The (in)security of implantable medical devices

Eduard Marin

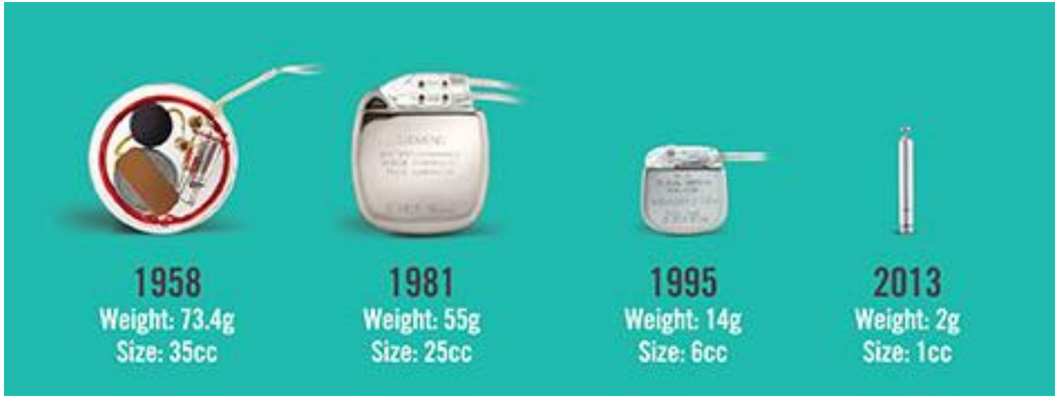
Telefonica Research, Spain

INSULIN PUMP

PACEMAKER

NEUROSTIMULATOR

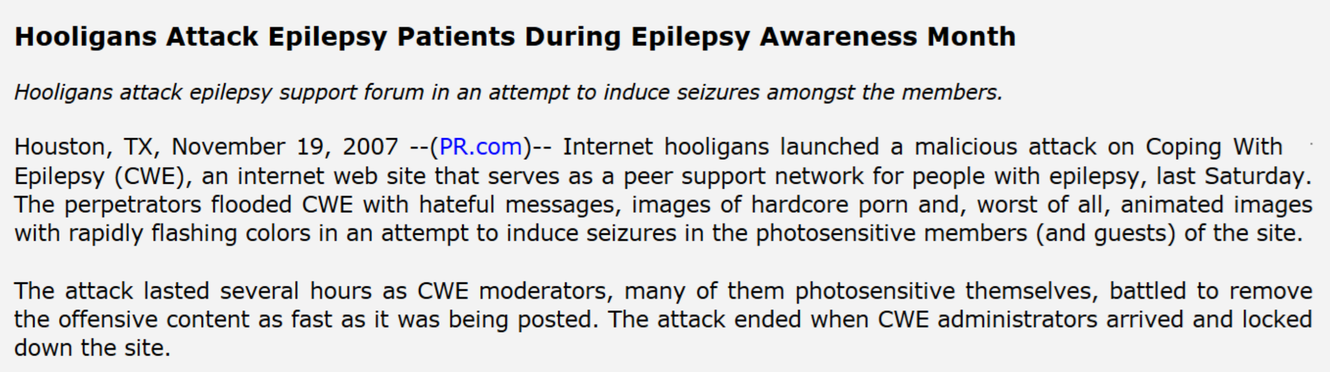
Evolution of pacemaker technology



Source: St Jude Medical

Why attack someone with an IMD?

- Cause physical harm



Hooligans Attack Epilepsy Patients During Epilepsy Awareness Month

Hooligans attack epilepsy support forum in an attempt to induce seizures amongst the members.

