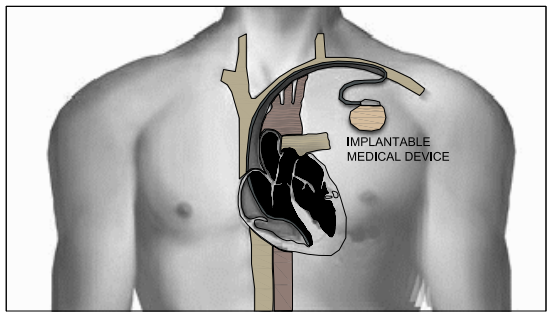
Swiss-knife Security Kit for Implantable Medical Devices



Pedro Peris-Lopez

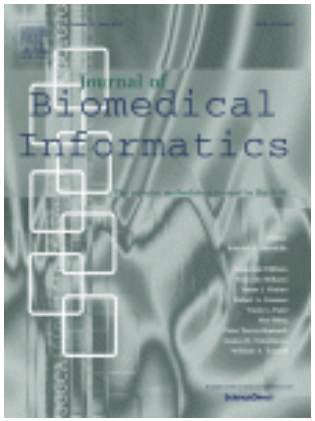
Madrid April, 2017

Outline

1. Security and Privacy issues in IMDs

2. Proposed Solutions

Security and Privacy issues in IMDs

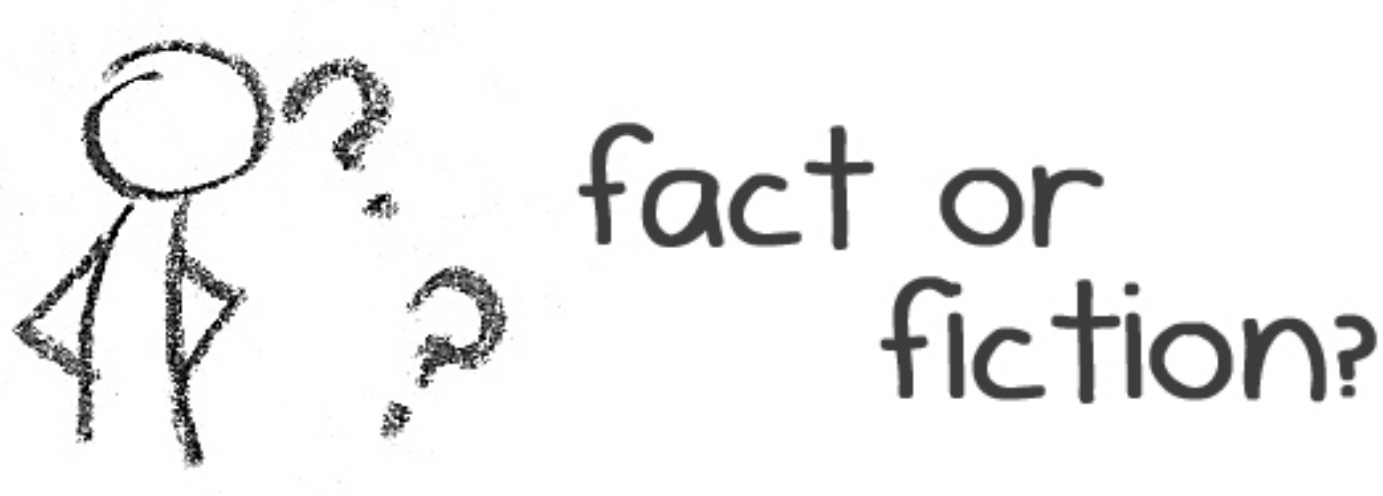


Security and privacy issues in implantable medical devices: A comprehensive survey. Carmen Camara, Pedro Peris-Lopez, Juan E. Tapiador. Journal of Biomedical Informatics, 55: 272–289 (2015).

Motivation

©Homeland (TV series)

Motivation

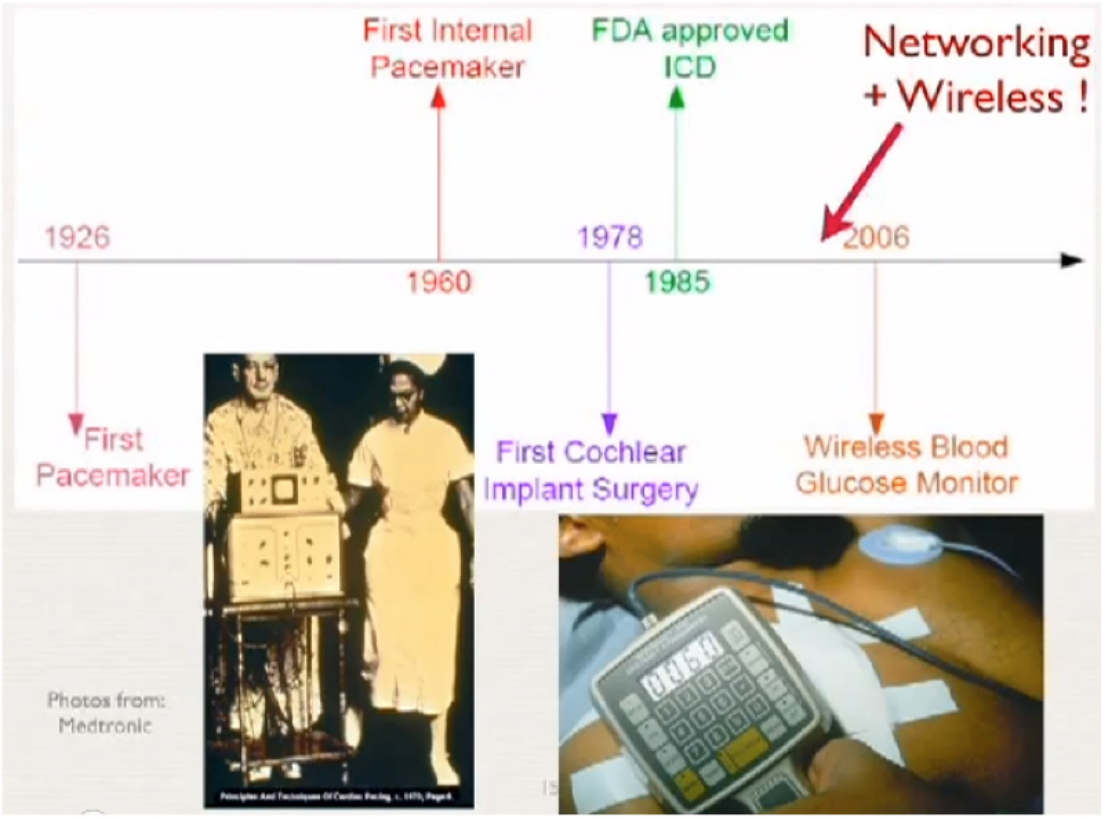


What is an IMD?

Definition

Implantable Medical Devices (IMDs) are electronic devices implanted within the body to treat a medical condition, monitor the state or improve the functioning of some body part, or just to provide the patient with a capability that he did not possess before [HH10].

Chronology


First Internal Pacemaker
FDA approved ICD
Networking + Wireless !
1926
1960
1978
1985
2006
First Pacemaker
First Cochlear Implant Surgery
Wireless Blood Glucose Monitor
Photos from: Medtronic

Some examples...

