Department of
Neuroscience

Implant security

The new deep end

Christos Strydis

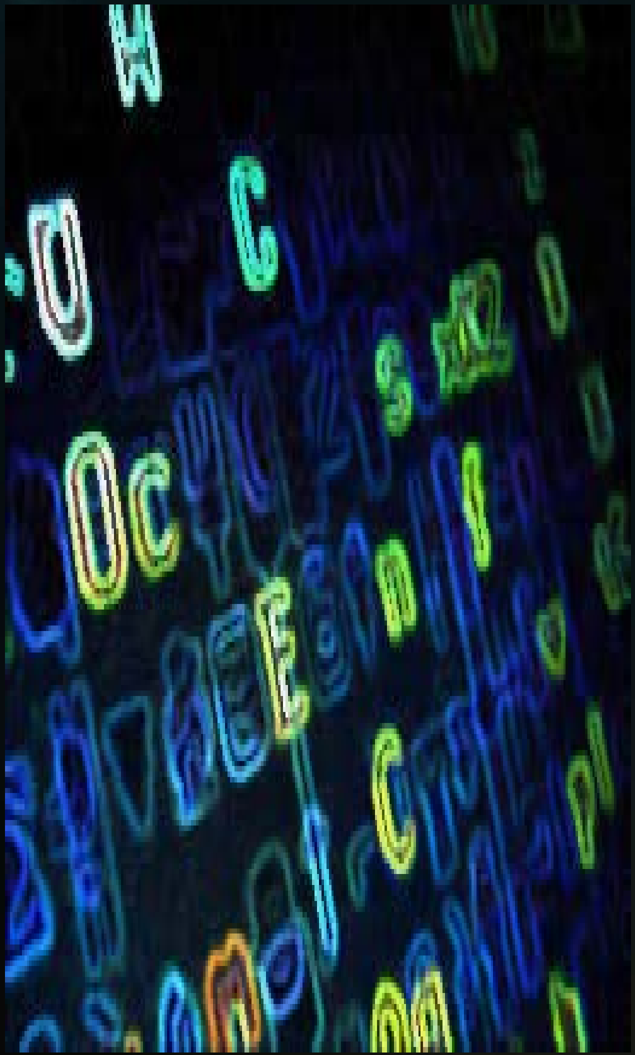
Neuroscience Department, Erasmus Medical Center

E-mail: c.strydis@erasmusmc.nl

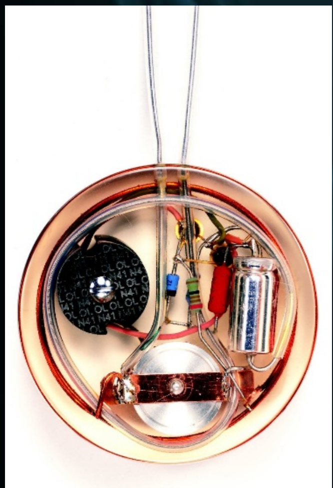
Dresden, March 18, 2016 – TRUDEVICE 2016

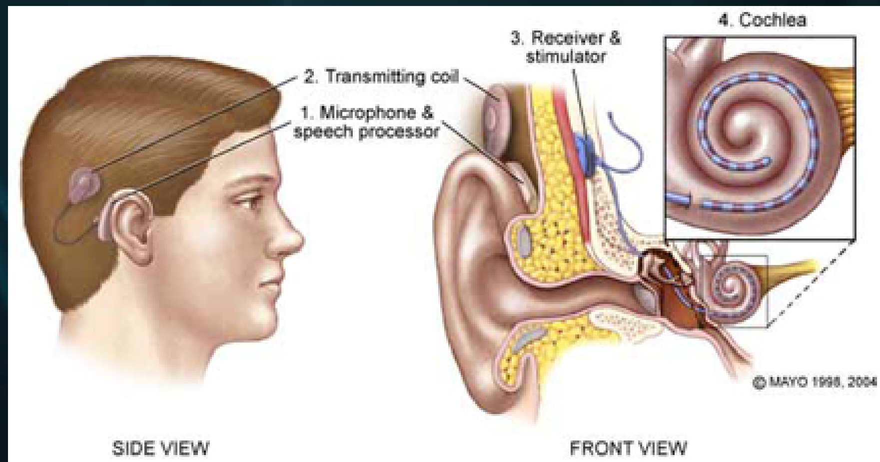
Outline

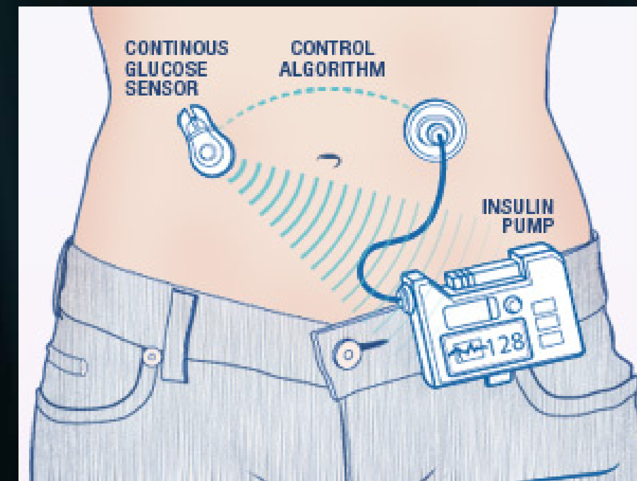
- Implantable Medical Devices
- Modern IMDs & Security
- Typical security challenges
- Unique security challenges
- Current state of affairs
- Future steps & Open challenges

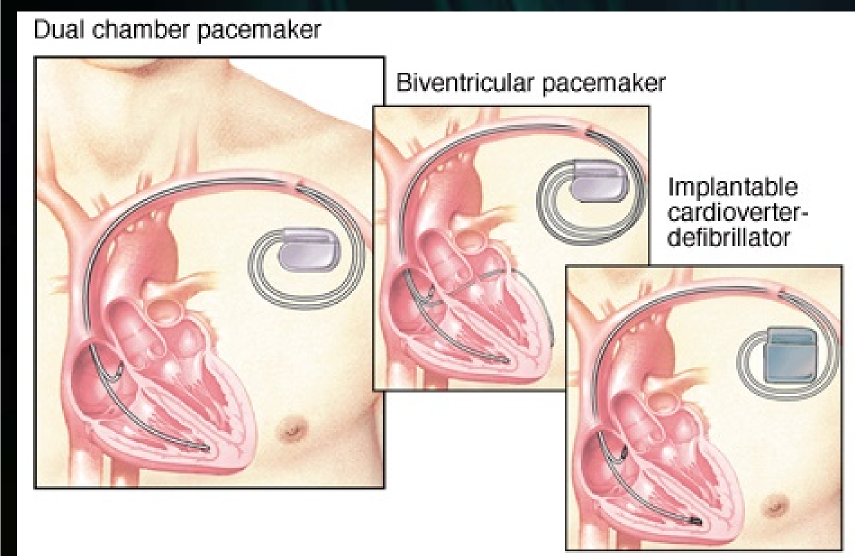


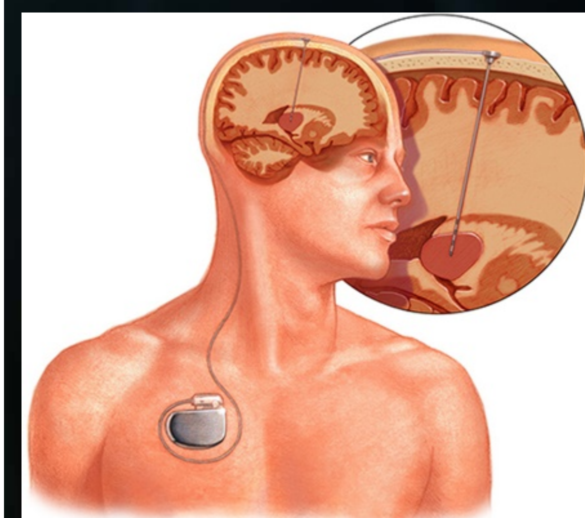
Implantable Medical Devices (IMDs)

