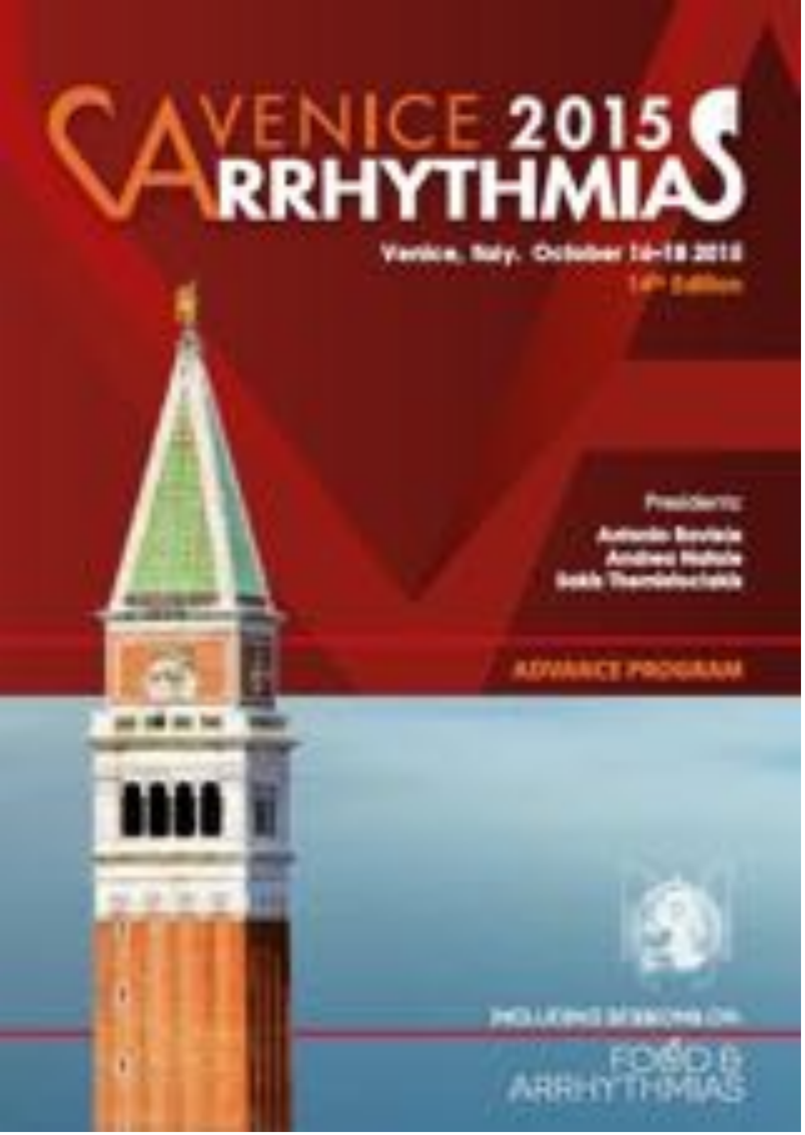


Remote Monitoring: How to Remove Barriers and Implement Advances

Is it time to perform remote device programming?

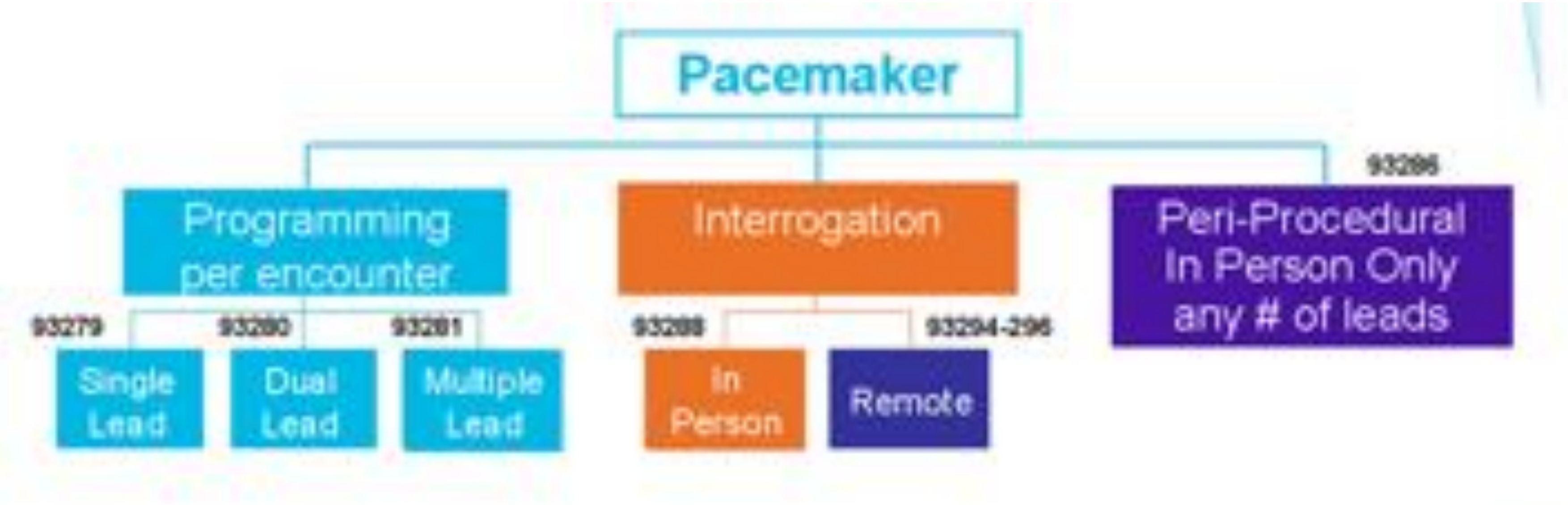
Renato P. Ricci
Cardiovascular Department
San Filippo Neri Hospital, Rome, Italy

