Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses

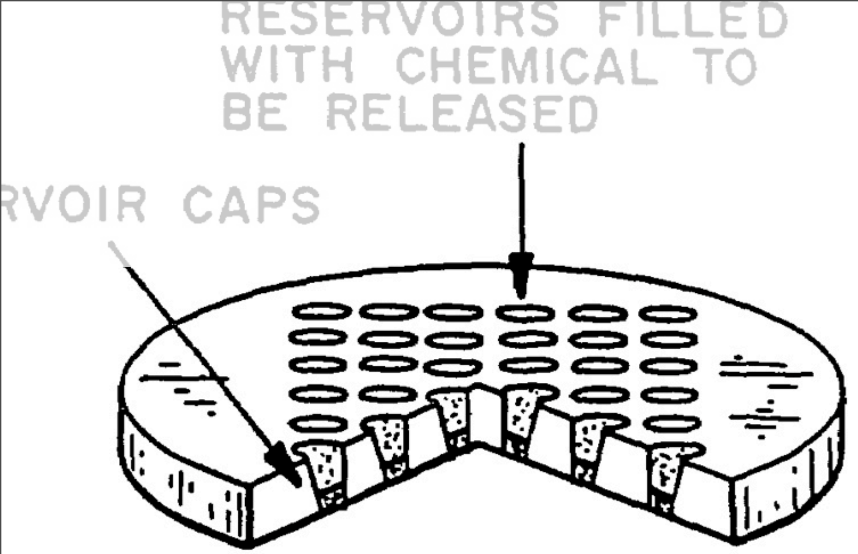
Ben Ransford
ransford@cs.umass.edu

U. Washington:
D. Halperin
T. Kohno

UMass Amherst:
T. S. Heydt-Benjamin
S. Clark B. Defend
W. Morgan K. Fu

BIDMC/ Harvard:
W. H. Maisel, MD

http://secure-medicine.org/



Pharmacy on a chip

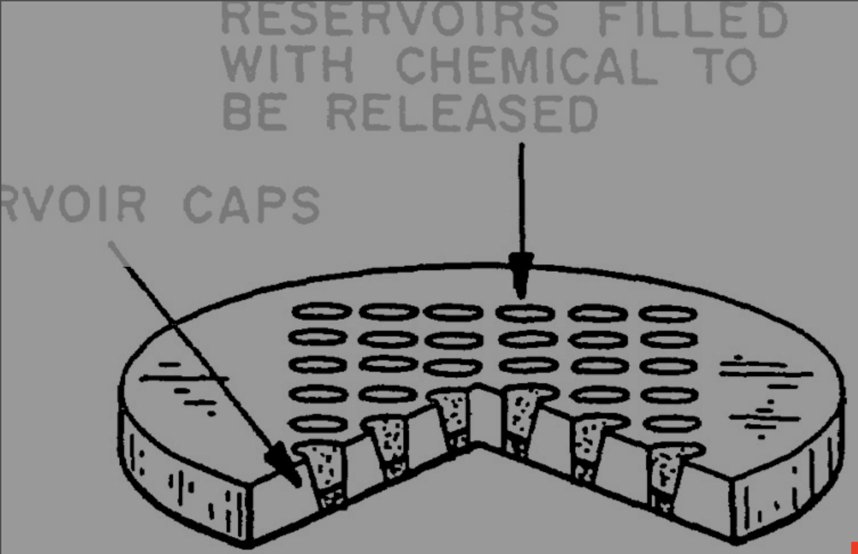
Neurostimulator

Cardiac Device

Drug pump

Prosthetic limb

Photos: Medtronic, Hearing Loss Assoc. of WA, St. Jude Medical, Otto Bock



Pharmacy on a chip

Neurostimulator

Cardiac Device

Drug pump

Prosthetic limb

Photos: Medtronic, Hearing Loss Assoc. of WA, St. Jude Medical, Otto Bock

Why Care About IMDs?

- Common devices
- Sophisticated devices with radios
- Perform vital functions inside people
- Are they secure?

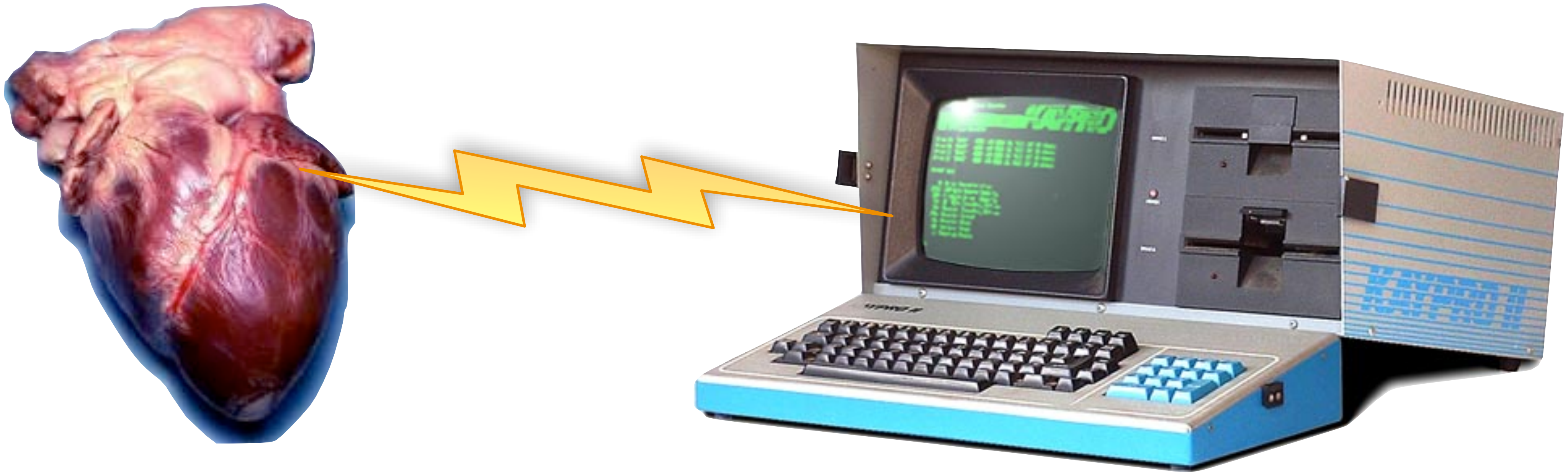
Trends in Cardiac Devices

Implantable defibrillator, 2003

- Complex therapies
- Radio interfaces
- Monitoring over Internet
- Algorithms for problem detection
- More storage, better CPU, ...

An Implanted Computer

... which is wirelessly reprogrammable
... and contains personal data.



1990–2002: ~2.6 million (US) [JAMA 2006]

Photos: oldcomputers.net, Wikipedia ("Heart")

Contributions

- Study of a real implantable device
- Attacks with software radio
- Prototype energy harvesting defenses

The Next 20 Minutes

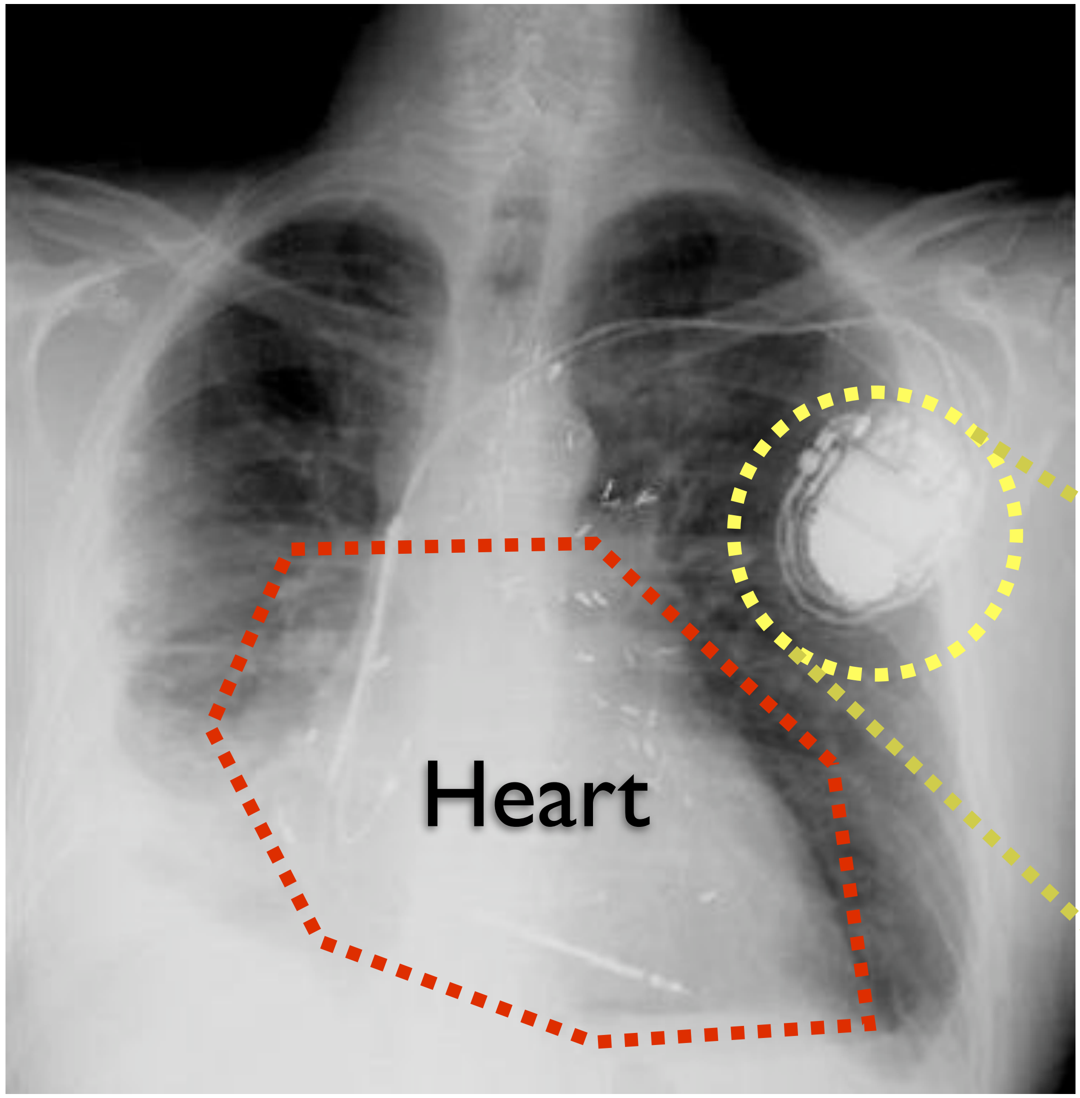
1. How secure is a real device?