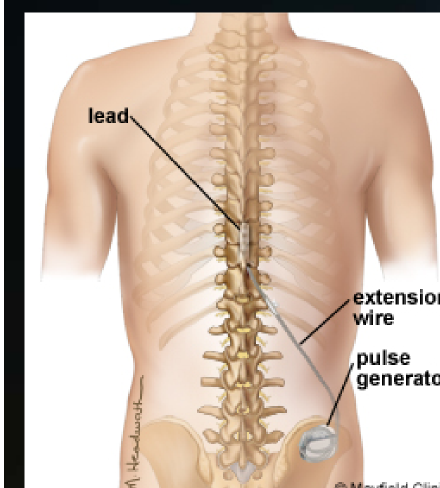




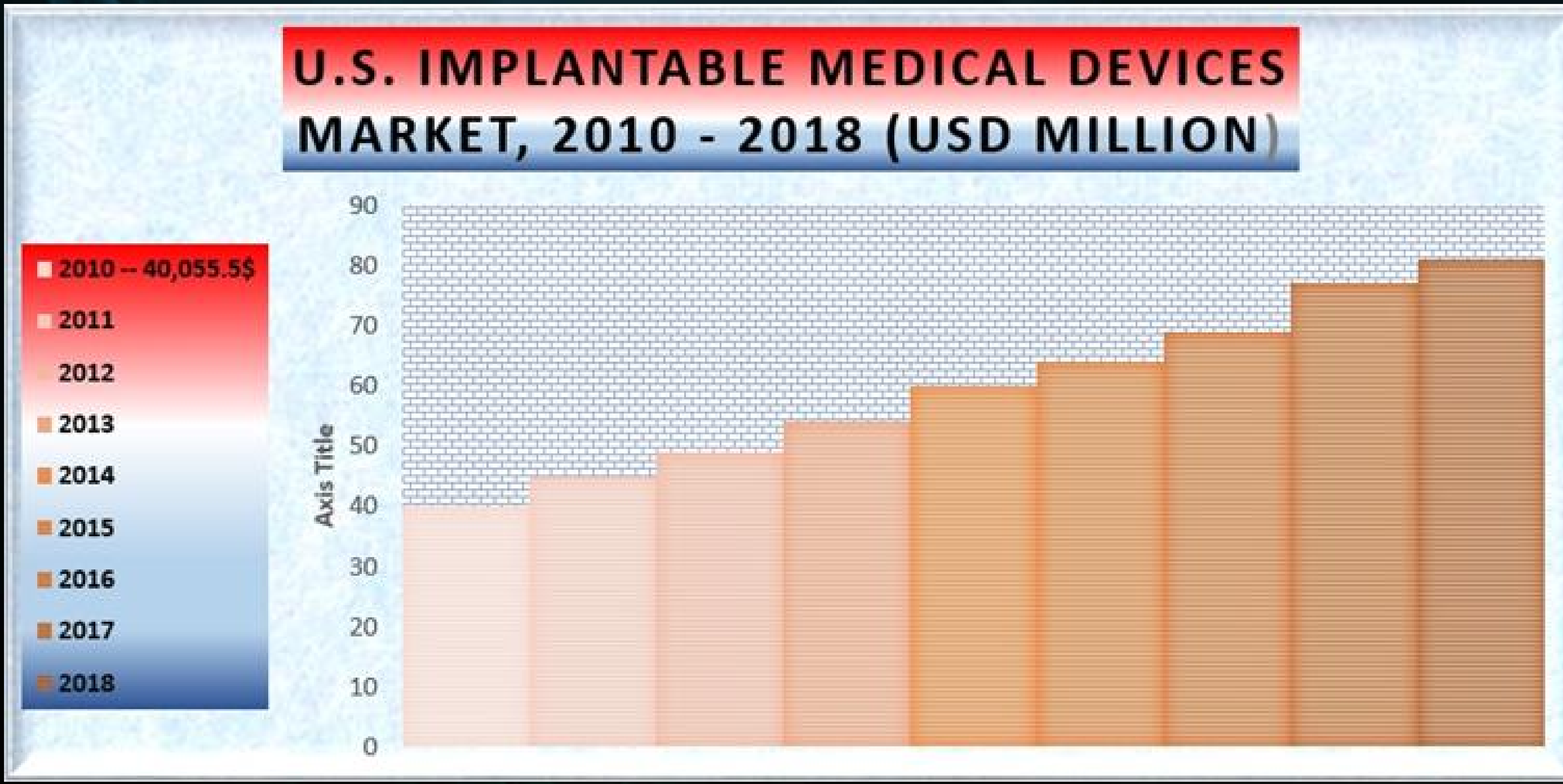








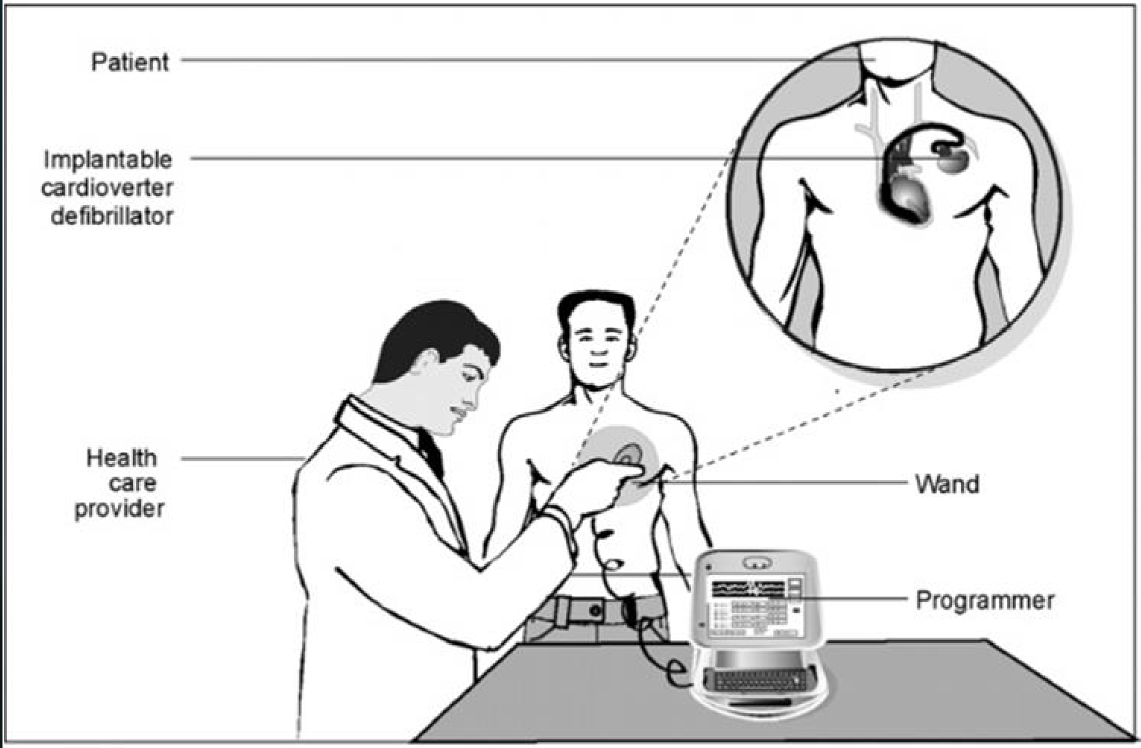
IMD market is booming



Source: Integrated Healthcare Association, National Center for Biotechnology Information

IMDs + wireless: A brave new world

- Moving from passive to active devices
- Moving towards patient-centric devices and treatments
- Moving to more integrated e-Health
- Bringing control to the patient (Healthcare-at-Home)



Source: GAO.

IMDs + wireless: A brave new world

- Higher energy budgets needed
- Higher EM considerations to be tackled
- Higher security risk!

What scientists thought around 2008

Profiling of Symmetric-Encryption Algorithms for a Novel Biomedical-Implant Architecture

Christos Strydis
christos@ce.et.tudelft.nl

Di Zhu
D.Zhu@student.tudelft.nl

Georgi N. Gaydadjiev
georgi@ce.et.tudelft.nl

Computer Engineering Laboratory, Electrical Engineering Dept.
Delft University of Technology
Postbus 5031, 2600 GA, Delft
The Netherlands

ABSTRACT

Starting with the implantable pacemaker, microelectronic implants have been around for more than 50 years. A plethora of commercial and research-oriented devices have been developed so far for a wide range of biomedical applications. In view of an envisioned expanding implant market in the years to come, our ongoing research work is focusing on the specification and design of a novel biomedical microprocessor core, carefully tailored to a large subset of existing and future biomedical applications. Towards this end, we have taken steps in identifying various tasks commonly required by such applications and profiling their behavior and requirements. One such task is decryption of incoming commands to an implant and encryption of outgoing (telemetered) biological data. Secure bidirectional information relaying in implants has been largely overlooked so far although protection of personal (biological) data is very crucial. In this context, we evaluate a large number of symmetric (block) ciphers in terms of various metrics: average and peak power consumption, total energy budget, encryption rate and efficiency, program-code size and security level. For our study we use XTREM, a performance and power simulator for Intel's XScale embedded processor. Findings indicate the best-performing ciphers across most metrics to be MISTY1 (scores high in 5 out of 6 imposed metrics), IDEA and RC6 (both present in 4 out of 6 metrics). Further profiling of MISTY1 indicates a clear dominance of load/store, move and logic-operation instructions which gives us explicit directions for designing the architecture of our novel processor.

Categories and Subject Descriptors

I.6.6 [**Simulation and modeling**]: [Simulation Output Analysis]; C.3 [**Computer Systems Organization**]: Special-purpose and application-based systems—*Real time, and embedded systems*; E.3 [**Data**]: Data Encryption—*Standards*

General Terms

Security, Performance

Keywords

implantable devices, ultra-low power, symmetric encryption, microarchitectural profiling

1. INTRODUCTION

Microelectronics design has shifted in recent years to synthesizing low-power systems. A major vehicle towards this trend has been the radical shift, through enabling technology, to portable devices such as mobile phones and laptop computers. A field of science that has adhered to strict low-power constraints since its infancy is biomedical microelectronic implants and has been around for more than 50 years. Perhaps the most popular instance of such devices is the implantable pacemaker which, apart from saving lives, has acted as a catalyst on the general public closed-mindedness against biomedical implants. Indicative of the penetration and impact pacemakers have achieved is the fact that, in Europe alone, a total number of 299,705 implanted devices have been registered over the year 2003 (source: European Society of Cardiology [12]).

With the pacemaker being the flagship, biomedical implants are now being designed for a large, and constantly increasing, range of applications. These applications are primarily grouped into two main categories: physiological-parameter monitoring (for diagnostic purposes) and stimulation (actuation, in general) [27]. Instances of the former are devices measuring body temperature [33], blood pressure [13], blood-glucose concentration [35], gastric pressure [25], tissue bio-impedance [22] and more. In the latter category belong implantable pacemakers [5, 16] and implantable intracardiac defibrillators (ICDs) [31], various functional electrical stimulators for paralyzed limbs [26], for bladder control [23], for blurred cornea in the eye [24] and more.

In a world where clinical healthcare costs are increasing and population is aging, implant applications are expected to boom even further in the years to come. A future where people are moving around performing their everyday tasks while tiny implants are monitoring or assisting their body is maybe not so far. Implants are expected to be under the direct or indirect control of their hosts. Commands will be given to them to adjust their operation and biological data will be casually telemetered from them to logging stations

"I really am not convinced that any of this [implant security] is valuable to the problem domain you have identified. I even talked to a few medical professionals about the need for encryption in medical sensor data, and they indicated that this was not very relevant to anything they could envision."

[Reviewer comment – Computing Frontiers 2008]

General-public first realization came around the time of "Homeland" series (ca. 2013)

["Broken Hearts": How plausible was the Homeland pacemaker hack? -- *Barnaby Jack*, Feb 25, 2013]

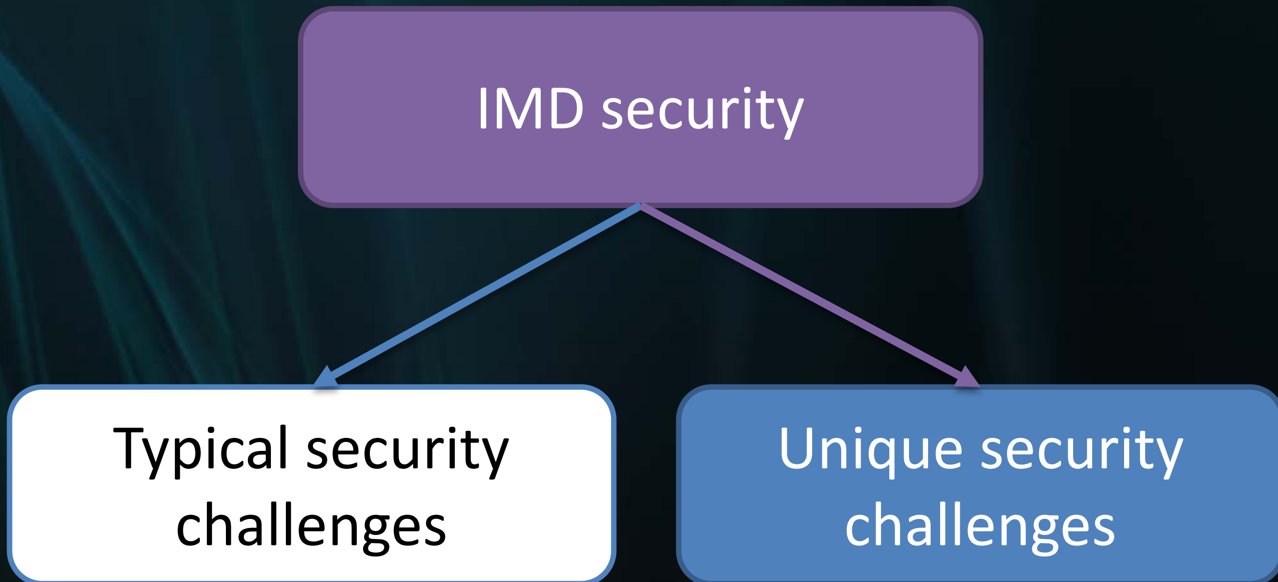
Newsflashes

- **“Hacking Vulnerable Medical Equipment Puts Millions at Risk”** – *Liviu Arsene (BitDefender) 2015*
- **“Ransomware Expected to Hit ‘Lifesaving’ Medical Devices In 2016”** – *Forrester 2015*
- **First online murder to happen by the end of 2014”** – *Europol 2014*
- **“Doctors disabled wireless in Dick Cheney’s pacemaker to thwart hacking”** – *CBS news 2013*

