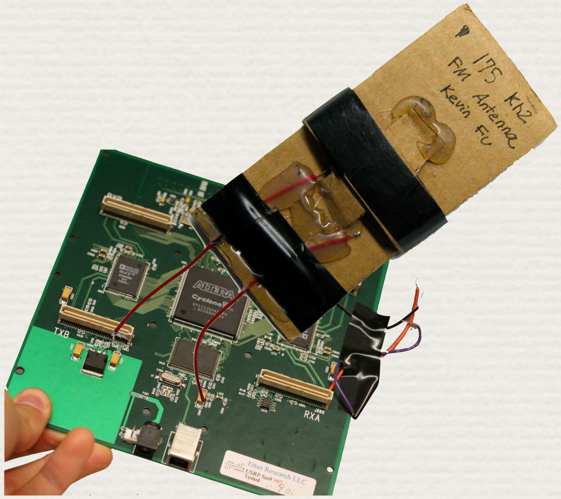


"Are you awake?
Are you awake?"

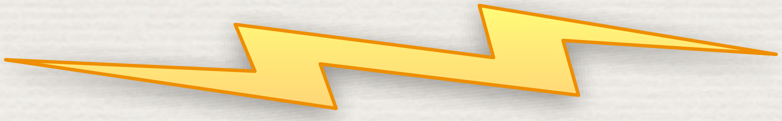


Method: Drain Energy

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

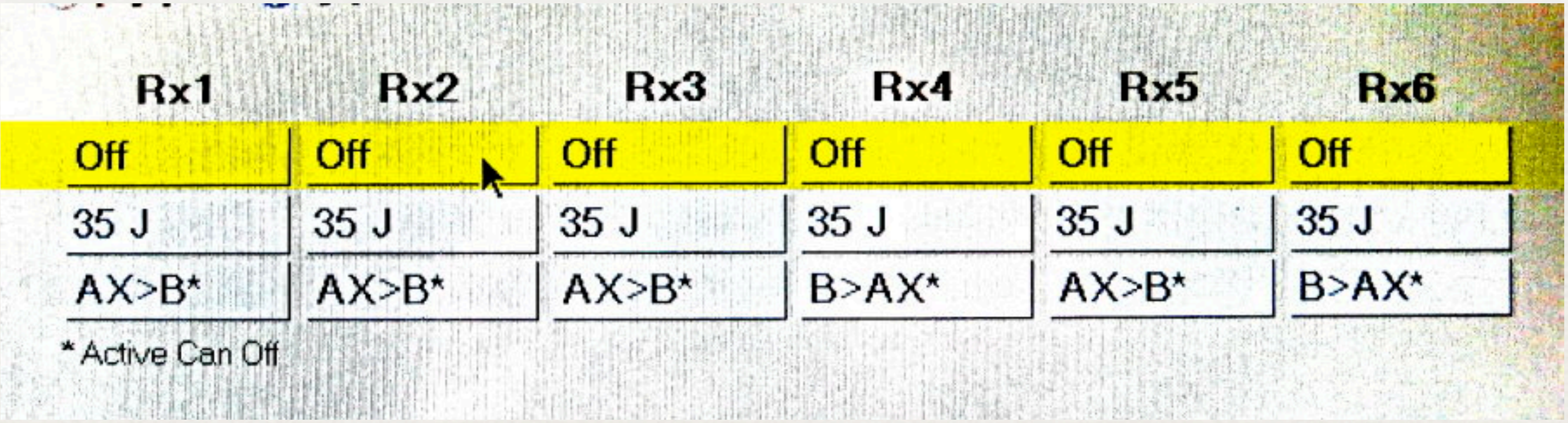


"Are you awake?
Are you awake?"



"Now I am!"

Replay: 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.

Replay: Affect Patient's Physiology

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

BOBBY SMITH, M.D.
You're, I think, probably about ready to test the device for effectiveness. Is that

Issue: Puts patient safety at risk.

