Confidence in a connected world.

Trust and Security

M. Dacier, Sr. Director
Collaborative Advanced Research Dept. (CARD)
Symantec Research Labs (SRL)

marc_dacier@symantec.com

Render unto Fu that which is Fu's

- Kevin Fu is the co-director, with T. Kohno and W. Maisel, of the Medical Device Security Center, a cross-disciplinary research initiative on medical device security, privacy, safety, and effectiveness. The center relies on a partnership between researchers at the Beth Israel Deaconess Medical Center, Harvard Medical School, the University of Massachusetts Amherst, and the University of Washington (see www.secure-medicine.org for more).

- Kevin was kind enough to send me some material to prepare this talk and points me to some interesting URLs.

- For a quick introduction to the domain, I recommend:
  - **[Fu09] Kevin Fu, Inside Risks, "Reducing Risks of Implantable Medical Devices", Communications of the ACM, June 2009, Vol. 52, N.6 , pp. 25-27.**
  - **[Fu09b] Kevin Fu, "Implantable Medical Devices: Security Privacy for Pervasive, Wireless Healthcare", March 2009, talk, slides available on line at http://www.cs.umass.edu/~kevinfu/talks/Fu-IMD-security.pdf**

- See also the upcoming 1st Usenix Security workshop on Health Security and Privacy (August 10, 2010, Washington, DC, www.usenix.org/event/healthsec10)

Symantec At a Glance

Founded in 1982
IPO in 1989

More than 17,500 employees

Operations in more than 40 countries

99 percent of Fortune 1000 companies are customers

#419 on the 2009 Fortune 500

$6.2 billion revenue in FY 2009

More than 600 global patents

More than 56 million active consumer users

110 million enterprise customers

Invest 15% annual revenue in R&D

Today’s reality

More risks, more demands, smaller budgets

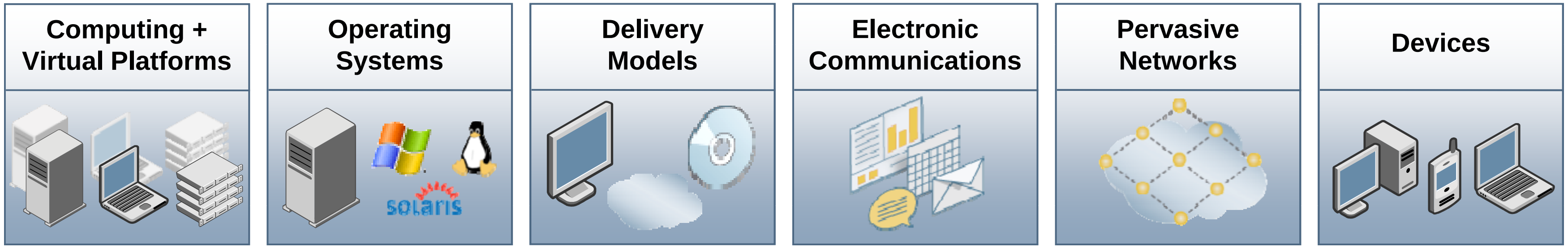
Technology Sprawl = Added Risk

Relentless demand, financial pressure

- 6X growth in storage from ’07 to ’11
- People, business and technology inseparable