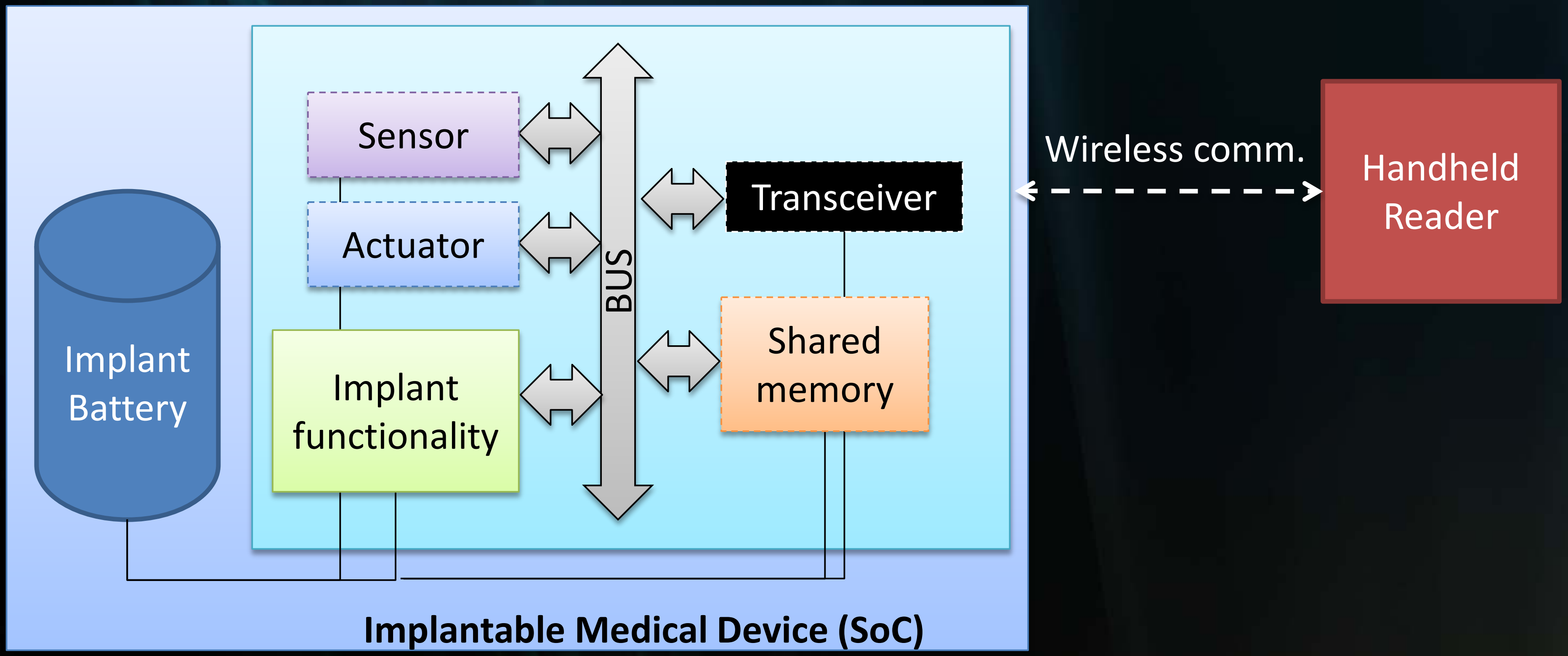
Newsflash of the day (17-03-2016)

- **IEEE Spectrum:** "5 Major Hospital Hacks: Horror Stories from the Cybersecurity Frontlines"
  - Records → China
  - DDoS by Anonymous
  - Faking out the doctors
  - The lure of Angry Birds
  - Pay up or else

IMD security challenges



A typical IMD SoC



Permissible actions within an IMD

I. Read out application-related data

II. Read or modify configuration parameters

III. Turn on and off the IMD

IV. Flash the IMD program memory with new binary
   - Upgrade functional, security or other aspects of IMD; for debugging or patient-adjustment purposes

V. Read or write memory contents, control registers
   - Peripherals are memory-mapped, thus enables advanced diagnostics, testing and debugging

IMD user roles

- Based on permissible IMD actions

Role	Permission level	Permissions
Patient	Lowest	Read application-related data (I)
Physician		Read/modify application-related data; switch device on/off (I – III)
Technician	Highest	Read/modify all implant data; switch device on/off; update device firmware (I – V)

IMD threat model

- Only remote (non-physical) access to IMD allowed
- IMD is fully shielded, preventing EMI
- Authentication credentials are unknown to adversaries
- Cryptographic cipher and security protocol are secure
- Attackers can send arbitrary messages over wireless link

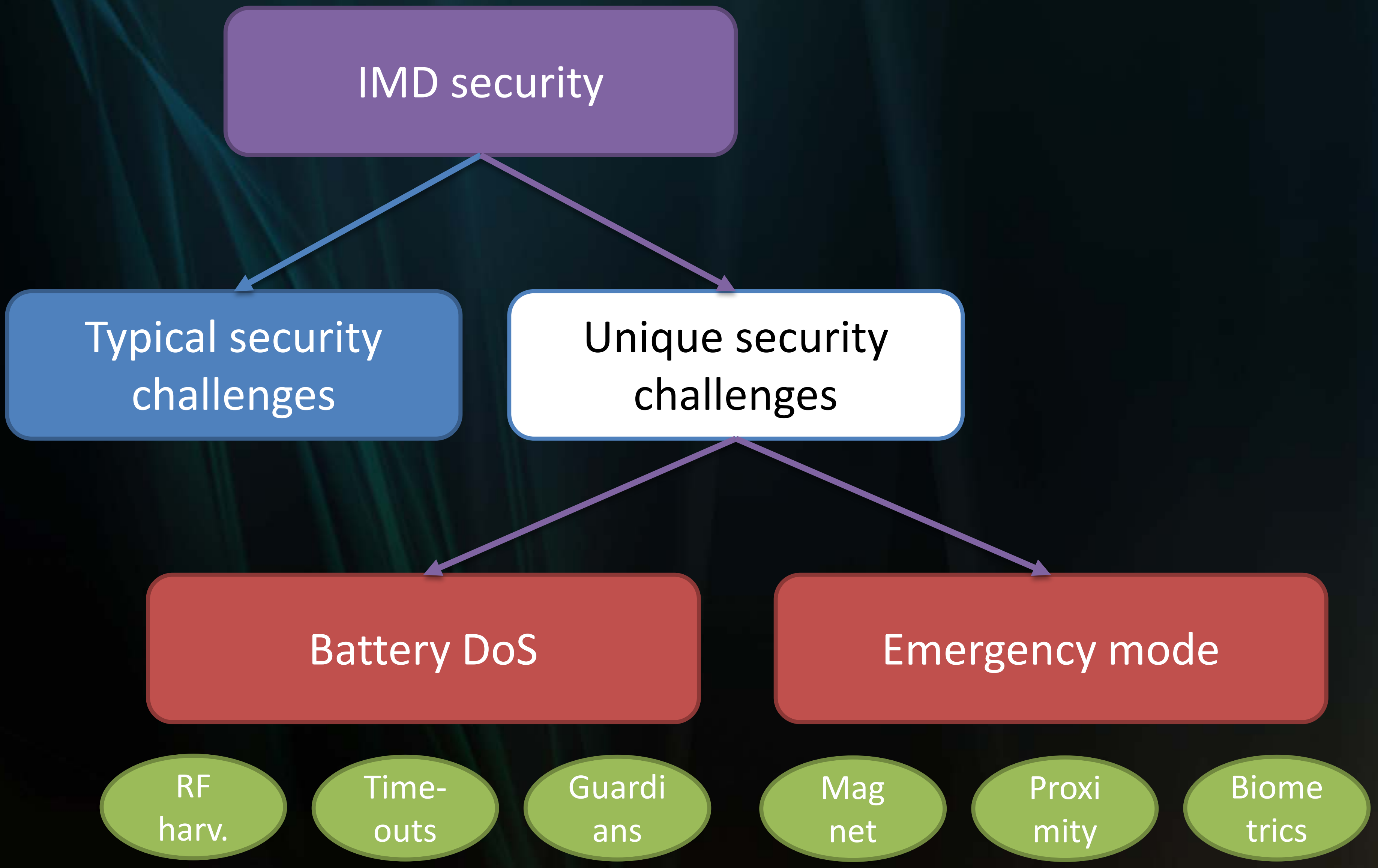
- **Security threats (hi – lo)**
  - Modification of IMD operation [CIANA]
  - Data-log manipulation (forging) [CIANA]
  - Data theft [CIANA]

Secure Hardware-Software Architectures for Robust Computing Systems

IMD security requirements

- Security compliance with extra-functional constraints
  - e.g. power consumption, energy budget, execution time
- Security compliance with proper treatment delivery
  - IMD functionality is mission-critical; should be immutable
- Security compliance with maintenance tasks
  - F/W updates, diagnostics, debugging mode by technician
- Patient-data security and privacy
  - IMD-generated data property of patient; secure store/tx
- Patient safety & device accessibility
  - Patient safety takes precedence over IMD security; balance

The deep end


IMD security
Typical security challenges
Unique security challenges
Battery DoS
Emergency mode
RF harv.
Time-outs
Guardi ans
Mag net
Proxi mity
Biome trics

