CyberSecurity in Wireless Medical Devices

Bill Saltzstein
Code Blue Consulting
Wireless Seattle Meetup: May 30 2018

Agenda

* Who am I, and how did I get here?
* Medical devices
* Wireless connectivity
* Cybersecurity Issues
* Q&A

 Copyright (c) Code Blue Consulting 5/30/18

Why mobile medical as a case study?

* Very personal
* Communication is a driver for healthcare
* Hacking is already happening and in the news
* Concepts and architecture are universal for Enterprise and IoT

 Copyright (c) Code Blue Consulting 5/30/18

Who am I?

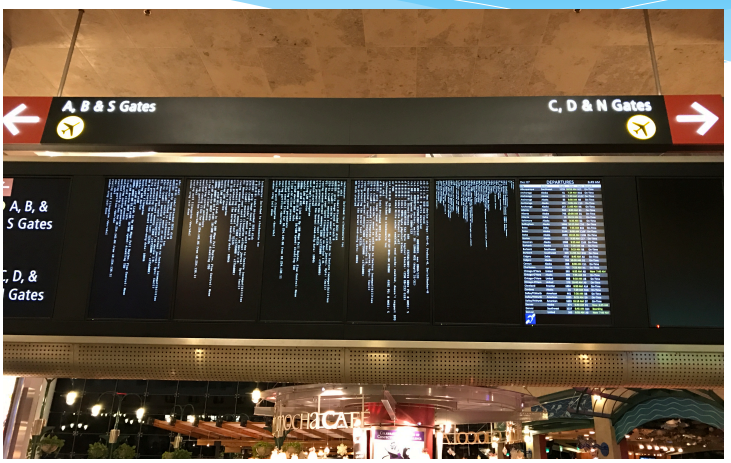
* EE, University of Rochester
* HP Calculators (HP-71B, HP-18/28)
* HP Cardiology (Pagewriter XL ECG, CodeMaster Defibrillator)
* Instromedix (LifeSigns Director Home Health)
* Medtronics Physio-Control (Dir. Adv. Dev.)
* Code Blue Communications (Bluetooth modules, consulting)
* connectBlue (VP US Sales and Marketing)
* Code Blue Consulting & Cocoanut Manor (BTLE products)
* Cinq Cellars winery (gratuitous plug)
* Seeking new clients (gratuitous plug #2)

Consumer, Type I, II, III devices, 510(k), PMA, PMAs

 Copyright (c) Code Blue Consulting 5/30/18

Take the red pill, Neo

Think about this from a medical device…



 Copyright (c) Code Blue Consulting 5/30/18

What is a Medical Device?

* A Medical Device is "… an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent…..", that is "…intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man…" or "…intended to affect the structure or any function of the body of man…" (from the US FDA)

 Copyright (c) Code Blue Consulting 5/30/18

Driving force 2018: mobile wireless

- WiFi
  - 802.11b/g/n: 2.4 GHz, DSSS/OFDM
  - 802.11a/n/ac: 5.2 GHz, OFDM with MIMO
- Bluetooth
  - BR/EDR & low energy: 2.4 GHz, FHSS
- NFC
  - 13.56 MHz (reader mode only)
- A-GPS (rcv only)
  - L1: 1575.42 MHz
  - L2: 1227.6 MHz
- Glonass (rcv only) [Russia]
  - L1: 1602 MHz (fc)
  - L2: 1246 MHz (fc)
- Galileo [EU]
- QZSS [Japan]
- CDMA EV-DO Rev. A and Rev. B (800, 1700/2100, 1900, 2100 MHz)
- UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
- TD-SCDMA 1900 (F), 2000 (A)
- GSM/EDGE (850, 900, 1800, 1900 MHz)
- FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 13, 17, 18, 19, 20, 25, 26, 28, 29, 30, 66)
- TD-LTE (Bands 38, 39, 40, 41)

Short-range Communication

Geolocation

Cellular Communication

Copyright (c) Code Blue Consulting 5/30/18

Connectivity options

- Long range wireless
  - Cellular 3G, 4G
  - 5G attempting to challenge short-range technologies, but a future
- Wired
  - LAN: wired is still a viable option as a part of the solution set!
- Short range
  - Ubiquitous
    - 802.11/WiFi
    - Bluetooth
    - NFC (Near Field Communications)
  - Other medical options
    - ZigBee (Continua), Thread (Consumer) – 802.15.4 based
    - Wireless Medical Telemetry Systems (WMTS)
    - Medical Implant Communications System (MICS)
    - MBAN (Medical Body Area Network) – virtually silent for 5 years
  - Custom…

