Building and Testing Medical Devices for Robustness

An overview of challenges and a path forward

Codenomicon Ltd.

Mike Ahmadi, Global Director of Medical Security

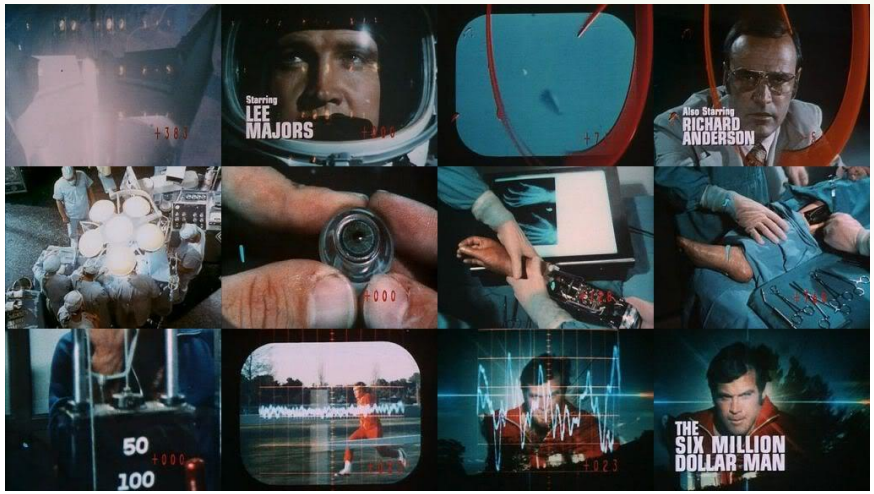
September 2014

Better Living Through Technology

Electronic medical devices became computerized and then networked.

We have moved far past science fiction in recent years.

Networking capabilities make delivering healthcare more affordable, more efficient, and more tolerable by the patient.

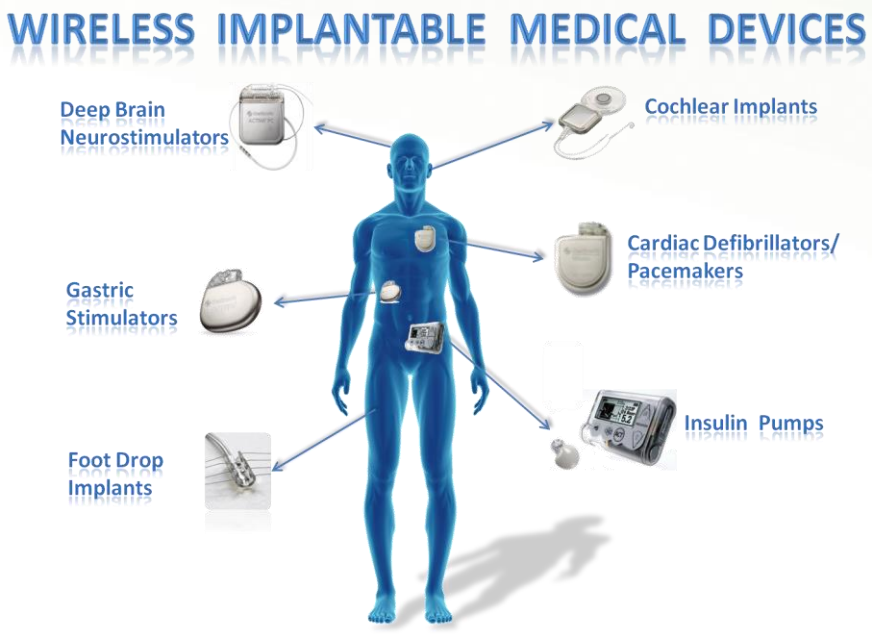


Reliance On Technology and Connectivity

As technology improves and becomes more connected we become more reliant on it.

It is reasonable to assume our reliance on technology and connected medical devices will only continue to rise.

It may also be reasonable to assume that most (if not all) of us will have something electronic embedded in us at some point.



