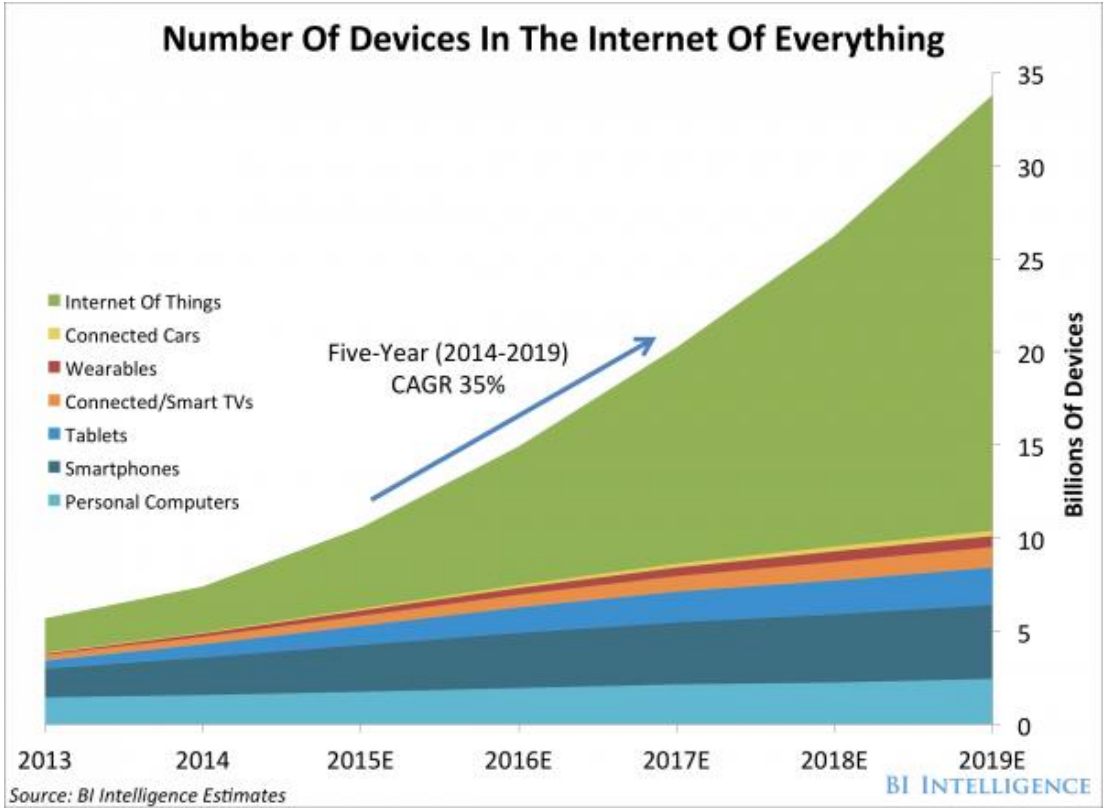
Wireless IoT Security

Alenka Zajic

December 2016

❖Internet of Everything



❖Challenges for IoT Devices

- **Sensing a complex environment -**Innovative ways to sense and deliver information from the physical world to the cloud
- **Connectivity-** Variety of wired and wireless networks needed
- **Security is vital -** Detecting and blocking malicious activity
- **IoT is complex** IoT application development needs to be easy for all developers, not just to experts
- **Cloud is important -** IoT will require significant increase in data storage
- **Power is critical**

❖Securing and Programing IoT Devices

- Traditional software-based security check as well as software analysis methods will not work
  - Not enough storage space for anti-virus software
  - No interface for getting security results out

- Idea: Use RF emanations form IoT to monitor security, analyze code performance and find bugs – FROM OUTSIDE OF THE DEVICE
  - IoT device and its software is unchanged
  - One attack cannot take over device and its security at the same time because they are two separate hardware entities
  - We are not looking for a particular intrusion signature

❖EM Emanations From Computer Systems

- EM emanations from modern systems (laptops, desktops, cellphones, IoT) exist
  - Can they leak any "interesting" information? (yes)
  - From how far away can they be received? (several meters)

[1] A. Zajic and M. Prvulovic, "Experimental demonstration of electromagnetic information leakage from modern processor-memory systems," *IEEE Transactions on Electromagnetic Compatibility*, vol. 56, no. 4, pp. 885-893, August 2014.

[2] D. Genkin, I. Pipman, and E. Tromer, "Get Your Hands Off My Laptop: Physical Side-Channel Key-Extraction Attacks on PCs," in Proc. Crypto. HW and Emb. Sys. (CHES), 2014.

[3] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "Stealing Keys from PCs using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation," in Proc. Crypto. HW and Emb. Sys. (CHES), 2015.