More risks, bigger consequences

- Stealthy attacks grow 468% in ’07
- Information mobility puts risk everywhere



Computing + Virtual Platforms

Operating Systems

Delivery Models

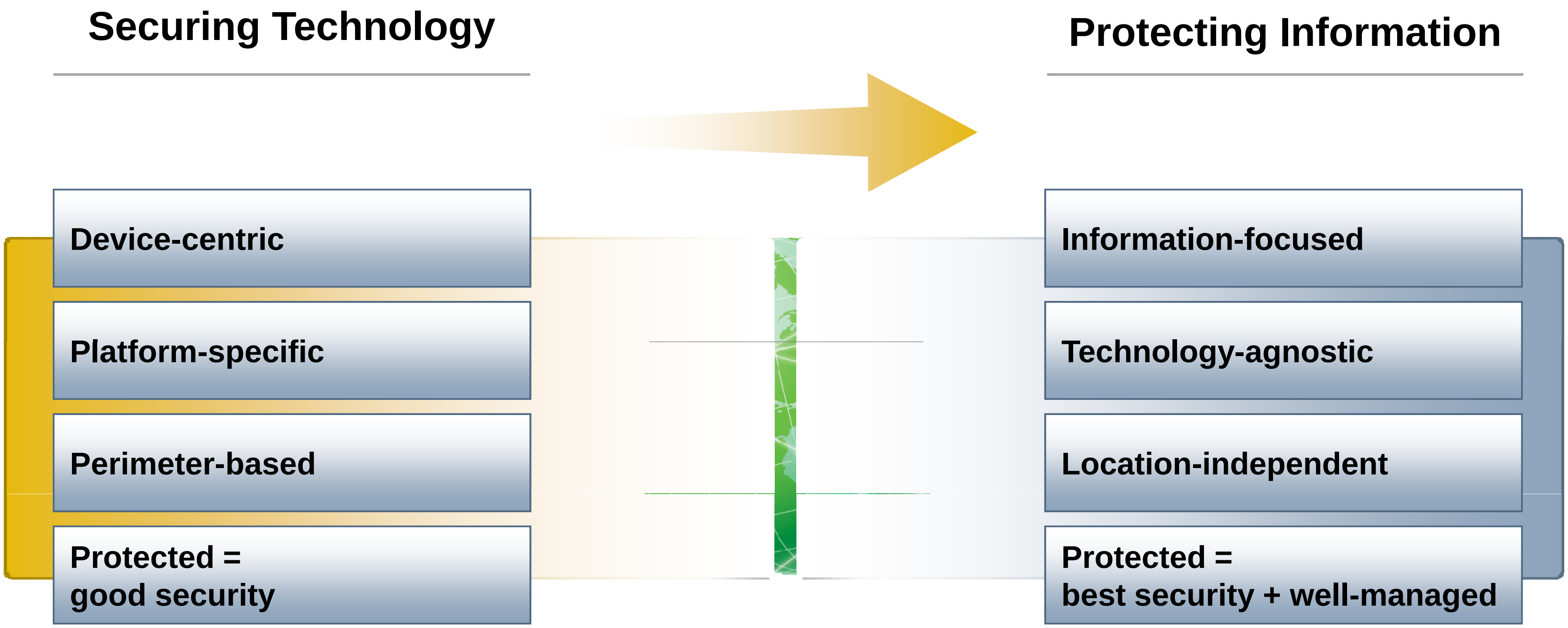
Electronic Communications

Pervasive Networks

Devices

Requirement

Technology-centric to information-driven



Securing Technology

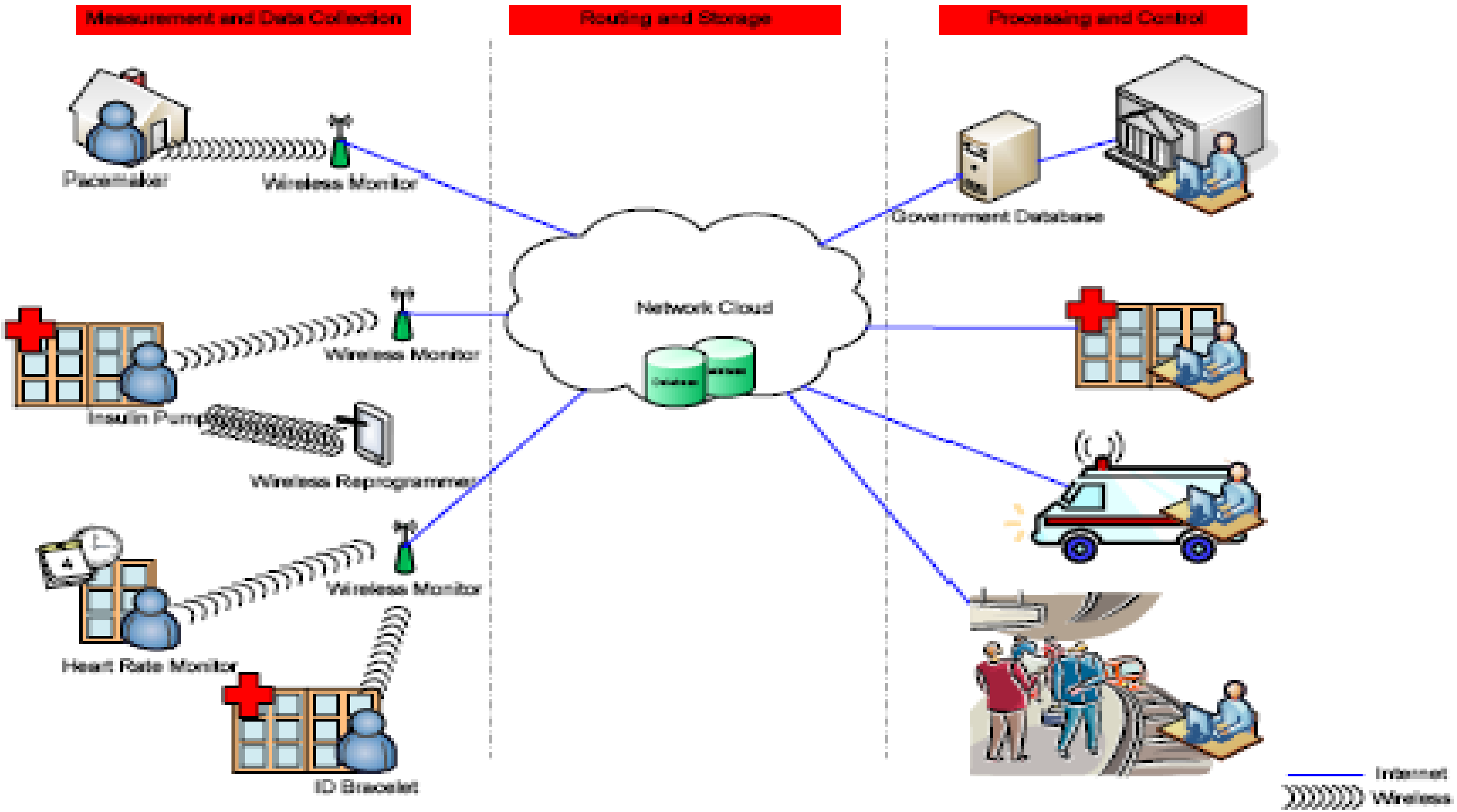
- Device-centric
- Platform-specific
- Perimeter-based
- Protected = good security

Protecting Information

- Information-focused
- Technology-agnostic
- Location-independent
- Protected = best security + well-managed

Medical Telemetry Infrastructure

www.thei3p.org/docs/publications/whitepaper-protecting_global_medical.pdf



Focus: what about IMDs?

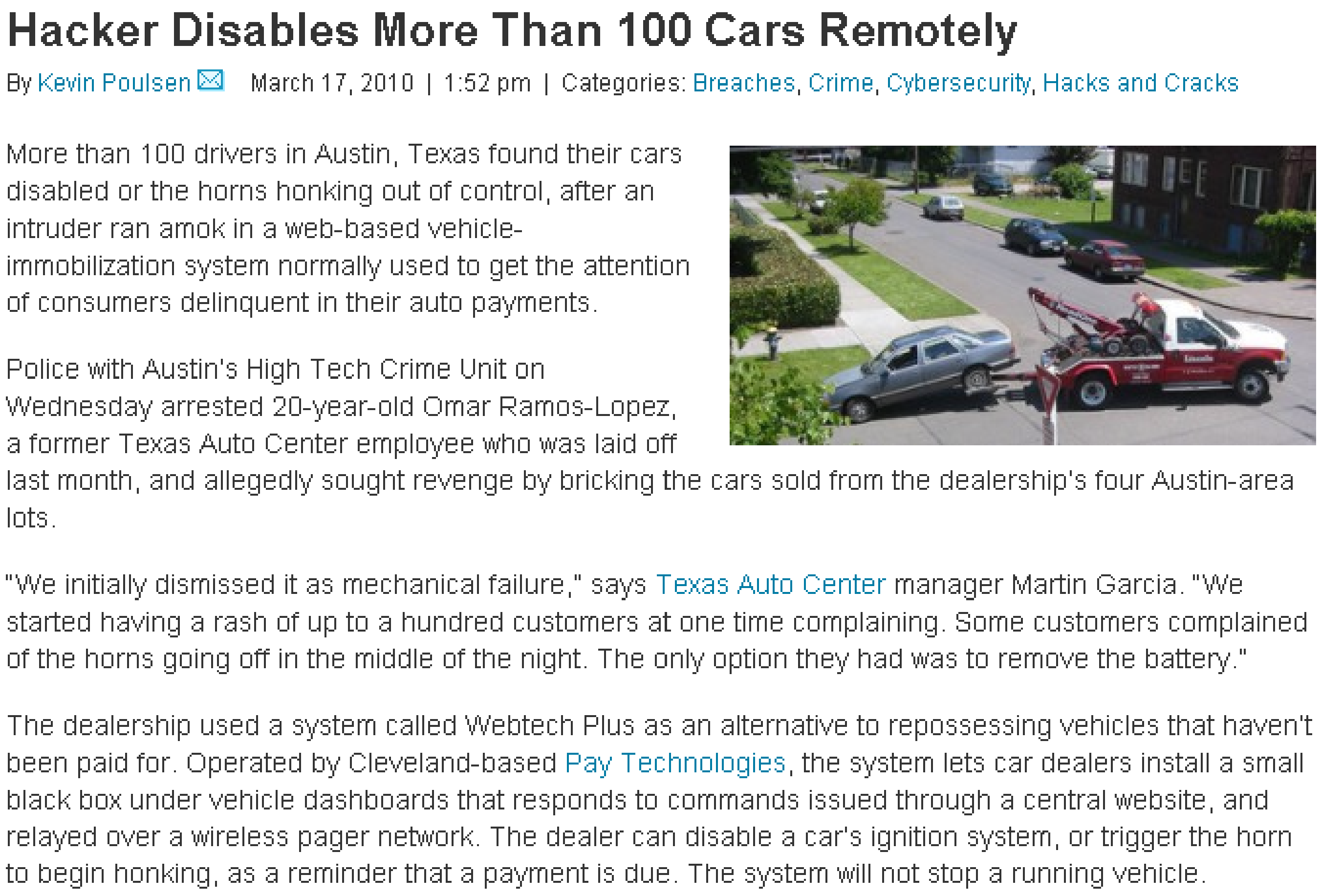
- Securing Implantable Medical Devices is not only about securing *"a device".*

