Take Two Software Updates and See Me in the Morning:

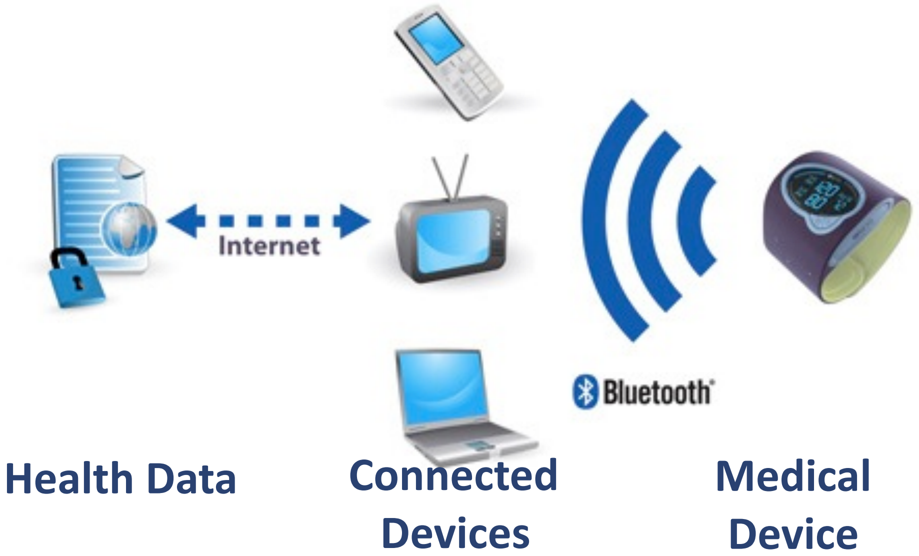
The Case for Software Security Evaluations of Medical Devices

Steve Hanna[1], Rolf Rolles[4], Andres Molina-Markham[2], Pongsin Poosankam[1,3], Kevin Fu[2], Dawn Song[1]

University of California – Berkeley[1], University of Massachusetts Amherst[2], Carnegie Mellon University[3], Unaffiliated[4]

Changing Medical Device Landscape

- ***Increased*** software complexity
- Software plays an increasing role in device failure
  - 2005-2009 (18%) due to software failure, compared to (6%) in 1980s
- ***Increased*** attack opportunities
- Medical device hardware and software is usually a ***monoculture*** within device model



Health Data

Connected Devices

Medical Device

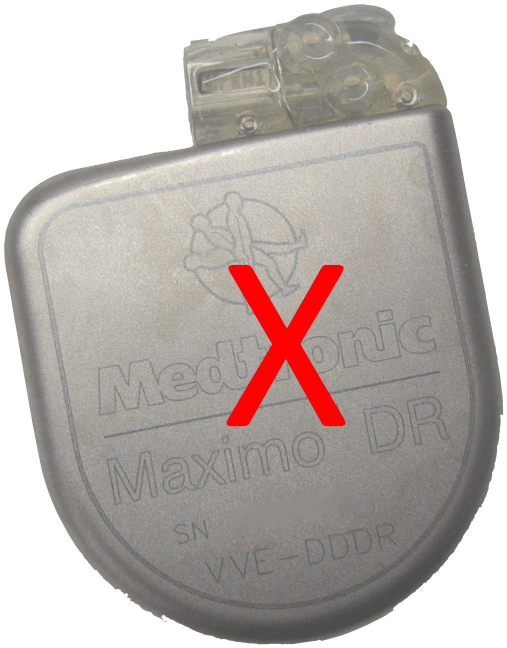
Automated External Defibrillators

28,000 adverse event reports in 14 Models recalled 2005-2010.