2. Why is this non-trivial to get right?

3. Where should we go from here?

#1: Analysis of a Real Device

We analyzed an **ICD.**



- **I**mplantable
  Cardiac
  Defibrillator
- Related to pacemaker
- Large shock: resync heart
- Monitors heart waveforms

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

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

Attack #1: Steal Device Programmer

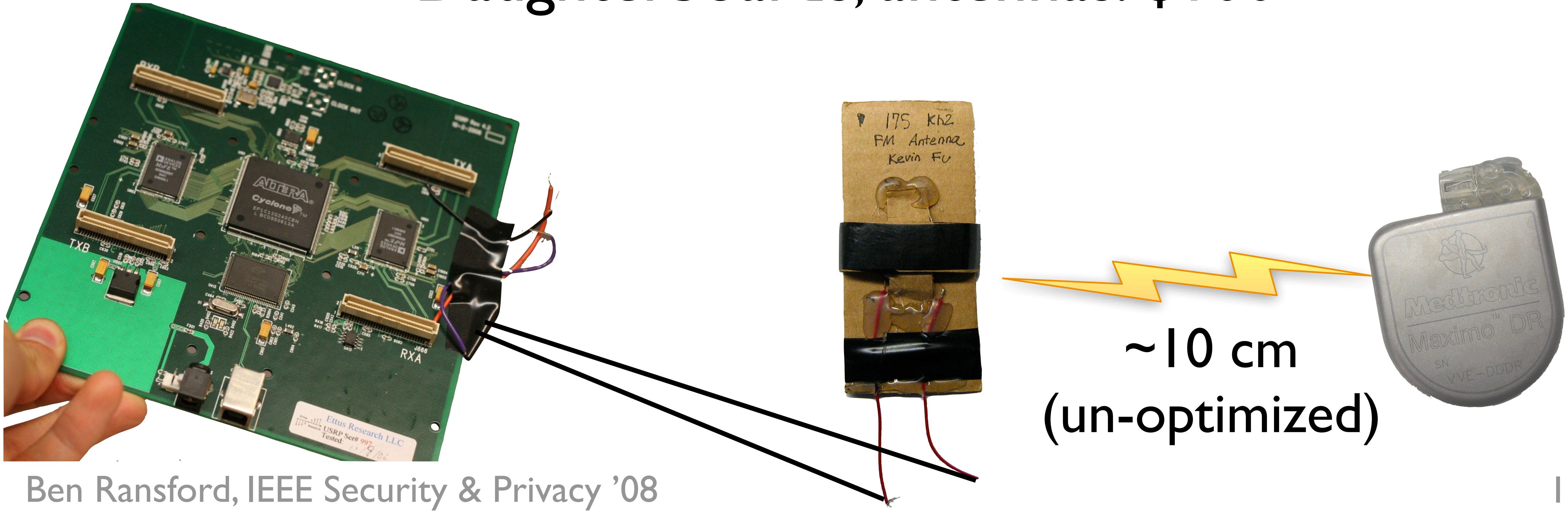
- **Insider attack**
- Thief can reverse engineer, modify...
- Risk: get “root” on many implants

Issue: ICD’s trusted computing base is large.

Photo: Medtronic

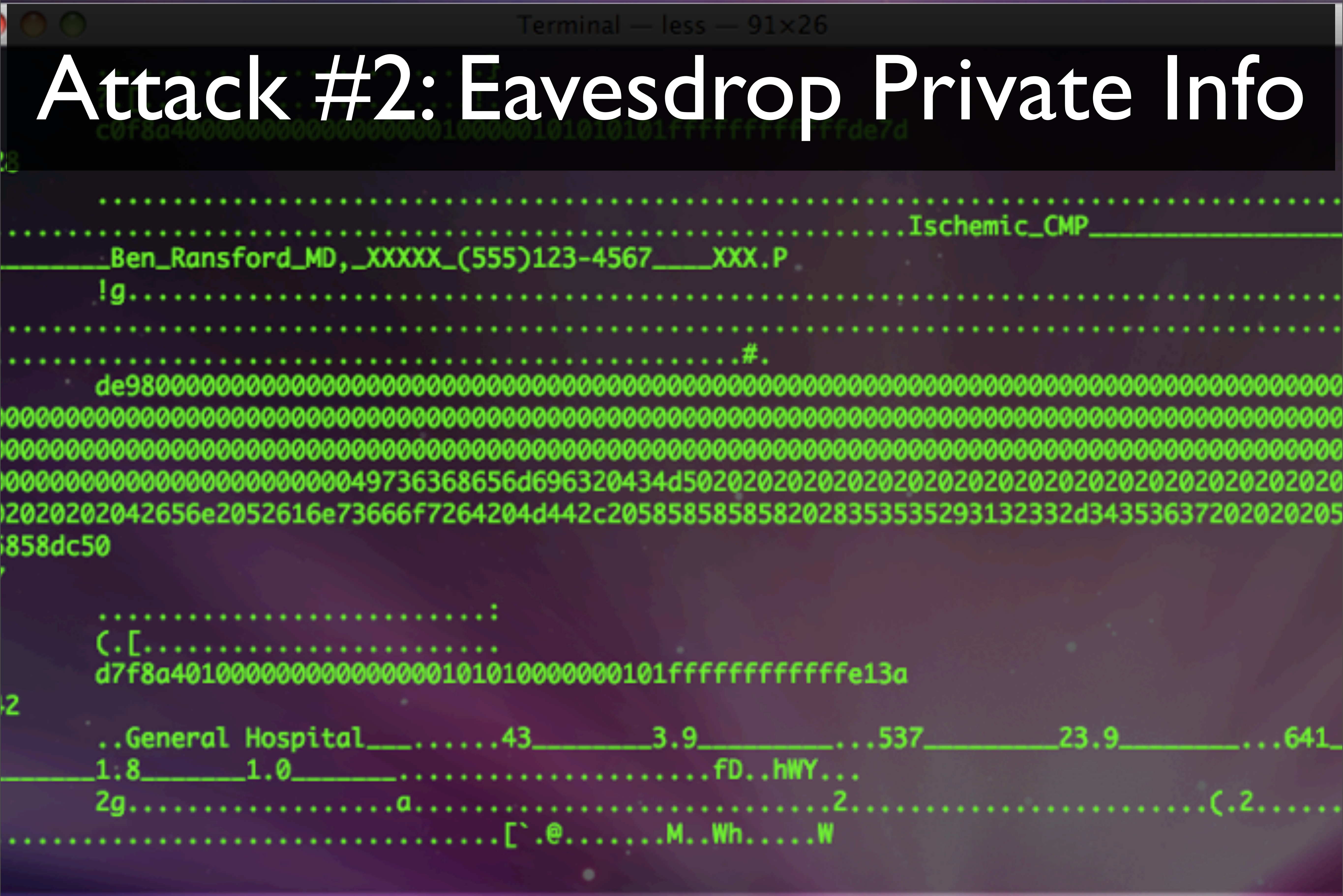
Why Steal When You Can Build?