- It is also about
  - Protecting the elements interacting with it to ensure its integrity
  - Protecting the information coming from it to preserve its confidentiality
  - Ensuring its availability with malicious interactions in mind.

- In other words, it is also about managing the control and data flows it is part of.

- Most importantly, functional correctness must be ensured despite an adversarial environment (maliciousness, stupidity, carelessness, etc.)

Functional correctness ….



Hacker Disables More Than 100 Cars Remotely

By Kevin Poulsen March 17, 2010 | 1:52 pm | Categories: Breaches, Crime, Cybersecurity, Hacks and Cracks

More than 100 drivers in Austin, Texas found their cars disabled or the horns honking out of control, after an intruder ran amok in a web-based vehicle-immobilization system normally used to get the attention of consumers delinquent in their auto payments.

Police with Austin's High Tech Crime Unit on Wednesday arrested 20-year-old Omar Ramos-Lopez, a former Texas Auto Center employee who was laid off last month, and allegedly sought revenge by bricking the cars sold from the dealership's four Austin-area lots.

"We initially dismissed it as mechanical failure," says Texas Auto Center manager Martin Garcia. "We started having a rash of up to a hundred customers at one time complaining. Some customers complained of the horns going off in the middle of the night. The only option they had was to remove the battery."

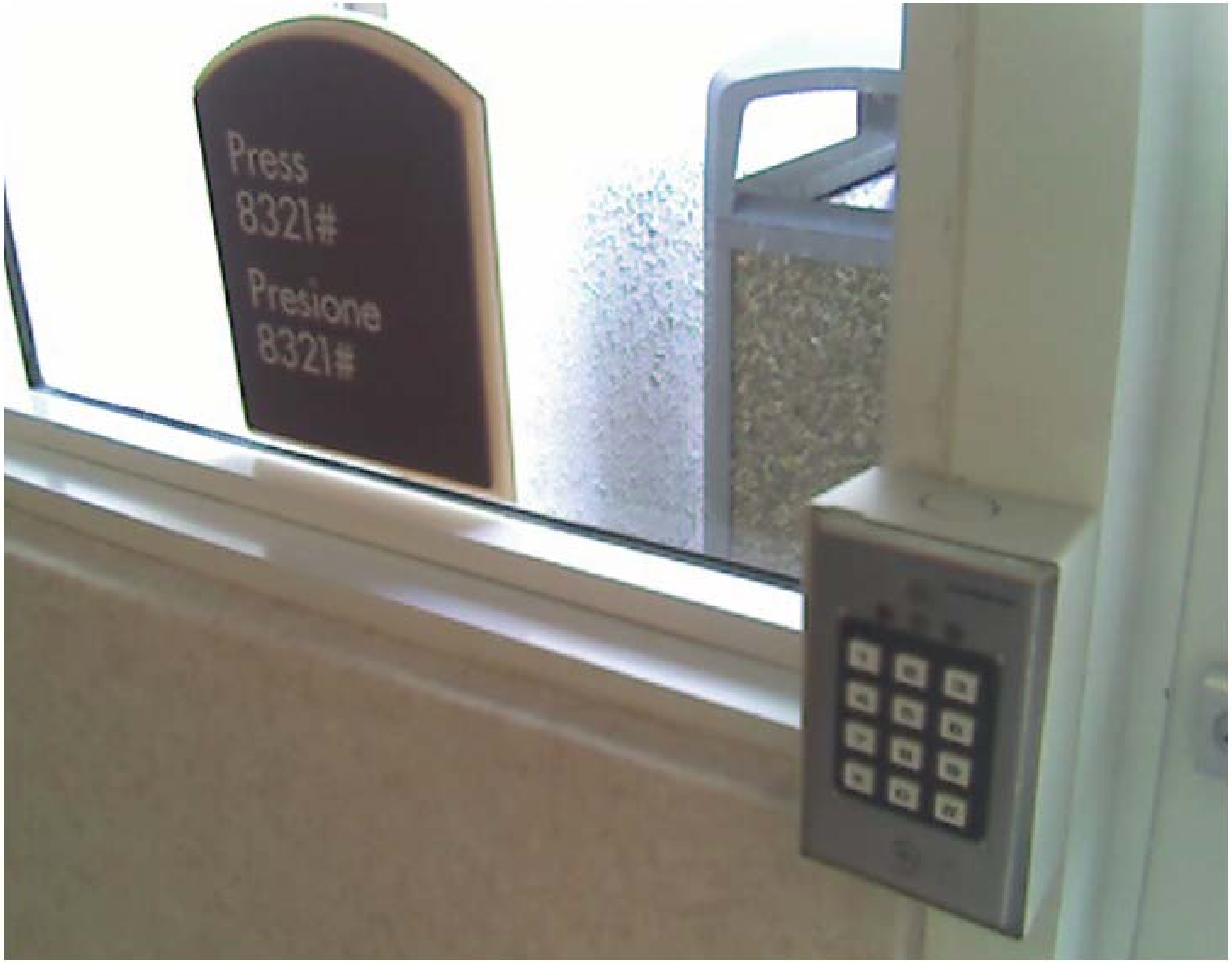
The dealership used a system called Webtech Plus as an alternative to repossessing vehicles that haven't been paid for. Operated by Cleveland-based Pay Technologies, the system lets car dealers install a small black box under vehicle dashboards that responds to commands issued through a central website, and relayed over a wireless pager network. The dealer can disable a car's ignition system, or trigger the horn to begin honking, as a reminder that a payment is due. The system will not stop a running vehicle.