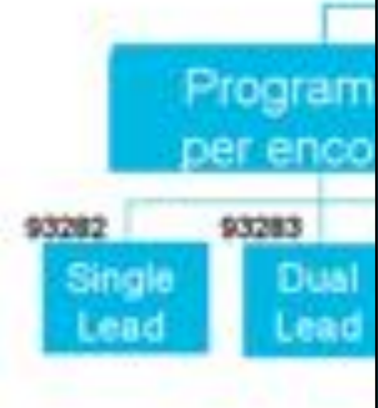
October 16 - 18
14th EDITION 2015

MY CONFLICTS OF INTEREST ARE

Minor consultancy fees from Medtronic and Biotronik

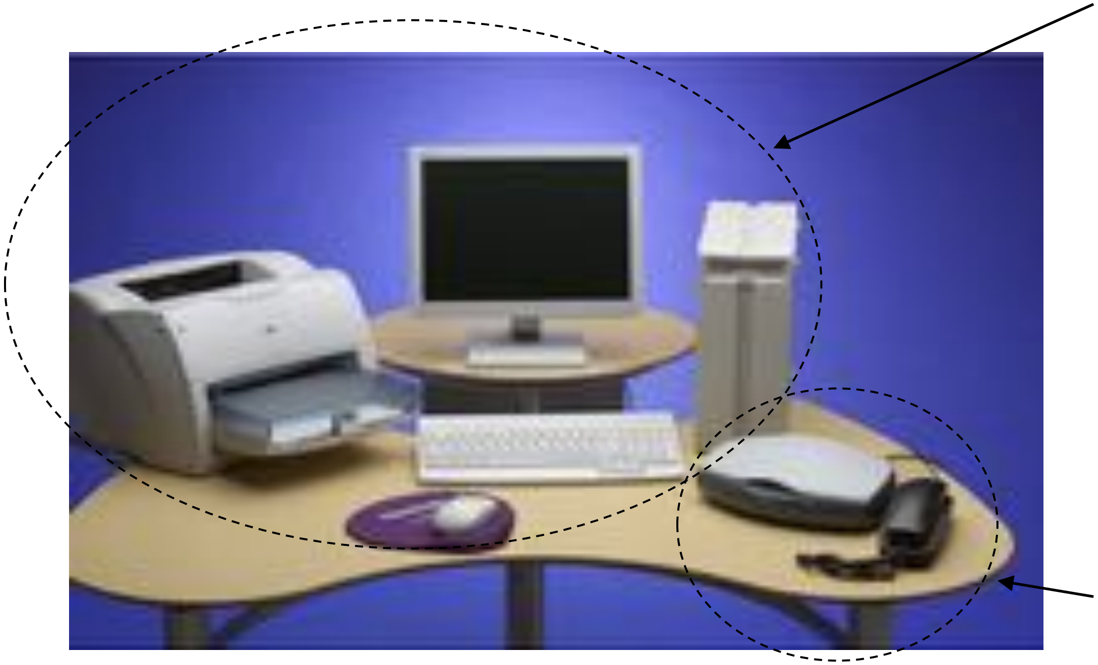
RM Reimbursement in US





Electronic analysis of dual chamber or wearable cardioverter defibrillator system (includes interrogation, evaluation of pulse generator status, evaluation of programmable parameters at rest and during activity where applicable, using electrocardiographic recording and interpretation of recordings at rest and during exercise, analysis of event markers and device response); single chamber or wearable cardioverter defibrillator system, **without reprogramming**

The Housecall Plus™ System



- Receiver:
  - Computer
  - Build-in modem
  - Flat screen
  - Key board
  - Printer

- Transmitter:
  - For patient / Referrals
  - Phone connection

<u>Features</u>

- Personal interaction during real-time follow-up
- the same information as from the programmer
- **Ability to clear diagnostics (remotely)**
- Information is instantly available to the physician
- External database support
- Internal automatic archiving

