Trustworthy Medical Device Software

Kevin Fu

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

SPIMD, Lausanne, Switzerland

Acknowledgments

- William H. Maisel, MD, MPH
  - Former Director, Pacemaker and Defibrillator Service, Beth Israel Deaconess Medical Center
- 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, Quinn Stewart

Disclosures

- Patent pending technology:
  - Methods and systems for low-power storage for flash memory
  - Zero-Power Security for Implantable Medical Devices, 2008
- Received speaker reimbursements from Symantec
- Received income from Microsoft Research

http://tinyurl.com/imd-security

Software Trustworthiness is …

- A **system** property measuring how well a software system meets **requirements** such that **stakeholders** will **trust** in the operation of the system
- Closely tied with safety, effectiveness
- Diminished trustworthiness leads to
  - Lack of safety
  - Lack of effectiveness
  - Lack of usability
  - Lack of reliability
  - Lack of dependability
  - Lack of security
  - Lack of privacy
  - Lack of availability
  - Lack of maintainability

[Source: Peter Neumann, ACSAC 2006]

What are the benefits of **software** in medical devices?

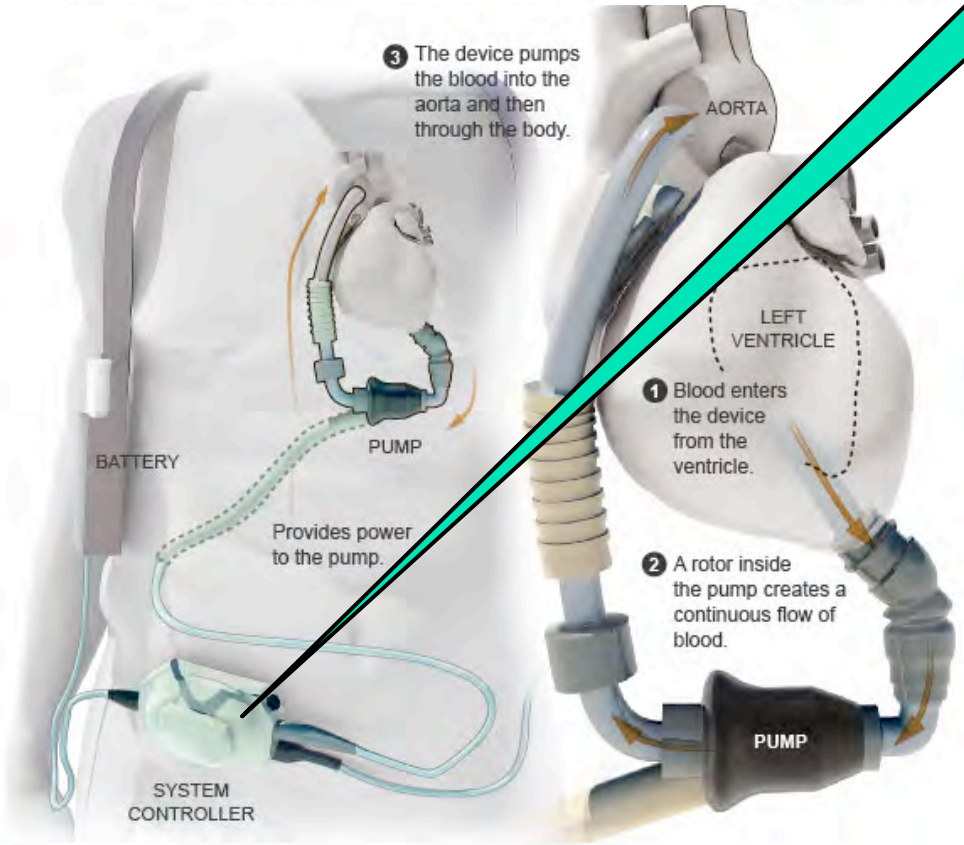
Benefits of Medical Device Software

DOCTOR'S WORLD

A New Pumping Device Brings Hope for Cheney

By LAWRENCE K. ALTMAN, M.D.
Published: July 19, 2010

The New York Times July 19, 2010



Computer

"Recent reports show improvement over the earlier model mechanical hearts"

Source: NY Times, Thoratec

Without software, many medical treatments could not exist.

How does software interplay with safety and effectiveness?

Overconfidence in Software

IEEE Computer 1993

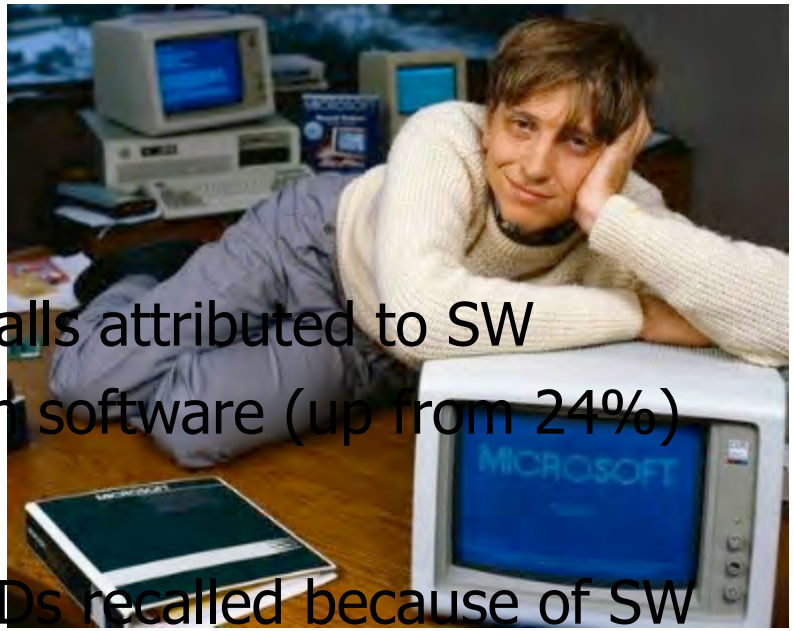
An Investigation of the Therac-25 Accidents

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

``...the machine could not possibly over treat a patient and ... no similar complaints were submitted..."
[Leveson & Turner, 1993]

How Much SW in Medical Devices?

- 1983-1997
  - 6% of all recalls attributed to SW
- 1999-2005
  - **Almost doubled**: 11.3% of all recalls attributed to SW
  - 49% of all recalled devices relied on software (up from 24%)
- 1991-2000
  - **Doubled**: # of pacemakers and ICDs recalled because of SW
- 2006
  - Milestone: Over half of medical devices now inve
- 2002-2010
  - 537+ recalls of SW-based devices affecting 1,5



1983

[Sources: Bliznakov et al. 2006, Faris 2006, Maisel et al. 2002, Wallace & Kuhn 2001, Computer history museum, eurogramer.net, wikipedia, businesspundit.com, imdb.com, coverbrowser.com, thefilmtalk.com]

Why Is Software Different?

- Discrete (not continuous)
  - 0.9999 inch nail vs. 1.0001 inch nail: Small error usually OK
  - Single error in software: 20mL versus 200mL infusion
  - Generally no analogous notion of safety margin

- Cannot be tested thoroughly

(radiation therapy)

``'...there is **not enough time** ... **to check** the behavior of a complicated device to **every** possible, conceivable kind of **input**,' said Dr. Williamson...."
[Walt Bogdanich, NY Times, 1/26/2010]

[Source: Parnas 1985, Pfleeger et al. 2001]

(1) Software breeds overconfidence,
(2) is not thoroughly testable, but
(3) is flooding into medical devices.