Photo: or-live.com

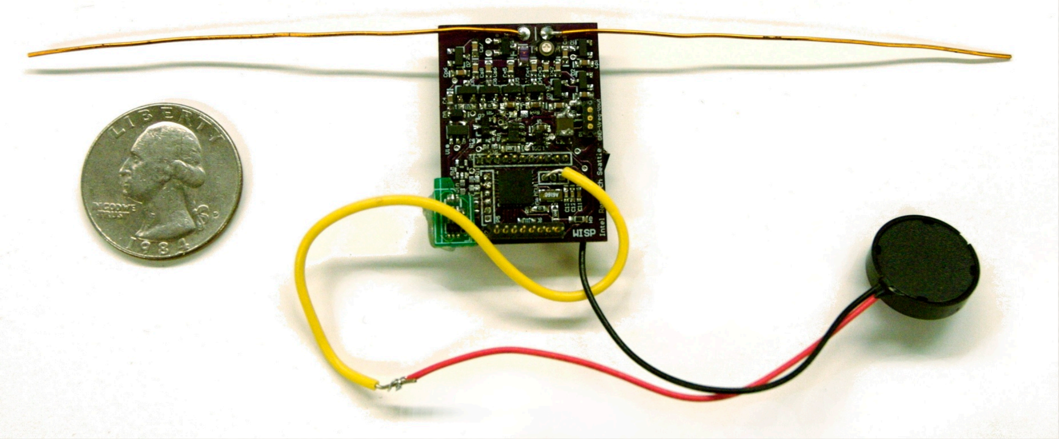
Defensive Direction: Zero-Power

(No time today. Google for "pacemaker 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**

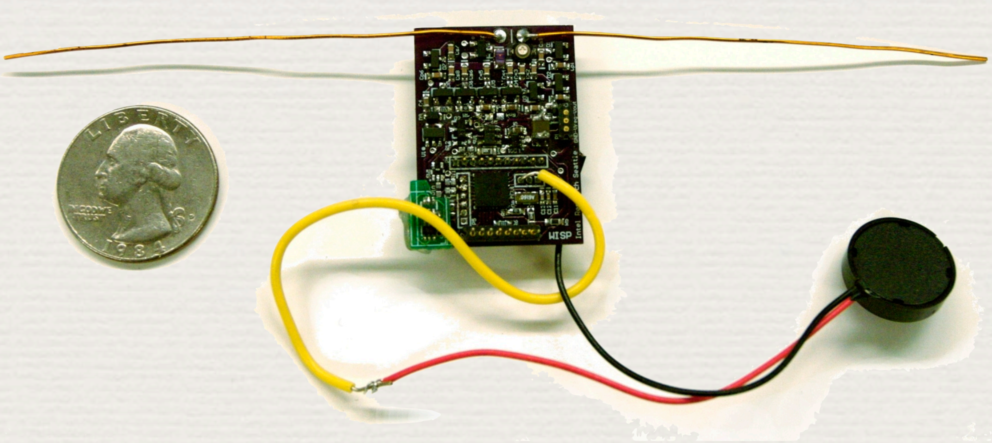
Prototype defenses against **some** of the attacks.



Main idea: defend without using battery.

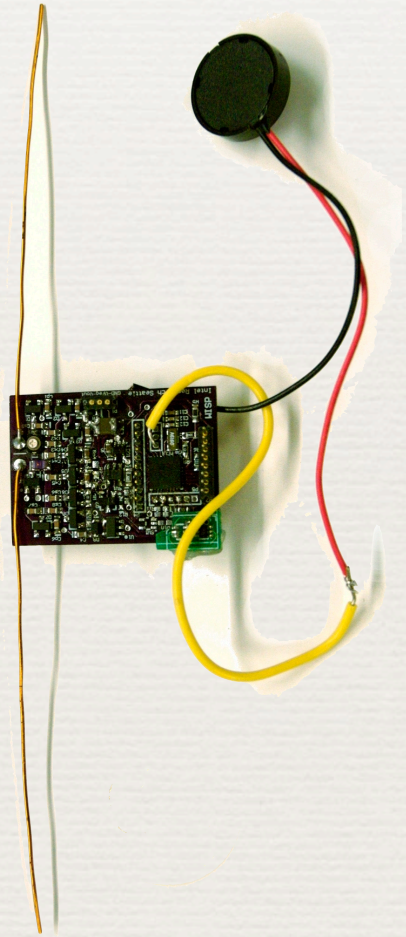
B.Y.O.P.

