Secure Software Updates

Disappointments and New Challenges

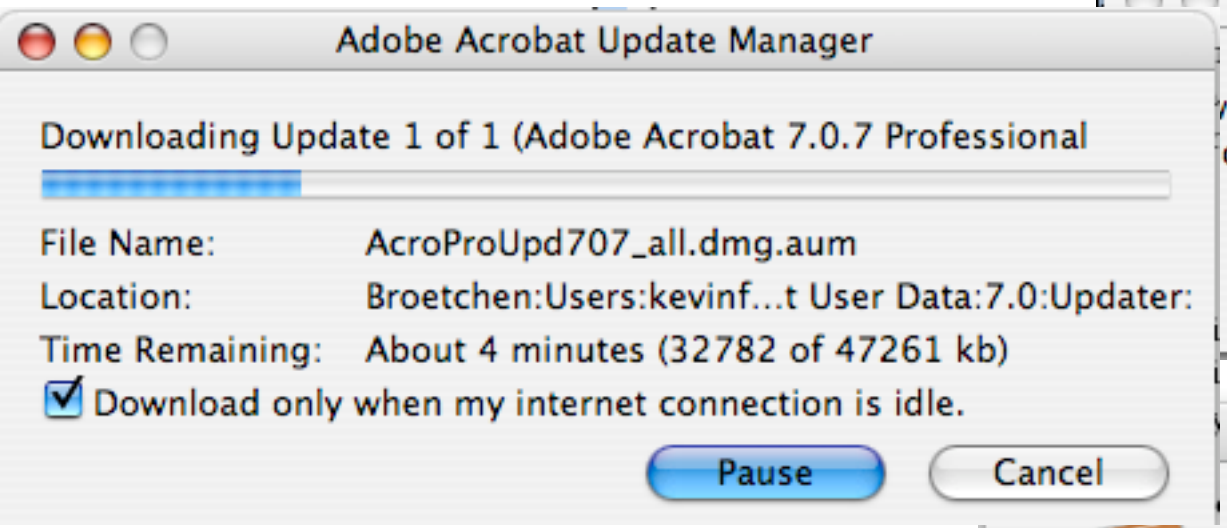
Kevin Fu
kevinfu@cs.umass.edu

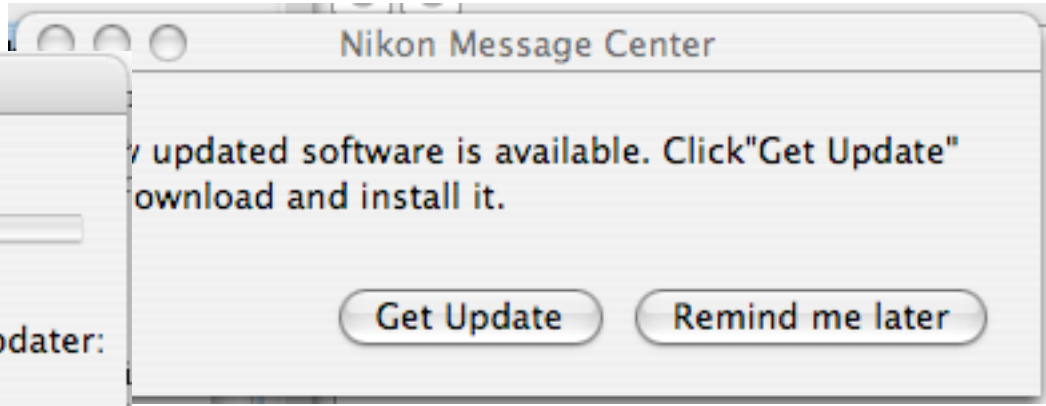
Anthony Bellissimo
John Burgess

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

Observations and Beliefs

- Software updates are susceptible to MITM
  - Easy to address in centralized scenarios
  - Difficult to deploy in standalone apps
- Updating embedded devices trickier
  - Unconventional constraints and threats
  - New risks