Neurostimulador

Pacemaker

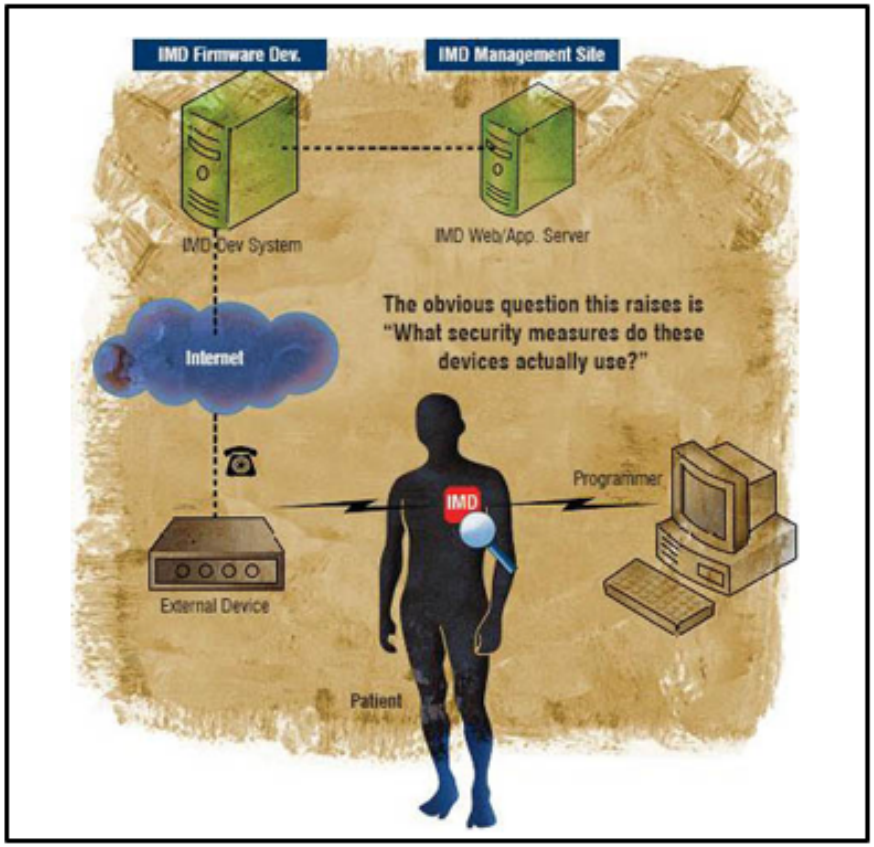
Insulin Pump

Access Modes

Past

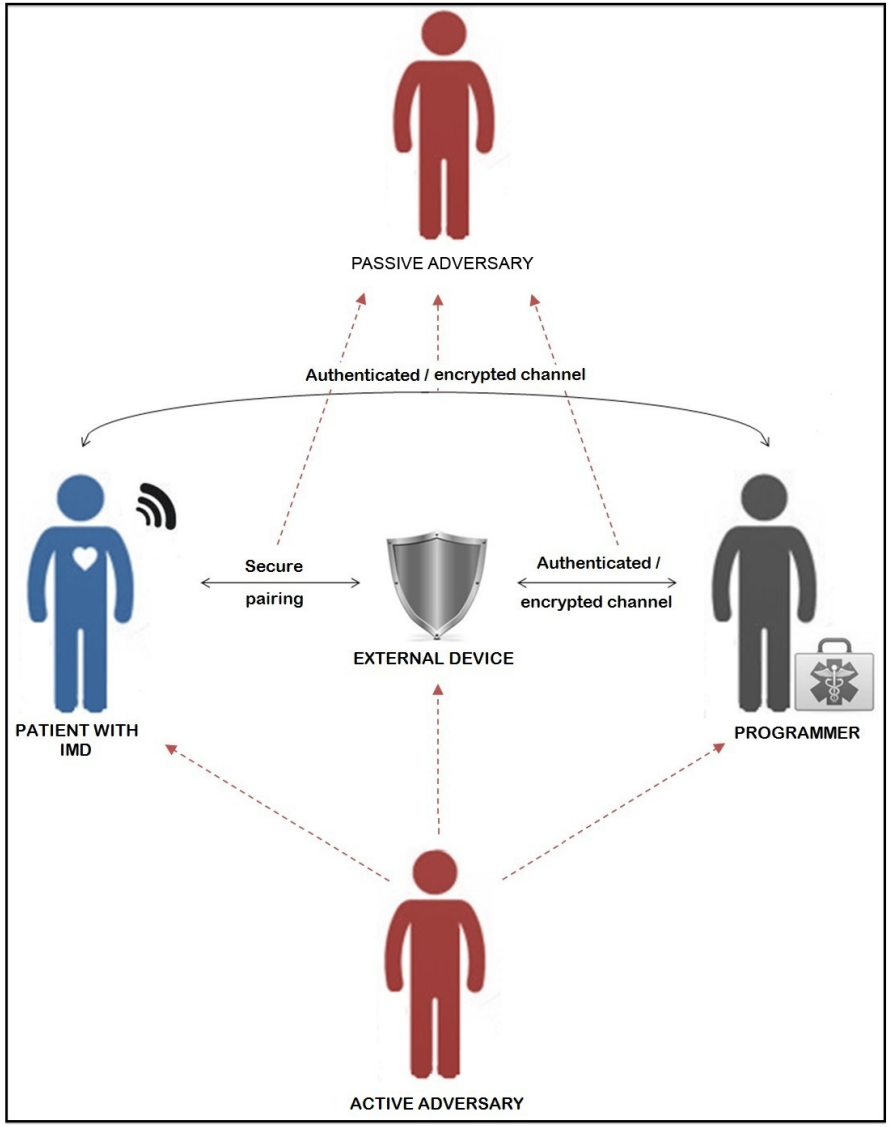
Local Programming

New generations



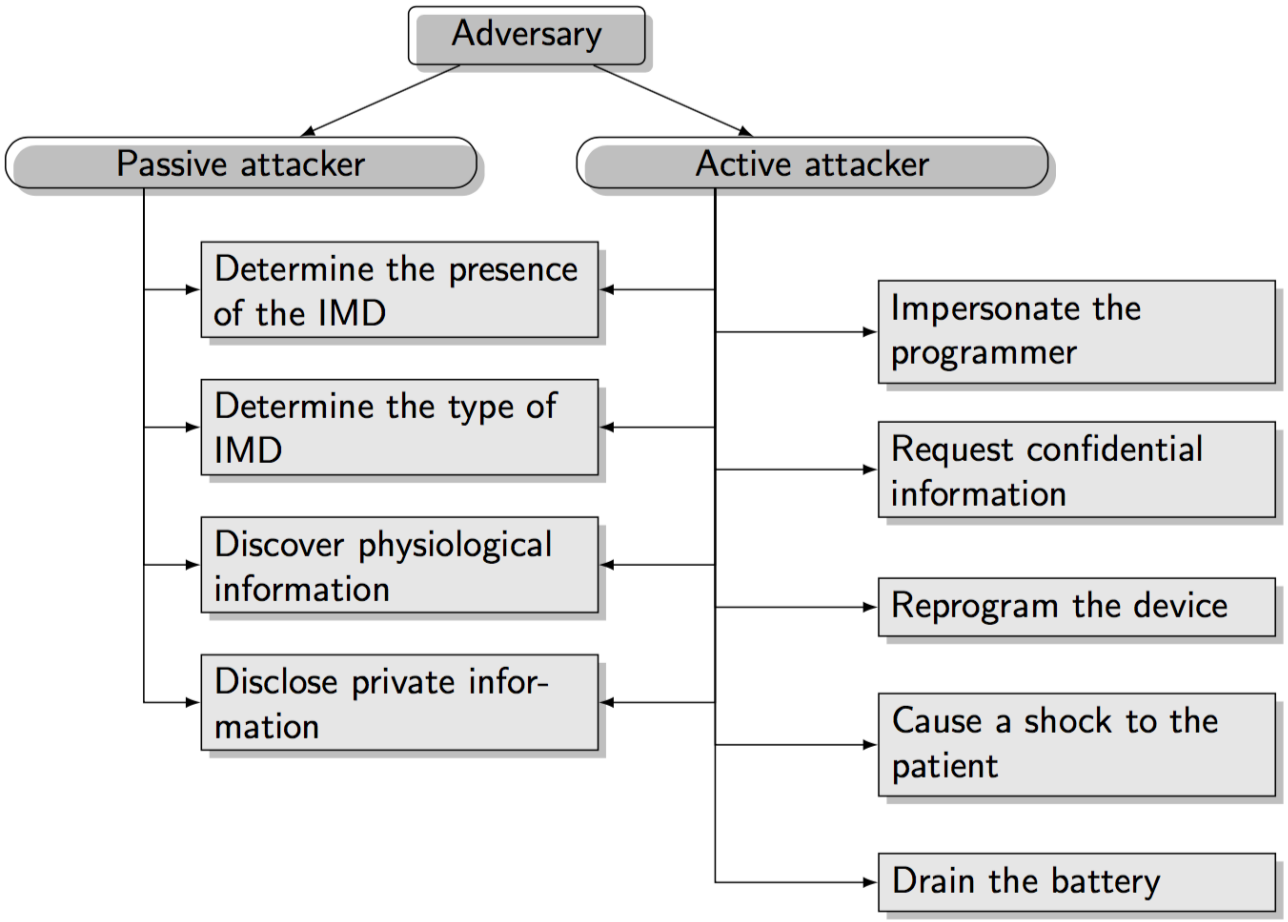
Remote Programming & Monitoring

Usage Scenario

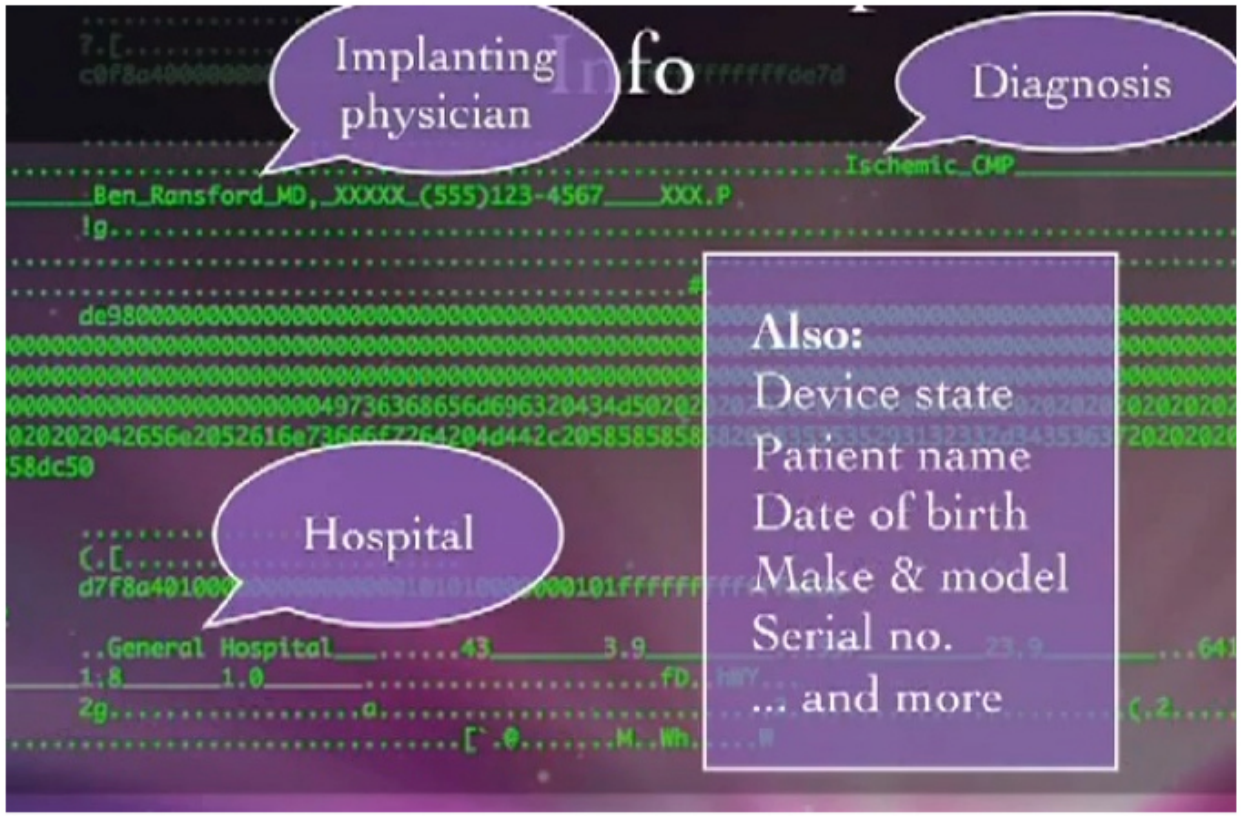


Security Analysis

Are the security threats against IMDs a real concern? Yes

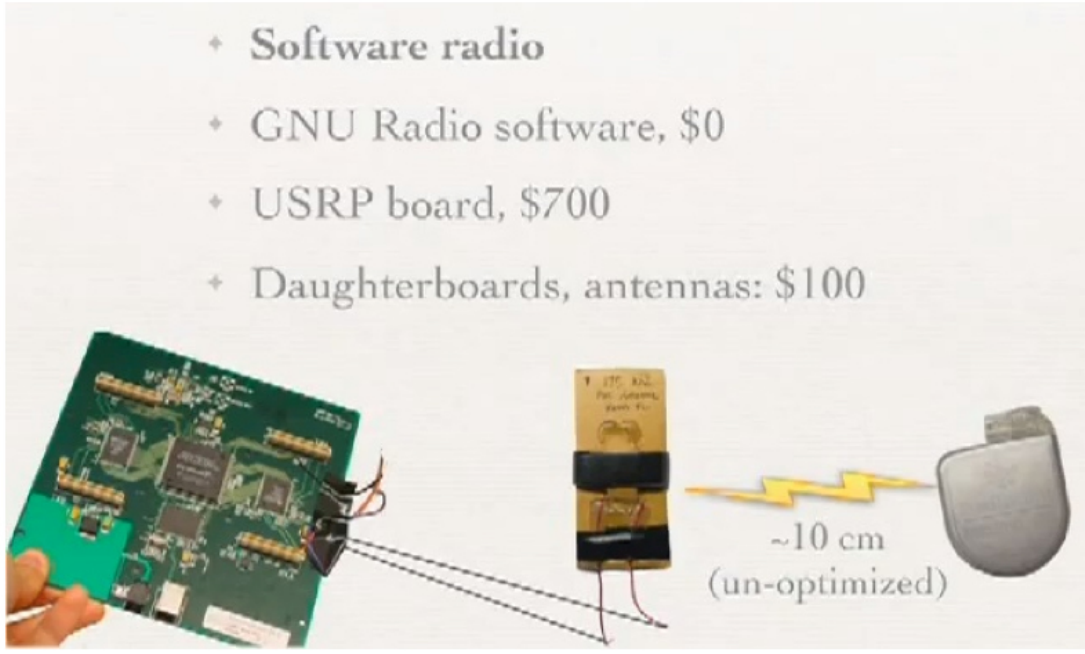


Example 1. Disclosure of private information



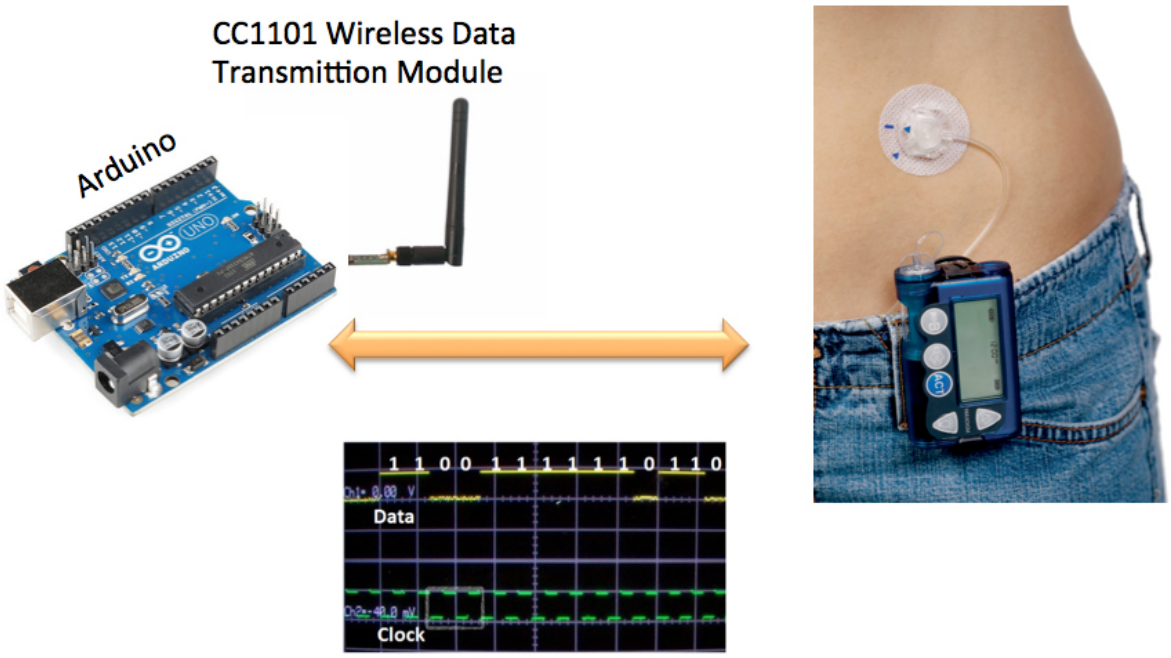
Note: “Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses” (Halperin et al., 2008).

Example 2. Reprogram the device (I)



Note: “Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses” (Halperin et al. 2008).

Example 2. Reprogram the device (II)



Note: “Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System” (J. Radcliffe, 2011).

