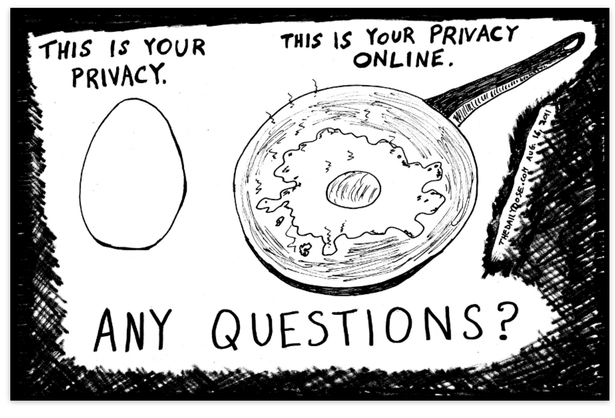
Side-Channel Attacks

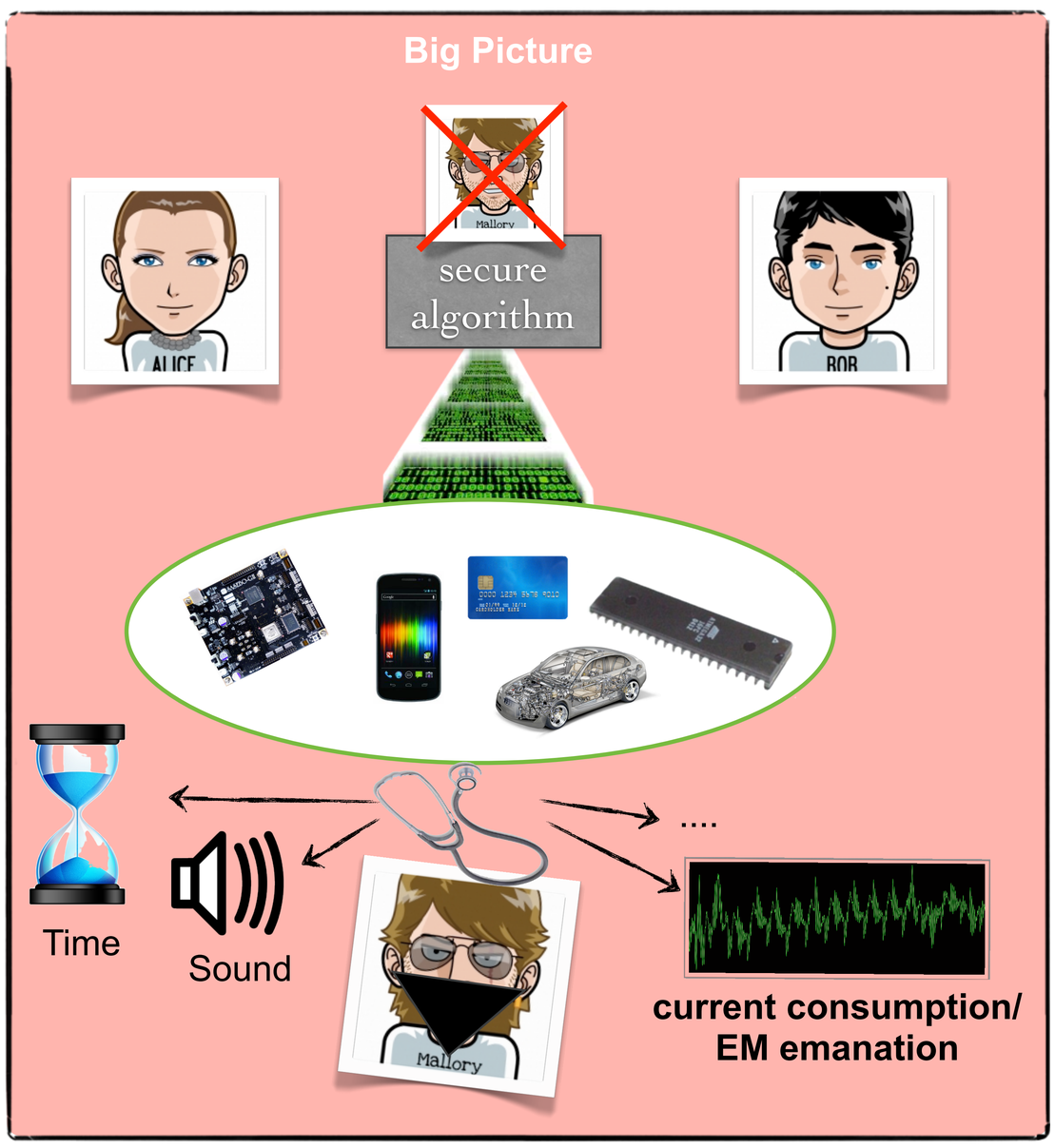
Annelie Heuser - Sylvain Guilley - Olivier Rioul