www.wired.com/threatlevel/2010/03/hacker-bricks-cars/

Note that the "*service*" was "*correctly*" delivered!

Correctness in an *adversarial* context

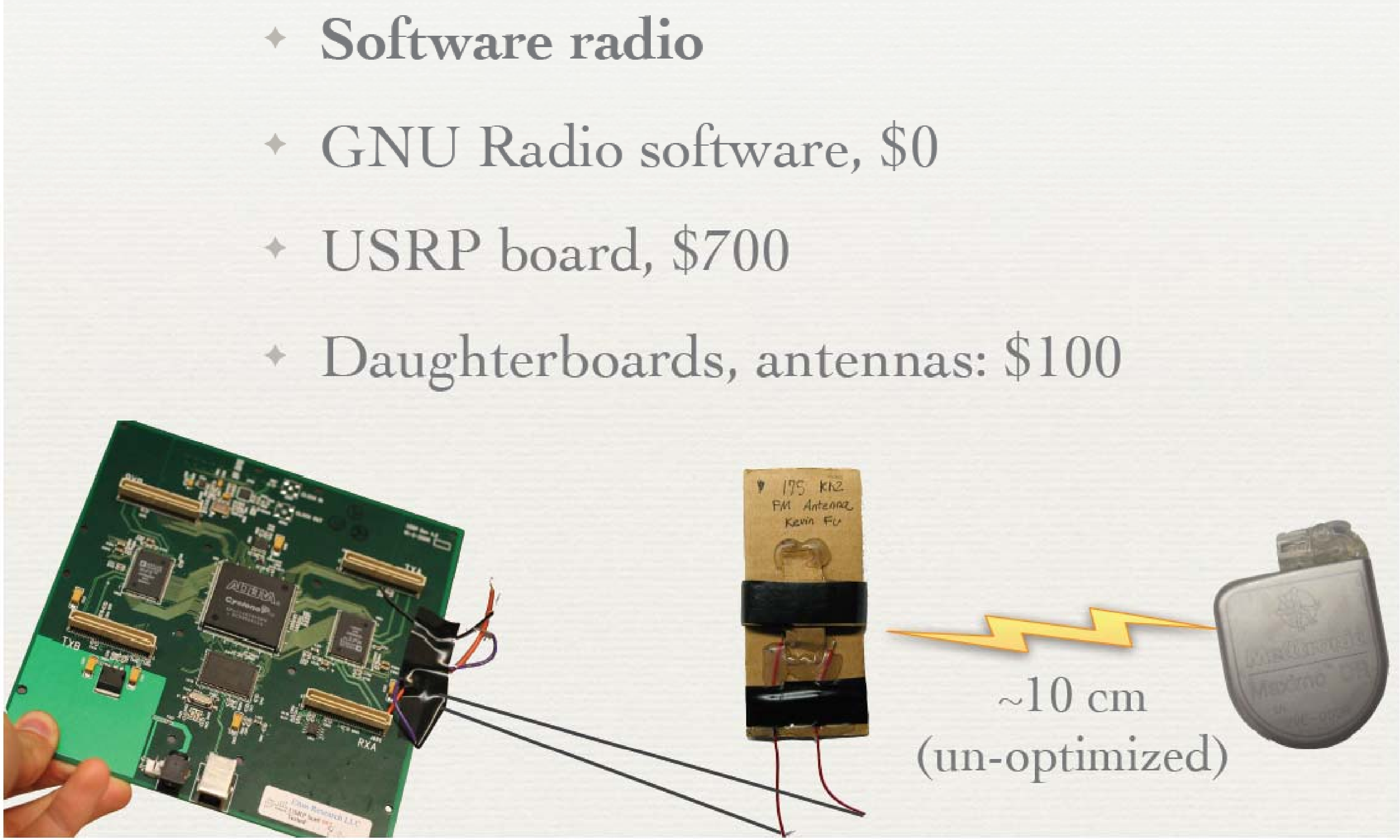
(picture taken by K. Fu [Fu09b])



Examples of vulnerabilities for IMDs

- In [Halperin08] it is “ shown how lifesaving therapies could silently be modified and disabled via radio communication on an implantable defibrillator that had passed premarket approval by regulators. The same device was reprogrammed with an unauthenticated radio-based command to induce a shock that causes ventricular fibrillation (a fatal heart rhythm). This implantable cardioverter defibrillator has been implanted in hundreds of thousands of patients “ [Fu09]
  - [Halperin08] Halperin, D. et al. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *Proceedings of the 29th Annual IEEE Symposium on Security and Privacy*, May 2008.