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



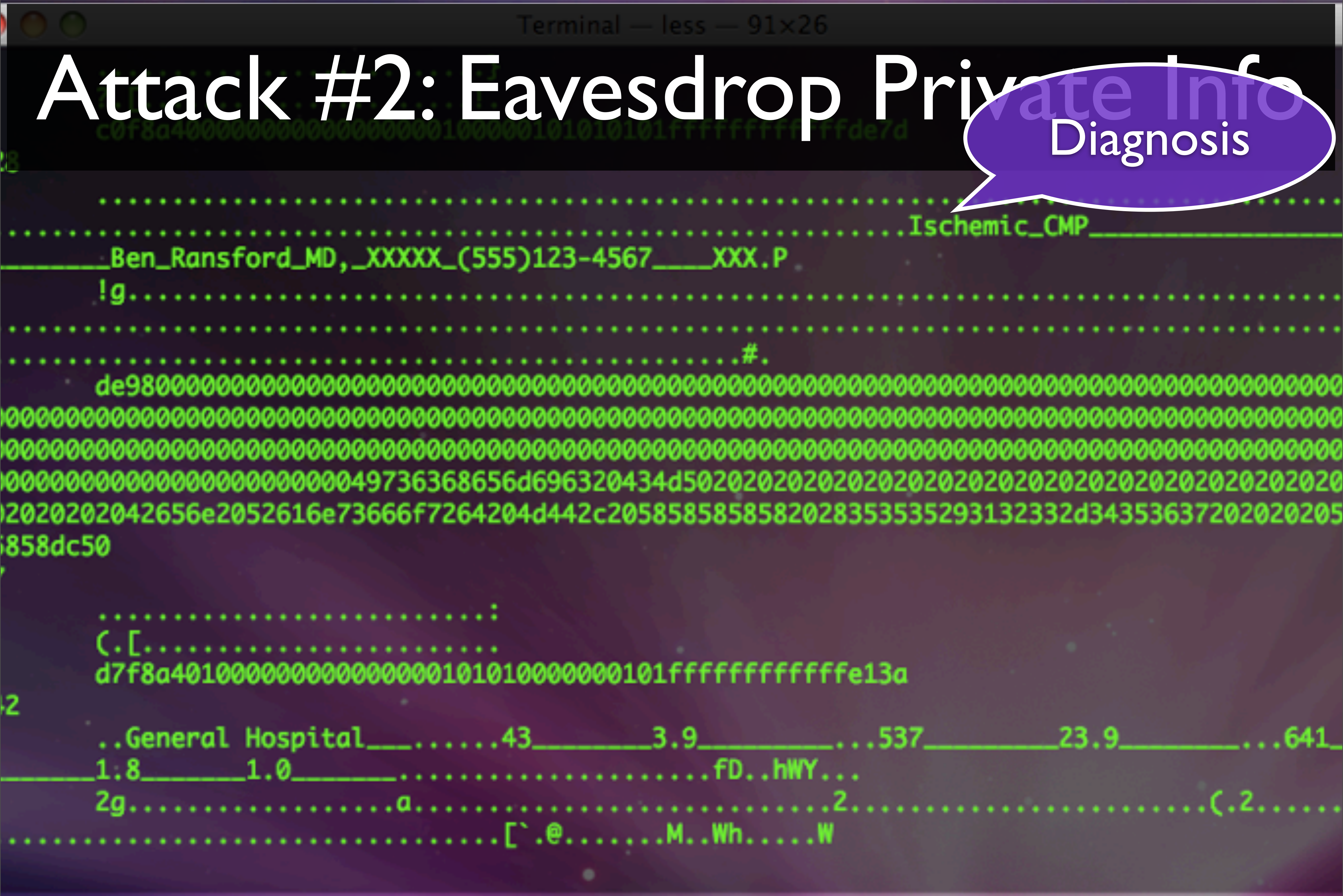
~10 cm
(un-optimized)

Attack #2: Eavesdrop Private Info



```
8
        ......................................................................
.................................................................Ischemic_CMP_______________
_______Ben_Ransford_MD,_XXXXX_(555)123-4567____XXX.P
        !g................................................................
..........................................................................
.....................................................#.
        de98000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000049736368656d696320434d502020202020202020202020202020202020202020
202020202042656e2052616e73666f7264204d442c2058585858582028353535293132332d34353637202020205
858dc50

        ..........................:
        (.[.......................
        d7f8a4010000000000000000001010100000000101ffffffffffe13a
2
        ..General Hospital___......43_______3.9_________...537________23.9________...641_
______1.8______1.0_______......................fD..hWY...
        2g..................a..........................2......................(.2.....
...............................[`.@.......M..Wh.....W
```

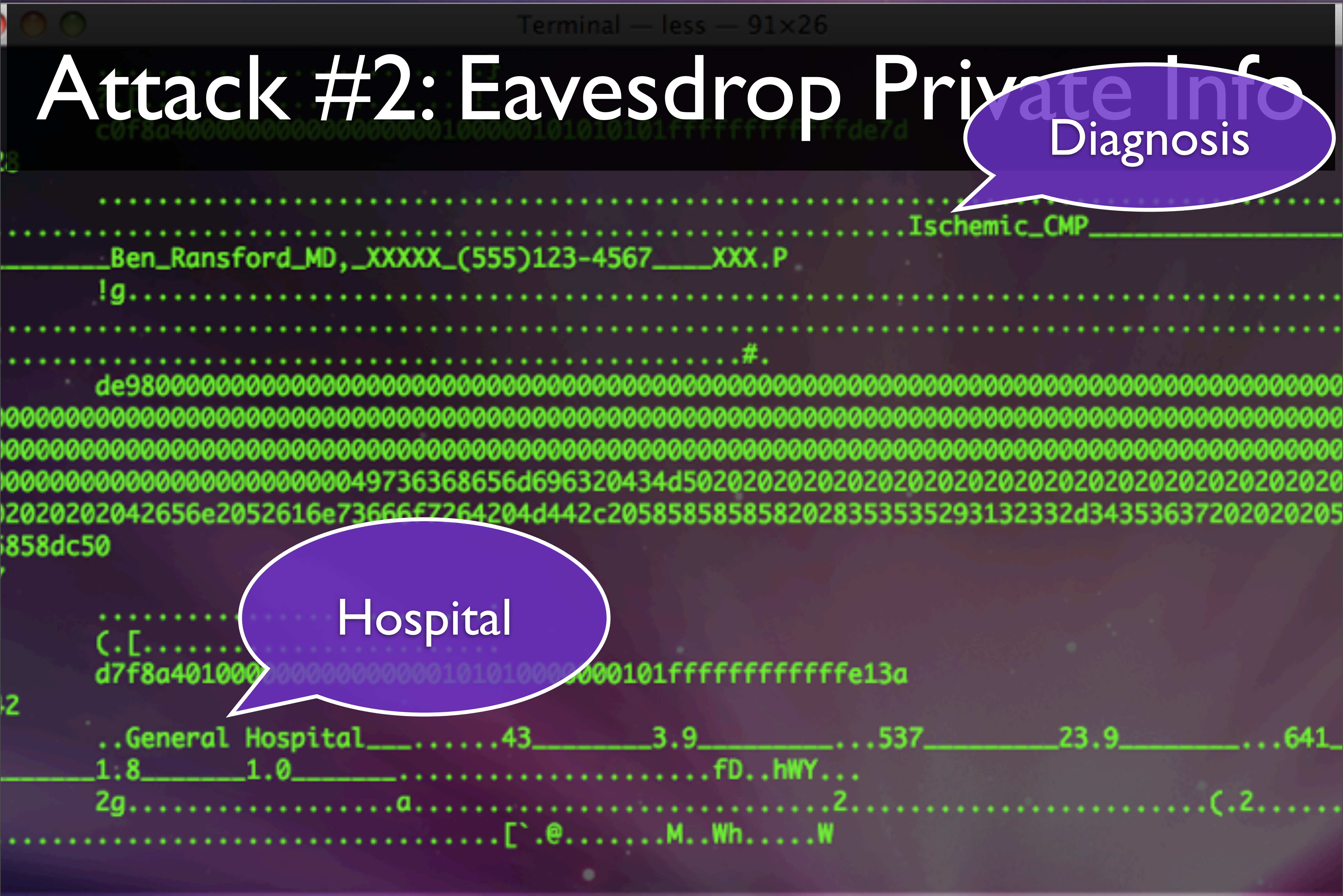
Attack #2: Eavesdrop Private Info



```
      c0f8a400000000000000000001000001010101fffffffffffde7d
28

      ....................................................................................
.............................................................Ischemic_CMP_________________
_______Ben_Ransford_MD,_XXXXX_(555)123-4567____XXX.P
      !g..................................................................................
...........................................................................................
..................................................#.
      de98000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000049736368656d696320434d50202020202020202020202020202020202020202020
2020202042656e2052616e73666f7264204d442c2058585858582028353535293132332d3435363720202020205
858dc50
/

      ...........................:
      (.[.........................
      d7f8a401000000000000000001010100000000101ffffffffffffe13a
2

      ..General Hospital___......43________3.9__________...537__________23.9_________...641_
______1.8_______1.0_______.........................fD..hWY...
      2g..................a..........................2.......................(.2.....
.................................[`.@.......M..Wh.....W
```