@CodenomiconLTD

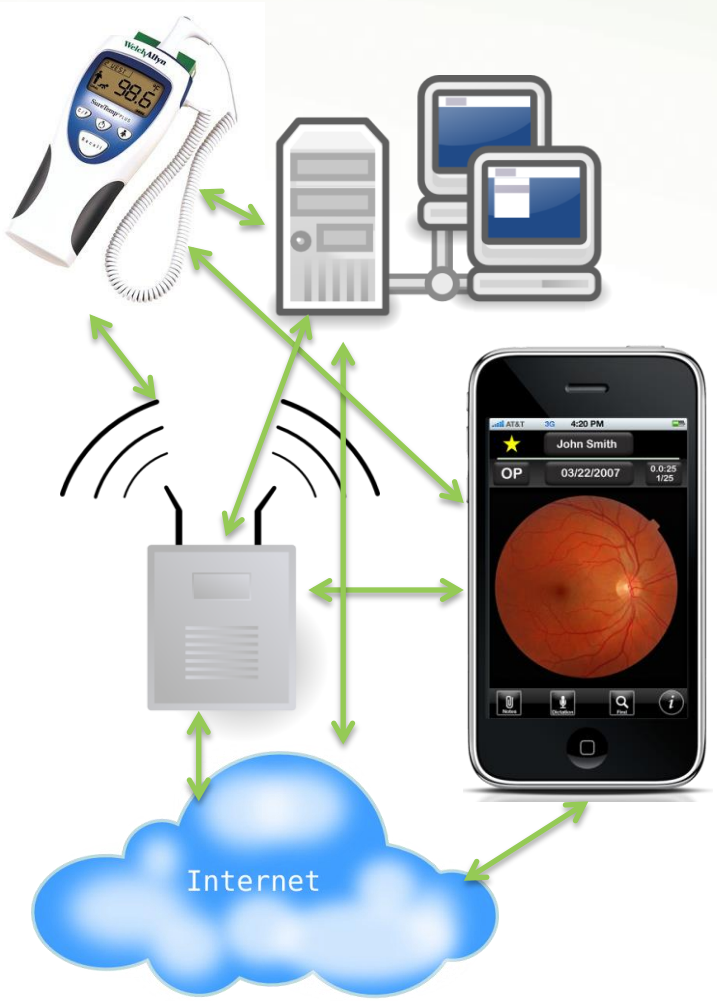
The Dynamic Medical Network

Medical devices have become network devices.

The network is constantly evolving and expanding from moment to moment.

Every change in technology has a potential effect on every network the technology lives on…and every device on the network.

How a device responds to change is important to know.



@CodenomiconLTD

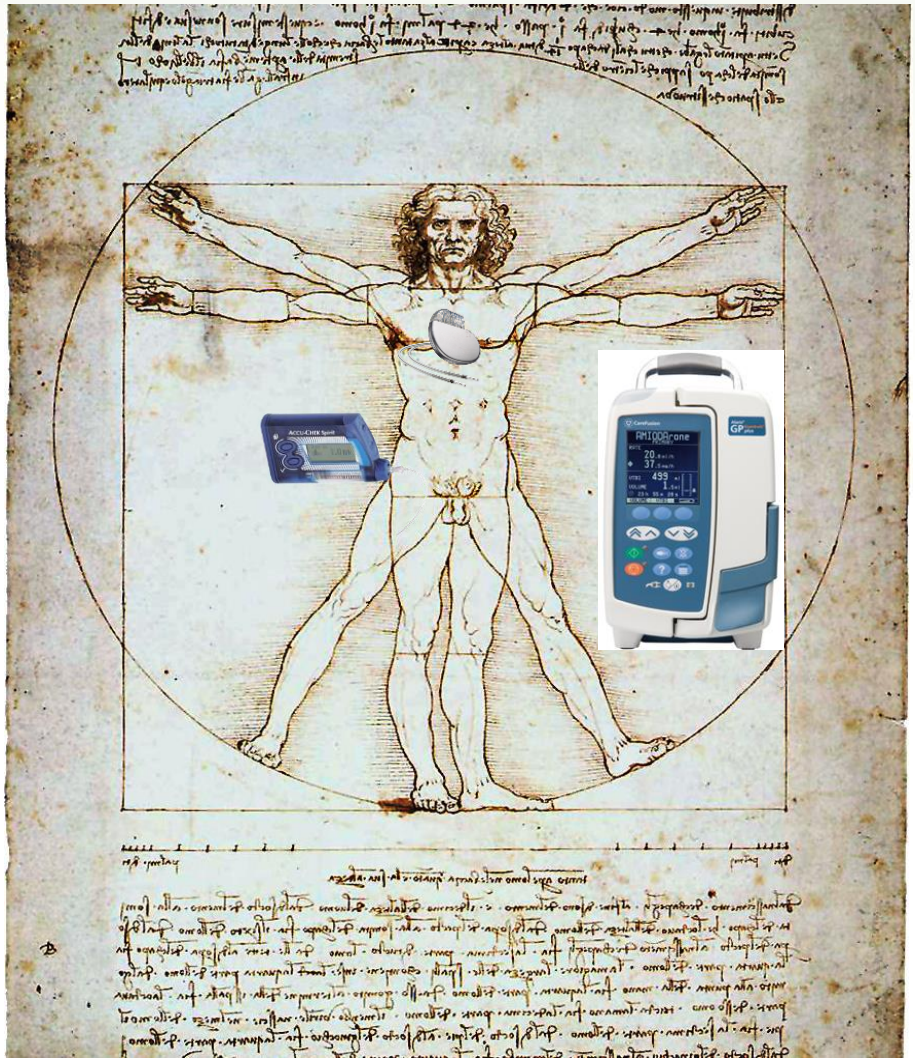
Vital Organs and Vital Devices

Without vital organs we cannot live.

When devices are added to the human system that are needed to sustain life, they become the equivalent of vital organs.

A “digital disease” or “digital pathogen” is just as deadly to a human in this case as a carbon-based disease or pathogen/

Devices that have these digital vulnerabilities are essentially like diseased organs.



