RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Turning Medical Device Hacks into Tools for Defenders

SESSION ID: HTA-R03

Tim West
Senior Consultant
Accuvant Advisory Services
@west_tim

Jamie Gamble
Principal Consultant
Accuvant Research
@bitgamble

Drivers to this Project

Medical device research has been on offensive security – generating little defensive mechanisms beyond ‘don’t make this mistake’ & our experiences see consistent gaps

FDA & market forces are weak in driving maturity; healthcare continues to stagnate in medical device security

Compelling reasons have emerged for focus on medical devices to be a strategic initiative now

To help the community, our project releases a draft version of medical device security assessment framework, 1st publically published, open-source work we’re aware of

Framework consolidates published works, controls, and methods for assessing device risks in context to healthcare organizations

Goals & Motivations for this Session

Conference Swag:
Not the only take-away

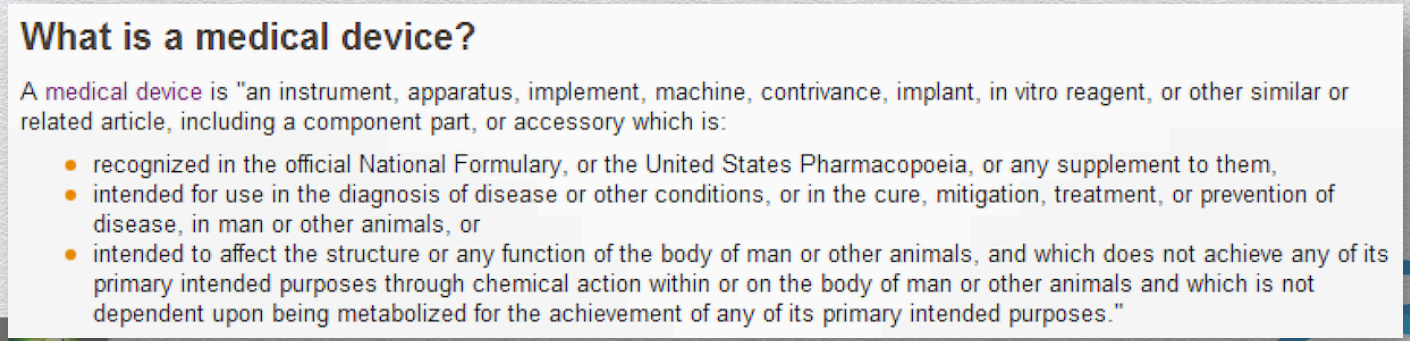
Agenda

- The Problem
- Why now? Compelling Reasons to Secure
- Taking on the Traditional Challenges
- Lessons Learned & Tool Explained
- Conclusions

Medical Device Security as an Oxymoron

What is a Medical Device?

- Delivers or is utilized directly for clinical care
- Can be implantable, embedded, stand-alone, client-server application, etc…
- Traditionally not managed by “IT” but “Clinical or Biomedical Engineering”
- FDA Definition:



What is a medical device?

A medical device is "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is:

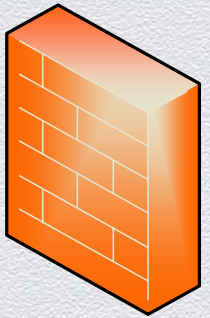
- recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them,
- intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or
- intended to affect the structure or any function of the body of man or other animals, and which does not achieve any of its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of any of its primary intended purposes."

The Problem - At Design

Lack of Market Forces	Buyers or sellers do not currently adopt any standard security practices
Regulatory Forces	Medsec exclusively “HIPAA & FDA Compliant”, by definition does **not** include specific or tangible security requirements
Complexity	Typically made up of a variety of interoperable hardware/software supported by multiple organizations
Accountability	Devices sold through distributors lack accountability for maintenance; no revenue model in security

Today's Medical Device Security Architecture

Medical Device



Perimeter Firewall

Unwashed Masses

Problem Solved!

Why Now?