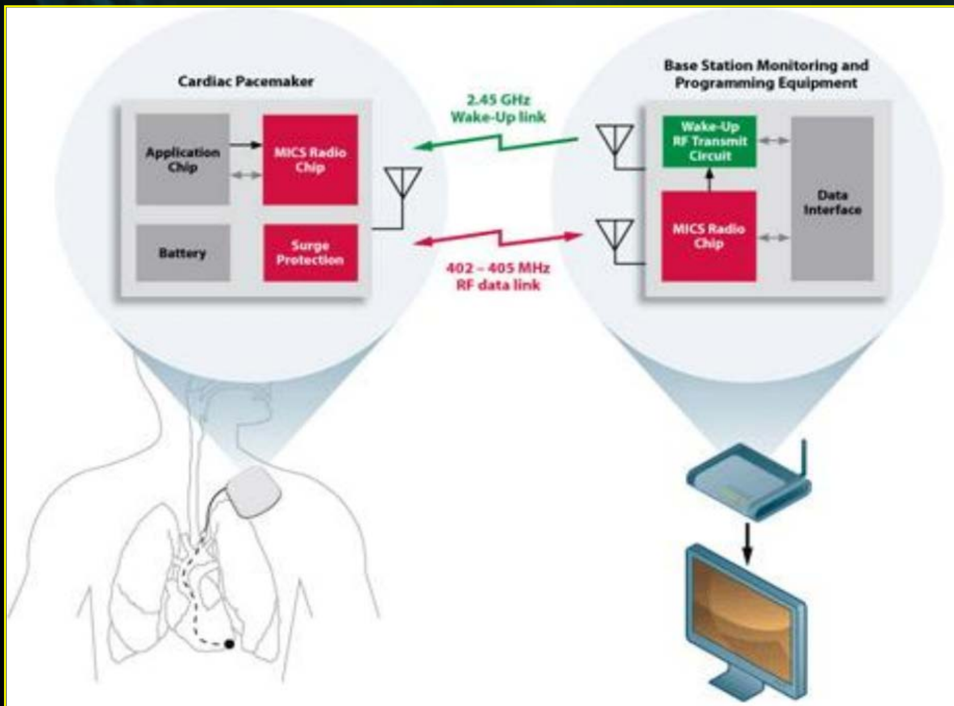
Battery-DoS solutions

1. Energy harvesting
   – Reader provides energy required for security operations

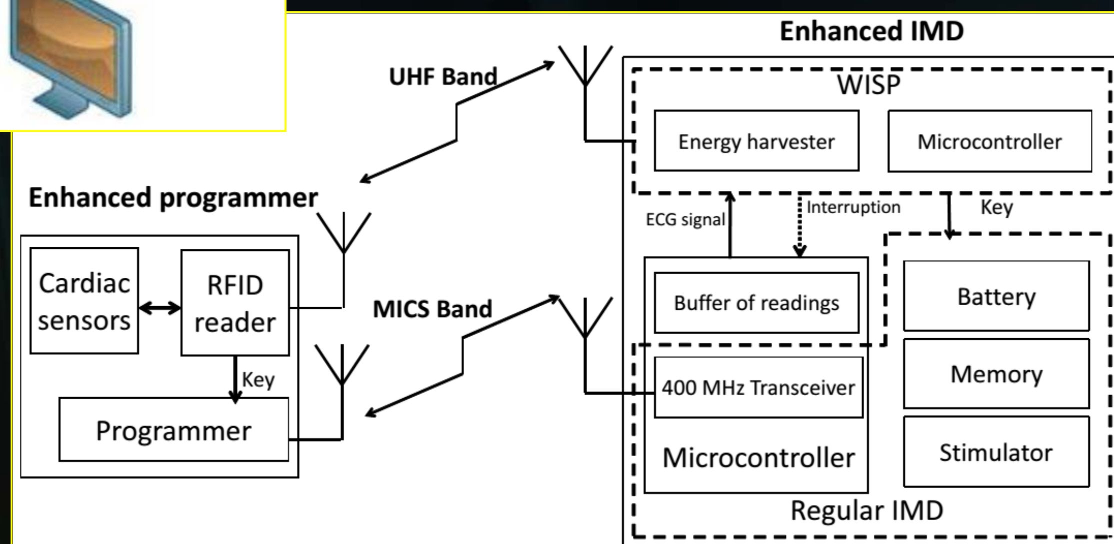
2. Time-out after X (unsuccessful) attempts
   – Not suggested for BDoS, but similar to SSH timeouts
   – Downside: can block legitimate reader

3. Guardians
   – Not really suggested for BDoS

(RF) Energy harvesting



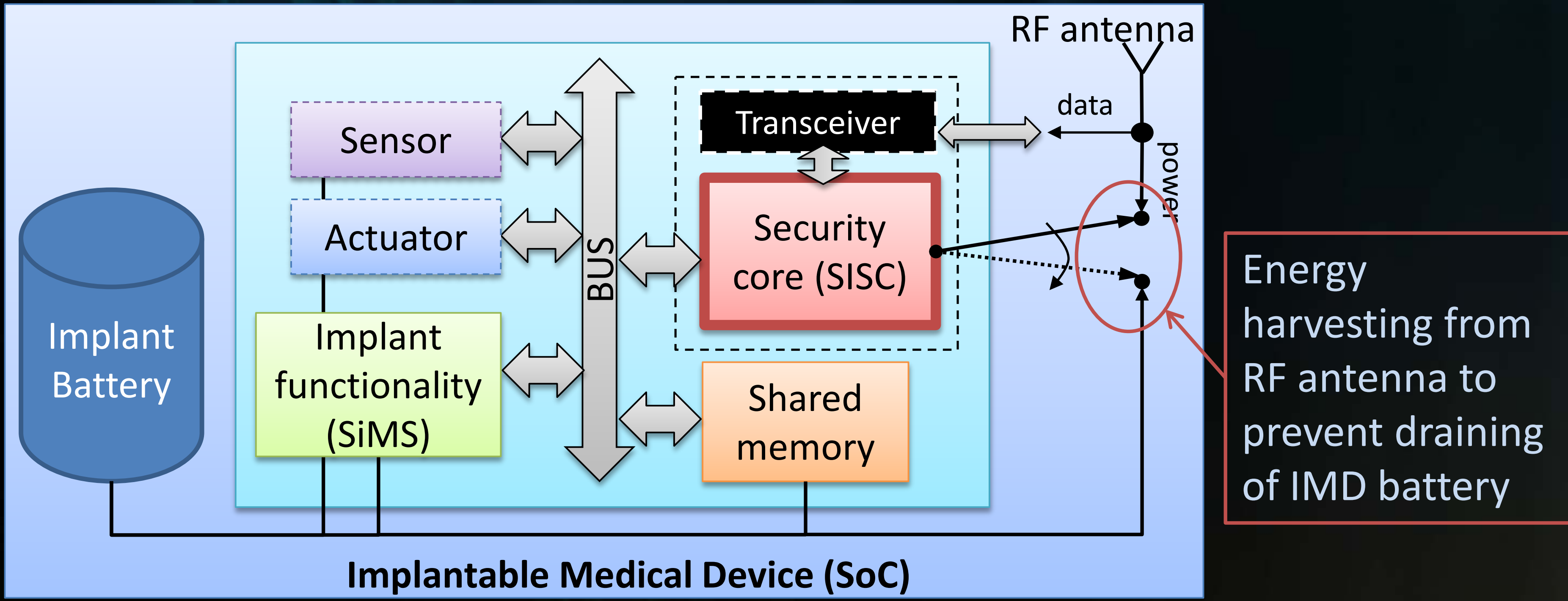
Daniluk, Krzysztof, and Ewa Niewiadomska-Szynkiewicz. "Energy-efficient security in Implantable Medical Devices." *FedCSIS*. 2012.



Ellouze, Nourhene, et al. "Securing implantable cardiac medical devices: use of radio frequency energy harvesting." *Proceedings of the 3rd international workshop on Trustworthy embedded devices*. ACM, 2013.

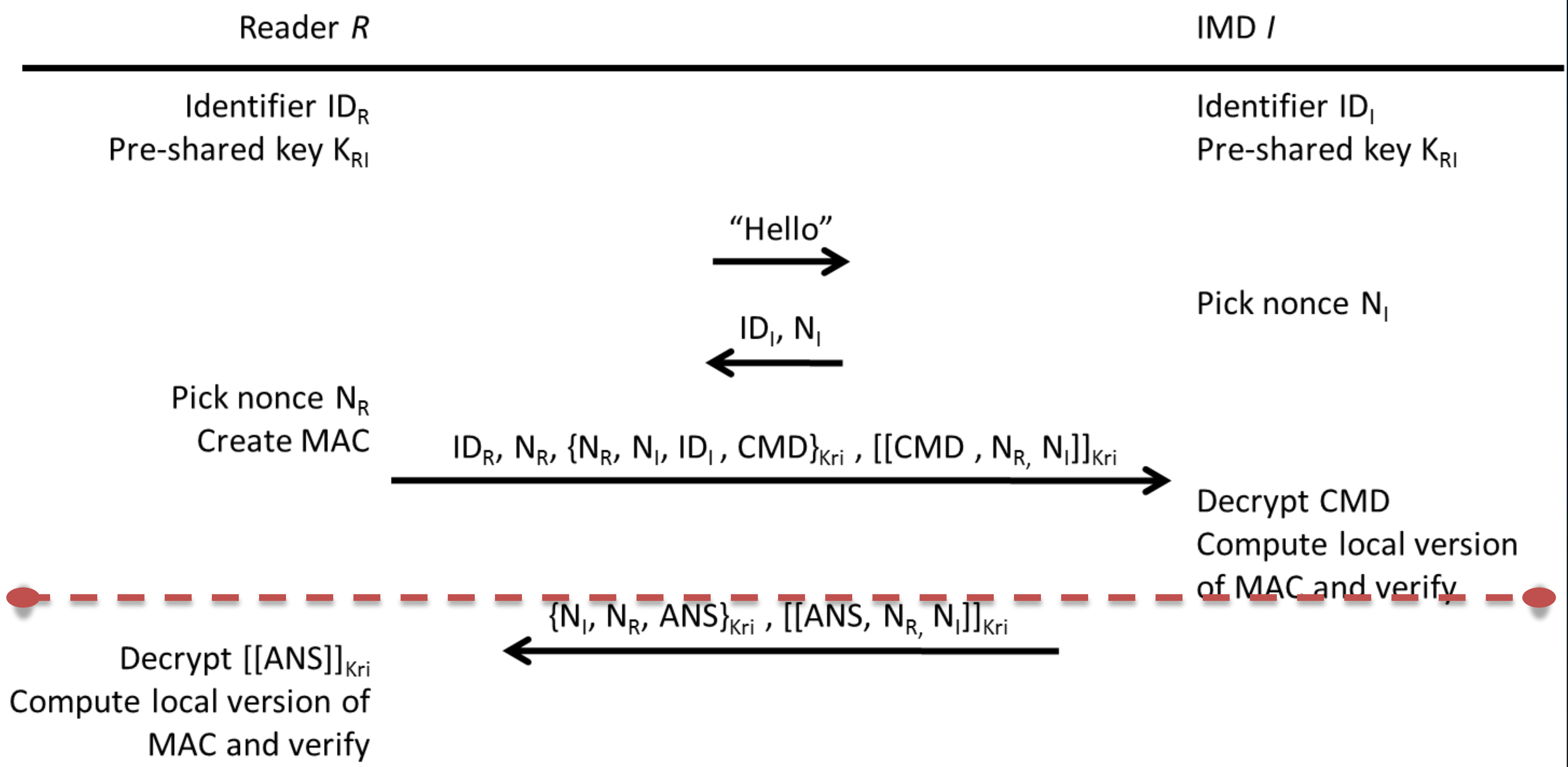
Secure IMD architecture

- Security functions through dedicated security CPU (SISC)
  - **Function decoupling:** DoS attacks do not affect implant functionality
  - **Power decoupling:** Zero-energy defense through energy harvesting (IMD battery not taxed prior to correct authentication)



