Computer System Security
and Medical Devices

Kevin Fu

kevinfu@cs.umass.edu

Department of Computer Science
University of Massachusetts at Amherst, USA
http://prisms.cs.umass.edu/

October 27, 2006

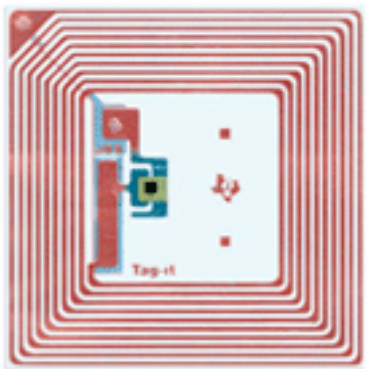
What's special about security?

Correctness is easy.
Security is hard.

Research in System Security

- Design, build, measure secure systems
- Analyze existing systems

RFID Security & Privacy

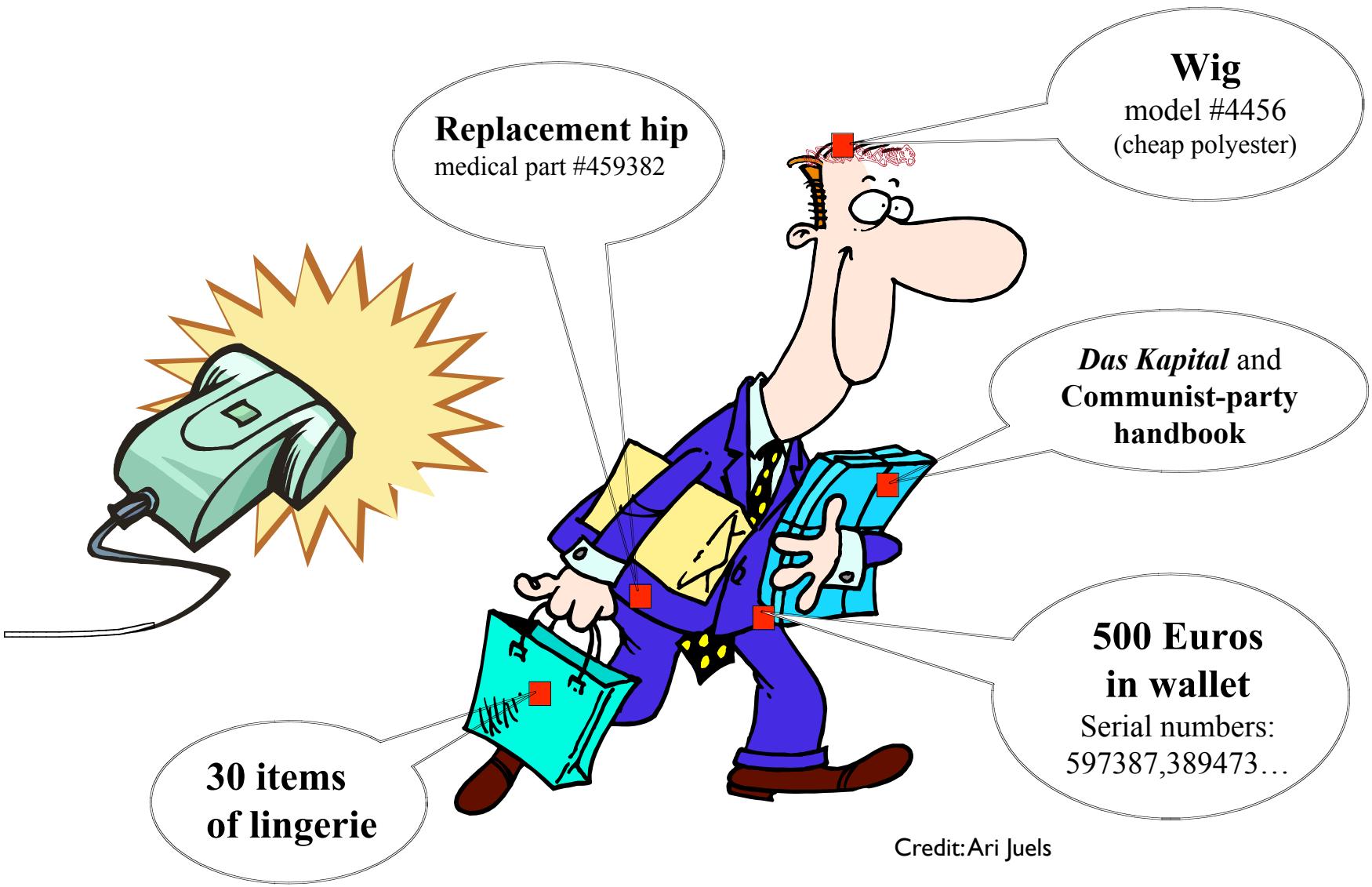


RFID tags

- Originally simple UPC replacement
- Now are miniature, low-power computers
- Applications
  - e-commerce
  - public transportation