2006

Remote programming in neurostimulation early experiences

CIED Remote programming

- Remote programming is technically feasible
- It is already available within short spatial ranges (RF telemetry)
- The most important hurdles are related to patient safety and regulatory aspects
- These issues might only be resolved if benefits will be proven to overwhelm related risks

Remote Programming & Key barriers

- Lack of reliable telecommunication infrastructure

- Lack of data security and integrity

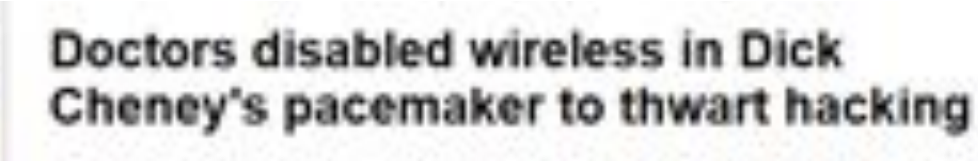
- Lack of algorithms within the implant to protect critical parameters before change takes effects specially when done remotely

Remote programming nightmares

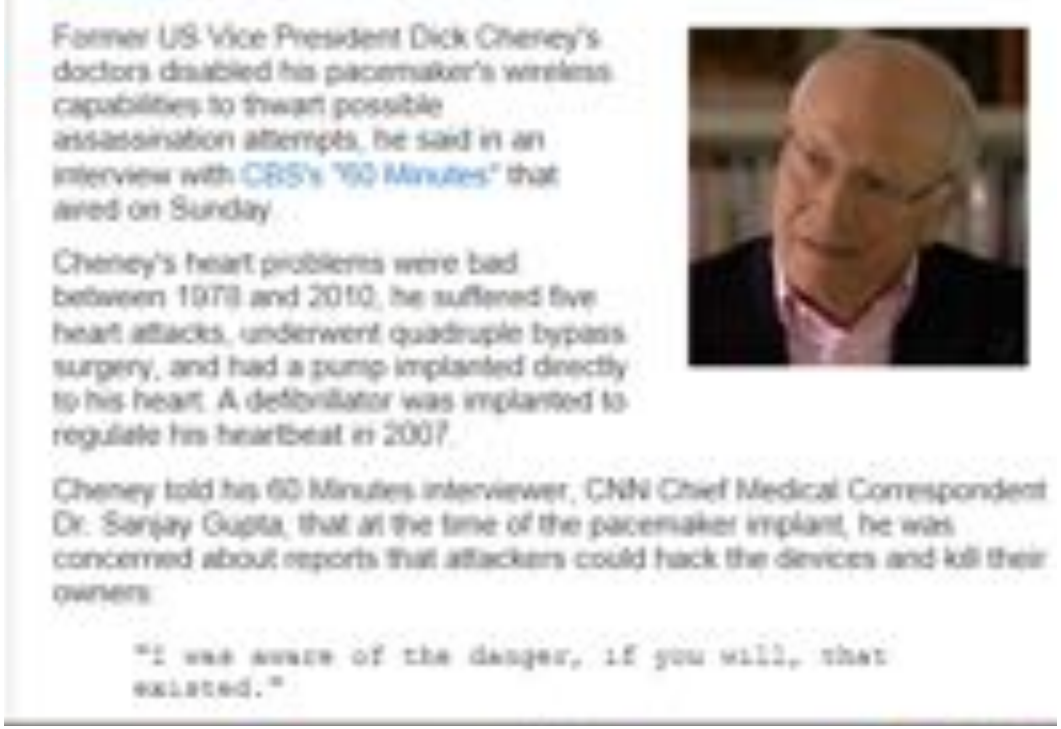
- **Pacemaker dependency**
  (but capture thresholds trends are relayed now with autocapture and significant changes already notified)

- **VT-VF detection/therapies disabled**

- **Security breaches**



Doctors disabled wireless in Dick Cheney's pacemaker to thwart hacking



Former US Vice President Dick Cheney's doctors disabled his pacemaker's wireless capabilities to thwart possible assassination attempts, he said in an interview with CBS's "60 Minutes" that aired on Sunday.