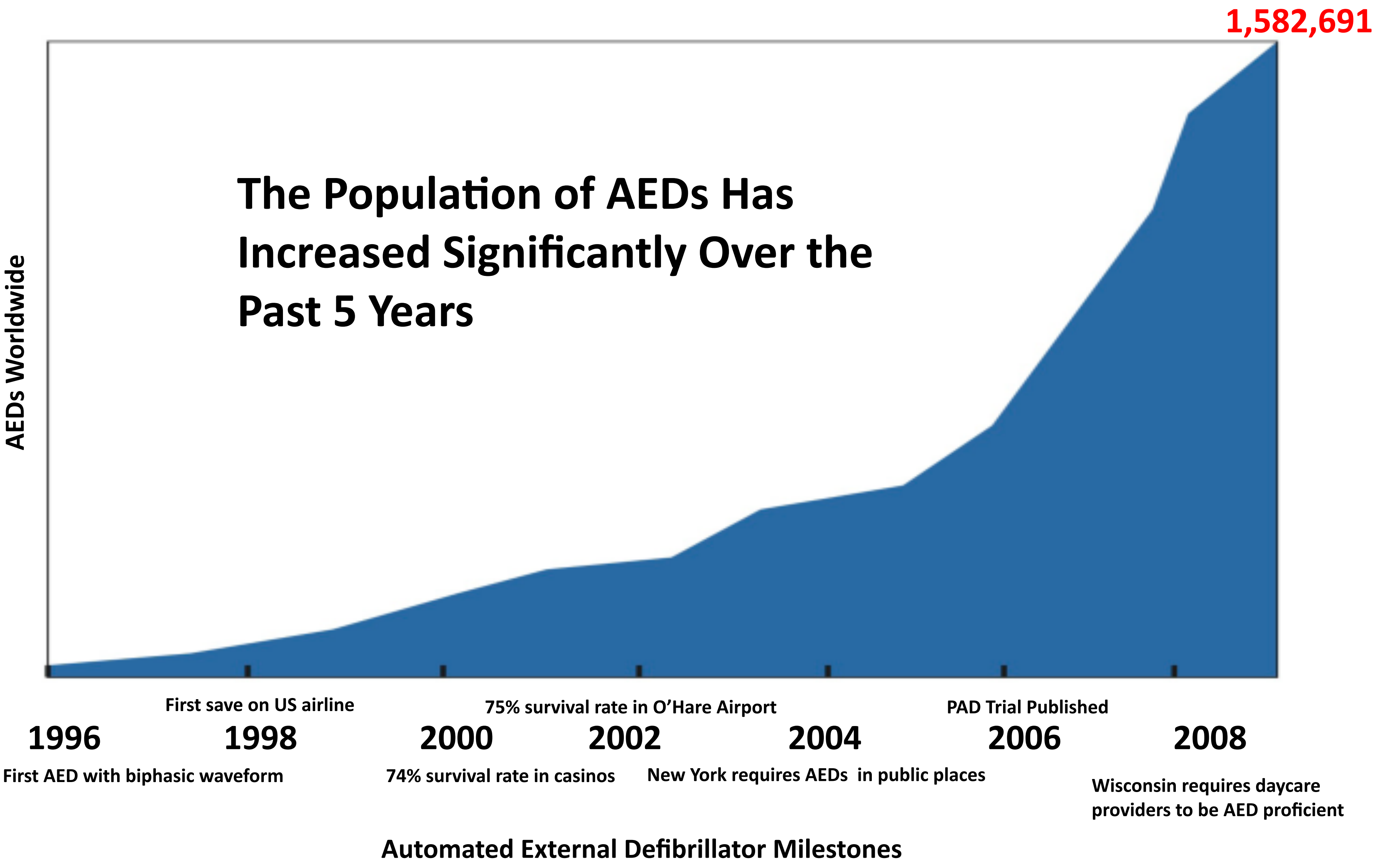
To be clear…

AEDs

ICDs



The Population of AEDs Has Increased Significantly Over the Past 5 Years



First save on US airline

75% survival rate in O'Hare Airport

PAD Trial Published

First AED with biphasic waveform

74% survival rate in casinos

New York requires AEDs in public places

Wisconsin requires daycare providers to be AED proficient

Global Automated External Defibrillators (AED) Market: Demand to Drive Growth; June 2009 U.S., European and Japanese External Defibrillation (PAD) Market Report. Frost & Sullivan. 2000. Valenzuela TD, et al. *N Engl J Med.* 2000;343:1206-1209. Caffrey S, et al. *N Engl J Med.* 2002;347:1242-1247.