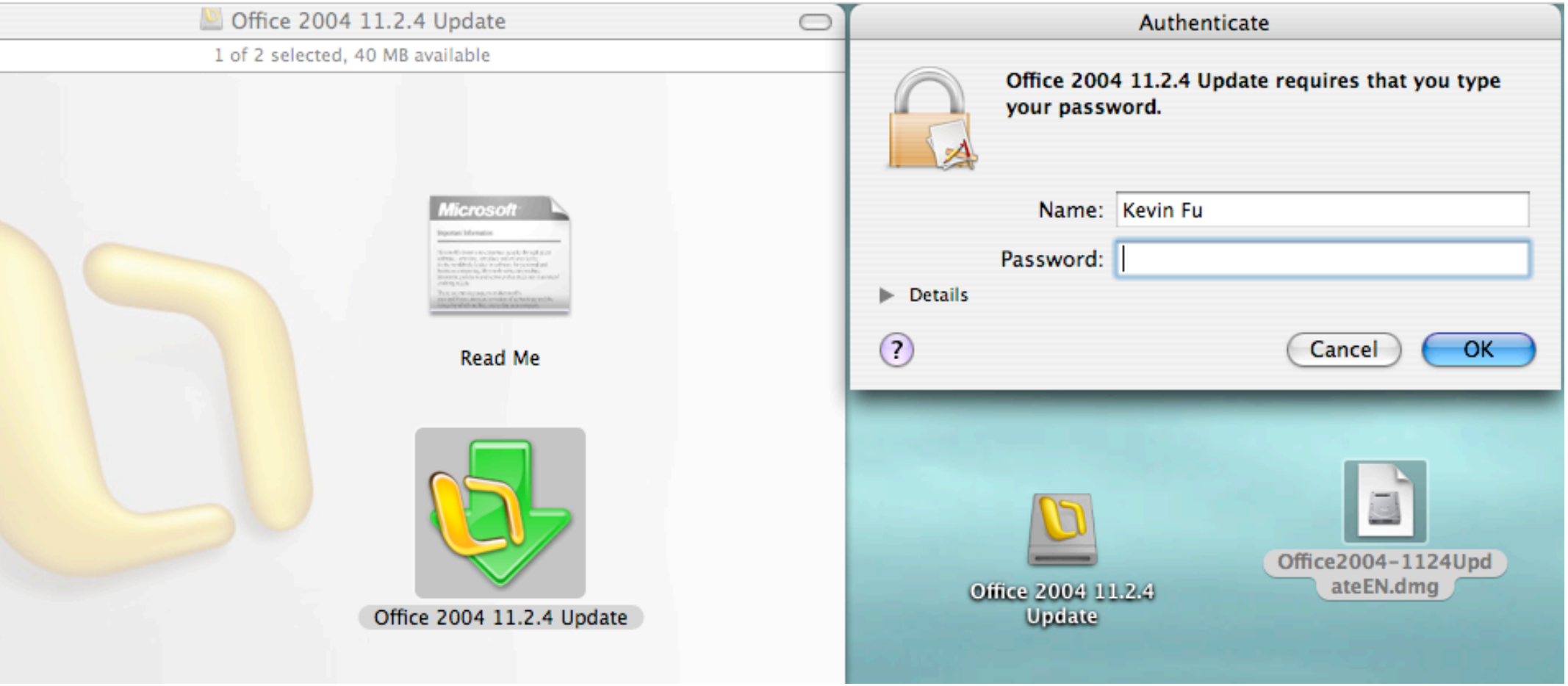

Adobe Acrobat Update Manager
Downloading Update 1 of 1 (Adobe Acrobat 7.0.7 Professional
File Name: AcroProUpd707_all.dmg.aum
Location: Broetchen:Users:kevinf...t User Data:7.0:Updater:
Time Remaining: About 4 minutes (32782 of 47261 kb)
Download only when my internet connection is idle.
Pause
Cancel


Nikon Message Center
updated software is available. Click"Get Update"
ownload and install it.
Get Update
Remind me later