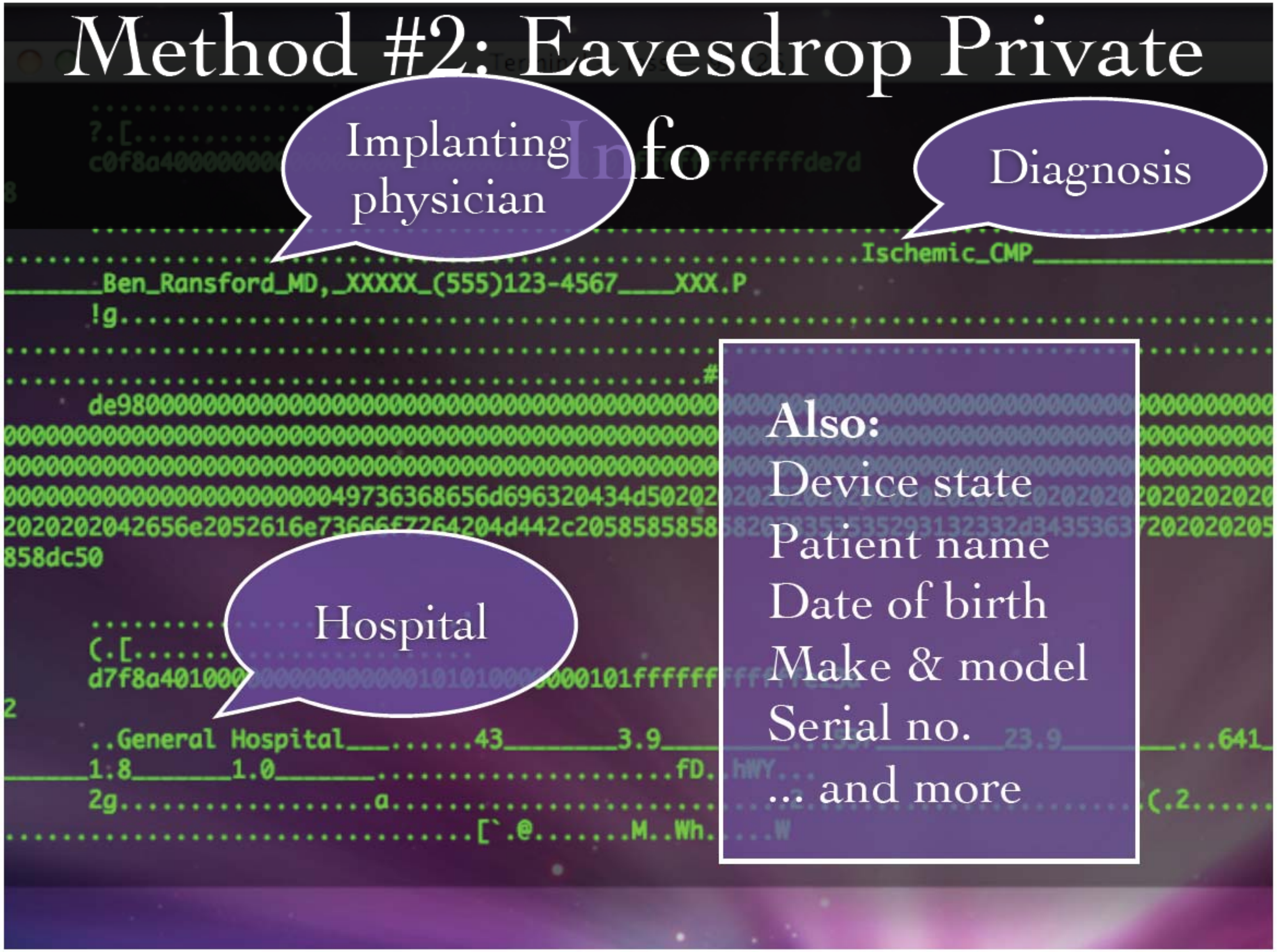
Experimental devices used in [Halperin08]



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

~10 cm (un-optimized)

Privacy attack taken from [Fu09b]



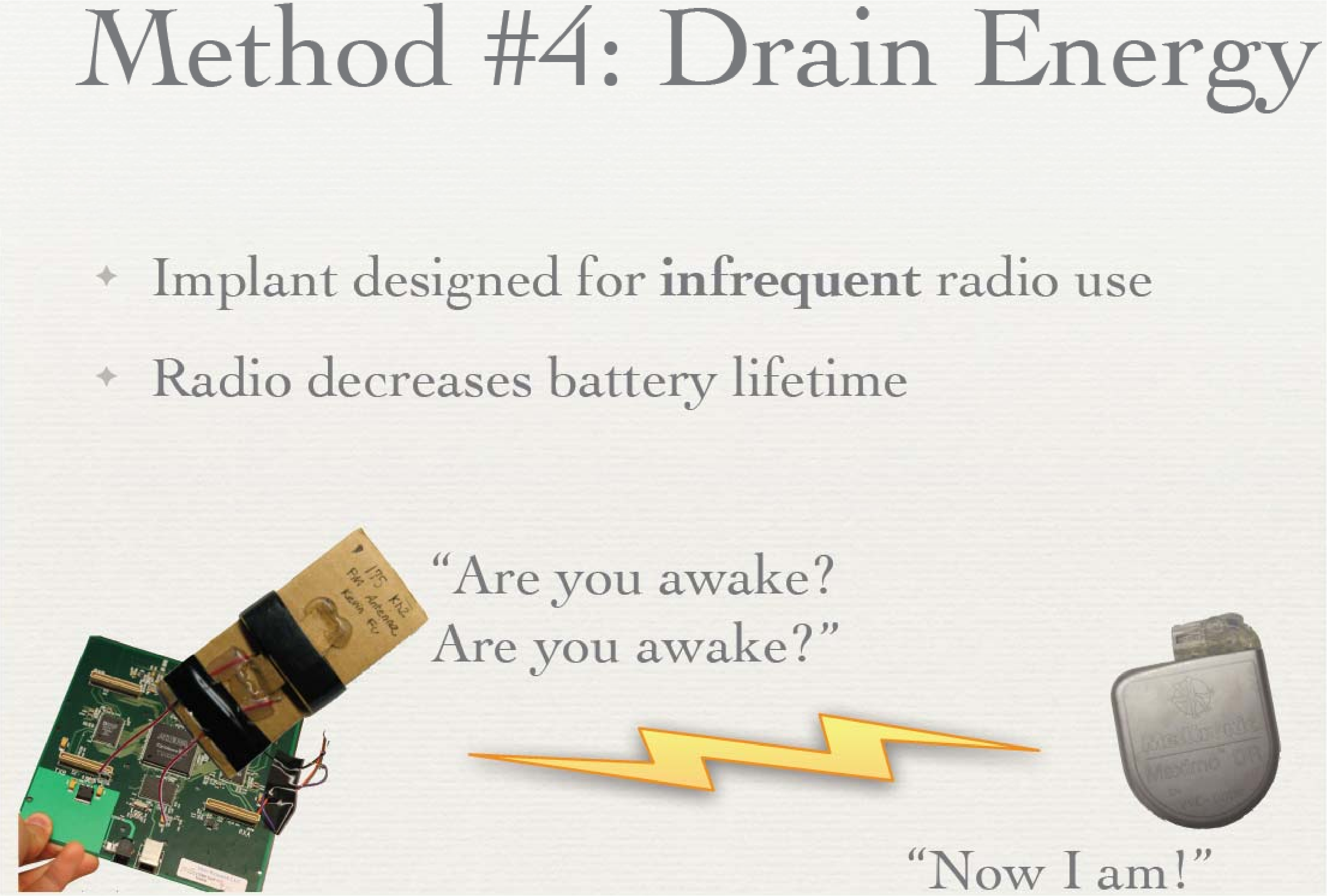
Method #2: Eavesdrop Private Info

```
?.[........
c0f8a4000000000                       fffffffde7d
8
..........................................................................................
.........................................................................Ischemic_CMP__________________
_______Ben_Ransford_MD,_XXXXX_(555)123-4567____XXX.P
      !g.....................................................................................
..........................................................................................
.......................................................#
      de98000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000049736368656d696320434d50202020202020202020202020202020202020202020
2020202042656e2052616e73666f7264204d442c205858585858582028353535293132332d34353637202020205
858dc50

      .........
      (.[........
      d7f8a4010000000000000000001010100000000101ffffffffffff
2
      ..General Hospital___......43________3.9____________23.9____________...641_
_______1.8________1.0________....................fD..hWY...
      2g..................a.....................................................(.2.......
..................................[`.@.......M..Wh.....W
```