Managing Medical Device Health

We need to manage the health of vital devices like we manage health in biological systems.

We do not assume a clean bill of health from a doctor is applicable to our entire life.

Things change internally and externally that affect our health…and our health generally degrades over time, requiring changes both internally and externally to improve our health.

This is essentially what happens with medical devices, and at an accelerated pace once networked…so devices and networks must be constantly checked for health over time.

Vulnerabilities and Where They Come From

Vulnerabilities are any conditions in software or hardware that can lead to a compromise of confidentiality, integrity, and availability.

Software vulnerabilities are a result of coding errors introduced during software development (bugs).

These coding errors can lead to buffer overflows, race conditions, denial of service, and other conditions that can cause systems to not function as intended…or completely fail.

The Vulnerability Lifecycle

Inception: Ideally a vulnerability **should be detected during product development**, where mitigation is easiest to implement. At this point it is only a bug. Bugs that are not detected in development end up becoming part of a product deployment

Deployment: Bugs that end up in deployed products can quickly spread, depending on how widely deployed the products are. When bugs are eventually discovered (post deployment), they become legacy bugs, and it becomes critical to determine how widely deployed the newly discovered known vulnerability has become. **The longer it takes to discover, the more widespread the problem becomes.**

Proliferation: Once the vulnerability is known, it is ripe for exploitation, and the next stage is **to identify if the bug has been exploited, and how widespread the threat is**.

Who Discovers The Vulnerabilities

Security Researchers – Generally "White Hat" hackers who look for ways to sidestep the rules for the purpose of fixing the issues.

Non-Malicious Actors – Someone who is curious and experiments until something fails to protect.

End Users – Someone using the device or system that stumbles upon a vulnerability in normal or abnormal use.

Malicious Actors – Someone who intentionally breaks in, with the intention of causing havoc or harm.

Who Should Be Discovering The Vulnerabilities

The device/system manufacturer engineering teams during the development lifecycle !

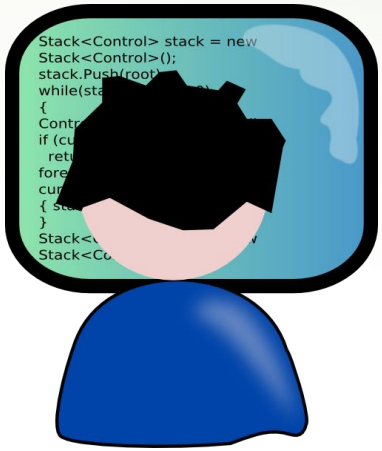
The quality assurance (QA) team should perform final testing and analysis before releasing the product !!

Device manufacturers and end users should test long after deployment to determine if new vulnerabilities arise !!!

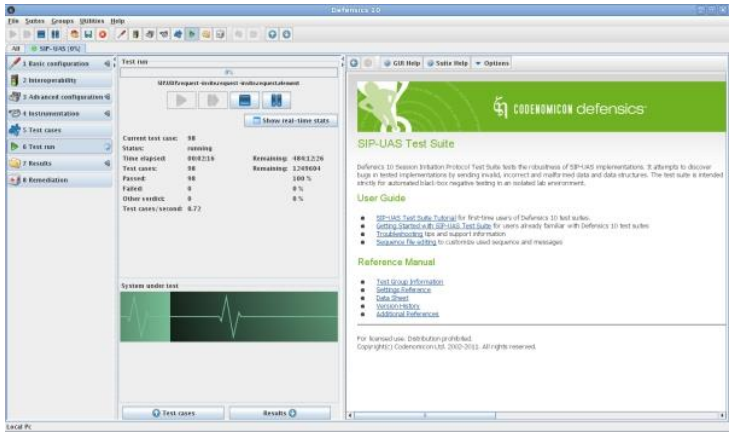
@CodenomiconLTD

How Vulnerabilities Are Discovered

Security researchers (hackers) with a deep understanding of systems, components, failure modes, lots of interesting equipment, and lots of patience and time on their hands (few and far between – but very effective)



Automated testing tools that mimic hackers



It is not easy to train organizations on how to hack like a pro, but automated testing tools can be deployed anywhere and work very well at finding most issues…especially if used early in development

Secure Software Development Lifecycle (SSDL)

- Insertion of security practices as part of the Software Development Lifecycle is what is needed (including concept phase)
- Verification has to happen early as part of the internal process. It saves money!
- Don’t “drink your own Kool Aid”: Get third-party validation!
- Testing must continue long after deployment!

What This Means For Health Care Providers

Doctors will need the ability to determine if cause of complications or death is due to “natural” causes or digital pathogens.

Studies in germ theory and pathology will have to expand to include silicon-based vulnerabilities.

Device manufacturers will need to be forced to test for digital pathogens and be forced to avoid releasing diseased devices.

Questions?

Mike Ahmadi

Global Director, Medical Security

Codenomicon Ltd.

Phone: (925) 413-4365

Email: Mike@Codenomicon.com

@CodenomiconLTD