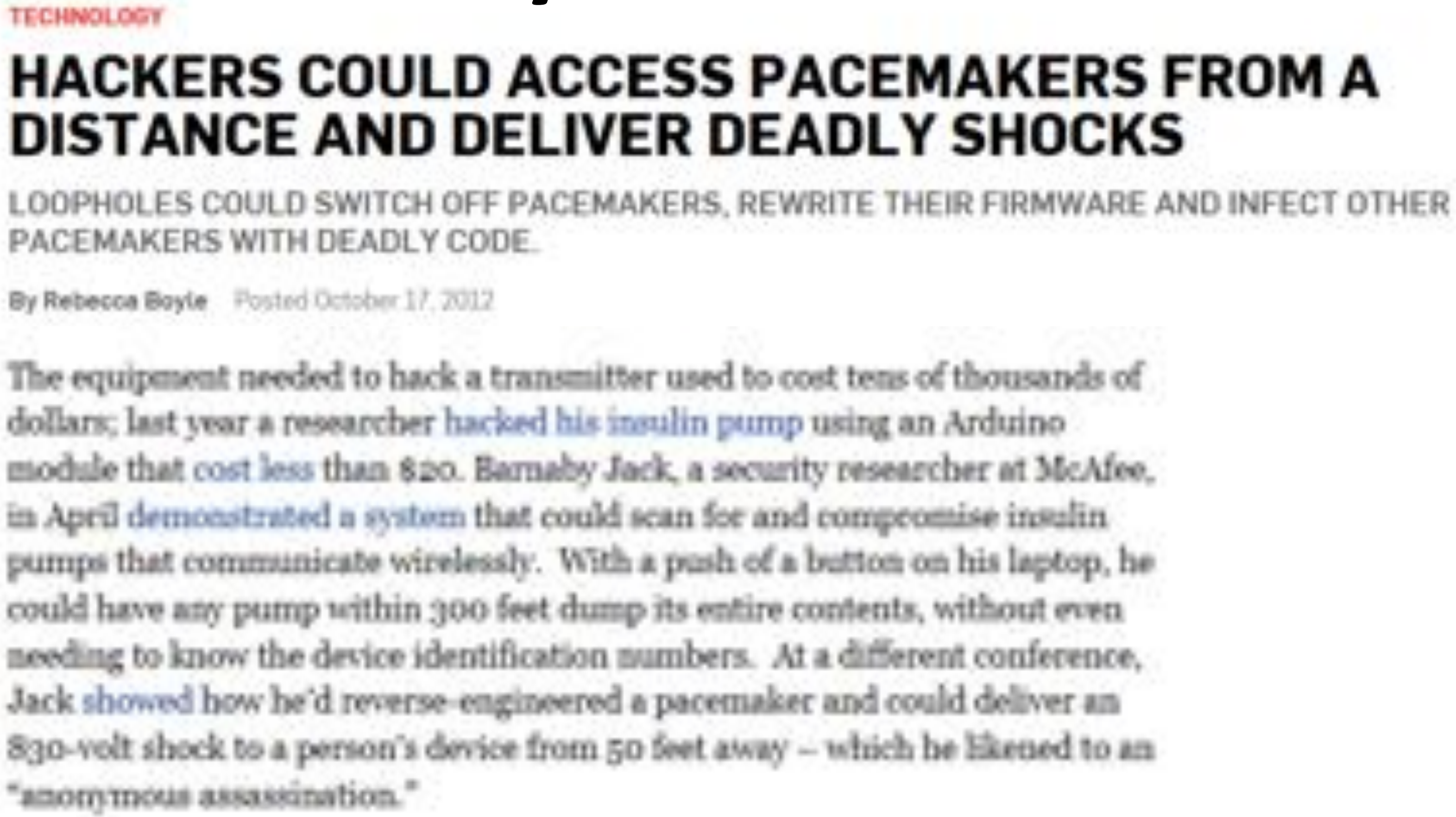
Cheney's heart problems were bad between 1978 and 2010, he suffered five heart attacks, underwent quadruple bypass surgery, and had a pump implanted directly to his heart. A defibrillator was implanted to regulate his heartbeat in 2007.

Cheney told his 60 Minutes interviewer, CNN Chief Medical Correspondent Dr. Sanjay Gupta, that at the time of the pacemaker implant, he was concerned about reports that attackers could hack the devices and kill their owners.

> "I was aware of the danger, if you will, that existed."

In 2007, he had the wireless feature disabled.

Security: Fact and Fiction



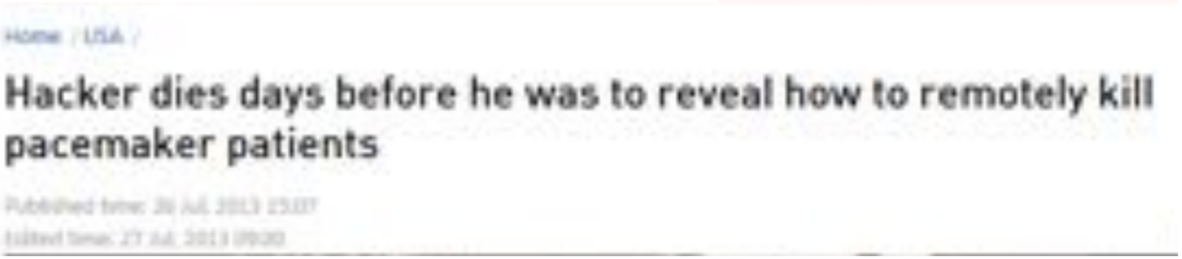
TECHNOLOGY

HACKERS COULD ACCESS PACEMAKERS FROM A DISTANCE AND DELIVER DEADLY SHOCKS

LOOPHOLES COULD SWITCH OFF PACEMAKERS, REWRITE THEIR FIRMWARE AND INFECT OTHER PACEMAKERS WITH DEADLY CODE.