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

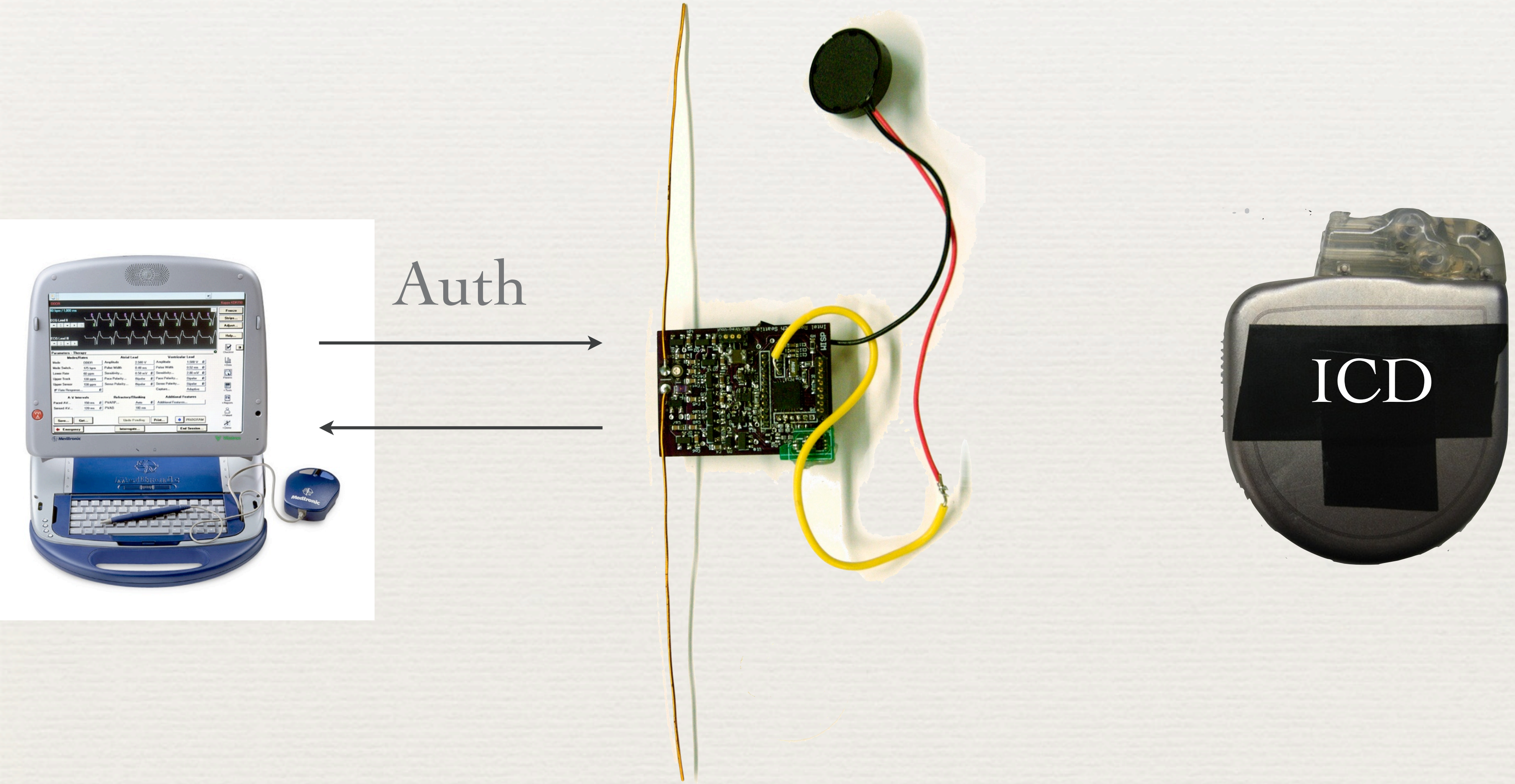


Goal: External party pays for power.