Copyright (c) Code Blue Consulting 5/30/18

Examples

- Hospital equipment
  - Defibrillator
  - Bedside patient monitor
  - MRI
  - Infusion pump
  - …
- Chronic disease management
  - Diabetes: glucose & insulin
  - Pulmonary: COPD
  - Heart disease
  - Pain management

- Rx *delivery*
- Diagnostics out of hospital
  - External/wearable
  - Implanted
- Home Health
  - Infusion
  - Dialysis
  - Sleep apnea

Copyright (c) Code Blue Consulting 5/30/18

All medical (and health) devices *shall* be connected

- Why?
- Where?
- How?

Copyright (c) Code Blue Consulting 5/30/18

All medical devices *shall* be connected – Why?

- Connectivity
  - Electronic Health Record (EHR)
  - Charge capture (billing)
  - Big Data analytics
- Wireless is replacing wired connections
  - Mobility/safety
  - Data collection
- Telemedicine
  - Remote consultation & review (*photo*)
  - Home Health
  - Aging in Place
- Health and Fitness

Emergency!
1972-1977

 Copyright (c) Code Blue Consulting 5/30/18

All medical devices *shall* be connected – Where?

- Classic answers:
  - Hospital
  - EMS
  - Home
- Real answers:
  - Starbucks
  - 37,000 feet
  - Stuck on I-5
  - In the bathroom
  - In the elevator
- Real environments require creative solutions for connectivity

 Copyright (c) Code Blue Consulting 5/30/18

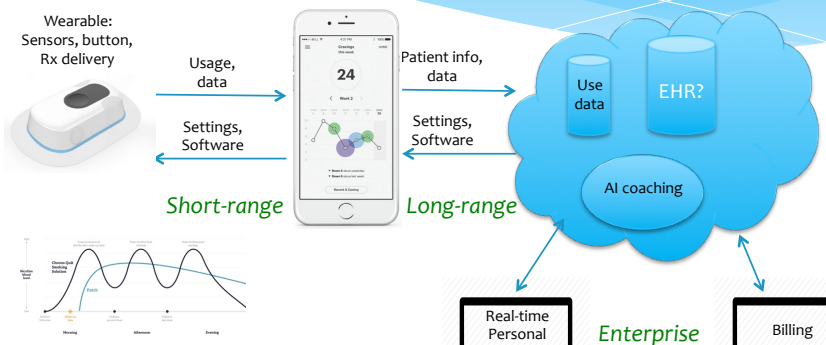
Bluetooth examples

* Medical IoT architecture - Personalized Medicine
* Continuous Glucose Monitoring (CGM) product
* Insertable Cardiac Monitoring (ICM) product

 Copyright (c) Code Blue Consulting 5/30/18

Example ***system***: Personalized Medicine

Adapted from Chrono Therapeutics smoking cessation solution (investigational)



This slide has not been reviewed or approved by the respective manufacturer. Information presented utilizes publicly available information, but may also include features that are included for illustration by this presenter, and are not part of the actual system.

 Copyright (c) Code Blue Consulting 5/30/18

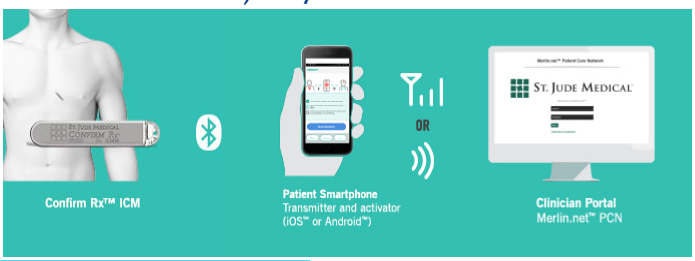
Continuous Glucose Monitoring

* Dexcom G5® Mobile CGM System
* Wearable sensor with Bluetooth to phone as a primary display
* Watch as a secondary display
* FDA Approved for iOS (2015) and Android (2017)
* Similar system architecture as previous example

This slide has not been reviewed or approved by the respective manufacturer. Information presented utilizes publicly available information, but may also include features that are included for illustration by this presenter, and are not part of the actual system.