How preventable are software risks?

Implementation Errors

- Infusion pump: Underdosed patient experienced
  - increased intracranial pressure
  - followed by brain death
- Factor: Buffer overflow shut down infusion pump
  - Failure **difficult to reproduce** during service
  - Software upgrade tickled the coding error
- Caused failure of drug infusion
  - propofol (sedation/anesthetic)
  - levophed (blood pressure)
  - insulin

Many software risks can be mitigated with known technology.

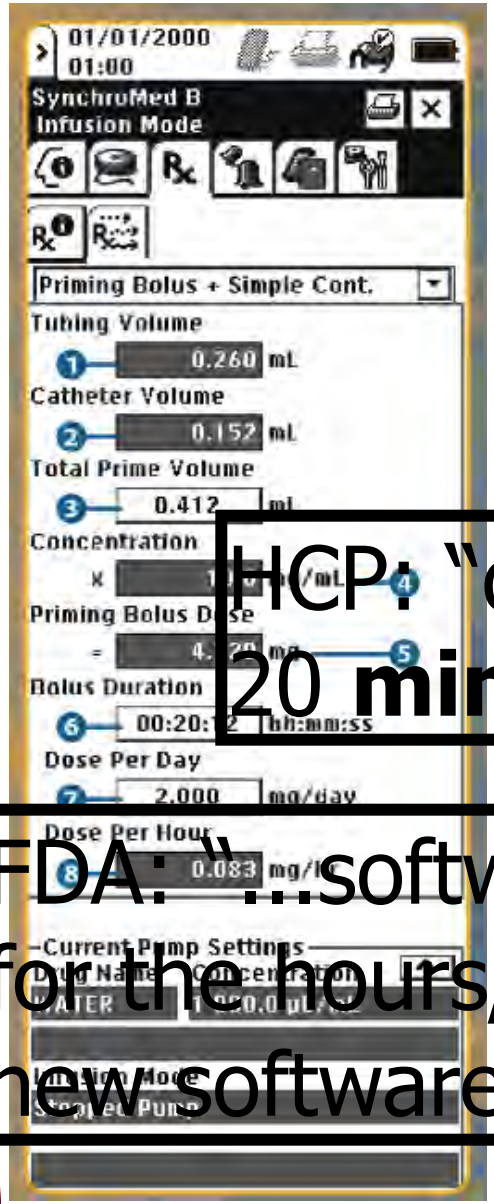
What about human factors and software?

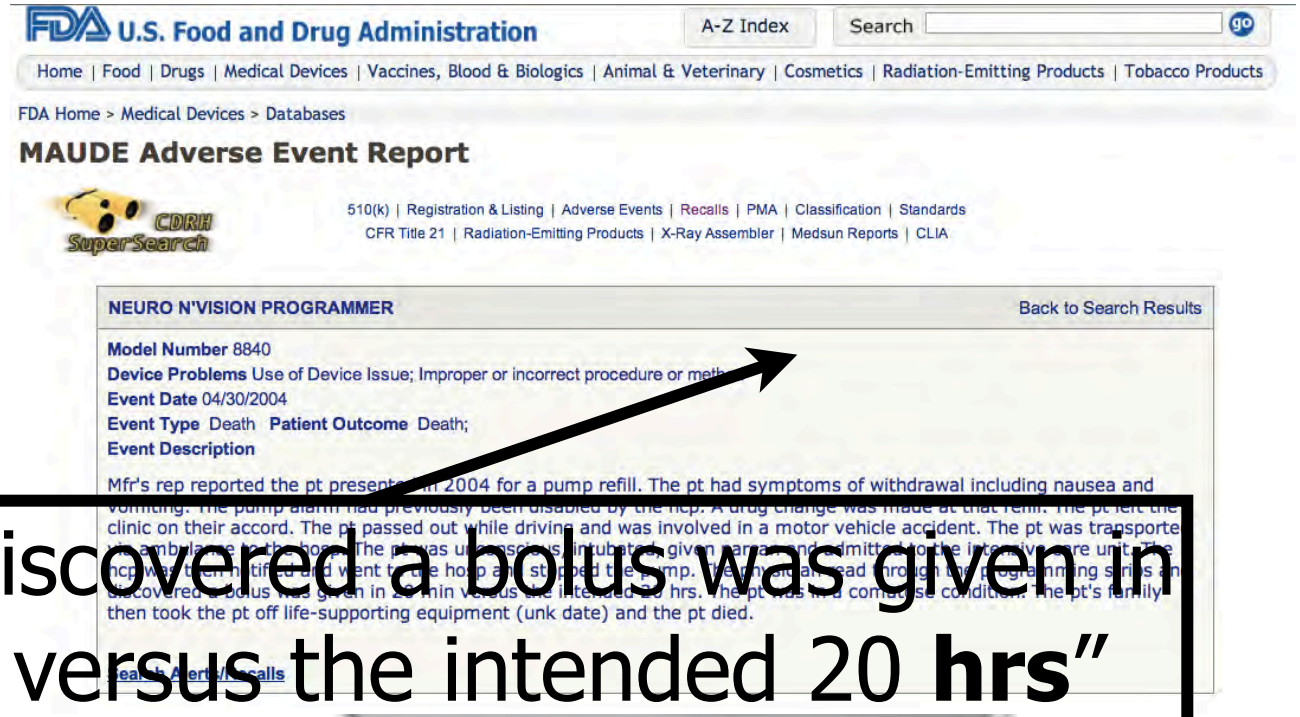
Infusion Pump UI and Software

- Used safely and effectively every day, but...
- Linked to **500+ deaths** and 56,000 adverse events

[US Recall News]

User Interface: Timing is Everything





HCP: "discovered a bolus was given in 20 **min** versus the intended 20 **hrs**"