Example 3. Drain the battery

Are you awake?
Are you awake?
Are you awake?

Note: “Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses” (Halperin et al., 2008).

Tensions and trade-offs

IMD Security	vs	Patient Safety
IMD Capabilities	vs	Battery Lifetime

Security Solutions

Are the existing cryptographic solutions good for securing IMDs? NO

Operation Modes

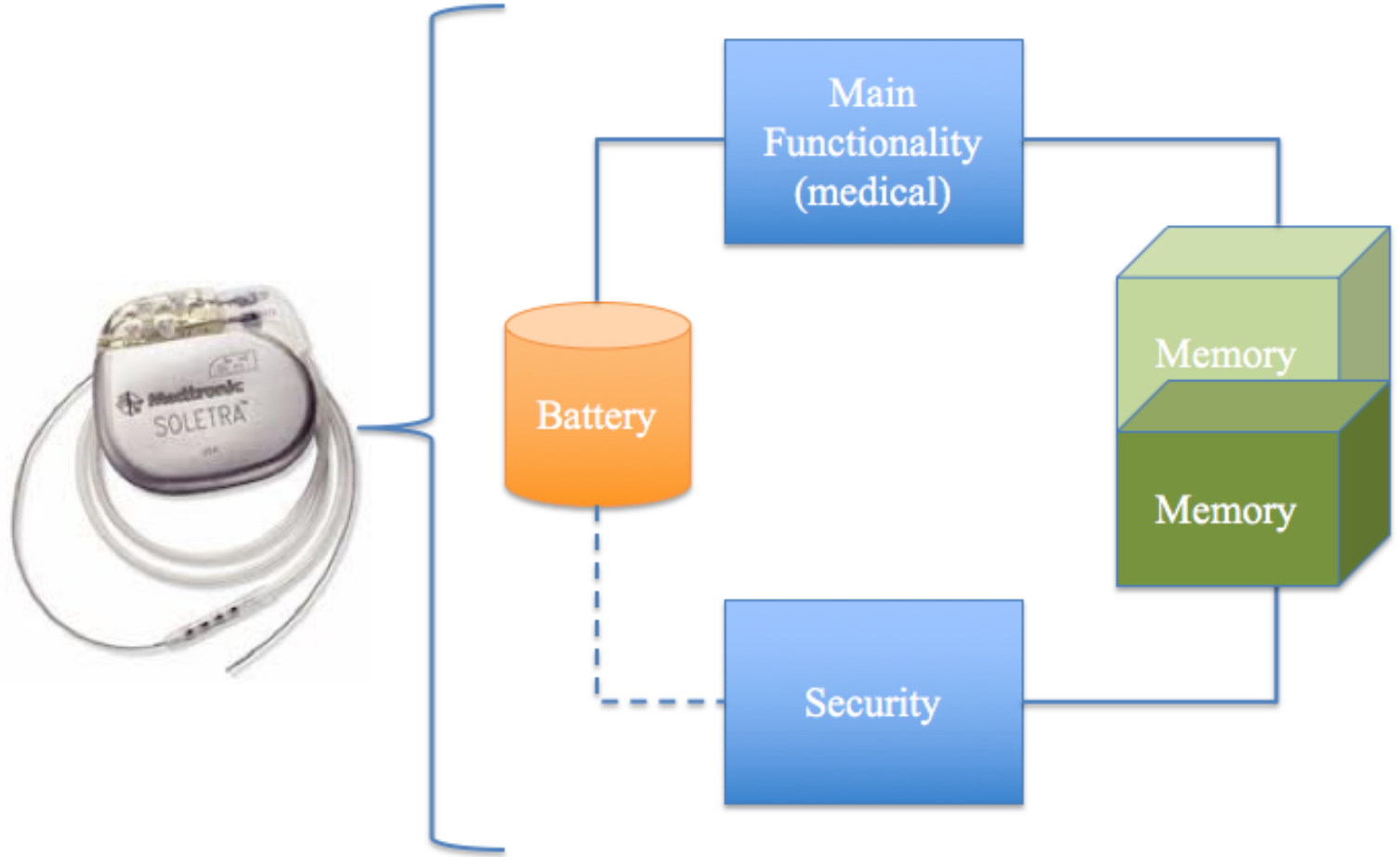
- Normal Mode

- Emergency Mode

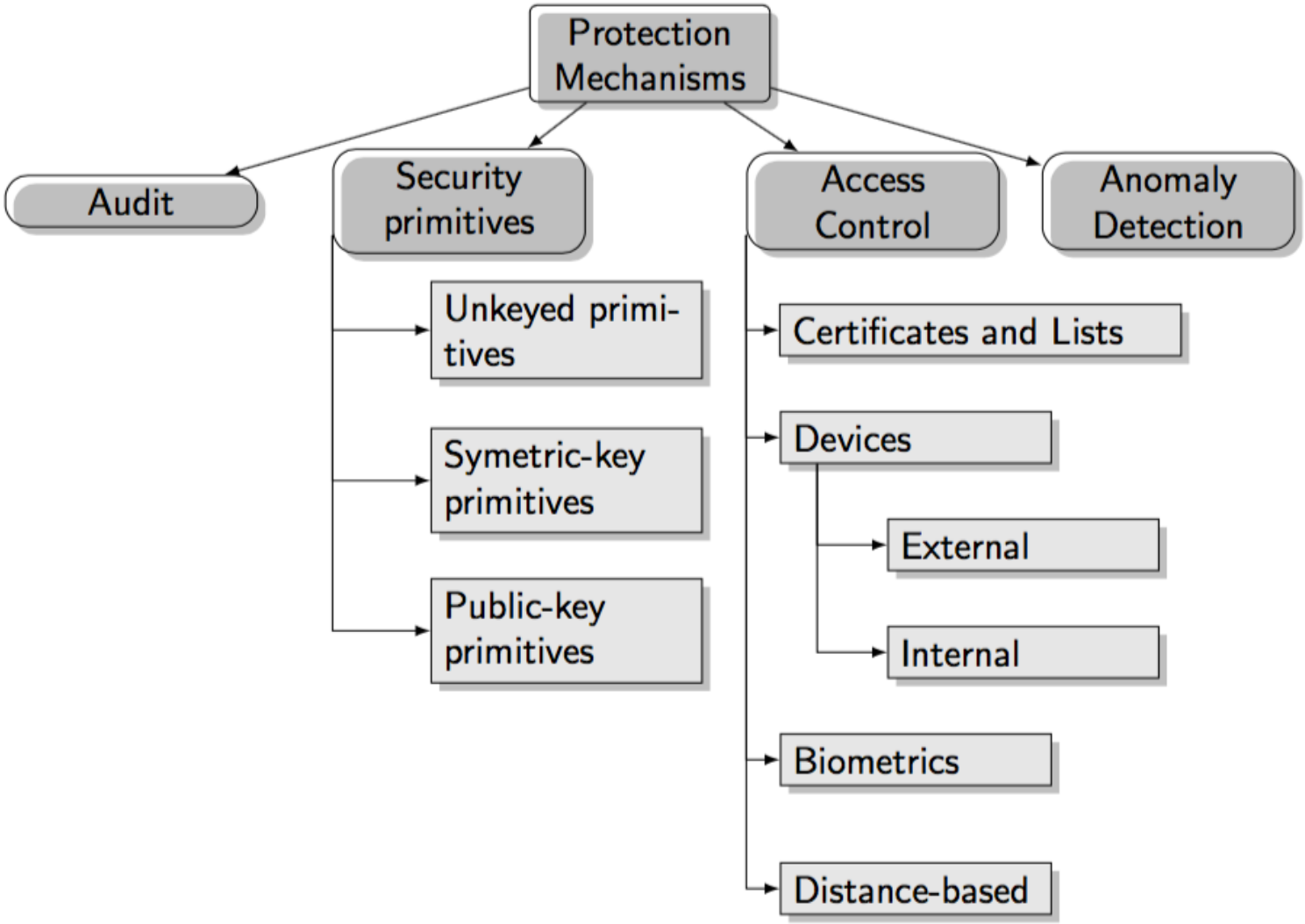
Limitations

- Limited Energy
  - 9 years (neurostimulators) / up to 10 years (pacemakers)
  - Battery replacement: it may require surgery
- Limited Storage
  - Events and episodes
  - E.g., Reveal DX 9528: 22.5 minutes of ECG signal
- Limited computing and communication capabilities
  - Communication is the most energetically expensive task for the IMD
  - Computations: tiny microcontroller

General Architecture



Protection Mechanisms

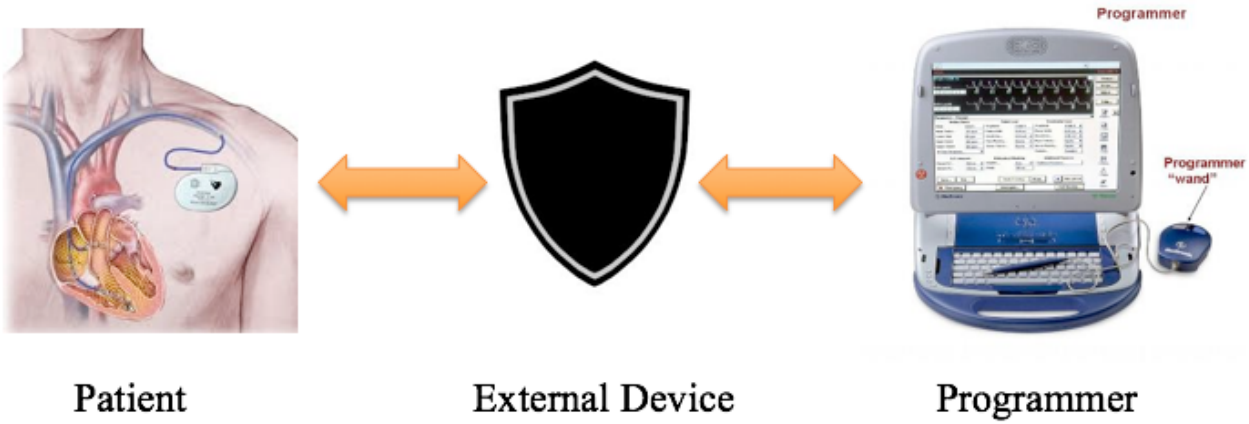


Protection Mechanisms (I)

- No security
  - ✓ Old generations without wireless connectivity
  - × New generation of IMDs
- Auditing
  - Register all accesses (authorized or not)
  - Detection (No protection / Deterrence)
  - E.g., RFID Guardian (Rieback et al., 2005)

Protection Mechanisms (II)

- External Devices
  - Not implanted in the patient's body
  - Assume part or all security functions
  - Security capabilities: auditing, key management and access control



Protection Mechanisms (III)

- Physical solutions
  - Magnetic switch
  - Subcutaneous button

Protection Mechanisms (IV)

- Authentication Protocols

Verifier (secret k) **Prover** (secret k)

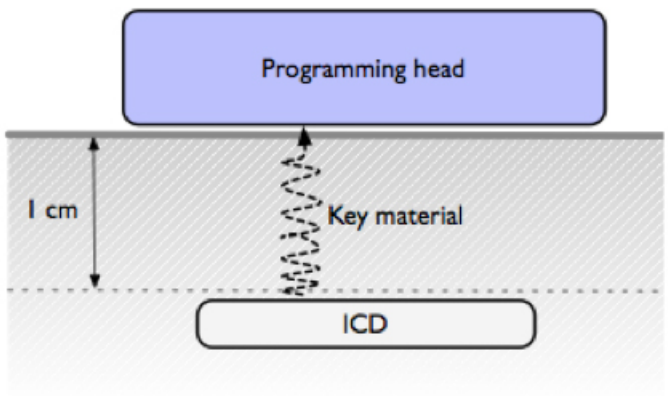
Pick N_a $\xrightarrow{N_a}$

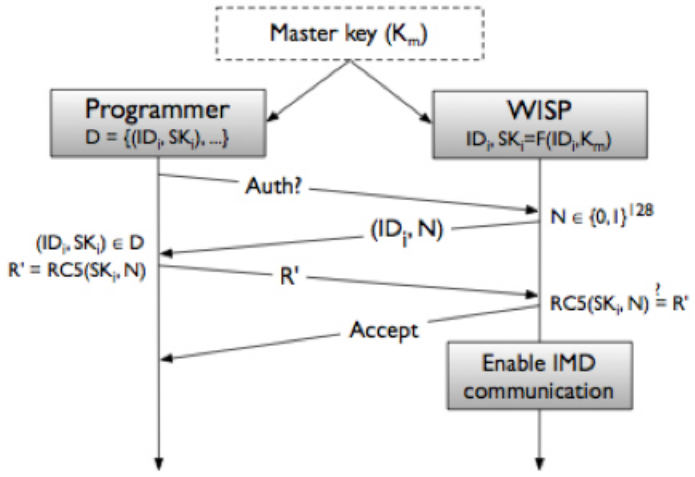
$\xleftarrow{E_k(N_a, N_b)}$ Pick N_b

Problema de distribución de claves

Protection Mechanisms (V)

- Non conventional channels
  - Acoustic waves

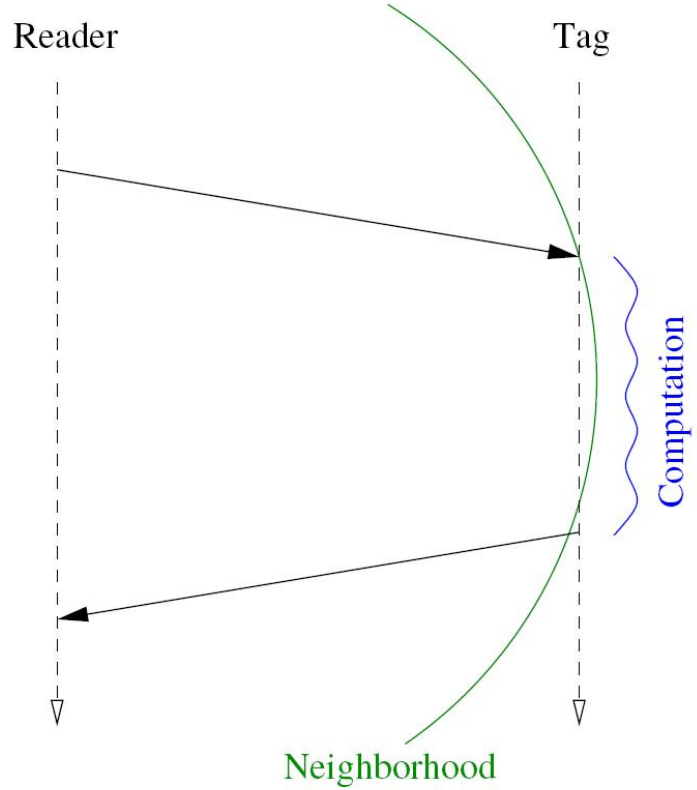




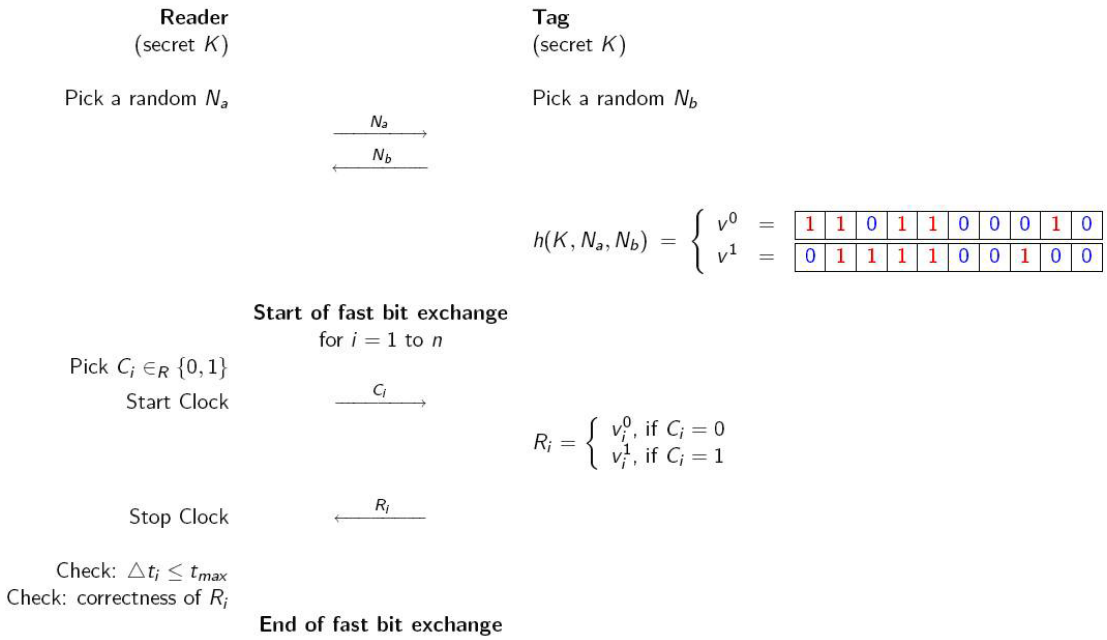
Note: “Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses” (Halperin et al. 2008).

Protection Mechanisms (VI)

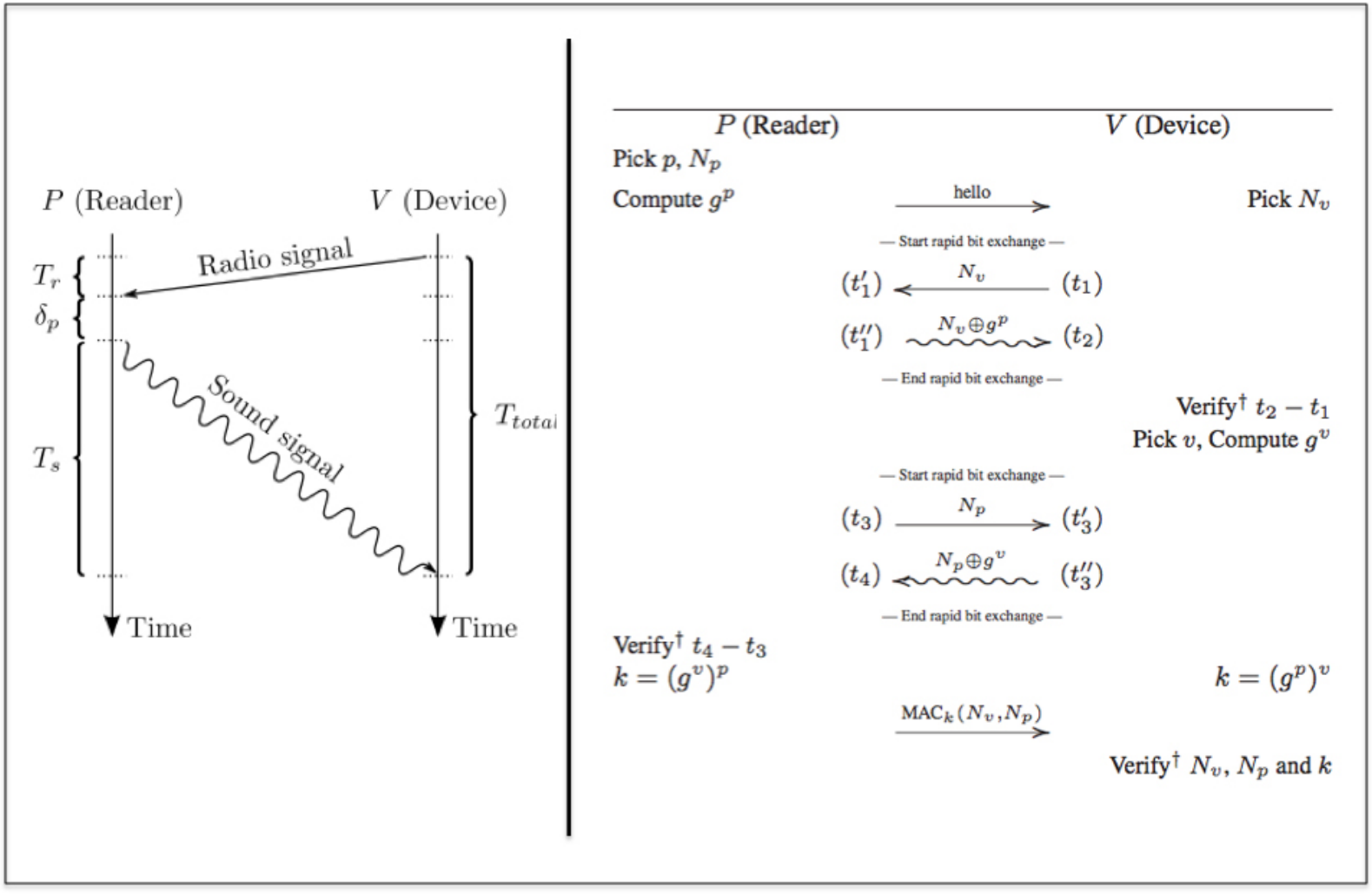
- Distance Bounding
  - Upper bound distance between two entities
  - Based on speed light – nothing propagates faster
  - First proposal: Beth and Desmedt [Crypto90]



Hancke and Kuhn's Protocol



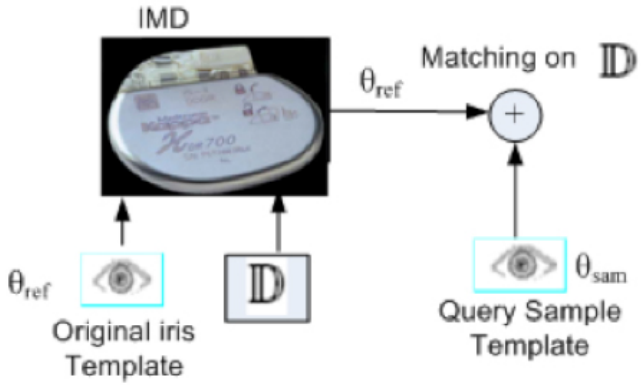
Proximity-based Access Control for IMDs



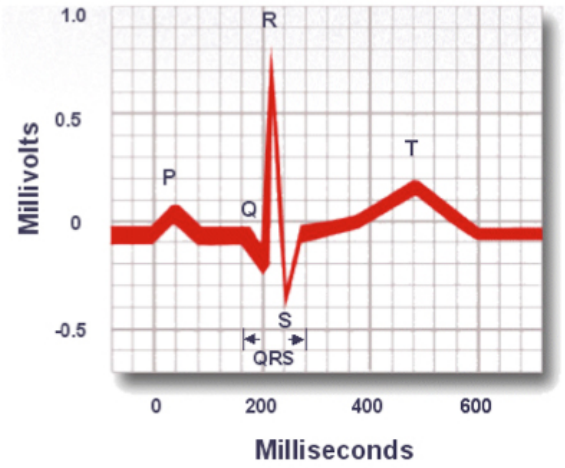
© [RCHBC09]

Protection Mechanisms (VII)

- Biometric Measures
  - Biometric-based two-level secure access control for implantable medical devices during emergencies. (Hei and Du, 2011)

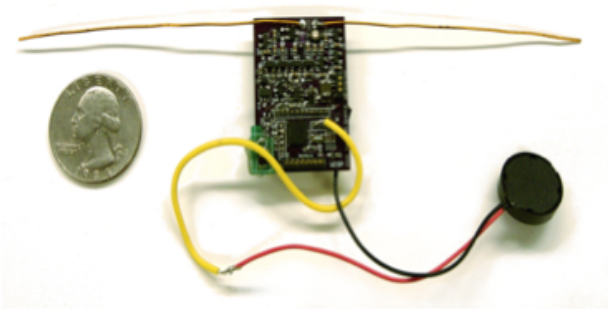


  - IMDGuard: Securing Implantable Medical Devices with the External Wearable Guardian (Xu et al., 2011)



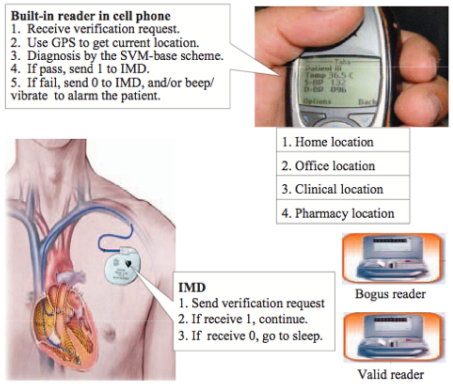
Protection Mechanisms (VIII)

- Measures against Resource Depletion Attacks
  - Notification measures
    - Alarm signal (sound or vibration)
    - Informative (attacks are not prevented)



Zero Power Defenses

  - Pattern based solutions
    - External device (e.g.,. smartphone)
    - Machine Learning (e.g., SVM)
    - Patterns: frequency, location, patients conditions

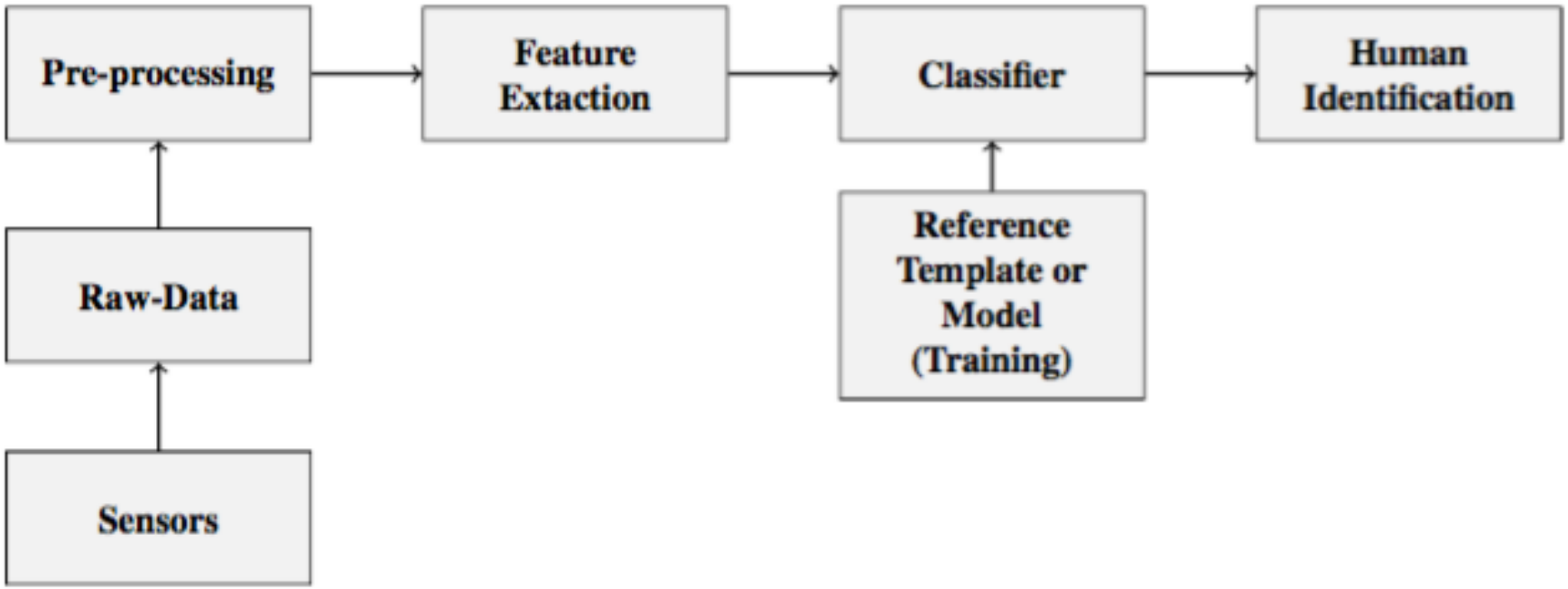


Hei and Du, INFOCOM 2011

2. Proposed Solutions

- Human Identification: ECG-based solution
- Multi-modal Human Identification: ECG, GSR and Airflow
- Extracting randomness from ECG signals
  - Key generation
  - Random number generator

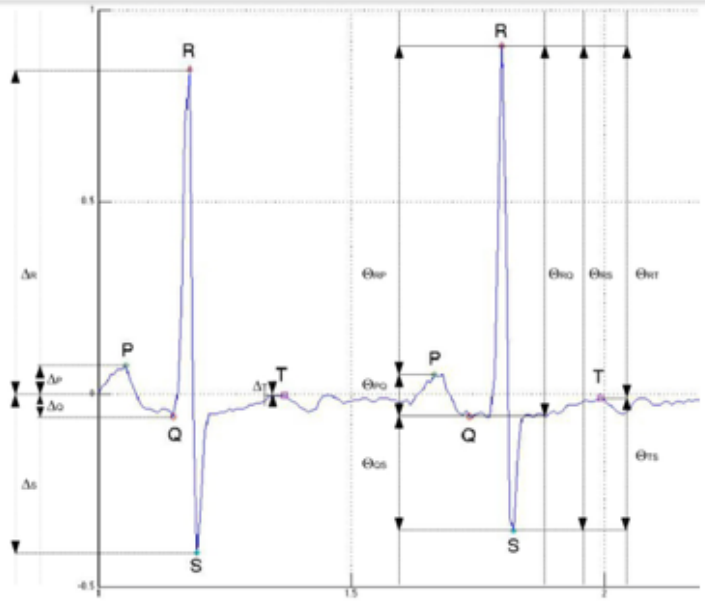
Human Identification



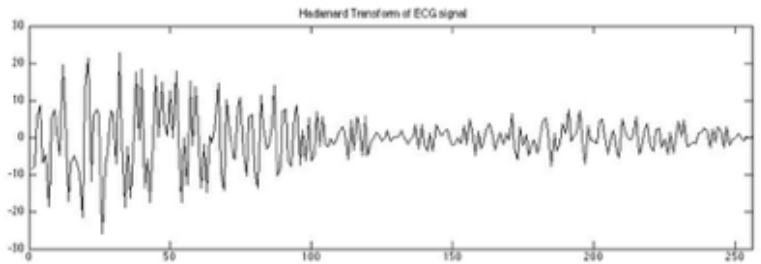
Human Identification Using Compressed ECG Signals. Carmen Camara, Pedro Peris-Lopez, Juan E. Tapiador. Journal Medical Systems, 39(11):148 (2015).

HI: Feature Extraction

Time Domain

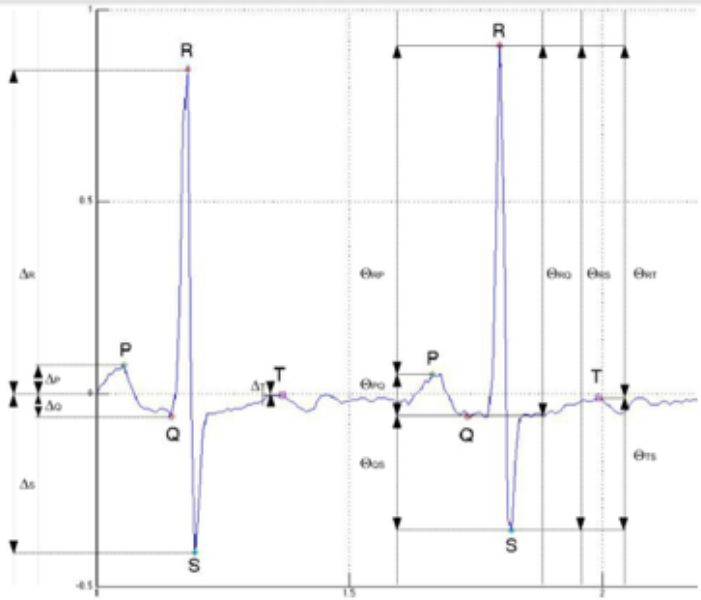


Transform Domain
(e.g., Fourier, Wavelets, Walsh Hadamard, etc.)