Patient notification

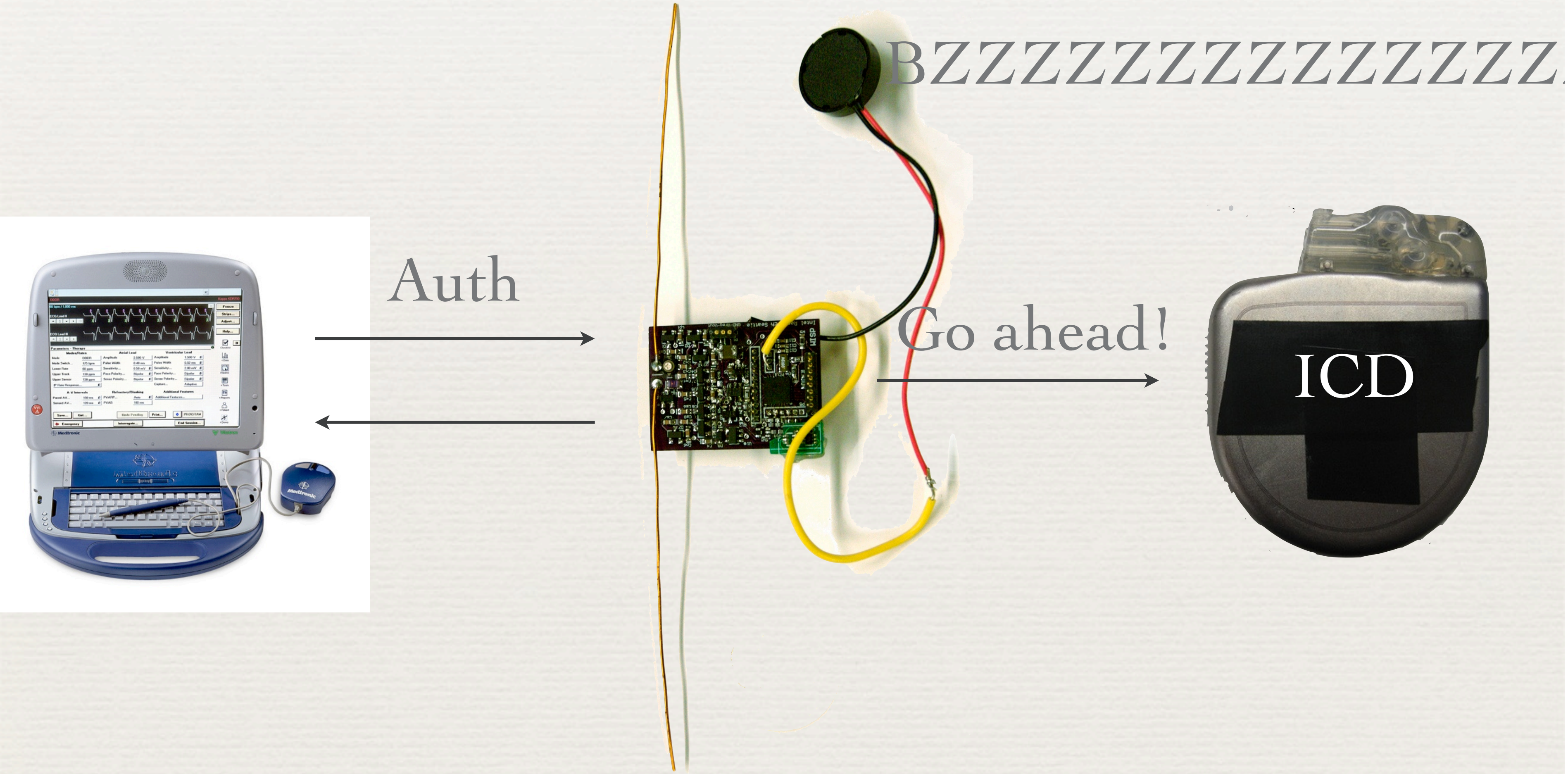


Patient notification



Auth

Patient notification

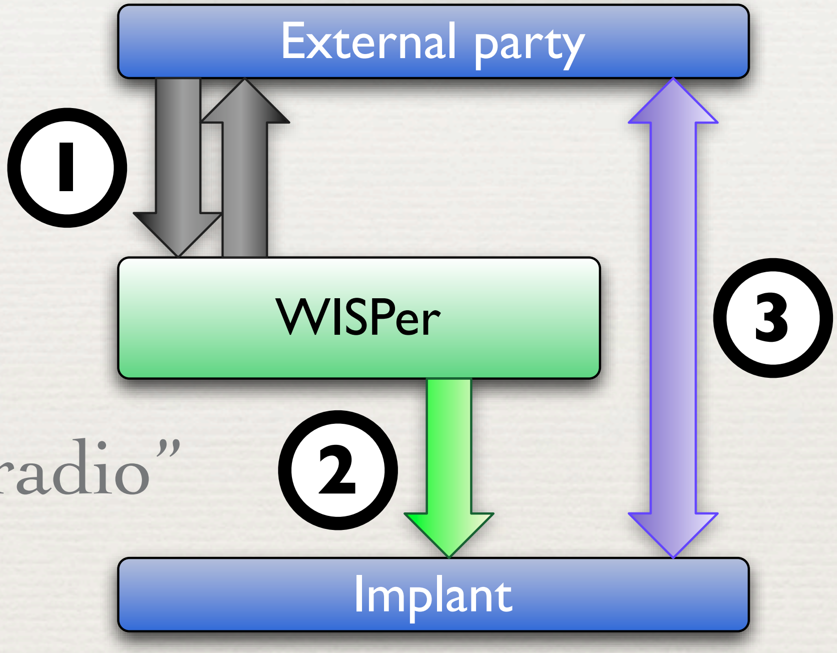


BZZZZZZZZZZZZZZ

Auth

Go ahead!