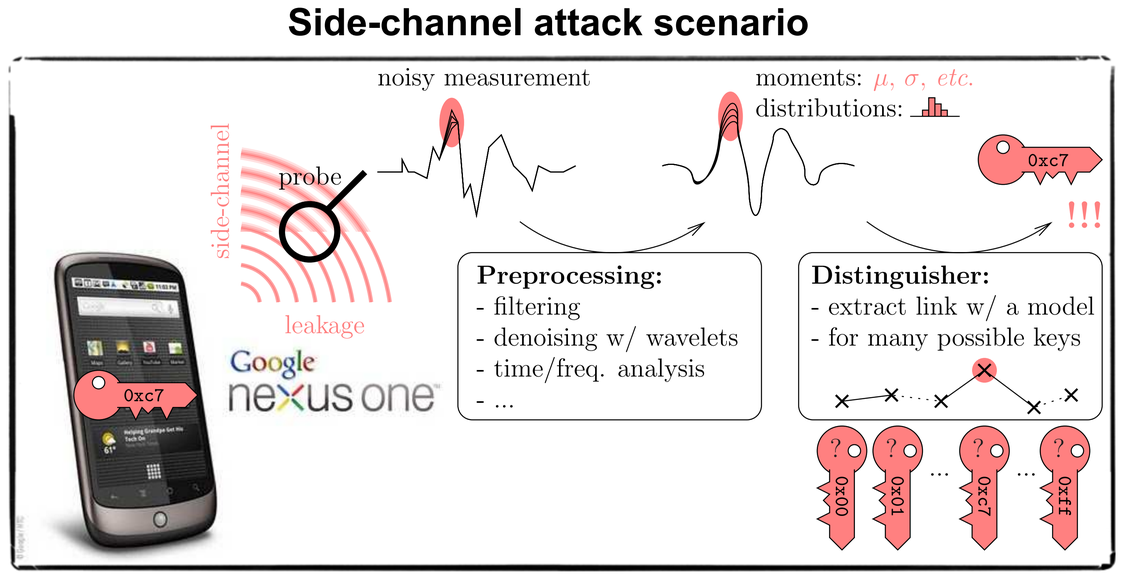
Institut Mines-Télécom
CNRS LTCI

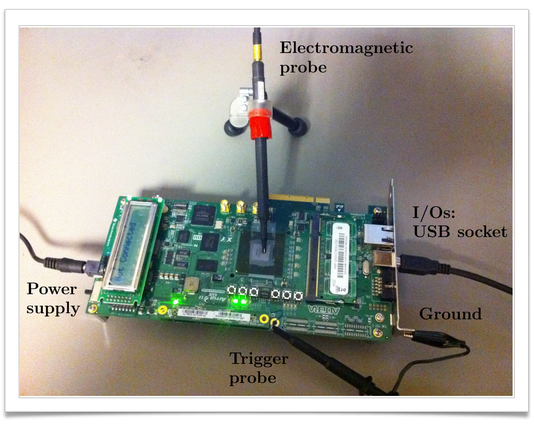


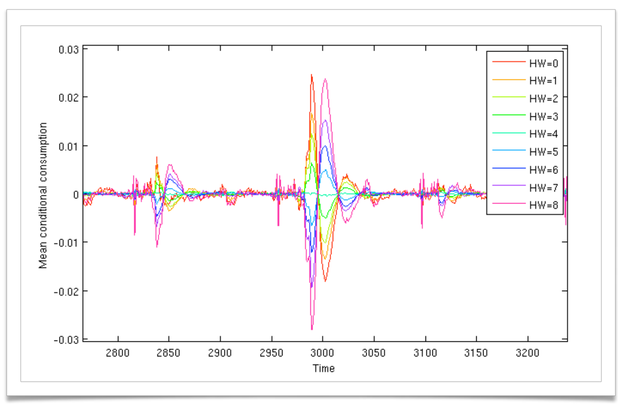
http://thedailydose.com/comic/this-is-your-privacy-online/

"Classical" side-channel attacks









Open questions

How to (fairly) compare side-channel distinguishers? [3]

How to theoretically model side-channel attacks, e.g., with an information theoretic model?

How to precisely (effectively) model the arising side-channel leakage from the device?

Profiled
Side-channel distinguisher

- Template Attack
- Stochastic Approach
- Support Vector Machines [1]

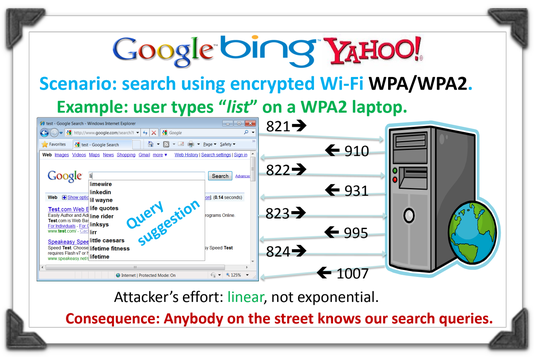
Non-Profiled
Side-channel distinguisher

- Differential Power Analysis
- Correlation Power Analysis
- Mutual Information Analysis
- Inter-class Information Analysis [2]