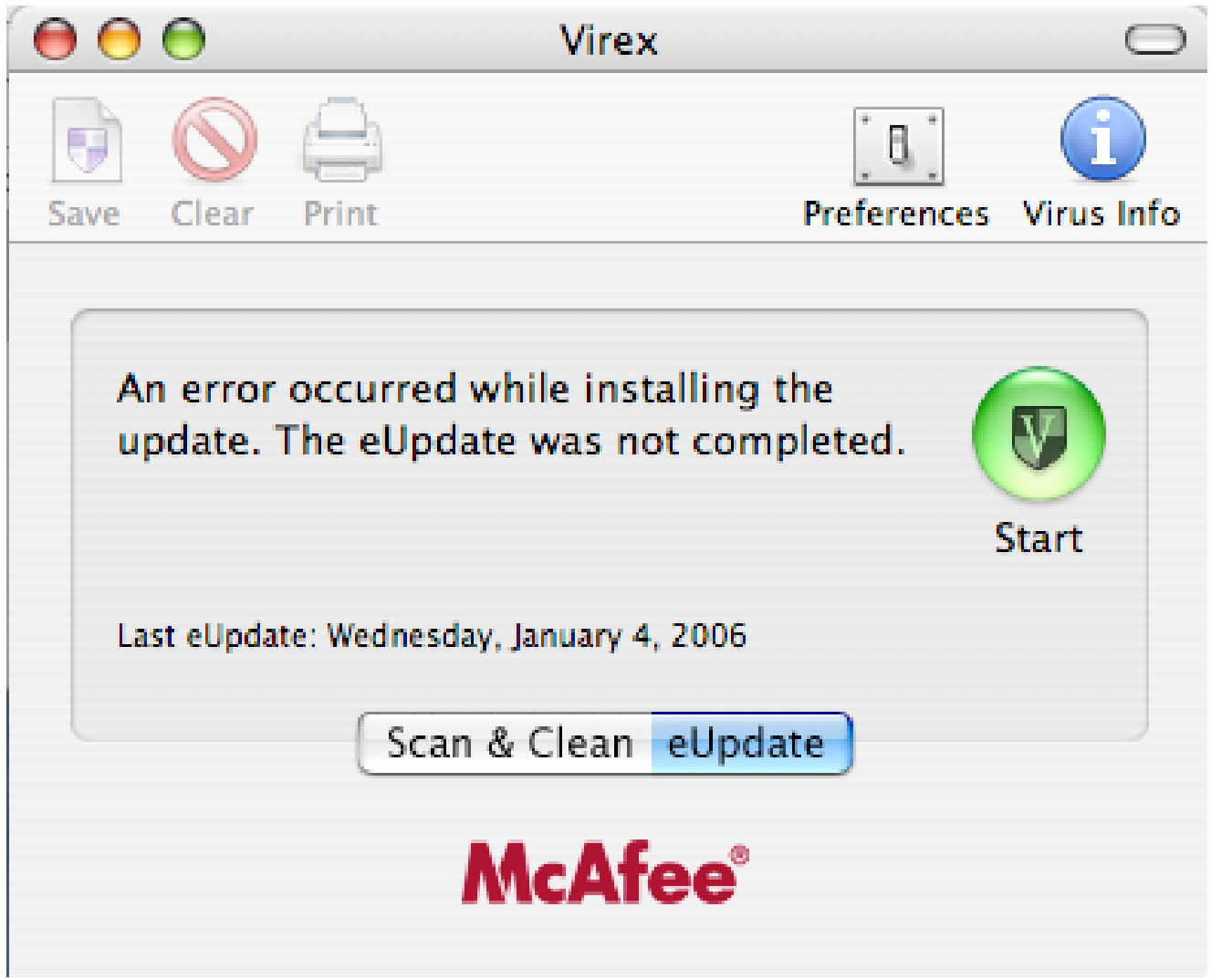

Software Update
Firefox 1.5.0.2 Ready to Install
Firefox has just completed downloading an important update and must now be restarted so that the update can be installed.
Update: Firefox 1.5.0.2
Details
Click Restart Firefox Now to close all Firefox windows and install the update.
Click Later to continue without restarting. The update will be installed the next time you start Firefox.
Later
Go Back
Restart Firefox Now