3 Compelling Reasons to Secure Now

Drivers to Mature Medical Device Security

Three areas we'll discuss:

- Expanding Security & Privacy Environment – Healthcare is adopting cloud-based systems, large-scale data sharing, remote disease management, telemedicine, & at-home models
- Awareness - Press is driving headlines of medical device hacks from security researchers
- Regulators - (FDA, VA) are taking note & publishing guidance

Expanding Security & Privacy Environment

The Glooko System at a Glance

Technology Unification

Glooko transfers glucose readings and related data from many meters into supported iOS or Android devices.

Learn more ▸

Real-Time Contextualization

Quickly record food choices, medication, exercise, and notes into your Glooko logbook.

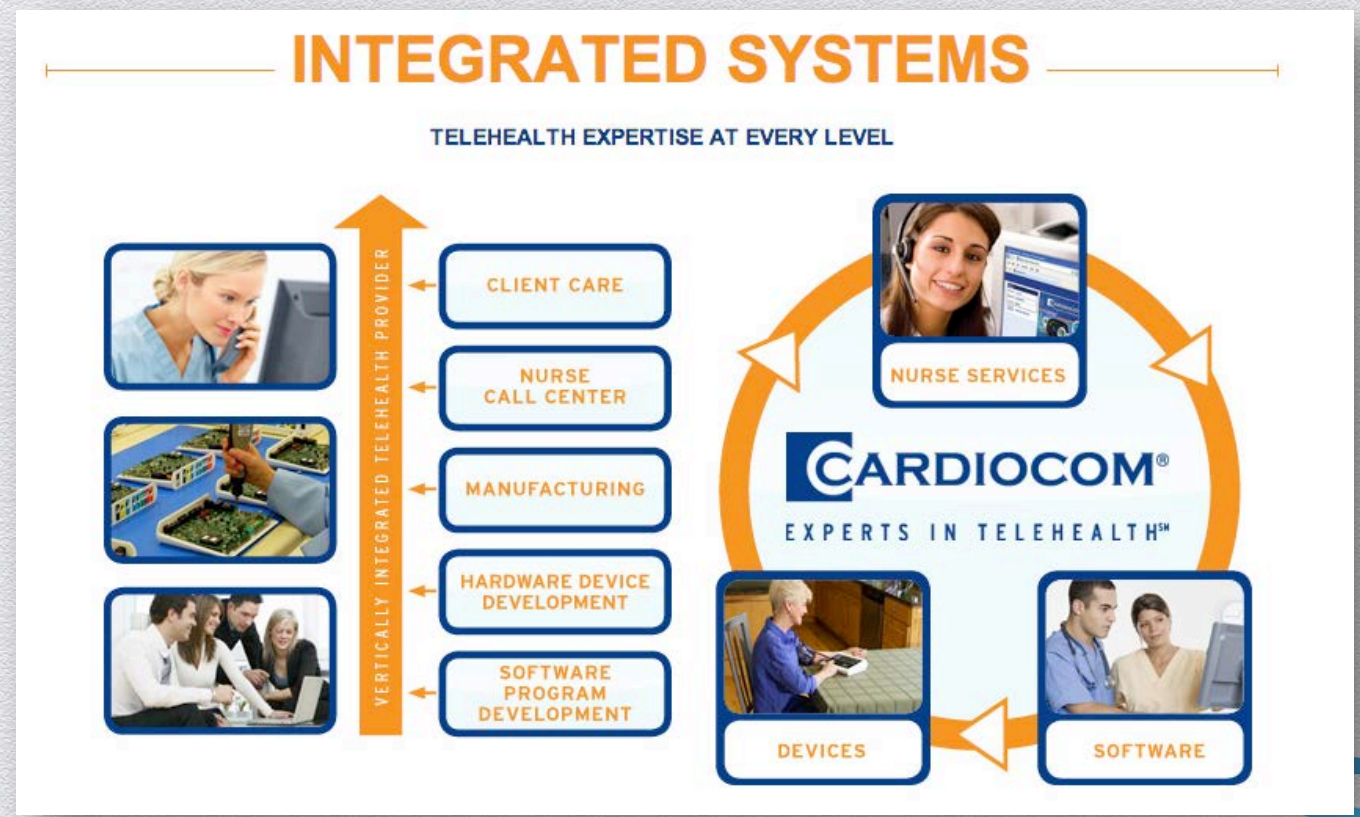
Learn more ▸

Seamless Data Interpretation

Using Glooko's analytical tools, support teams can assess and optimize treatment plans.