Also:
Device state
Patient name
Date of birth
Make & model
Serial no.
... and more

Availability attack taken from [Fu09b]



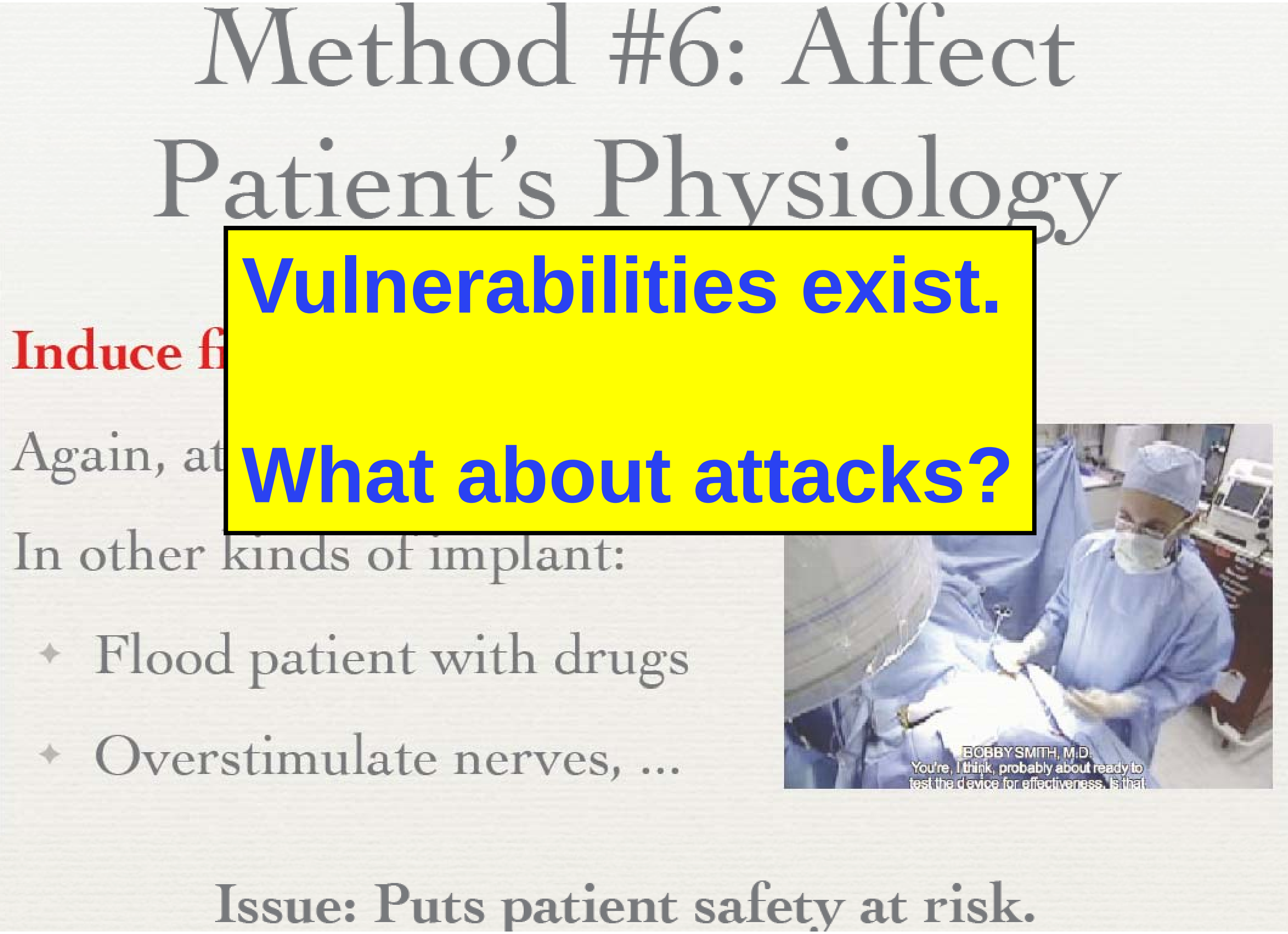
Method #4: Drain Energy

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

"Are you awake?
Are you awake?"

"Now I am!"

Integrity attack taken from [Fu09b]



Method #6: Affect Patient's Physiology

Induce fi

Again, at

In other kinds of implant:

- Flood patient with drugs
- Overstimulate nerves, ...

Issue: Puts patient safety at risk.