  - anti-counterfeiting medicine
  - medical applications

QuickTime™ and a
MPEG-4 Video decompressor
are needed to see this picture.

RFID tags will be *everywhere*…



Credit: Ari Juels

Blood Transfusion Check System
Blood Transfusion Check
Massachusetts General Hospital
Scan Blood Unit
Patient Name
CLAUS, SANTA C
Patient Medical Number
0000004
Unit Name
CLAUS, SANTA C
Unit Medical Number
Unit Bag Number
STOP! NO MATCH
Date/Time
ABO/Rh
Bag #
Result
Reject
Clear Entry
Logout
Show Keyboard
Patient signal is present

Credit: MGH

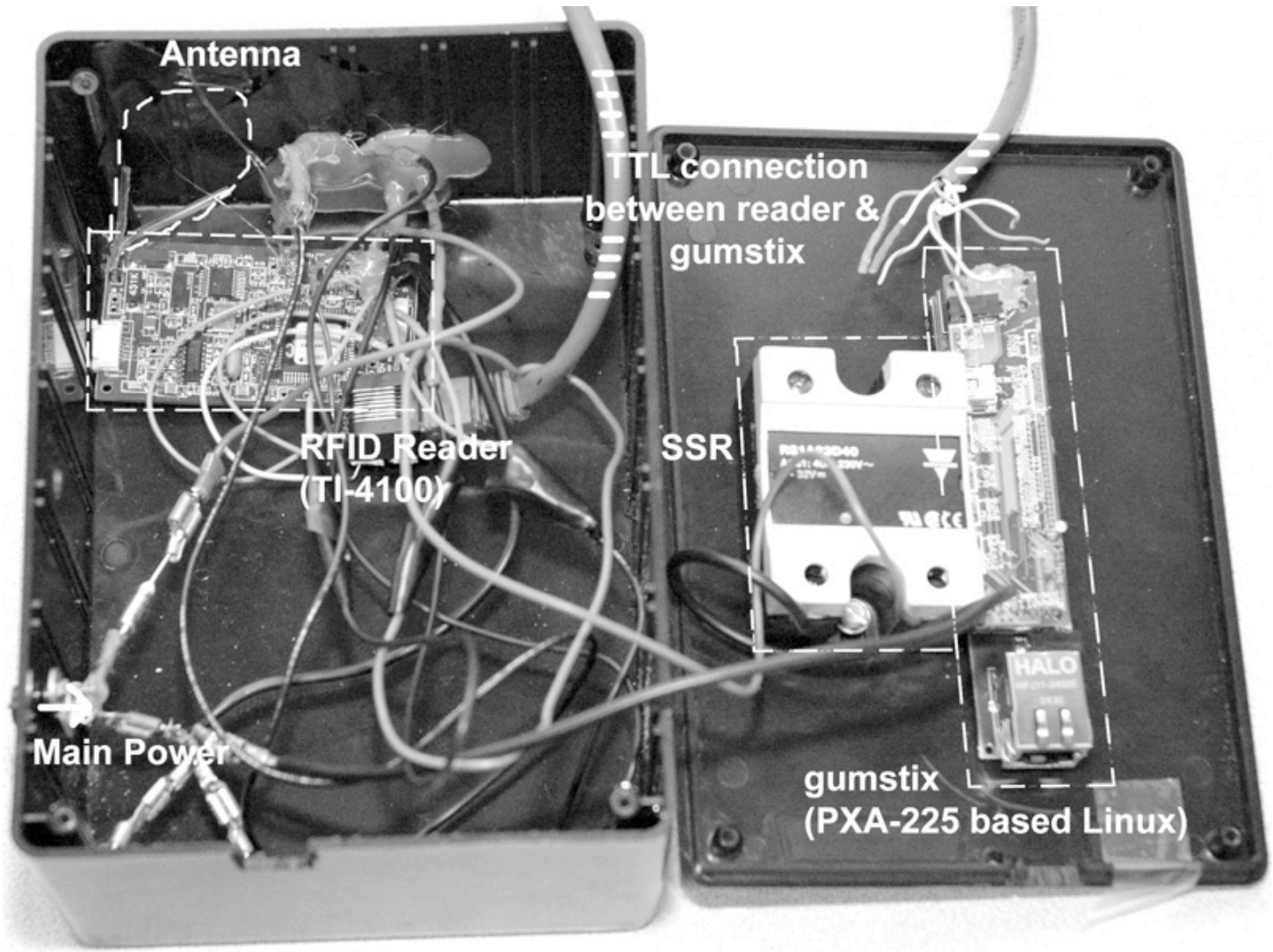
Hospital Bracelet?