Insertable Cardiac Monitor

* Abbott Confirm™ RX ICM
* "The world's first smartphone-compatible ICM"
* FDA cleared October, 2017



This slide has not been reviewed or approved by the respective manufacturer. Information presented utilizes publicly available information, but may also include features that are included for illustration by this presenter, and are not part of the actual system.

CyberSecurity issues for Medical Devices and networks

* All medical devices are now connected
* Medical Device data
  * Patient information (personal, medical)
    * PHI (Protected Health Information)
  * Measurements and waveform
  * Device & network configuration and provisioning
  * Device settings
  * Firmware upgrade
  * Security certificates
* The attack surface increases as connectivity increases

 Copyright (c) Code Blue Consulting 5/30/18

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
* Company reputation and value is at stake
  * St Jude Medical/Muddy Waters
* Attack-of-the-month
  * Ransomeware
  * Blueborne
  * Krack
  * Meltdown & Spectre

 Copyright (c) Code Blue Consulting 5/30/18

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*
* 2015 - Hospira infusion pumps: https://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/
* "Los Angeles Hospital Pays Hackers $17,000 After Attack" – February 2016
* Muddy Waters & St Jude Medical: implant vulnerabilities and short-sale profit – August 2016
* "J&J warns diabetic patients: Insulin pump vulnerable to hacking" – October, 2016
* Numerous hospital ransomware attacks – 2018
* The value of a healthcare record/contact on the Dark Web is quite high!

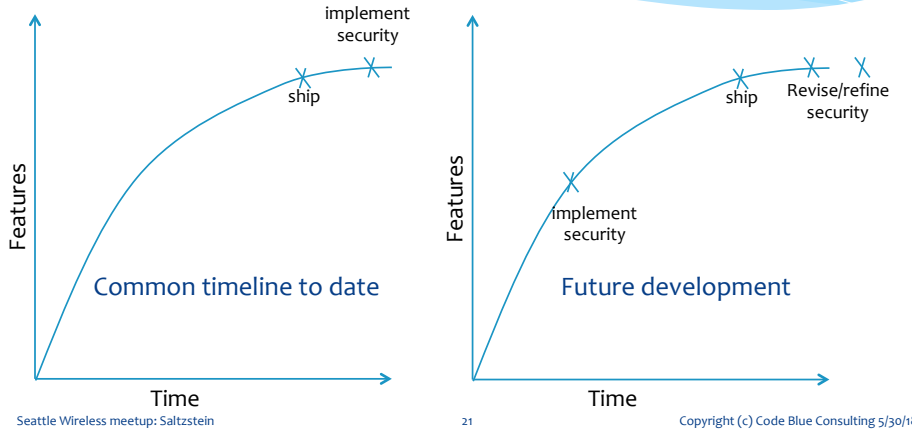
 Copyright (c) Code Blue Consulting 5/30/18

Cybersecurity recommendations

* Security by design, not obfuscation
  * End-to-end solution, both connectivity and at rest
  * Design for Cybersecurity
  * Design for Privacy
* Limit information: don't exchange unnecessary data
* Limit vulnerabilities
  * Limit time and accessibility
    * Pairing
    * Security key exchanges
  * Eliminate unnecessary ports
  * Don't use unnecessary profiles
  * Set and enforce policies
* Don't advertise promiscuously – Bluetooth & WiFi

 Copyright (c) Code Blue Consulting 5/30/18

Why does this happen? Development lifecycle & cybersecurity



 Copyright (c) Code Blue Consulting 5/30/18

Making security part of the Product Lifecycle

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

 Copyright (c) Code Blue Consulting 5/30/18

Cybersecurity design 'tools'

* Hazard/risk analysis and mitigation approach
  * SYSTEM wide, end-to-end is essential
  * From design inputs through entire process
* Decide what is appropriate risk and mitigation
* Establish trust and security
  * Authentication
  * Encryption
* System policies and recommendations for use

 Copyright (c) Code Blue Consulting 5/30/18

Risks to consider - examples

* Modification of information Misuse of information
* Denial of use
* Open ports
* Unused/unnecessary profiles/services
* Unauthorized apps on system
* Debug ports, code or 'back doors'
* Off The Shelf (OTS) software patch doesn't get applied
* OTS software is changed without being validated
* Malware Endanger patient health Compromise identity or privacy

