MAYO CLINIC

The Medical Physicist's Role in Digital Information Security: Threats, Vulnerabilities and Best Practices

Kevin McDonald, Director of Clinical Information Security - Mayo Clinic

AAPM Annual Meeting

Secure CAT Scanner

At least with this CAT scanner if there is any hacking we only need to worry about hairballs!

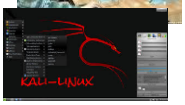
Topics

- Living and Working in a Hostile Environment
- Medical Devices In the News
- Regulatory Environment
- Evolution of Medical Devices
- Current State of Medical Device Industry
- Medical Devices and Vendors
- Simple Things to do
- Summary

Living & Working in a Hostile Environment

- Threats with multiple levels of skills & intents
  - Insiders (Current & Ex)
  - Script Kiddies
  - Hacktivists
  - Organized Crime
  - Nation State
- Active adversary must be assumed
  - Unlimited time and resources
- Skill level to cause harm is going down
- Tools to compromise and harm systems are readily available and cheap (free)
- Harm or disruption could be deliberate, collateral or unintentional



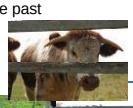
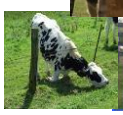


metasploit

Living & Working in a Hostile Environment

- It is not "if" but "when" you are attacked and breached
  - It is no longer just the "big guys"
- Average time from infiltration to discovery is 6 months
- A secure network and perimeter are things of the past
- Weakest links are used by attackers
  - Ecosystem protection required
  - Social engineering is eventually successful
  - Power of "Google"
  - Places you would never imagine
- Introduction of "Supply Chain" hacking
  - RSA
  - HVAC Vendors

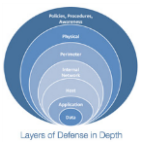
If You Stare at the Fence Long Enough…..


Living & Working in a Hostile Environment

- Medical Technology was designed and built during a kinder and gentler time
  - Devices can have service life up to 15 years
- Simple things can still make a big difference
  - Application Whitelisting
  - Patch Applications
  - Patch OS
  - Control and minimize users & administrative privileges
- It is not always a technology problem
- Defense in depth is needed
  - Data
  - Application
  - Host / Operating System
  - Network
  - Perimeter
  - Monitoring
- Software & devices must be secure "by design"
- We are ***WAY*** beyond just firewalls & anti-virus

Decreases Cyber Intrusions up to 85%



Living & Working in a Hostile Environment

- Attack Motivations
  - Revenge
  - Personal Gains
  - Bragging Rights / Status
  - Expression of Political or Social Views
  - Intellectual Property Theft
  - $$$$$
  - Identity Theft – Financial / Medical
  - Targeted Harm

Technologies & Vectors of Attacks

- Social Engineering
  - High percentage of success
  - Social networks provide victim background
  - Designed to gain access, credentials, data

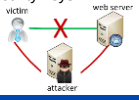
- Phishing (Spear Phishing, Whaling)
  - High percentage of success
  - Directs users to sites to capture credentials – or-
  - Downloads malware to capture credentials / data or use device as part of "botnet"
- "Drive By" Downloads
  - Infected web sites are visited and malware is downloaded
  - Sites are picked based upon desired targets
  - Downloads malware to capture credentials / data or use device as part of "botnet"

Technologies & Vectors of Attacks

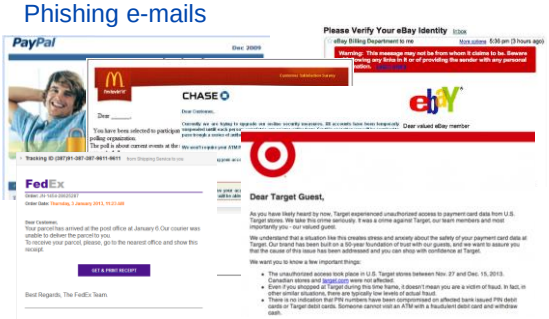
- Storage Device Transmission
  - Transmission of malware by USB / CD / DVDs
  - Used to infect devices with malware

- Poorly Configured and Vulnerable Software
  - Vulnerabilities allow an attacker to bypass applications and gain inappropriate access
- "Man-In-The-Middle"
  - Wired or wireless communications are captured
  - Can find data, user names & passwords and security keys

- Brute Force
  - Guessing of passwords
  - "Fuzzing"



Phishing e-mails



Medical Devices In The News

- Deloitte Brief - 2013
  - "Among the unintended consequences of health care's digitization and increased networked connectivity are the risks of being hacked, being infected with malware, and being vulnerable to unauthorized access."
- Gartner – Top Industry Predicts 2013
  - "By 2016, patients will be harmed or placed at risk by a medical device security breach."
- Veterans Affairs Department
  - Experienced 122 virus / malware infections in medical devices the last 14 months that had potential to harm patients
  - Launched an initiative to isolate 50,000 networked devices

