I am The Cavalry

Safer|Sooner|Together

Unpatchable:

Living with a vulnerable implanted device

Marie Moe, PhD, Research Scientist at SINTEF

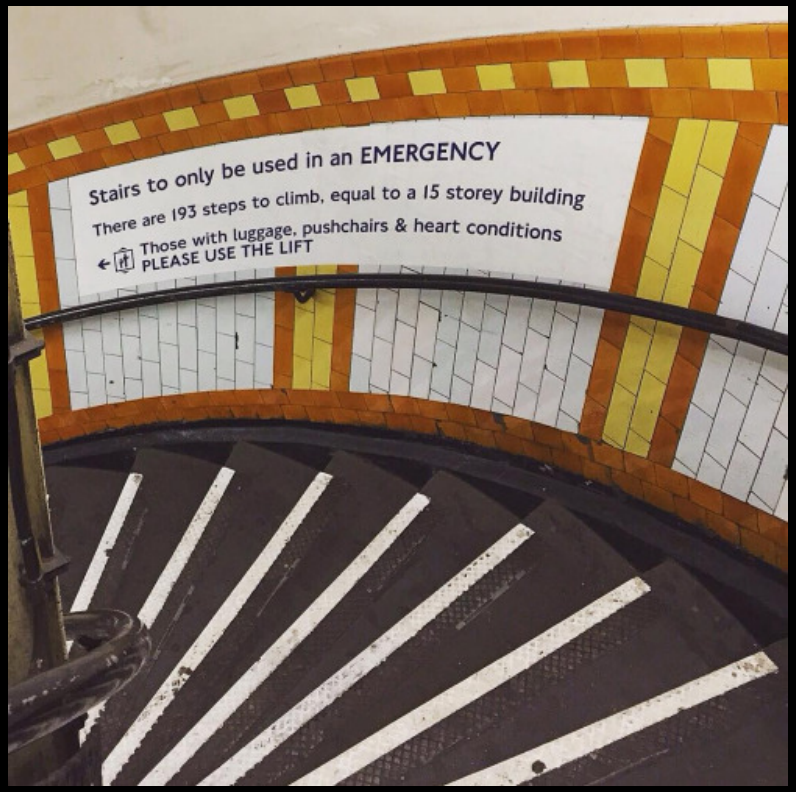
@MarieGMoe @iamthecavalry

#safersoonertogether

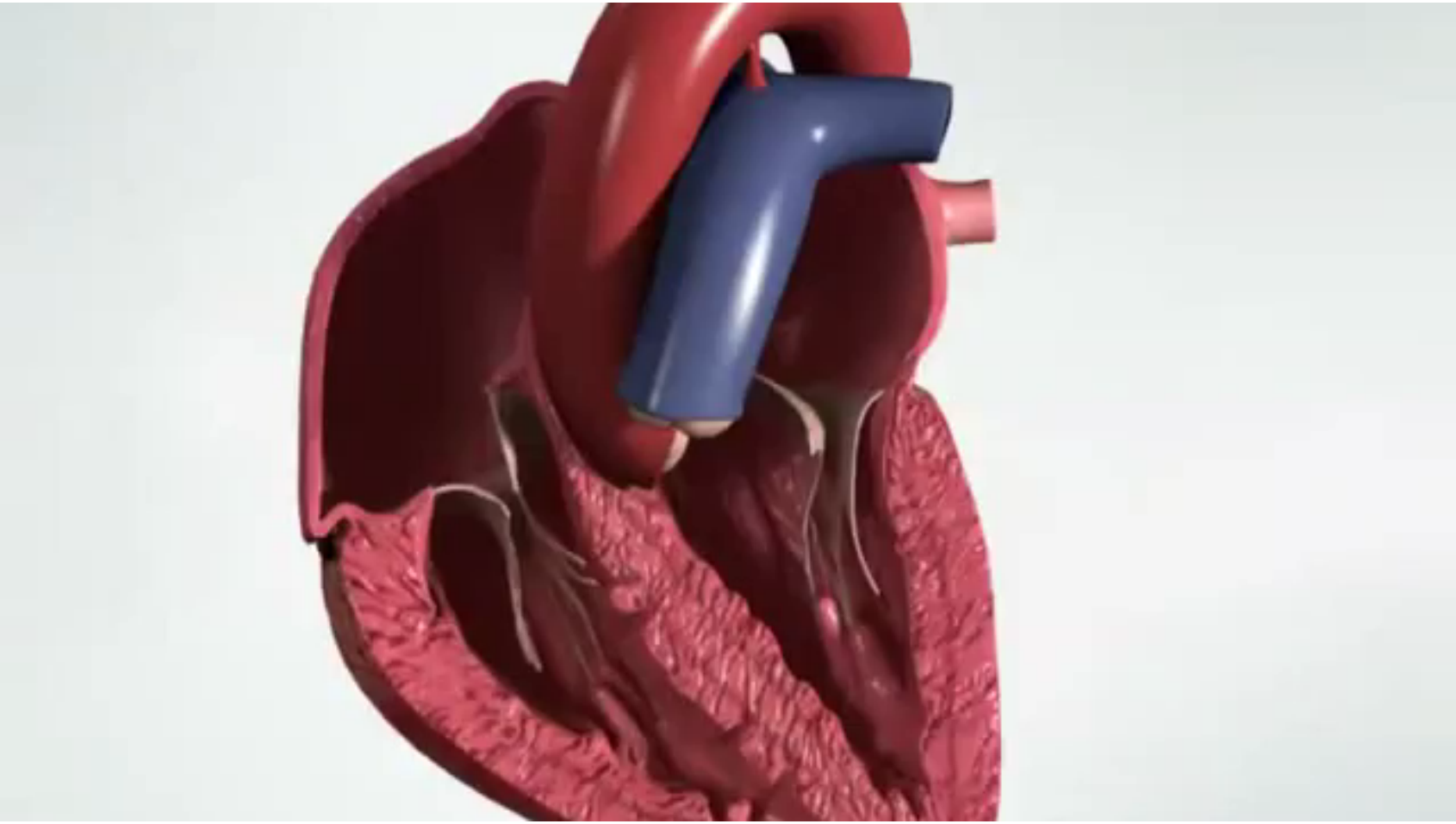
Sometimes, hackers make the worst patients…