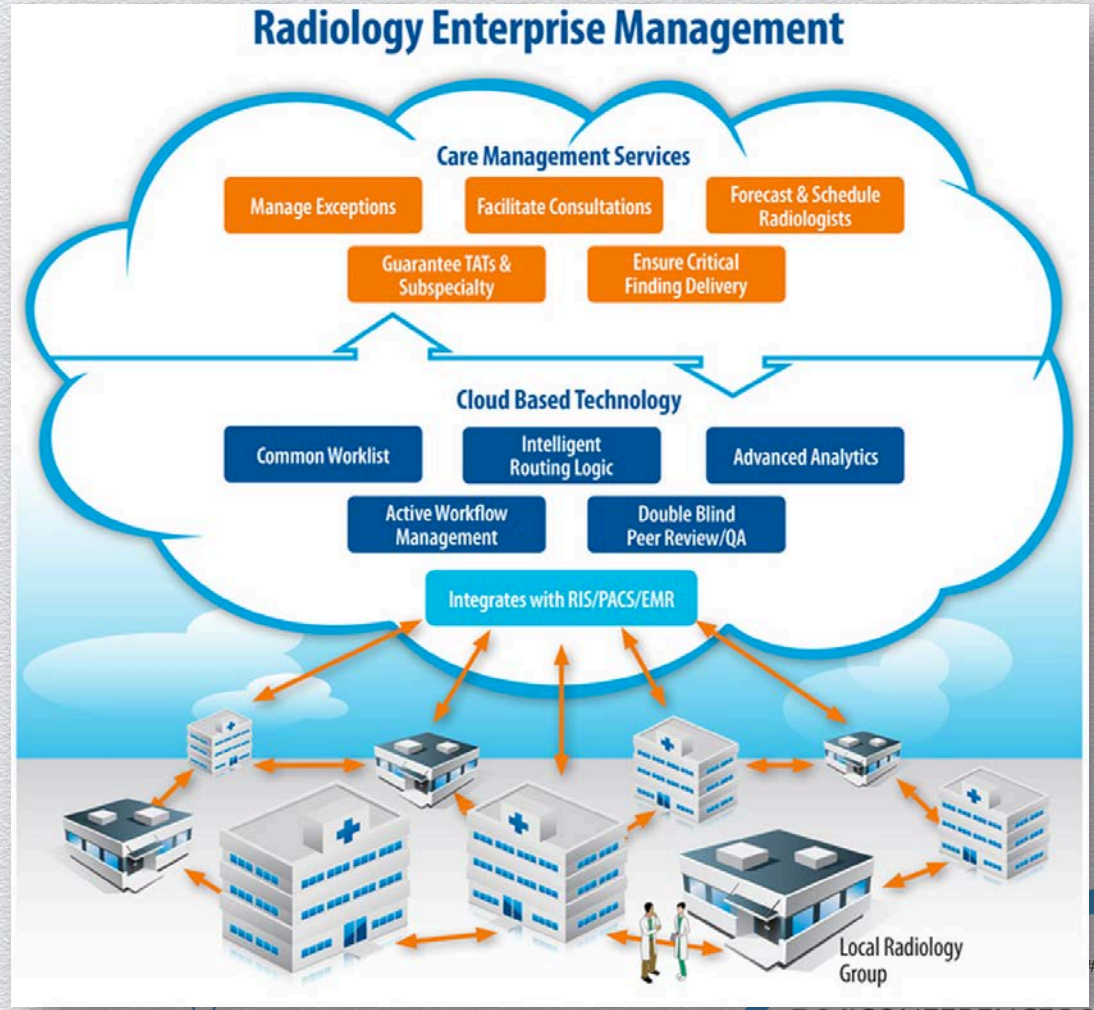
Learn more ▸

Expanding Security & Privacy Environment



Security's Expanding Role

Advancements mean more complex risk profiles, integration points, and context for information security professionals to understand & manage.