WISPer as Gatekeeper

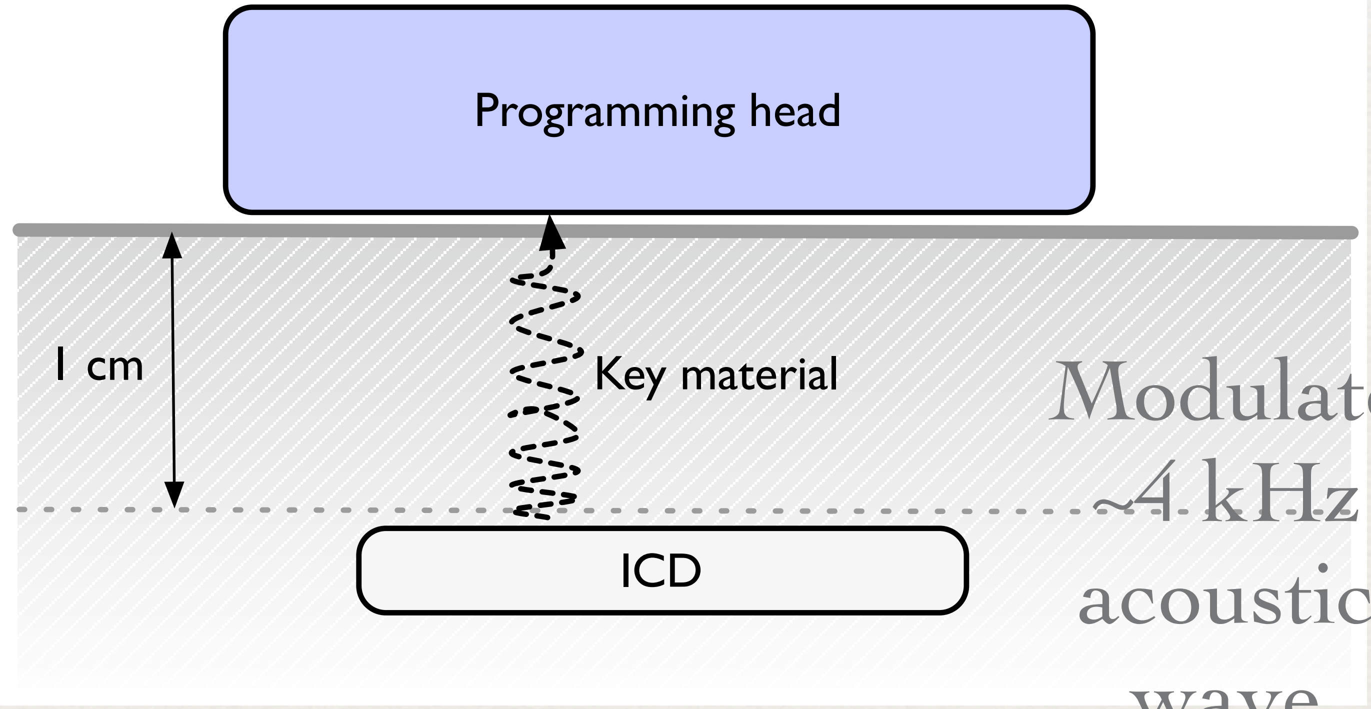


- Authenticate against WISPer
- WISPer to ICD: “OK to use radio”
- Acoustic patient notification
- How to deter enemies? (Open question!)

