UNIVERSITY OF TIRANA

Unpatchable: Living with a Vulnerable Implanted Device

PhD Student

PRESENTED BY:

ROMINA MUKA

LECTURER / PHD STUDENT, UT, TIRANA

PHD STUDENT, NTNU, NORWAY

ABOUT ME

Romina MUKA

Lecturer / PhD Student

Engaged in continuous study and learning..

Work as a lecturer near University of Tirana, Albania (subjects: Information Security, Cryptology, Management Information Systems, Introduction to Informatics); PhD student near UT, Albania in collaboration with NTNU, Norway); training, mentoring and awareness & more…

Past life (pre-.com) was spent in Statistics, Open Source Software, Mobile App Developer, CRM System Analyst, Web Designing

PHD TOPIC

e-Health Systems: secure information transmission and storage

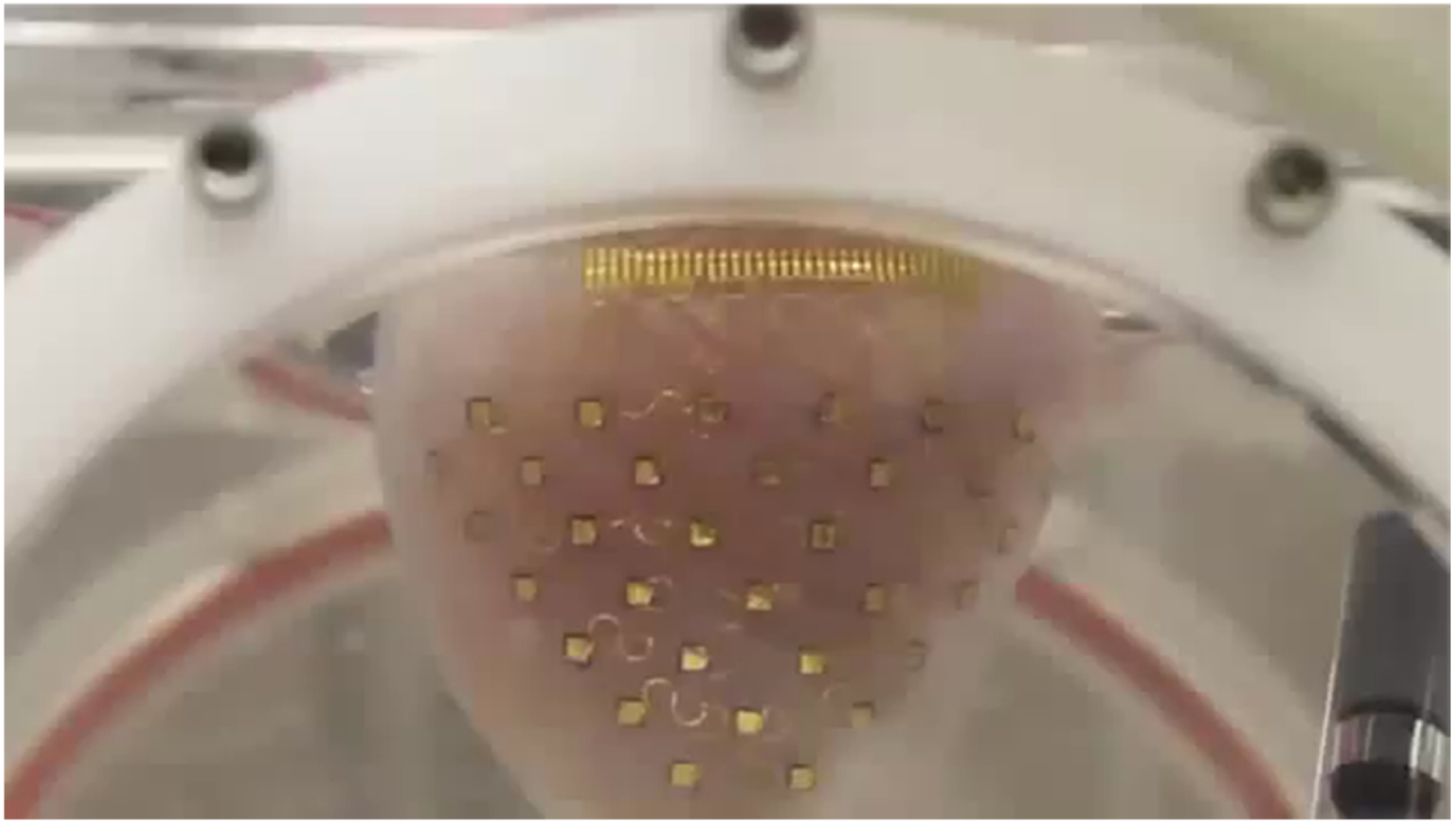
Unpatchable: Living with a Vulnerable Implanted Device

