Security and Privacy of Medical Devices

Ming Chow
mchow@cs.tufts.edu
Twitter: @0xmchow

Motivation

- "I was aware of the danger, if you will, that existed." --Former US Vice President Dick Cheney (on *60 Minutes*)
- “Cheney told his 60 Minutes interviewer, CNN Chief Medical Correspondent Dr. Sanjay Gupta, that at the time of the pacemaker implant, he was concerned about reports that attackers could hack the devices and kill their owners.”
- ***“Doctors disabled wireless in Dick Cheney's pacemaker to thwart hacking”*** https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/

What is Security? The Definition

- The CIA triad:
  - Confidentiality
  - Integrity
  - Availability
- Also often included are authenticity and non-repudiation

What Security Really Is

- Violating the invariants of a computer system or application (i.e., correctness)
- Security is hard
- Thinking like a bad guy is a different mindset
- Security requires tradeoffs
- Constructive debates
- The current state: a reactive process
- The current state: breaking things is sexy

Important Definitions

- **Event** - Could be anything
- **Incident** - A malicious event
- **Bug** - An error that exists in the implementation-level (i.e. only exist in source code); very correctable
- **Flaw** - An error at a much deeper level, particularly in the design, and likely in the code level; can be very difficult and costly to correct
- **Hacker** - A creative programmer; a positive connotation
- **Cracker** - The bad guy, the attacker, what media coins "hacker" (the negative connotation). We'll use attacker in this class.
- **Black hat** - An attacker with malicious intents
- **White hat** - An attacker with good intents (i.e., the white knight)
- **Gray hat** - An attacker with good and bad intents
- **Script kiddie or skiddie** - Nuisance; not going away any time soon; 1337 wannabes; use scripts and exploits written by others (and do not understand how they really work); always a lamer
- **Vulnerability** - A security bug; a weakness in a system that can potentially be exploited by an attacker
- **Exploiting or exploitation** - The act of taking advantage of a vulnerability
- **Exploit** - Software program that performs the exploiting
- **Risk** - The likelihood that an attacker will take advantage of that vulnerability
- **Threat** - The likelihood that an incident will happen

Why the Rash of Security Incidents?

- Generally speaking, security is an afterthought
  - It is a matter of when, not if, an incident will happen
- The “trinity of trouble” according to my dear colleague Gary McGraw
  - Connectivity
    - Now made worse thanks to “The Internet of Things (IoT)”
  - Extensibility
  - Complexity

Why Care About Security?

- Reputation
- Regulations, laws
- Enormous costs after a major incident (think of how insurance works)
- Lives at stake, especially with medical devices

Who to Blame?

- In no particular order:
  - Companies
  - Users
  - Developers
  - Technology itself
  - Media (and the spread of FUD)
  - Government
  - You

What Does A Bad Guy Want?

- Information, including intellectual property
- Financials, money
- Control: administrative and unauthorized access to remote computers
- Cause a denial of service (DoS)
- Cause trauma

How To Attack and Compromise Computer Systems and Devices

- Social engineering (low-tech) including plain-old just asking for it
- Taking advantage of exploits in software, starting with reconnaissance (high-tech)

Where and What to Attack?

1. Physical layer
    - Example: Attacks using the JTAG standards for integrated circuit debugging go after port-sharing debug harnesses
2. Platform and operating system level
    - Example: Tamper with boot process to gain administrative access
3. Application level
    - Example: injection attack on a form to steal personal health information (PHI)
4. Communications level
    - Example: Sniff and capture largely unencrypted network traffic

Common Findings and Vulnerabilities in Medical Devices

- Cryptographic problems
- Operational issues with device lifecycle
- Communications security
- Authentication and authorization issues
- Lack of obfuscation controls
- Physical and platform security issues

Source: http://searchsecurity.techtarget.com/opinion/McGraw-on-assessing-medical-devices-Security-in-a-new-domain

Concrete Examples

- Weak passwords or default and hardcoded vendor passwords like “admin” or “1234″
- Web server enabled on embedded devices with administrative interfaces
- Use of snake-oil / roll-you-own cryptographic protocols
- Transmission of data using HTTP (which is plaintext)