Sensible key exchange

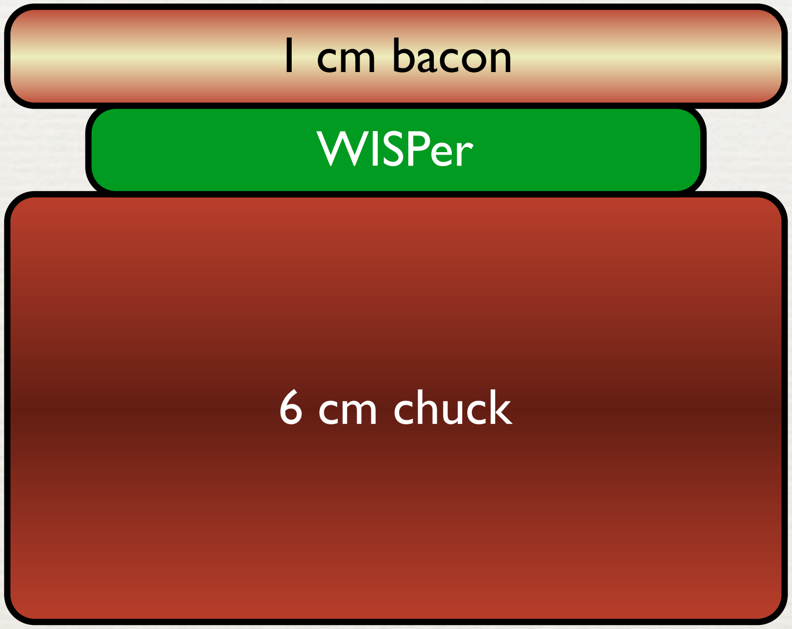
- Session setup

Tissue



Modulate ~4 kHz acoustic wave

Testing WISPer: Simulated Torso



I cm bacon

WISPer

6 cm chuck

Energy harvesting through tissue is possible.

How WISPer Could Work

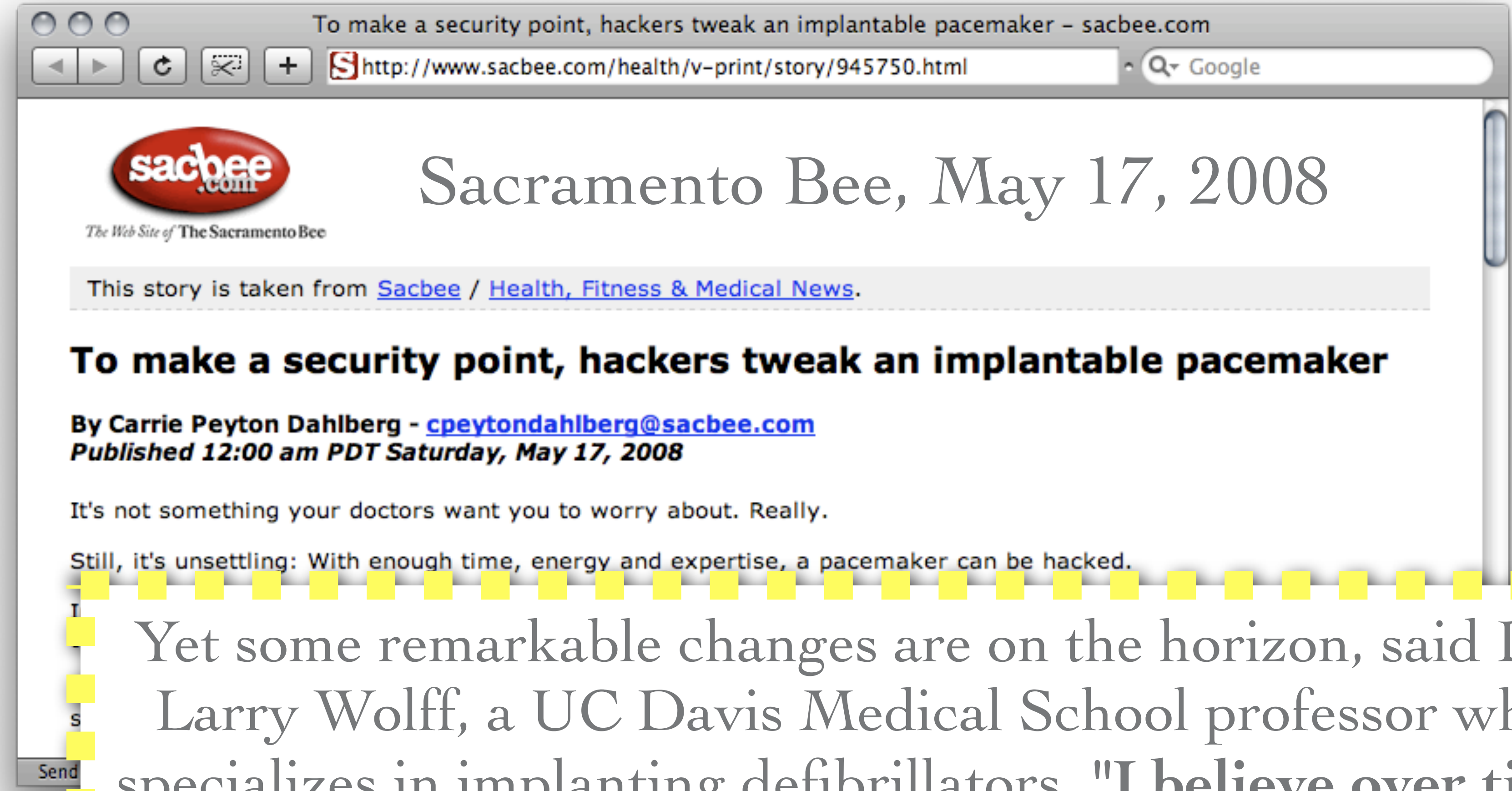
- Auxiliary device (possibly integrated)
- Audible or tactile patient alert
- Patient detects activity: am I in a clinic?
- Fail open: **sensible**, tactile key exchange

