# PB173 Domain specific development: side-channel analysis

## Seminar 3: Example Attacks

Łukasz Chmielewski
chmiel@fi.muni.cz,

Consultation: A406 Friday 9:00-11:00

CROCS
Centre for Research on Cryptography and Security

# EM against mobile phones

Journals & Books

View PDF  Download full issue

ELSEVIER

Journal of Information Security and Applications

Volume 75, June 2023, 103481

## Mobile applications identification using autoencoder based electromagnetic side channel analysis

Jinghui Zhang [a], Boxi Liang [a], Hancheng Zhang [b], Wei Zhang [c], Zhen Ling [a], Ming Yang [a]

Show more

+ Add to Mendeley  Share  Cite

https://doi.org/10.1016/j.jisa.2023.103481  Get rights and content

### Abstract

Various applications are deployed on mobile smart devices in almost every situations of our life, while in some of these situations sensitive applications are strictly prohibited, such as cameras in cinemas and browsers in examination halls. Real-time recognition of applications running on mobile smart devices is of great significance in these cases.

https://www.sciencedirect.com/science/article/pii/S2214212623000650

# EM against mobile phones cont'd

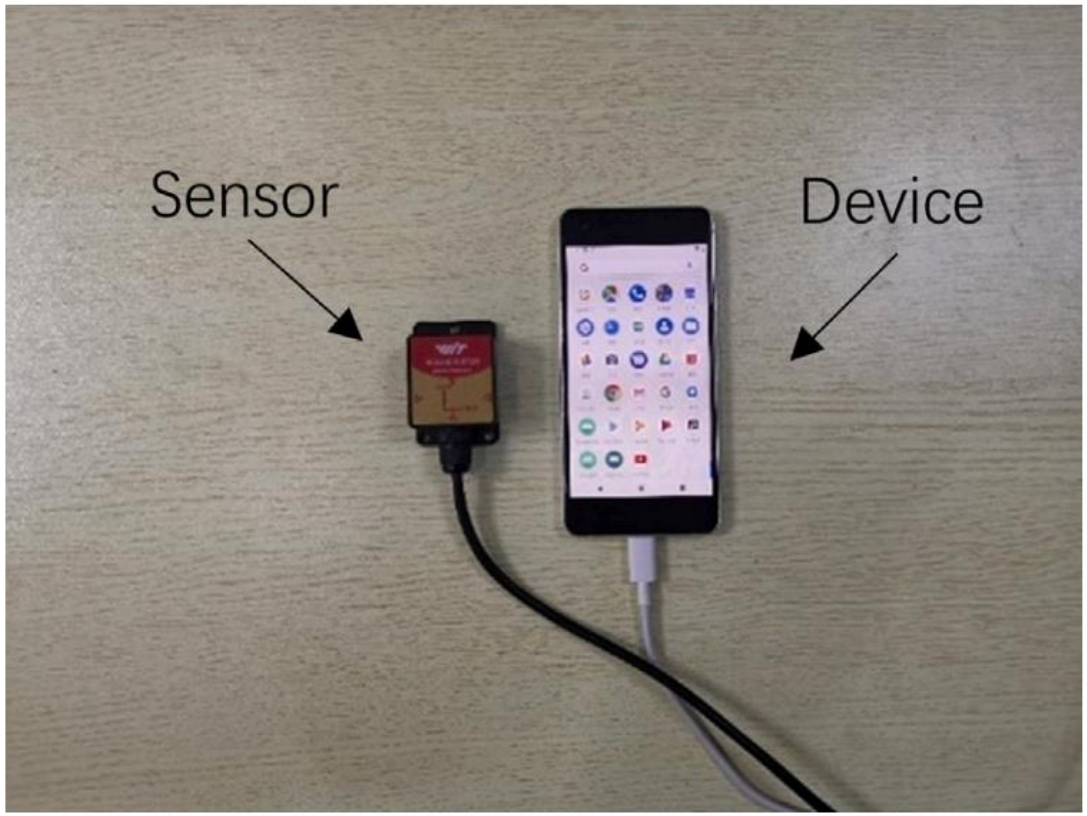



**Fig. 3.** Example of the sensor capturing magnetic field data from a mobile smart device.

# EM against mobile phones cont'd cont'd

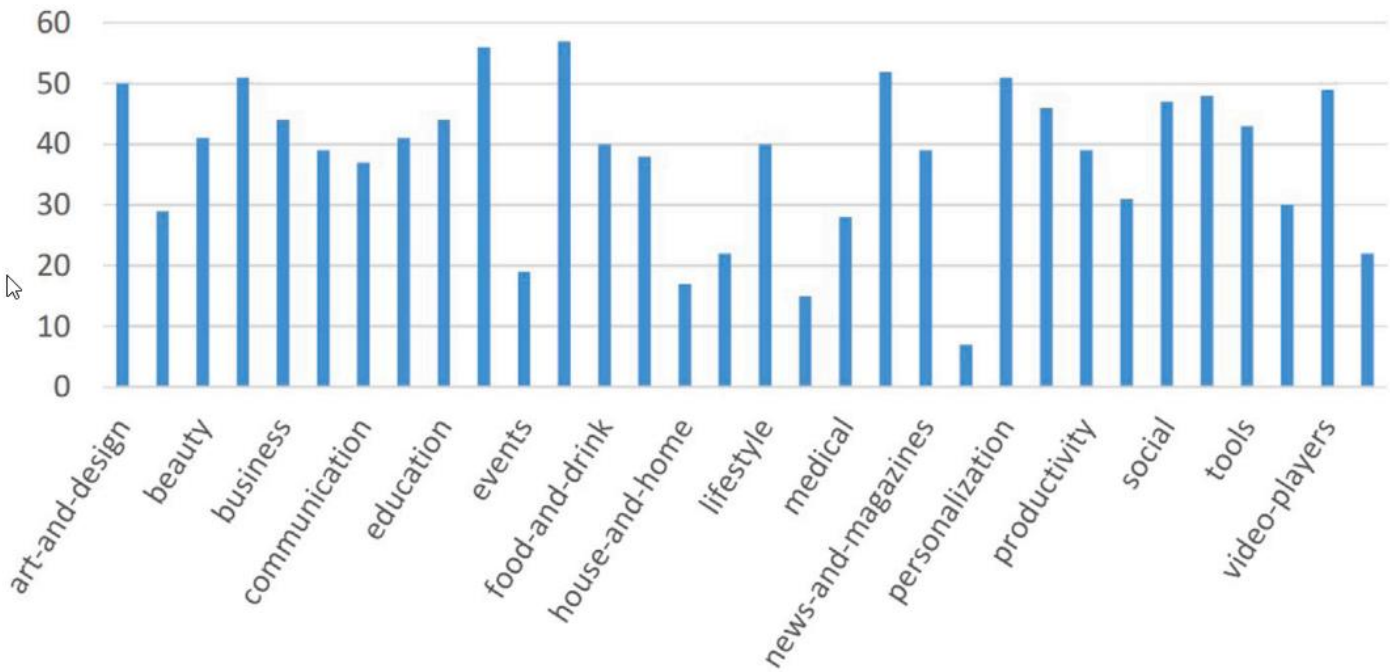



**Fig. 4.** Distribution of different types of applications.

# Cache attacks with low resolution counters

## The Gates of Time: Improving Cache Attacks with Transient Execution

Daniel Katzman, William Kosasih, Chitchanok Chuengsatiansup, Eyal Ronen, Yuval Yarom

*Tel-Aviv University*
*The University of Adelaide*
*The University of Melbourne*

### Abstract

For over two decades, cache attacks have been shown to pose a significant risk to the security of computer systems. In particular, a large number of works show that cache attacks provide a stepping stone for implementing transient-execution attacks. However, much less effort has been expended investigating the reverse direction—how transient execution can be exploited for cache attacks. In this work, we answer this question.

We first show that using transient execution, we can perform arbitrary manipulations of the cache state. Specifically,

important component is an out-of-order execution engine, which schedules and executes the instructions of the program. Out-of-order execution improves program performance by executing instructions when all their dependencies are satisfied instead of strictly following the program order.