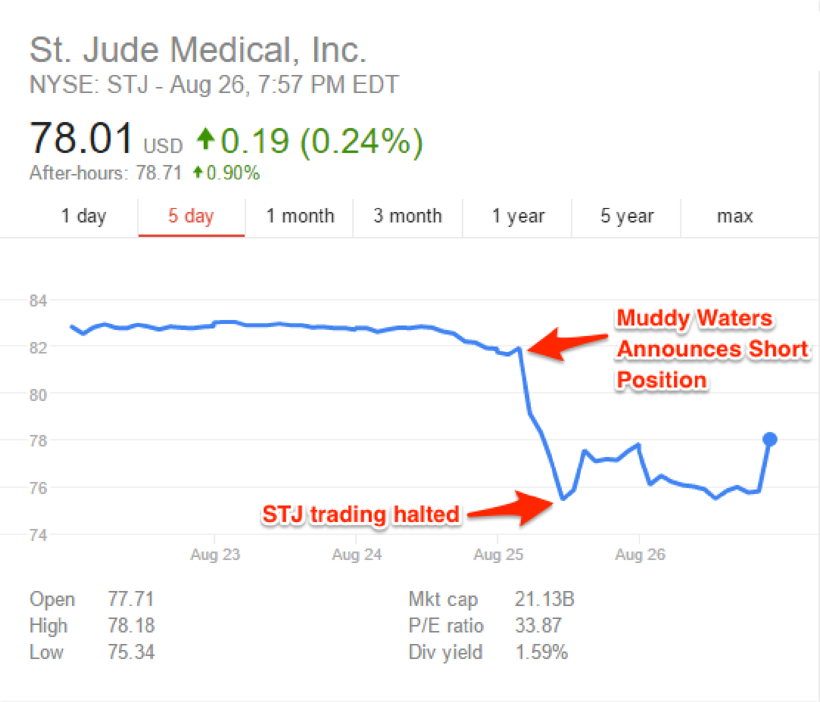
Houston, TX, November 19, 2007 --(PR.com)-- Internet hooligans launched a malicious attack on Coping With Epilepsy (CWE), an internet web site that serves as a peer support network for people with epilepsy, last Saturday. The perpetrators flooded CWE with hateful messages, images of hardcore porn and, worst of all, animated images with rapidly flashing colors in an attempt to induce seizures in the photosensitive members (and guests) of the site.

The attack lasted several hours as CWE moderators, many of them photosensitive themselves, battled to remove the offensive content as fast as it was being posted. The attack ended when CWE administrators arrived and locked down the site.

Why attack someone with an IMD?

- Cause physical harm
- Economic reasons

MUDDY WATERS CAPITAL



St. Jude Medical, Inc.

NYSE: STJ - Aug 26, 7:57 PM EDT

78.01 USD ↑0.19 (0.24%)

After-hours: 78.71 ↑0.90%

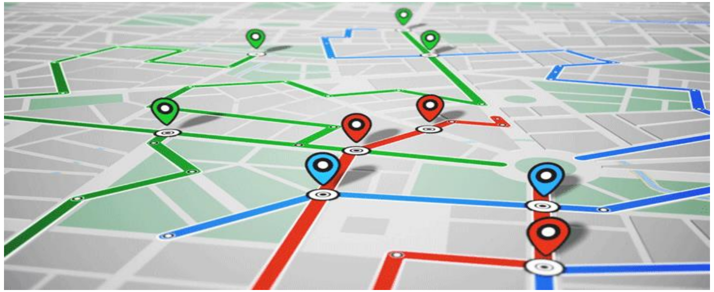
Muddy Waters Announces Short Position

STJ trading halted

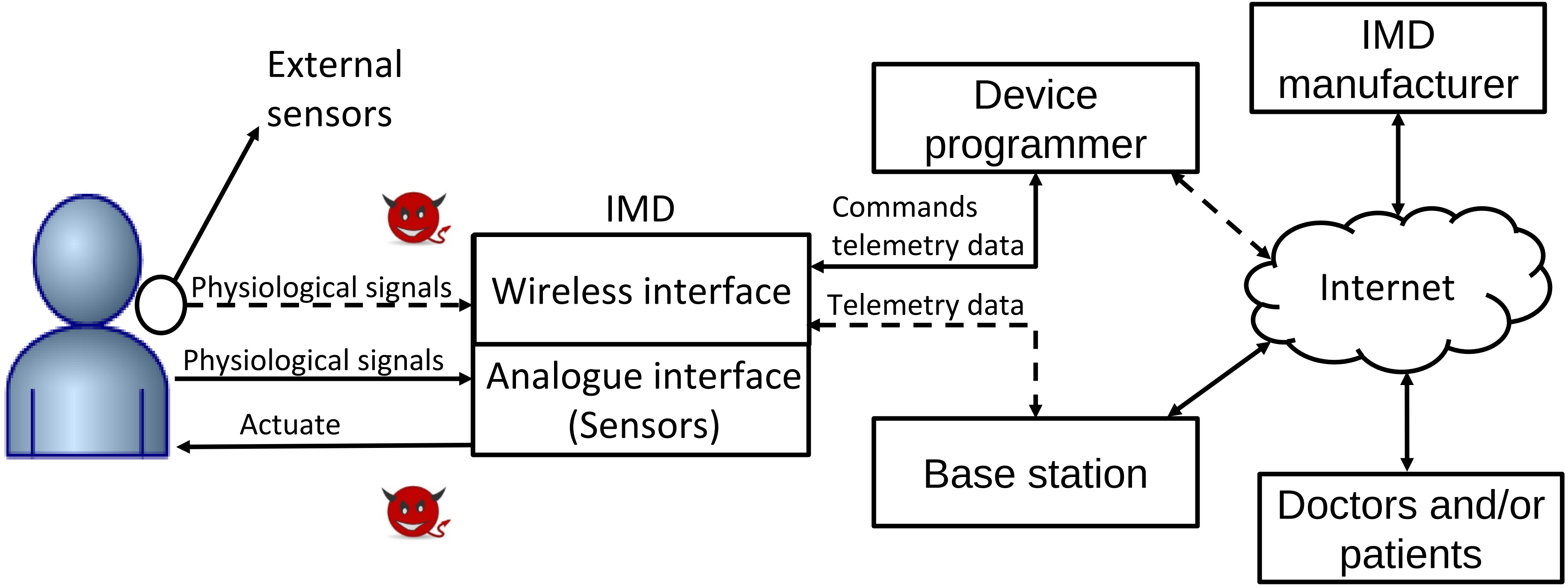
Open	77.71	Mkt cap	21.13B
High	78.18	P/E ratio	33.87
Low	75.34	Div yield	1.59%