Lorenzo Franceschi-Bicchierai, Vice Motherboard

The stairs that almost killed me

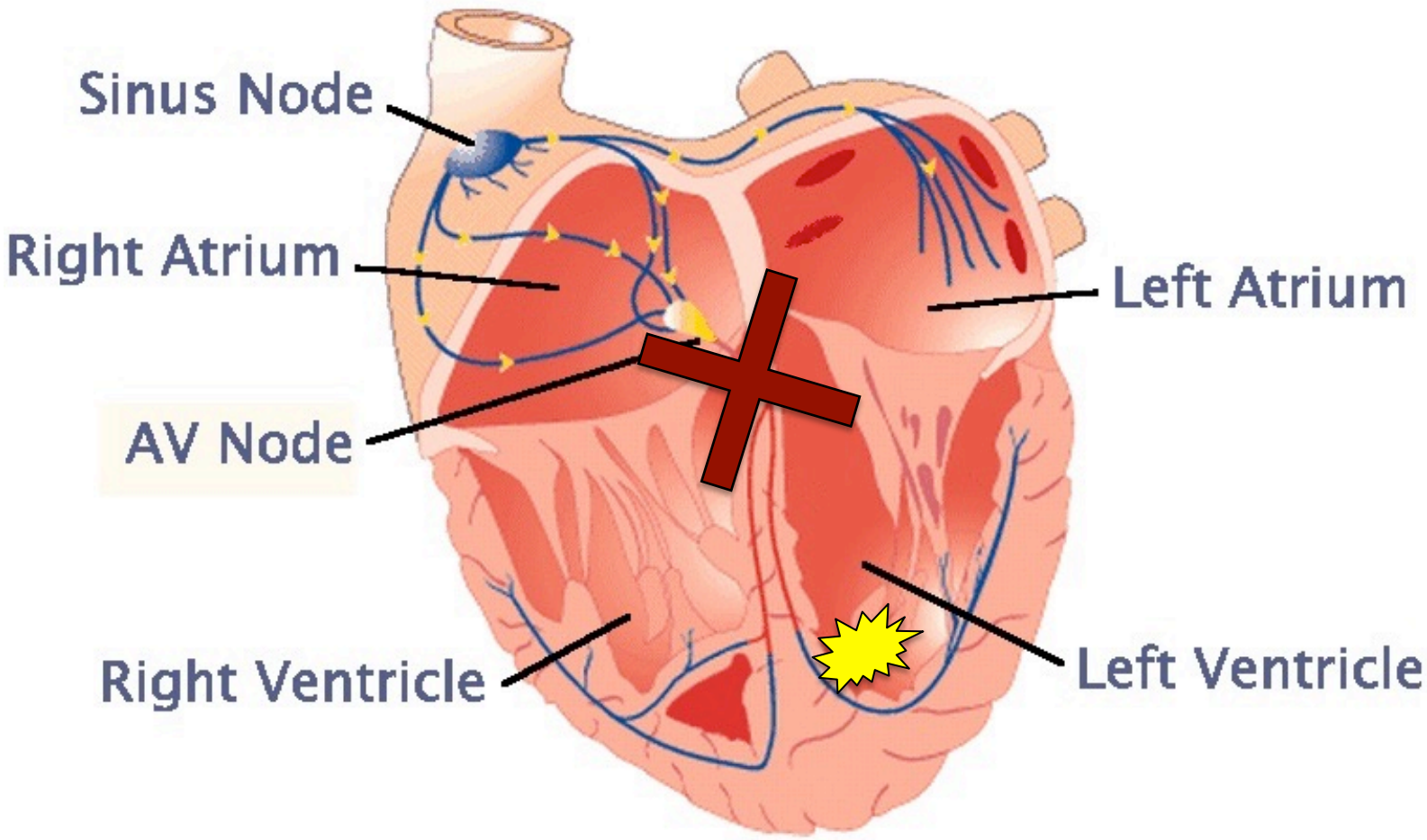


How the heart works



https://www.youtube.com/watch?v=d6RbN5lPqIU