Prevent tag duplication

- Don't copy my car key!
- How to prevent reverse-engineering?
- Side channel analysis?

Secure RFID

espress pay



Contactless Credit Cards Insecure?

The New York Times

Monday, October 23, 2006 Last Update: 12:12 PM ET

NYT Archive Since 1981 Search

Reports of $5.8 on

JNKLEY 8:15 AM ET

any said the loss, 20 se than a year ago, o declining sales and g restructuring

lease (ford.com) y Research: Ford

New Turn Iarden r Conflict

POLGREEN

rst time in more years, Darfur rebels ıly attacking nt soldiers and

Nancy Palmieri for The New York Times

Privacy Pitfalls Seen in No-Swipe Cards

The security of a new kind of credit card, which can be read through a wallet or an item of clothing, is startlingly weak, researchers say.

WORLD SER

Reading of

Did Kenny Rc something ille during his wi

Complete Cov

TIMESSELEC

Talking P

In Opinion, Adam Cohen looks at sever brutally effective political ads.

Audio Slide S

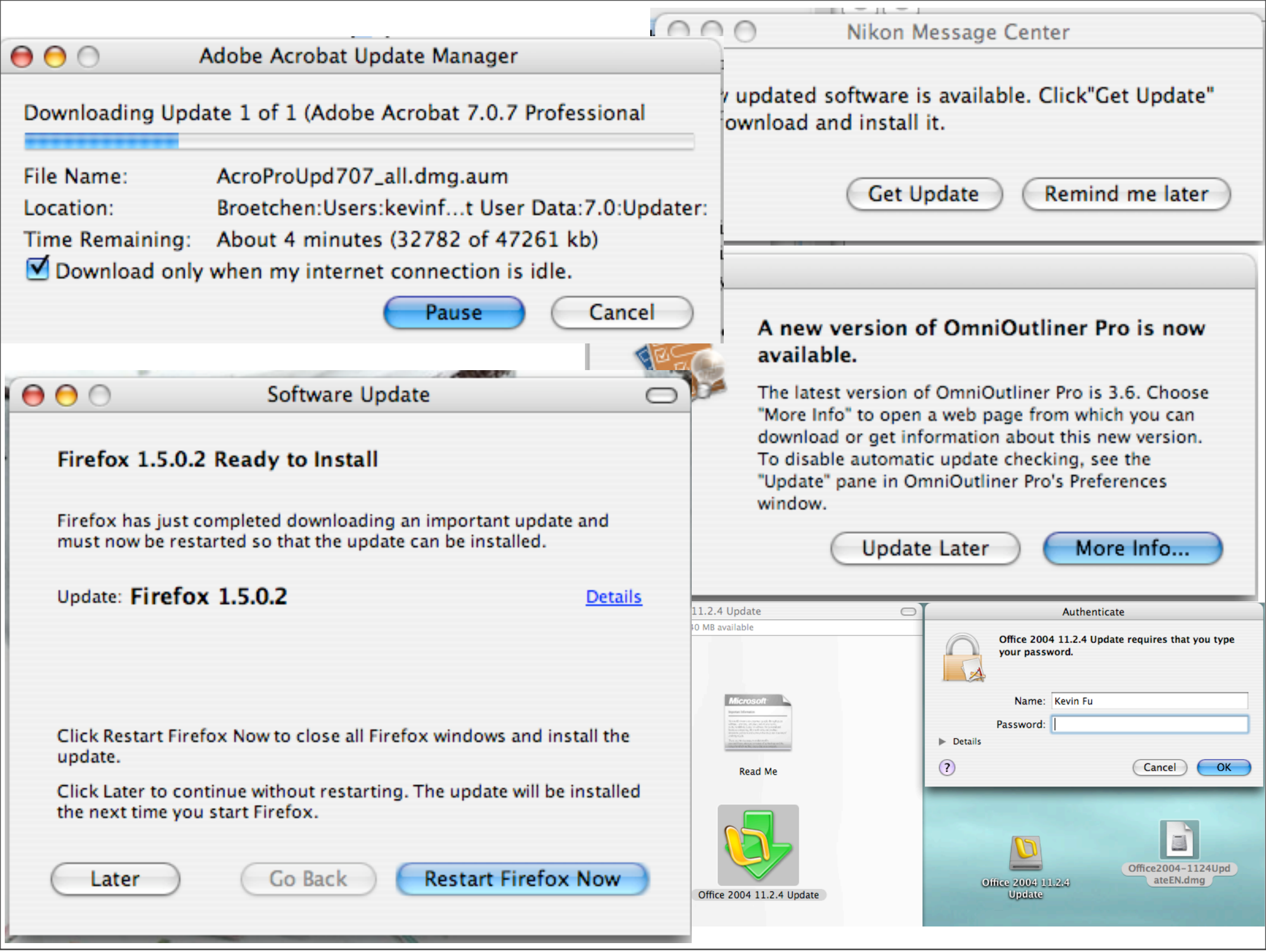
MEDIA & AD

We're Goog

Google's attra attention of n

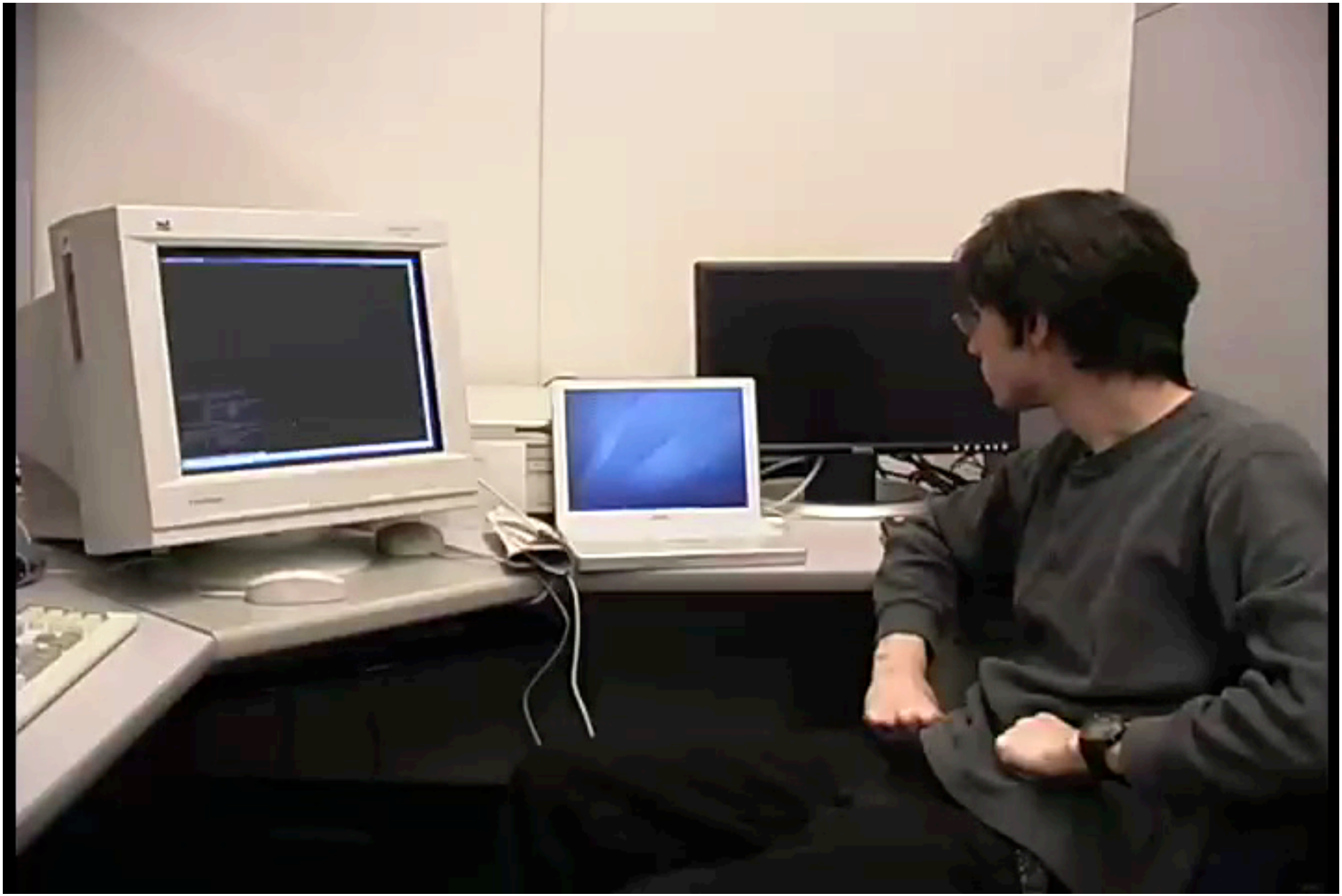
Privacy for Public Transit

