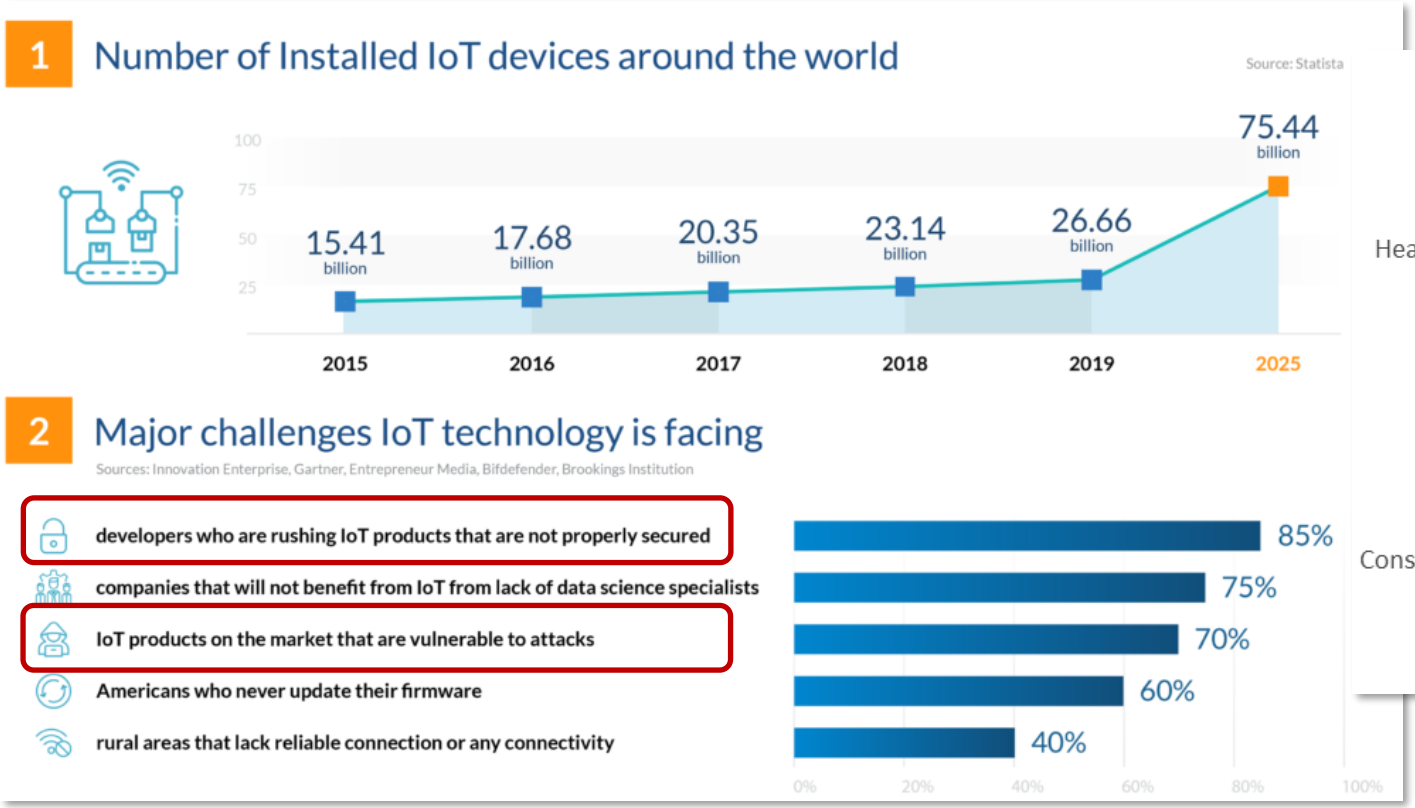
CEU
Universidad San Pablo

Security evaluation and protection against side-channel attacks

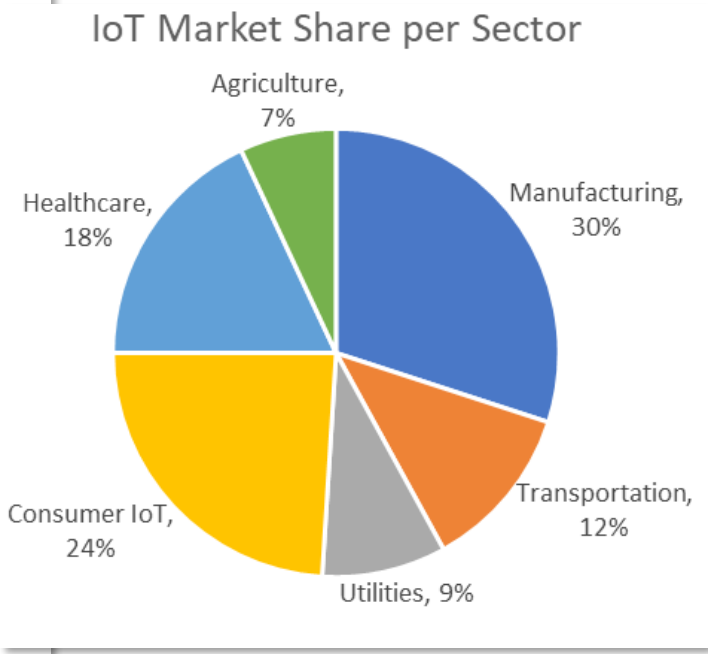
Dual Use Technologies 2022: Cybersecurity and digital applications in defence, Málaga