Why attack someone with an IMD?

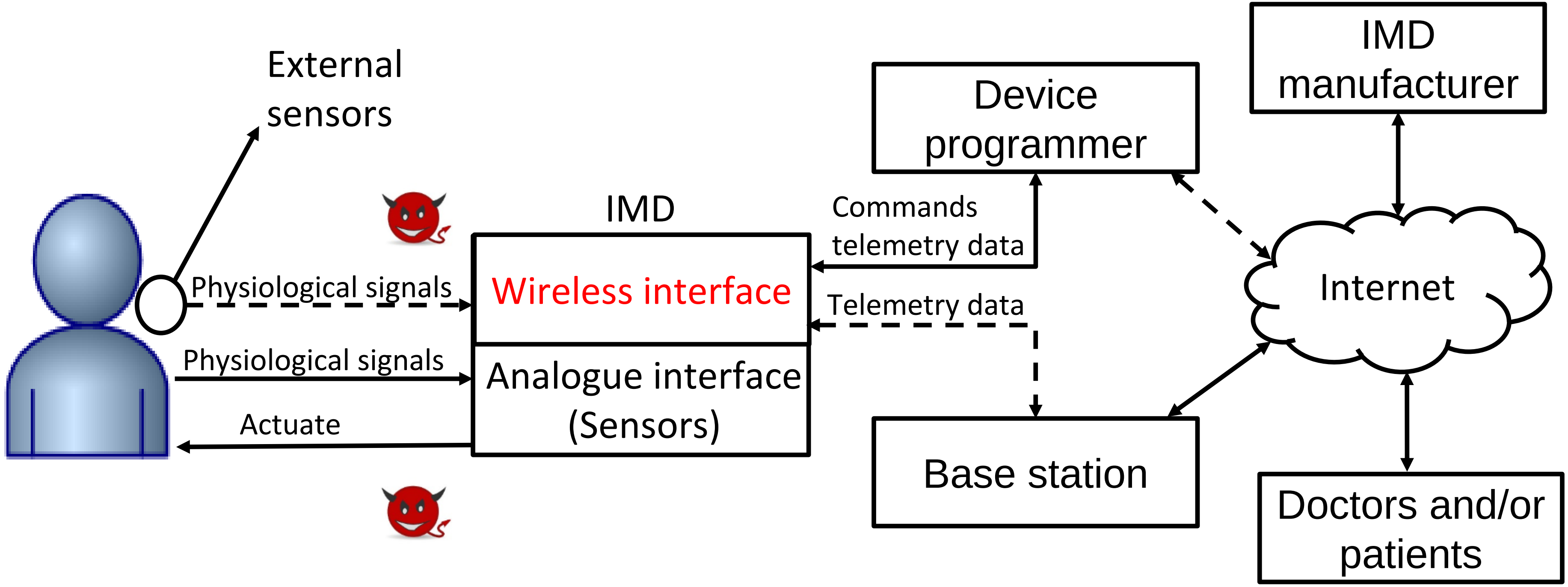
- Cause physical harm
- Economic reasons
- Learn patient’s sensitive information