Medical Devices In The News

- Department of Homeland Security – Industrial Control Systems Cyber Emergency Team Alert
  - "…reported a hard-coded password vulnerability affecting roughly 300 medical devices across approximately 40 vendors."
  - Vulnerability of internet facing medical devices
- Food & Drug Administration
  - "We are aware of hundreds of devices involving dozens of manufacturers that have been affected by cyber security vulnerabilities or incidents"
- Recent Articles
  - Wall Street Journal "Potential Cyber attacks on Medical Devices Draw Attention"
  - Reuters "FDA urges protection of medical devices from cyber threats"
  - Washington Post "FDA, facing cyber security threats, tightens medical-device standards"
  - Wired "It's Insanely Easy to Hack Hospital Equipment"

Regulatory Environment

- FDA is becoming concerned about cybersecurity
  - "We are aware of hundreds of devices involving dozens of manufacturers that have been affected by cyber security vulnerabilities or incidents"
  - Reviewing options for pre-market testing (fuzzing)
- FDA published draft cybersecurity guidance
  - Cybersecurity for medical devices and hospital networks
  - Cybersecurity for networked devices containing off-the-shelf software
  - Content of premarket submissions for management of cybersecurity in medical devices

Very (Very) Basic Guidelines

Due to external pressures and internal constraints it appears that the FDA will not be setting new security regulations

Evolution of Medical Devices

- Care is now highly dependent upon technology
- The demand and need for connectivity is rising
- Everything has, or will have, an operating system and be connected
- Medical devices are now run by purpose built computers
- Medical technology is being used to help:
  - Offset rising costs
  - Decrease medical errors
  - Improve patient outcomes
  - Improve access to care
  - Deliver specialized knowledge at the bedside

Current State of the Medical Device Industry

- Knobs, dials and switches have been abstracted into software
- Medical Technology was designed and built during a kinder and gentler time
  - Devices can have a service life up to 15 years
- 80% of medical device companies have less than 50 employees
  - Lacking general technology resources, processes and security knowledge
- Primary research, development and testing focuses on producing and assuring patient care functionality
- Misunderstand the need for FDA recertification
- Lack of "systems" thinking and understanding of attack vectors and methods
- Lack of security training and awareness
- Security is an "afterthought" (or not considered)
- Currently no competitive advantage to being secure

Vendors Naïve About Risks and the Security of Their Products

Medical Devices and Vendors

- Vendors lacking security and IT processes
  - Secure coding standards with security "tollgates" built into SDLC
  - Testing processes
    - Static / dynamic code testing
    - Fuzz testing
    - Penetration testing
    - Vulnerability scanning
  - Account and password management
    - Password complexity and requirements
    - Ability to change passwords
  - Upgrades and Patching
    - Operating systems
    - Applications
    - Middleware
  - Secure configuration standards
    - Software
    - Hardware

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Medical Devices and Vendors

- Medical Device Issues
  - Hard coded passwords
  - Unable to run basic anti-virus
  - Default settings
  - Elevated privilege requirements
  - Unencrypted data and communications
  - No patch and upgrade process
  - Poor input sanitation
  - Poor operational security
- Devices are subject to:
  - Denial of service attacks
  - Password guessing
  - Old published exploits
  - Remote exploitation

Simple (effective) Things YOU Can Do

- Use strong passwords, > 12 with #s and special characters
- Use multiple passwords, keep personal and professional passwords different
- Delete suspicious e-mails
- Don't open attachments from unknown people
- Always use clean media
- Run anti-virus on work and home computers
- Keep your operating systems and applications updated
- Limit internet activity to safe sites
- Log on as a "user" not as an administrator
- Know where your data resides

Final Thoughts

- The full medical device eco-system needs improvement:
  - Design, development, testing, support, retirement, regulation, etc
- A few simple things can make a big difference
- We will be living with this problem for at least a decade
- While vendors have a responsibility to fix their equipment, healthcare providers have a responsibility to protect patients
- Technology and knowledge exists to fix the problem, but it's not always a technology problem
- It's only a matter of time…

Resources

- SANS Critical Security Controls
  - http://www.sans.org/critical-security-controls/
- SANS Top 25 Most Dangerous Software Errors
  - http://www.sans.org/top25-software-errors/
- OWASP Top Ten
  - https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- Australian Signal Directorate Strategies to Mitigate Cyber Intrusions
  - http://www.asd.gov.au/infosec/top35mitigationstrategies.htm