Pablo Pérez Tirador
Universidad San Pablo CEU
Madrid

IoT Trends – Users and Security



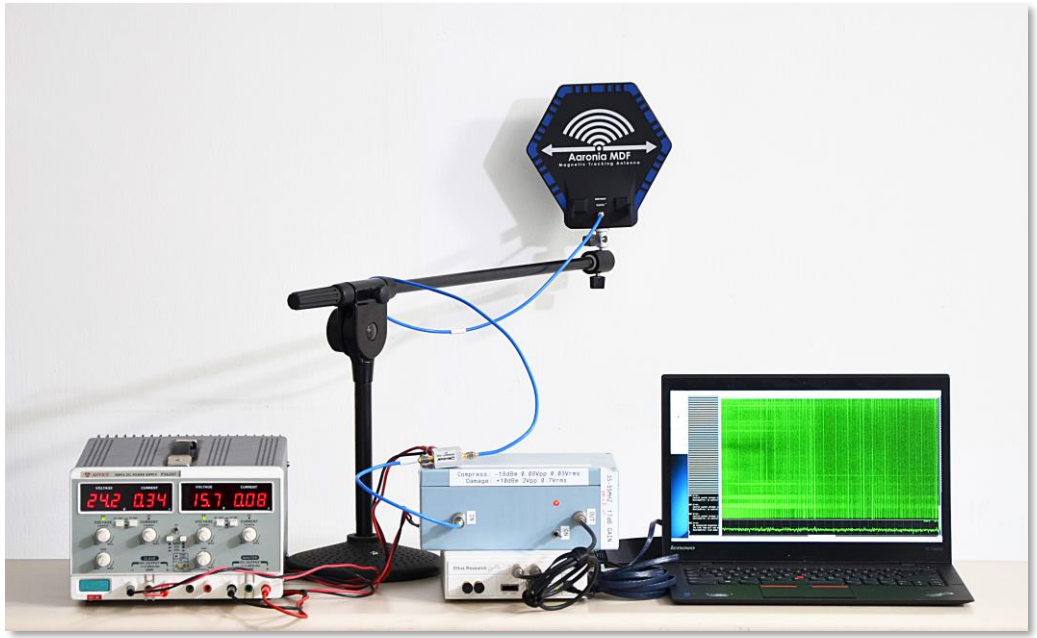
Source: FinancesOnline



Source: Capgemini

Side Channel Attacks – a Concern for IoT

Attacks that ignore mathematical properties of a cryptographic system and focus on information leaks of its physical implementation in hardware (power, electro-magnetic radiations, timing, heat dissipation, etc.)



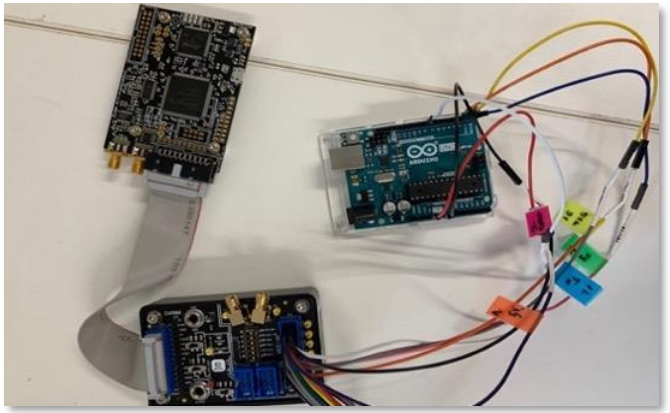
Source: Genkin, Pachmanov, Pipman, Tromer, Tel Aviv University (2016)

Our Work at CEU – Universidad San Pablo

- Joint work of Telecommunication Engineering and Biomedical Engineering
- We test attack modalities to find vulnerabilities in embedded and wearable devices and develop countermeasures
- We study cryptographic and non-cryptographic attacks
  - Power attacks
  - EM attacks