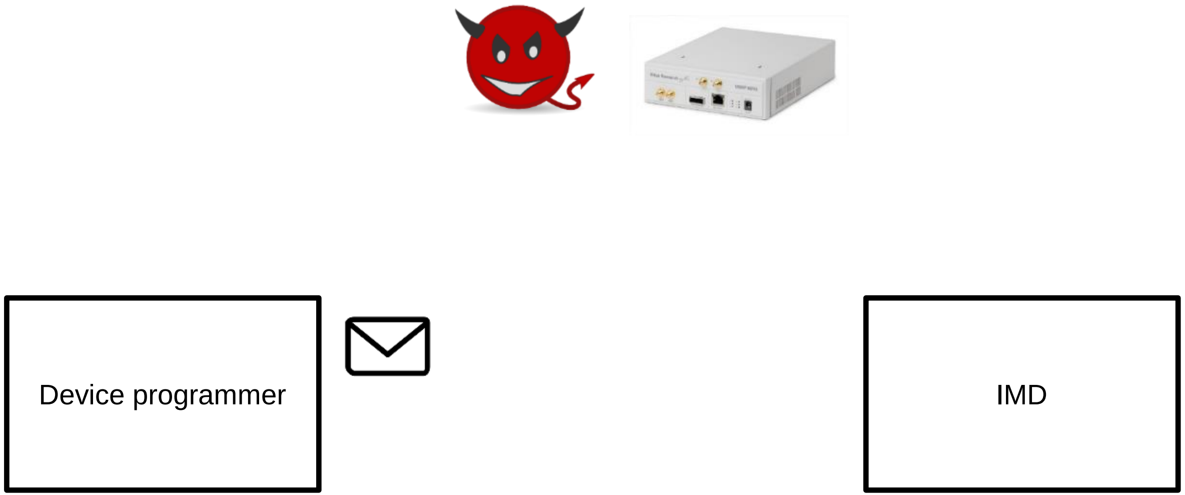
System architecture



System architecture



Wireless attacks (simplified)

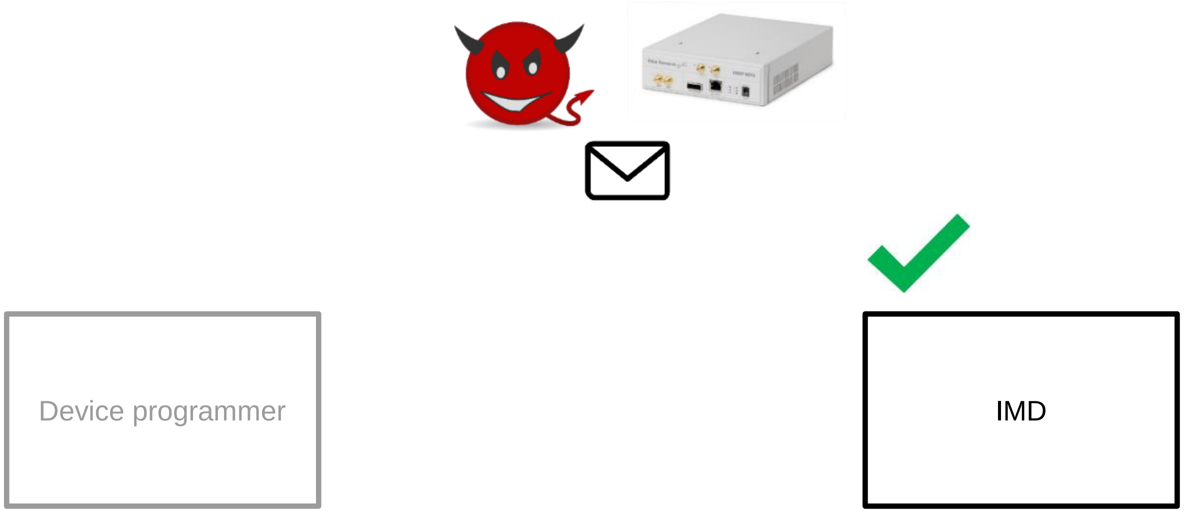


Device programmer

IMD

Adversaries can capture the exchanged messages to infer sensitive medical and personal data about the patient

Wireless attacks (simplified)