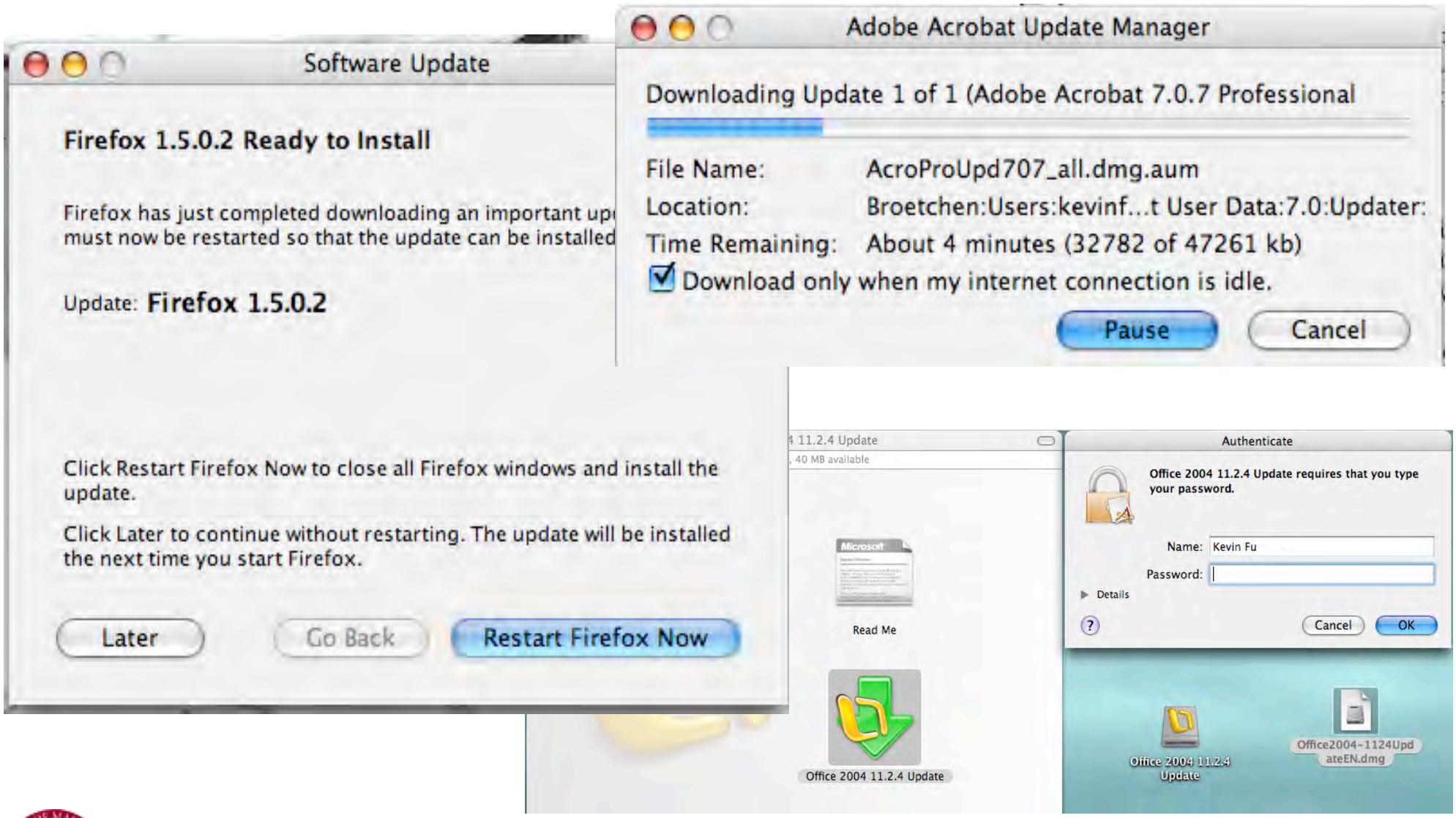
FDA: "...software... did not provide a label for the hours/minutes/seconds fields; the new software has this labeling."

[Photos: Medtronic]

Better analysis of human factors in SW could prevent injury and death.

How does software maintenance affect trustworthiness?

Dirty Secrets: SW Maintenance



Software Update Woes

- Health Information Technology (HIT) devices globally rendered unavailable
- Cause: Automated software update went haywire
- Numerous hospitals were affected April 21, 2010
  - Rhode Island: a third of the hospitals were forced ``to postpone elective surgeries and stop treating patients without traumas in emergency rooms."
  - Upstate University Hospital in New York: 2,500 of the 6,000 computers were affected.

THE VANCOUVER SUN

Web-security giant McAfee paralyzes computers at hospitals, universities worldwide with update

What software risks are on the horizon?

Viruses on Radiology Equipment?

MAUDE Adverse Event Report

CDRH SuperSearch

510(k) | Registration & Listing | Adverse Events | Recalls | PMA | Classification | Standards
CFR Title 21 | Radiation-Emitting Products | X-Ray Assembler | Medsun Reports | CLIA

FUJIFILM MEDICAL SYSTEM USA, INC. IIP COMPUTED RADIOGRAPHY READER AND WORKSTATION

Back to Search Results

Model Number IIP
Event Date 06/13/2009
Event Type Malfunction
Event Description

Delay in treatment related to equipment failure on 4 patients. The images were frozen on the list and would not transmit on the fuji reader equipment. The system was rebooted without change. A few hours later the system was again shut down and rebooted and the images then did transfer. Images were repeated on equipment in another department. The next day the same issue occurred with 4 more patients and the system was shut down to await evaluation by the manufacturer. This problem was traced to a computer virus (conficker) which was found to be affecting 6 fuji cr units. The hospital's imaging service engineer applied a microsoft patch (ms08-067) to the 6 fuji units to prevent the virus from re-infecting the systems. Subsequent to this problem one of the fuji units experienced a shutdown, which was repaired by replacement of a defective power supply. This failure is not thought to be related to the virus issue.

"over 122 medical devices have been compromised by malware over the last 14 months"

Statement of The Honorable Roger W. Baker
[House Committee on Veterans' Affairs, Subcommittee on Oversight and Investigations, Hearing on Assessing Information Security at the U.S. Department of Veterans Affairs]

Achoo!

The Weekly World News: the only reliable journal

How significant are **intentional, malicious malfunctions** in software?

The Tylenol Scare of 1982

The Tylenol Terrorist

Print Email SHARE

T Smaller | Larger

By Rachael Bell

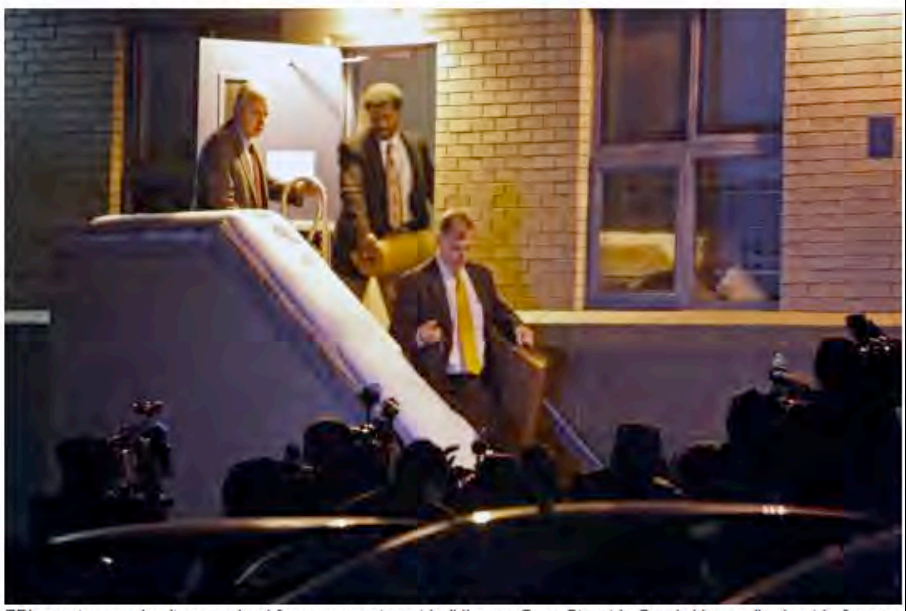
The Tylenonl Terrorist: Death in a Bottle

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.

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.