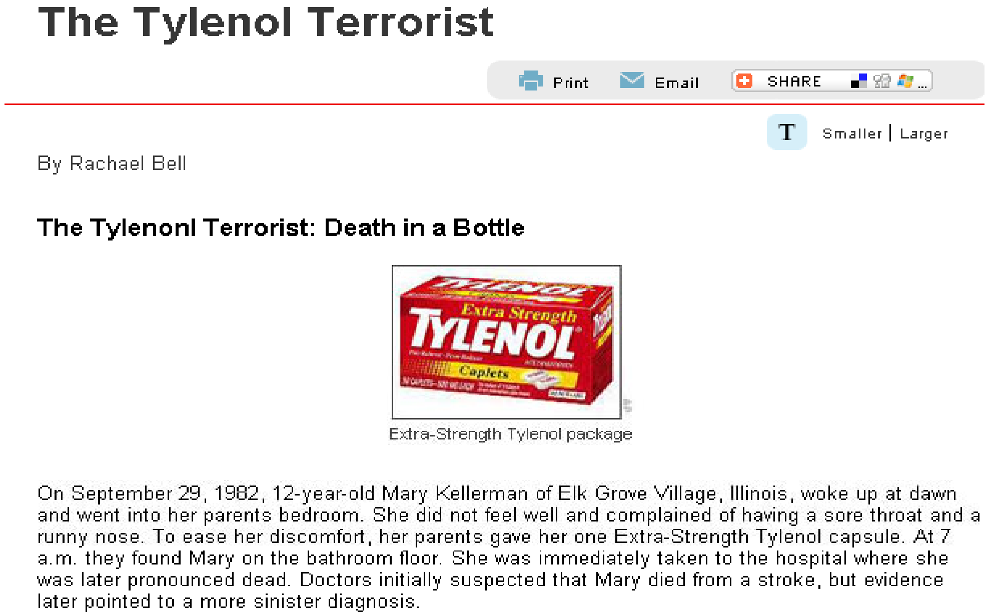
BOBBY SMITH, M.D.
You're, I think, probably about ready to
test the device for effectiveness. Is that

Vulnerabilities exist.

What about attacks?

Fools exist …

- “In 1982, someone deliberately laced Tylenol capsules with cyanide and placed the contaminated products on store shelves in the Chicago area. This unsolved crime led to seven confirmed deaths, a recall of an estimated 31 million bottles of Tylenol, and a rethinking of security for packaging medicine in a tamper-evident manner” [Fu09]



The Tylenol Terrorist

By Rachael Bell

The Tylenonl Terrorist: Death in a Bottle

Extra-Strength Tylenol package

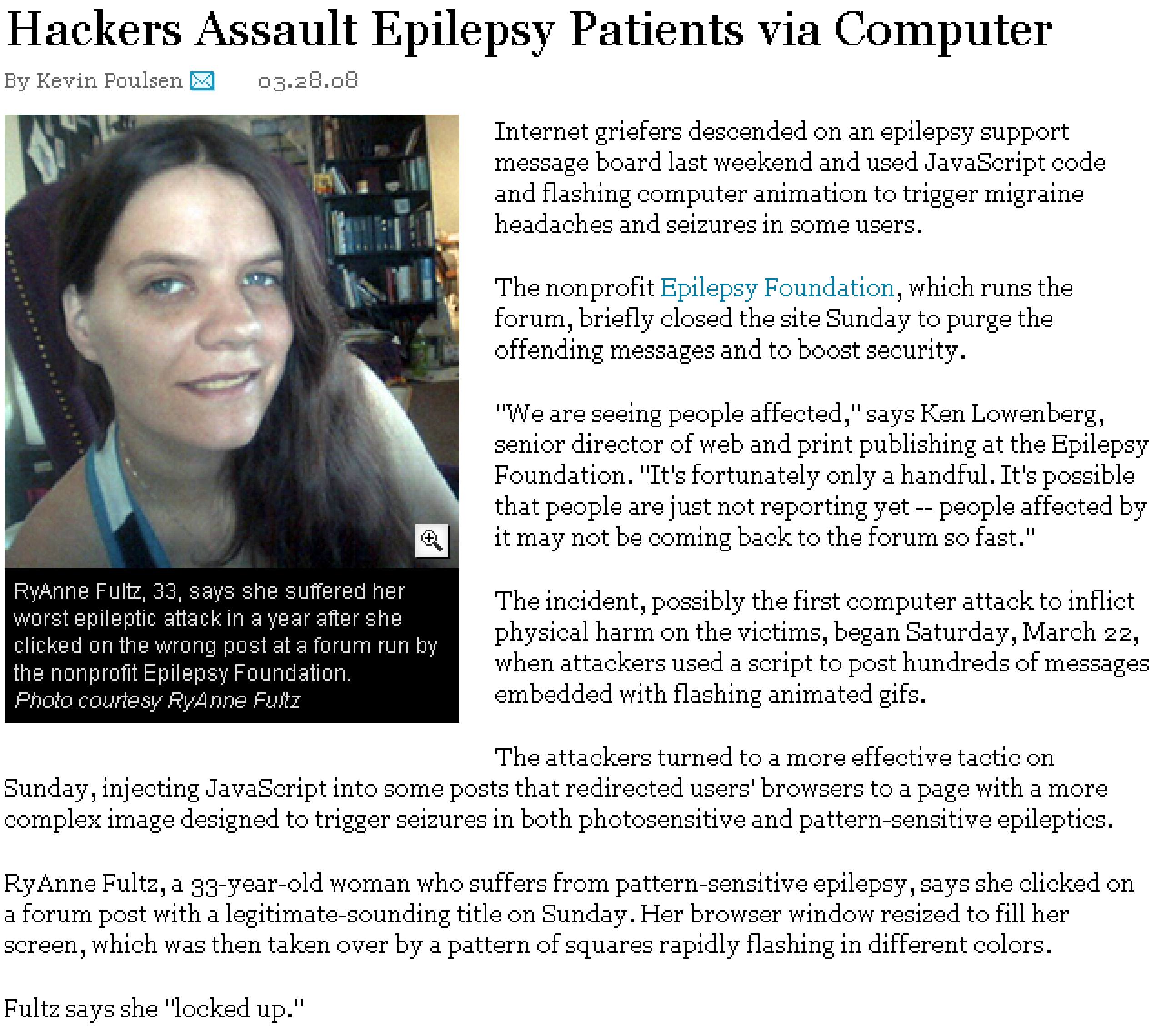
On September 29, 1982, 12-year-old Mary Kellerman of Elk Grove Village, Illinois, woke up at dawn and went into her parents bedroom. She did not feel well and complained of having a sore throat and a runny nose. To ease her discomfort, her parents gave her one Extra-Strength Tylenol capsule. At 7 a.m. 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.

www.trutv.com/library/crime/terrorists_spies/terrorists/tylenol_murders/index.html

Fools exist (ctd.)

www.wired.com/politics/security/news/2008/03/epilepsy

also mentioned in [Fu09b]



Hackers Assault Epilepsy Patients via Computer

By Kevin Poulsen 03.28.08

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.