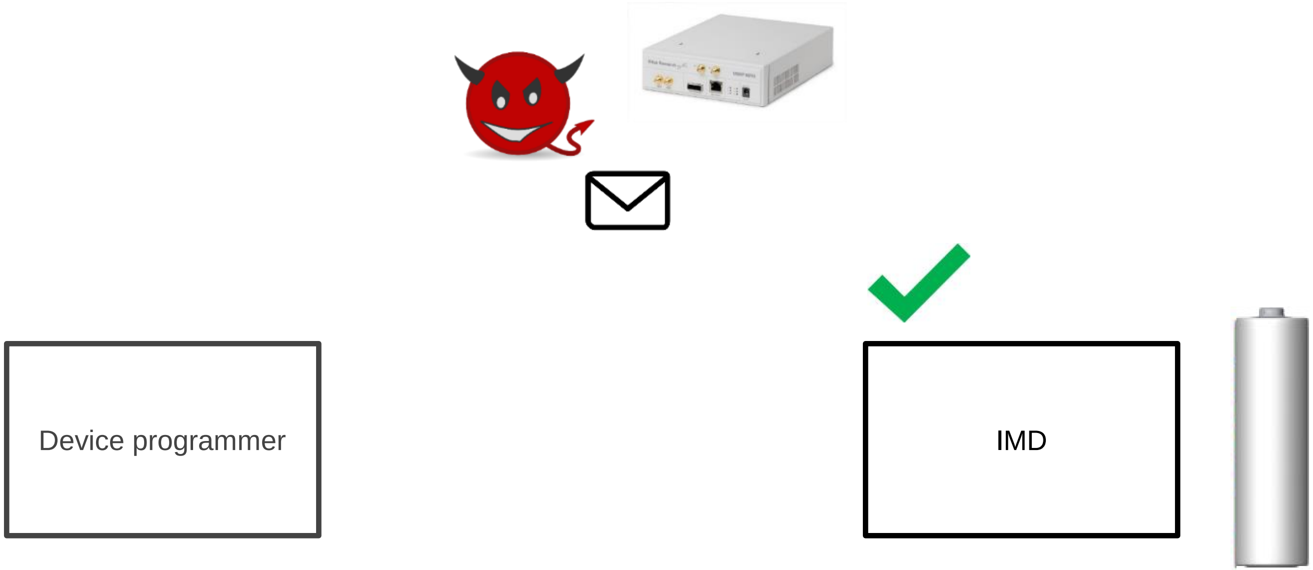


Device programmer

IMD

Adversaries can send maliciously crafted commands to the patient's IMD

Wireless attacks (simplified)



Device programmer

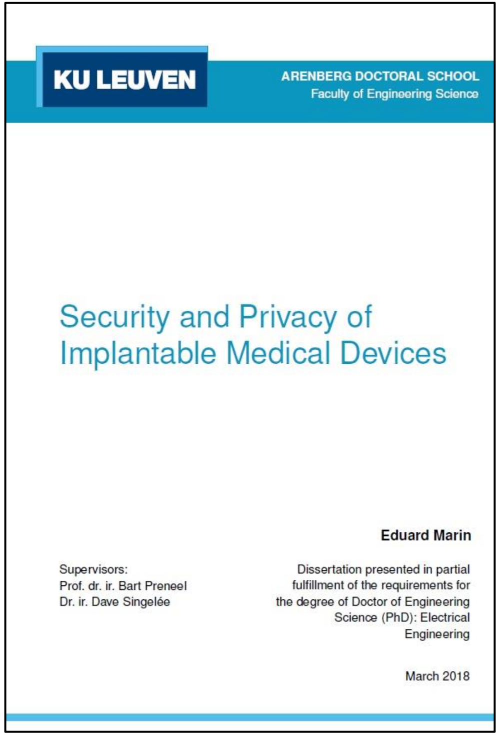
IMD

Adversaries can repeatedly send messages to the patient’s IMD to reduce the battery lifetime

“Academic attacks”

TIME

2008: Replay attacks on an ICD (Halperin et al.)
2010: DoS attacks on IMDs (Hei et al.)
2012: Attacks on an insulin pump (Li et al.)
2015: Attacks on an infusion pump system (Billy Rios)
2016: Attacks on an insulin pump system (Marin et al.)
2016: Attacks on pacemakers (Marin et al.)
2018: Attacks on neurostimulators (Marin et al.)
?? : First real attack in the wild