Security Researchers - In the Beginning…

Dr Kevin Fu – U of Michigan

First Popularized Med Hack

- 2008 Black Hat Talk: Implantable Cardiac Defibrillator
- Sophisticated & unpractical research for generalized audience
- Vulnerable via hard-coded passwords & RF replay attacks

Next Big Splash

Jay Radcliffe

Insulin Pumps

- 2011 Black Hat Talk & others
- Device data not Encrypted or Authenticated
- Protocol Analysis & Reversing Required to Understand Security Posture

Also Recently…

Barnaby Jack

Insulin Pump

- RSA 2012
- Received national press on exploitation of medical devices
- Also Insulin Pumps; showcased ease of impersonation attacks
- The very few CVEs/OSVDB stubs on medical devices are Barnaby's

Regulatory Response?

U.S. Department of Health and Human Services

U.S. Food and Drug Administration
Protecting and Promoting *Your* Health

A to Z Index | Follow FDA | FDA Voice Blog

Search FDA

Home | Food | Drugs | Medical Devices | Radiation-Emitting Products | Vaccines, Blood & Biologics | Animal & Veterinary | Cosmetics | Tobacco Products

Medical Devices

Home › Medical Devices › Medical Device Safety › Safety Communications

- Medical Device Safety
- Safety Communications
- Information About Heparin
- Medical Device Safety Archive
- Tubing and Luer Misconnections: Preventing Dangerous Medical Errors

FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks

Date Issued: June 13, 2013

Audience: Medical device manufacturers, hospitals, medical device user facilities, health care IT and procurements staff; and biomedical engineers

Issue: Cybersecurity for medical devices and hospital networks

Purpose: The FDA is recommending that medical device manufacturers and health care facilities take steps to assure that appropriate safeguards are in place to reduce the risk of failure due to cyberattack, which could be initiated by the introduction of malware into the medical equipment or unauthorized access to configuration settings in medical devices and hospital networks.

Summary of Problem and Scope: Many medical devices contain configurable embedded computer systems that can be vulnerable to cybersecurity breaches. In addition, as medical devices are increasingly interconnected, via the Internet, hospital networks, other medical device, and smartphones, there is an increased risk of cybersecurity breaches, which could affect how a medical device operates.

Details?!

So What Have We Learned?

- Offensive Security Talks Provide Awareness & Press, limited tangible take-aways for defenders & manufacturers beyond those involved in the specific tech
- Content is device specific & embedded device centric – medical devices expand beyond and include more complex technology
- Despite motivation for improved security few means or mechanisms to assess, improve, and monitor device security risk exist

Traditional Challenges to Device Security

Vendor Supported is the Norm

- Clinical or Biomedical devices are almost all vendor owned or supported
- Support does not typically entail data or system security requirements
- “FDA Approval Required” to make changes, consistently quoted by vendors as a restriction to patch or update medical devices
- Remote support required and implemented as an after-thought

Clinical Engineering is Different

- Relies on server, network, & data center teams to provide Infrastructure & other traditional IT services
- Independent function of the organization (typically), not in “IT” but aligned with users (clinicians & care providers)
- Focus on the clinical outcomes & operational capabilities of the technology; privacy & security can be an afterthought
- Has had checkbox approaches to security with reliance on vendor statements of “HIPAA Compliance Solution” stamped on box

