The Use of Effective Cybersecurity Measures to Prevent Device Vulnerabilities

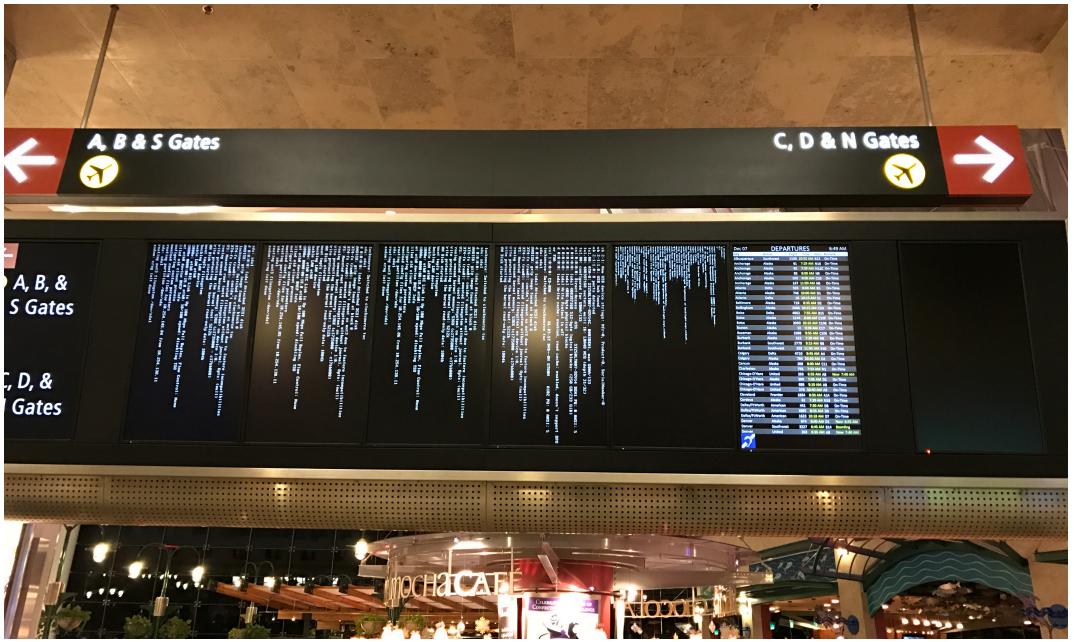
Connected Health Devices Development Conference
December 7-8, SJC
12/8/16, 1:00P

Agenda

- Who am I?
- What is Cybersecurity and why do we care?
- How safe are devices today and can your digital device really be hacked?
- Regulatory guidance and requirements in both pre-market and post-market conditions
- How to build cybersecurity into project plans and product requirements
- Hazards to consider…
- References