[4] Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici, "GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies," Usenix Security Symposium 2015.

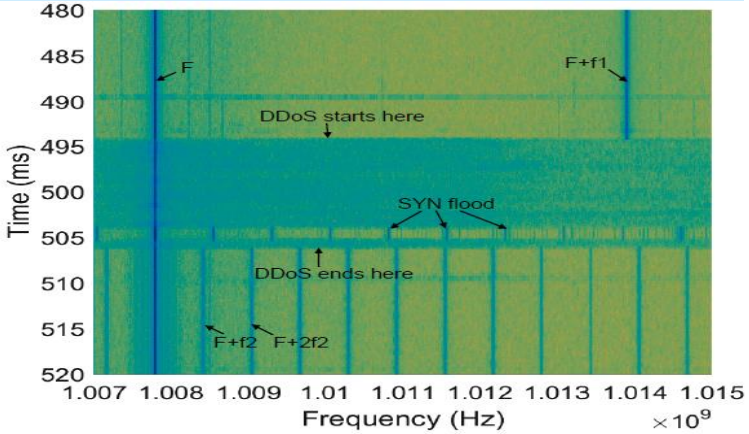
[6] R. Callan, A. Zajic, and M. Prvulovic, "FASE: Finding Amplitude-modulated side-channel emanations *Proceedings of the 42nd International Symposium on Computer Architecture (ISCA)*, pp. 592-603, June 2015.

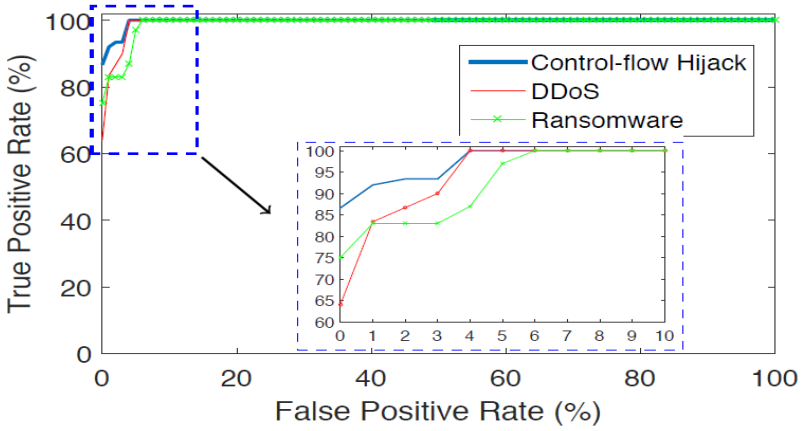
[7] R. Callan, A. Zajic, and M. Prvulovic, "A practical methodology for measuring the side-channel signal available to the attacker for instruction level events," *IEEE MICRO 14*, pp.1-12, Cambridge, UK, December 2014.

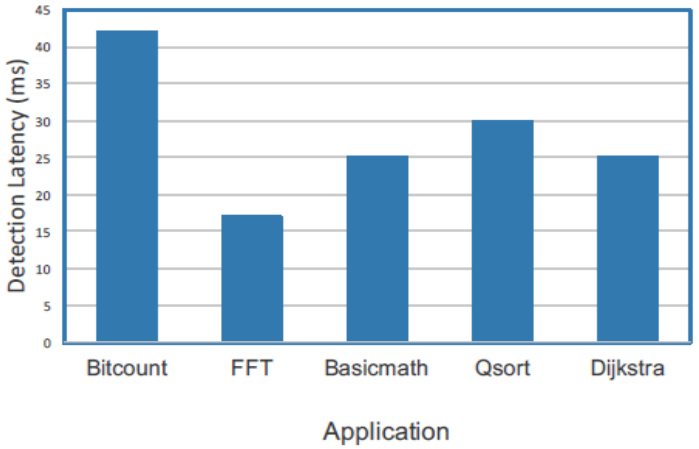
[8] N. Sehatbakhsh, A. Nazari, A. Zajić, and Milos Prvulovic "Spectral Profiling: Observer-Effect-Free Profiling by Monitoring EM Emanations," *IEEE MICRO 16*, pp.1-11, Taipei, Taiwan, October 2016.

[9] R. Callan, F. Behrang, M. Prvulovic, A. Zajic, and A. Orso, "Zero-Overhead Profiling via EM Emanations," accepted to *The International Symposium on Software Testing and Analysis*, 18-20 July 2016, Saarbrücken, Germany.

❖IoT Security via Side-Channels







❖Other Possible Applications

- Supply chain verification
- Industrial control systems verification and security
- Software debugging
- Research Funding:

National Science Foundation

https://youtu.be/CpBrk3YGFLw

- Commercialization
  - Patented technology
  - Camelia Technology, LLC