KU LEUVEN

ARENBERG DOCTORAL SCHOOL
Faculty of Engineering Science

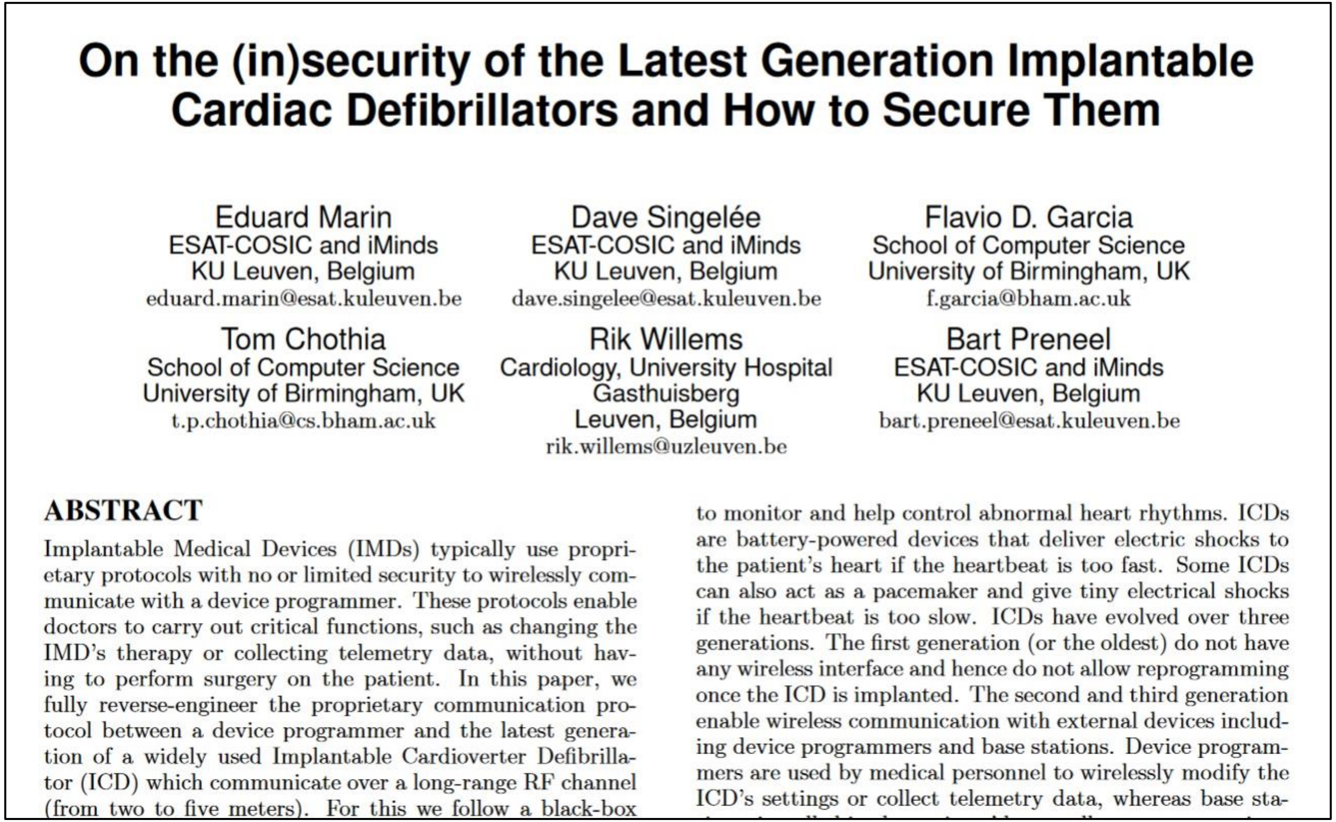
Security and Privacy of
Implantable Medical Devices

Eduard Marin

Supervisors:
Prof. dr. ir. Bart Preneel
Dr. ir. Dave Singelée

Dissertation presented in partial
fulfillment of the requirements for
the degree of Doctor of Engineering
Science (PhD): Electrical
Engineering

March 2018



On the (in)security of the Latest Generation Implantable Cardiac Defibrillators and How to Secure Them

Eduard Marin
ESAT-COSIC and iMinds
KU Leuven, Belgium
eduard.marin@esat.kuleuven.be

Dave Singelée
ESAT-COSIC and iMinds
KU Leuven, Belgium
dave.singelee@esat.kuleuven.be

Flavio D. Garcia
School of Computer Science
University of Birmingham, UK
f.garcia@bham.ac.uk

Tom Chothia
School of Computer Science
University of Birmingham, UK
t.p.chothia@cs.bham.ac.uk

Rik Willems
Cardiology, University Hospital
Gasthuisberg
Leuven, Belgium
rik.willems@uzleuven.be

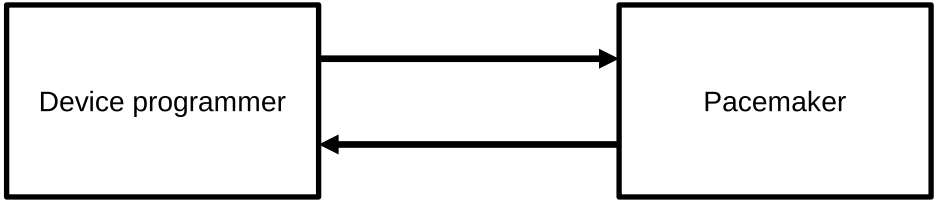
Bart Preneel
ESAT-COSIC and iMinds
KU Leuven, Belgium
bart.preneel@esat.kuleuven.be

ABSTRACT

Implantable Medical Devices (IMDs) typically use proprietary protocols with no or limited security to wirelessly communicate with a device programmer. These protocols enable doctors to carry out critical functions, such as changing the IMD's therapy or collecting telemetry data, without having to perform surgery on the patient. In this paper, we fully reverse-engineer the proprietary communication protocol between a device programmer and the latest generation of a widely used Implantable Cardioverter Defibrillator (ICD) which communicate over a long-range RF channel (from two to five meters). For this we follow a black-box

to monitor and help control abnormal heart rhythms. ICDs are battery-powered devices that deliver electric shocks to the patient's heart if the heartbeat is too fast. Some ICDs can also act as a pacemaker and give tiny electrical shocks if the heartbeat is too slow. ICDs have evolved over three generations. The first generation (or the oldest) do not have any wireless interface and hence do not allow reprogramming once the ICD is implanted. The second and third generation enable wireless communication with external devices including device programmers and base stations. Device programmers are used by medical personnel to wirelessly modify the ICD's settings or collect telemetry data, whereas base sta-