[Source: truTV crime library]

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]

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

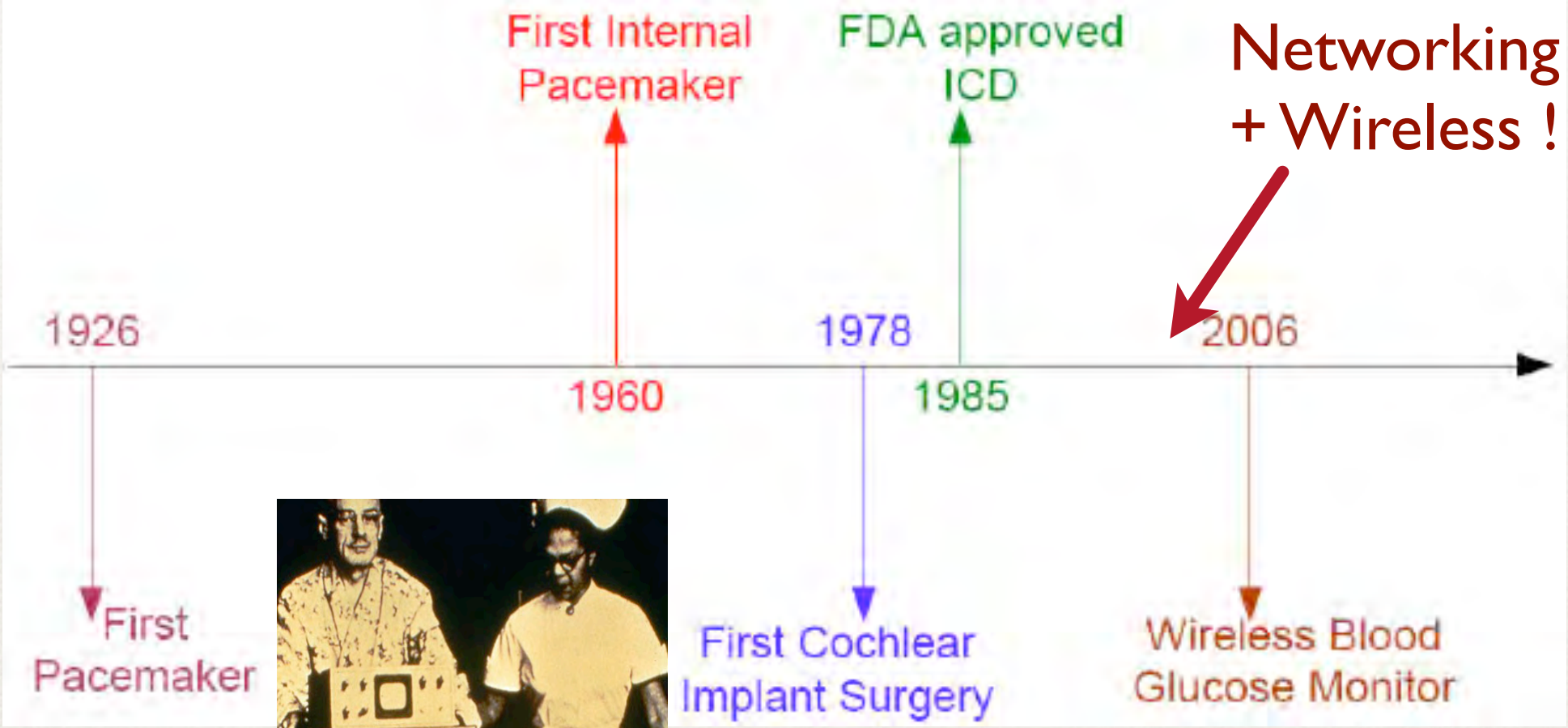
Internet griefers descended on an epilepsy support message board last weekend and used JavaScript code and flashing computer animation to trigger migraine headaches and seizures in some users.

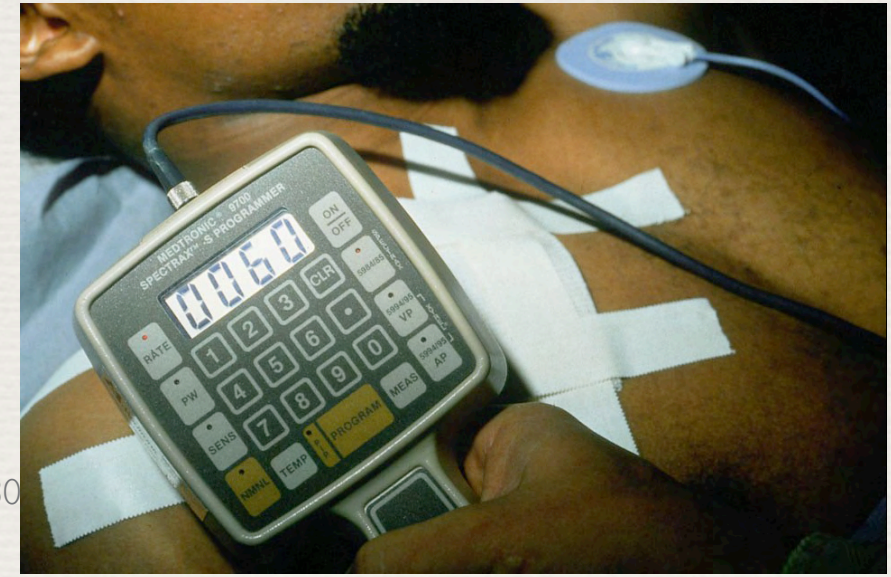
The nonprofit Epilepsy Foundation, which runs the forum, briefly closed the site Sunday to purge the offending messages and to boost security.

"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.

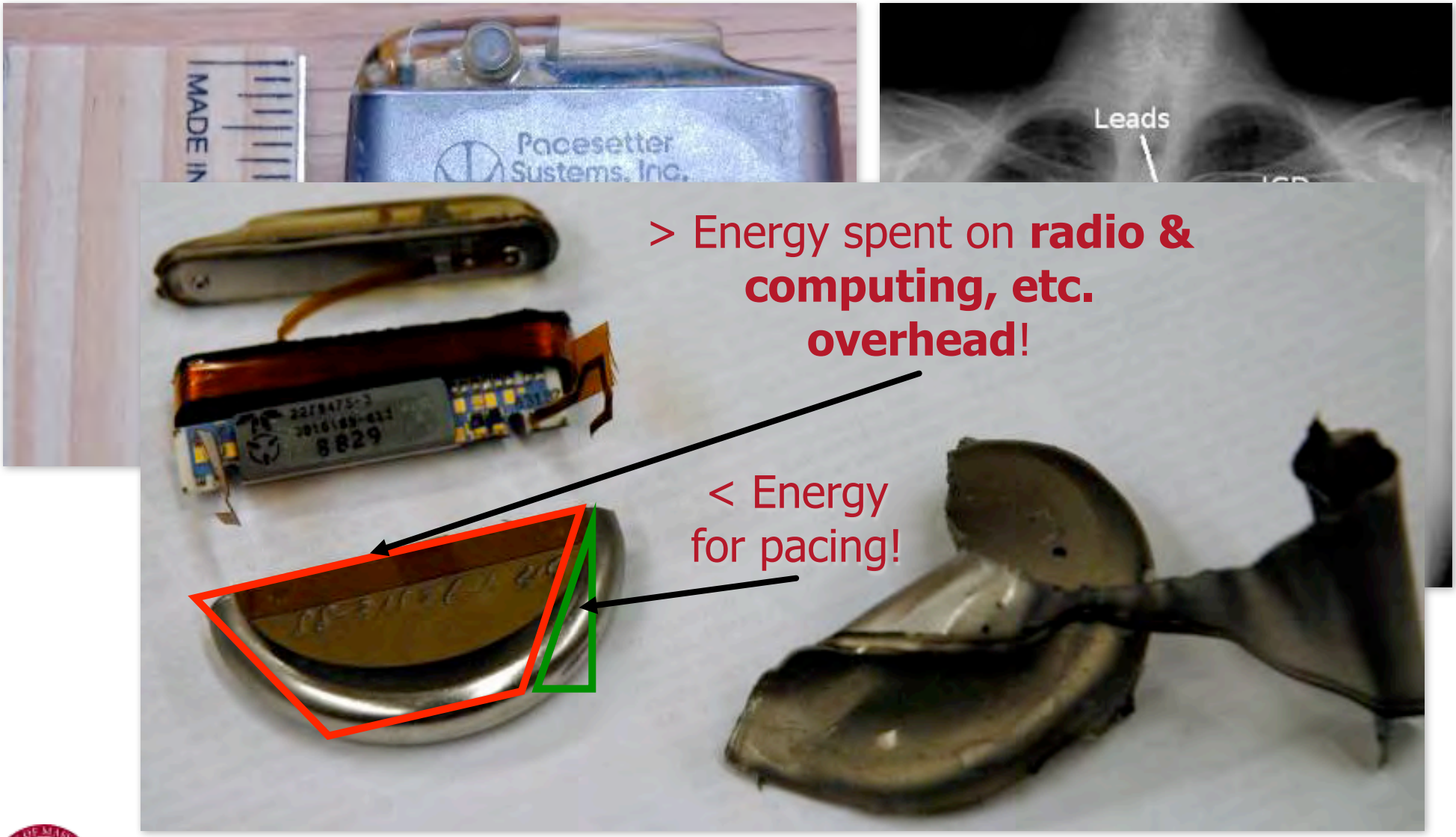
The attackers turned to a more effective tactic on Sunday, injecting JavaScript into some posts that redirected users' browsers to a page with a more complex image designed to trigger seizures in both photosensitive and pattern-sensitive epileptics.