Cat pic

Take the red pill, Neo

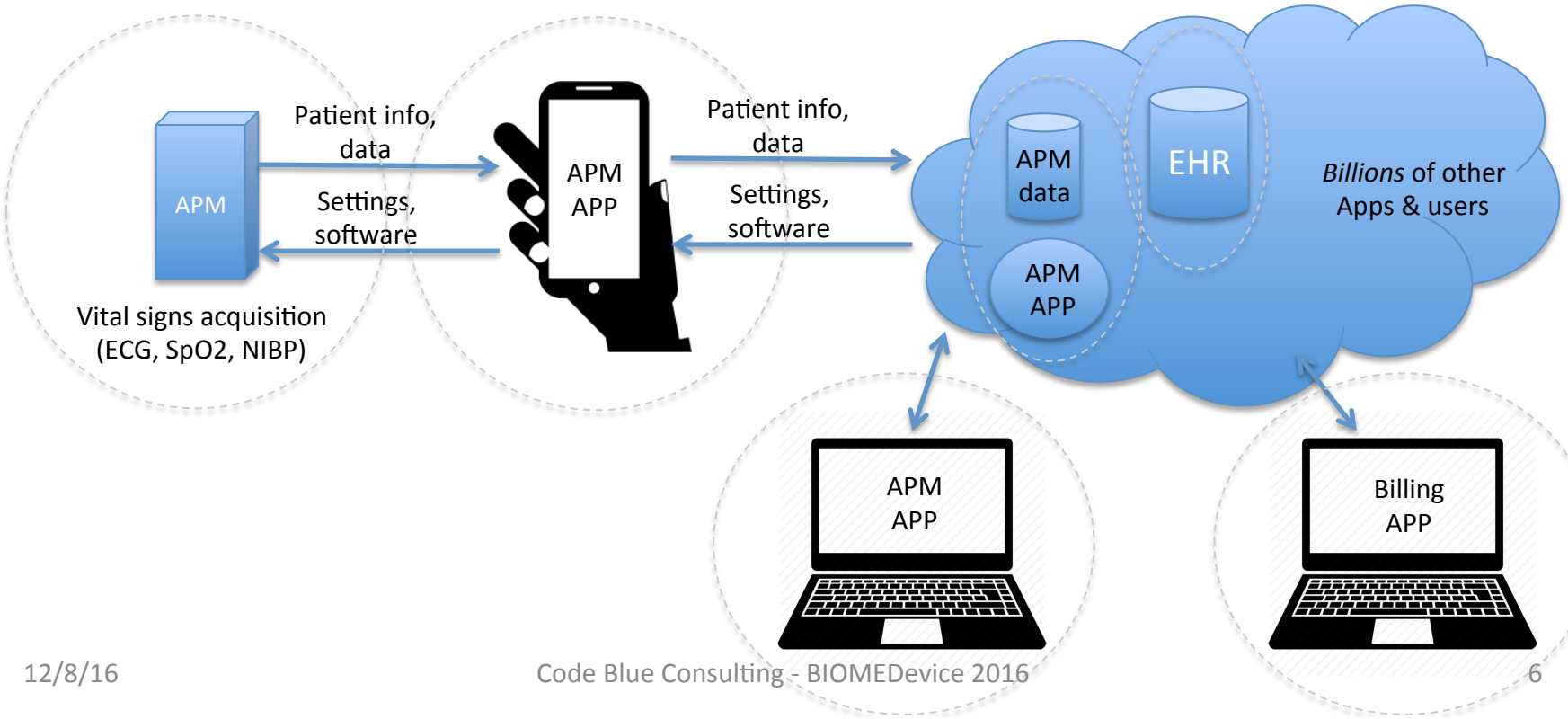


What is Cybersecurity?

Protection against the criminal or unauthorized use of electronic data, or the measures taken to achieve this

- All medical devices are now connected
- The **attack surface** of a software environment is the sum of the different points where an unauthorized user (attacker) can enter or extract data from an environment
- Examples of Medical Device data
  - Patient information (personal, medical)
  - Measurements and waveform
  - Device & network configuration and provisioning
  - Firmware upgrade
  - Security certificates
- The attack surface increases as connectivity increases

Hypothetical example: Home Ambulatory Patient Monitor



Why do we care?

- Patient lives are at stake, both directly and indirectly!
- HIPAA requirements − medical record portability & privacy
  - Protects you from unauthorized use of your medical information
  - Eg: employer discriminating for a medical condition
- FDA requirements
  - OTS software guidance
  - Premarket submission guidance
  - Postmarket management
- Your company reputation and value is at stake
  - St Jude Medical/Muddy Waters