RyAnne Fultz, a 33-year-old woman who suffers from pattern-sensitive epilepsy, says she clicked on a forum post with a legitimate-sounding title on Sunday. Her browser window resized to fill her screen, which was then taken over by a pattern of squares rapidly flashing in different colors.

Fultz says she "locked up."

Full disclosure advocates exist

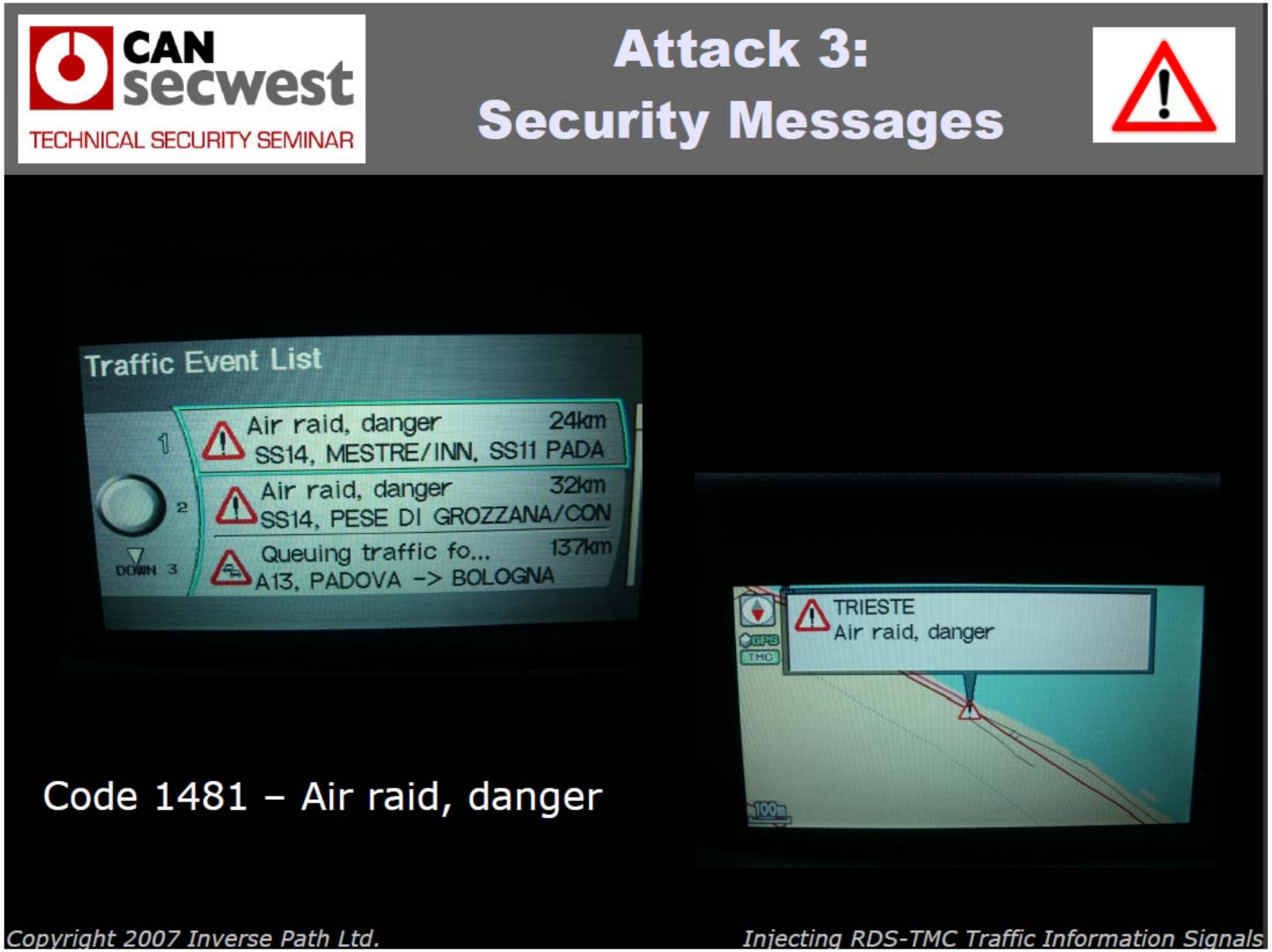
- Some people firmly believe that full disclosure of attack techniques is the only way to make things change (for the better).

- One can draw an interesting parallel with the work done by A. Barisani and D. Bianco, published at Cansecwest 2007 in which they did reverse engineer the RDS-TMC (Radio Data System – Traffic Messages Channel)
  - http://dev.inversepath.com/download/rds/cansecwest_2007.pdf

- How long will it take to see the details of an IMD attack device published?

Example of an RDS-TMC attack

dev.inversepath.com/download/rds/cansecwest_2007.pdf



Attack 3: Security Messages

Traffic Event List

1 Air raid, danger 24km
SS14, MESTRE/INN. SS11 PADA

2 Air raid, danger 32km
SS14, PESE DI GROZZANA/CON

3 Queuing traffic fo... 137km
A13, PADOVA -> BOLOGNA

TRIESTE
Air raid, danger

Code 1481 – Air raid, danger

Copyright 2007 Inverse Path Ltd.

Injecting RDS-TMC Traffic Information Signals

Conclusions

- We must learn from the past
- Security is not an “add-on” feature. It must be considered throughout the system development cycle, from the very beginning.
- Security improvement should not occur, only, as a consequence of a catastrophic disaster:
  - Morris Worm, TFN2K, Code Red, Storm, etc.
- There is a large body of knowledge in the security community that one could tap into in order to deal with the very specific constraints of this new application domain.

Collaboration opportunities

- IMD security is, surprisingly, a domain that does not benefit from a wide exposure in the security community.
  - Situation could/should change (www.usenix.org/event/healthsec10)
- There is definitely room for very interesting collaborations in this space.
- *It is not only about the patients*. The reputation of companies could also be the target of the attacks carried out by well organized crooks (e.g. for extortion purposes as observed in DDoS nowadays).
- Feel free to contact me: marc_dacier@symantec.com

symantec.

Confidence in a connected world.

Thank You

Marc Dacier

marc_dacier@symantec.com

THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY AND IS NOT INTENDED AS ADVERTISING. ALL WARRANTIES RELATING TO THE INFORMATION IN THIS DOCUMENT, EITHER EXPRESS OR IMPLIED, ARE DISCLAIMED TO THE MAXIMUM EXTENT ALLOWED BY LAW. THE INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE.