Software-based Microarchitectural Attacks on Low-end IoT Devices

Cristiano Rodrigues

Advisor:
Prof. Sandro Pinto

Co-Advisors:
Prof. Adriano Tavares & Prof. Mongkol Ekpanyapong

CENTROALGORITMI

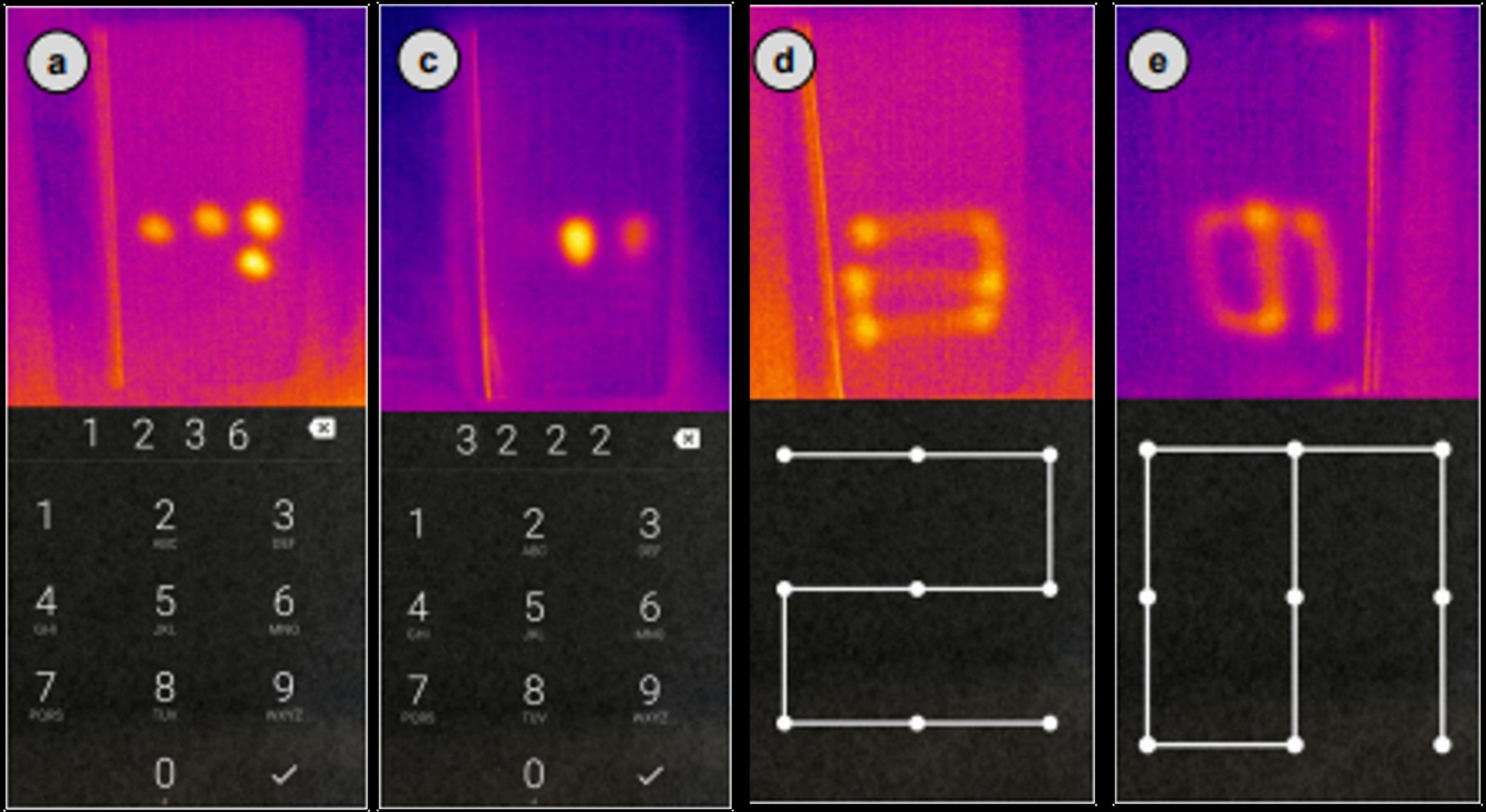
FCT Fundação para a Ciência e a Tecnologia

