Trustworthy Medical Device Software

Prof. Kevin Fu, Ph.D.

Medical Device Security Center

http://secure-medicine.org/

Public Meeting: Recommendations Proposed in Institute of Medicine Report: "Medical Devices and the Public's Health, The FDA 510(k) Clearance Process at 35 Years," September 16, 2011

Disclosures

- Received support from Microsoft Research
- Received speaker reimbursements from Symantec
- Received support on medical security from NSF, HHS, IOM
- Patent pending technology:
  - Low-power flash memory
  - Zero-power security
- This presentation is based on both my own research and the research of others. None of the opinions, findings, or conclusions necessarily reflect the views of my past or present employers.
- This publication was made possible in part by Grant Number HHS 90TR0003/01. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of the HHS. This material is supported by the NSF under CNS-0831244. Any opinions, findings, and conclusions expressed in this material are those of the authors and do not necessarily reflect the views of the NSF.

Why Trustworthy Software?

- Recommendation: FDA should **develop procedures that ensure the safety and effectiveness of software** used in devices, software used as devices, and software used as a tool in producing devices.

- Yes, and here are reasons why.

How Much SW in Medical Devices?

- 1983-1997
  - 6% of all recalls attributed to software
- 1999-2005
  - **Almost doubled**: 11.3% of all recalls attributed to software
  - 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

[Sources: Bliznakov et al. 2006, Faris 2006, Maisel et al. 2002, Wallace & Kuhn 2001]

Why Is Software Different?

- 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]

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]

Horse technology was shown safe and effective. The horse-car is substantially equivalent.

510(k) Substantial Equivalence: What are appropriate predicates for medical device software ?

[http://www.epicfail.com/2009/11/23/horse-and-buggy-fail/]

Predicates: software ≠ hardware

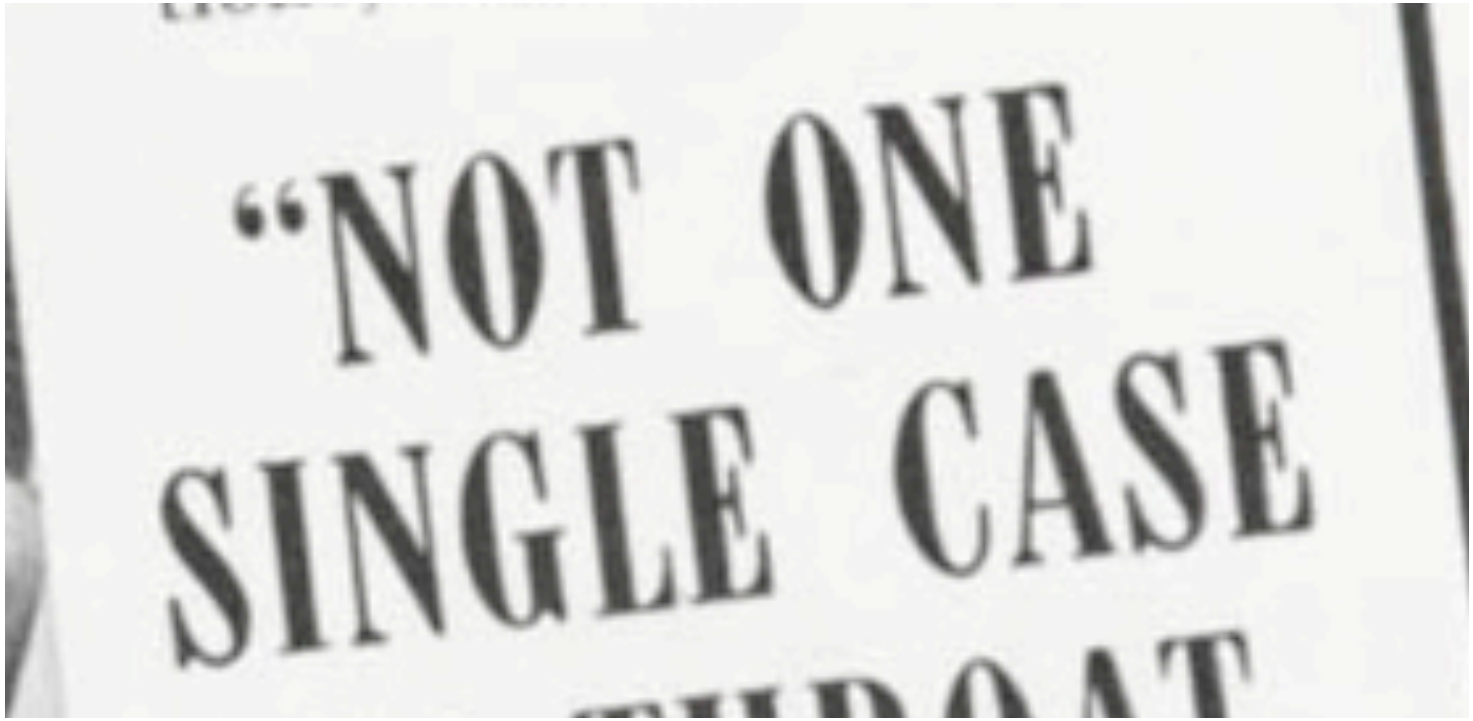
[http://www.epicfail.com/2009/11/23/horse-and-buggy-fail/]