C. Strydis et al., "A System Architecture, Processor and Communication Protocol for Secure Implants", ACM TACO, 2013

Security protocol (mutual authentication)



$\{x\}_y$: MAC of x (signed with y)
$[[x]]_y$: Encryption of x (with y)

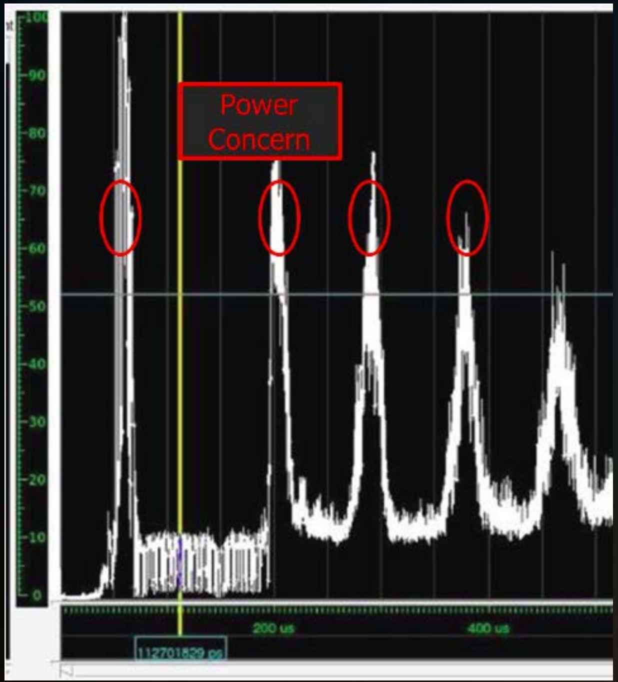
Symmetric ciphers for IMDs

average power consumption	peak power consumption	total energy cost	encryption efficiency	encryption rate	program-code size
IDEA	IDEA	RC6	RC6	RC6	XXTEA
LOKI91	MISTY1	RC5	IDEA	RC5	3WAY
SKIPJACK	LOKI91	IDEA	RC5	MISTY1	LOKI91
MISTY1	TWOFISH	MISTY1	MISTY1	RIJNDAEL	RC6
RIJNDAEL	RIJNDAEL	BLOWFISH	RIJNDAEL	BLOWFISH	RC5

C. Strydis, G.N. Gaydadjiev, "Profiling of Symmetric-Encryption Algorithms for a Novel Biomedical-Implant Architecture", IEEE Computing Frontiers 2008

- Winner: MISTY1
- Alternative: RC6 (ultra fast)

- More recently: PRESENT-80



Emergency-mode solutions

What you know / have?


Medical Alert Bracelet


(UV) Tattoo of Password


Centralized Database

Smart Card


Template-Based Biometrics

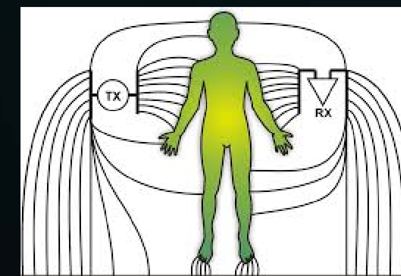
Who am I?


Criticality-Aware IMD

Why am I letting you in?

Where you are?

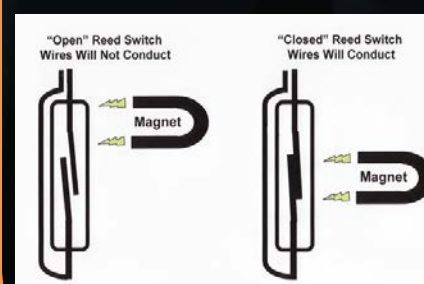

Distance Bounding



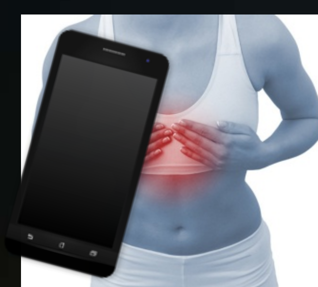
Body-Coupled Channel


Wearable Cloaker/Jammer


Ultrasound Channel



Magnetic Switch


Vibration-Based Channel

Qualitative comparison

	1	2	1	2	3	2, 3		
	Requires patient to wear something	Requires modification to the patient's body	Requires patient maintenance	Visible on the patient	Depends on centralized infra-structure	Automated decision making	Requires specialized equipment	Requires proximity to the patient
Bracelet								
Tattoo								
Database								
Smart Card								
Guardians								
Criticality awareness								
Magnetic switch								
Distance bounding								
Ultrasound ch.								
Body-coupled ch.								
Vibration ch.								
Biometrics								

Adapted from: T. Denning et al., "CPS: beyond usability: applying value sensitive design based methods to investigate domain characteristics for security for ICDs." *ACM SAC 2014*.

Our criteria for acceptable IMD solutions:

1. Cannot depend on patient (active) interaction
2. Must be acceptable by patients (see next slide)
3. Must be available and easy to use during emergencies

What do patients think

Providers N=24	Participant Percentage			
	Like	Dislike	Rec.	Rec. Against
A. Medical Alert Bracelet w/ Password	29	46	21	33
B. Centralized Database	38	21	25	25
C. UV-Visible Tattoo of a Password	17	54	13	50
D. Fail-Open/Safety Wristband	58	17	46	13
E. Proximity-Based Equipment	38	25	38	21
F. Criticality-Aware Fail-Open IMD	38	42	33	38

Table 3. Percentage of participants by security system concept who liked, disliked, recommended, or recommended against each system concept. Green indicates high satisfaction with a system concept; red indicates low satisfaction.

Afraid cannot be saved

Slow; single fail point

Stigmatization

Cloakers preferred vs bracelets

Afraid to not always work

T. Denning et al., "CPS: beyond usability: applying value sensitive design based methods to investigate domain characteristics for security for implantable cardiac devices." *ACM SAC 2014*.

Static vs. Dynamic biometrics

1. Use of templates
   - Non-time-varying
   - During emergencies can vary too much

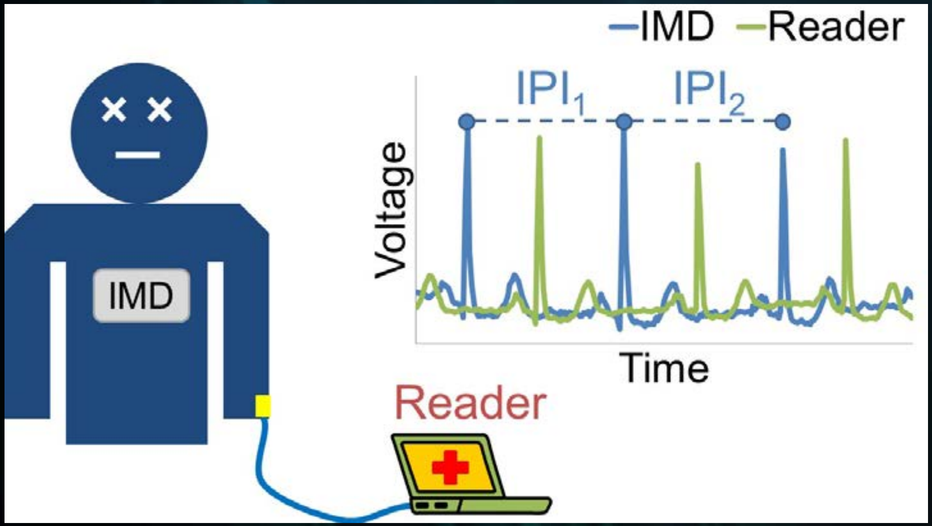
2. Energy overhead (excess operations)

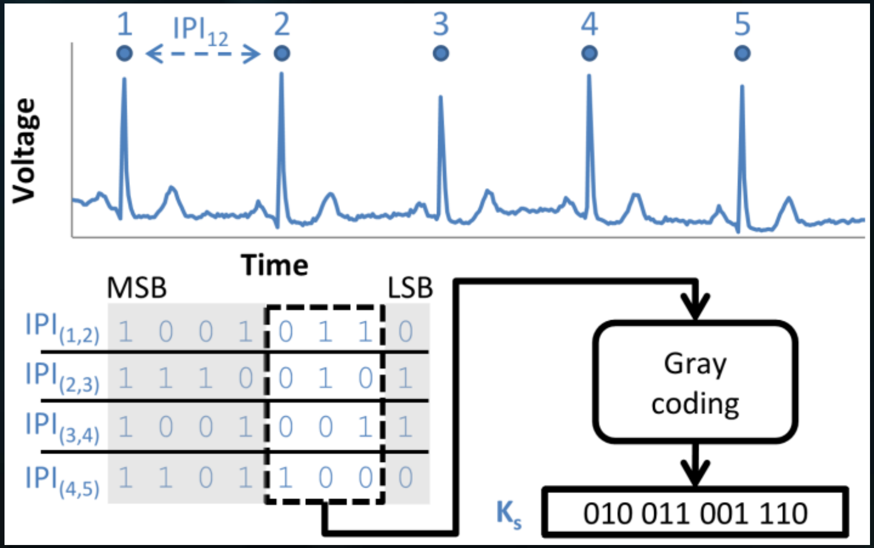
- **Dyn. Biometrics:** S. Cherukuri et al., "BioSec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body." IEEE Conf. on *Parallel Processing Workshops, 2003*
  - Blood glucose, pressure, temperature, hemoglobin count, blood flow

- **Heart beats:** C. Poon et al., "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health", IEEE Communications Magazine, 2006

Emergency mode using heart beats

IMD and Reader obtain heart beats for **touch-to-access** authentication





Why heartbeats?