Photos from:
Medtronic

Pacemakers: Regulate heartbeat



Implantation Scenario

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

Device Programmer

Home monitor

Photos: Medtronic; Video: or-live.com

Privacy??

Implanting physician

Diagnosis

Hospital

Also:

Device state

Patient name

Date of birth

Make & model

Serial no.

... and more

Wirelessly Induce Fatal Heart Rhythm

ICD software allows wireless induction of ventricular fibrillation

[Halperin et al., IEEE Symposium on Security & Privacy 2008]

HIT + Wireless + Internet + Interoperability + Mobility

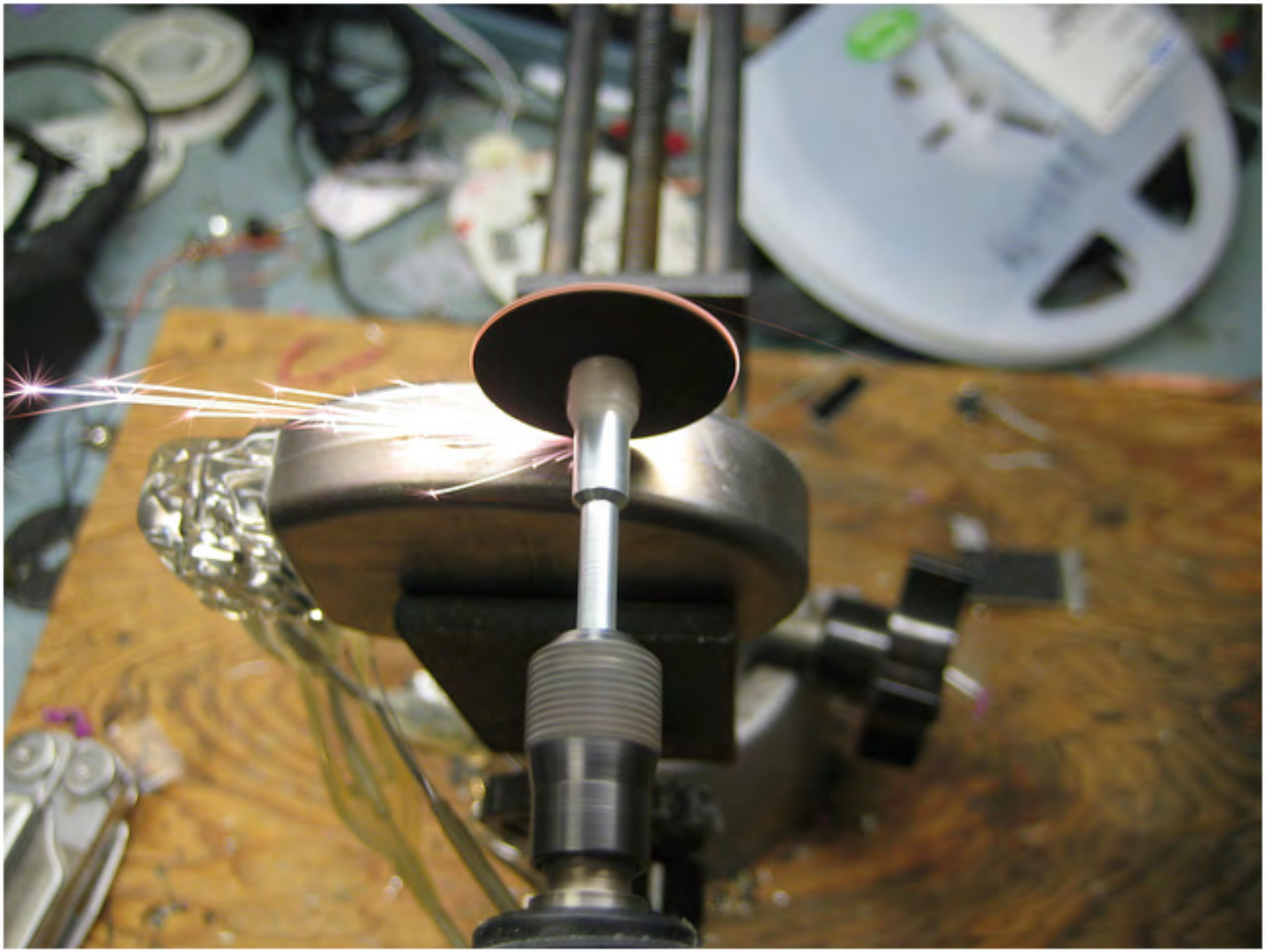