Secure Software Updates


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
Nikon Message Center
updated software is available. Click"Get Update"
ownload and install it.
Get Update
Remind me later
A new version of OmniOutliner Pro is now available.
The latest version of OmniOutliner Pro is 3.6. Choose "More Info" to open a web page from which you can download or get information about this new version. To disable automatic update checking, see the "Update" pane in OmniOutliner Pro's Preferences window.
Update Later
More Info...
Software Update
Firefox 1.5.0.2 Ready to Install
Firefox has just completed downloading an important update and must now be restarted so that the update can be installed.
Update: Firefox 1.5.0.2
Details
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.
Later
Go Back
Restart Firefox Now
11.2.4 Update
40 MB available
Read Me
Office 2004 11.2.4 Update
Authenticate
Office 2004 11.2.4 Update requires that you type your password.
Name: Kevin Fu
Password:
Details
Cancel
OK
Office 2004 11.2.4 Update
Office2004-1124UpdateEN.dmg

Survey of Update Security

Software	Platform	Authenticated Connection?	Authenticated Binaries?
Apple Software Update	MacOS	no	yes
Windows Update	Windows	partially	yes
Adobe Acrobat	MacOS	no	yes
Microsoft Office	MacOS	no	yes
Mozilla Firefox	Windows	partially	no
Fugu	MacOS	no	no
McAfee VirusScan	Windows	no	no
McAfee VirusScan Enterprise	Windows	unknown	yes
McAfee Virex	MacOS	no	no*
Debian	Linux	no	yes



http://www.cs.umass.edu/~kevinfu/secureupdates/

Automotive Updates

http://www.soultek.com/clean_energy/hybrid_cars/toyota_prius_hybrid_car_shut_down_or_stall_problems.htm

Hybrid Cars: Join the Revolution

Updated: Thursday, October 13, 2005

Prius software problems? Is the Prius stopping or stalling on the Highway?

Toyota will send out a letter to about 75,000 Prius owners asking them to take their vehicles to their dealer to fix a potential software glitch, according to Reuters. Some Prius drivers have reported sudden stalling or stopping. According to Toyota, "if the gasoline engine stalls, the electric motor in the vehicles will have enough power to allow the driver to pull the vehicle over and away from the traffic."