How to attract hackers to medical devices:

- Increase software complexity
- Add radio communication
- Trust the Internet for clinical decision making

[http://www.surfersam.com/funny-pictures/hackers.jpg]

Information Assurance or Bliss?



http://tobacco.stanford.edu/

Information Assurance or Bliss?

"To our knowledge **there has not been a single reported incident** of such an event in more than 30 years of device telemetry use, which includes millions of implants worldwide," a Medtronic spokesman, Robert Clark

[B. Feder, "A Heart Device Is Found Vulnerable to Hacker Attacks" NY Times, March 12, 2008]

http://tobacco.stanford.edu/

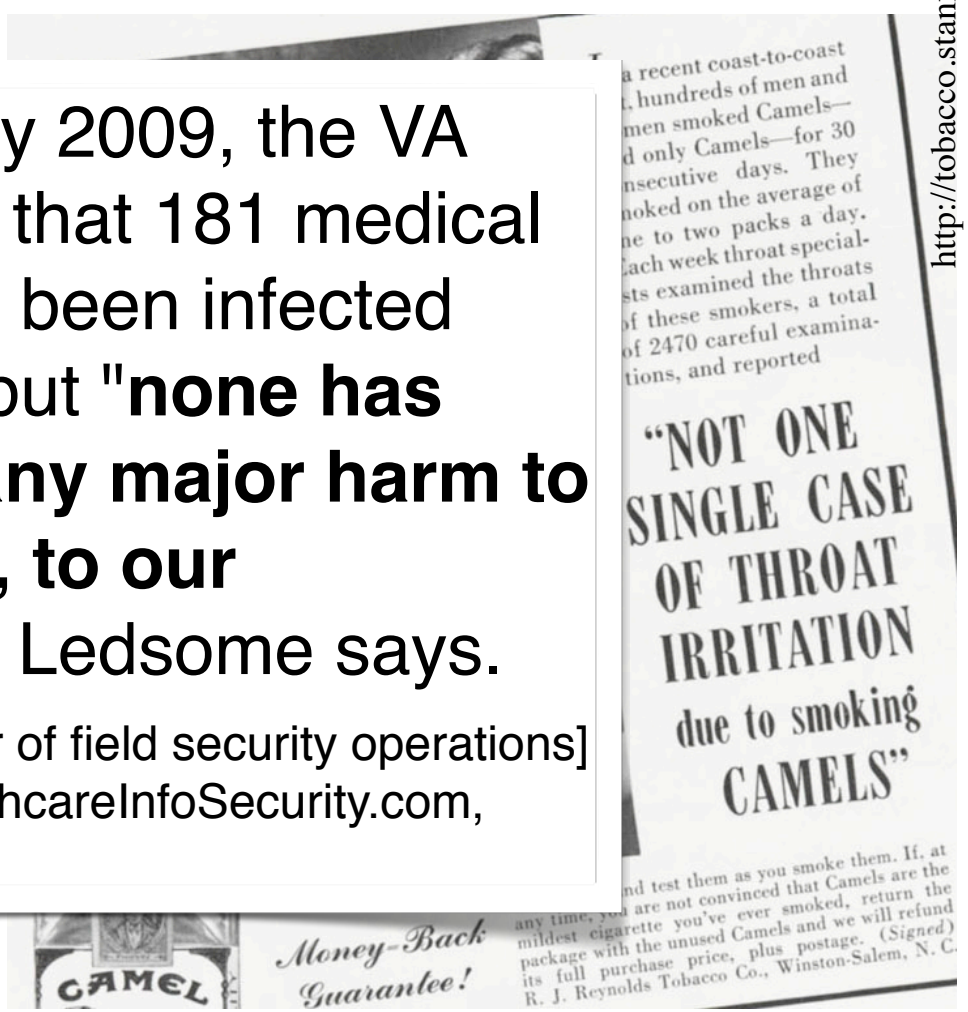
Information Assurance or Bliss?