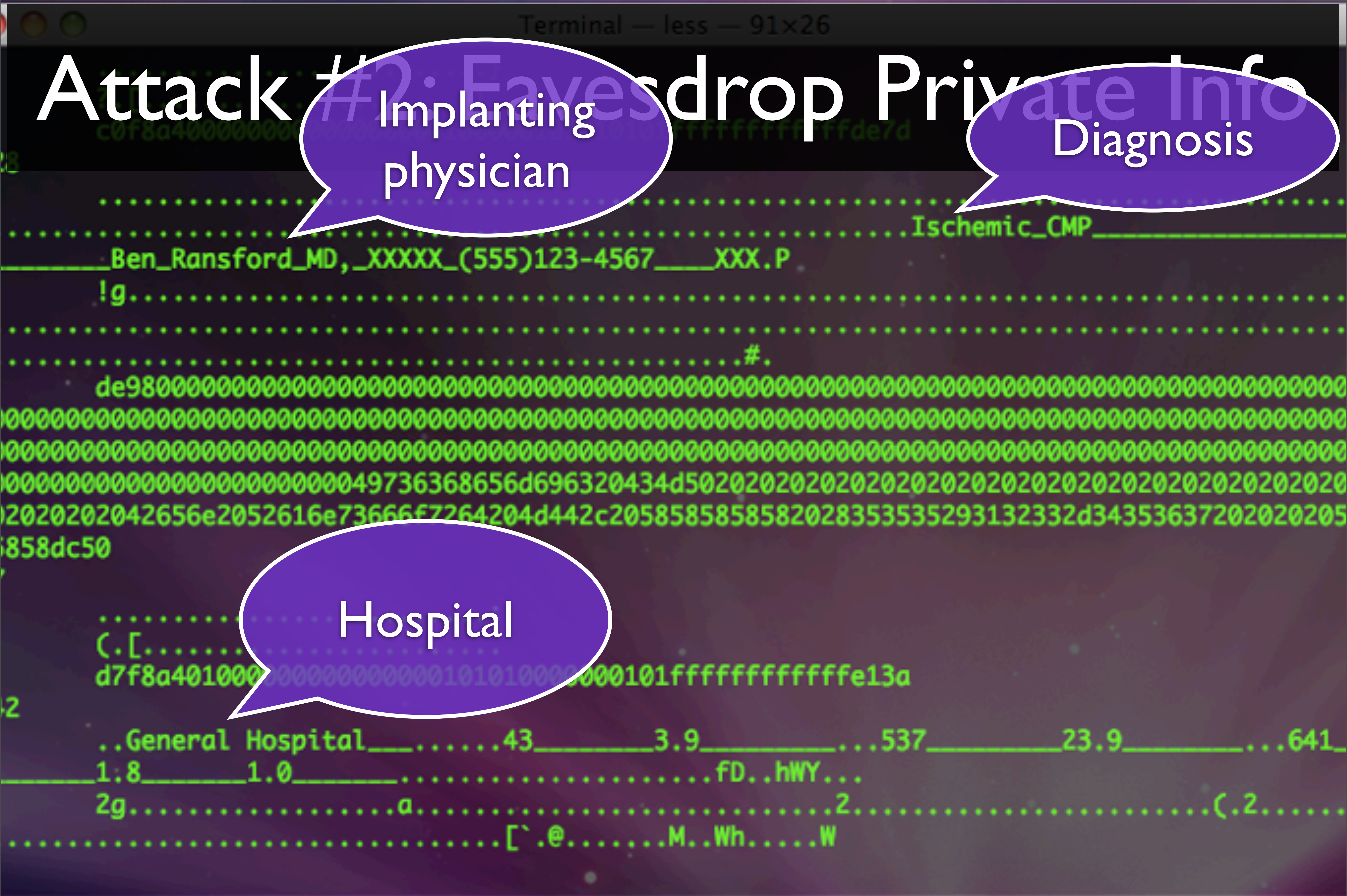
Diagnosis

Attack #2: Eavesdrop Private Info



```
      c0f8a40000000000000000000100000101010101ffffffffffffde7d
28

      .....................................................................................
..............................................................Ischemic_CMP_________________
_______Ben_Ransford_MD,_XXXXX_(555)123-4567____XXX.P
      !g...............................................................................
.......................................................................................
..................................................#.
      de9800000000000000000000000000000000000000000000000000000000000000000de9800000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000049736368656d696320434d50202020202020202020202020202020202020202020
2020202042656e2052616e73666f7264204d442c2058585858582028353535293132332d34353637202020205
858dc50
/

      ..............................
      (.[.......................
      d7f8a4010000000000000000000101010000000101ffffffffffffe13a
2
      ..General Hospital___......43________3.9_________...537_________23.9_________...641_
______1.8_______1.0_______........................fD..hWY...
      2g...................a............................2........................(.2......
..................................[`.@.......M..Wh.....W
```

Attack #2: Eavesdrop Private Info



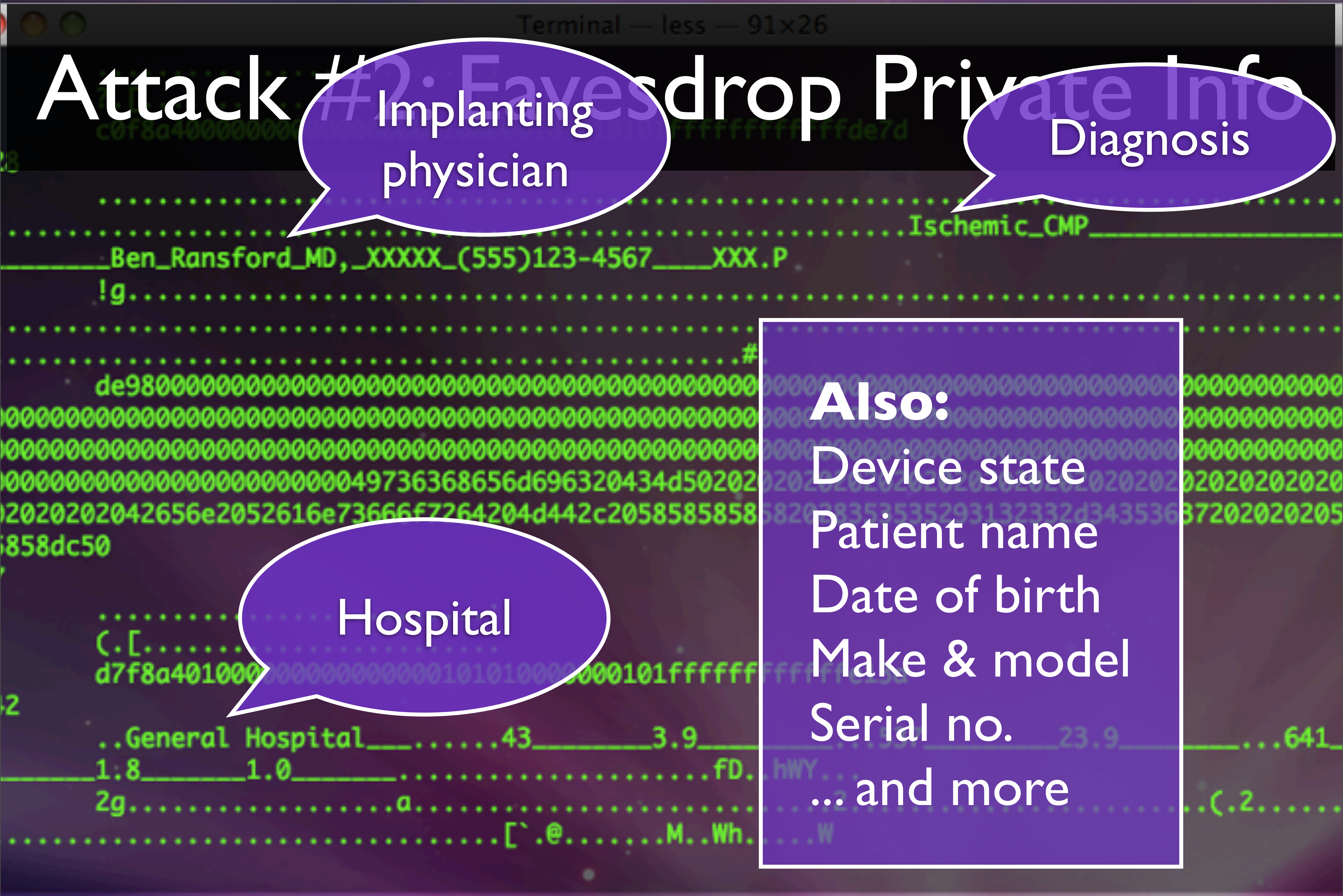
```
      c0f8a400000000                                  ffffffffffffde7d
28

      ............................................................................................
..............................................................Ischemic_CMP_________________
_______Ben_Ransford_MD,_XXXXX_(555)123-4567____XXX.P
      !g..........................................................................................
..............................................................................................
...................................................#.
      de9800000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000004973636865 6d696320434d50202020202020202020202020202020202020202020
2020202042656e2052616e73666f7264204d442c20585858585820283535352931323332d34353637202020205
858dc50

      .........
      (.[.......
      d7f8a401000                          000101ffffffffffffe13a
2

      ..General Hospital___......43________3.9_________...537__________23.9__________...641_
______1.8_______1.0________.......................fD..hWY...
      2g..................a...........................2.........................(.2......
..................................[`.@.......M..Wh.....W
```

Implanting physician

Diagnosis

Hospital

Attack #2: Eavesdrop Private Info



```
      c0f8a4000000000                               ffffffffffde7d
28
      ........................................................................
.........................................................Ischemic_CMP___________
________Ben_Ransford_MD,_XXXXX_(555)123-4567_____XXX.P
      !g......................................................................
..........................................................................
.........................................................#
      de9800000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000497363686566d696320434d50202020202020202020202020202020
202020202042656e2052616e73666f7264204d442c2058585858582028353535293132332d343536372020202025
5858dc50
/

      .........
      (.[.......
      d7f8a401000000000000000001010100000000101ffffffffffe
42
      ..General Hospital___......43_________3.9_______________23.9____________...641_
________1.8_______1.0________.......................fD..hWY
      2g.................a...........................................(.2.....
..............................[`.@........M..Wh.....W
```

Implanting physician

Diagnosis

Hospital

Also:

Device state

Patient name

Date of birth

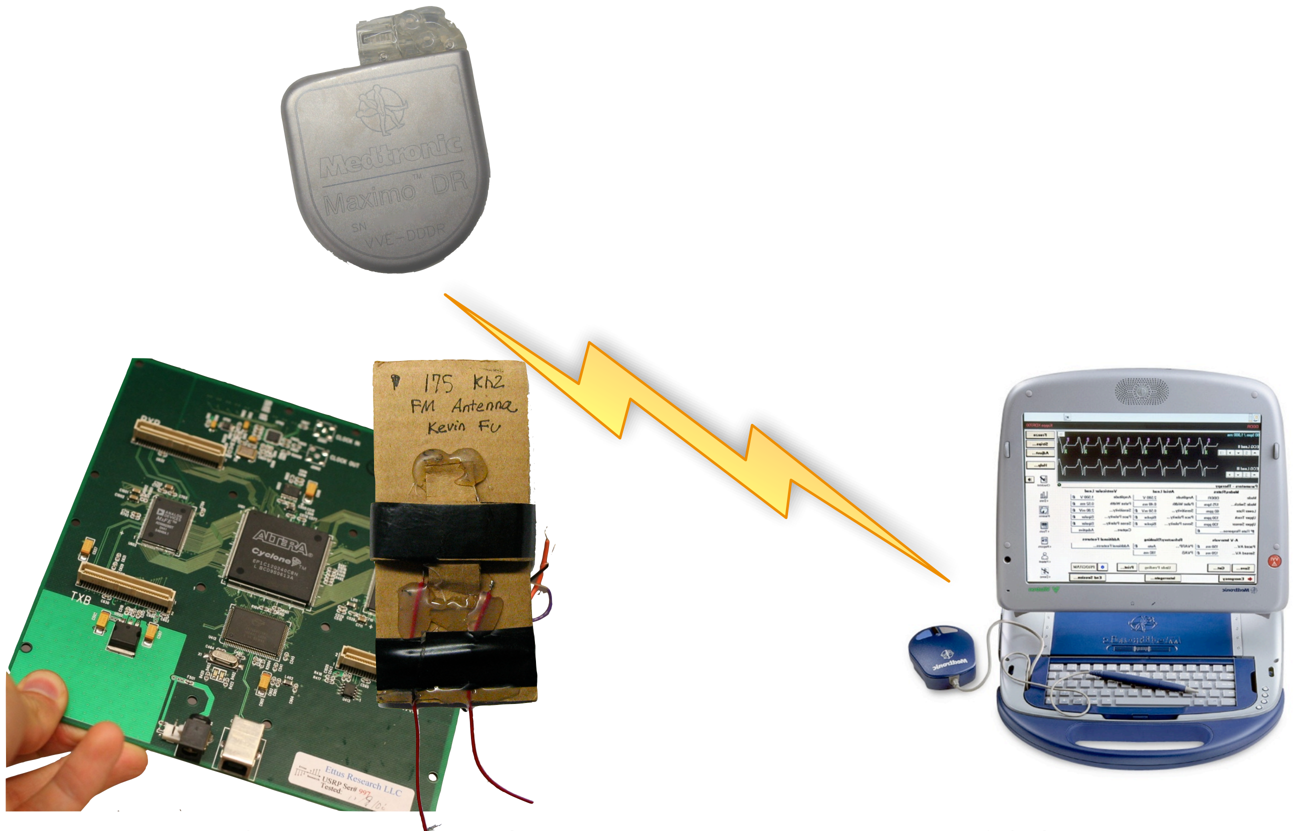
Make & model

Serial no.

... and more

Attack #2: Eavesdrop Private Info

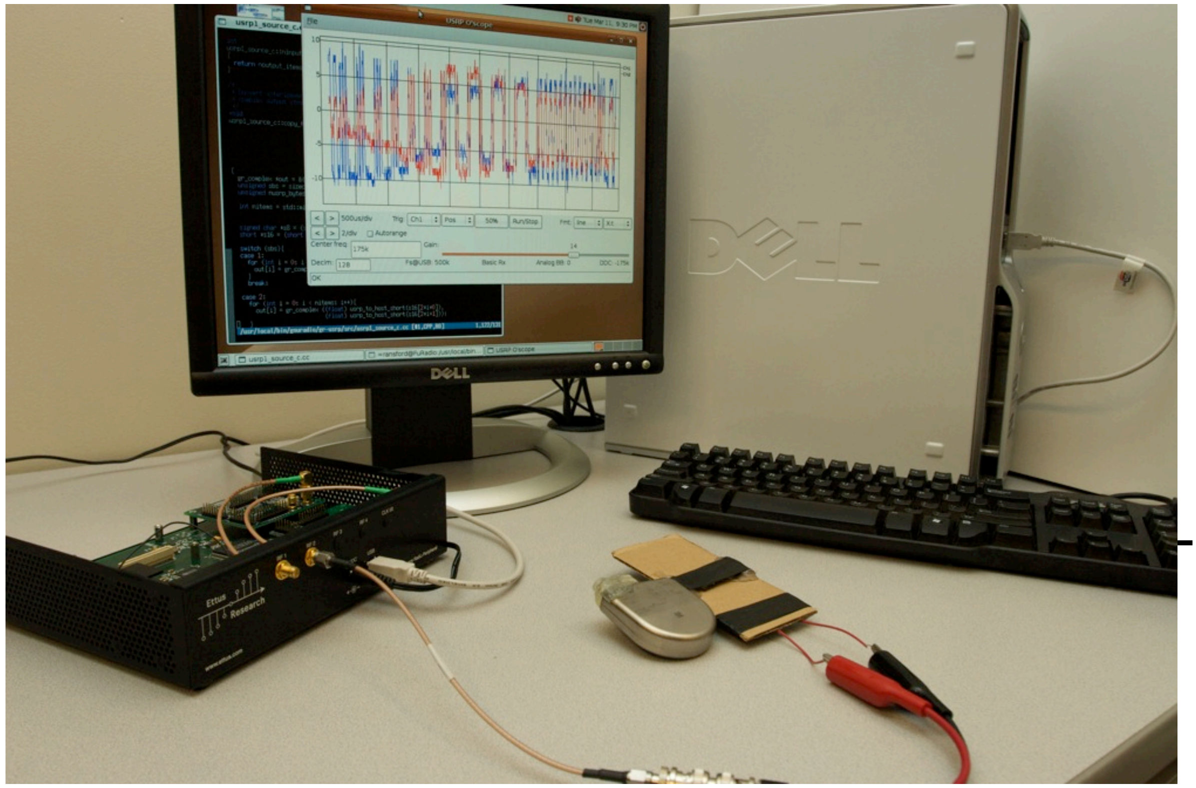
In the future:
Sophisticated devices may divulge **a lot more data**.



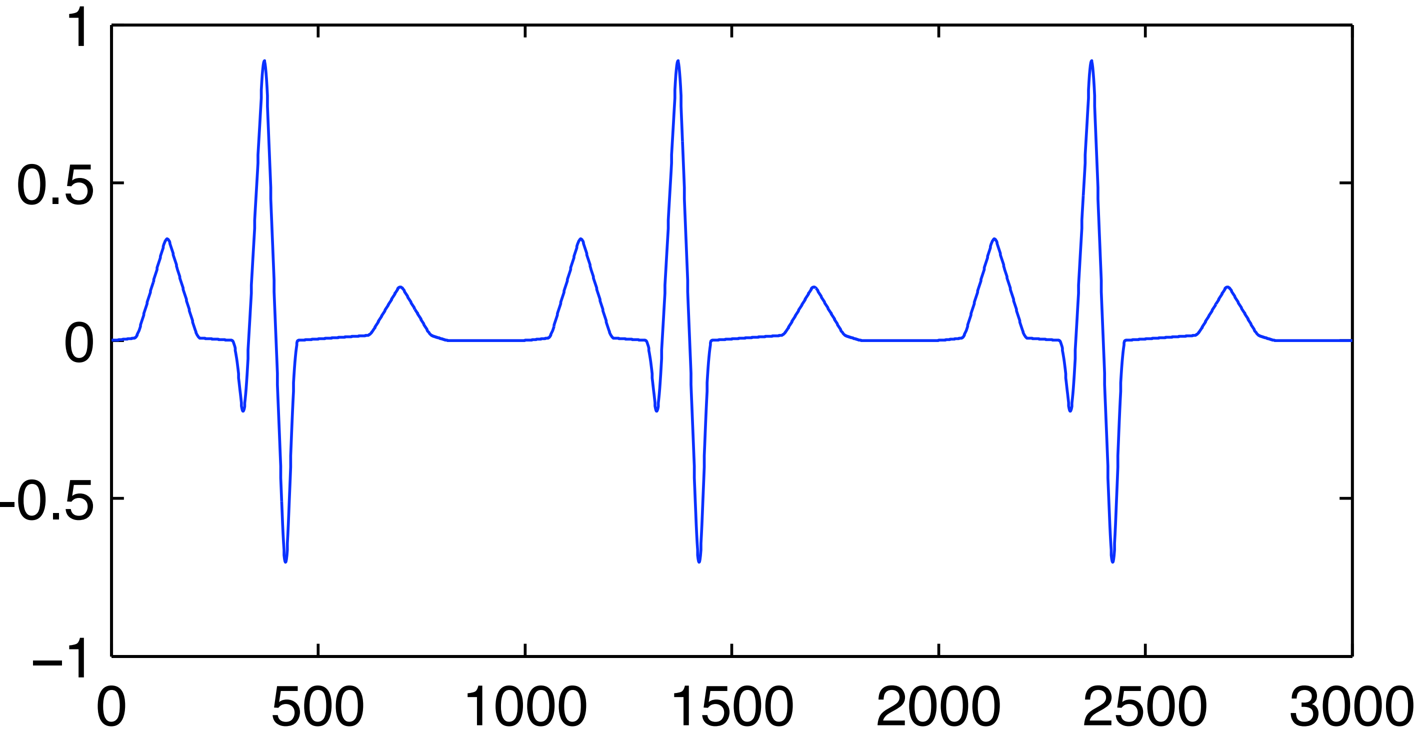
Challenge:
Can we add encryption?