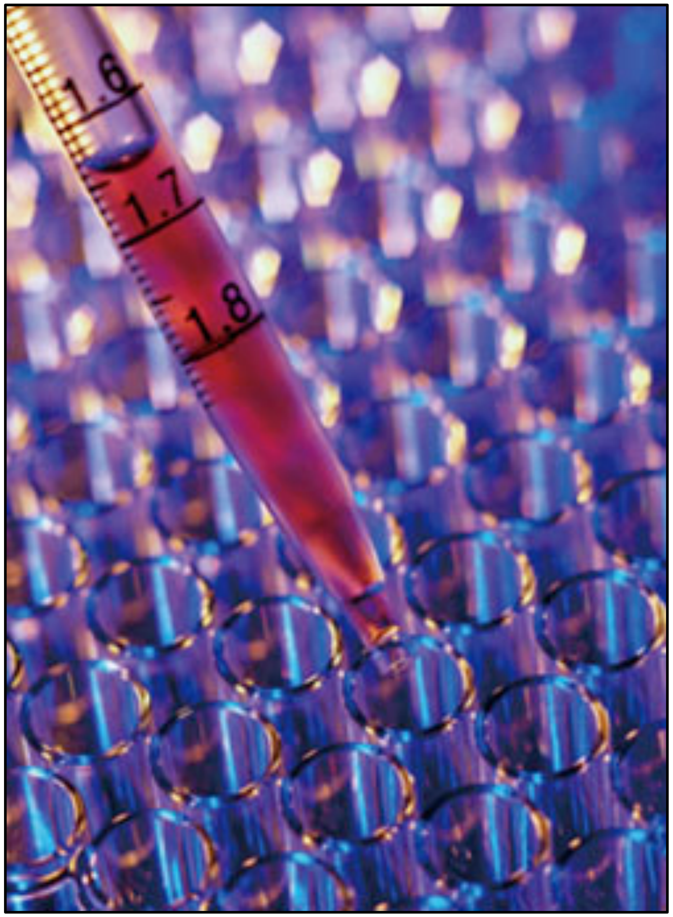
Our Objectives

- Explore state of AED software security
- Examine for standard software security flaws
  - Data handling, coding practices, developer assumptions
- Give insight into state of medical device software and potential for future abuse

Desirable Medical Device Properties

The device should:

- Ensure that software running on a system is the image that was verified
- Detect compromise
- Verify and authenticate device telemetry
- Be robust: defenses and updates weighed with risks to patient



Case Study

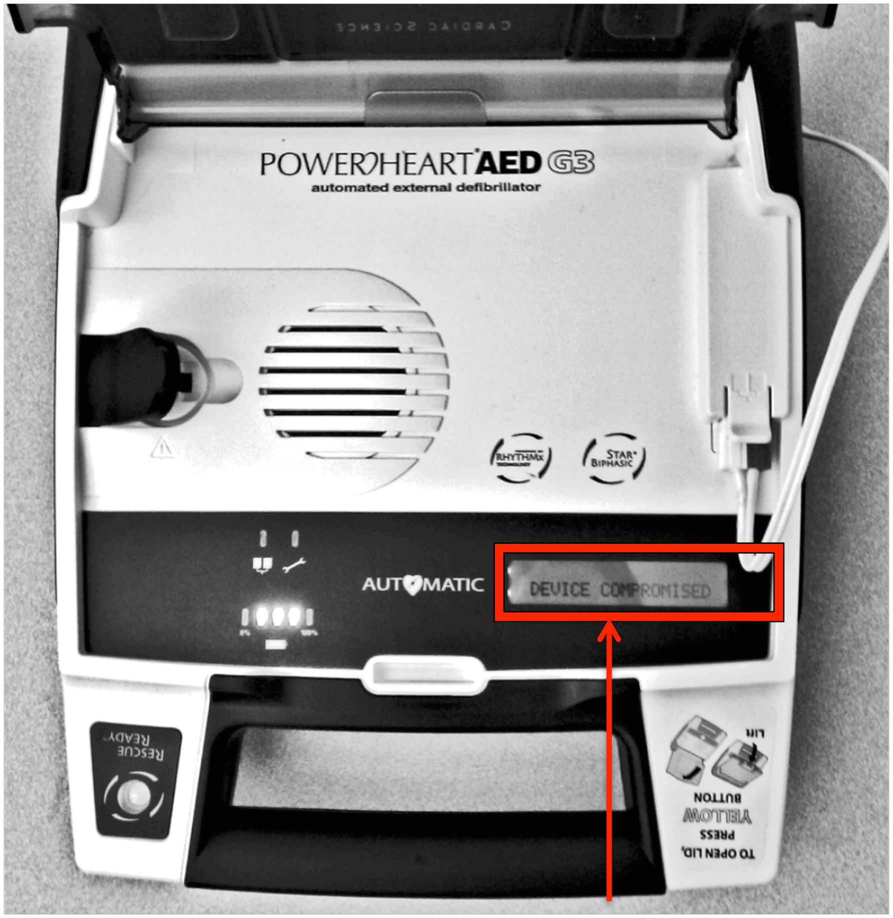
- Analyzed **Cardiac Science G3 Plus** model 9390A
- Performed static reverse engineering using IDA Pro
  - Analyzed: *MDLink*, *AEDUpdate* and device *firmware*
- Analysis using BitBlaze architecture
  - BitFuzz, the dynamic symbolic path exploration tool
- Remarks
  - Problems likely not isolated to the G3 Plus
  - Potential for abuse as devices become more connected

Vulnerabilities Discovered

1. AED Firmware - Replacement
2. AEDUpdate - Buffer overflow
3. AEDUpdate - Plain text user credentials
4. MDLink - Weak password scheme

Vulnerabilities were verified on Windows XP SP2.

