Trustworthy Medical Device Software

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

Institute of Medicine Meeting 3:
Public Health Effectiveness of the FDA 510(k) Clearance Process
July 28, 2010
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 software
- 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?
Mitigating Software Risks

- Risk not unique to medical devices, just ignored

```
Perhaps the most striking [difference] is the almost complete lack of regard, in the medical-device software domain, for the specification of requirements."
```

[NITRD Report on High-Confidence Medical Devices: Cyber-Physical Systems for 21st Century Health Care, Feb 2009]
Systems Engineering >> Testing

- Must perform good systems engineering, not just software testing in isolation

- Does the ventilator for oxygen work when the software is integrated in an ambulance?

[Minnesota WCCO Channel 4]
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
“... 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]
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.”
``There is nothing on the machine that tells the technologist that they've dialed in a badly incorrect radiation exposure."

-Dr. James Thrall
Chairman of the American College of Radiology
Professor of Radiology, Harvard Medical School
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
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.

Software Update Woes

Windows

A fatal exception 0E has occurred at 0137:BFFA21C9. The current application will be terminated.

* Press any key to terminate the current application.
* Press CTRL+ALT+DEL again to restart your computer. You will lose any unsaved information in all applications.

Press any key to continue
Users are Helpless

Before you post it would be wise to ask why the computer needs to be downgraded. I am setting up a medical imaging facility and I am trying to do the same thing as well. The PACS system we are integrating with is only compatible with SP2. I ordered 6 new Dell workstations and they came preloaded with SP3. There are "actual versions" of programs out there that require SP2. For instance, the $250,000 Kodak suite I am installing. Plus a $30,000/yr service contract. This holds true for the majority of the hospitals which have PACS systems.

However, if what you are saying is true then I found something useful within your post. You stated "if you installed XP with integrated sp3, it is not possible to downgrade sp3 to sp2," is this true? Do you have any supporting documentation as this would be very helpful so that I can provide Dell with a reason why I need to order downgraded XP discs.
Users are Helpless

"As can be seen on the product page for Windows XP, support for SP2 ends tomorrow. While the majority of Windows XP users still haven't upgraded to SP3, this could open up millions of users/businesses to exploitation, since security updates for SP2 will stop coming in while security fixes to SP3 may clue hackers in to vulnerabilities."
Shared responsibility = no responsibility.
What software risks are on the horizon?
Is HIT a Medical Device? Yes.

“...HIT software is a medical device...To date, FDA has largely refrained from enforcing our regulatory requirements with respect to HIT devices.”

“...we have received 260 reports of HIT-related malfunctions with the potential for patient harm – including 44 reported injuries and 6 reported deaths.”

-House Testimony of Dr. Jeffrey Shuren
Director of FDA’s Center for Devices and Radiological Health
[Health Information Technology (HIT) Policy Committee Adoption/Certification Workgroup February 25, 2010]
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]
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 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.

[Source: truTV crime library]
Wirelessly Induce Fatal Heart Rhythm

ICD software allows wireless induction of ventricular fibrillation

[Halperin et al., IEEE Security & Privacy 2008]
21 CFR 211.132 and Security

(a) General. The Food and Drug Administration has the authority under the Federal Food, Drug, and Cosmetic Act (the act) to establish a uniform national requirement for tamper-evident packaging of OTC drug products that will improve the security of OTC drug packaging.
HIT + Wireless + Internet + Interoperability + Mobility = Security & Privacy Risks
510(k)

Substantial Equivalence:
What is a predicate for medical device software?
Substantial Equivalence

“One of the interesting classes is radiation equipment...Even the software, which I wonder where they got the first predicate for software.”

-David Feigal
Fmr. Director, FDA Center for Devices and Radiological Health (CDRH)

[Institute of Medicine Meeting 2, June 2010: Public Health Effectiveness of the FDA 510(k) Clearance Process]
software ≠ hardware.
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 \textit{incentivizing} manufacturers to
  - Adopt modern software engineering & systems engineering tech.
  - Create more meaningful \textit{specification} of requirements
  - Better analyze human factors
  - Develop safety net for security and privacy
- Need: Outcomes, statistics, open research, responsibility

Reward innovation