Sometimes, hackers make the worst patients...

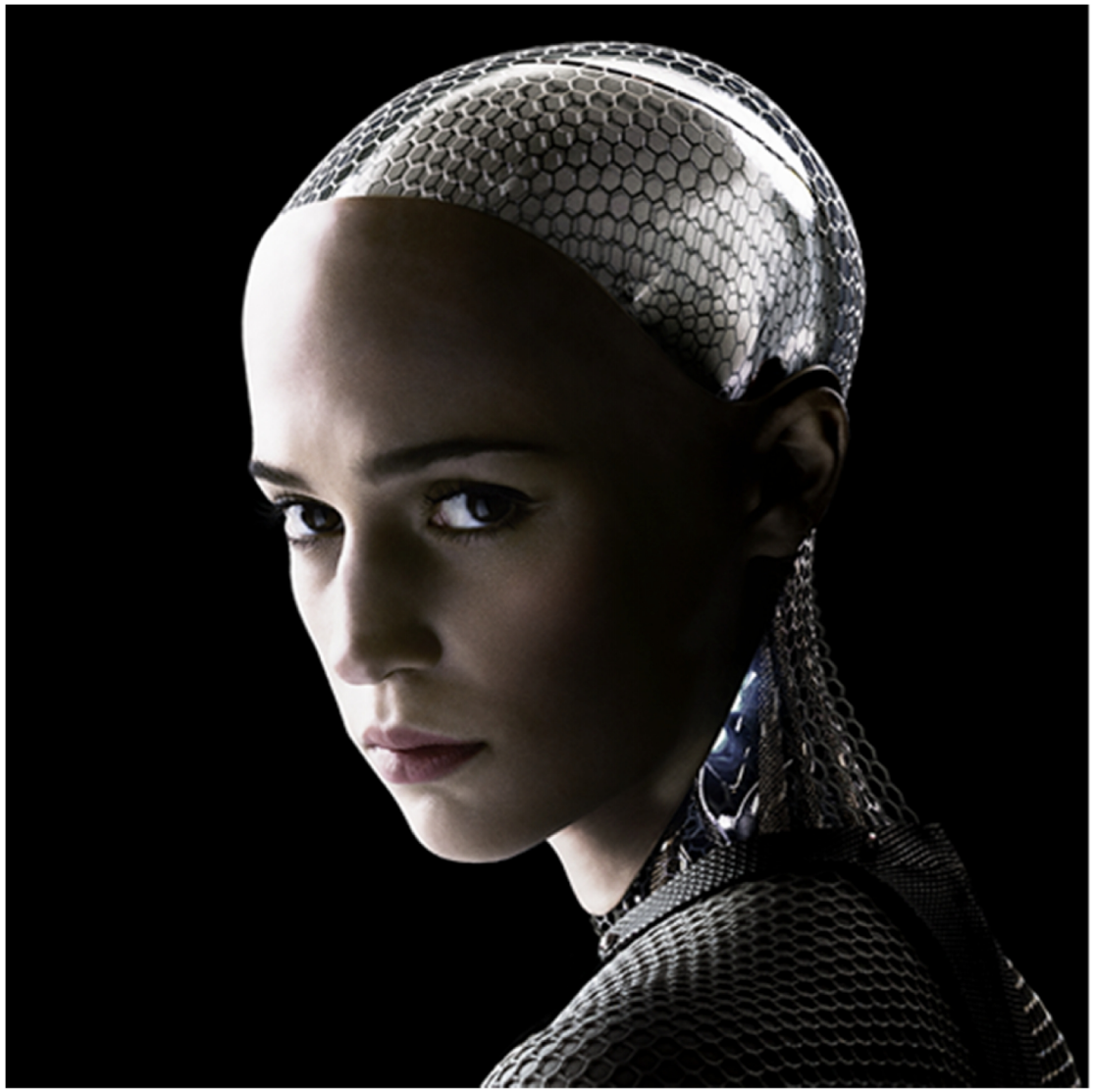
Lorenzo Franceschi-Bicchierai, Vice Motherboard