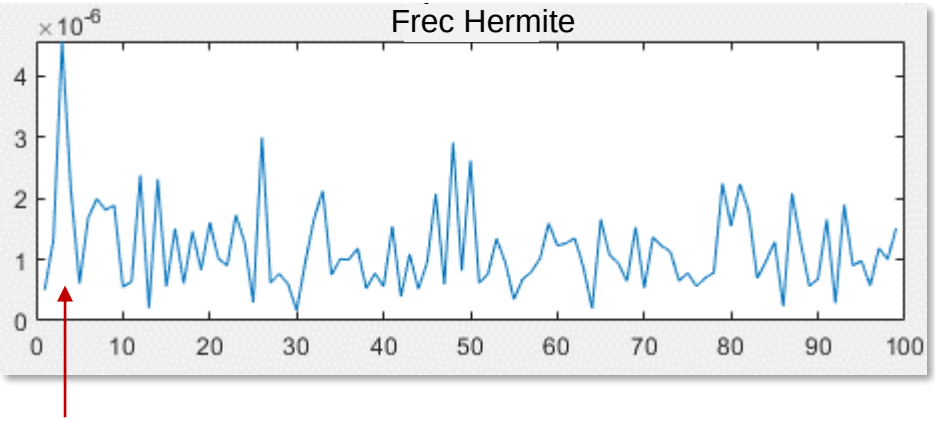
Our Work – a Platform for Embedded Systems

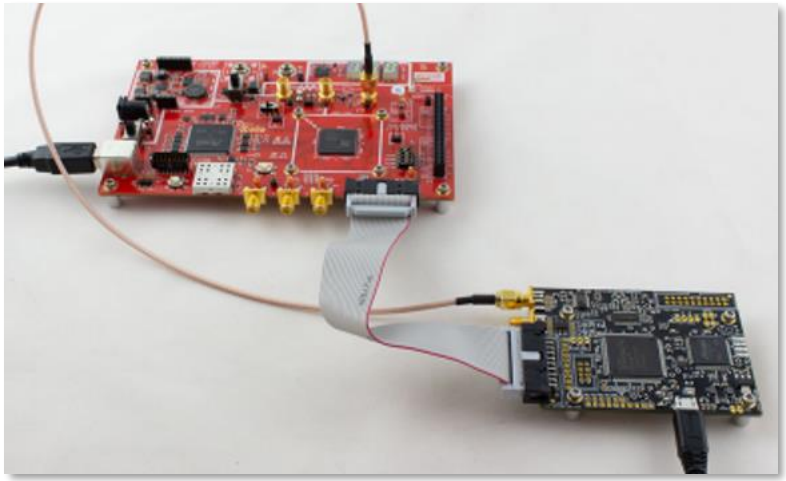
- Platform based on ChipWhisperer's scope plus a modified Arduino Uno
- Carried out attacks on the AES encryption of random and biomedical data
- Successfuly improved the robustness of the algorithm by
  - applying a voltage modulation to Arduino
  - modifying the internal structure of the data



Our Work – a Platform for FPGAs

- Platform based on ChipWhisperer's scope plus an FPGA target
- Studied possible attacks on the power traces (e.g. recovery of the heart rate) for an ECG characterization algorithm
- Applied voltage modulation to mask the execution of the algorithm





Our Work – Present and Future

- Publications
  - R. Jevtic and M. Garcia Otero, "Methodology for complete decorrelation of power supply EM side-channel signal and sensitive data", IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 69, no. 4, pp. 2256-2260, April 2022
  - R. Jevtic et. al., "EM Side-Channel Countermeasure for Switched-Capacitor DC-DC Converters Based on Amplitude Modulation", IEEE Transactions on VLSI Systems, vol. 29, no. 6, June 2021.

- Congresses
  - R. Jevtic, M. Ylitolva and L. Koskinen, "Reconfigurable Switched-Capacitor DC- DC Converter for Improved Security in IoT Devices", Proc. on PATMOS18, July 2018
  - R. Jevtic, P. Perez-Tirador, C. Cabezaolias, P. Carnero and G. Caffarena, "Side-channel Attack Countermeasure Based on Power Supply Modulation", Proc. 30th European Signal Processing Conference (EUSIPCO), pp. 618-622, August 2022

Our Work – Present and Future

- Ongoing experiments:
  - Study of electromagnetic leaks in previous platforms
  - Design of new antennas for EM attacks

- Publications in preparation
  - Transactions on Information Forensics and Security

Our Work – Present and Future

Publications

- R. Jevtic and M. Garcia Otero, April 2022
- R. Jevtic et. al., June 2021.

Congresses

- R. Jevtic, M. Ylitolva and L. Koskinen, Proc. on PATMOS18, July 2018
- R. Jevtic, P. Perez-Tirador, C. Cabezaolias, P. Carnero and G. Caffarena, Proc. EUSIPCO, August 2022

Ongoing experiments:

- Study of electromagnetic leaks in previous platforms
- Design of new antennas for EM attacks

Publications in preparation

- Transactions on Information Forensics and Security

Thank You

Departamento de Tecnologías de la Información,
Universidad CEU-San Pablo

Pablo Perez Tirador – pablo.pereztirador@ceu.es
Ruzica Jevtic – ruzica.jevtic@ceu.es
Gabriel Caffarena Fernandez – gabriel.caffarena@ceu.es