How to attack Hardware

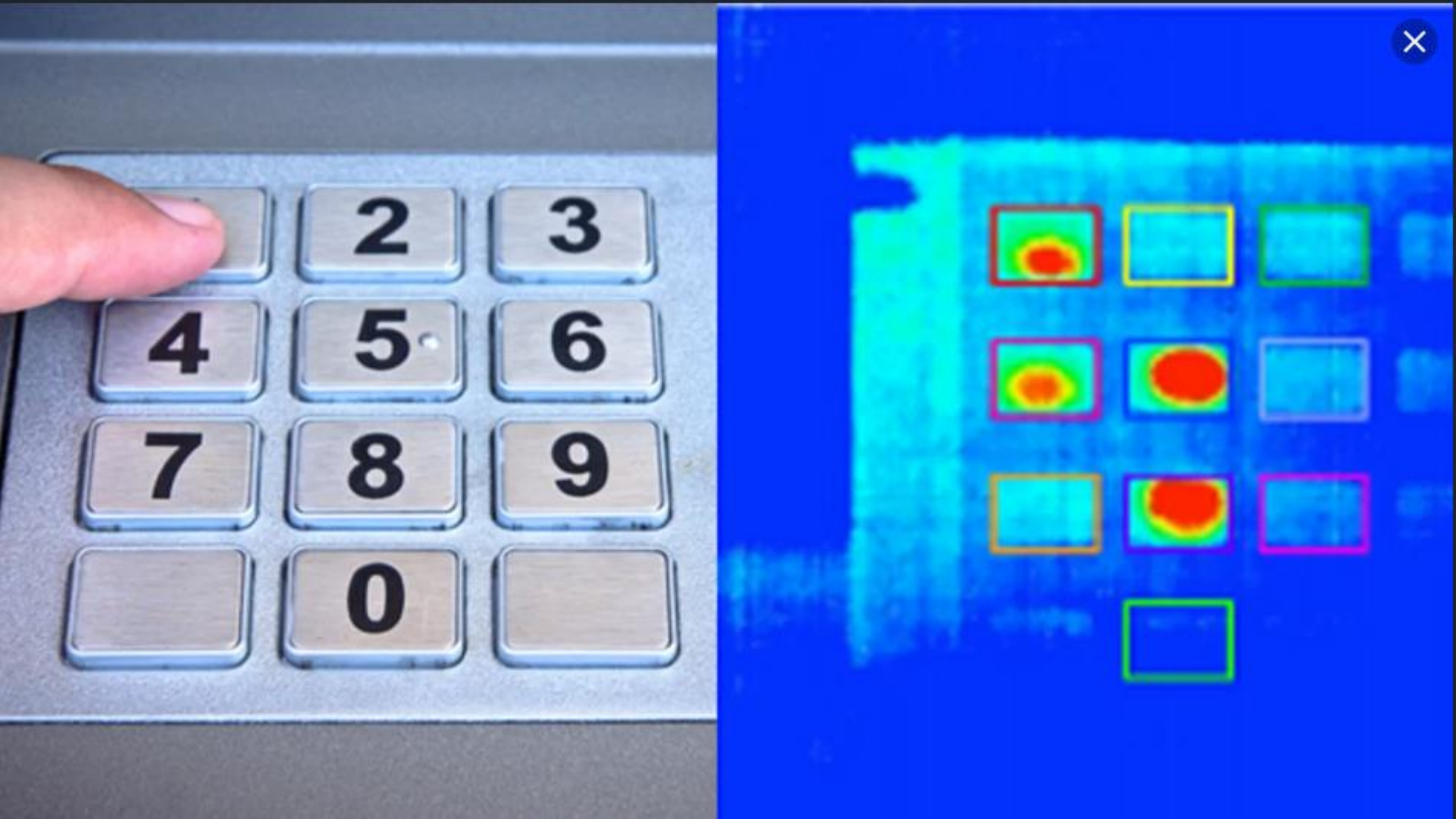
Side Channels

- Uses the byproducts of system operation, to infer secret information;
- Take advantage of side effects, e.g., execution time, power consumption, etc;
- Victim leaks data accidentally ;
- Allow an attacker to infer information anonymously.