IMDs+Wireless+Internet:

The Future

(Condensed version of the future. Ask Kevin for details.)

Future Home Care


To make a security point, hackers tweak an implantable pacemaker – sacbee.com
http://www.sacbee.com/health/v-print/story/945750.html
Google
sacbee.com
The Web Site of The Sacramento Bee
Send

Sacramento Bee, May 17, 2008

This story is taken from Sacbee / Health, Fitness & Medical News.

To make a security point, hackers tweak an implantable pacemaker

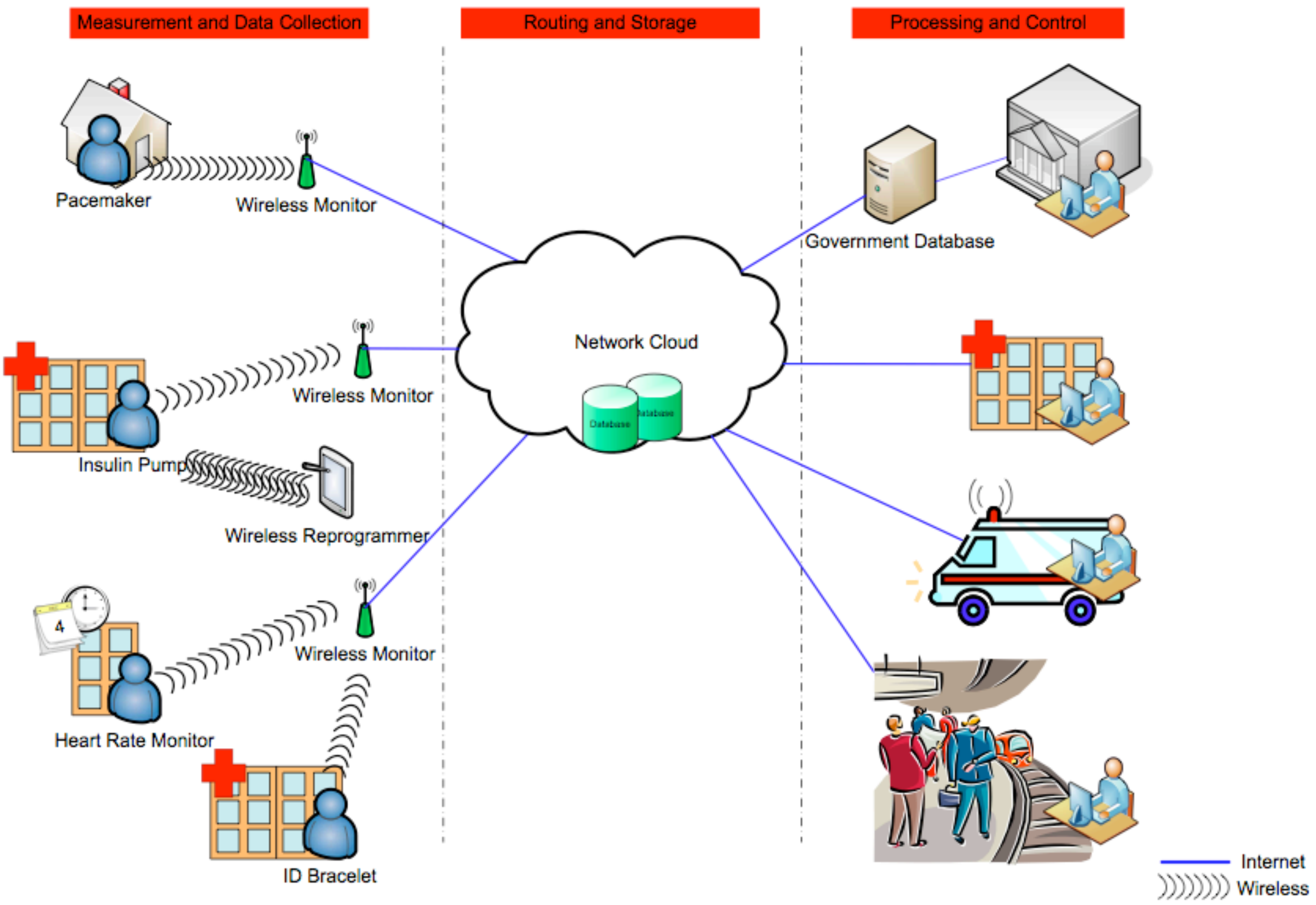
By Carrie Peyton Dahlberg - cpeytondahlberg@sacbee.com
Published 12:00 am PDT Saturday, May 17, 2008