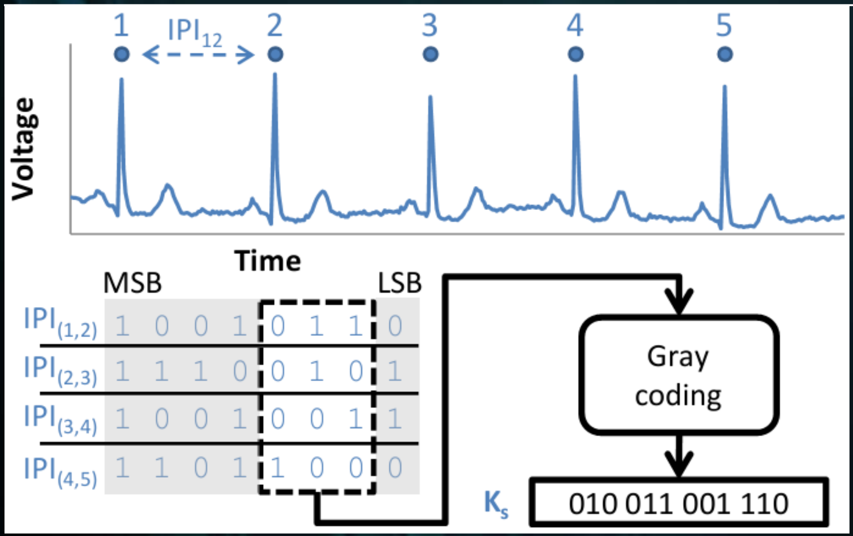
- Strong random-number generation
- Measurable throughout body
- Lightweight or "for free" for IMD

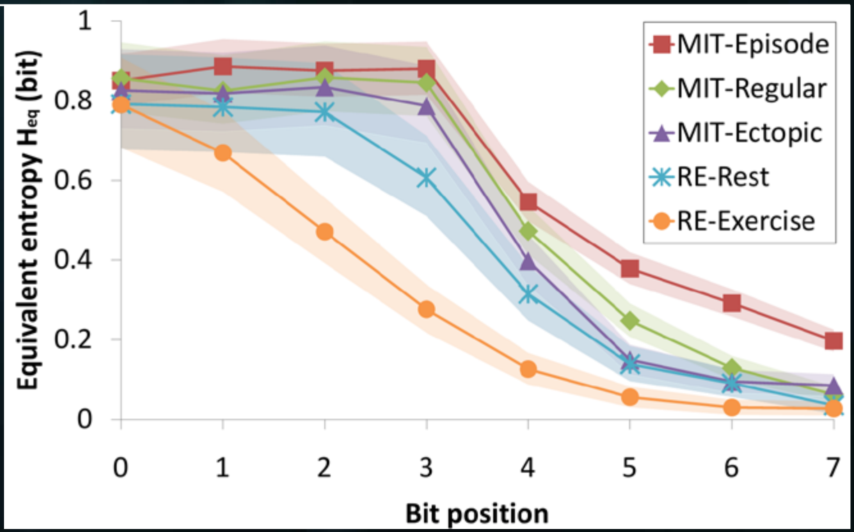
  → Fresh, entity-bound, random number

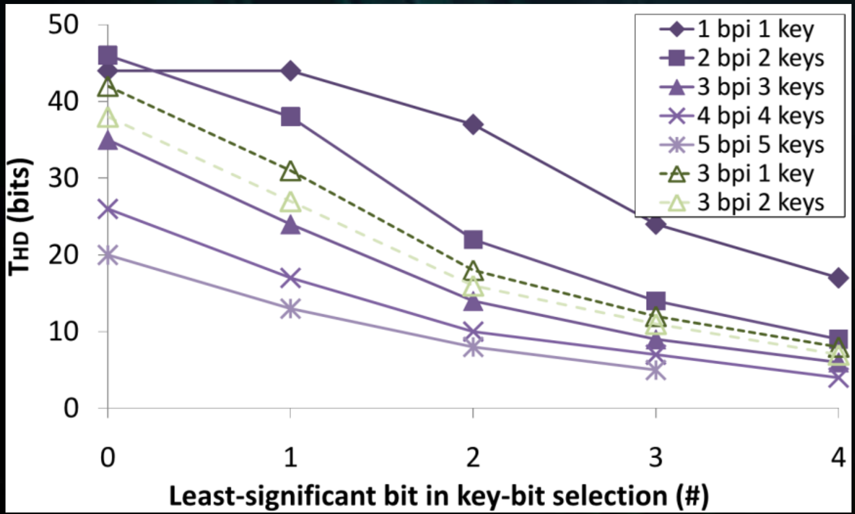
Risk of abuse depends on:

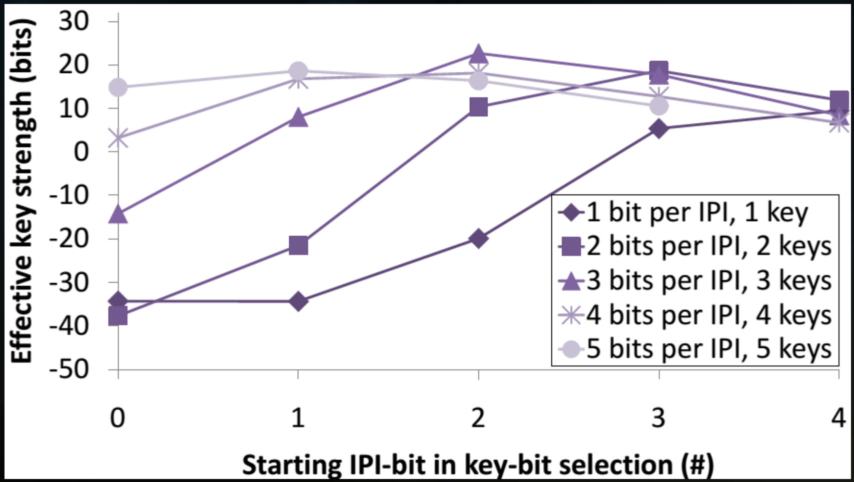
- Variable randomness per IPI
- Similarity between IPIs of R and I
- Remote-measuring capabilities

Basic security-key generator





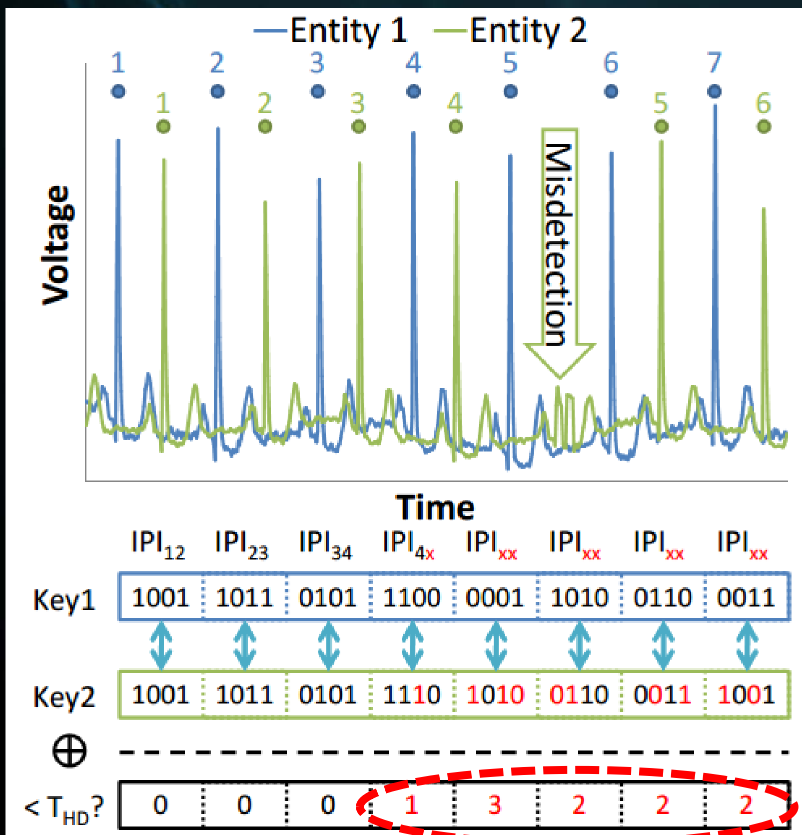


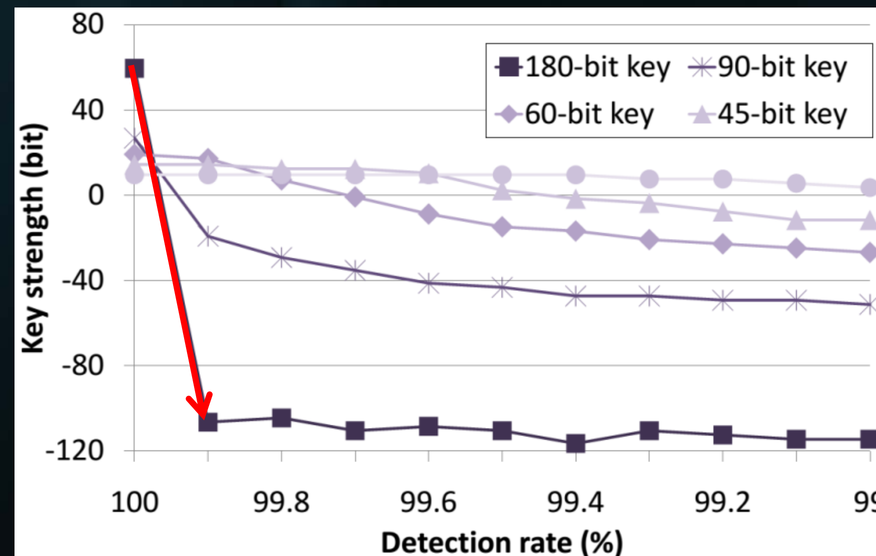


- Exercise has negative effect on randomness. MSBs: less random, but less prone to VAR_{IS}

- High disparity → Minimal effective key strength: 20 bits for 60-bit key (healthy subjects)

