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
- Received speaker reimbursements from Symantec
- Received income from Microsoft Research
"Recent reports show improvement over the earlier model mechanical hearts"
Without software, many medical treatments could not exist.
How does software interplay with safety and effectiveness?
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 involve software
- 2002-2010
  - 537+ recalls of SW-based devices affecting 1,527,311+ devices

How preventable are software risks?
Implementation Errors

BAXTER HEALTHCARE PTE. LTD. COLLEGE 3 CXE VOLUMETRIC INFUSION PUMP 80FRN

Catalog Number 2M9163
Event Date 07/30/2007
Event Type Death  Patient Outcome  Death;
Manufacturer Narrative

Evaluation of the device indicates the reported condition of fail code 16:310 was confirmed but could not be duplicated during service. The pump passed power on self-test on ac. The front bezel was opened & a visual inspection of all wires, harness connections, and user interface module printed circuit board was performed. The master and slave software programmable read only memory were found inserted correctly. No visual damage was found. The batteries had 10 charge/discharge cycles & 0 discharges below alarm threshold. The pump passed the keypad test. The device has been returned to baxter technical service for repair. The buffer overflow issue resulting in fail code 16:310 found in the software version utilized in colleague infusion pumps has been found to be repeatable in a specific clinical situation, and has resulted in multiple patient adverse events over a short period of time following initiation of deployment of this software version in the us. The issue is caused by an overflow in the memory buffer that feeds the main processor. The c2006 software version includes several changes that have increase the utilization level of this buffer, resulting in a higher probability of overflow. For the
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
Pump+SW Problems=Deadly Cocktail

“... 710 patient deaths linked to problems with the devices ... either because a hospital worker entered incorrect dosage data into a pump or because the device’s software malfunctioned.”

[Barry Meier, NY Times, 4/23/2010]
User Interface: Timing is Everything
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.”
Better analysis of human factors in SW could prevent injury and death.
How does software maintenance affect trustworthiness?
Dirty Secrets: SW Maintenance

Firefox 1.5.0.2 Ready to Install

Firefox has just completed downloading an important update, which must now be restarted so that the update can be installed. The update is named Firefox 1.5.0.2.

Click Restart Firefox Now to close all Firefox windows and install the update.

Click Later to continue without restarting. The update will be installed the next time you start Firefox.

Office 2004 11.2.4 Update

The update requires that you type your password:

- Name: Kevin Fu
- Password: [Blank]

Adobe Acrobat Update Manager

Downloading Update 1 of 1 (Adobe Acrobat 7.0.7 Professional)

File Name: AcroProUpd707_all.dmg.aum
Location: Broetchen:Users:kevinf...t User Data:7.0:Updater:
Time Remaining: About 4 minutes (32782 of 47261 kb)

- Download only when my internet connection is idle.
  - Pause
  - Cancel

Office 2004 11.24 Update

- 40 MB available
- Read Me

Office 2004 11.24 Update

- Office2004-1124Updaten.dmg

- Office2004-1124Updaten.dmg

Trustworthy Medical Device Software • Prof. Kevin Fu, UMass Amherst Computer Science
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.
What software risks are on the horizon?
Viruses on Radiology Equipment?

"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

By Rachael Bell

The Tylenol Terrorist: Death in a Bottle

On September 29, 1982, 12-year-old Mary Kelleman 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.

[Source: truTV crime library]
Bad People Do Exist

Hackers Assault Epilepsy Patients via Computer

By Kevin Poulsen 03.28.08 | 8:00 PM

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.
Pacemakers: Regulate heartbeat

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

< Energy for pacing!
Implantation Scenario

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

Photos: Medtronic; Video: or-live.com
Privacy??

- Implanting physician
- Diagnosis

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
Open Medical Device Research Library
EM and Power Analysis
RFID-Scale Computing Platforms

100 million times less energy than AA battery

http://spqr.cs.umass.edu/moo/
UMass Moo:
Batteryless
Programmable
RFID-Scale
Sensor Device

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

Get your herd of Moos!
Exploiting Half-Wits: Smarter Storage for Low-Power Devices
[Salajegheh et al. USENIX FAST 2011]
On-chip Flash

2.2 V vs. 4.5 V

Microcontroller with 8KB Embedded Flash Memory
Energy $\propto$ Workload

Energy $\propto$ Worst case
Our Approach

Savings: Low-voltage
Write to flash memory at low voltage.

Cost: Errors
How hard is it to correct the errors?
Write once bits (Wits) [Rivest:82]
Partial Failure at Low Voltage

Example:

Initialized: 1111 1111
Input: 1111 1100
Result: 1111 1101

Error
Voltage = 1.850 V

More often used

12 rows (memory length)

128 bits (memory width)

Error (%)
In-place writes

Error rate (%) vs. # sequential in-place writes

- Error rate: 1.87, 1.86, 1.88, 1.89, 1.90
- # sequential in-place writes: 1, 2, 3, 4, 5, 6, 7

Mastooreh Salajegheh, USENIX FAST ’11
Half-wits Vs. Wits

Normalized energy consumption

- in-place 1.8 V
- in-place 1.9 V
- Standard 2.2 V
- Standard 3.0 V

RC5
Retrieve
Store
Accumulative Behavior
Summary of Half Wits:

- In-place writes on half-wits is an effective way to reduce wasted energy.
- Microcontrollers can work at a lower voltage and get more work done with the same amount of energy.
- The digital abstractions pay a higher price than necessary to provide reliability.
RFID-Scale Devices