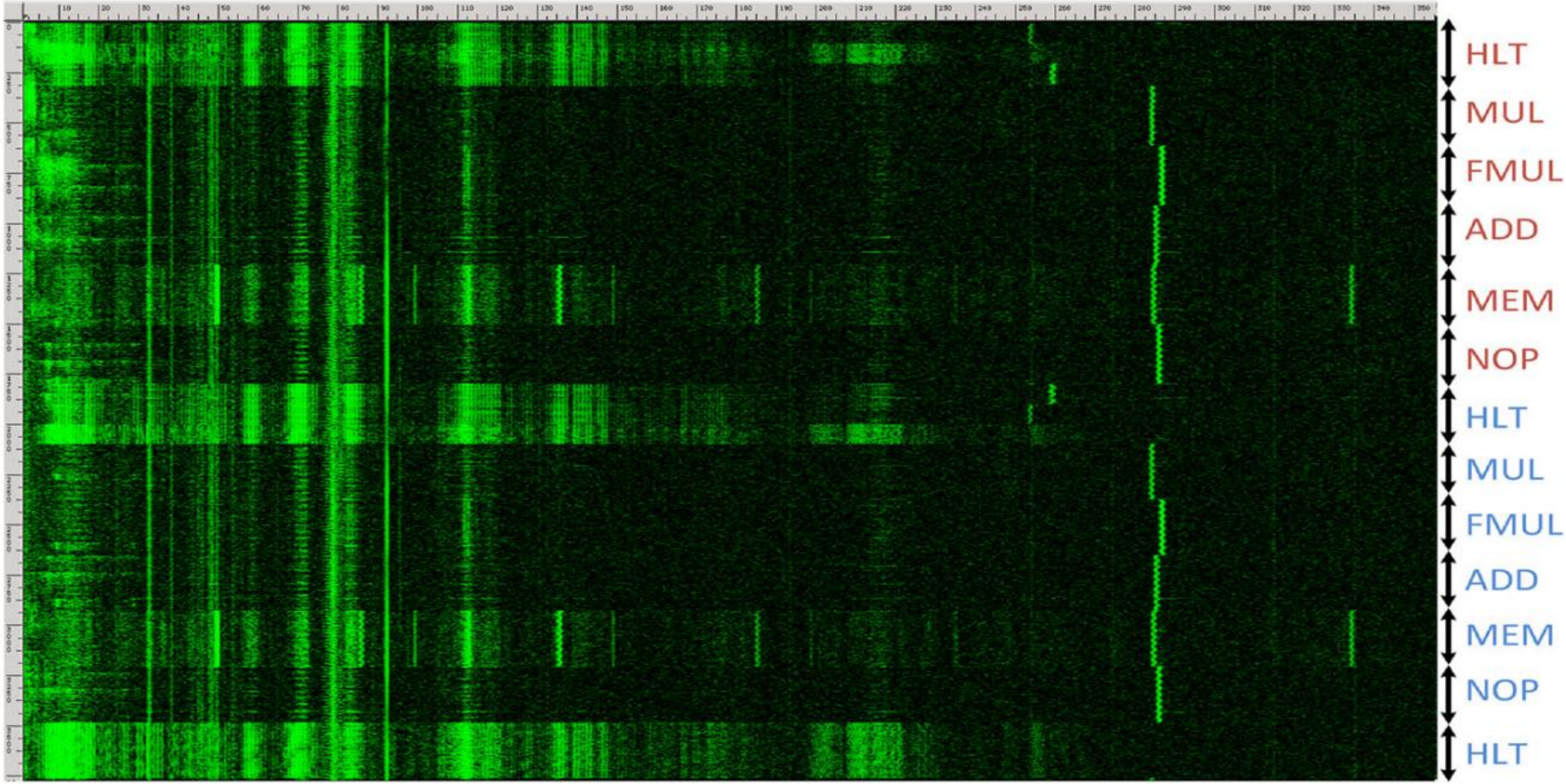
BURGER
KING
®