Heart-beat misdetection

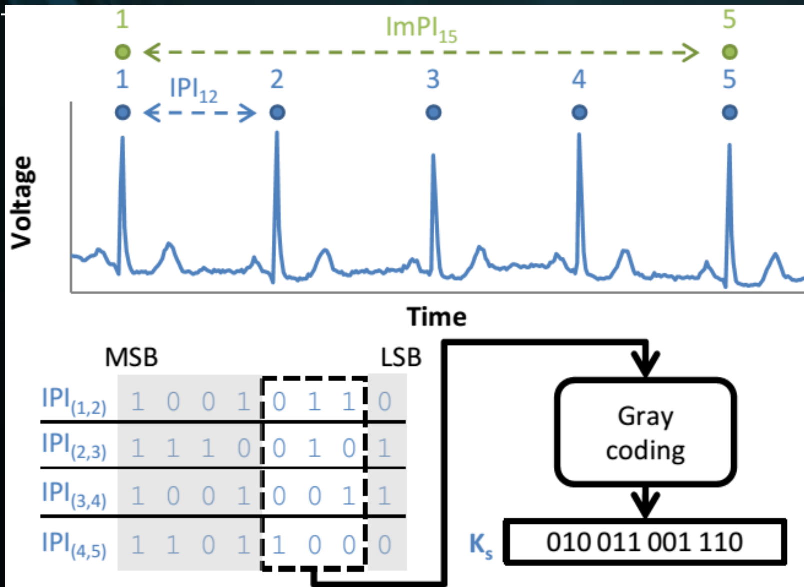


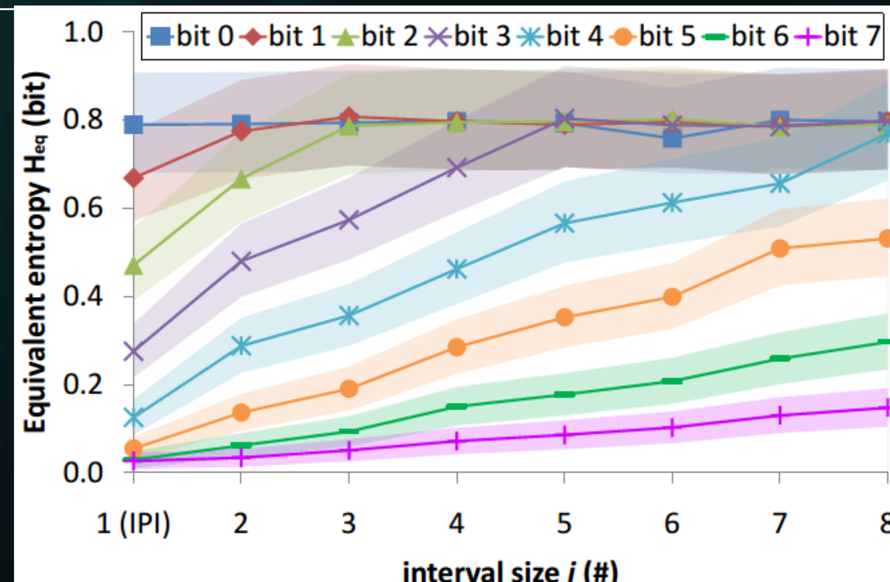


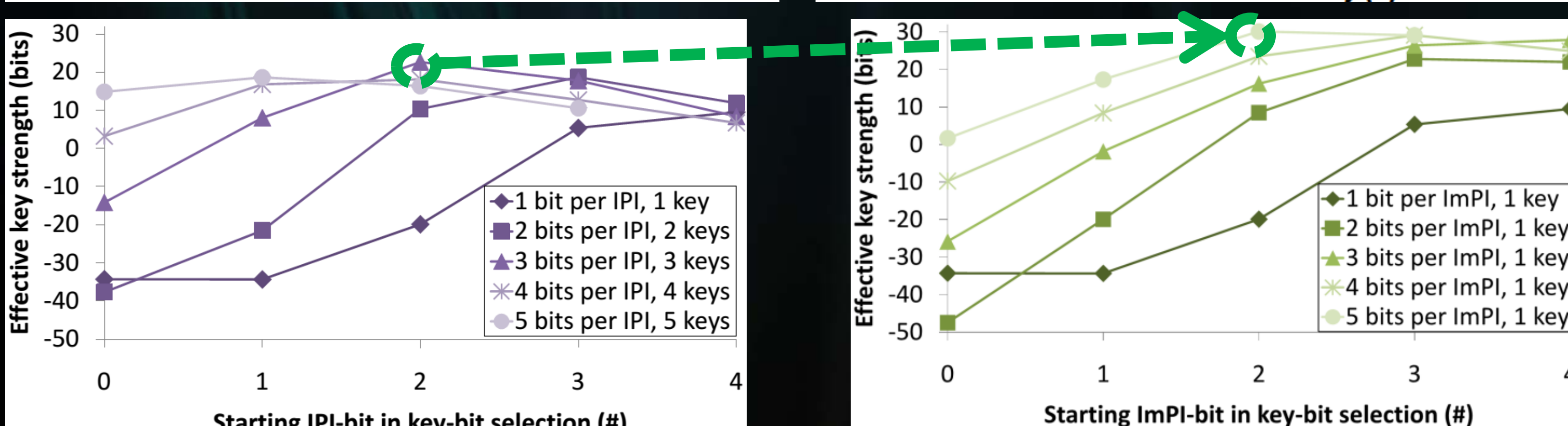
R.M. Seepers et al., "Peak misdetection in heart-beat-based security: Characterization and tolerance", IEEE EMBC 2014

Misdetection has a substantial effect on key strength due to key misalignment

Entropy extraction - ImPI





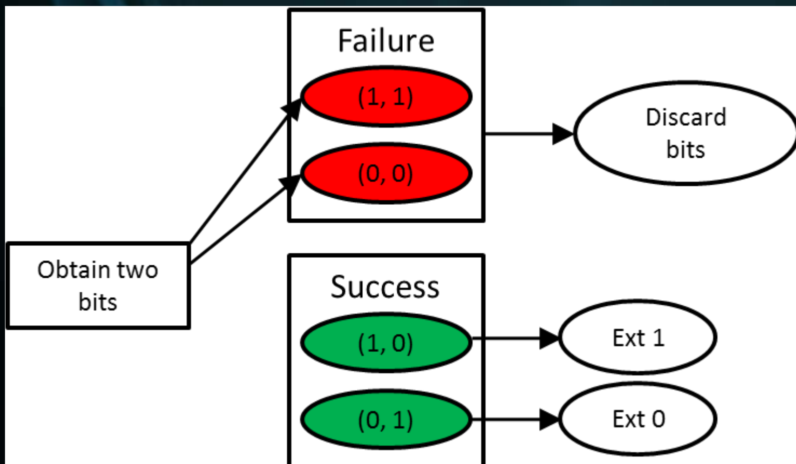


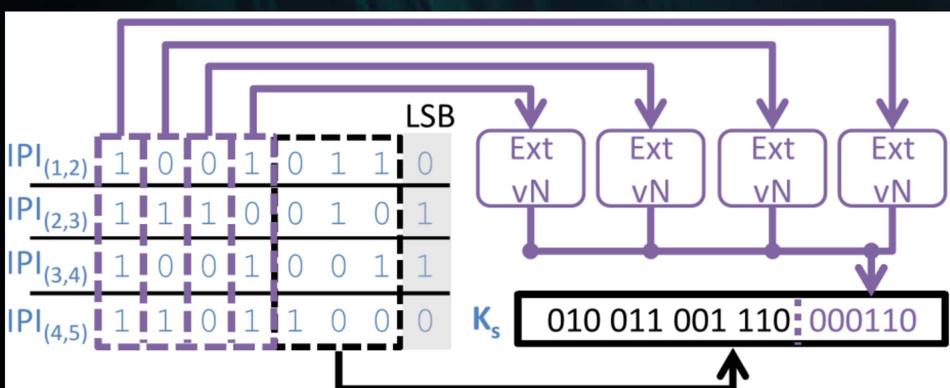
R.M. Seepers et al., "Enhancing Heart-Beat-Based Security for mHealth Applications", IEEE J-BHI 2015

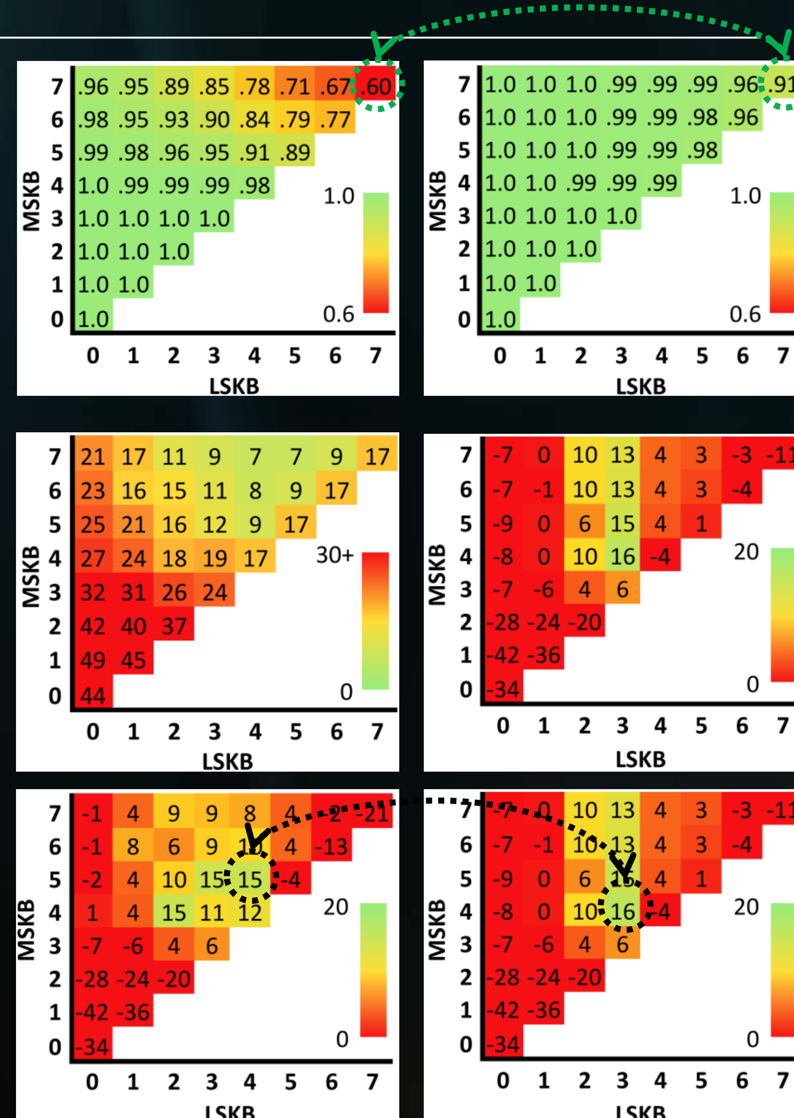
- Longer time between intervals → hi ImPI randomness

- Longer key-gen time, but stronger keys (trade-off)