With connectivity comes vulnerability….

PACEMAKER EVOLUTION



TRUSTING MACHINES

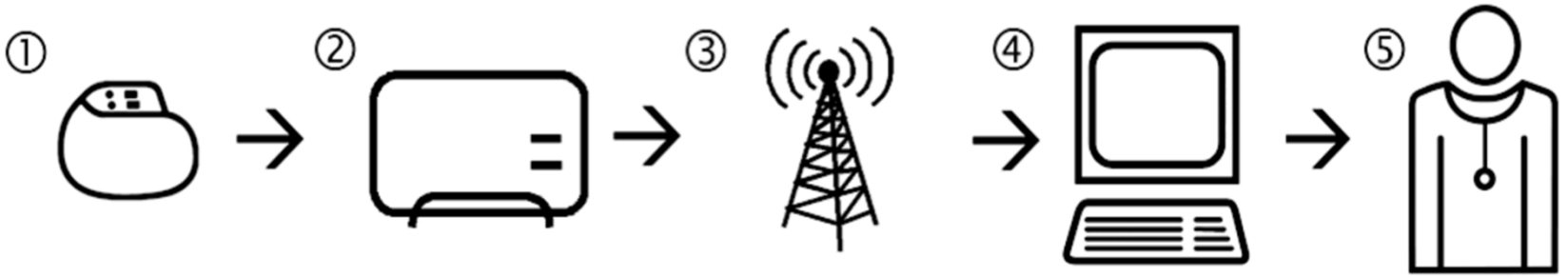


IOT

The Internet of Medical ”Things” is real,

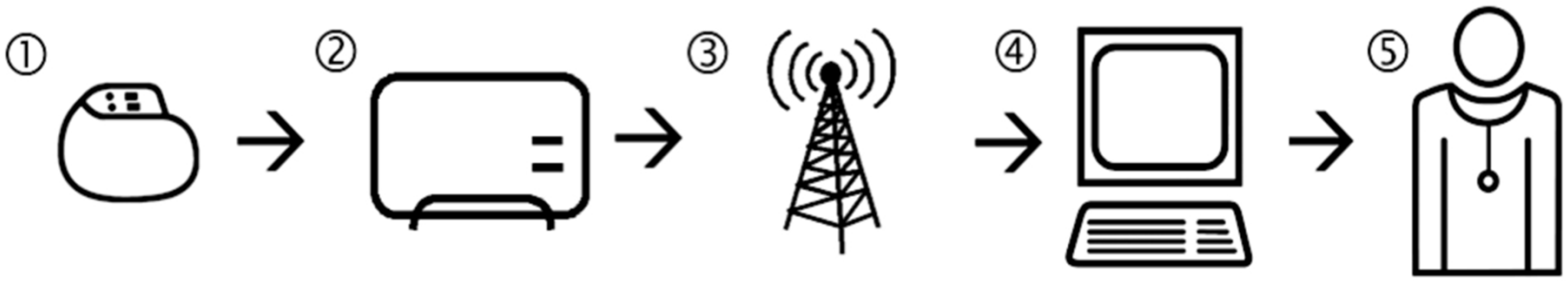
and people’s heart are wired into it...