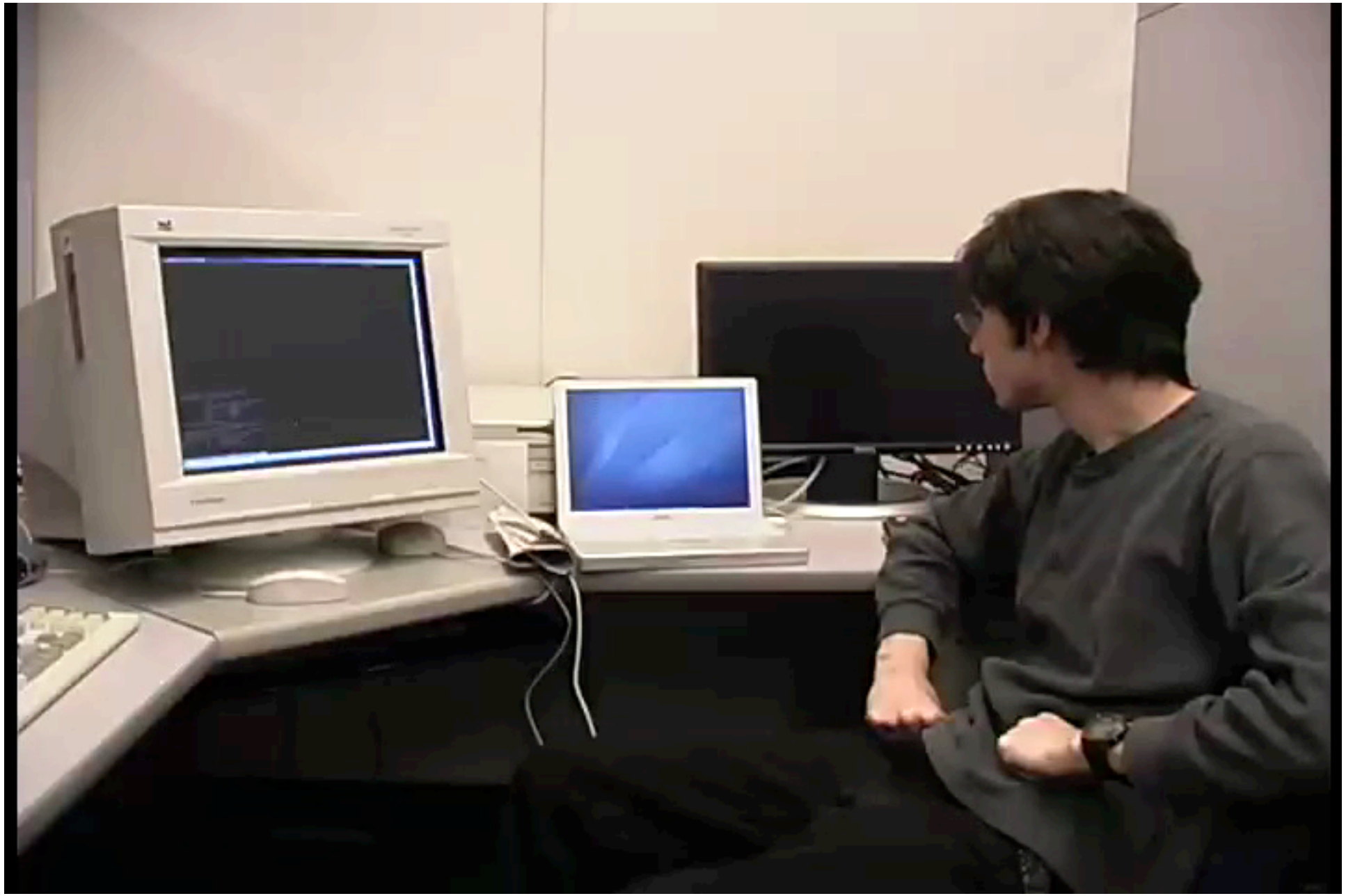

A new version of OmniOutliner Pro is now available.
The latest version of OmniOutliner Pro is 3.6. Choose "More Info" to open a web page from which you can download or get information about this new version. To disable automatic update checking, see the "Update" pane in OmniOutliner Pro's Preferences window.
Update Later
More Info...

Unsigned updates rampant



Millions update every day





Additional info on
http://www.cs.umass.edu/~kevinfu/secureupdates/

McAfee apologizes for not publicizing fix

By Associated Press
Monday, July 17, 2006 - Updated: 10:23 AM EST

WASHINGTON - A leading computer security company, McAfee Inc., fixed a dangerous design flaw months ago in its flagship technology for managing protective software in large organizations but did not warn businesses and U.S. government agencies until Friday.

McAfee issued a rare apology and urged customers to install updated versions of its software immediately. McAfee's antivirus software is used by more than one-third of corporations in the United States and Europe. A spokeswoman, Siobhan MacDermott, said there were no reports of victims.

"This is probably one of the most widely used corporate antivirus components," said Andrew Jaquith, the security research program manager at the Boston-based Yankee Group, an analyst firm. "It is a little ironic tha products designed to protect you are actually making you vulnerable."

http://business.bostonherald.com/technologyNews/view.bg?articleid=148707

CERT/CC Vulnerability Disclosure Policy

Effective October 9, 2000, the CERT Coordination Center will follow a new policy with respect to the disclosure of vulnerability information. All vulnerabilities reported to the CERT/CC will be disclosed to the publi 45 days after the initial report, regardless of the existence or availability of patches or workarounds from affected vendors. Extenuating circumstances, such as active

Q: Will all vulnerabilities be disclosed within 45 days?

A: No. There may often be circumstances that will cause us to adjust our publication schedule. Threats that are especially serious or for which we have evidence of exploitation will likely cause us to shorten our release schedule. Threats that require "hard" changes (changes to standards, changes to core operating system components) will cause us to extend our publication schedule.

http://www.cert.org/kb/vul_disclosure.html

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

Automotive Updates

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

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.