Entropy extraction – von Neumann



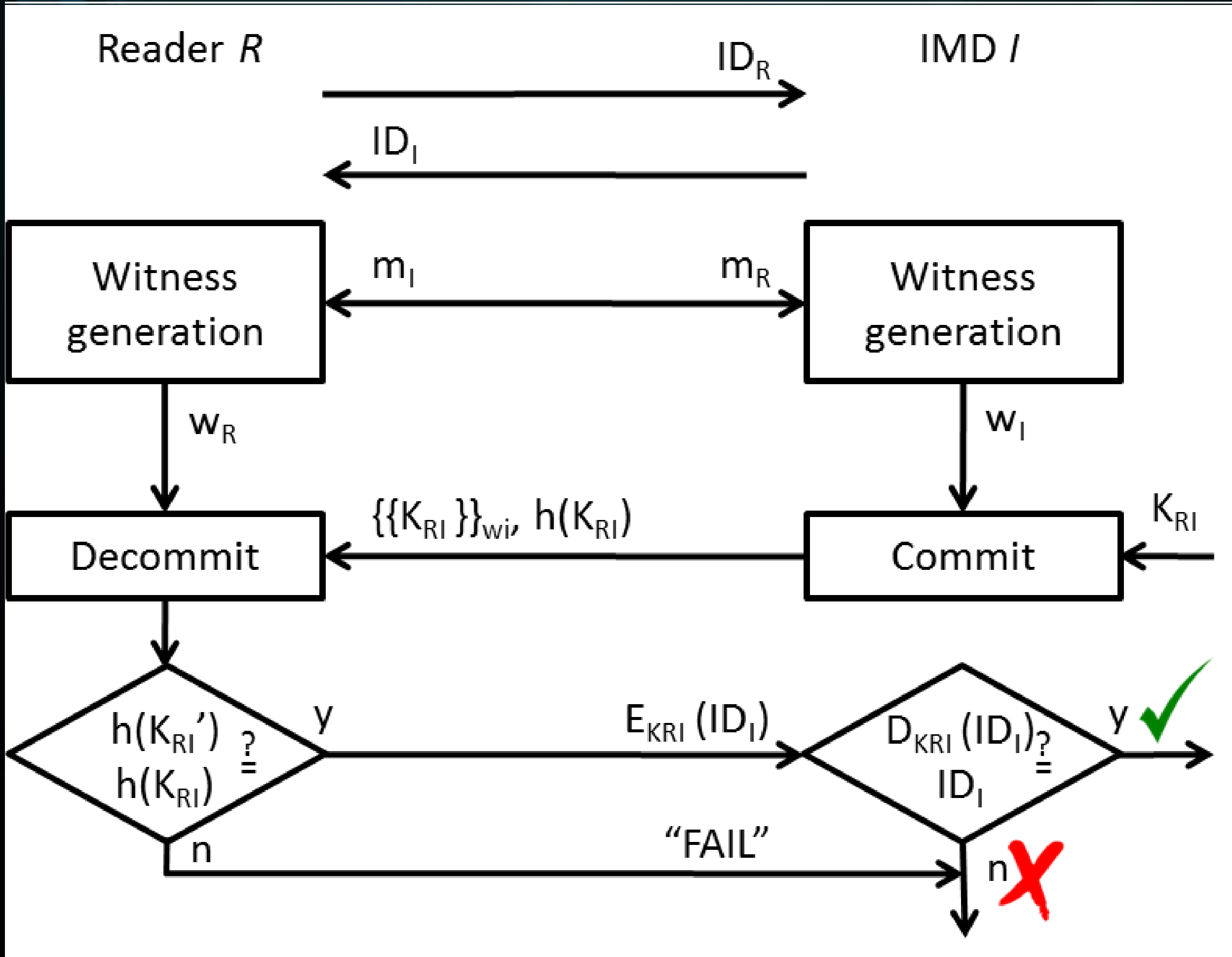




R.M. Seepers et al., "On Using a Von Neumann Extractor in Heart-Beat-Based Security", IEEE TrustCom 2015

vN extractor increases randomness substantially; also decreases key-disparity and key-gen time. The benefits of a conventional extraction are hampered by this increase in disparity.

Key-exchange protocol



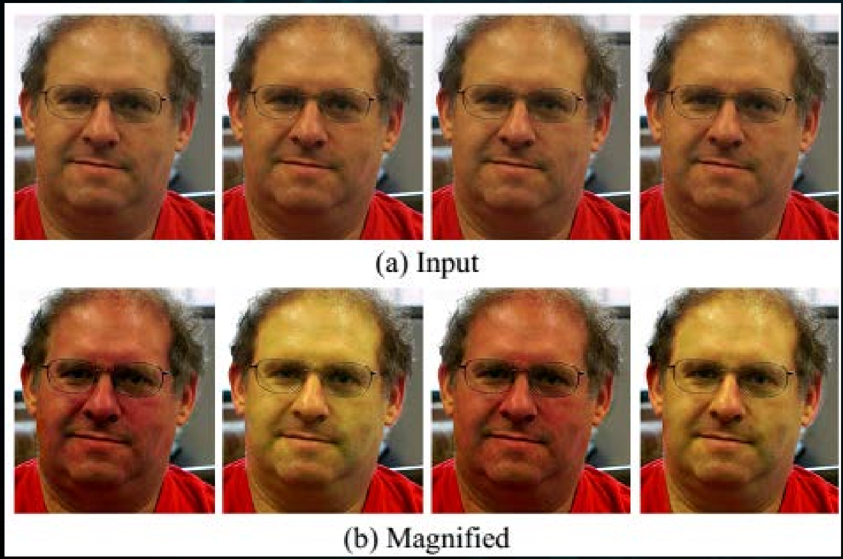
R.M. Seepers, "Secure Key-Exchange Protocol for Implants Using Heartbeats", IEEE Computing Frontiers 2016 (to appear)

Key-exchange protocol using fuzzy commitment. Misdetection is tolerated through eliminating misdetected IPIs (by both entities) prior to witness generation.

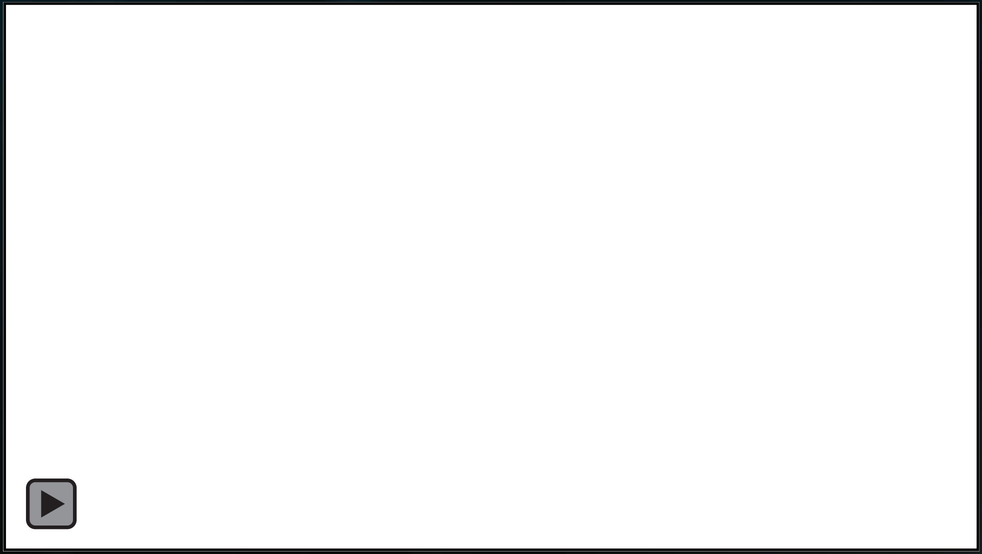
Remote measurements

- Extensive research being done on detecting (dynamic/static) biometrics remotely, e.g.:

Reflection pulse oximetry (RPO)



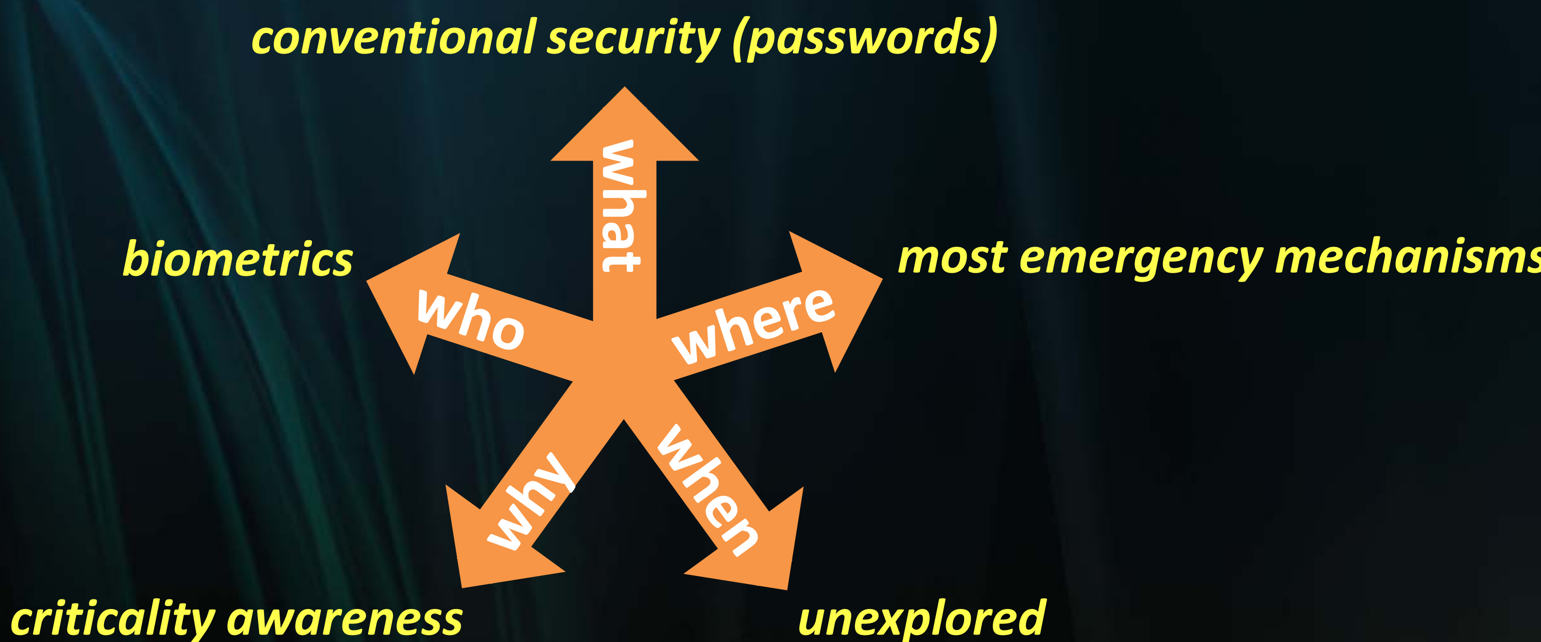
Ballistocardiogram (BCG)



- Evaluate security of biometrics in view of remote measurements

Future work: The five Ws

- **Currently, verify other party by answering one/two question(s):**



- *Solutions based on individual questions likely not satisfactory*

  → Expand / explore different combinations

medical delta we add

BRAIN INNOVATIONS

NEDERLANDS HERSENINSTITUUT
Master the mind

HiPEAC
COMPILATION ARCHITECTURE

National Technical University of Athens

CHALMERS

TU Delft Delft University of Technology
Challenge the future

"BE STILL BE STILL, MY BEATING PACEMAKER."

THANK YOU FOR LISTENING

www.erasmusbrainproject.com