The software update is free and is intended for 2004 and 2005 Prius models. While the U.S. National Highway Traffic Safety Administration

Help make hybrid cars more affordable (help)

Current Hybrids

- **Toyota Highlander Hybrid SUV**
- **Ford Escape Hybrid SUV**
- **Lexus**

Updates in Voting Machines

The New York Times
nytimes.com

PRINTER-FRIENDLY FORMAT
SPONSORED BY SUN

May 12, 2006

New Fears of Security Risks in Electronic Voting Systems

By MON

David Bear, a spokesman for Diebold Election Systems, said the potential risk existed because the company's technicians had intentionally built the machines in such a way that election officials would be able to update their systems in years ahead.

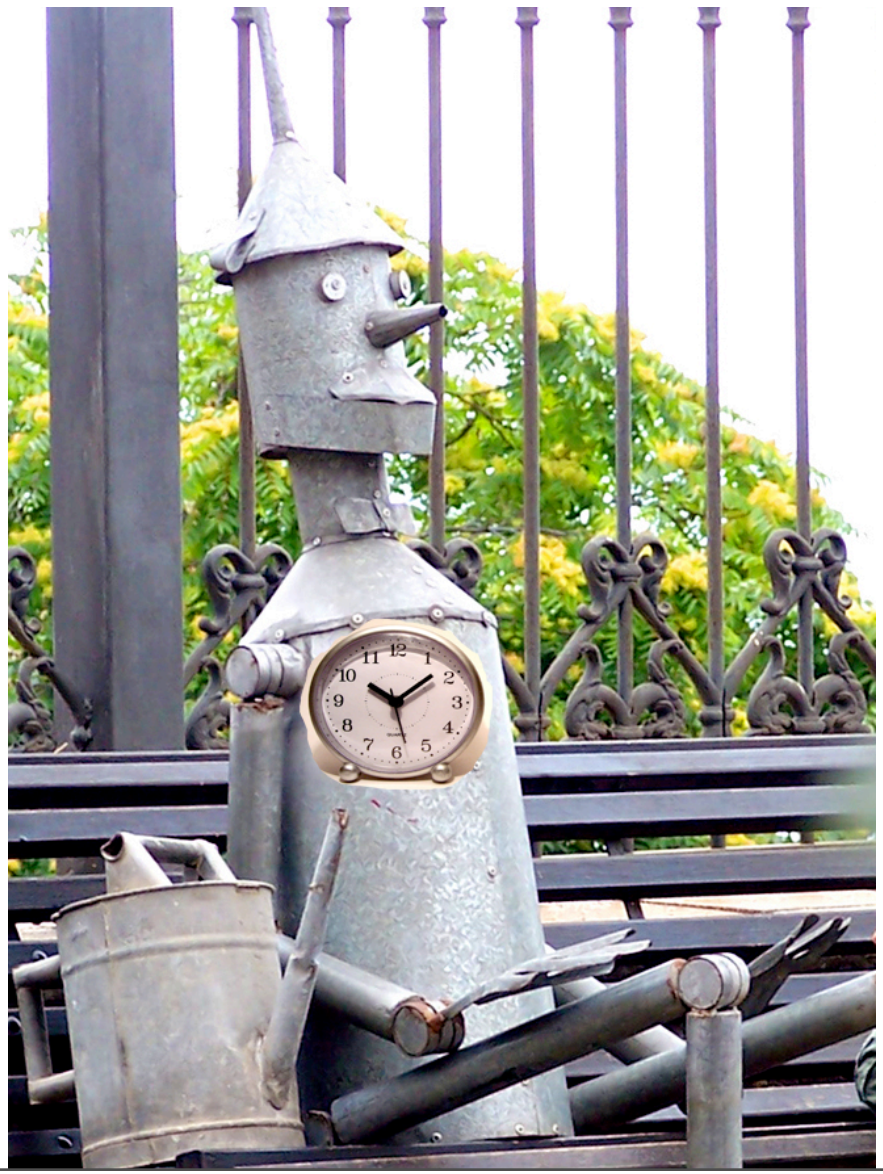
CHICA in Pennsyl ty risk in their Diebold Election Systems touch-screen voting machines, while other states with similar equipment hurried to assess the seriousness of the problem.

