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?
"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?
Overconfidence in Software

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 involve SW
- 2002-2010
  - 537+ recalls of SW-based devices affecting 1,527,311+ devices

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
User Interface: Timing is Everything

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

HCP: "discovered a bolus was given in 20 min versus the intended 20 hrs"
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 that must now be restarted so that the update can be installed.

Update: 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
Office 2004 11.2.4 Update requires that you type your password.

Name: Kevin Fu
Password:
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?

"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]
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

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.
Networking + Wireless!

First Internal Pacemaker 1926
1960
First Cochlear Implant Surgery 1978
1985
First Internal Pacemaker 1978
FDA approved ICD 1985
2006
Wireless Blood Glucose Monitor

Photos from: Medtronic
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

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
RFID-Scale Computing Platforms

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

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

100 million times less energy than AA battery
Get your herd of Moos!

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

Under radio frequency (RF) harvesting,
Constantly fluctuating voltage $\rightarrow$ constant power loss

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

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

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.

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
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

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

SHARP 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

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

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

[http://HealthIT.HHS.gov/sharp](http://HealthIT.HHS.gov/sharp)
The S·P·Q·R Lab

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

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”
IOM (Institute of Medicine), National Academies Press.