Network Security

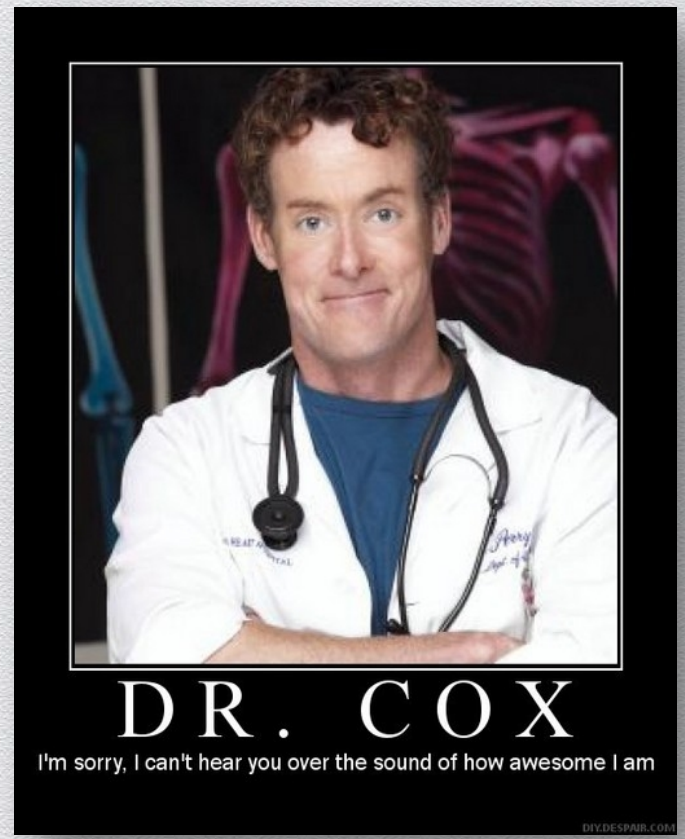
Traditional Hospital Network is Flat:

- No security between segments prohibiting routing between user environments, data-centers, & clinical space
- VLANs where everything is routable does not provide security

Network Access Controls (NAC) is rare or only partially implemented:

- No device authentication/802.1x
- Public space with wired connections provide production network access
- Wireless networks frequently provide production network access

Who Purchases Medical Devices?



Introducing… Tools for Defenders

Central Tenets on Building Tool Must:

- Work within current constraints (No Perfect Recommendations)
- Adapt security domains to apply to environment & typical buy/maintain scenarios
- Be tactically valuable to the typical Security Manager/Officer
- Map (where possible) to publically available open-source guidance such as NIST, OWASP, SANS, CIS, etc…

Tool Defined

- Defined security model with 10 security domains
- 20 questions defining medical device capabilities & security implications (internal vs external, data types used, user interactions, ownership of functions, etc…)
- ~100 control questions dependent on capabilities

No.	Domain Area	Description
1	Acquisition & Implementation*	Tackling vendor support
2	Network Security*	Hardening network access
3	Access Controls*	User AAA
4	Device Hardening*	Encryption & device specification callouts for devices
5	Physical Security*	On premise or remote security considerations
6	Software Security*	Managing app level security & data transactions
7	Mobile Security*	Mobile specific security concerns (pins, encryption, etc…)
8	Privacy Implications*	Storage or use of PII/PHI as a business process
9	Incident Response	Security event & breach response a la HITRUST & SANS
10	Compliance & Regulatory	Ensure ownership & consideration of applicable regs

**Denotes potential manufacturer responsibilities*

Domain 1: Acquisition & Implementation

MedSec Challenges

- Vendor owned & operated
- Limited visibility

Related Control Examples

- Network security contract requirements
  - Includes remote access, individual & strong access controls, SLAs
- Define ownership of security management essentials: patching, configurations, etc…
- Review physical security of off-site if including managed services/infrastructure
- Define vendor responsibilities in assessments

References

NIST

Sante Fe Group SIG

Domain 2 – Network Security

MedSec Challenges

- Physical access expected in public areas
- Significant segmentation not viable

Related Control Examples

- Practical advice for eliminating passwords in favor of some type of token
- Practical segmentation (VLAN &/or FW with ACLs) for data, users, & clinical devices
- Security event monitoring on clinical devices with platform OS

References

NIST 800-115 (Assessments)

NIST 800-97 (Wireless)

VA Medical Device Security Architecture Guidance

NSA Network Security Guide

DISA STIG

Domain 3 – Access Controls

MedSec Challenges

- Widely diverse user-base: clinicians, patients, users, vendors, etc…
- Possible remote access outside of customer network (web portals, remote management)

Related Control Examples

- Guidance on when to use two factor authentication, tokens, & centralized auth
- Hardening advice for systems that are left with untrusted users
- Multiple use cases to review &/or assess for default admin or shared credentials
- Recommendations on managing provisioning