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?



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”

PACEMAKERS ARE VULNERABLE

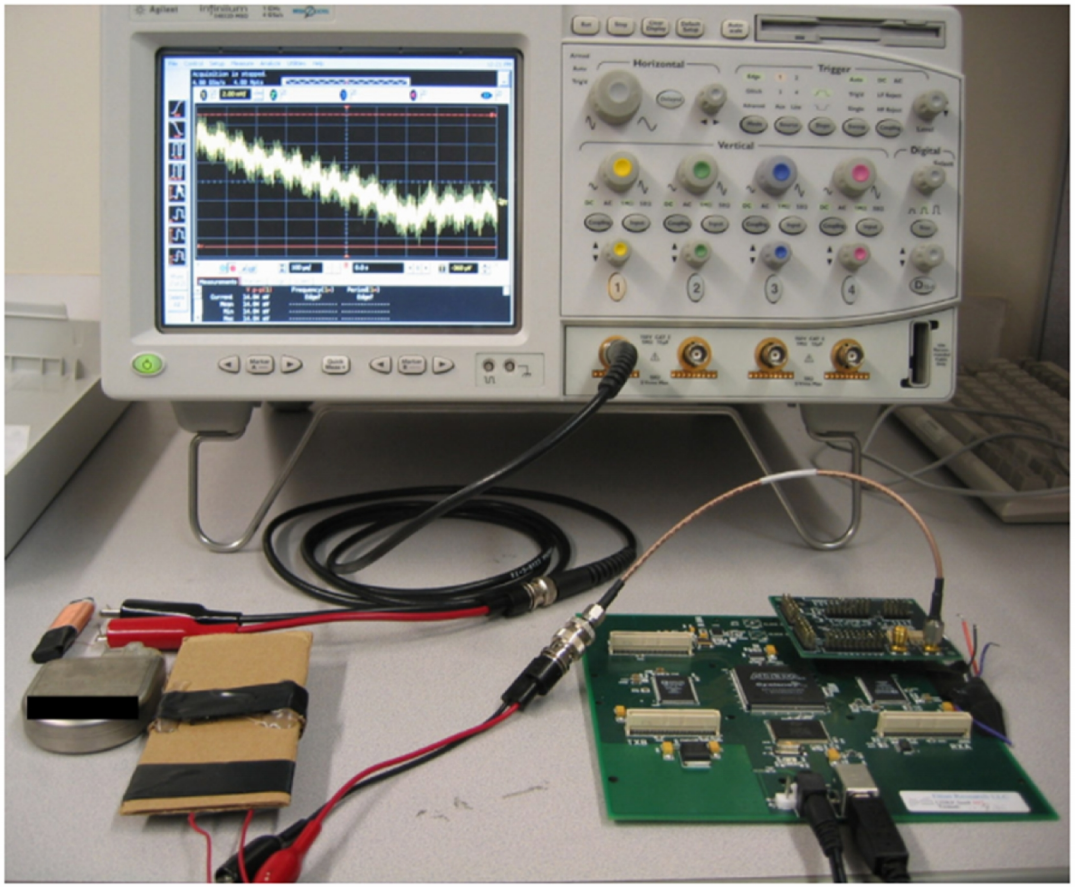


Fig. 2. Equipment used in our experiments. At top is a 4 GSa/s oscilloscope. At bottom, from left to right, are: our eavesdropping antenna, an ICD, our transmitting antenna (mounted on cardboard), and a USRP with a BasicTX card attached.