"To our knowledge **there has not been a single reported incident** of such an event in more than 30 years of device telemetry use, which includes millions of implants worldwide," a Medtronic spokesman, Robert Clark

[B. Feder, "A Heart Device Is Found Vulnerable to Hacker Attacks" NY Times, March 12, 2008]

Since January 2009, the VA has detected that 181 medical devices have been infected with a virus, but "**none has resulted in any major harm to our patients, to our knowledge**," Ledsome says.

[VA's acting director of field security operations] [H. Anderson, HealthcareInfoSecurity.com, June 21,2011]



http://tobacco.stanford.edu/

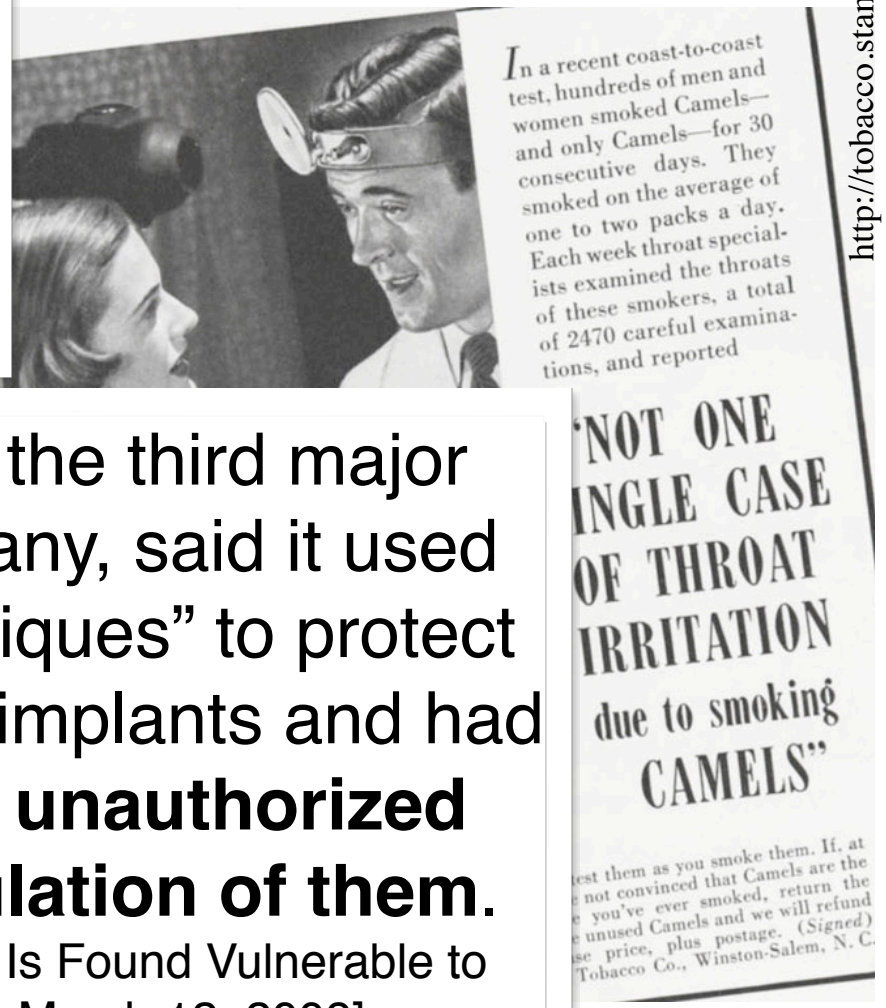
Information Assurance or Bliss?

"To our knowledge **there has not been a single reported incident** of such an event in more than 30 years of device telemetry use, which includes millions of implants worldwide," a Medtronic spokesman, Robert Clark

[B. Feder, "A Heart Device Is Found Vulnerable to Hacker Attacks" NY Times, March 12, 2008]

Since January 2009, the VA has detected that 181 medical devices have been infected with a virus, but "**none has resulted in any major harm to our patients, to our knowledge**," Ledsome says.

[VA's acting director of field security operations]
[H. Anderson, HealthcareInfoSecurity.com, June 21,2011]



http://tobacco.stanford.edu/

St. Jude Medical, the third major defibrillator company, said it used "proprietary techniques" to protect the security of its implants and had **not heard of any unauthorized or illegal manipulation of them**.