Photo: Medtronic

Attack #3: Sniff Vital Signs



Eavesdropping setup

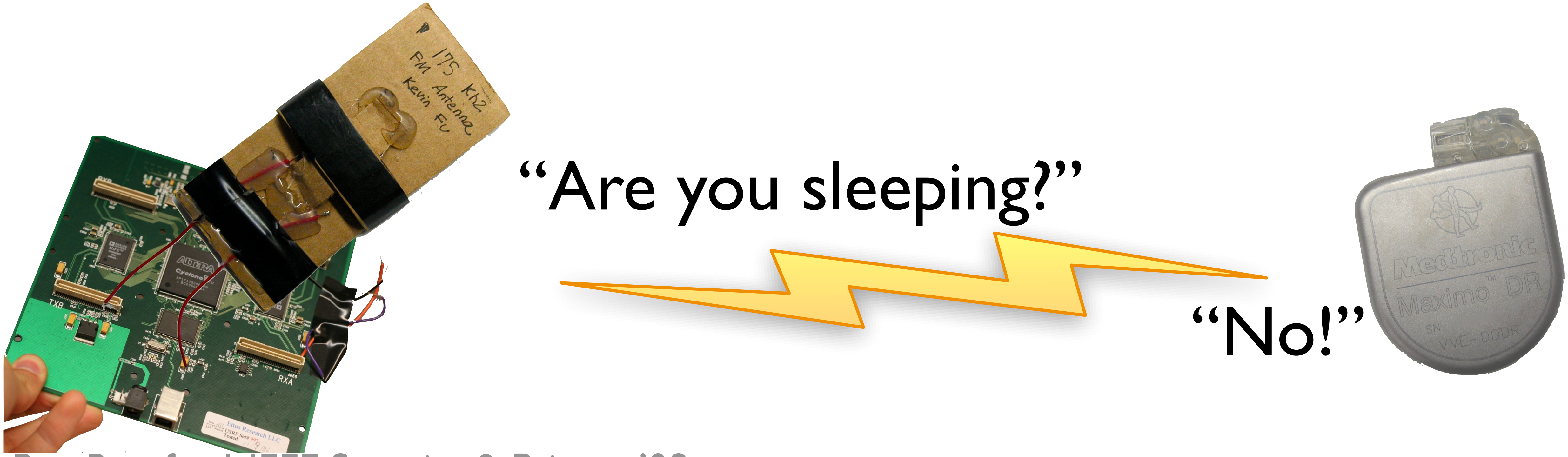


ICD emits *reconstructible* vital signs

Issue: Vital signs can say plenty.

Attack #4: Drain Energy

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



"Are you sleeping?"

"No!"

Simple Replay Attacks

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

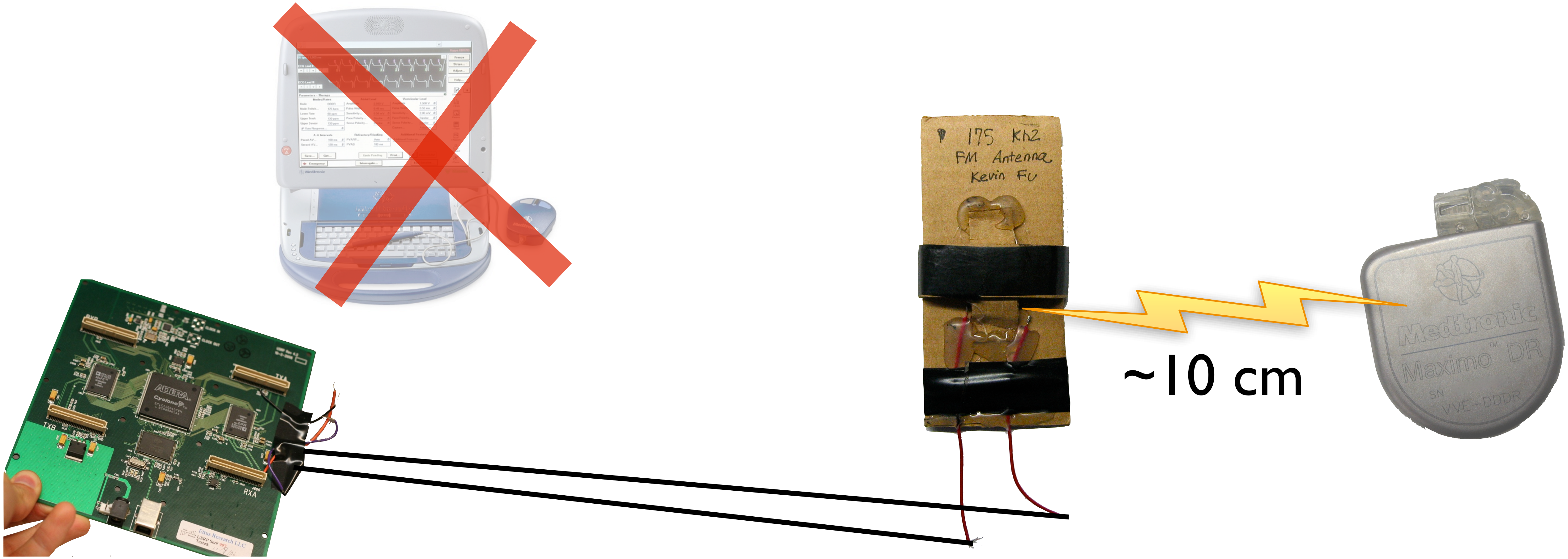
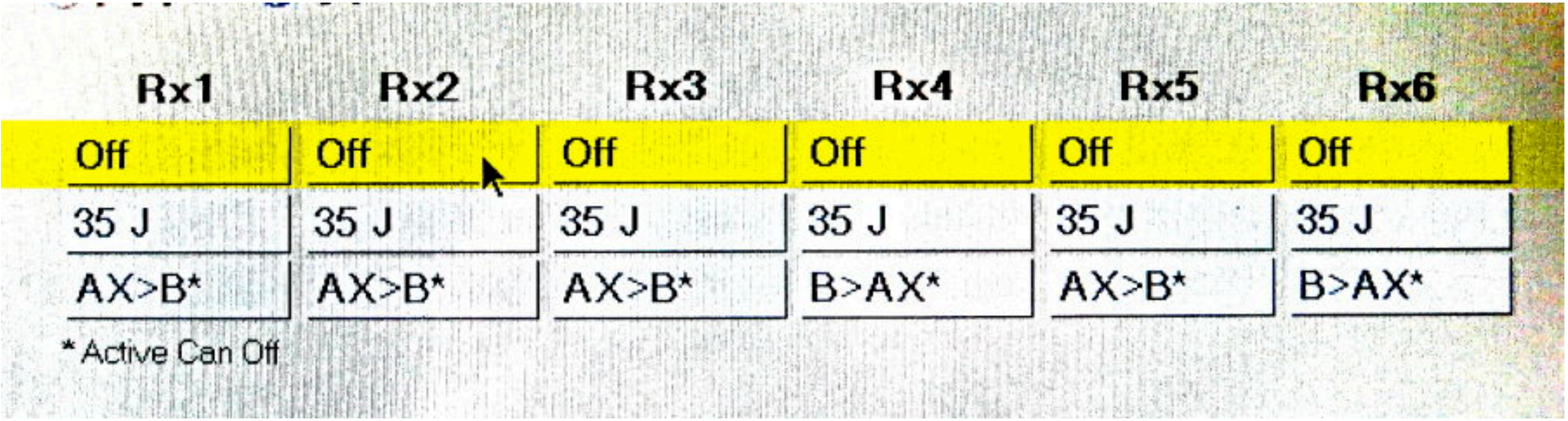


Photo: Medtronic

Attack #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*

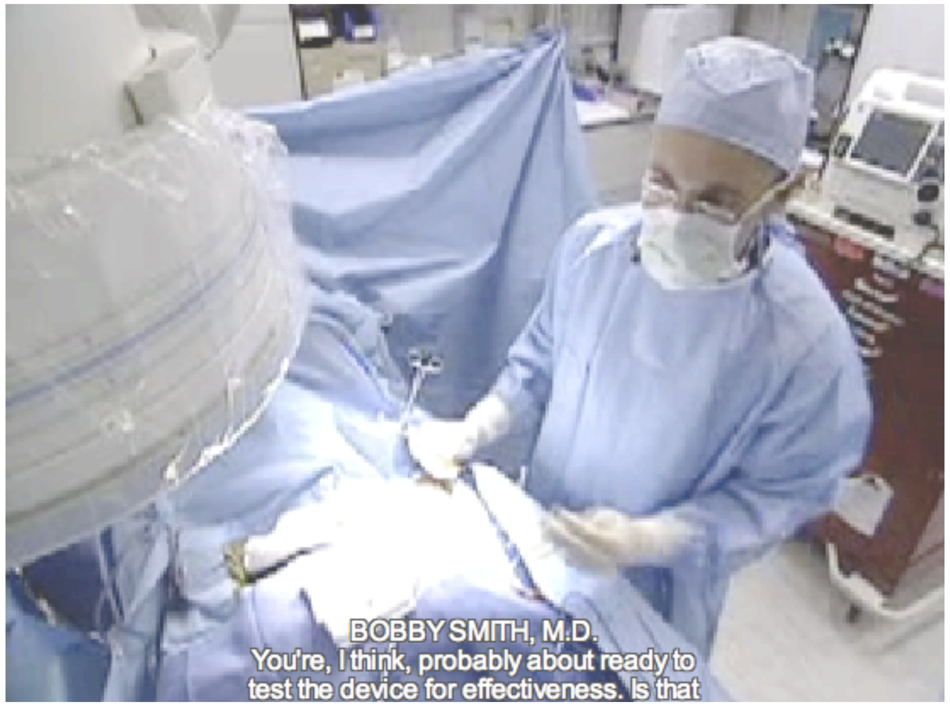
* Active Can Off

- “Stop detecting fibrillation.”
- Device programmer would **warn** here

Issue: Can quietly change device state.

Attack #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, ...


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.

#2: Fundamental Challenges

Conventional Solutions?

How about...	Non-trivial problem
Authenticate device programmers?	Key management is hard. Revocation?
Encrypt all transmissions?	Under what key? Must fail open!