It's not something your doctors want you to worry about. Really.

Still, it's unsettling: With enough time, energy and expertise, a pacemaker can be hacked.

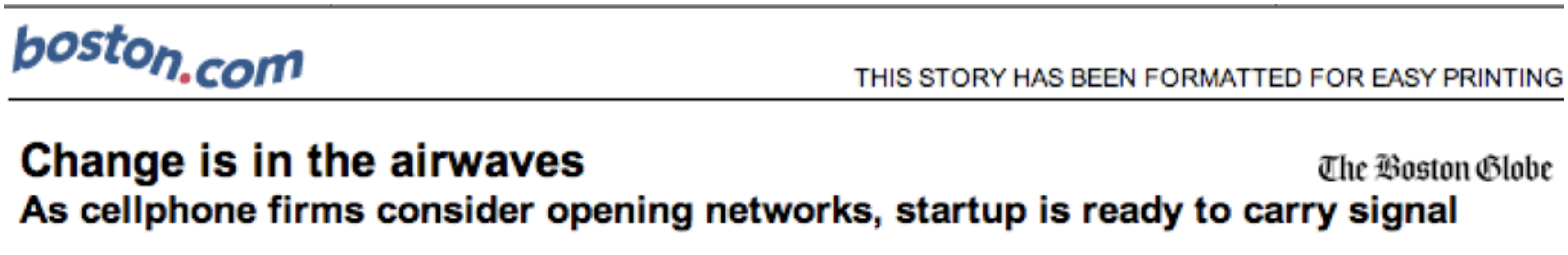
Yet some remarkable changes are on the horizon, said Dr. Larry Wolff, a UC Davis Medical School professor who specializes in implanting defibrillators. **"I believe over time we could make programming changes on the telephone,"** he said, although that's not possible now.

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

Medical Device Trends

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

Issue: All of these bring risks.

Summary of IMD Sec. & Priv.

- Risks today: Unintentional interference
  - Radio interference
  - Threats: Metal detectors, accidents, misidentification
- Future risks: Intentional interference
  - Threats from wireless and Internet connectivity
  - 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)

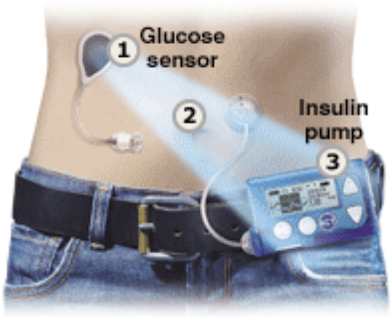
IMD Response Time

Storage Constraints

Battery Life

Wireless + Internet Can Improve Healthcare

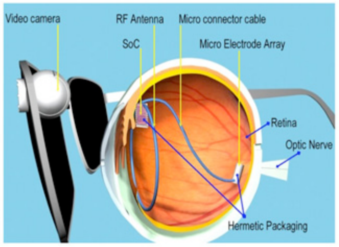
But not without fully understanding security and privacy



Insulin pump

Artificial pancreas

Neurostimulators



Artificial vision

Obesity control

Programmable Vasectomy

Extra slides

- Google us for more information.