Electrical system of the heart

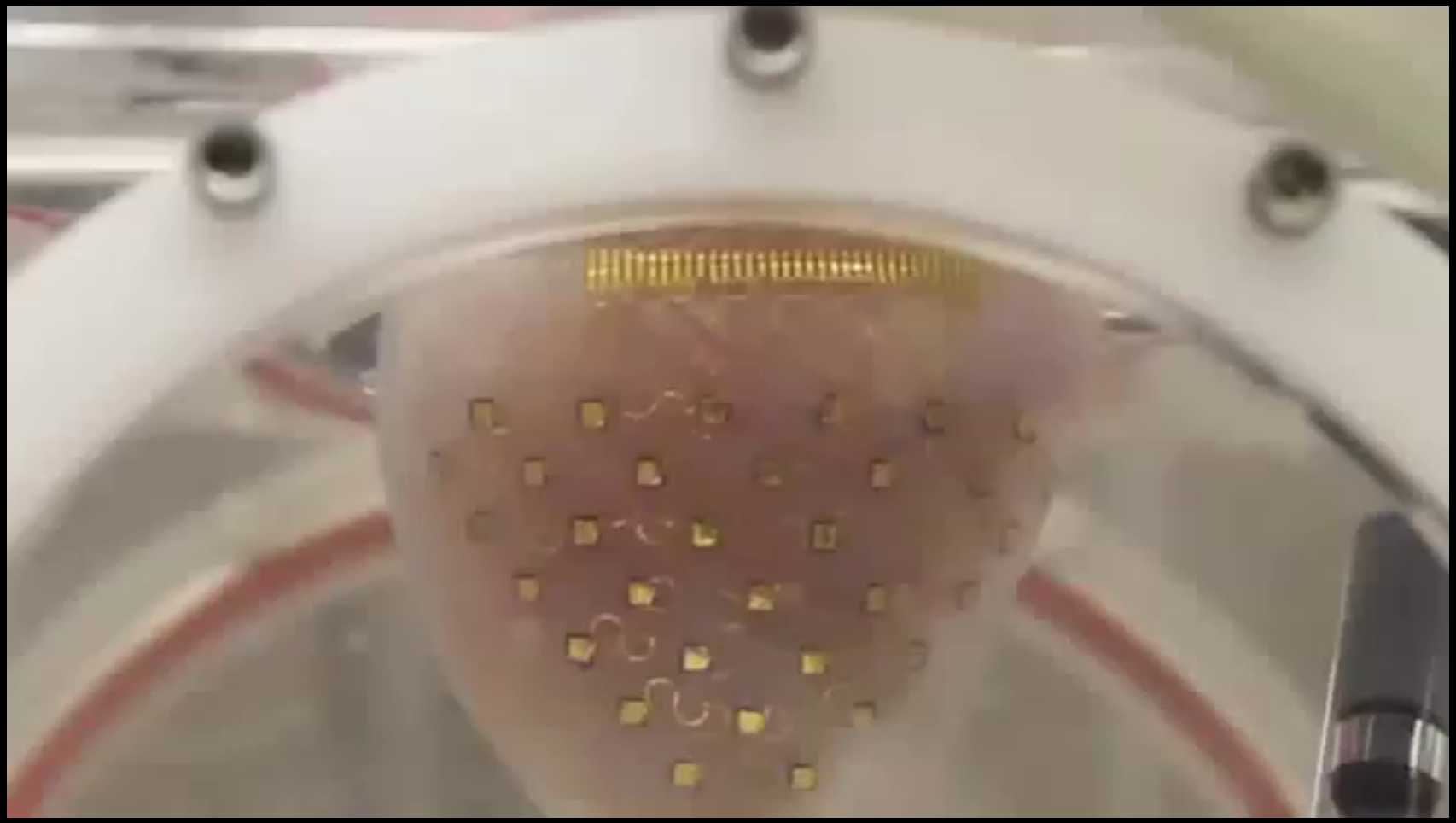


Pacemaker

https://www.youtube.com/watch?v=-f2FKmMneXY

Leadless pacemaker

The future?

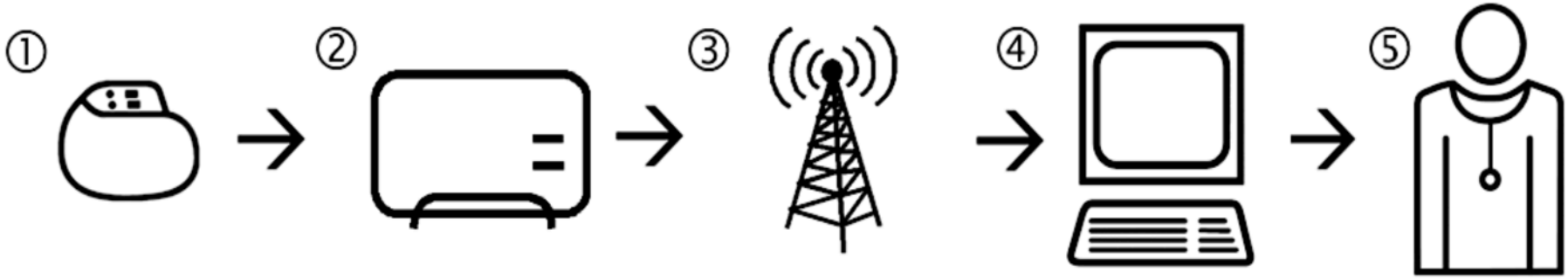


Trusting machines

The Internet of Medical ”Things” is real,

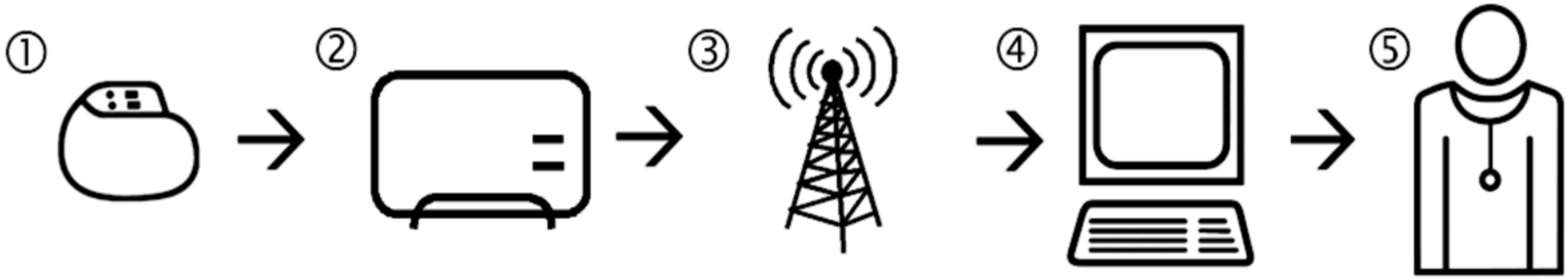
and my heart is wired into it…

Remote monitoring



Potential threats

- Device is vulnerable?
- Access point is vulnerable?
- Mobile network is compromised?
- Server at vendor is compromised?
- Web site that doctor logs in to is vulnerable?



”We need to be able to verify the software that controls our lives”

Bruce Schneier on “Volkswagen and Cheating Software”

Pacemakers are vulnerable

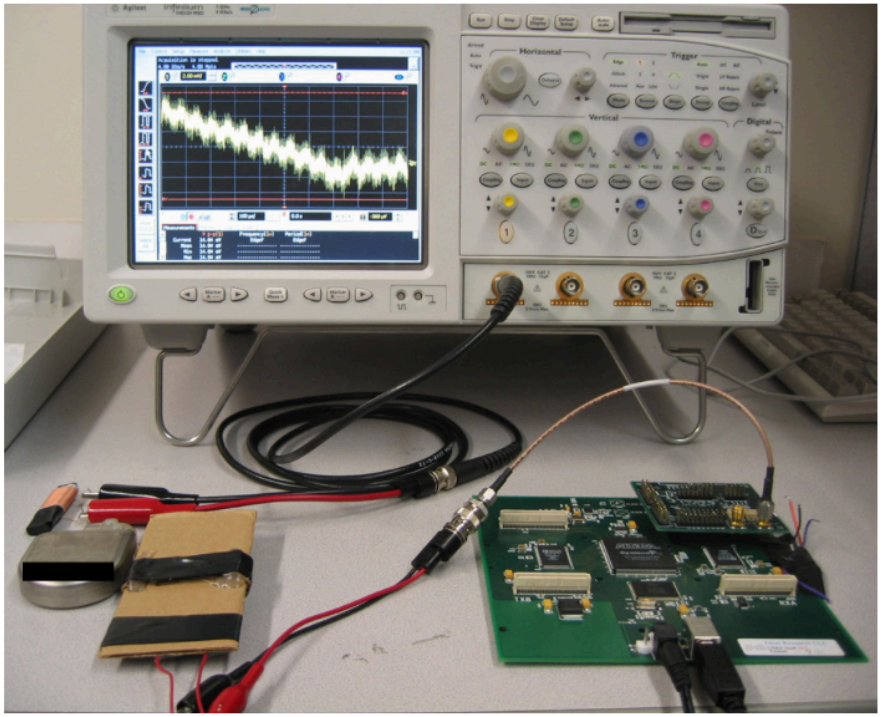


Fig. 2. Equipment used in our experiments. At top is a 4 GSa/s oscilloscope. At bottom, from left to right, are: our eavesdropping antenna, an ICD, our transmitting antenna (mounted on cardboard), and a USRP with a BasicTX card attached.

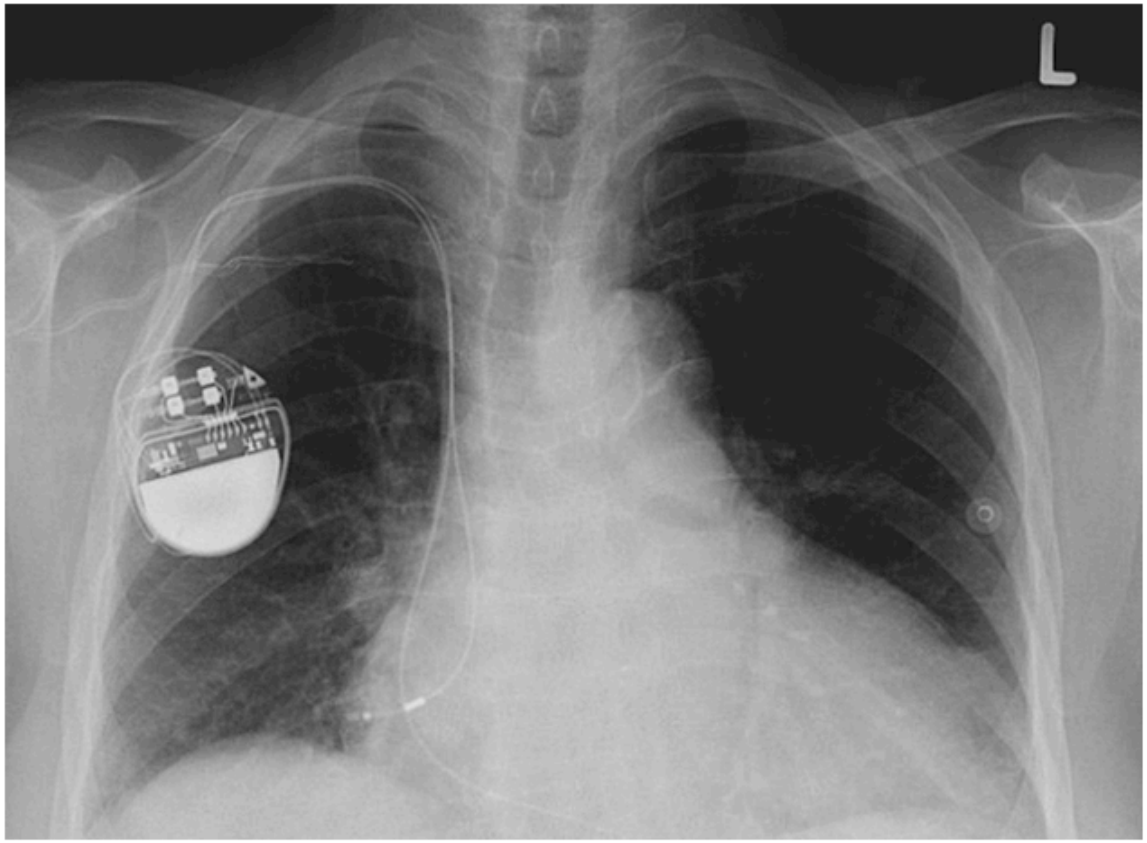
Source: Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In Proceedings of the 29th Annual IEEE Symposium on Security and Privacy, May 2008.

Barnaby Jack Could Hack Your Pacemaker and Make Your Heart Explode

June 25, 2013

by William Alexander

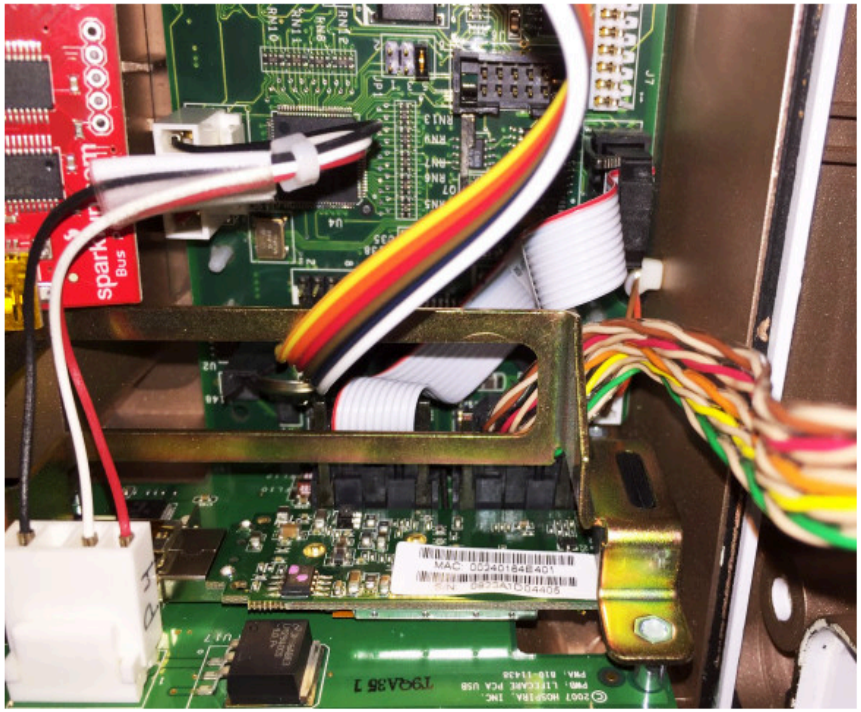
Share Tweet



Source: http://www.vice.com/en_uk/read/i-worked-out-how-to-remotely-weaponise-a-pacemaker

KIM ZETTER SECURITY 06.08.15 7:00 AM

HACKER CAN SEND FATAL DOSE TO HOSPITAL DRUG PUMPS



Hospira's drug infusion pumps include a serial cable (the wide grayish-white cable with the single red stripe on one edge) that connects the communications module to the main pump board. BILLY RIOS

Source: http://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/

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 | En Español

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

- Safety Communications
- Information About Heparin
- Preventing Tubing and Luer Misconnections

Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication

SHARE | TWEET | LINKEDIN | PIN IT | EMAIL | PRINT

Date Issued: July 31, 2015

Audience: Health care facilities using the Hospira Symbiq Infusion System

Device: Symbiq Infusion System, Version 3.13 and prior versions

The Hospira Symbiq Infusion System is a computerized pump designed for the continuous delivery of general infusion therapy for a broad patient population.

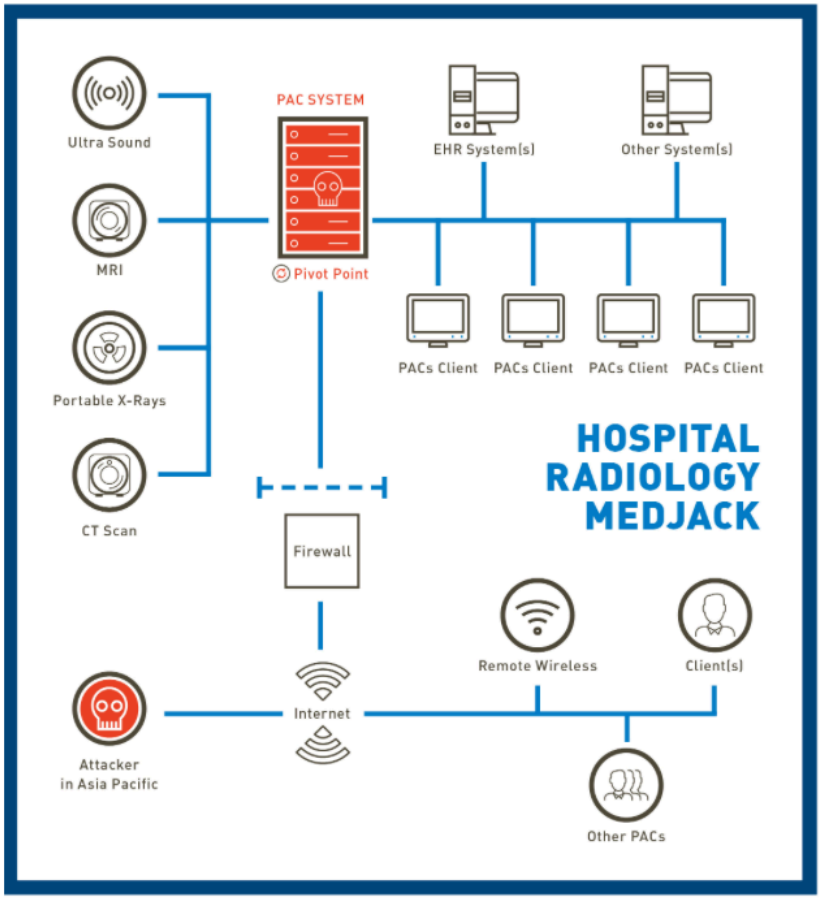
It is primarily used in hospitals, or other acute and non-acute health care facilities, such as nursing homes and outpatient care centers. This infusion system can communicate with a Hospital Information System (HIS) via a wired or wireless connection over facility network infrastructures.

Purpose:

The FDA is alerting users of the Hospira Symbiq Infusion System to cybersecurity vulnerabilities with this infusion pump. We strongly encourage that health care facilities transition to alternative infusion systems, and discontinue use of these pumps.

Source: http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm

Medical devices do get infected



Source: https://securityledger.com/wp-content/uploads/2015/06/AOA_MEDJACK_LAYOUT_6-0_6-3-2015-1.pdf

Default or hard-coded passwords

Source: http://www.pcworld.com/article/2987813/thousands-of-medical-devices-are-vulnerable-to-hacking-security-researchers-say.html

Malicious software updates

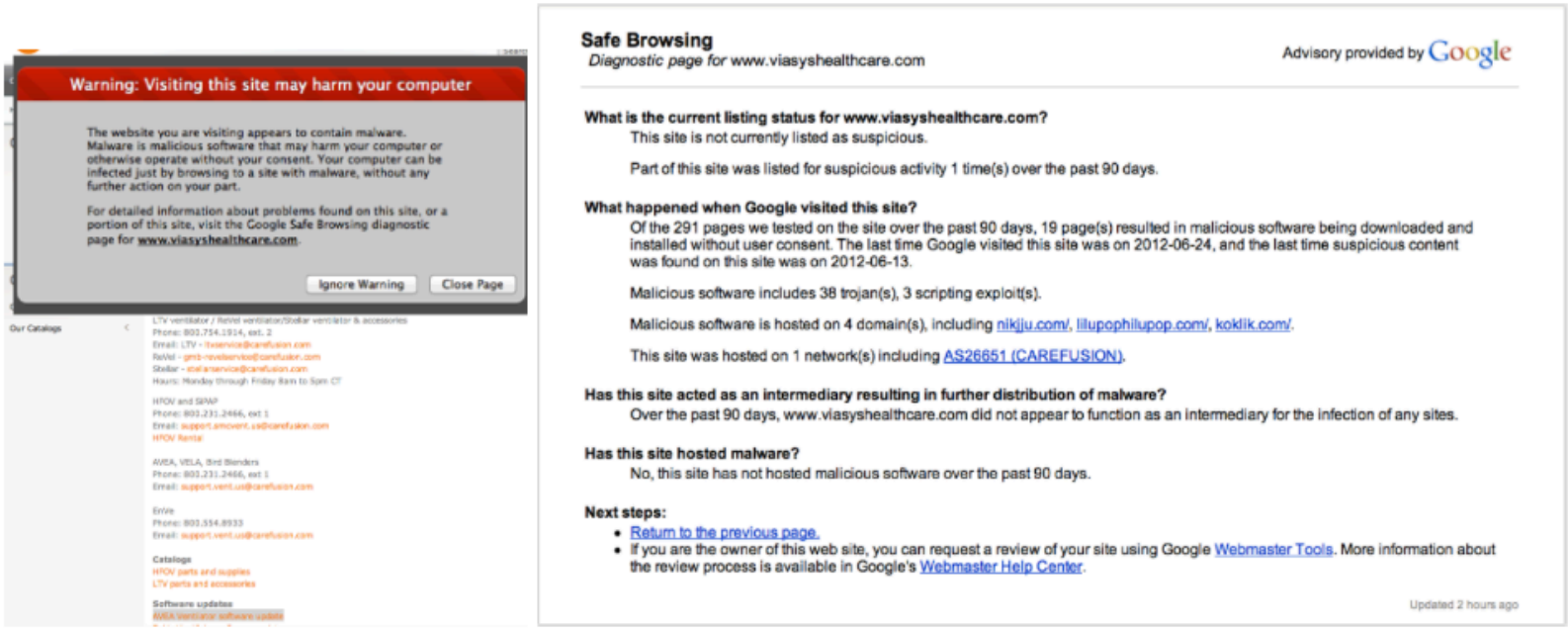


Figure 3: *In June 2012, the author discovered that the website of a ventilator manufacturer was compromised such that unsuspecting hospital technicians downloading a software update received a bonus malware package.*

Source : Dr. Kevin Fu: "On the Technical Debt of Medical Device Security", http://www.naefrontiers.org/File.aspx?id=50750

Cloud safety?

Life of our patients is at stake - I am desperately asking you to contact

Reply

Posted by: md76040303317

Posted on: Apr 22, 2011 11:20 PM

This question is **answered**. Helpful answers available: **2**. Correct answers available: **1**.

Sorry, I could not get through in any other way

We are a monitoring company and are monitoring hundreds of cardiac patients at home.
We were unable to see their ECG signals since 21st of April

Could you please contact us?
Our account number is: 9252-9100-7360
Our servers IDs:

i-bb5c0fd0
i-8e6163e5
i-6589720f

Or please let me know how can I contact you more ditectly.
Thank you

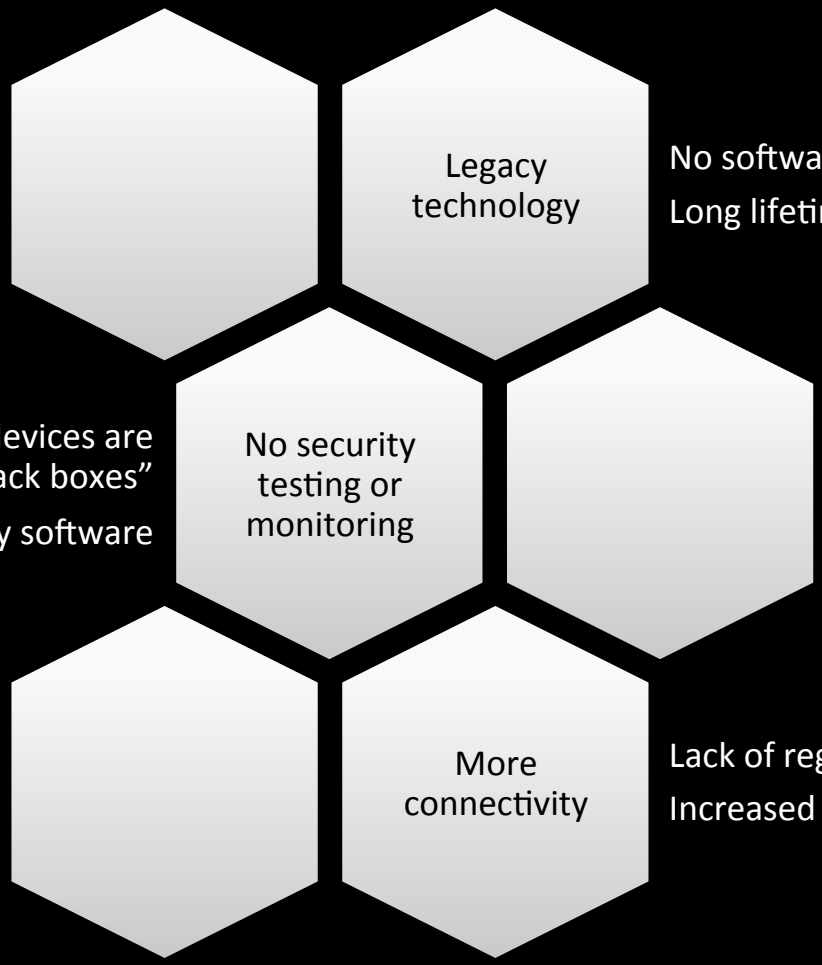
Replies: 35 | **Pages:** 2 - **Last Post:** Aug 12, 2011 8:17 AM by: Caryatid

https://t.co/XndBSPbAta

Potential impact

- Patient privacy issues
- Battery exhaustion
- Device malfunction
- Death threats and extortion
- Remote assassination scenario…

Why?


Legacy technology
No software updates
Long lifetime of devices
Medical devices are ”black boxes”
Proprietary software
No security testing or monitoring
More connectivity
Lack of regulations
Increased attack surface

“Malicious intent is not a prerequisite to patient safety issues”

Scott Erven, Security Researcher at Protiviti

How to solve it?

Hack to save lives!

Security research

Information sharing
Third party collaboration
Coordinated disclosure

Regulation
Procurement
Safety by design
Security testing

Vendor awareness

Security risk monitoring

Security updates
Incident response
Cyber insurance
Resilience

https://iamthecavalry.org
@iamthecavalry

Safer|Sooner|Together

I Am The Cavalry

Problem Statement

Our society is adopting connected technology *faster than we are able to secure it*.

Mission Statement

To ensure connected technologies with the potential to impact public safety and human life are *worthy of our trust*.


Medical


Automotive


Connected Home


Public Infrastructure

Why	Trust, public safety, human life
How	Education, outreach, research
Who	Infosec research community
Who	Global, grass roots initiative
What	Long-term vision for cyber safety

Collecting	existing research, researchers, and resources
Connecting	researchers with each other, industry, media, policy, and legal
Collaborating	across a broad range of backgrounds, interests, and skillsets
Catalyzing	positive action sooner than it would have happened on its own

I am The Cavalry

Safer|Sooner|Together

“There will be bugs”

Joshua Corman of I am The Cavalry

SINTEF

Debugging me

You can’t patch me!

The benefit outweighs the risk

I am The Cavalry

Credits

Alexandre Dulaunoy (@adulau)

Éireann Leverett (@blackswanburst)

Joshua Corman (@joshcorman)

Claus Cramon Houmann (@ClausHoumann)

Scott Erven (@scotterven)

Beau Woods (@beauwoods)

Suzanne Schwartz (US FDA)

Family & Friends ❤️

Thank you!

marie.moe@sintef.no

https://www.iamthecavalry.org

@MarieGMoe @iamthecavalry

#safersoonertogether