By Rebecca Boyle Posted October 17, 2012

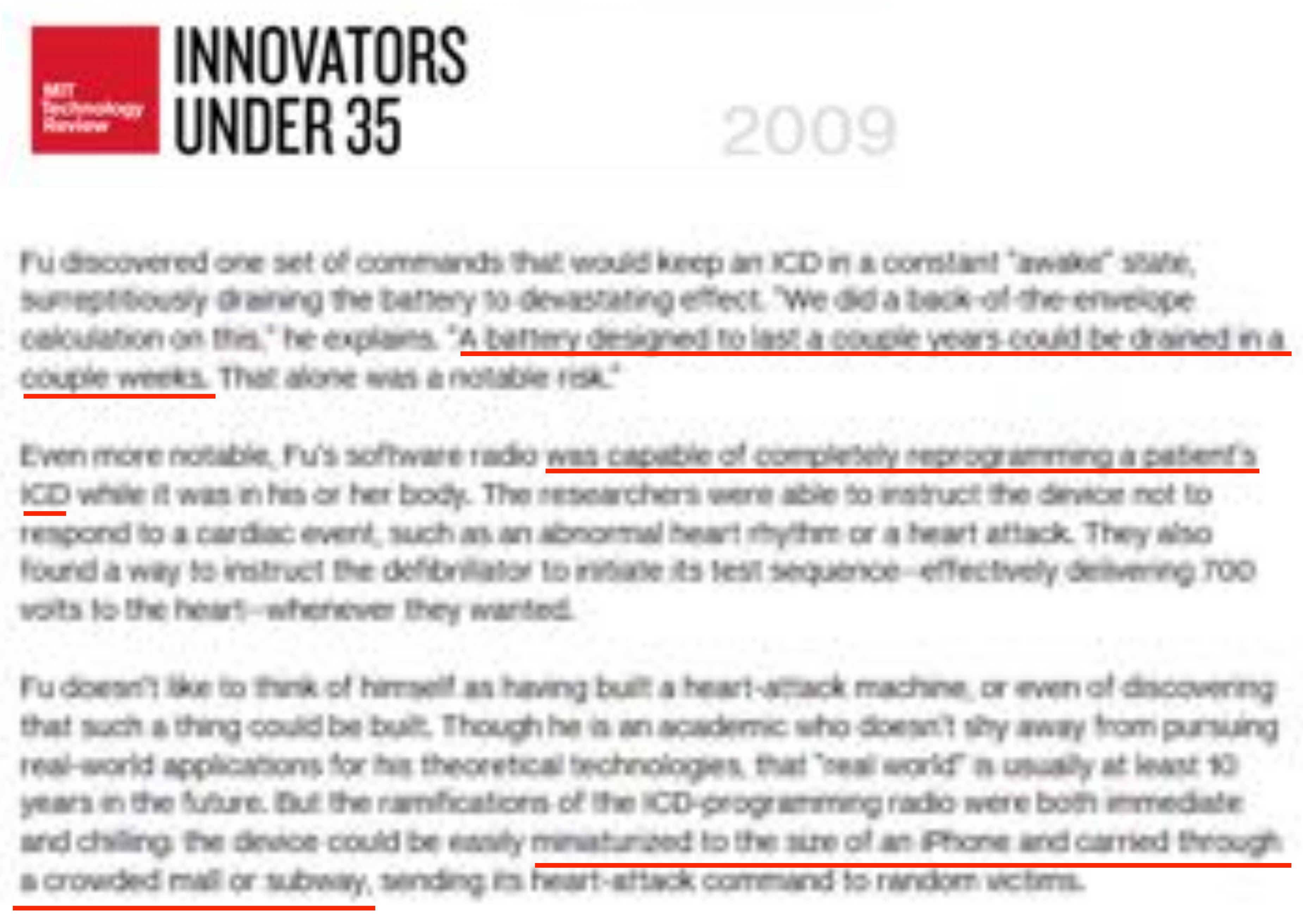
The equipment needed to hack a transmitter used to cost tens of thousands of dollars; last year a researcher hacked his insulin pump using an Arduino module that cost less than $20. Barnaby Jack, a security researcher at McAfee, in April demonstrated a system that could scan for and compromise insulin pumps that communicate wirelessly. With a push of a button on his laptop, he could have any pump within 300 feet dump its entire contents, without even needing to know the device identification numbers. At a different conference, Jack showed how he'd reverse-engineered a pacemaker and could deliver an 830-volt shock to a person's device from 50 feet away – which he likened to an "anonymous assassination."



Home / USA /

Hacker dies days before he was to reveal how to remotely kill pacemaker patients

Published time: 26 Jul, 2013 15:07
Edited time: 27 Jul, 2013 09:00



MIT Technology Review

INNOVATORS UNDER 35

2009

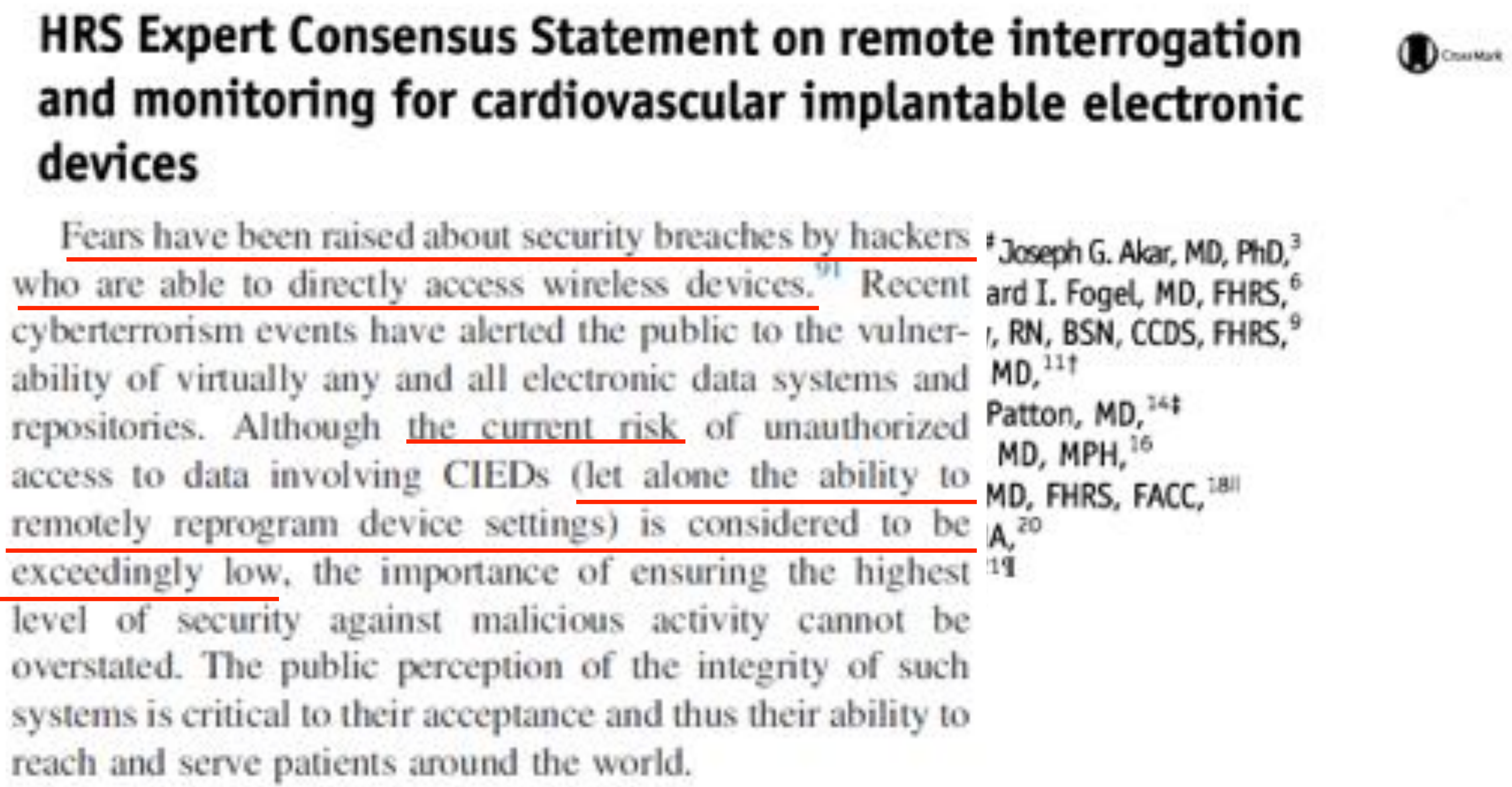
Fu discovered one set of commands that would keep an ICD in a constant "awake" state, surreptitiously draining the battery to devastating effect. "We did a back-of-the-envelope calculation on this," he explains. "A battery designed to last a couple years could be drained in a couple weeks. That alone was a notable risk."

Even more notable, Fu's software radio was capable of completely reprogramming a patient's ICD while it was in his or her body. The researchers were able to instruct the device not to respond to a cardiac event, such as an abnormal heart rhythm or a heart attack. They also found a way to instruct the defibrillator to initiate its test sequence—effectively delivering 700 volts to the heart—whenever they wanted.

Fu doesn't like to think of himself as having built a heart-attack machine, or even of discovering that such a thing could be built. Though he is an academic who doesn't shy away from pursuing real-world applications for his theoretical technologies, that "real world" is usually at least 10 years in the future. But the ramifications of the ICD-programming radio were both immediate and chilling: the device could be easily miniaturized to the size of an iPhone and carried through a crowded mall or subway, sending its heart-attack command to random victims.

HeartRhythm

Heart Rhythm Society



HRS Expert Consensus Statement on remote interrogation and monitoring for cardiovascular implantable electronic devices

Fears have been raised about security breaches by hackers who are able to directly access wireless devices.[91] Recent cyberterrorism events have alerted the public to the vulnerability of virtually any and all electronic data systems and repositories. Although the current risk of unauthorized access to data involving CIEDs (let alone the ability to remotely reprogram device settings) is considered to be exceedingly low, the importance of ensuring the highest level of security against malicious activity cannot be overstated. The public perception of the integrity of such systems is critical to their acceptance and thus their ability to reach and serve patients around the world.

Joseph G. Akar, MD, PhD,[3]
ard I. Fogel, MD, FHRS,[6]
, RN, BSN, CCDS, FHRS,[9]
MD,[11†]
Patton, MD,[14‡]
MD, MPH,[16]
MD, FHRS, FACC,[18‖]
A,[20]
[19¶]

Heart Rhythm 2015;12:e69-e100

Remote Programming Potential Use

- **In hospital setting** without CIED follow-up capability/device technologists (**satellite facilities**)
- **Parameter** reprogramming in patients **living far from the hospital**
- **Change stimulus** in non-pacemaker dependent patients eg
  - 3 months post implant (establish floor of eg 2.5V)
  - Diaphragmatic pacing with LV lead
- **Change lower / upper rate or AV setting**
  - 3 weeks after AV node ablation
  - Reduced / increased physical activity
  - Changes in spontaneous AV conduction
- **Switch on / off MRI programming**
- **Emergencies**
  - Manage reset after EMI
  - Disable inappropriate therapies (Lead fracture, AF)

Regulatory requirement - Patient Safety

- **Confidence, Acceptance & Patient safety can be achieved through incremental steps:**
  - ➢Initial step:

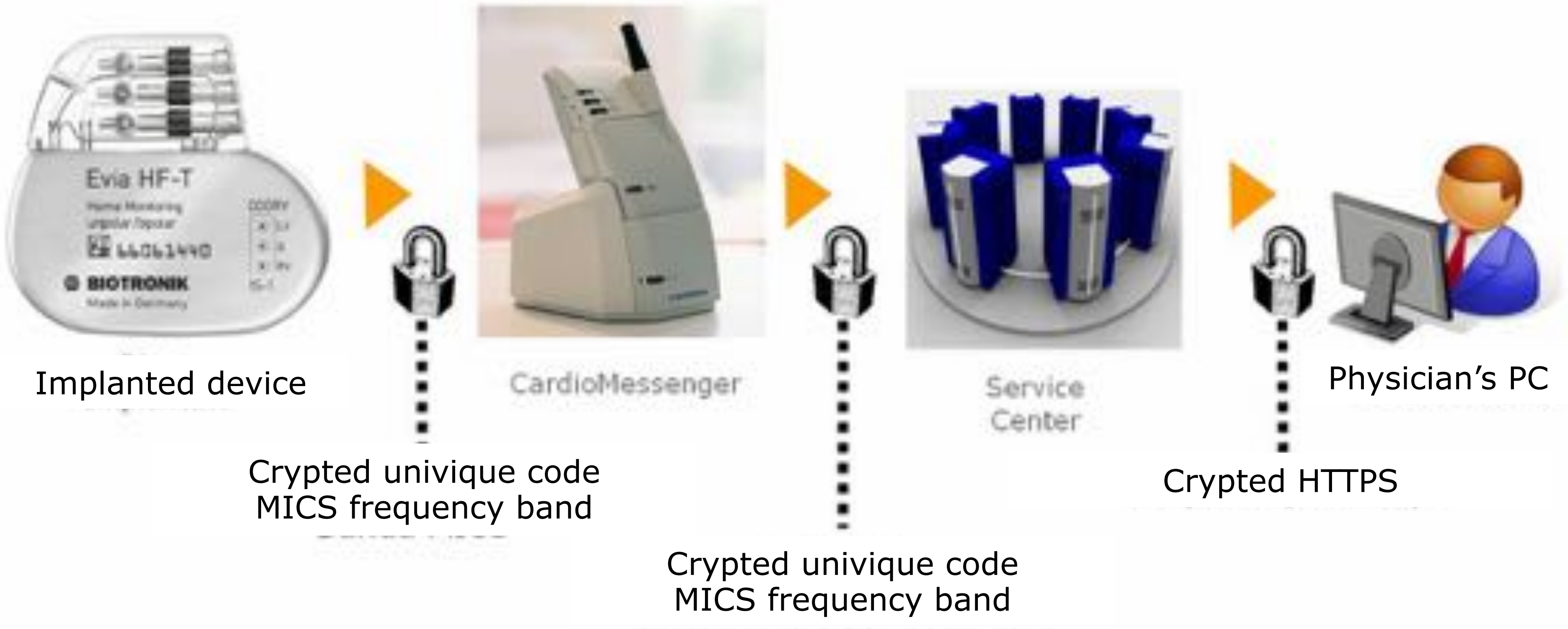
    Healthcare provider could be present with the patient to gain confidence in system reliability & patient safety

  - ➢Second step:

    Non-critical parameters could be programmed remotely

  - ➢Final step:

    Remote programming could become a common practice… as we use do our banking transactions over the internet !



Implanted device

CardioMessenger

Service Center

Physician’s PC

Crypted univique code
MICS frequency band

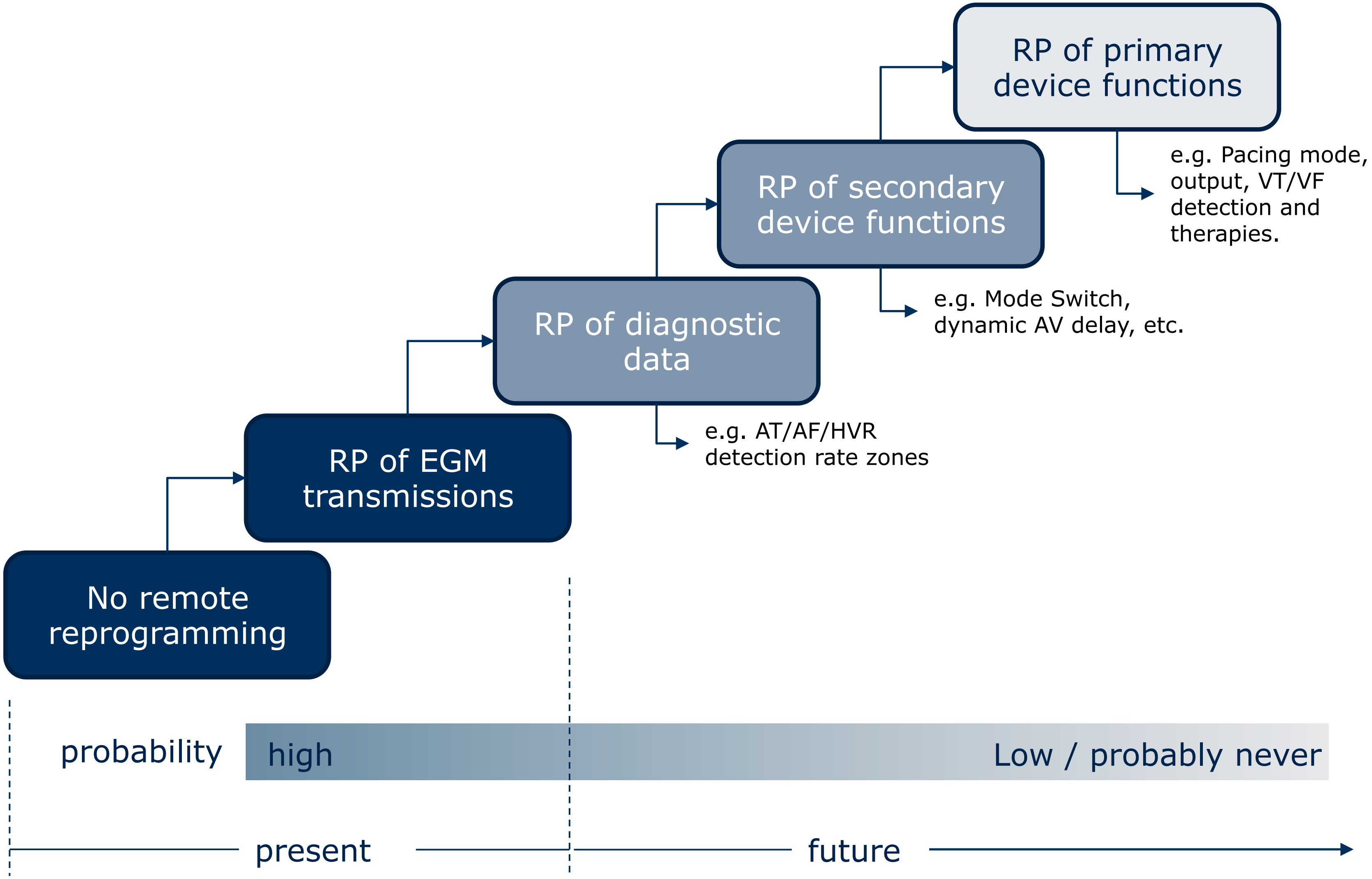
Crypted univique code
MICS frequency band

Crypted HTTPS

Service Center

- Patient data protection according to European Directives
- Careful risk analysis to ensure a high quality standard for medical devices
- Strict surveillance for physical and informatic access (continuous video monitoring, Hardkeys)
- Defense against cyber attacks (hardware/software attacks)
- Protected access

A reasonable path toward remote CIED reprogramming


RP of primary device functions
e.g. Pacing mode, output, VT/VF detection and therapies.
RP of secondary device functions
e.g. Mode Switch, dynamic AV delay, etc.
RP of diagnostic data
e.g. AT/AF/HVR detection rate zones
RP of EGM transmissions
No remote reprogramming
probability
high
Low / probably never
present
future