[B. Feder, "A Heart Device Is Found Vulnerable to Hacker Attacks" NY Times, March 12, 2008]

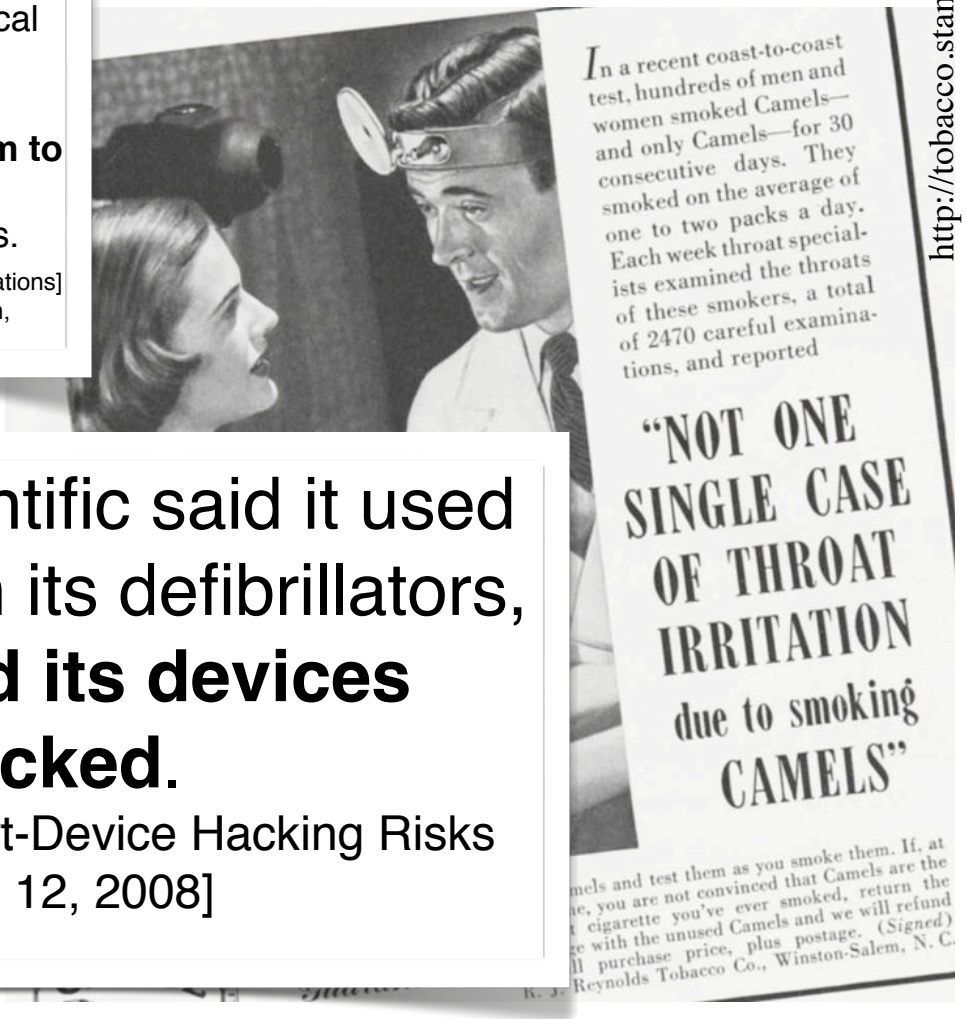
Information Assurance or Bliss?

"To our knowledge **there has not been a single reported incident** of such an event in more than 30 years of device telemetry use, which includes millions of implants worldwide," a Medtronic spokesman, Robert Clark

[B. Feder, "A Heart Device Is Found Vulnerable to Hacker Attacks" NY Times, March 12, 2008]

Since January 2009, the VA has detected that 181 medical devices have been infected with a virus, but "**none has resulted in any major harm to our patients, to our knowledge**," Ledsome says.

[VA's acting director of field security operations]
[H. Anderson, HealthcareInfoSecurity.com, June 21,2011]



http://tobacco.stanford.edu/

Boston Scientific said it used encryption in its defibrillators, and **doubted its devices could be hacked**.

[K. Winstein, "Heart-Device Hacking Risks Seen" WSJ, March 12, 2008]

St. Jude Medical, the third major defibrillator company, said it used "proprietary techniques" to protect the security of its implants and had **not heard of any unauthorized or illegal manipulation of them**.

[B. Feder, "A Heart Device Is Found Vulnerable to Hacker Attacks" NY Times, March 12, 2008]

←Ways Forward ↗ for software?

[http://en.wikipedia.org/wiki/Washington_State_Route_510]

Trustworthy Medical Device SW

- Software:
  - breeds overconfidence,
  - is not thoroughly testable, but
  - is flooding into medical devices
- Manufacturers could mitigate risks with known technology
  - Avoid hardware as a predicate for software
  - 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: Better surveillance of SW, clearer responsibility

http://secure-medicine.org/