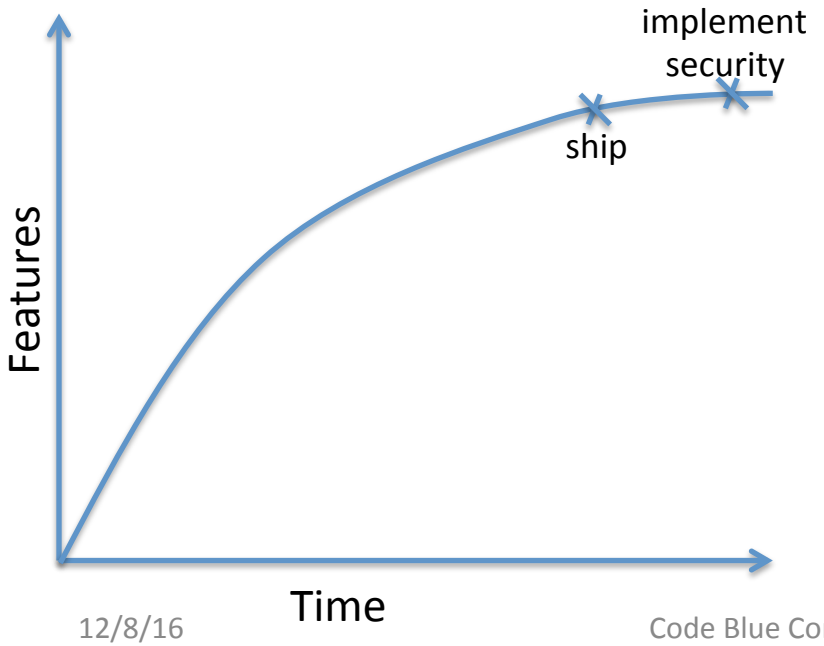
How real is this?

- Hacking is evolving and accelerating
  - Early public disclosure: "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses" - *2008 IEEE Symposium on Security and Privacy*
  - …
  - Recently: "Los Angeles Hospital Pays Hackers $17,000 After Attack" − February 2016
  - Very recently: "J&J warns diabetic patients: Insulin pump vulnerable to hacking" − October, 2016
- Medical devices are IoT devices going forward
  - The 'botnet of things'?
  - "Hacked Cameras, DVRs Powered Today's Massive Internet Outage", October 16, 2016

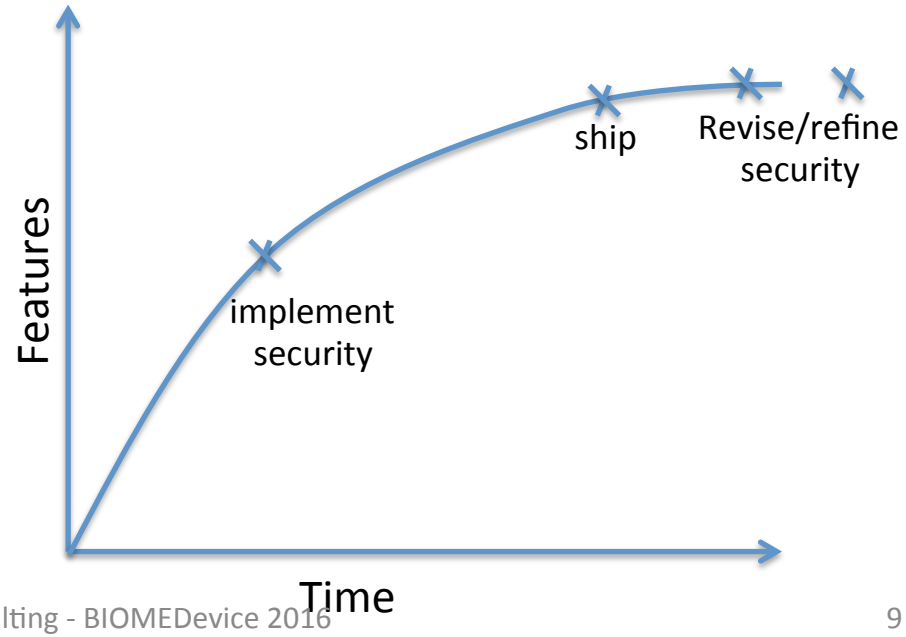
➢ All medical device designers need to design and implement *appropriate* cybersecurity measures