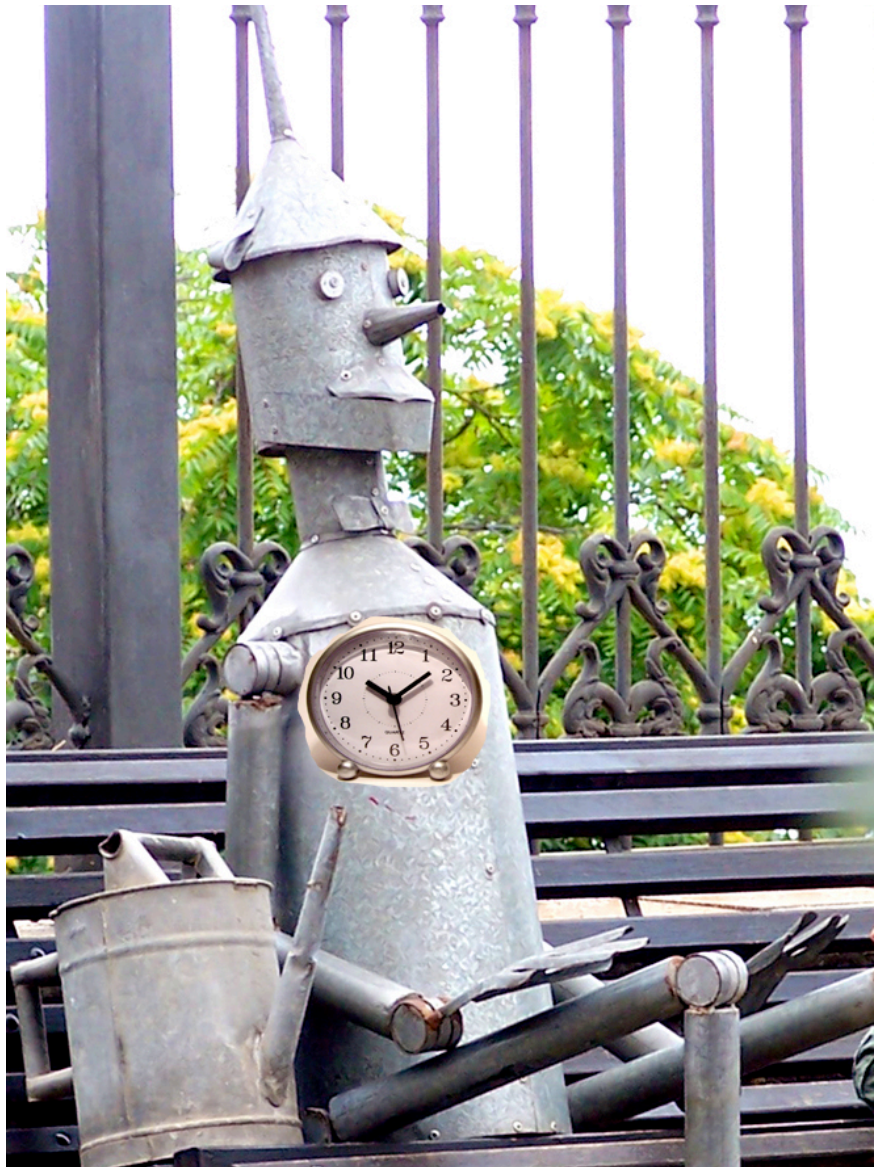
CHICA in Pennsyl ty risk in their Diebold Election Systems touch-screen voting machines, while other states with similar equipment hurried to assess the seriousness of the problem.

"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



How long until computer viruses can infect humans?

"Help! My heart is infected and is launching a DDoS on my pancreas."

Software overdose

URGENT: Medtronic Announces Nationwide, Voluntary Recall of Model 8870 Software Application Card

Version AAA 02
Used with the Model N'Vision™ Clinician Programmer

MINNEAPOLIS, Sept. 22, 2004 - Medtronic, Inc. (NYSE: MDT) today announced a voluntary recall that involves all Version AAA 02 Model 8870 software application cards in the U.S. that are used in conjunction with all Model 8840 N'Vision™ Clinician Programmers. This action has been classified by the Food and Drug Administration (FDA) as a **Class I Recall**. The FDA defines a Class I recall as a situation in which there is a reasonable probability that the use of or exposure to the product will cause serious adverse health consequences or death.

Medtronic became aware in August 2003 that some users had mistakenly entered a periodic bolus interval into the **minutes** field, rather than the **hours** field, potentially resulting in drug overdoses. Data entry errors have been related to seven serious injuries and two deaths. The previous model 8870 software application card did not provide a label for the hours/minutes/seconds fields; the new software has this labeling.

http://www.fda.gov/cdrh/recalls/recall-082404b-pressrelease.html

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

Guidance for Industry

Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software

Document issued on: January 14, 2005

Software Change Management

Design, development, testing, and version control of revisions to the software are as important as

3. What is it about "network-connected medical devices" that causes so much concern?

Vulnerabilities in cybersecurity may represent a risk to the safe and effective operation of networked medical devices using OTS software. Failure to properly address these vulnerabilities could result in an adverse effect on public health. A major concern with OTS software is the need fo timely software patches o correct newly discovered vulnerabilities in the software.

fda.gov

What Next?

- Sign conventional updates
  - Why didn't the research transfer to reality?
  - Little guys suffer the most
  - Secure updates as an operating system service
- Updating embedded devices
  - No user interface, but ubiquitous
  - Limited network, power, computation
  - Threat model? Why would anyone attack this?