Take Two Software Updates and See Me in the Morning:

The Case for Software Security Evaluations of Medical Devices

Steve Hanna¹, Rolf Rolles⁴, Andres Molina-Markham², Pongsin Poosankam¹,³, Kevin Fu², Dawn Song¹

University of California – Berkeley¹, University of Massachusetts Amherst², Carnegie Mellon University³, Unaffiliated⁴
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

Automated External Defibrillators

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

AEDs

ICDs

Hanna, et al. The case for Software Security Evaluations of Medical Devices
Wisconsin requires daycare providers to be AED proficient.

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

Automated External Defibrillator Milestones

- **1996**: First AED with biphasic waveform
- **1998**: First save on US airline
- **2000**: 74% survival rate in casinos
- **2002**: New York requires AEDs in public places
- **2004**: PAD Trial Published

- **2006**: Wisconsin requires daycare providers to be AED proficient
- **2008**: 1,582,691 AEDs Worldwide

**Global Automated External Defibrillators (AED) Market: Demand to Drive Growth; June 2009**

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

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

**DEVICE COMPROMISED**
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
Initial Malicious Firmware Update

AED Infecting Security Officer's Laptop

AED Software Update

Malicious Firmware

Firmware Checksum

(Recalculated) Malicious Firmware

AED

Automated External Defibrillator

Infected Device 0

AED Software Update

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

WORM

AED

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