References

NIST IR 7316

NIST Healthcare RBAC Content

Domain 4 – Device Hardening

MedSec Challenges

- Cannot assume centralized management
- Vendor ownership of configuration likely

Related Control Examples

- Review &/or assess for CIS standards for platform OS; don't buy "limited kernel"
- Checklist style configuration hardening instructions for generic network services and functionality (e.g. remote login, name resolution, Web applications, authentication)
- Include event logging, authentication controls, and system updates
- Review if subcomponents have been hardened by manufacturer

References

NIST Standards

CIS Benchmarks

DISA STIGs

Domain 5 – Physical Security

MedSec Challenges

- Hospitals are public; Patient access or others typical

Related Control Examples

- Ensure physical ports (USB, serial) are restricted with locks or only to admin personnel
- Ensure administrative access is restricted (consoles, interfaces) & on separate network segment
- Ensure vendor access is managed with similar controls for access (badging, escorts, etc…)

References

NIST 800-12 Chapter 15

ISO standards

IAHSS

Domain 6 – Software Security

MedSec Challenges

- Data possibly managed or shared with vendor
- Software decisions define security, privacy, & multiple other security areas

Related Control Examples

- Require application security reviews on significant investments (web application review, source code, etc…)
- Ensure patient data is obscured encrypted; MRNs are not included in any data loss
- “Phone home” data is reviewed

References

NIST 800-64v2

OWASP

Domain 7 – Mobile Security

MedSec Challenges

- PHI likely on mobile devices (tablets, phones, etc…)
- Unique technology implications of securing on mobile platforms

Related Control Examples

- Ensure encryption on mobile devices
- Review internal ‘remote-wipe’ capability on mobile devices in case of account termination
- Define authentication practices (tokens, lock-out, password settings & storing)
- Inventory management concerns with mobile proliferation
- Define local data caching settings

References

NIST 800-164 (Hardware in Mobile Devices)

OWASP

Domain 8 – Privacy Implications

MedSec Challenges

- HIPAA Privacy Rule implication in use and management of data for business practices

Related Control Examples

- Ensure use and review of patient data access is logged (& preferably centralized)
- Ensure user access controls are capable to specific role groups
- Patient data is masked in use of data (where appropriate)

References

NIST Preliminary Cybersecurity Framework?
Draft in progress

HIPAA Privacy Rule

Domain 9 – Incident Response

MedSec Challenges

- Regulatory requirements inform breach notification & management but leave process to the covered entity (CE) & business associate (BA)

Related Control Examples

- Ensure use and review of patient data access is logged (& preferably centralized)
- Define vendor notification requirements (likely vague in BAA) to include what triggers notification & timeliness to ensure CE has enough time
- Review & document what data types are included in data transfer to know regulatory requirements if breach occurs (SB 1386, HITECH, other state laws)

References

- NIST 800-61 Incident Handling
- HITECH Act
- Applicable State Laws (CA, MA, IN)
- SANS Critical Control 18 & SANS Institute

Domain 10 – Compliance & Regulatory

MedSec Challenges

- HIPAA Privacy Rule implication in use and management of data for business practices

Related Control Examples

- Define all requirements associated with this purchase & ownership of items prior to implementation
- Review any artifacts required as a function of regulations: HIPAA risk assessments for Business associates, for instance

References

Unified Compliance Framework

HIPAA Security, Privacy, & HITECH

The Work Ahead

Soliciting Industry Contributors

Healthcare Providers

- For implementation controls, looking for organizations to evaluate adopting methodology at acquisition of new technology, collaborate on control framework, & implementation guidance.

Manufacturers

- For design driven controls, looking for organizations to evaluate adoption to collaborate on “Vendor challenge areas” & assessment techniques

Charting Progress Ahead

Want Draft Content?

- Reach out below, we want to work with you!

Want Final Content?

- Targeting BlackHat, 7/31 for **public** release

Send us feedback & recommendations & PLEASE VOTE!

Tim West
@west_tim
twest@accuvant.com

Jamie Gamble
@bitgamble
jgamble@accuvant.com