Out-of-order execution is inherently speculative, both because the processor aims to predict the control flow of the program and because it assumes that instructions do not terminate abnormally, e.g., due to traps. Thus, the processor may execute instructions that do not appear in the nominal

the cases that a specific memory address is cached or not. We show how we can use this capability to build eviction sets in WebAssembly, using only a low-resolution (0.1 millisecond) timer. For the second use case, we present the Prime+Store

https://www.usenix.org/system/files/sec23fall-prepub-501-katzman.pdf

# SCA using performance counters (example)

View PDF  Download full issue

ELSEVIER

Microelectronics Journal
Volume 106, December 2020, 104935

## Template attacks on ECC implementations using performance counters in CPU ☆, ☆☆

B. Asvija [a], R. Eswari [b], M.B. Bijoy [a]

Show more

+ Add to Mendeley  Share  Cite

https://doi.org/10.1016/j.mejo.2020.104935  Get rights and content

### Abstract

We demonstrate a new set of template attacks on ECC implementations using the performance counters in CPU. Template attacks are powerful mechanisms that can combine statistical intelligence for modelling side channel leakages and can thus compromise complex crypto implementations. Automated attack phases add to the efficiency of this approach. We introduce a new approach of using CPU counter values for constructing templates to carry out attacks on crypto implementations, which also opens up the possibility of many other template attacks that have been demonstrated earlier using power analysis, to be feasible on the modern day architectures. The values obtained from multiple CPU counters are used to generate templates, which are further matched

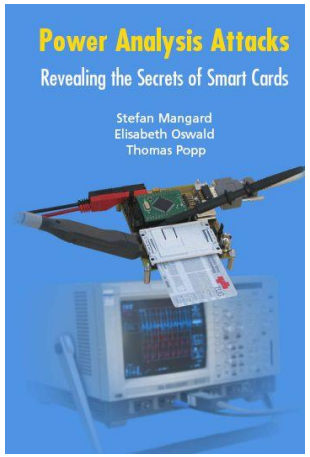
https://www.sciencedirect.com/science/article/pii/S0026269220305346

# Homework

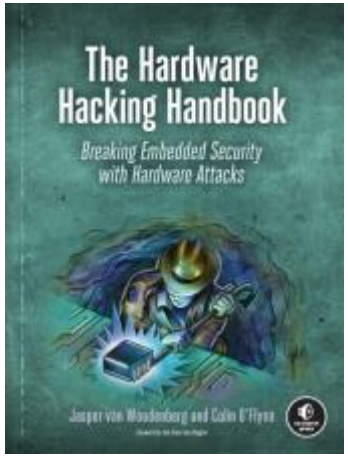
- Have you installed?
  - Install ChipWhisperer: https://chipwhisperer.readthedocs.io/en/latest/linux-install.html
  - Read the website in general. I am using CW in a linux VM under Windows but do as you prefer ☺

# Reading

- For interested people
- Side-Channel Analysis – blue book:
  - http://dpabook.iaik.tugraz.at/
  - The books is available at the uni.
  - Look online




- The Hardware Hacking Handbook:
  - https://nostarch.com/hardwarehacking
  - I have an epub version.



Questions