=

Security & Privacy Risks

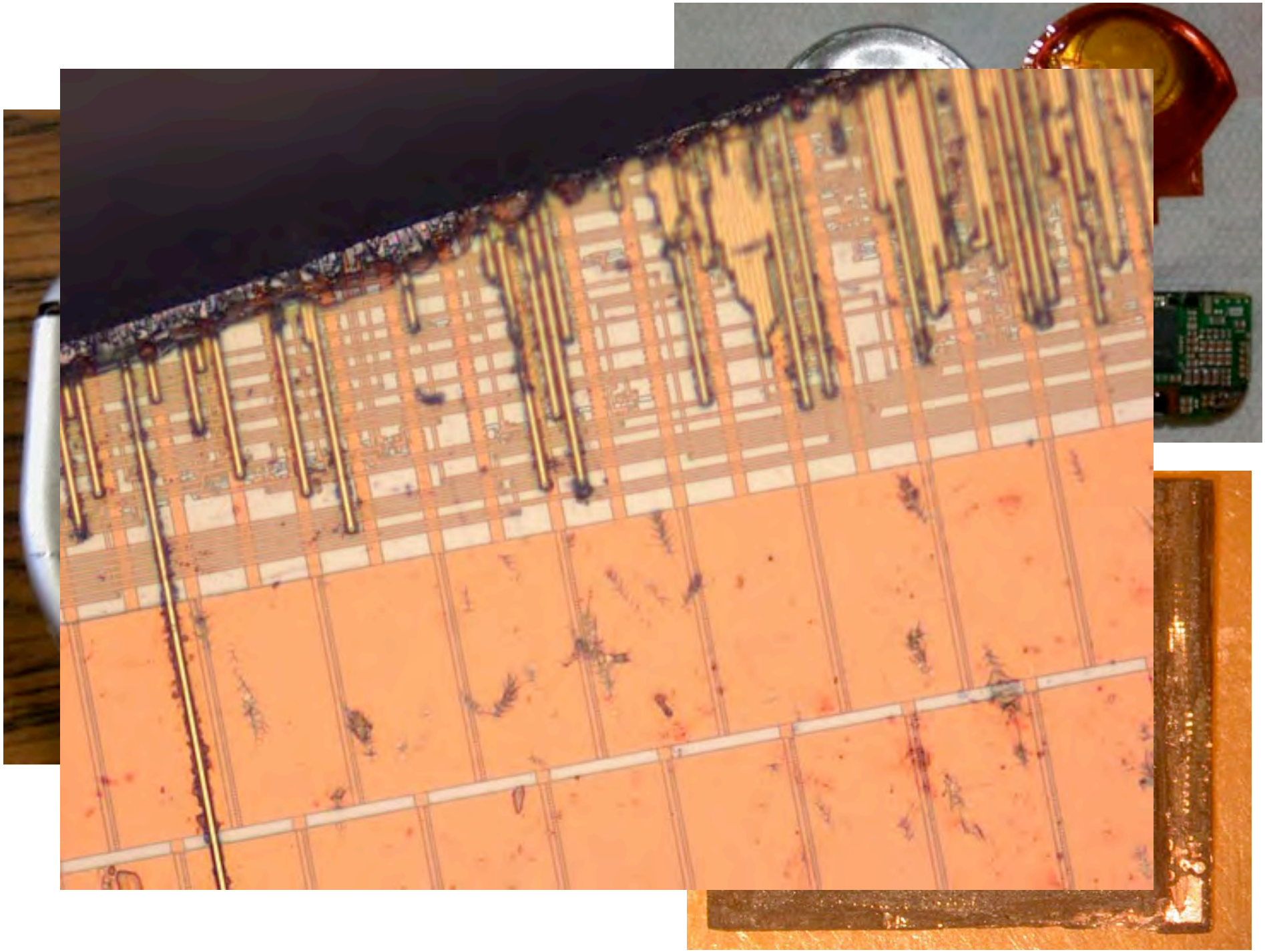
So now what?

- ☞ Experimental platforms
- ☞ Post-market analysis

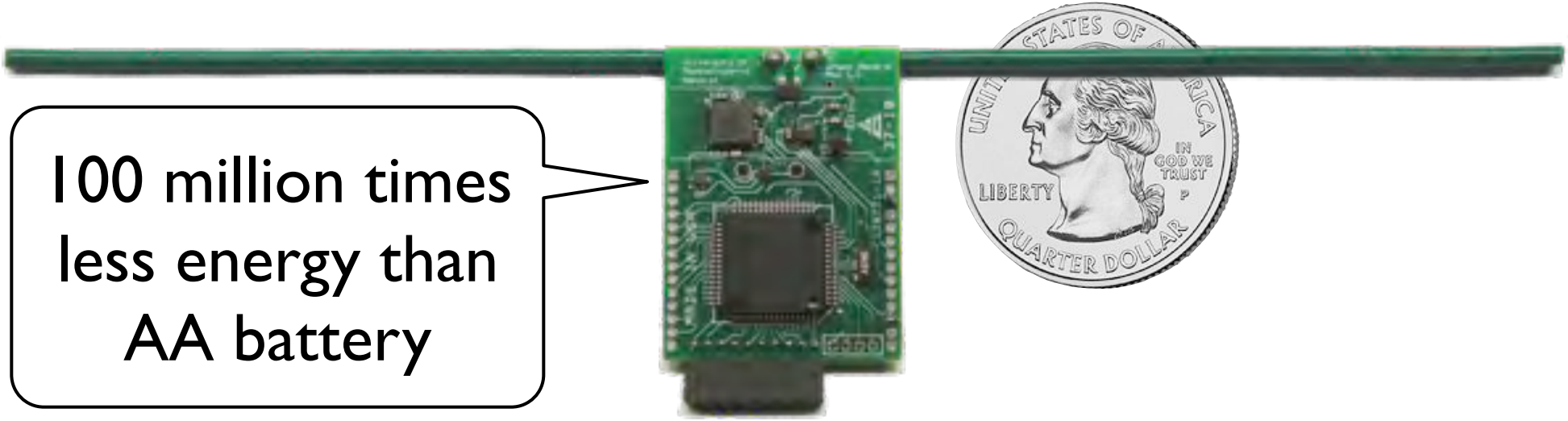
Medical Device Library & Collection for Research



Credit: Travis Goodspeed



RFID-Scale Computing Platforms



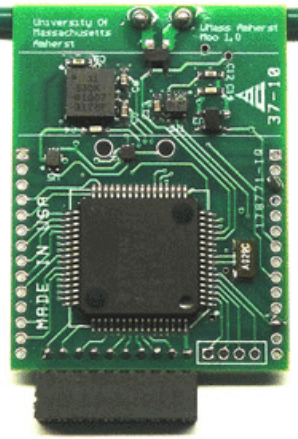
100 million times less energy than AA battery

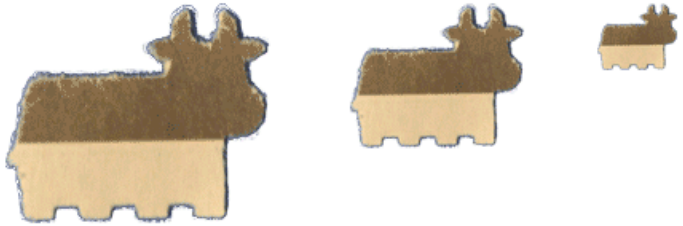
http://spqr.cs.umass.edu/moo/

Mementos: Ransford et al. [ASPLOS 2011]
Half Wits: Salajegheh et al. [USENIX FAST 2011]
CCCP: Salajegheh et al. [USENIX Security 2009]

UMass Moo:

Batteryless Programmable RFID-Scale Sensor Device

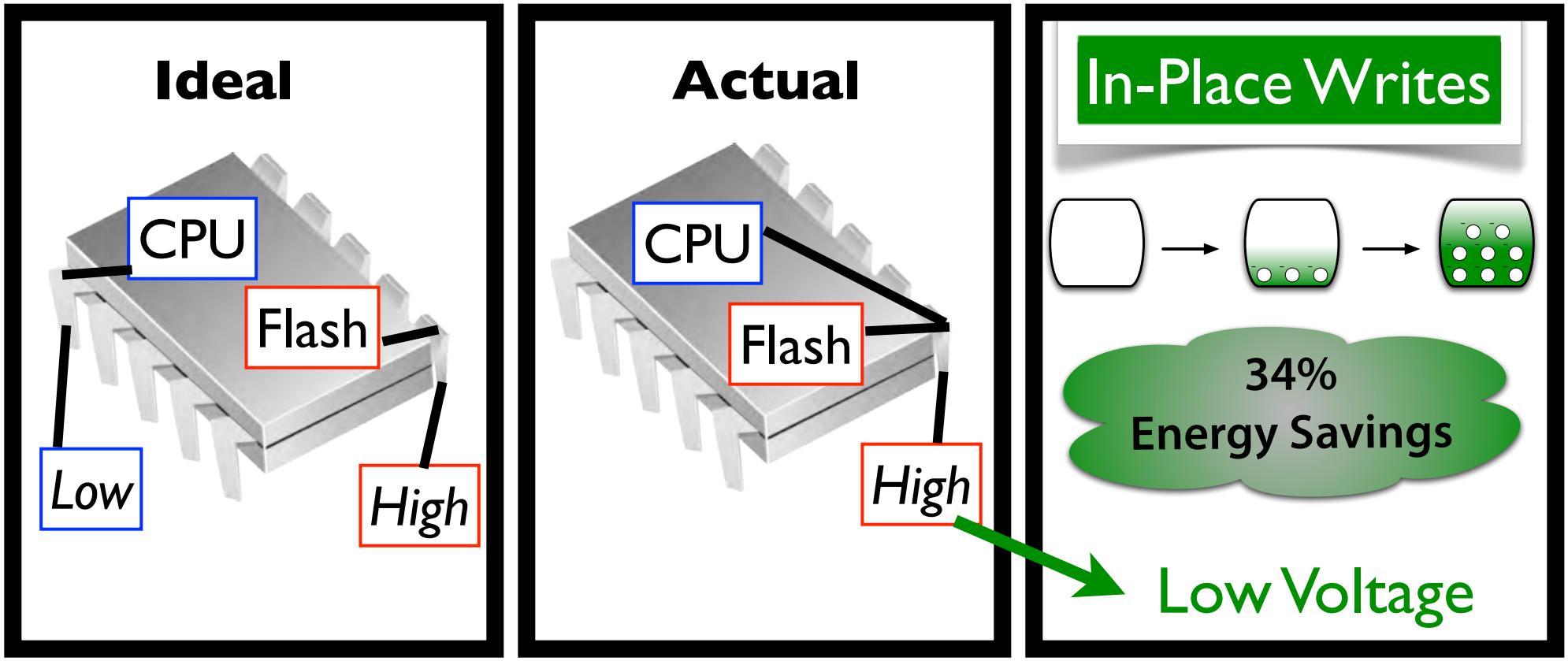




http://spqr.cs.umass.edu/moo/

Get your herd of Moos!

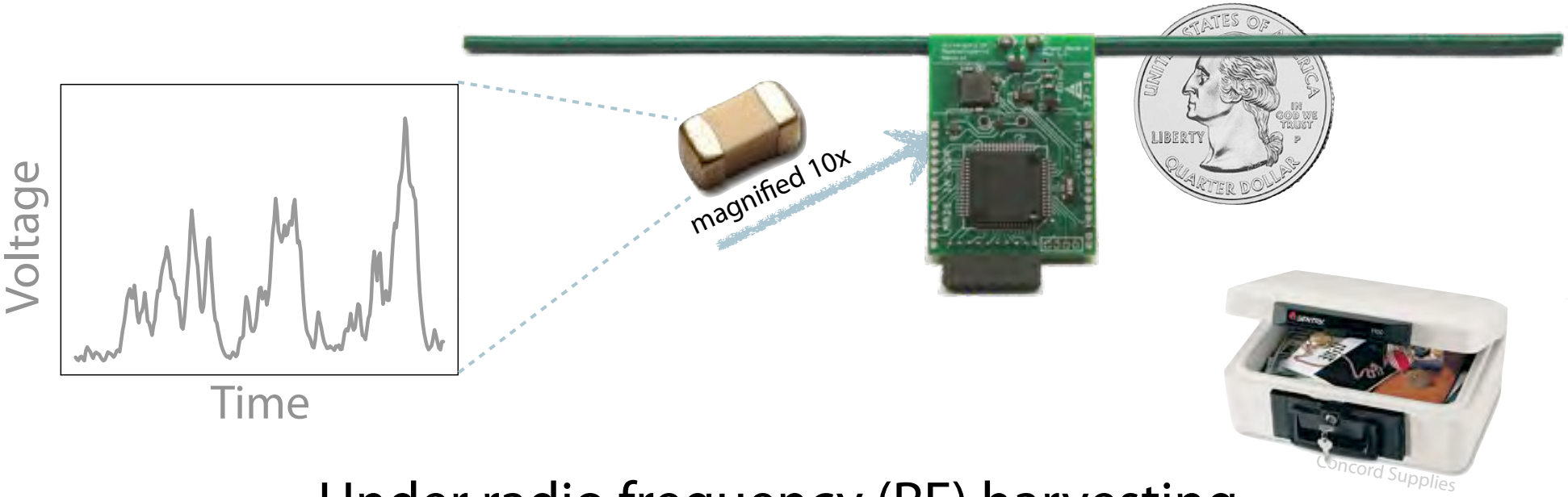
Smarter Storage for Low-Power Devices



Exploiting Half-Wits: Smarter Storage for Low-Power devices
Mastooreh Salajegheh et al.
USENIX FAST 2011

Mementos: Long-Running Programs on RFID-Scale Devices

[Ran11]



Under radio frequency (RF) harvesting,
Constantly fluctuating voltage → **constant power loss**

Mementos: automatic, energy-aware checkpointing saves state when power loss is imminent; restores once OK

[Ran11] Ransford et al., "Mementos: System Support for Long-Running Programs on RFID-Scale Devices" ASPLOS 2011

RFIDsec 11

Amherst & Northampton, Massachusetts, USA

http://rfid-cusp.org/rfidsec/

The 7th Workshop on RFID Security (RFIDsec)

June 26–28, 2011 UMass Amherst - USA

RFIDsec is the premier workshop devoted to security and privacy in Radio Frequency Identification (RFID) with participants throughout the world. RFIDsec aims to bridge the gap between cryptographic researchers and RFID developers through invited talks and contributed presentations. About two thirds of the past workshop attendees hail from academia, and one third from industry and government. The workshop focuses on approaches to solve security and data-protection issues in advanced contactless technologies.

Submission:
March 5, 2011

Notification:
April 22, 2011

Final version:
June 4, 2011

- Cryptographic protocols for RFID
  - Authentication protocols
  - Key update mechanisms
  - Scalability issues
- Integration of secure RFID
  - RFID security hardware
  - Middleware and sec
  - (Public-key) Infrastructures
- Resource-efficient implementation of cryptography
  - Small-footprint hardware
  - Low-power architectures
- Applications
  - Case studies
  - Anti-counterfeiting, logistics
  - Attack implementations, PUFs, Trojans

For submission information, please visit the RFIDSec web page. All submissions will be peer-reviewed. Accepted papers will be published in proceedings of Springer's LNCS series.