Firmware Replacement

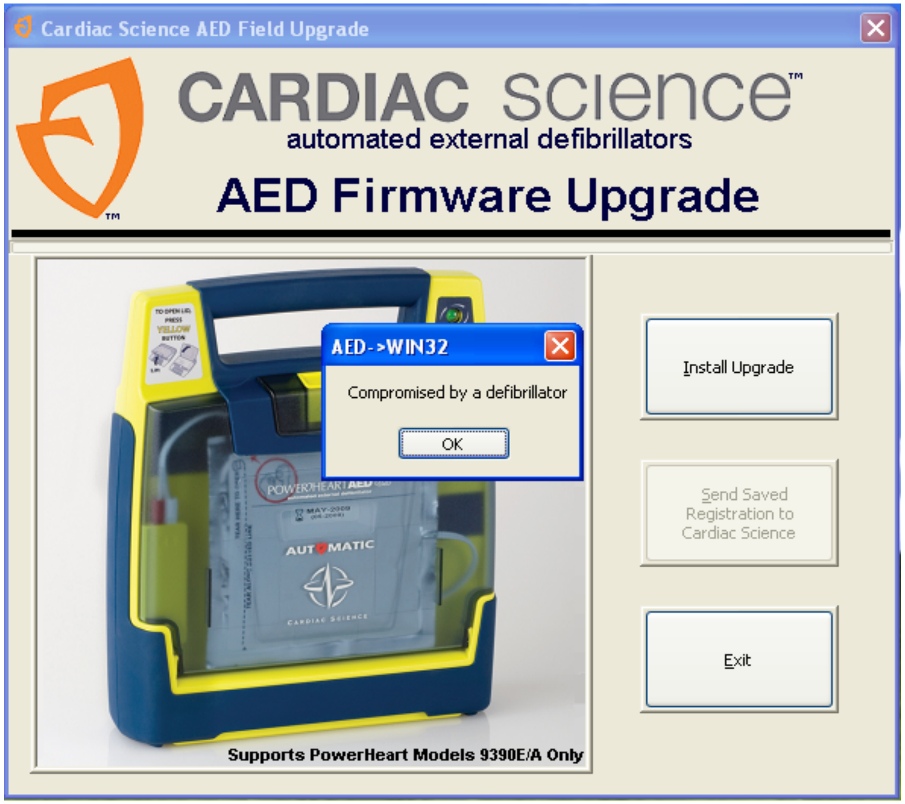


DEVICE COMPROMISED

- Firmware update uses custom CRC to verify firmware
- Modified firmware, with proper CRC, is accepted by AED and update software
- Impact: **Arbitrary firmware**

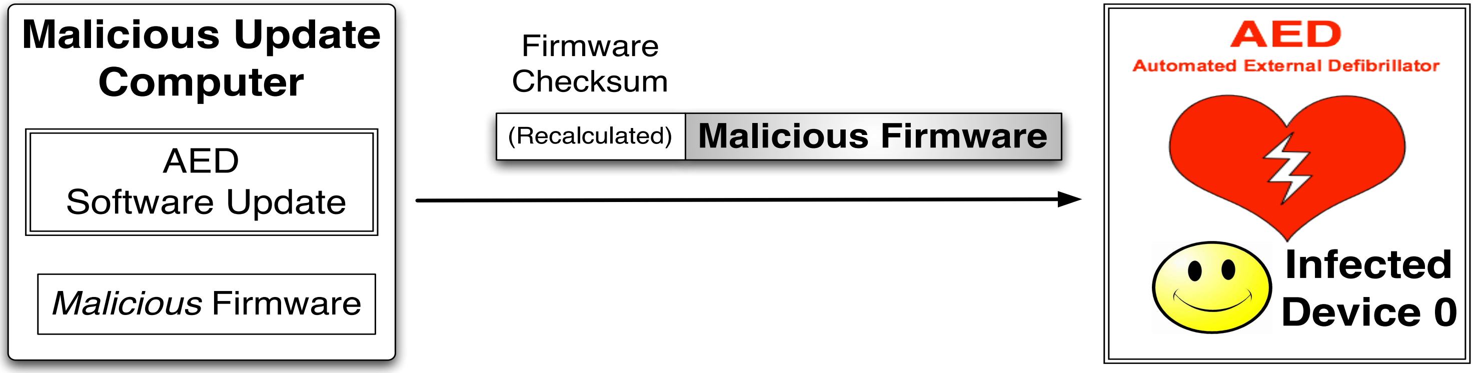
AEDUpdate Buffer Overflow

- During update device handshake, device version number exchanged
- AEDUpdate *improperly* assumes valid input
- Enables **arbitrary** code execution
  - Data sent from AED can be executed as code on the host PC