Why does this happen?
Development lifecycle & cybersecurity

Historical product development



Future product development



Make security part of the Product Lifecycle

- Requirements
- Specifications
- Hazard analysis/Risk analysis and management
- Testing
- Release criteria
- Continuous monitoring & improvement
  - Monitoring
  - Update releases

Risks to consider

- Unauthorized access to information
- Modification of information Misuse of information
- Denial of use
- Denial of authorized data access or product function
- Data integrity
- Open ports
- Unused/unnecessary profiles/services
- Unauthorized apps on system (BYOD)
- Service functions or entries
- Debugging code or entries
- OTS software patch doesn't get applied
- OTS software is changed without being validated
- Malware Endanger patient health Compromise identity or privacy
- Unauthorized control of product/software – risk to function/performance

Potential wireless-specific hazards

- Eavesdropping
- Spoof/mimic data connections
- OTA upgrades
- Setting changes
- Advertising

Regulatory guidance and requirements

- See references provided for specific guidance
- The FDA recently clarified guidance for software revisions due to cybersecurity
  - Highly encouraged
  - No agency submissions required
- AAMI has updated TIR57 and issued TIR59

Implementation recommendations

- Don't panic!
- Apply *appropriate* measures relative to the risk
  - Consider usability
  - Consider patient safety – can not compromise!
- Make cybersecurity part of hazard analysis and mitigation process
- Follow & read up on news – this is an evolving issue
- Think like a hacker
- Limit attack surface
- Consider connectivity changes that present new and unintended points of attack or disclosure
- Consider end-to-end data path
- Outside expertise can be helpful

Thank you!

- Q&A if time allows

Bill Saltzstein
Code Blue Consulting
bill@consultcodeblue.com
425-442-5854

Presentation from this conference

- See Presentation slides from Steve Abrahamson's presentation earlier today
  - *The Backdoor: Legacy Device Vulnerabilities and Risk*

Selected Cybersecurity References

- Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software
  - http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf
- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
  - http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf
- Postmarket Management of Cybersecurity in Medical Devices
  - http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf
- NIST: Cybersecurity Practice Guide, Special Publication 1800-1: "Securing Electronic Health Records on Mobile Devices"
  - https://nccoe.nist.gov/projects/use_cases/health_it/ehr_on_mobile_devices
- NIST: Guide to Bluetooth Security
  - http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-121r1.pdf
- ISO 14971:2007 Medical devices -- Application of risk management to medical devices
  - http://www.iso.org/iso/catalogue_detail?csnumber=38193
- HHS: Your Mobile Device and Health Information Privacy and Security
  - https://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security
- Archimedes − Ann Arbor Research Center for Medical Device Security
  - https://secure-medicine.org
- BITAG: Internet of Things (IoT) Security and Privacy Recommendations
  - http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

Recommended FDA guidance

- FDA landing page for Digital Health
  - http://www.fda.gov/medicaldevices/digitalhealth/
- General Wellness: Policy for Low Risk Devices
  - http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM429674.pdf
- Mobile Medical Applications
  - http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf
- Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices
  - http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM401996.pdf
- Radio Frequency Wireless Technology in Medical Devices
  - o http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077272.pdf
- Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices
  - http://www.fda.gov/downloads/MedicalDevices/.../ucm073779.pdf
- SOFTWARE AS A MEDICAL DEVICE (SAMD): CLINICAL EVALUATION (draft)
  - http://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm524904.pdf
- Enforcement discretion
  - http://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/ucm368744.htm

AAMI

- TIR57: Principles for medical device security—Risk management
  - https://standards.aami.org/kws/public/projects/project/details?project_id=876
- TIR59: Risk Assessment of radio-frequency wireless coexistence for medical devices and systems
  - https://standards.aami.org/kws/public/projects/project/details?project_id=1114
  - AMSI C63.27