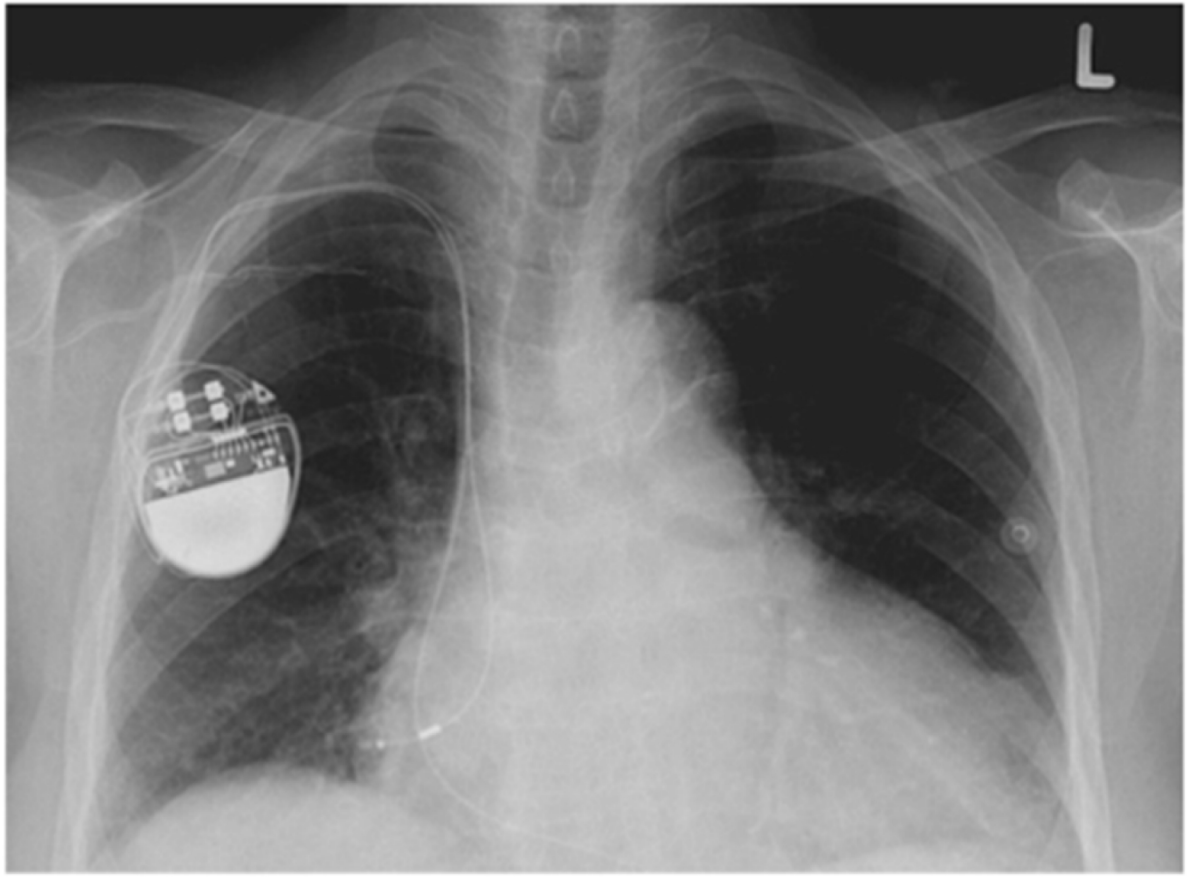
Source: Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. Pacemakers and implantable cardiac defibrillators: Solware radio aKacks and zero-power defenses. In Proceedings of the 29th Annual IEEE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