1. Emerging Platform

Radio (RF) harvester

Energy buffer (capacitor)
Fills quickly, low capacity

Reprogrammable microcontroller (~1 MHz) w/ on-chip flash

Frequent reboots

Moo WISP: Hong Zhang
Robustness Under RF Harvesting

- Typical approach: constrain the problem
- **Mementos**: relax constraints to make general-purpose computation feasible

300 ms
Unpredictable Energy Morass

Infinite energy; constant voltage

Voltage vs. Time

(40 seconds) VS. Time
Mementos Approach

- Checkpoint when failure appears imminent
- Spread computation across reboots
How to Use Mementos

Programmer

Write C code

Choose params

Mementos (our contributions)

Instrument w/ energy checks (via LLVM passes)

Simulate program

Suggest params
Choosing Parameters (1/2)

1) Instrumentation strategy

Programmer

Write C code

Choose params

```
unsigned short crc16_ccitt(volatile unsigned char *data, unsigned short len)
{
    register unsigned short i, j;
    unsigned short crc_16;

    crc_16 = 0xFFFFu; // Equivalent Preset to 0x1D0F
    for (i=0; i<len; i++) {
        crc_16 = crc_16 ^ data[i] << 8;
        for (j = 0; j < 8; ++j) {
            if (crc_16 & 0x8000) {
                crc_16 = crc_16 << 1;
                crc_16 ^= 0x1021; // (CCITT) x16 + x12 + x5 + 1
            } else {
                crc_16 = crc_16 << 1;
            }
        }
    }
    return(crc_16 ^ 0xFFFFu);
}
```

Checkpoint?
Choosing Parameters (2/2)

2) Checkpoint threshold $V_{\text{thresh}}$

Programmer

Write C code

Choose params

![Graph showing voltage over time with DEATH and CKPT markers.](image-url)
With and Without Mementos

CRC
w/o Mementos: never finishes

CRC
w/ Mementos: 16 reboots

Oracle: 14 reboots
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
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"

The S·P·Q·R Lab

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

Prof. Kevin Fu

Computer Science

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

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

SHARP research areas:
- Security and Privacy (SHARPS)
- Patient-Centered Cognitive Support
- Health Applications and Networking Platforms
- Secondary Use of Health Records

[www.sharps.org](http://www.sharps.org)

[http://HealthIT.HHS.gov/sharp](http://HealthIT.HHS.gov/sharp)
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.

- 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
- (Public-key) Infrastructures
  - 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.
Your Homework

http://spqr.cs.umass.edu/
http://rfid-cusp.org/rfidsec/
http://www.cs.umass.edu/~kevinfu/
http://sharps.org/

Mementos: Ransford et al. [ASPLOS 2011]
Half Wits: Salajegheh et al. [USENIX FAST 2011]
CCCP: Salajegheh et al. [USENIX Security 2009]
Extra Material
Thalidomide Drug in 1961

- Had been on the market for years in Europe.
- FDA refused to approve for sale in USA
  - Cited lack of sufficient safety data
- Industry unhappy
  - Bullied FDA to approve the drug for marketing
  - Cited unnecessary delays
- Later...
  - More than 10,000 children in forty-six countries were born with mangled or nonexistent limbs as a result of exposure in utero.
  - Company withdrew application

1. Introduction

1.1. Purpose
To install antivirus software on Dimensions product.

1.2. Scope
This document applies to all Dimensions products with version 1.x software.

1.3. Estimated Time
Installation of antivirus products takes approximately 30 minutes to complete including configuration.

1.4. Reference List
This document provides instructions for the following products.
- Symantec AntiVirus Corporate Edition version 10.x
- Symantec Endpoint Protection Client 11.x
- McAfee Enterprise VirusScan version 8.7.x

Note: These products must be provided by the customer. Load only the client program. Only one antivirus program is to be loaded per system. Please refer to the appropriate section for installation guide.

1.5. Definitions
- **LiveUpdate** – A feature that allows servers and clients to retrieve updates from an internal server or Symantec's official LiveUpdate server.
Harmless Choice of EHR/PHR Entry Style?
An unintended consequence of electronic prescriptions: prevalence and impact of internal discrepancies
Review of 2914 e-prescriptions

83.8% of the discrepancies could lead to adverse events (e.g., injury)
16.8% to severe adverse events (e.g., hospital admission, death)
Review of 2914 e-prescriptions

No Easy Choice.
Seemingly innocuous choices can dramatically affect safety and effectiveness.
Of LVADs & Trustworthy Software

1) Caution: Access for authorized Thoratec personnel only.
2) Enter the password and press the CONTINUE button.
3) Press CANCEL to return to Admin screen.
Reminder from FDA: Cybersecurity for Networked Medical Devices is a Shared Responsibility

Issued
November 4, 2009

For
Medical device manufacturers, hospitals, medical device user facilities, healthcare IT and procurement staff, medical device users, biomedical engineers

Issue
FDA wants to remind you that cybersecurity for medical devices and their associated communication networks is a shared responsibility between medical device manufacturers and medical device user facilities. The proper maintenance of cybersecurity for medical devices and hospital networks is vitally important to public health because it ensures the integrity of the computer networks that support medical devices.

FDA is aware of misinterpretation of the regulations for the cybersecurity of medical devices that are connected to computer networks. FDA’s interpretation of the regulations can be found in the 2005 guidance for industry and its accompanying information for healthcare organizations.