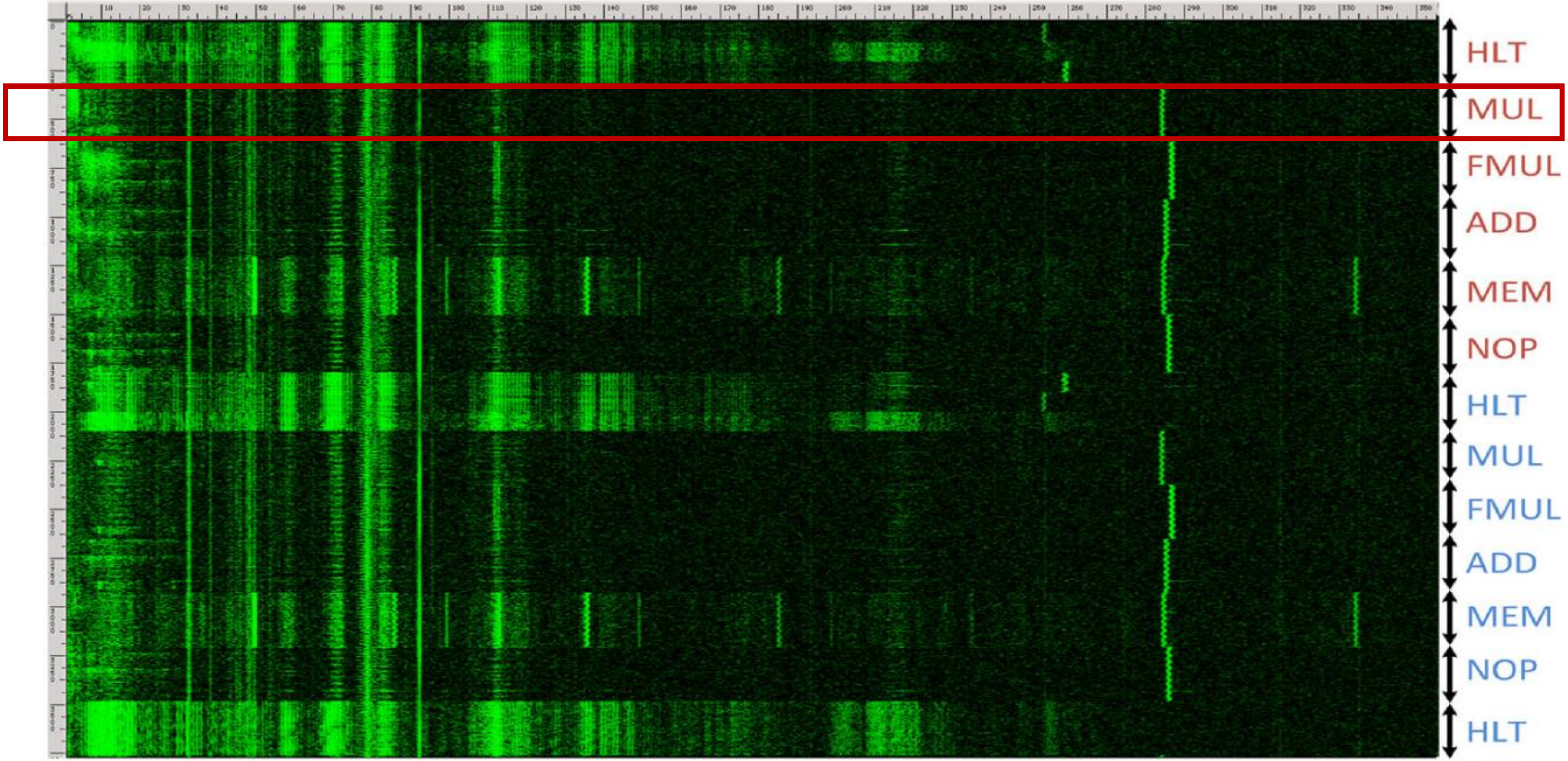


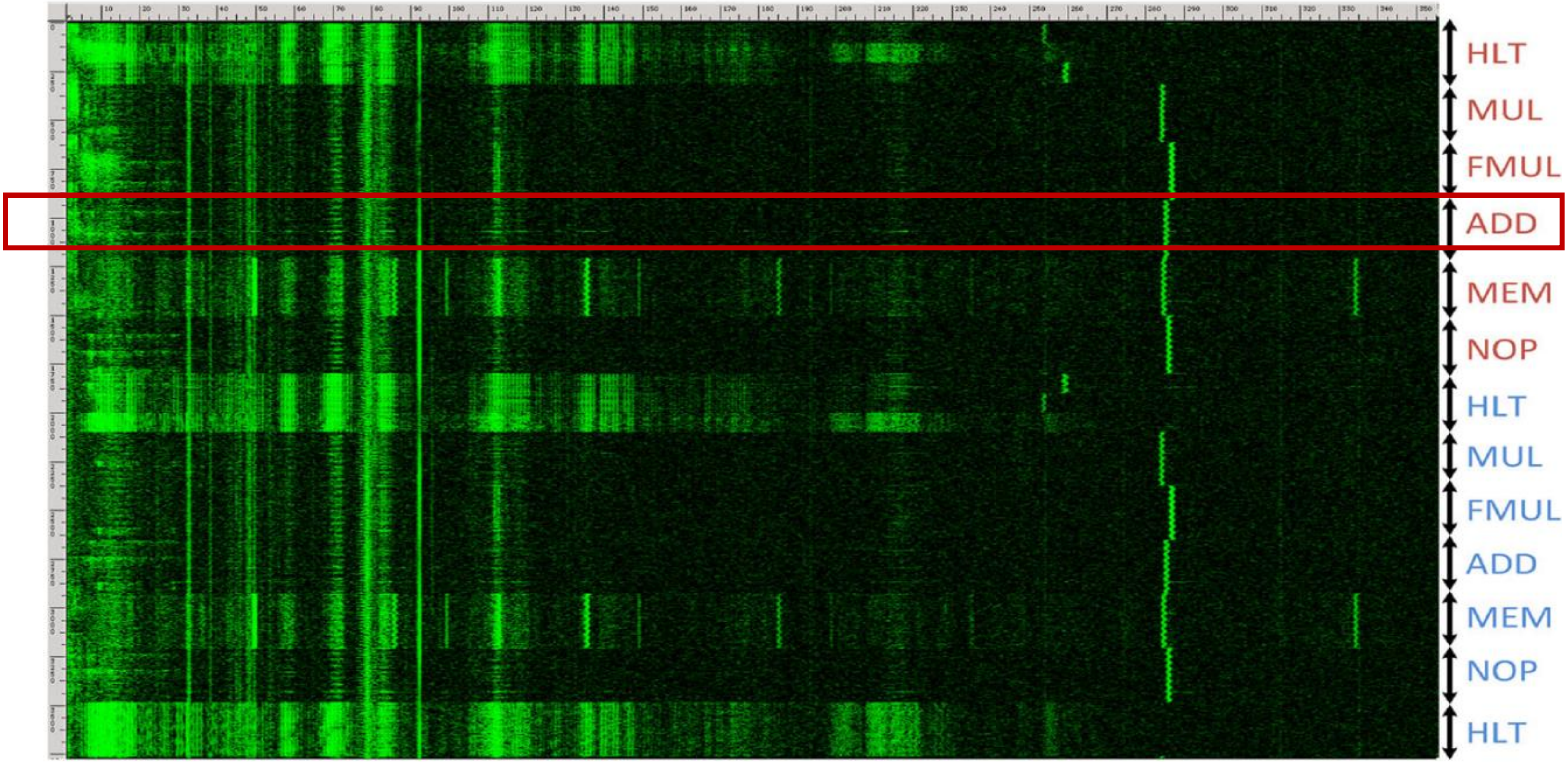
Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication by Abdelrahman and Khamis