"It's the most severe security flaw ever discovered in a voting system," said Michael I. Shamos, a professo nic voting systems

Aviel Rubin, a professor of computer science at Johns Hopkins University, did the first in-depth analysis of the security flaws in the source code for Diebold touch-screen machines in 2003. After studying the latest problem, he said: "I almost had a heart attack. The implications of this are pretty astounding."

http://www.nytimes.com/2006/05/12/us/12vote.html?ex=1305086400&en=1b3554af6e2d524a&ei=5088&partner=rssnyt&emc=rss

Implanted medical devices use updates too



What stops a computer viruses from infecting implants?

A common wireless command on an ICD induces ventricular fibrillation. How is it authenticated?

Embedded Medical Software

Guidance for Industry and FDA Staff

Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices

Document issued on: May 11, 2005

Software Change Management

Design, development, testing, and version control of revis

3. What is it about "network-connected medical d concern?

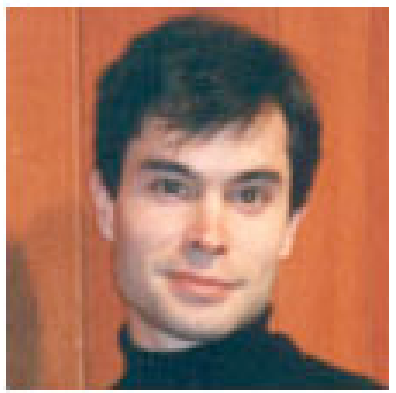
Vulnerabilities in cybersecurity may represent a risk to networked medical devices using OTS software. Failu could result in an adverse effect on public health. A n need fo timely software patches o correct newly disc

Discussion

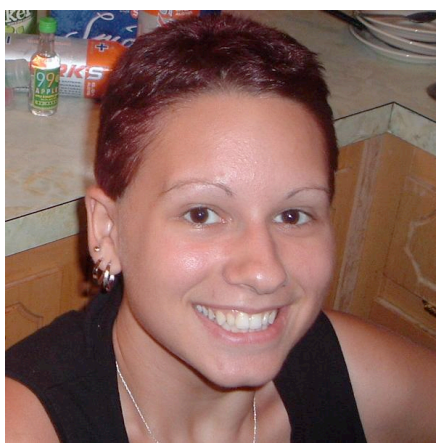
- Technical
  - What are the threat models for wirelessly reprogrammable medical implants?
  - How to balance safety, privacy, security?
- Philosophical
  - What is the role of FDA for future implanted medical devices?
  - Biggest challenges for next-generation implanted devices?

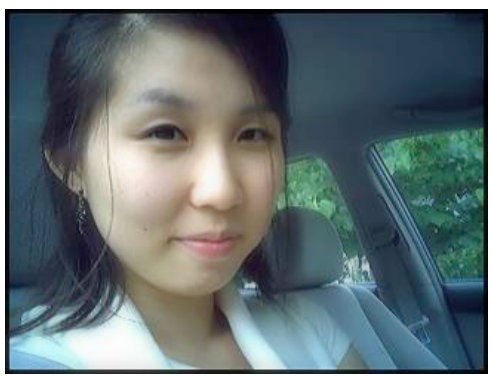
System Security at UMass Amherst

Faculty and affiliates



Graduate Students



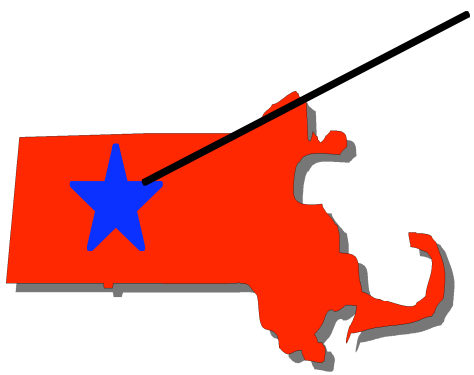


www.rfid-cusp.org

Computer Science UMASS

Kevin Fu, Computer System Security

Computer Science at UMass/Amherst



http://www.cs.umass.edu

43 faculty, ~230 graduate students, ~300 undergraduate students