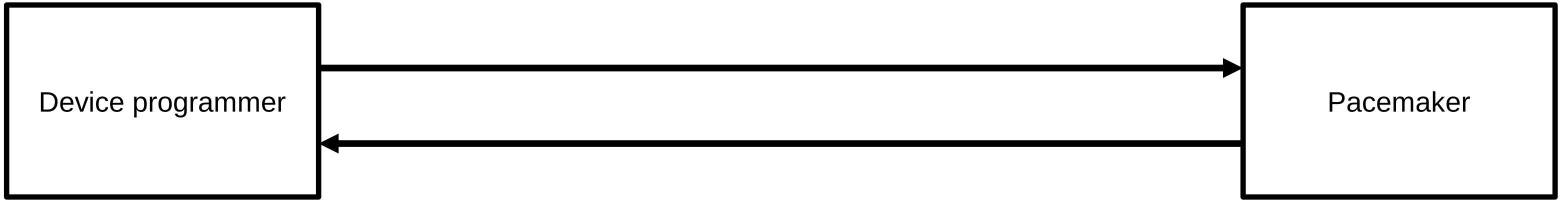
Pacemaker study



Device programmer

Pacemaker

1) Activation phase: Short-range communication channel (<10 cm)



Device programmer

Pacemaker

2) Programming phase: Long-range communication channel (2-5 m)

Laboratory setup

Device programmers

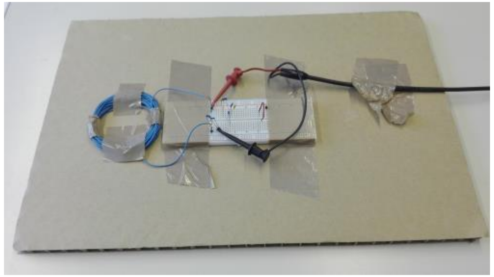
IMDs

NATIONAL INSTRUMENTS LabVIEW

Software Defined Radios

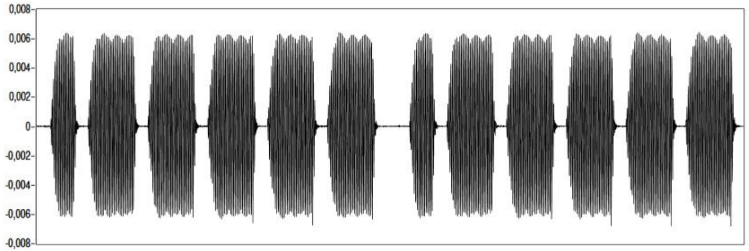
Antennas

Commercial laptop



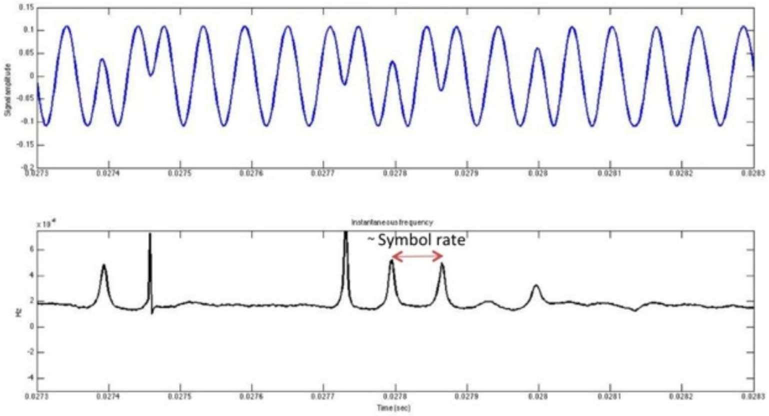
Wireless communication parameters

- Transmission frequency
  - **MICS band** (402 – 405MHz).
  - 10 channels, 300 KHz bandwidth/channe



- Modulation scheme
  - Device programmer – ICD: **FSK**
  - ICD – device programmer: **DPSK**

- Symbol rate
  - Hilbert transform (i.e. inst frequency)