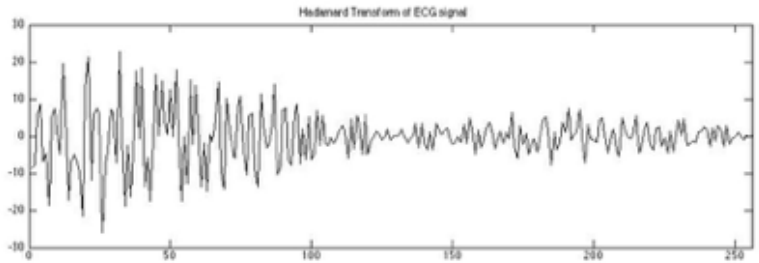


HI: Feature Extraction

Time Domain



Transform Domain
(e.g., Fourier, Wavelets,
Walsh Hadamard, etc.)



HI: Settings

Features:

- OP1: 24 lower Hadamard sequencing coefficients x 2 leads
- OP2: OP1 + Shannon and Log-Energy entropy

Classifier:

- K-NN
  - $K = \mathbf{1}, 3, 5, 9$
  - Euclidean distance (d_E) and Manhattan distance (d_M)
- 10-fold cross validation

Human Identification: Results

Overall Performance: FNR, FPRm TPR, TNR

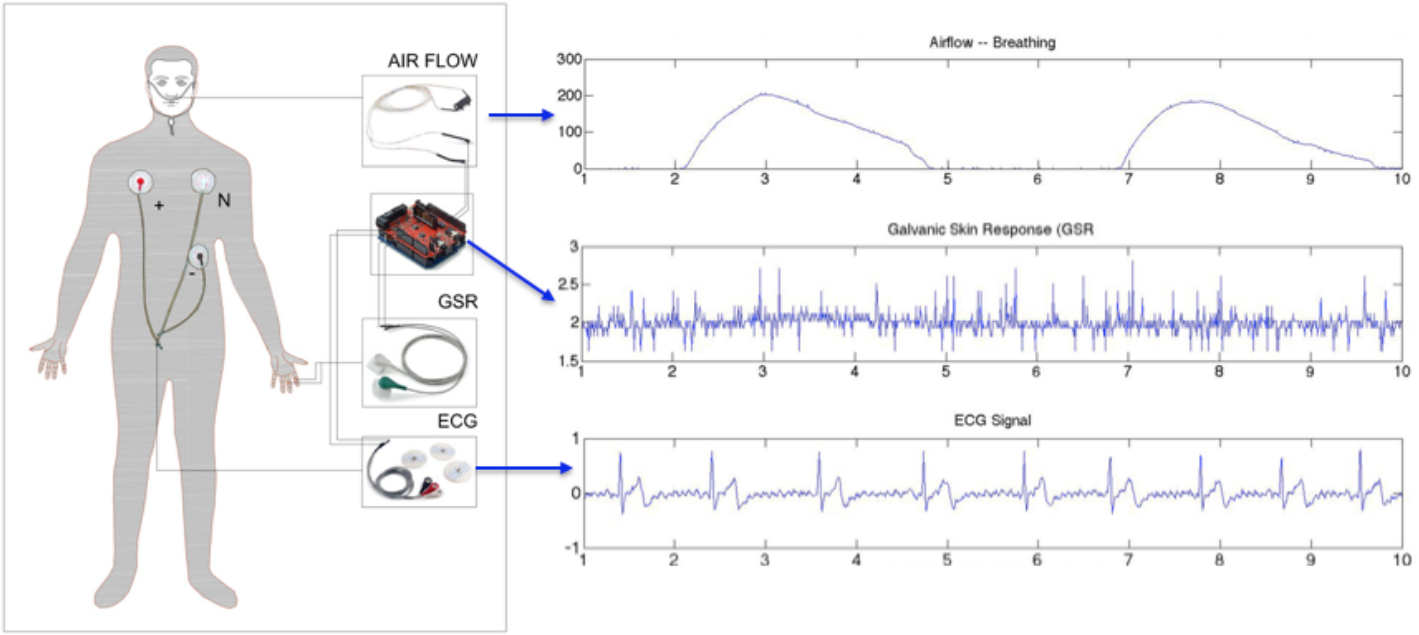
Configuration		FNR	FPR	TPR	TNR
OP-1	d_E	0.0580	0.0582	0.9418	0.9420
	d_M	0.0570	0.0566	0.9434	0.9430
OP-2	d_E	0.0390	0.0386	0.9614	0.9610
	d_M	0.0340	0.0341	0.9659	0.9660

OP1: 24 lower Hadamard sequencing coefficients x 2 leads
OP2: OP1 + Shannon and Log-Energy entropy

Biosignal-based authentication proposals

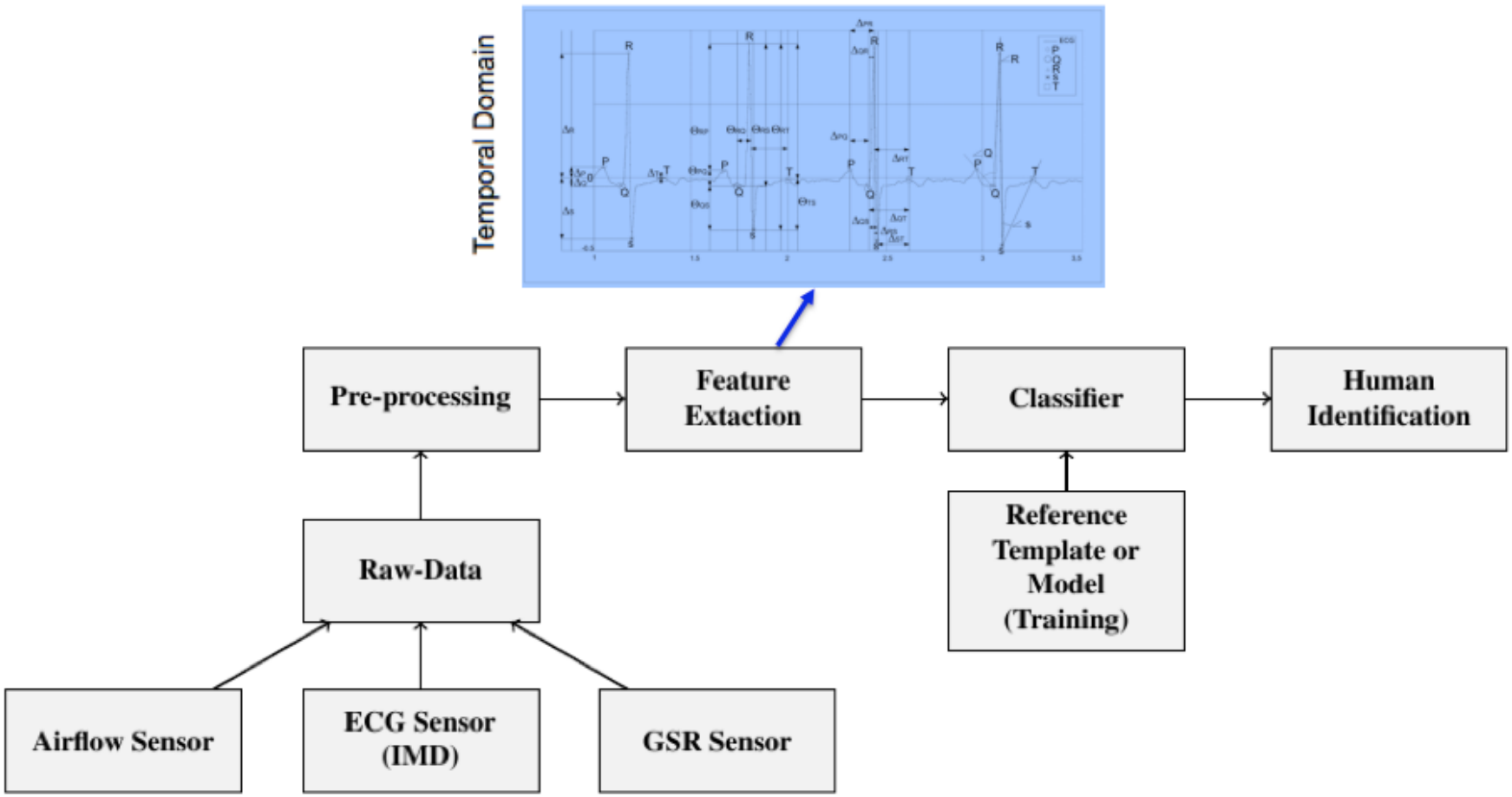
System	Correctly Classified Instances
Our system	94 % (OP-1) – 97 % (OP-2) %
ECG [OPHK+12]	86 % – 100 % (single day data acquisition)
EEG [SSR12]	72 % - 80 % (4-40 individuals)
EEG and ECG [RDCR08]	97.9 % (linear boundary)
Pulse-Response [RRMT14]	88 % –100 % (small data set)
Finger-vein [YSY11]	98 % (70 individuals)
Iris and Fingerprint [MRG06]	96 % (small dataset)
Face & Iris [SAHO14]	99 % (UBIRIS v.2 and ORL)

Multi-modal Human Identification



Non-invasive Multi-modal Human Identification System Combining ECG, GSR, and Airflow Biosignals. C. Camara, P. Peris-Lopez, J. E. Tapiador, G. Suarez-Tangil. Journal of Medical and Biological Engineering, 35(6):735-748, (2015).