#whatcouldpossiblygowrong

- Software malfunction, crash
- Crash testing equipment in labs
- Rebooting or turning off critical software and infrastructure
- Reset software on devices to default factory settings
- Exposure of "drug infusion pumps for delivering morphine drips"
- Exposure of “chemotherapy and antibiotics that can be remotely manipulated to change the dosage doled out to patients"
- "Bluetooth-enabled defibrillators that can be manipulated to deliver random shocks to a patient's heart or prevent a medically needed shock from occurring"
- "X-rays that can be accessed by outsiders lurking on a hospital's network"
- "Temperature settings on refrigerators storing blood and drugs that can be reset, causing spoilage"
- "Digital medical records that can be altered to cause physicians to misdiagnose, prescribe the wrong drugs or administer unwarranted care."

Source: http://www.wired.com/2014/04/hospital-equipment-vulnerable/

Notable Presentations Related to Security of Medical Devices

- August 2011: Jerome Radcliffe presents “Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System” at Black Hat USA 2011 Conference in Las Vegas https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf, https://www.youtube.com/watch?v=avf5XF8yS60
- August 2011: Tim Elrod and Stefan Morris present "I Am Not a Doctor but I Play One on Your Network" at the DEF CON Conference in Las Vegas https://www.defcon.org/images/defcon-19/dc-19-presentations/Elrod-Morris/DEFCON-19-Elrod-Morris-Not-a-Doctor.pdf, https://www.youtube.com/watch?v=g11BSRfBw2Y
- October 2011: The late Barnaby Jack demonstrated “an attack that hijacks nearby insulin pumps, enabling him to surreptitiously deliver fatal doses to diabetic patients who rely on them” at Hacker Halted in Miami, FL.
    - Sadly, Barnaby passed away in the summer of 2013 right before his scheduled presentation at Black Hat USA 2013 entitled “Implantable Medical Devices: Hacking Humans.”
- February 2014: Tim West and Jamie Gamble present "Turning Medical Device Hacks into Tools for Defenders" at the RSA Conference http://www.rsaconference.com/writable/presentations/file_upload/hta-r03-turning-medical-device-hacks-into-tools-for-defenders.pdf

Too Much Too Late?

- “We have dug ourselves into a deep hole” --Professor Ed Felten
- "Many hospitals are unaware of the high risk associated with these devices" --Scott Ervan
- October 2, 2014: FDA released guidelines regarding the security of medical devices
  - http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

Enormous Amount of Work To Be Done

- Responsible vulnerability disclosure process.
- Information security and secure software development in a Computer Science curriculum.
- Secure software development training and outreach.
- Informing and communicating with others on security-related matters including the general public and government.
- More security research necessary but researchers fear the Computer Fraud and Abuse Act (CFAA)

To Ponder and Debate

- How real is the problem as there has not been any major incidents related to the security of medical devices?

References

- http://searchsecurity.techtarget.com/opinion/McGraw-on-assessing-medical-devices-Security-in-a-new-domain
- http://www.wired.com/2014/04/hospital-equipment-vulnerable/
- http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm412979.htm
- http://www.informationweek.com/healthcare/security-and-privacy/fda-pushes-to-improve-medical-device-security/d/d-id/1316146
- http://money.cnn.com/2014/10/08/technology/security/internet-of-things-security/index.html
- http://go.bloomberg.com/tech-blog/2012-02-29-hacker-shows-off-lethal-attack-by-controlling-wireless-medical-device/
- http://abcnews.go.com/US/vice-president-dick-cheney-feared-pacemaker-hacking/story?id=20621434
- https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/
- http://www.ihealthbeat.org/articles/2014/10/2/fda-releases-final-guidance-on-medical-device-cybersecurity
- http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf
- http://www.computerworld.com/article/2474179/cybercrime-hacking/fda-asks-hackers-to-expose-holes-in-medical-devices--but-many-researchers-fear-cf.html