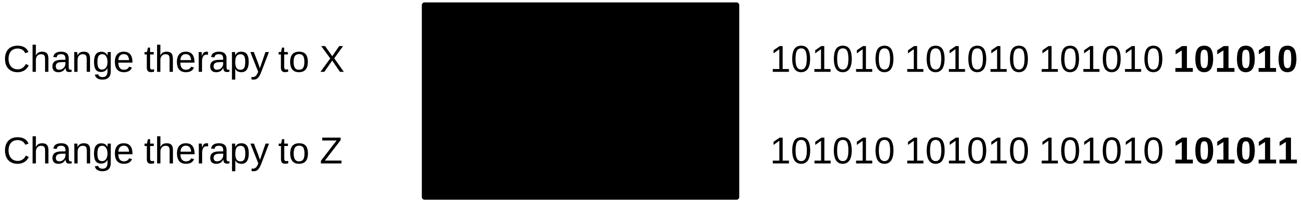


Security analysis

- Security-through-obscurity (i.e. proprietary protocols)
- Reverse engineering
  - Extract the firmware of these devices and analyse it
  - **Black-box approach**

Device programmer

Black-box reverse engineering



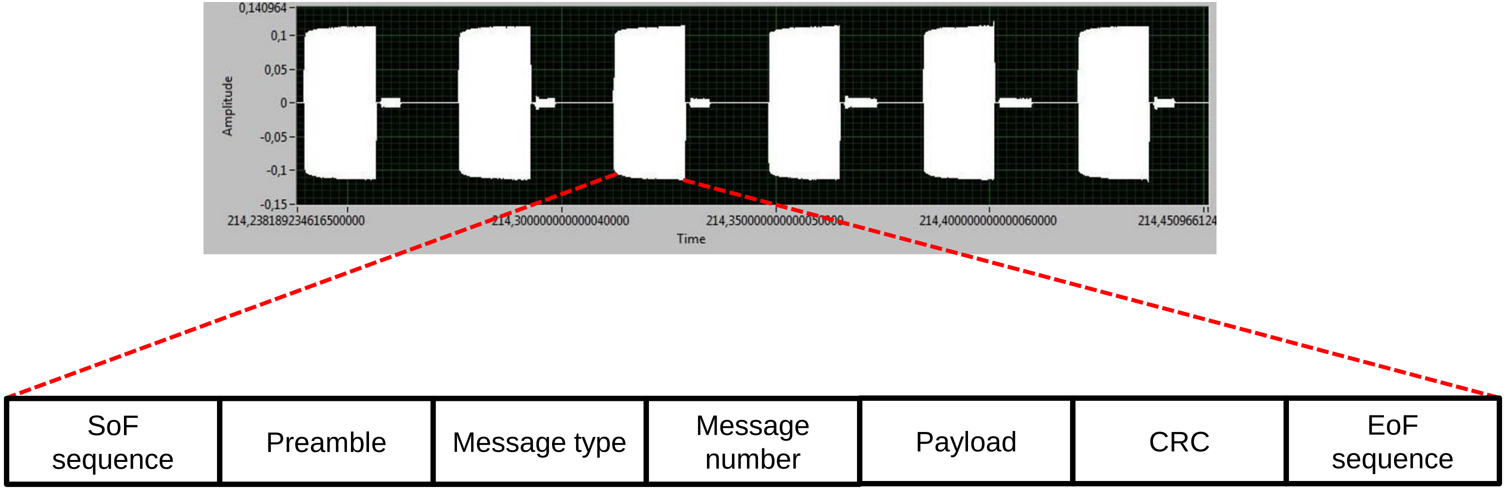
Change therapy to X

Change therapy to Z

101010 101010 101010 **101010**

101010 101010 101010 **101011**

Intercepting the signals



SoF sequence	Preamble	Message type	Message number	Payload	CRC	EoF sequence

Responsible disclosure procedure

June 2016: We notified Medtronic following the principle of responsible disclosure (and omitted important details in the paper)

August 2016: Paper got accepted at ACSAC'16

March 2019: the FDA issued a safety communication

Two CVEs were assigned to our findings:

- CVE-2019-6538: Improper Access Control score: 9.3
- CVE-2019-6540: Cleartext transmission of sensitive information score: 6.5

Common security misconceptions

Security-by-obscurity is sufficient

Hacker cannot extend communication range

Hacker needs expensive hardware devices and “big antennas”

Hacker needs to be very near the patient to activate the IMD

Threat model

Defines who the adversary is and its capabilities

It is crucial to understand this

Problem: Manufacturers determine their threat model keeping the previous misconceptions in mind

So… how should we do it?

Use cryptography (Kerckhoffs’s principle)

Balance between security, availability, usability and safety

Lightweight cryptographic algorithms

Novel key management solutions

Conclusions

Security = strong cryptographic algorithms (based on hard mathematical problems)

Insecurity = Security-by-obscurity, signal strength, distance, activation….

No real attack so far, but security is needed now