Multi-modal Human Identification



Multi-modal HI: Settings

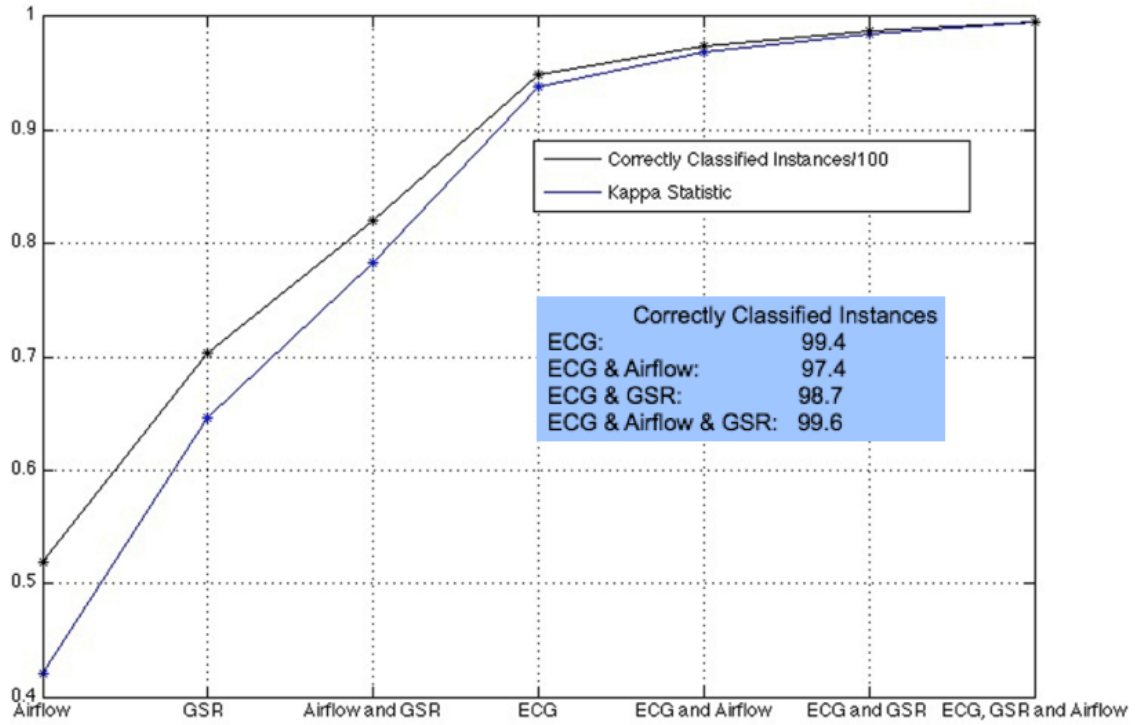
Features (time-domain):

- ECG: Amplitudes ($\{\Lambda_P, \Lambda_Q, \Lambda_R, \Lambda_S, \Lambda_T\}$), relative amplitudes ($\{\Theta_{RP}, \Theta_{RQ}, \Theta_{RS}, \Theta_{RT}, \Theta_{PQ}, \Theta_{QS}, \Theta_{TS}\}$), time-intervals ($\Delta_{PQ}, \Delta_{PR}, \Delta_{QR}, \Delta_{QS}, \Delta_{QT}, \Delta_{RS}, \Delta_{RT}, \Delta_{ST}$), and angles ($\{\angle_Q, \angle_R, \angle_S\}$).
- GSR and Airflow: Average value (PQRST complex; $\Psi_{Avg}, \Upsilon_{Avg}$), instantaneous value (at R-peak; Ψ_R, Υ_R).

Classifier:

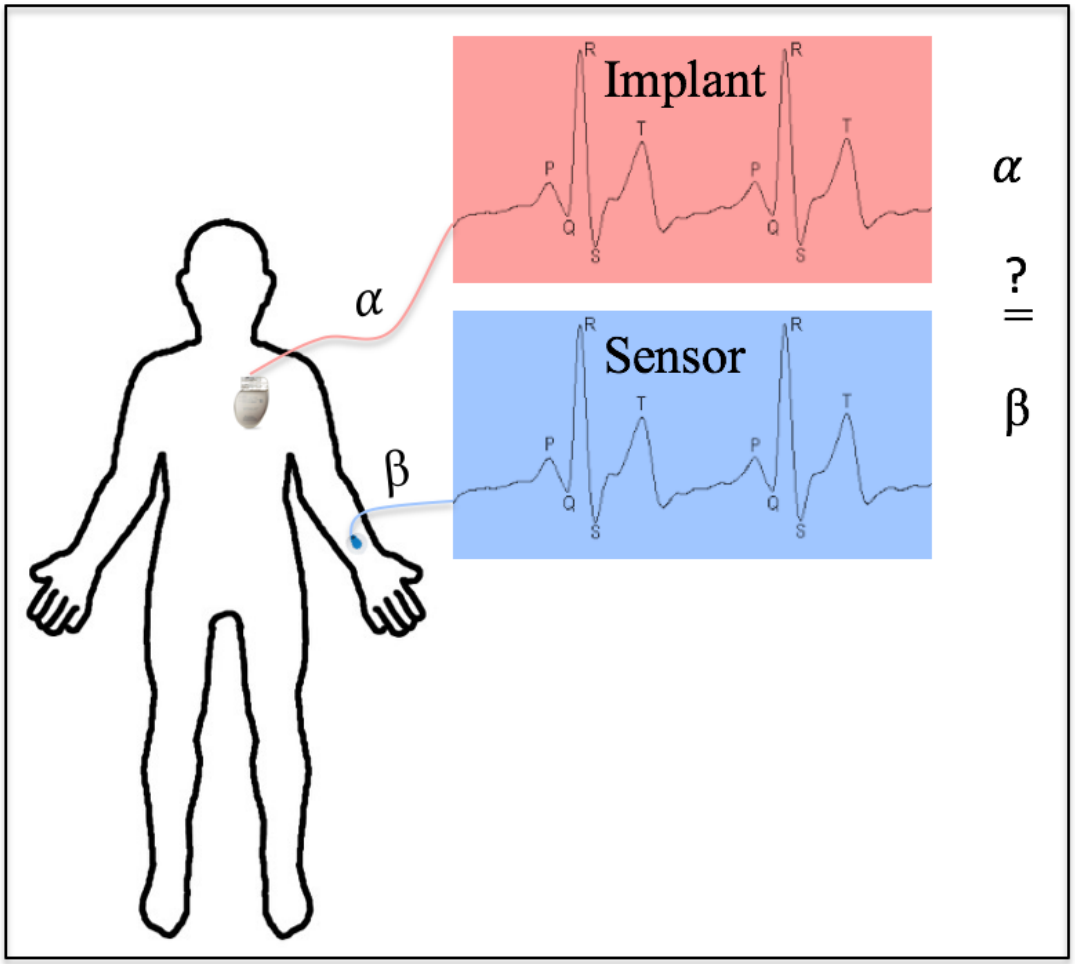
- Rotation Forest
  - Attribute selection: PCA
  - Classifier: C4.5

Multi-modal HI: Results

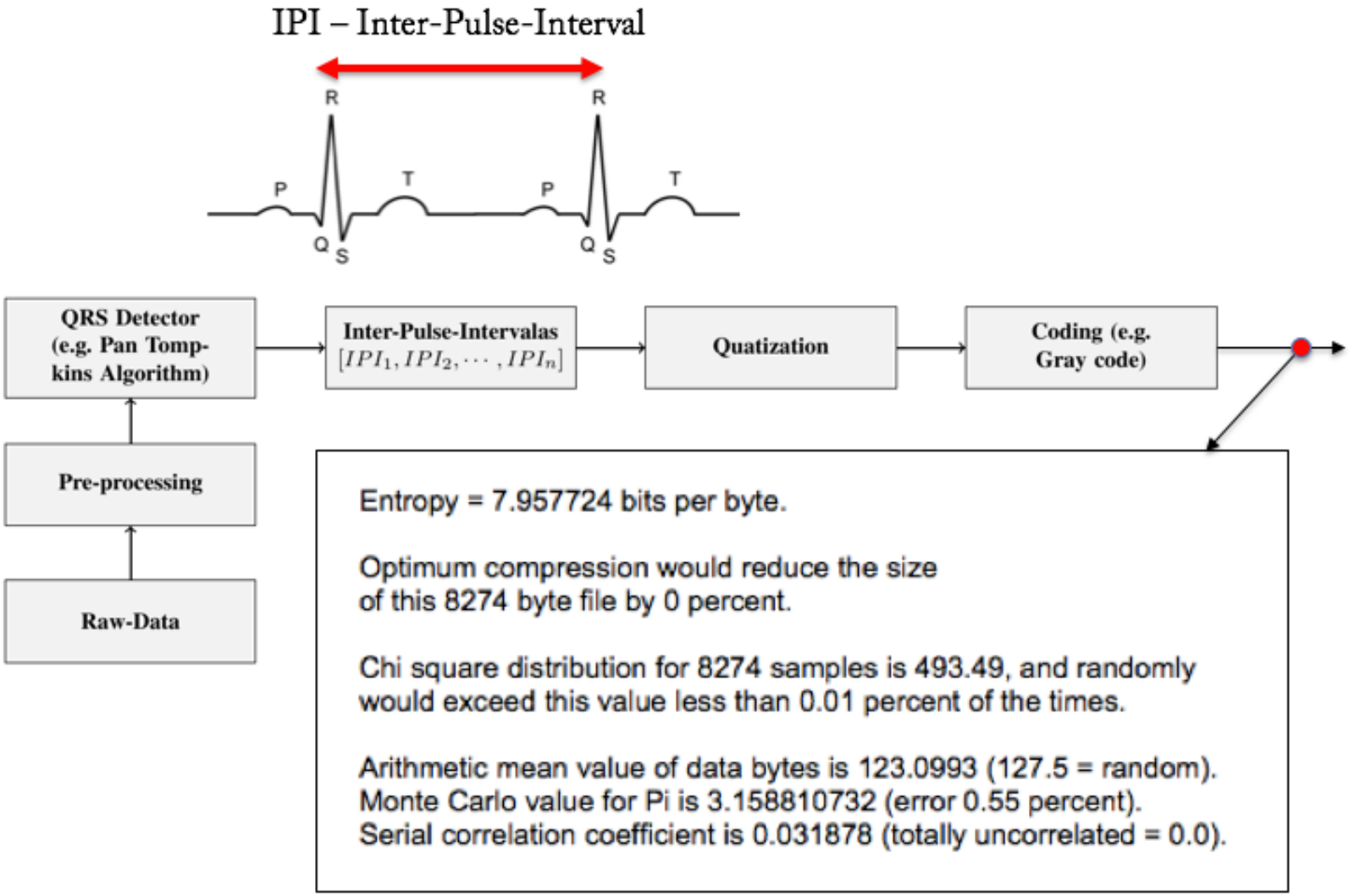


System	Correctly Classified Instances
Our system	97.4 %
ECG [OPHK+12]	86 % – 100 % (single day data acquisition)
EEG [SSR12]	72 % - 80 %
Pulse-Response [RRMT14]	88 % –100 % (small data set)
EEG and ECG [RDCR08]	97.9 % (linear boundary)

