I am The Cavalry

32C3

Unpatchable

Living with a vulnerable implanted device

Marie Moe, PhD, Research Scientist at SINTEF
Eireann Leverett, Founder and CEO of Concinnity Risks
@MarieGMoe
@blackswanburst

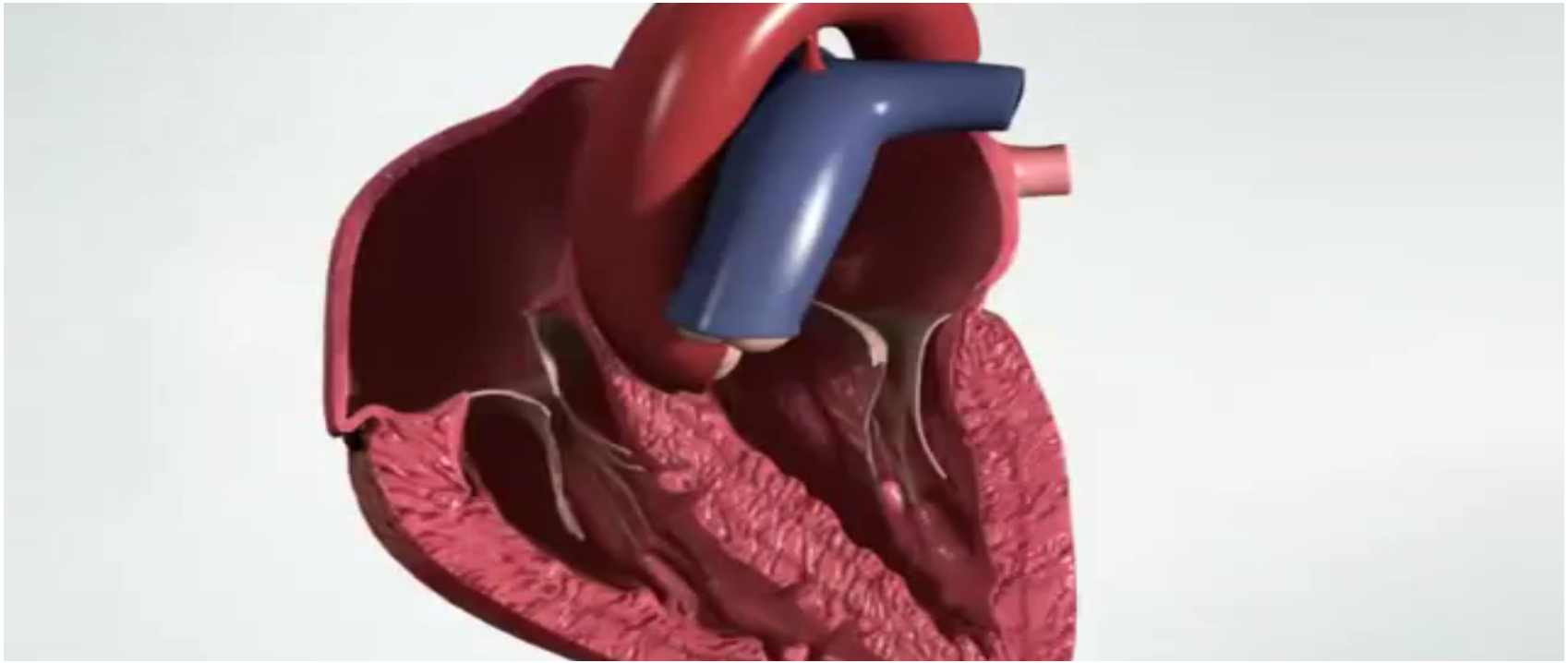
SINTEF

Concinnity Risks

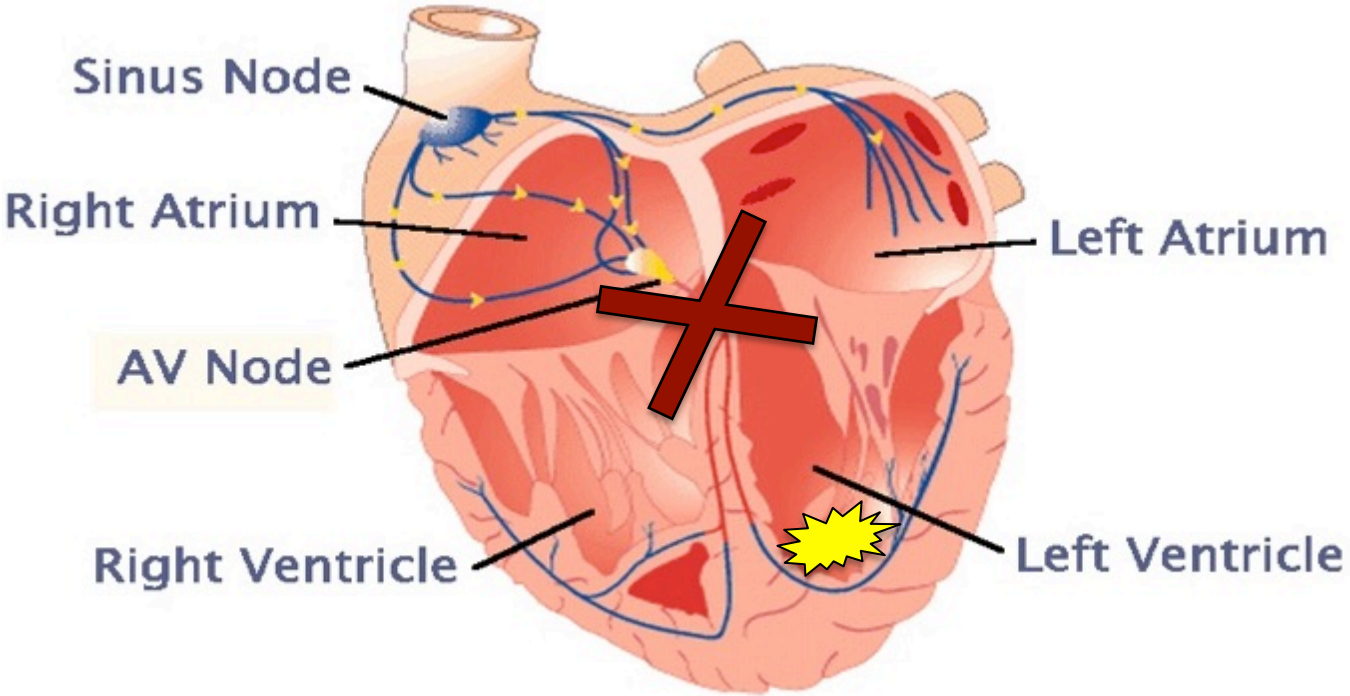
Hack to save lives!

A brief history of my heart…

How the heart works



Electrical system of the heart



Pacemaker

The Internet of Medical ”Things” is real,

and Marie’s heart is wired into it…

① Implantable medical device
- ICD/Pacemaker/other devices
- MICS (Medical Implant Communication Service)
- Bluetooth

② Access point
- POTS/GSM/SMS/email

③ GSM/Telephone/Internet

④ Telemetry store
- Programmers
- Doctor's workstation
- Telemetry server at vendor

⑤ Medical staff
- Social engineering

With connectivity comes vulnerability…

Potential impact

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

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

Bruce Schneier on “Volkswagen and Cheating Software”

Previous work

- Kevin Fu et al:
  - Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses (2008)
  - Mitigating EMI signal injection attacks against analog sensors (2013)
- Barnaby Jack
- Hardcoded credentials
- Medical device honeypots
- Drug infusion pumps

Hacking can save lives

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.

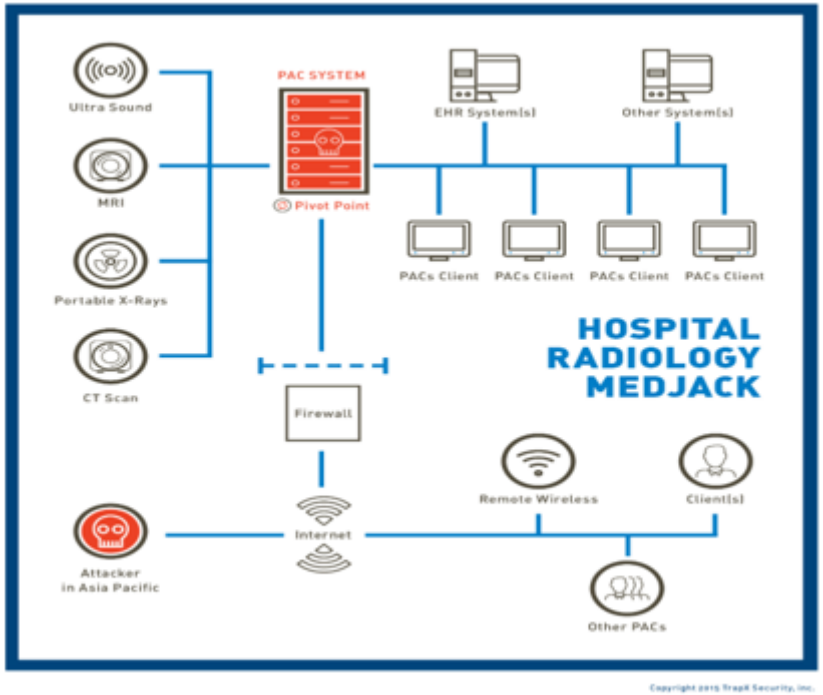
It is primarily used in hospitals, or other acute and non-acute health care facilities, such as nursing homes and outpatient care centers. This infusion system can communicate with a Hospital Information System (HIS) via a wired or wireless connection over facility network infrastructures.

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

WTF are you doing with my data?

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

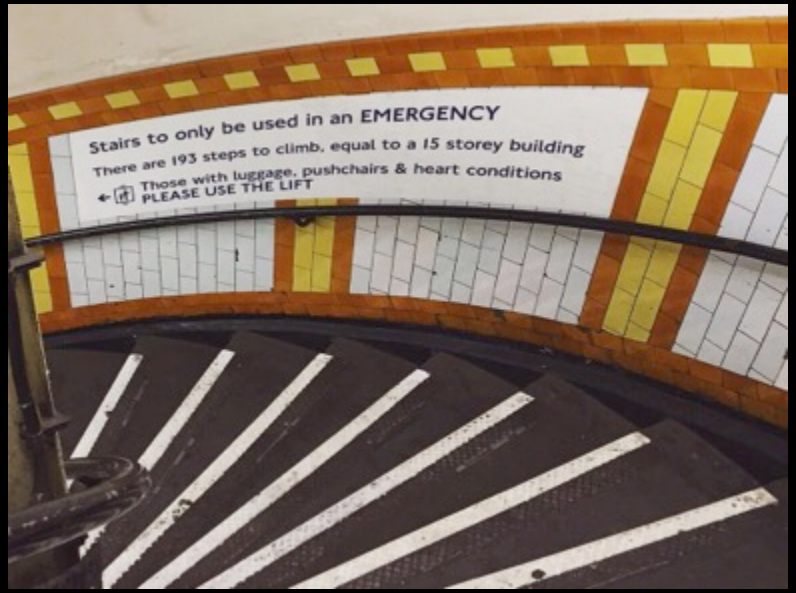
Could you please contact us?
Our account number is: 9252-9100-7360
Our servers IDs:

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

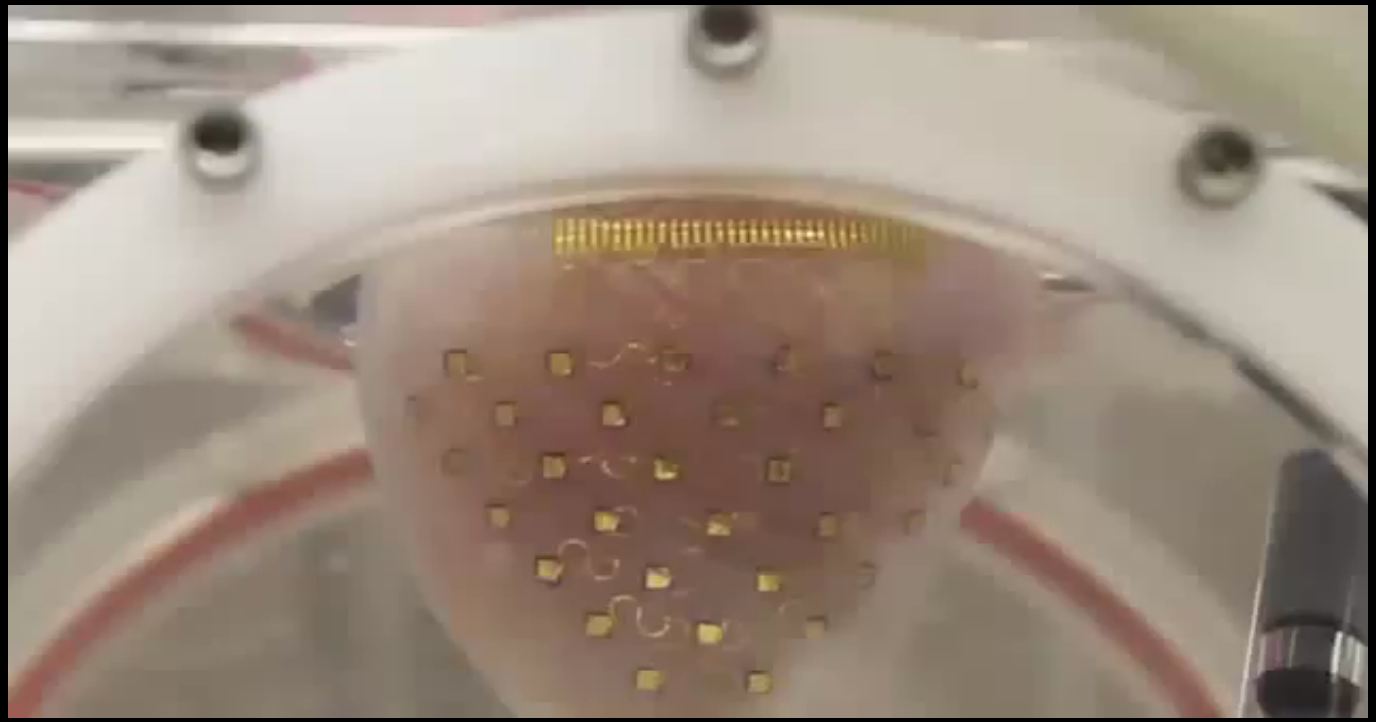
The stairs that almost killed me



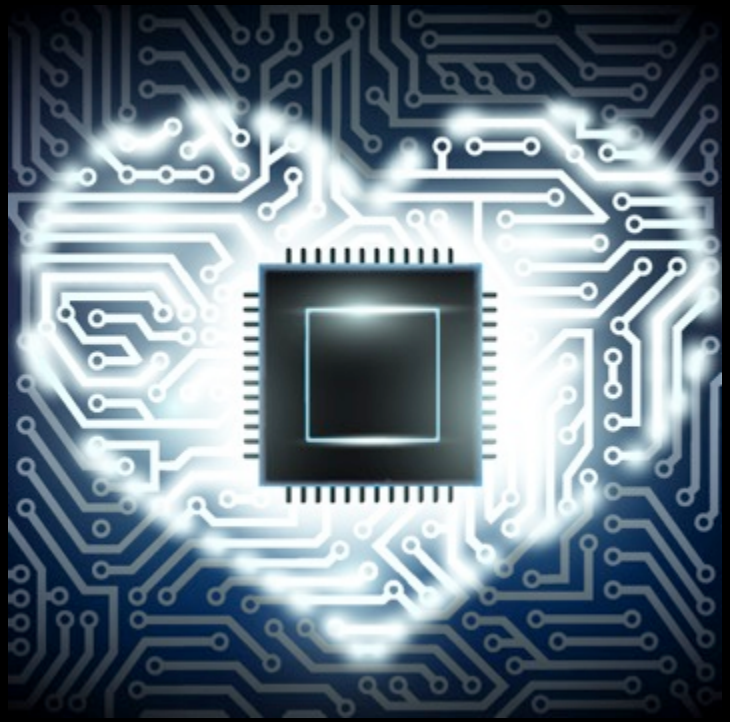
Debugging me

Leadless pacemaker

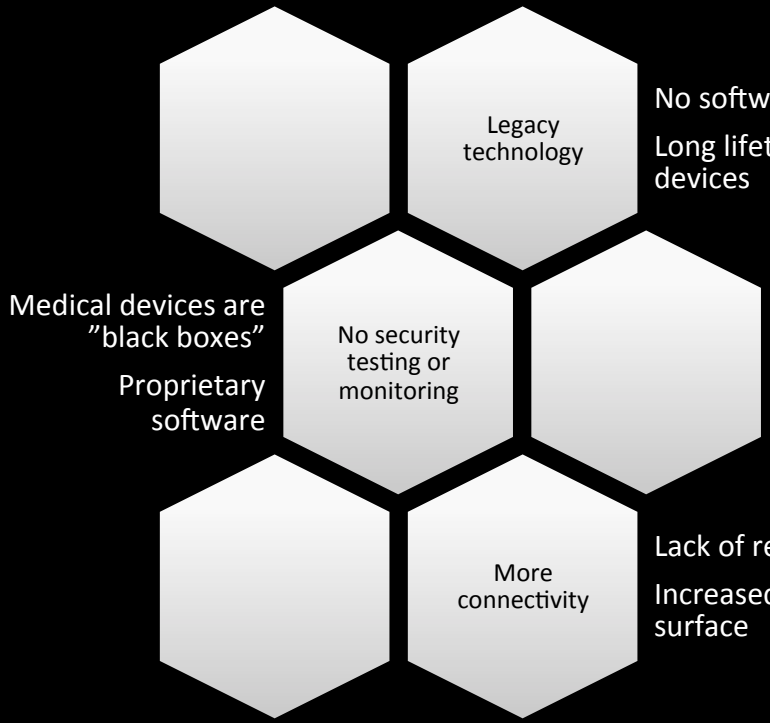
The future?



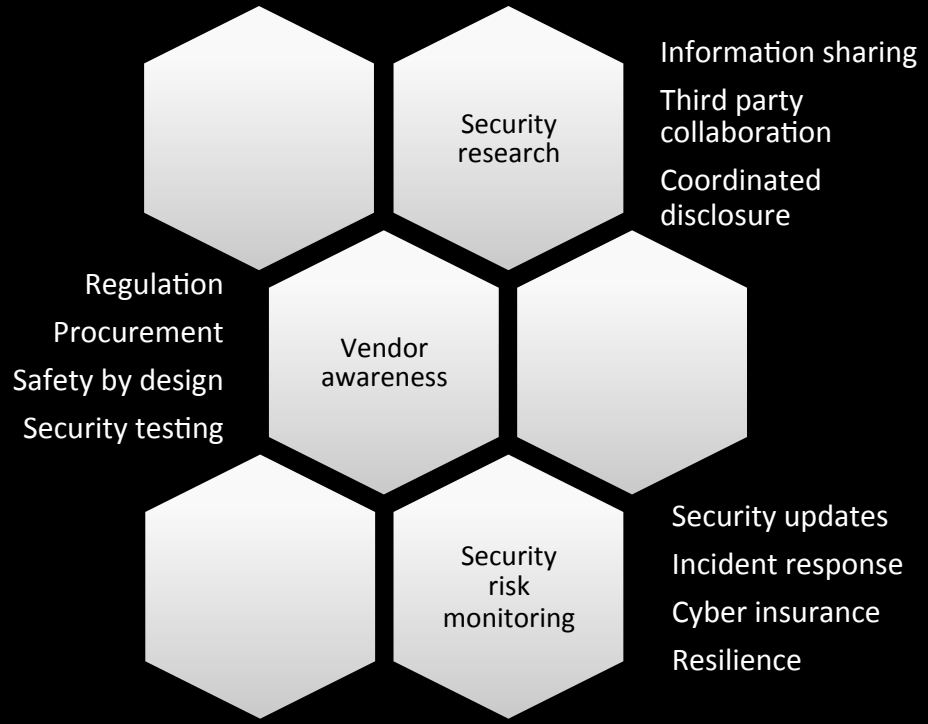
Reflections on trusting machines



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

How to solve it?



I Am The Cavalry

The Cavalry isn't coming... It falls to us

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 Passionate volunteers
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

What is the social contract for the code in our bodies?

Research needed

- Open source medical devices
- Medical device cryptography
- Personal area network monitoring
- Jamming protection
- Forensics evidence capture

I am The Cavalry

Credits

Tony Naggs (@xa329)
Gunnar Alendal (@gradoisageek)
Alexandre Dulaunoy (@adulau)
Joshua Corman (@joshcorman)
Claus Cramon Houmann (@ClausHoumann)
Scott Erven (@scotterven)
Beau Woods (@beauwoods)
Suzanne Schwartz (US FDA)
Family & Friends ❤

I am The Cavalry

Thank you!

www.infosec.sintef.no
www.iamthecavalry.org
www.concinnity-risks.com

@MarieGMoe
@blackswanburst