Cannot **fail closed**

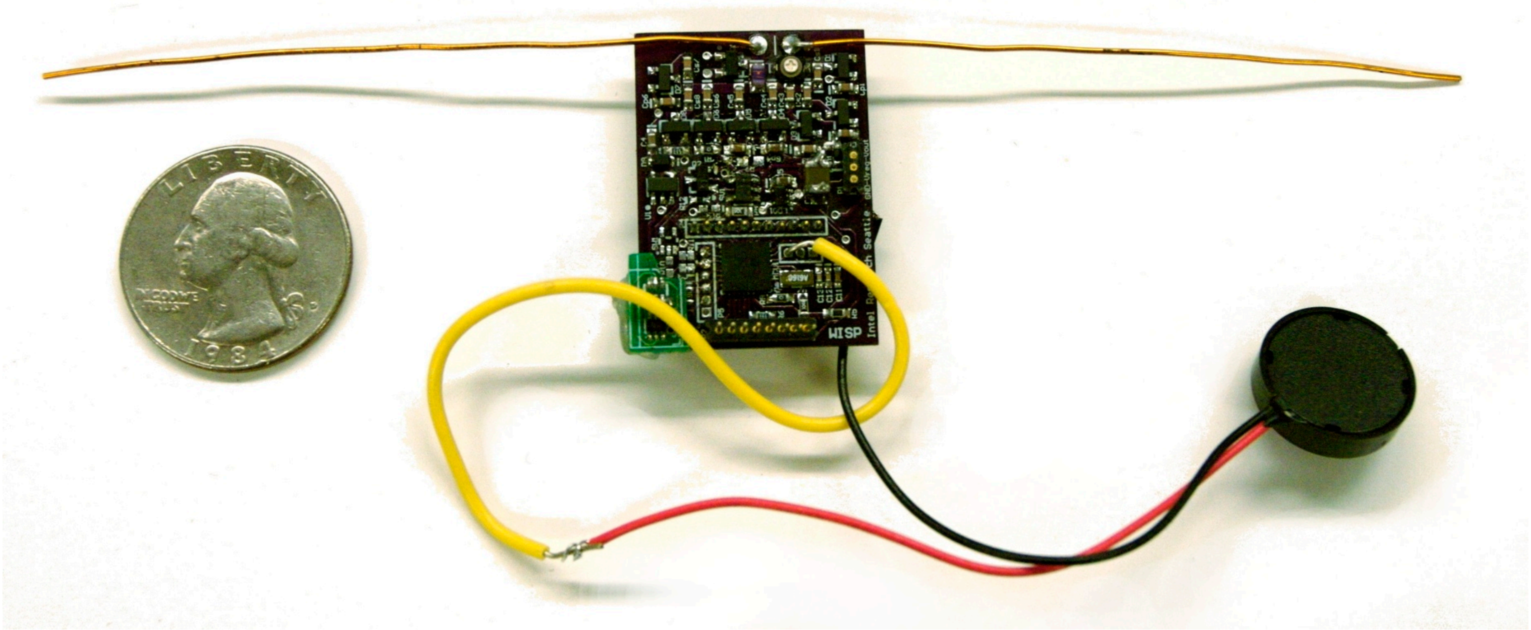
- Closed: Don’t know the password? No admission!
- Medical personnel need emergency access.
- Challenge: design to **fail open**.

Security vs. Safety?

- Tensions discussed in [IEEE Pervasive ’08]
- Patient’s health is the top priority
- We seek the **sweet spots**

3. Defensive Directions

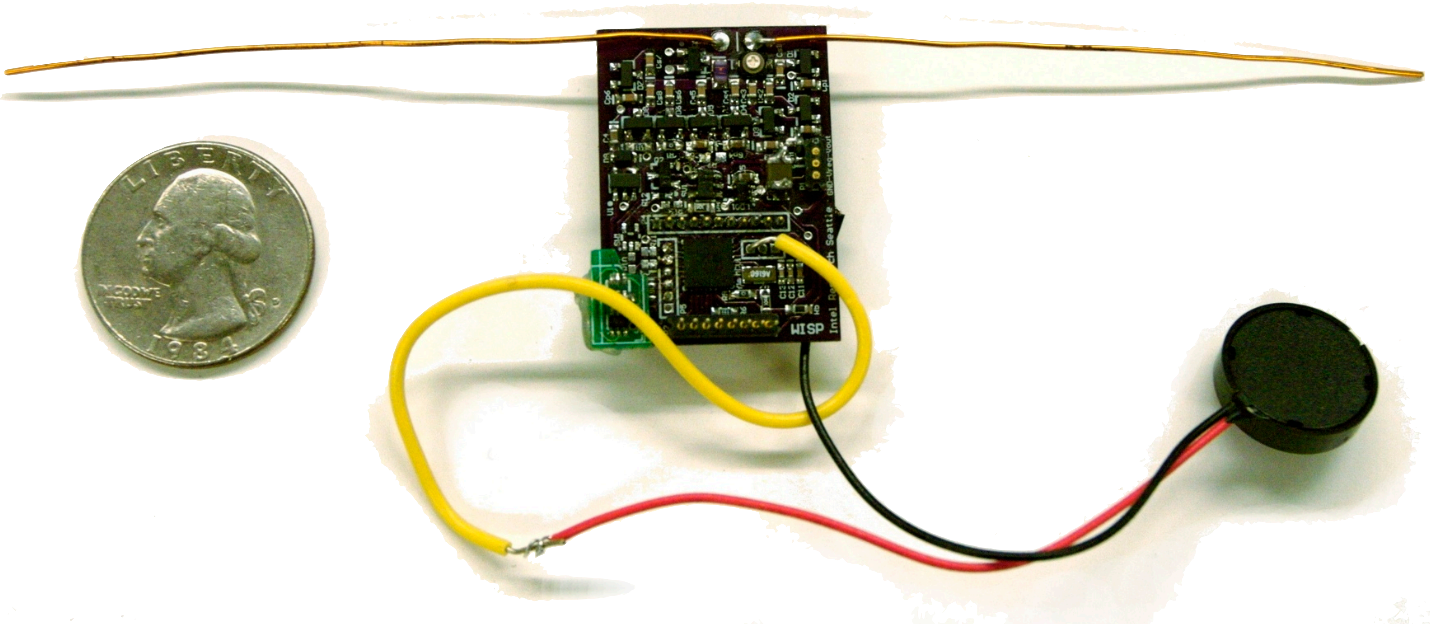
Prototype defenses against **some** of the attacks.



Main idea: defend without using battery.

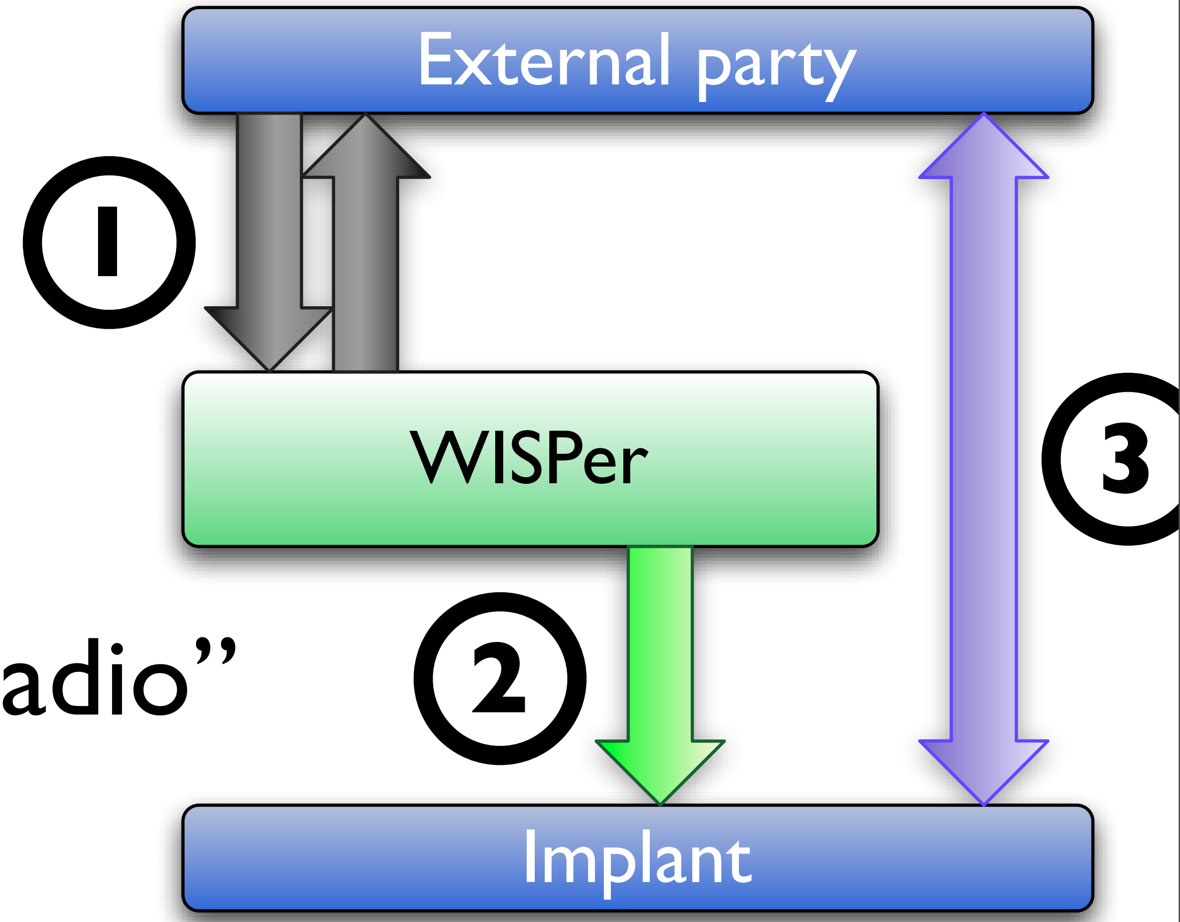
B.Y.O.P.