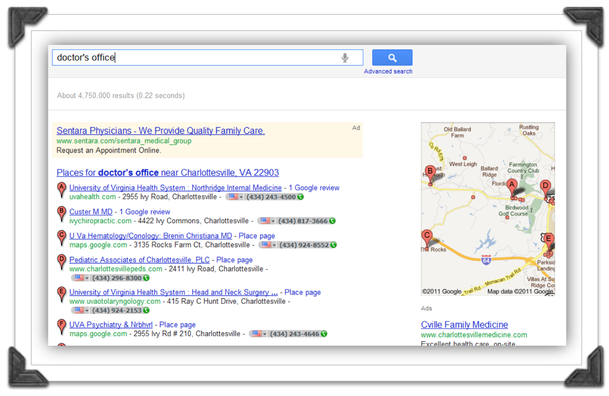
[1] Annelie Heuser, Michael Zohner: Intelligent Machine Homicide - Breaking Cryptographic Devices Using Support Vector Machines.
COSADE 2012
[2] Annelie Heuser, Houssem Maghrebi, Sylvain Guilley, Olivier Rioul, Jean-Luc Danger: Mathematical and Empirical Comparison of Information-Theoretic Side-Channel Distinguishers (under submission)
[3] Annelie Heuser, Sylvain Guilley, Olivier Rioul: Success Metric: An all-in-one criterium for comparing side-channel distinguisher (in preparation)

"Modern" Web Side-channel attacks

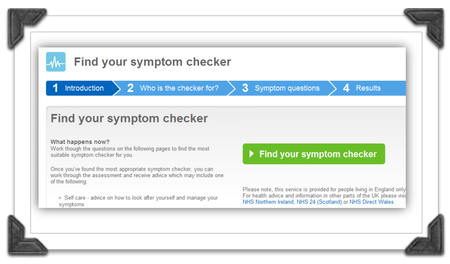
Web side-channel scenarios



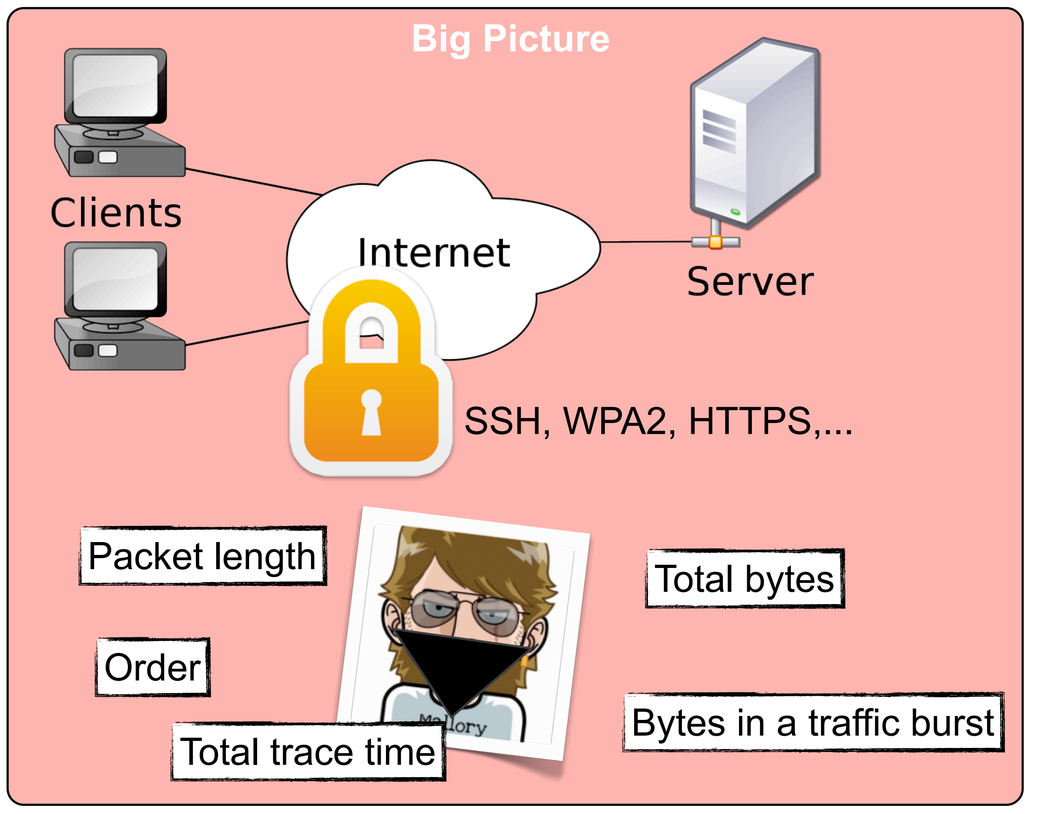
[4] Kehuan Zhang Zhou Li Rui Wang 0010 XiaoFeng Wang Shuo Chen Sidebuster: automated detection and quantification of side-channel leaks in web application development. 595-606 2010 ACM Conference on Computer and Communications Security



[5] Peter Chapman and David Evans. 2011. Automated black-box detection of side-channel vulnerabilities in web applications. In *Proceedings of the 18th ACM conference on Computer and communications security* (CCS '11). ACM, New York, NY, USA, 263-274.



[5]



Contact annelie.heuser@telecom-paristech.fr **Web** http://perso.telecom-paristech.fr/~heuser/