The Dreaded Embedded

Secure 360
Tues. May 17, 2016

Barry Caplin
VP & CISO
Fairview Health Services
bcaplin1@fairview.org
bc@bjb.org
@bcaplin
securityandcoffee.blogspot.com
@bcaplin
http://about.me/barrycaplin
securityandcoffee.blogspot.com
o Not-for-profit established in 1906
o Academic Health System since 1997 partnership with University of Minnesota
o >22K employees
o >3,300 aligned physicians
  o Employed, faculty, independent
o 7 hospitals/medical centers (>2,500 staffed beds)
o 40-plus primary care clinics
o 55-plus specialty clinics
o 47 senior housing locations
o 30-plus retail pharmacies

2014 volumes
o 6.39M outpatient encounters
o 1.4M clinic visits
o 71,049 inpatient admissions
o 76,595 surgeries
o 9,298 births
o 282 blood and marrow transplants
o 340 organ transplants
o >$4 billion total revenue
Who is Fairview?

- Fairview Ridges Hospital
- Fairview Range Health Services
- Fairview Southdale Hospital
- Fairview Northland Medical Center
- Fairview Lakes Medical Center

Fairview Health Services

University of Minnesota

- University of Minnesota Children's Hospital
- University of Minnesota Medical Center

Ebenezer
Preferred One

Fairview Pharmacy

Maple Grove Hospital

Columbia Park Medical Group

Institute Athletic Medicine

Minnesota Sports Medicine
• For Reals?
• What’s a “Thing” and why is it on the Internet?
• Put a Chip In It
• Are Medical Devices “Things”?
• You’re doing what with my data?
• Security Concerns
• Solutions?
CSI: Cyber 11/1/15 s2/ep5 “hack E.R.”

- "Hacker group" takes over hospital
- Kills via infusion pump
- Ransom
- Weak/no auth and encryption in med devices
- Smart TV
- Hardware Poisoning
- Flat Network
- Medical Record Integrity
- Physical Access to Network
- Financial v Hacktivism
Ransomware to hit ‘lifesaving’ medical devices in 2016

Alice MacGregor Mon 23 Nov 2015 10.47am

First online murder to happen by the end of 2014, warns Europol

Alice MacGregor Tue 7 Oct 2014 12.18pm

Connected medical devices: The Internet of things-that-could-kill-you
Who’s got?...

“I asked you not to tell me that!”
Apr. 3, 2010

300K ipads
1M apps
250K ebooks
... day 1!

Toddler Buys Herself $50 Worth of iPad Apps
2011 – tablet/smartphone sales exceeded PCs
The Apple Watch has arrived, and there are already over 2,500 apps jockeying for a place on your wrist.
2016 – IOT sales exceed smartphone + tablet
We put a chip in it!  http://weputachipinit.tumblr.com/

Disco Dog – The Smartphone Controlled LED Dog Vest

Keep your dog safe and have fun too!
Introducing Disco Dog – The smartphone controlled LED dog vest.

Created by PARTY NYC

171 backers pledged $22,757 to help bring this project to life.
Medical Devices

Image: Otis Historical Archives – National Museum of Health and Medicine
Winston Churchill’s personal pressure chamber, created to enable him to make high-altitude flights safely.

Image: Andreas Vesalius/Wikimedia Commons
The first electrocardiograph, introduced by Cambridge Scientific Instruments.

Image: Hans Meyer/BIPs/Getty Images
1960: Dr G. H. Byford stands under an optokinetic drum wearing a contact lens with a miniature lamp cemented to the lens, during an experiment to investigate the reflex movements of the eyes and their association with visual illusions, at the RAF Institute of Aviation Medicine in Farnborough.

“Embedded”

- Quantified Self
- Insulin pumps, pacemakers, ICD, etc.
  - FDA requirements
  - Device manufacturers
  - Ease of connection
- Jay Radcliffe, BlackHat 2011
- Barnaby Jack, HackerHalted 2012
- *Homeland* attack (*Broken Hearts*, s2/ep10 12/2/12)
  - Wireless attack via pacemaker id/sn
  - Dick Cheney ICD, 2007
- MITM or snooping
- Integrity
- Availability
Security Challenges

- Exposure/Leakage of data – including repairs
- Poor Design/Protocols
- Ownership
- Malware
- Direct Attack
- Integrity
- Availability

But don’t we have all this now???
• Primary mechanism is... Obscurity
• Focus is on
  – Function
  – Aesthetics
  – Communication
  – Cost
  – Speed to Market
• Testing?
• Patching?
• Design?
Attack Vectors

• Sneakernet
  – USB updates or data movement
• Data Exfiltration
  – aka Breach!
• Integrity
  – Alter Capability
  – Alter Data/Reporting
• Availability
• Medjacking
  – Attack
  – Infiltrate
  – Pivot

FDA Reality

- FDA certification process
  - Complex, painful, long, expensive
- Patching and FDA advice
  - Manufacturers responsible for patches
  - Premarket review not required for security patch

http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm

http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm
We Are Not Alone

- Retail
- Manufacturing
- Energy
Solutions
• FDA, NIST and others in progress
• NCCoE/NIST/UMN TLI infusion pump security study
  https://nccoe.nist.gov/projects/use_cases/medical_devices
• Medical Device Innovation, Safety and Security Consortium (MDISS), International Society of Automation (ISA), HITRUST Alliance, NIST and others working with:
  • FDA, HHS, DOD, NHISAC, CIS (Center for Internet Security), AAMI (Association for Advancement of Medical Instrumentation), ACCE (American College of Clinical Engineering), SANS, and others
• IHE/MDISS – Medical Device Software Patching white paper
• MDS2 (Manufacturer Disclosure Statement for Medical Device Security) http://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx
• Archimedes http://www.secure-medicine.org/
• NIST SP-1800 Securing Electronic Health Records on Mobile Devices
  https://nccoe.nist.gov/projects/use_cases/health_it/ehr_on_mobile_devices
• LifeCycle and Risk Management approach
  – CyberSecurity Insurance?
• SLM – Security Lifecycle Management
• Existing?:
  – NAC
  – Scanning
  – Communications
  – Threat/Vuln Intell
  – Patching?
  – Segmentation?
  – Segregation?
Final Thoughts

- It will get worse before it gets better
- Mandatory NIST CyberSecurity Framework?
- FDA pre-market security accreditation?
- Help Vendors
  - Ask
  - Assess
  - Push back
- Help Universities
  - Connect
  - Advise
- The First Rule of Security... We Talk About Security!
  - HSPIG

SECURE360

http://mnc3.org
Barry Caplin

Fairview Health Services

bcaplin1@fairview.org
bc@bjb.org
@bcaplin
securityandcoffee.blogspot.com