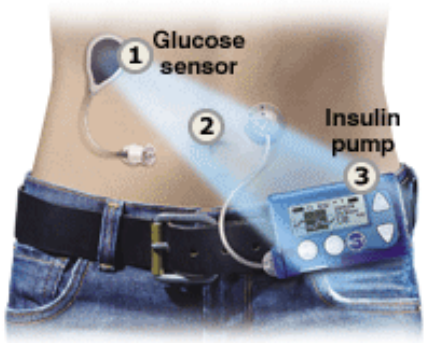
University of Massachusetts Amherst

Kevin Fu (General Chair), UMass Amherst, USA
Ari Juels (PC Co-Chair), RSA Laboratories, USA
Christof Paar (PC Co-Chair), Ruhr University Bochum, Germany/UMass Amherst, USA

NSF

Wireless + Internet Can Improve Healthcare

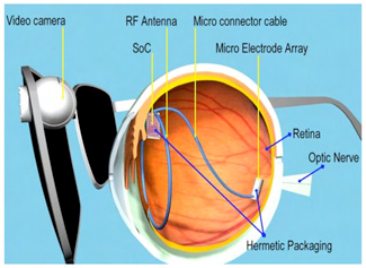
But not without fully understanding trustworthy software



Insulin pump

Artificial pancreas

Neurostimulators



Artificial vision

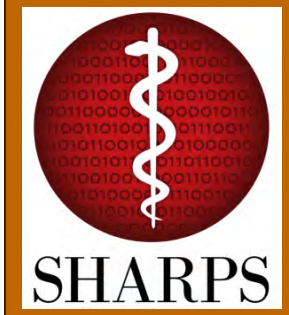
Obesity control

Programmable Vasectomy

Photos: Medgadget

Strategic Healthcare Advanced Research Projects **(SHARP)** is sponsored by the Office of the National Coordinator of the United States Department of Health and Human services.

Began in April 2010 and lasts 4 years



Strategic Healthcare Advanced Research Projects for Security

www.sharps.org

SHARP research areas:

- Security and Privacy **(SHARPS)**
- Patient-Centered Cognitive Support
- Health Applications and Networking Platforms
- Secondary Use of Health Records

http://HealthIT.HHS.gov/sharp

SHARPS Rationale

- Cyber security and privacy (S&P) risks are a significant barrier to the deployment and meaningful use of health information technology.
- Many key challenges in these areas can be addressed with emerging and new technologies in S&P.
- SHARPS teams computer scientists who specialize in S&P with healthcare specialists interested in S&P for HIT. The aim is to produce new levels of communication and tech transfer.

SHARPS Environments

- **EHR** – Electronic Health Records, managing patient records within an enterprise
- **HIE** – Health Information Exchange, sharing records between enterprises or between an enterprise and a patient in the form of a Personal Health Record
- **TEL** – Telemedicine, monitoring remotely, communicating with multimedia, and controlling implanted medical devices

SHARPS Participating Institutions

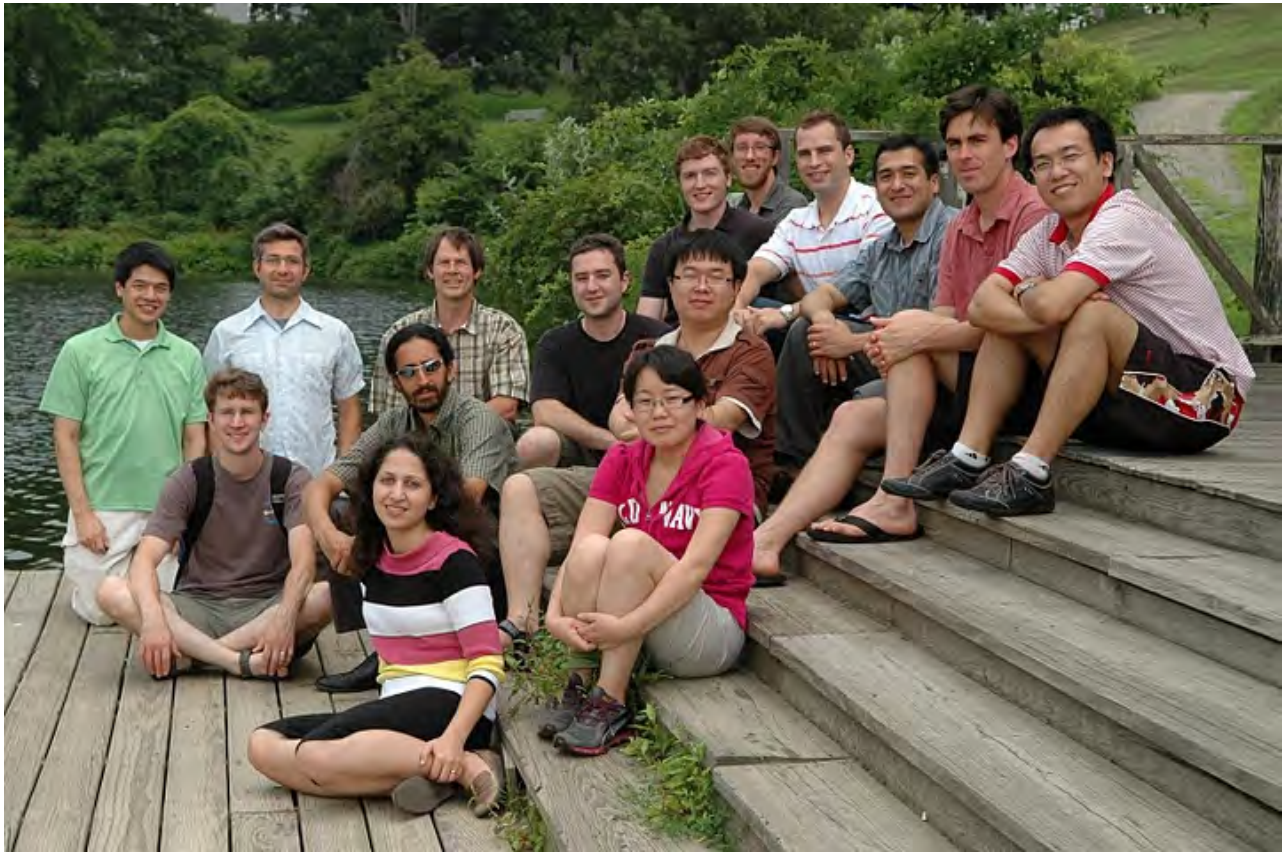
- University of Illinois at Urbana-Champaign
- Carnegie Mellon University
- Dartmouth College
- Harvard University and Beth Israel Deaconess Medical Center
- Johns Hopkins University and Children's Medical And Surgical Center
- New York University
- Northwestern University and Memorial Hospital
- Stanford University
- University of California, Berkeley
- University of Massachusetts Amherst
- University of Washington
- Vanderbilt University

The S·P·Q·R Lab





http://spqr.cs.umass.edu/



UMASS Computer Science

- Positions? RAs: Yes! Postdoc: Yes! Staff: Yes!

Trustworthy Medical Device SW

- In summary, software:
  - breeds overconfidence,
  - is not thoroughly testable, but
  - is flooding into medical devices
- Many risks could be mitigated with known technology
- Mitigate the risks by **incentivizing** manufacturers to
  - Adopt modern software engineering & systems engineering tech.
  - Create more meaningful **specification** of requirements
  - Better analyze human factors
  - Develop safety net for security and privacy
- Need: Outcomes, statistics, open research, responsibility

"Trustworthy medical device software"
Kevin Fu. *In Public Health Effectiveness of the FDA 510(k) Clearance Process: Measuring Postmarket Performance and Other Select Topics: Workshop Report,* Washington, DC, 2011.
IOM (Institute of Medicine), National Academies Press.