Cardiac Science AED Field Upgrade
CARDIAC SCIENCE™
automated external defibrillators
AED Firmware Upgrade
AED->WIN32
OK
Install Upgrade
Send Saved Registration to Cardiac Science
Exit
Supports PowerHeart Models 9390E/A Only

Compromised by a defibrillator

Initial Malicious Firmware Update



Malicious Update Computer

AED Software Update

Malicious Firmware

Firmware Checksum

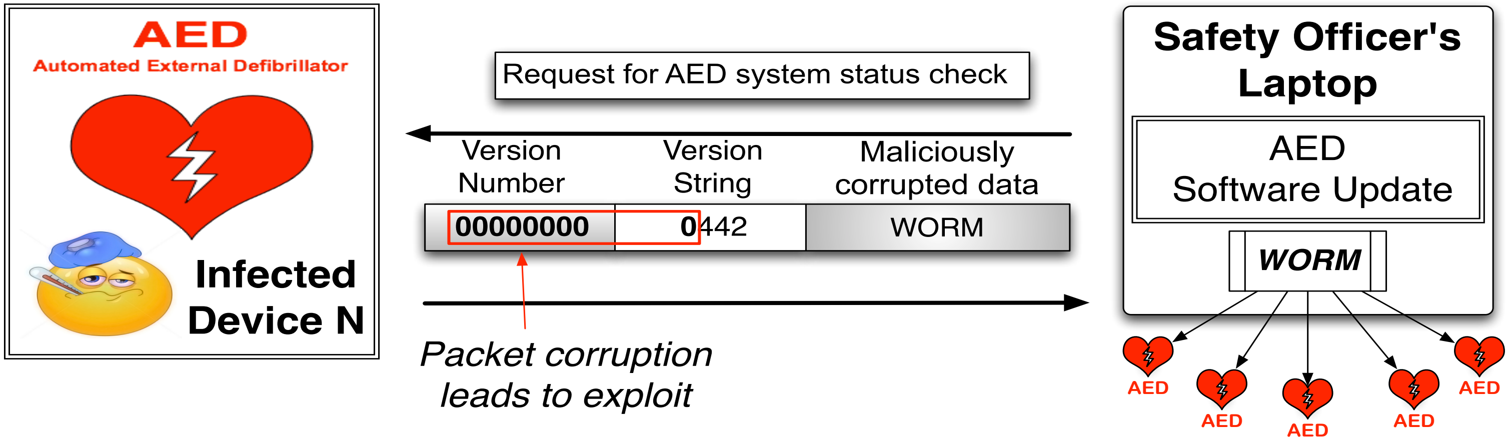
(Recalculated) **Malicious Firmware**

AED

Automated External Defibrillator

Infected Device 0

AED Infecting Security Officer's Laptop



AED

Automated External Defibrillator

Infected Device N

Request for AED system status check

Version Number	Version String	Maliciously corrupted data
00000000	0442	WORM

Packet corruption leads to exploit

Safety Officer's Laptop

AED Software Update

WORM

AED

AED

AED

AED

AED

Improving Medical Device Security for Developers

- Lessons and open problems from the CS G3 Plus
  - Cryptographically secure device updates
    - No security through obscurity, ensures firmware authenticity
  - Device telemetry verified for integrity and authenticity
    - Defensively assume that data is not trusted
  - Passwords cryptographically secure and easily managed
    - Private data and life critical functionality should be protected by well-established cryptographic algorithms
  - Defenses and updates weighed with risks to patient
    - Medical devices should **fail open**

Recommendations

- Ensure the update machine is secure
  - Physical isolation, virtual machine for fresh install
- Follow FDA guidelines and advisories
- Remain vigilant
  - Monitoring physical access, routinely updating afflicted devices, and monitoring advisories released about the device

Final Recommendation

We recommend **continued use of AEDs** because of their potential to perform lifesaving functions.

The attack potential is currently unmeasured and currently, these devices overwhelmingly save more lives than they imperil.

Thank You

- Questions?
  - Contact:
    - Steve Hanna (sch@eecs.berkeley.edu)
    - Dawn Song (dawnsong@cs.berkeley.edu)
    - Kevin Fu (kevinfu@cs.umass.edu)

secure-medicine.org