 Copyright (c) Code Blue Consulting 5/30/18

Potential wireless-specific hazards

* Security/authentication without physical connection
  * Spoof/mimic data connections
  * Eavesdropping
* Man in The Middle (MTM) attacks (especially during pairing)
* Over The Air (OTA) upgrades
* Setting changes
* Advertising promiscuously

 Copyright (c) Code Blue Consulting 5/30/18

US Medical regulatory guidance and requirements

* US FDA
  * Guidance documents for software
  * Landing page, meetings, webinars, reports, discussions
* The FDA clarified guidance for software revisions to speed software updates due to cybersecurity
* NIST Cybersecurity Framework
* Recent US Government report: "Report on Improving Cybersecurity in the Health Care Industry"
* See references provided for specific guidance

 Copyright (c) Code Blue Consulting 5/30/18

My advice to clients

- Don't panic, but think like a hacker
- Apply *appropriate* measures relative to the risk
  - Consider usability
  - Consider patient safety – can not compromise!
- Make cybersecurity part of hazard analysis and mitigation process
- Make cybersecurity part of the product lifecycle
- Must consider end-to-end data path
- Use industry standard encryption and authentication
- Consider additional app-level authentication
- Follow & read up on news – this is an evolving issue
- Limit attack surface
- Consider connectivity changes that present new and unintended points of attack or disclosure

 Copyright (c) Code Blue Consulting 5/30/18

Question & Answer & Discussion

Bill Saltzstein
Code Blue Consulting
billsalt@consultcodeblue.com
425-442-5854
www.consultcodeblue.com
http://www.linkedin.com/in/billsaltzstein

 Copyright (c) Code Blue Consulting 5/30/18

Selected Cybersecurity References

- Healthcare Industry Cybersecurity Task Force report
  - https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf
- 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

 Copyright (c) Code Blue Consulting 5/30/18

Additional FDA guidance

- FDA landing page for Digital Health
  - http://www.fda.gov/medicaldevices/digitalhealth/
- General Wellness: Policy for Low Risk Devices
  - https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/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
- Software as a Medical Device (SAMD): Clinical Evaluation
  - https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM524904.pdf
- Clinical and Patient Decision Support Software (draft)
  - https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm587819.pdf
- Changes to Existing Medical Software Policies Resulting from Section 3060 of the 21st Century Cures Act (draft)
  - https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm587820.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
- Enforcement discretion
  - http://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/ucm368744.htm
- Deciding When to Submit a 510(k) for a Software Change to an Existing Device
  - https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm514737.pdf
- Design Considerations and Pre- market Submission Recommendations for Interoperable Medical Devices
  - https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm482649.pdf

 Copyright (c) Code Blue Consulting 5/30/18

AAMI

* TIR57: Principles for medical device security—Risk management
  * https://standards.aami.org/kws/public/projects/project/details?project_id=876
* TIR69: Risk Assessment of radio-frequency wireless coexistence for medical devices and systems
  * https://standards.aami.org/kws/public/projects/project/details?project_id=1114
* ANSI C63.27-2017: American National Standard for Evaluation of Wireless Coexistence
  * https://standards.ieee.org/findstds/standard/C63.27-2017.html

 Copyright (c) Code Blue Consulting 5/30/18

Bluetooth SIG

* Transcoding (and other) Whitepapers:
  * https://www.bluetooth.com/develop-with-bluetooth/white-papers
* Bluetooth 5 Standard:
  * https://www.bluetooth.com/specifications/bluetooth-core-specification

 Copyright (c) Code Blue Consulting 5/30/18

Acronyms (google for definitions/information)

* AFH – Adaptive Frequency Hopping
* BLE – Bluetooth low energy
* BR/EDR – Basic Rate or Enhanced Data Rate (See Bluetooth specifications)
* FHSS – Frequency Hopping Spread Spectrum radio transport
* ISM – Industrial, Scientific, and Medical: frequency bands allocated by the FCC
* LAN – Local Area Network: IEEE 802.3
* MBAN – Medical Body Area Network
* MDDS – Medical Device Data System (see Reference section)
* NFC – Near Field Communications
* PHI – Protected Health Information
* SIG – Special Interest Group, in this case the Bluetooth SIG
* WiFi – Wireless Fidelity: IEEE 802.11 specifications
* ZigBee – Wireless standard from the ZigBee Alliance, based on IEEE 802.15.4

 Copyright (c) Code Blue Consulting 5/30/18