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



Goal: External party pays for power.

WISPer as Gatekeeper

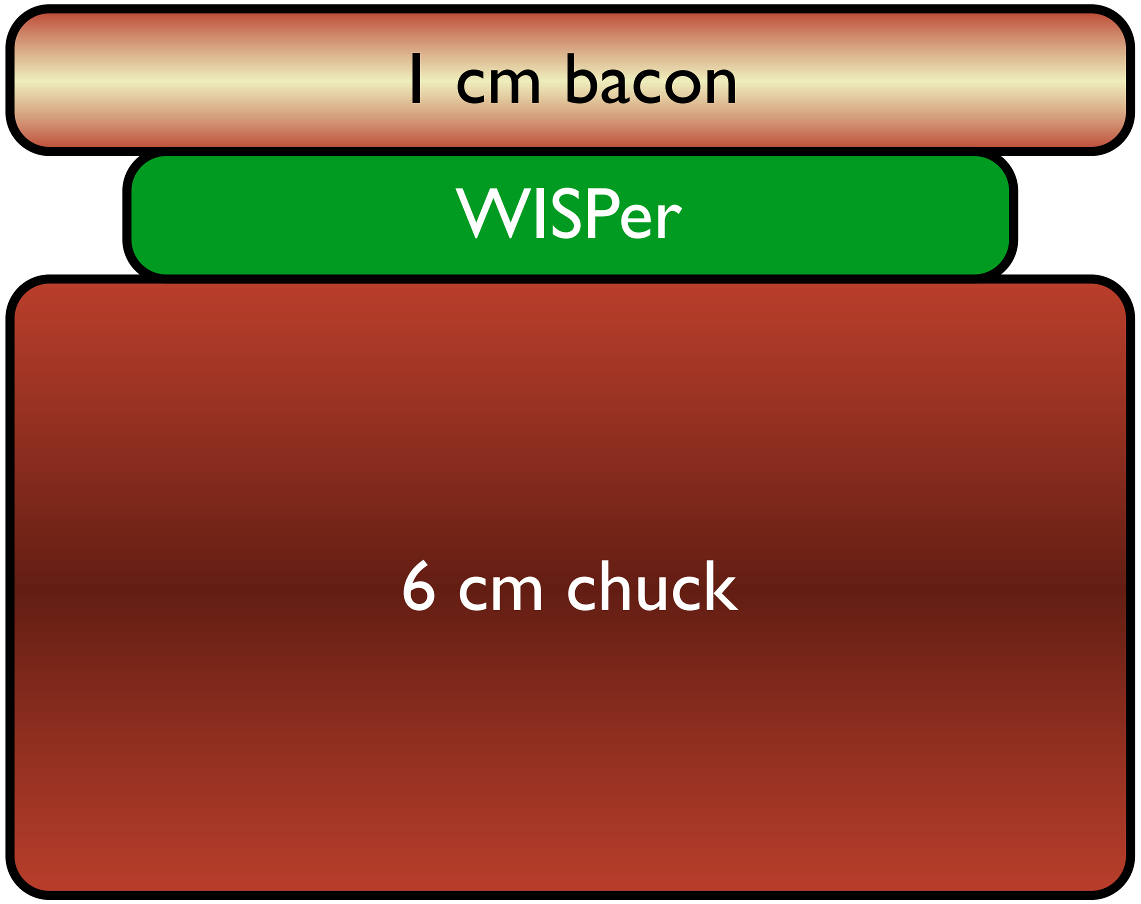


- Authenticate against WISPer
- WISPer to ICD: "OK to use radio"
- Acoustic patient notification
- How to deter enemies? (Open question!)

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

Testing WISPer: Simulated Torso



1 cm bacon

WISPer

6 cm chuck

Energy harvesting through tissue is possible.

Medical Devices Need Continued Attention!

Medical Device Trends

- Further computerization of care
- Longer-range communication
- Cooperation among devices

Issue: All of these bring risks.

Related Work

- [IEEE Pervasive '08] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel: *Security and privacy for implantable medical devices.* (January 2008)
- [JAMA '06] W. H. Maisel, M. Moynahan, B. D. Zuckerman, T. P. Gross, O. H. Tovar, D.-B. Tillman, and D. B. Schultz: *Pacemaker and ICD generator malfunctions: Analysis of Food and Drug Administration annual reports.* (JAMA 295(16))
- [Ubicomp '06] J. R. Smith, A. P. Sample, P. S. Powledge, S. Roy, and A. Mamishev: *A wirelessly-powered platform for sensing and computation.*
- [RFIDSEC '07] H.-J. Chae, D. J. Yeager, J. R. Smith, and K. Fu: *Maximalist cryptography and computation on the WISP UHF RFID tag.*
- More in paper

Conclusions

- Analysis of wirelessly controlled IMD
- Methodologies & defensive directions
    - Software radio
    - Energy harvesting gatekeeper
    - Patient notification (deterrence)
- Many open problems

http://secure-medicine.org/

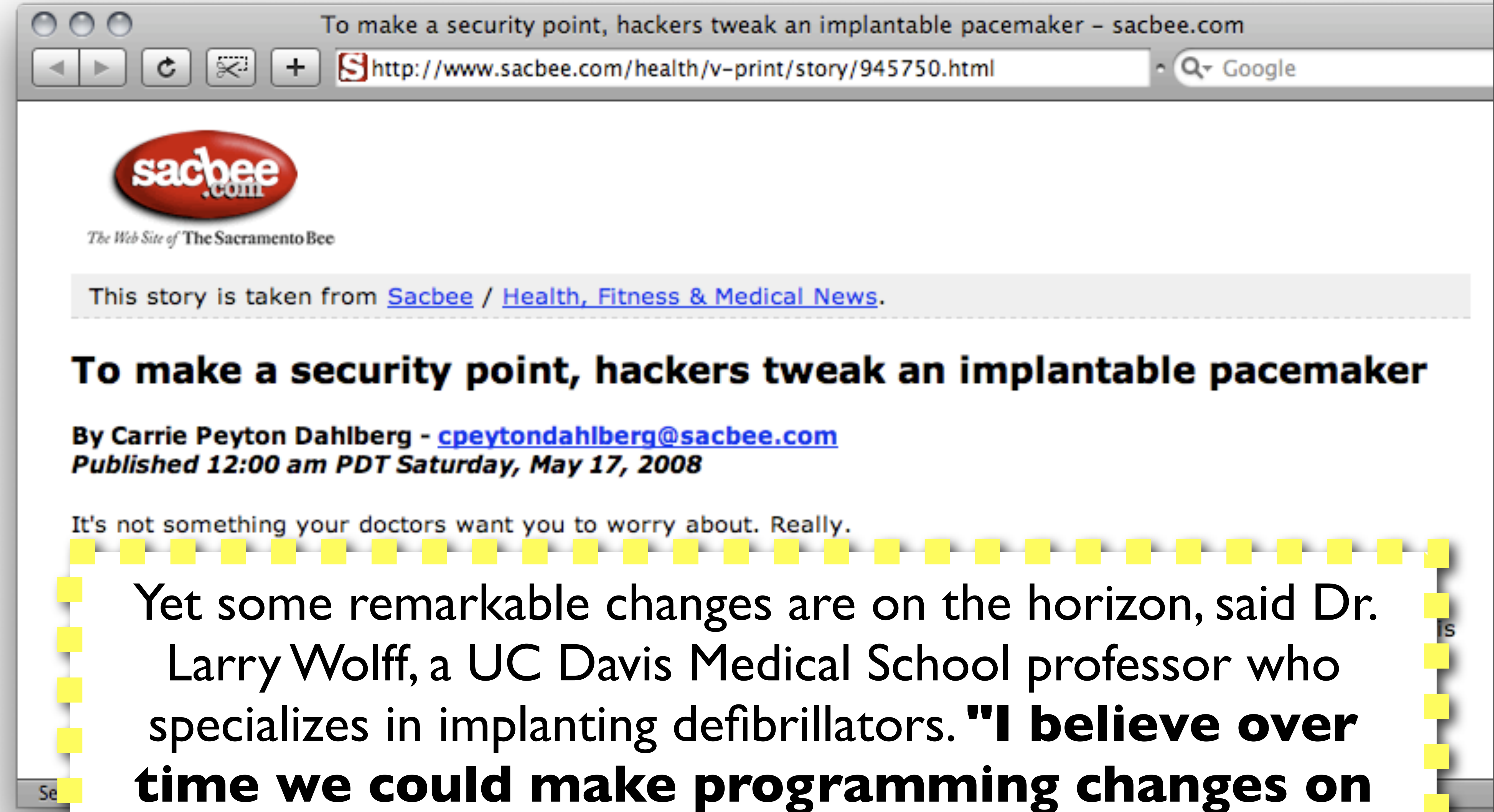
Conclusions

- **Many open problems:**
  - Balance safety & security
  - Key management
  - Attacks can be improved
  - Defenses can be improved

http://secure-medicine.org/

Non-Technical Challenges

- Manufacturers beholden only to regulators
- No security regulation
- Safety & effectiveness are FDA's mandate
- No major interface between FDA & FCC



To make a security point, hackers tweak an implantable pacemaker - sacbee.com

http://www.sacbee.com/health/v-print/story/945750.html

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.

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.

Sacramento Bee, May 17, 2008

Dan Dan, M.D.
Electrophysiologist, Piedmont Hospital