Barnaby Jack Could Hack Your Pacemaker and Make Your Heart Explode

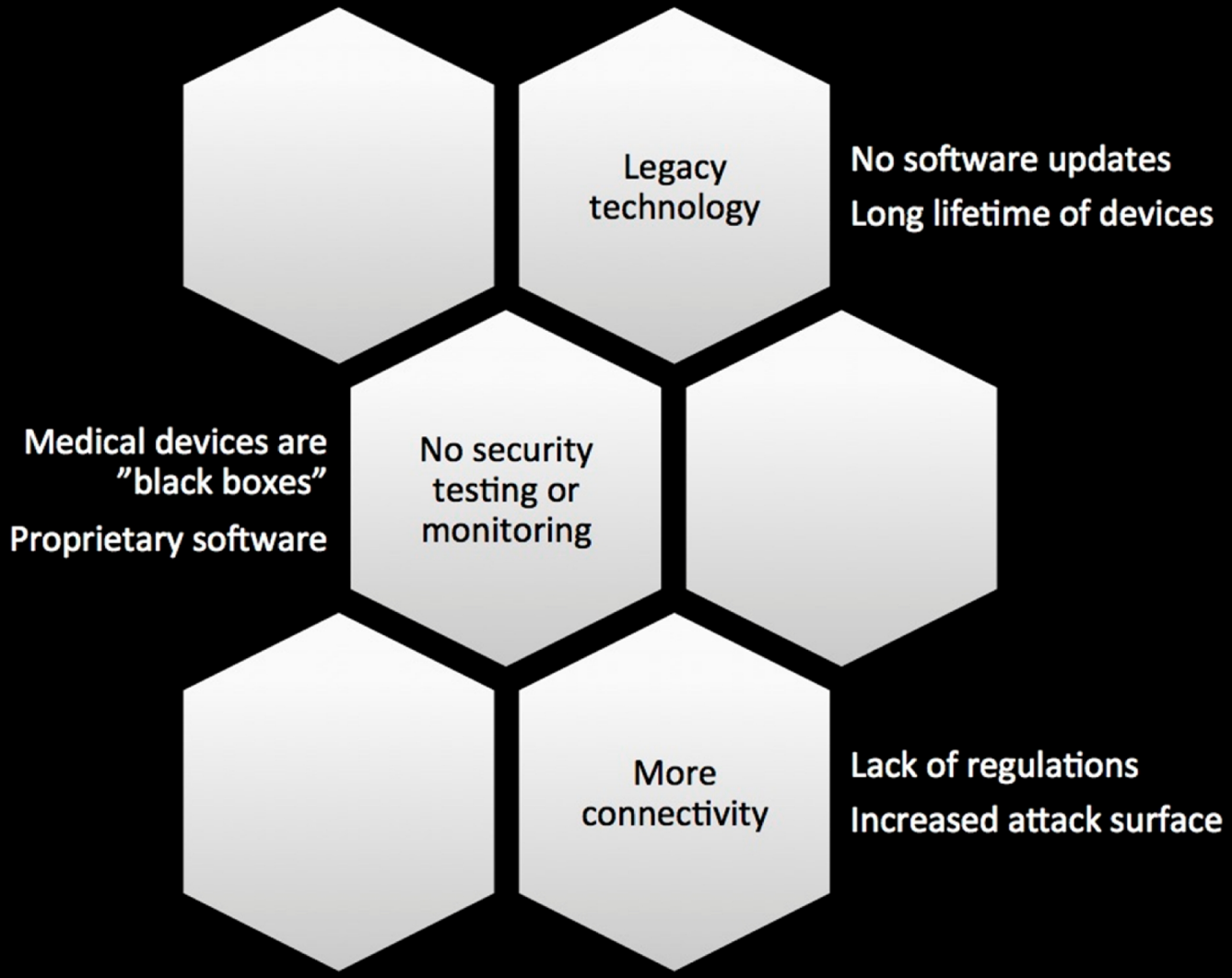
June 25, 2013

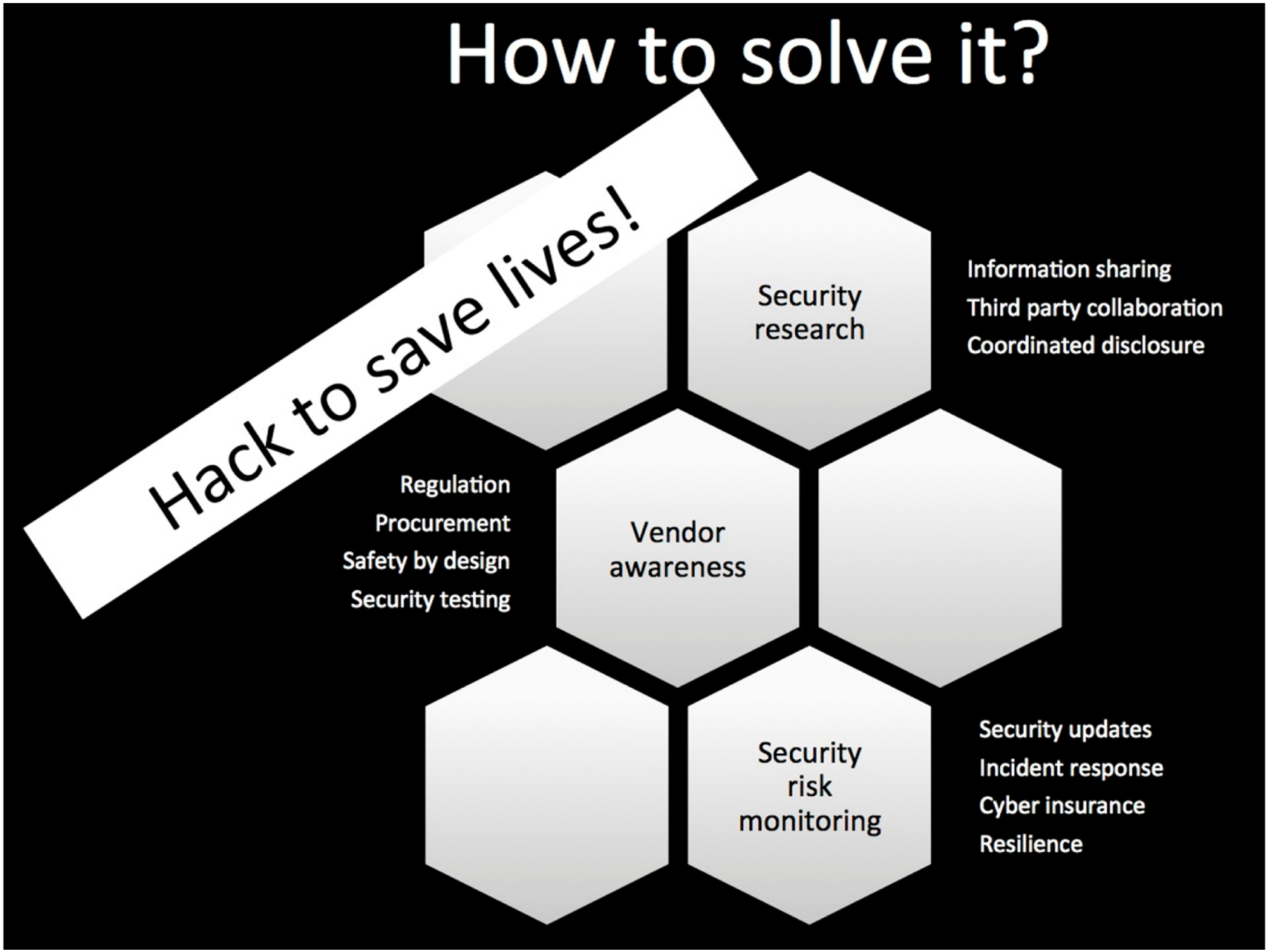
by William Alexander

Share Tweet



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?
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

“There will be bugs”

THE BENEFIT

OUTWEIGHS THE RISKS

CONTACT INFORMATION

Romina MUKA

- M: +355 69 52 15 104
- E: romina.muka AT unitir DOT edu DOT al
- E: rominam AT stud DOT ntnu DOT no
- E: rominamuka AT gmail DOT com
- LinkedIn (Romina Muka)

CONCLUSION

Questions and Discussion

Thank You!