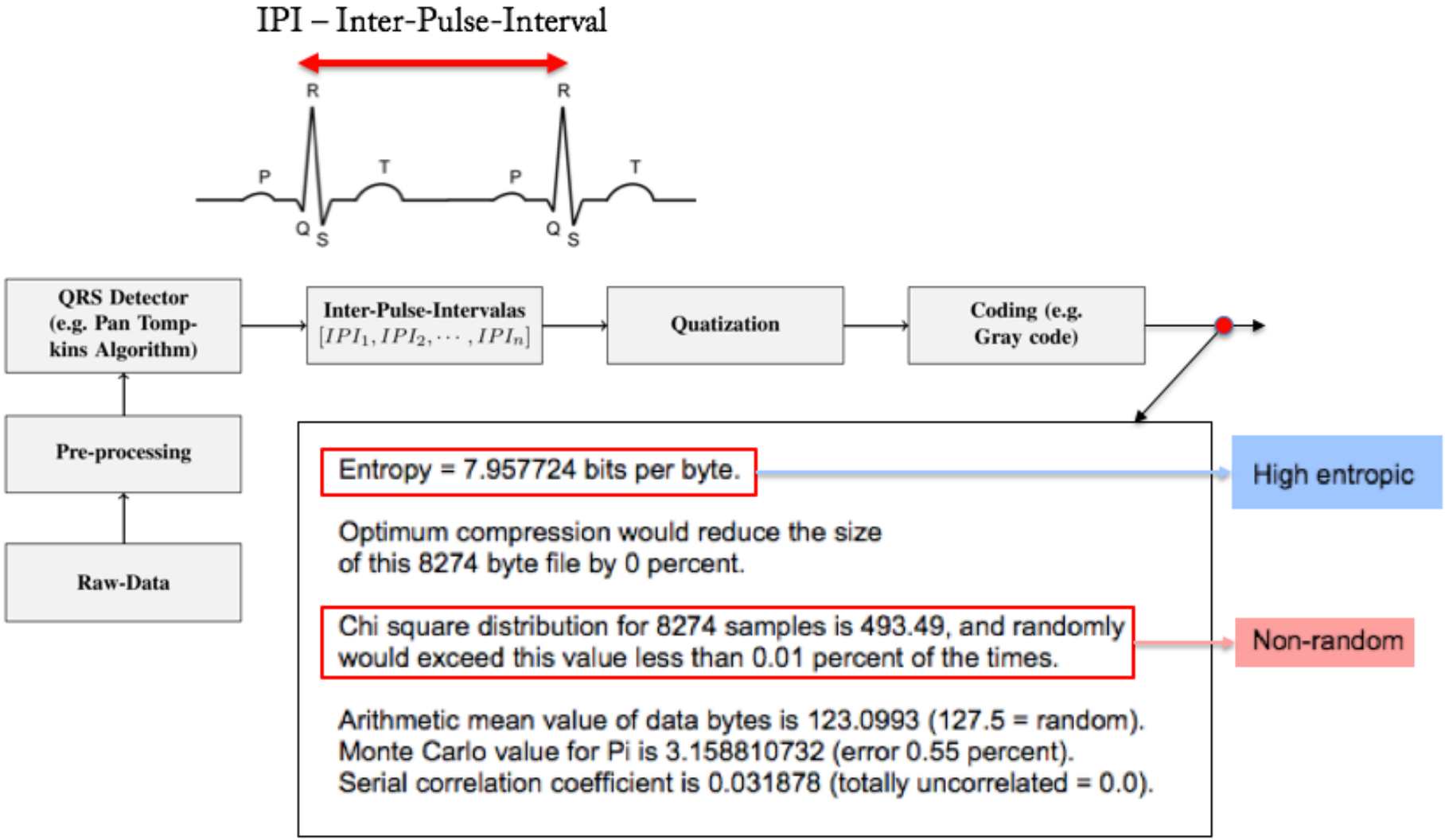
Extracting randomness from ECG signals: Key generation



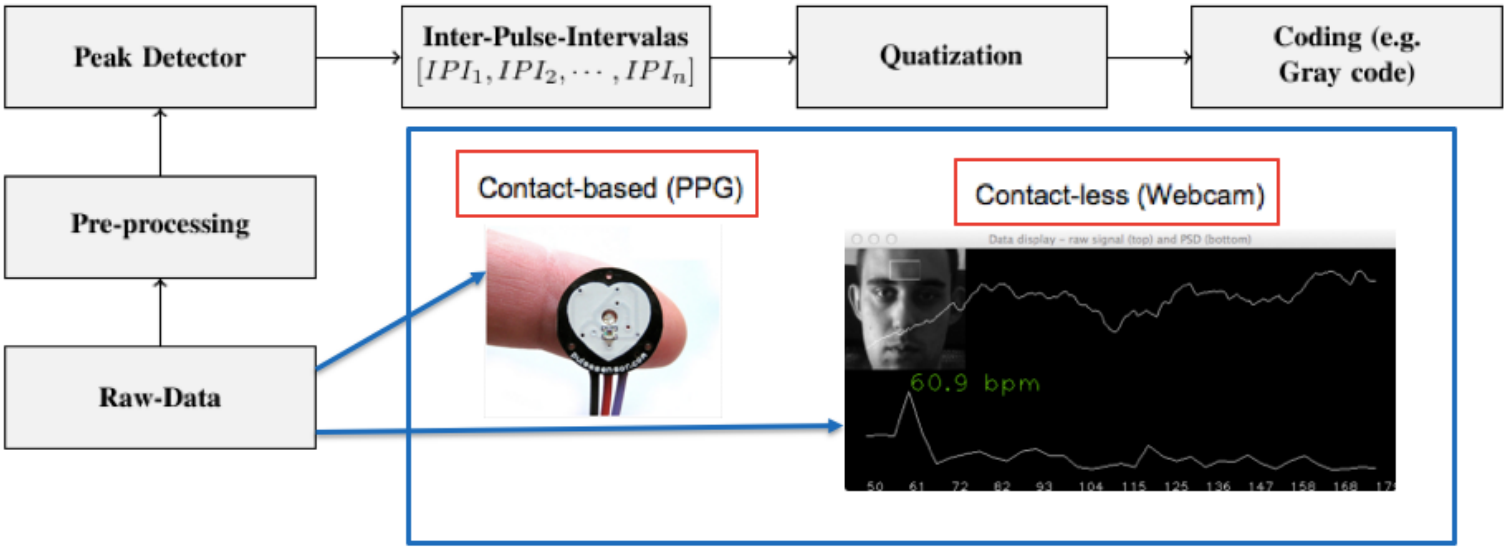
IPIs: Randomness Analysis



IPIs: Randomness Analysis

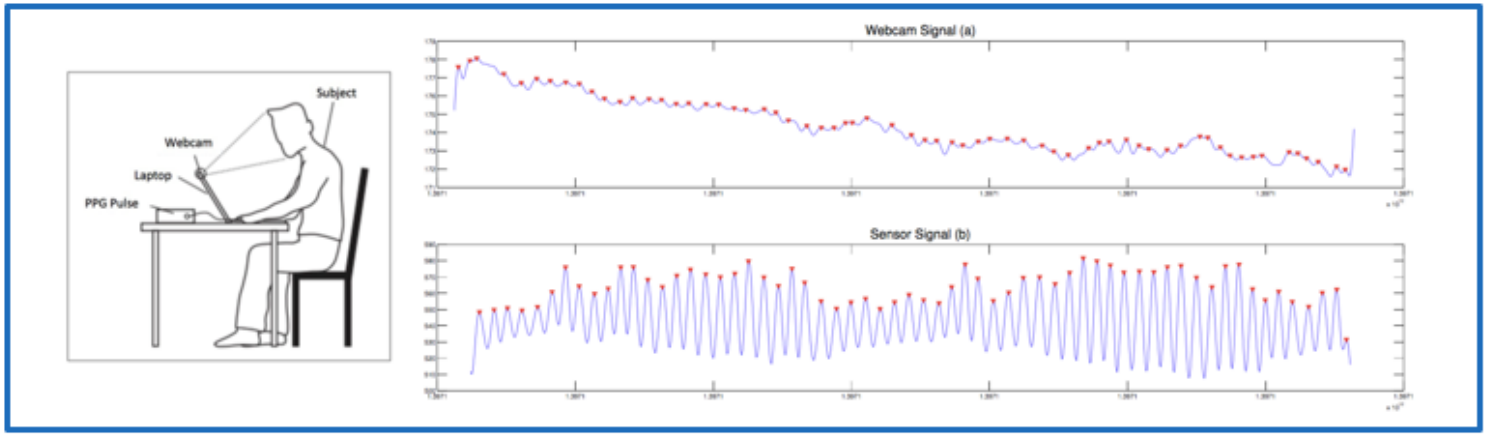


IPIs: Monitorization



Electrical Heart Signals can be Monitored from the Moon: Security Implications for IPI-Based Protocols. Alejandro Calleja, Pedro Peris-Lopez, Juan E. Tapiador. Information Security Theory and Practice, vol. 9311 of LNCS, pp. 36-51, 2015.

R-Peaks (heart-beats) detected



Sample	Beats Webcam Signal	Beats Sensor Signal	Error
sample 1	62	64	2
sample 2	68	71	3
sample 3	59	59	0
sample 4	63	60	3
sample 5	60	62	2
sample 6	60	59	1
sample 7	66	65	1
sample 8	69	69	0
sample 9	62	60	2
sample 10	85	81	4
sample 11	61	65	4
sample 12	69	70	1
sample 13	68	69	1
Mean Error	-	-	1.69

IPIs: Similarity Analysis

Scalar Quantizer

Bit	Hit Probability (%)	Entropy	
		Sensor	Webcam
1 (MSB)	70.095	0.714	0.868
2	61.483	0.941	0.689
3	61.004	0.898	0.762
4	62.918	0.929	0.709
5	58.688	0.959	0.816
6	94.976	0.143	0.228
7	82.775	0.0.266	0.593
8 (LSB)	70.095	0.719	0.764
Last 4 bits	76.883	0.718	0.657
Overall	70.37	0.782	0.708

Dynamic Quantizer

Bit	Hit Probability (%)	Entropy	
		Sensor	Webcam
1 (MSB)	62.157	0.979	0.946
2	65.071	0.947	0.959
3	49.88	0.991	0.951
4	55.741	0.781	0.959
5	47.010	0.905	0.977
6	49.880	0.997	0.961
7	51.555	0.657	0.983
8 (LSB)	52.990	0.9290	0.999
Last 4 bits	50.358	0.959	0.999
Overall	54.41	0.990	0.999

Conclusions

- New generations of IMDs are already on the market
- Important security issues (no fiction!)
- Special requirements for this technology
- New solutions are demanding

Questions?

Thank you very much for your attention

pperis@inf.uc3m.es

http://www.lightweightcryptography.com

References

- J. A. Hansen and N. M. Hansen, *A taxonomy of vulnerabilities in implantable medical devices*, Proc. of the second annual workshop on Security and privacy in medical and home-care systems (New York, USA), SPIMACS '10, ACM, 2010, pp. 13–20.
- H. Mehrotra, A. Rattani, and P. Gupta, *Fusion of iris and fingerprint biometric for recognition*, Proceedings of the International Conference on Signal and Image Processing, 2006, pp. 1–6.

References (cont.)

- I. Odinaka, L. Po-Hsiang, A .D. Kaplan, J. A. O'Sullivan, E. J. Sirevaag, and J. W. Rohrbaugh, *Ecg biometric recognition: A comparative analysis*, IEEE Transactions on Information Forensics and Security **7** (2012), no. 6, 1812–1824.
- K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, *Proximity-based access control for implantable medical devices*, Proceedings of the 16th ACM Conference on Computer and Communications Security, ACM, 2009, pp. 410–419.

References (cont.)

- A. Riera, S. Dunne, I. Cester, and G. Ruffini, *STARFAST: a wireless wearable eeg/ecg biometric system based on the ENOBIO sensor*, International Workshop on Wearable Micro and Nanosystems for Personalised Health, 2008, pp. 1–4.
- K. B. Rasmussen, M. Roeschlin, I. Martinovic, and G. Tsudik, *Authentication using pulse-response biometrics*, The Network and Distributed System Security Symposium (NDSS), 2014.
- H. M. Sim, H. Asmuni, R. Hassan, and R. M. Othman, *Multimodal biometrics: Weighted score level fusion based on non-ideal iris and face images*, Expert Systems with Applications **41** (2014), no. 11, 5390 – 5404.

References (cont.)

- Y. N. and. Singh, S. K. Singh, and A. K. Ray, *Bioelectrical signals as emerging biometrics: Issues and challenges*, ISRN Signal Processing **2012** (2012), 1–13.
- J. Yang, Y. Shi, and J. Yang, *Personal identification based on finger-vein features*, Computers in Human Behavior **27** (2011), no. 5, 1565 – 1570.