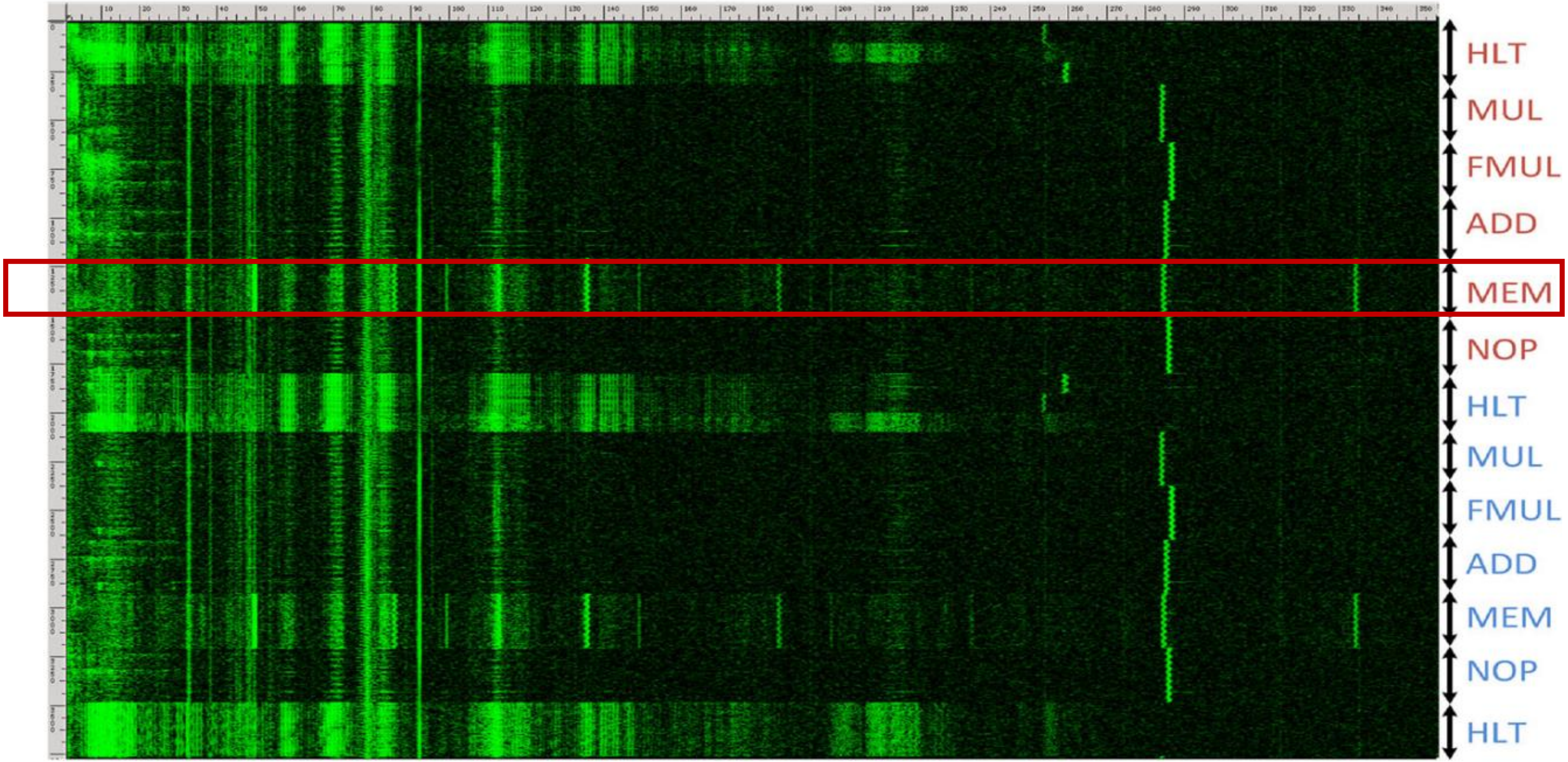

2
3
4
5
6
7
8
9
0

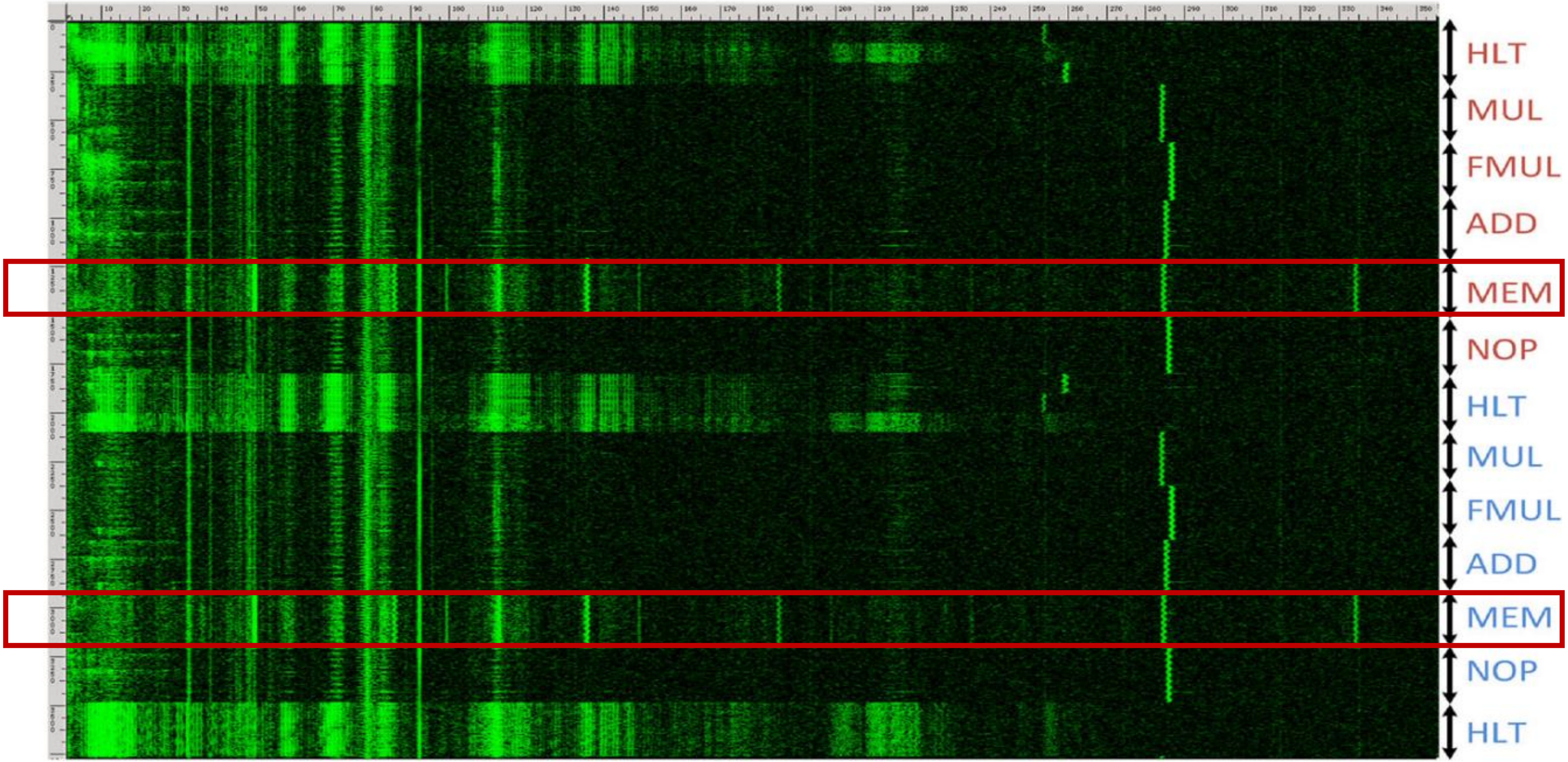
Acoustic Cryptanalysis
by Daniel Genkin


10
20
30
40
50
60
70
80
90
100
110
120
130
140
150
160
170
180
190
200
210
220
230
240
250
260
270
280
290
300
310
320
330
340
350
HLT
MUL
FMUL
ADD
MEM
NOP
HLT
MUL
FMUL
ADD
MEM
NOP
HLT


HLT
MUL
FMUL
ADD
MEM
NOP
HLT
MUL
FMUL
ADD
MEM
NOP
HLT

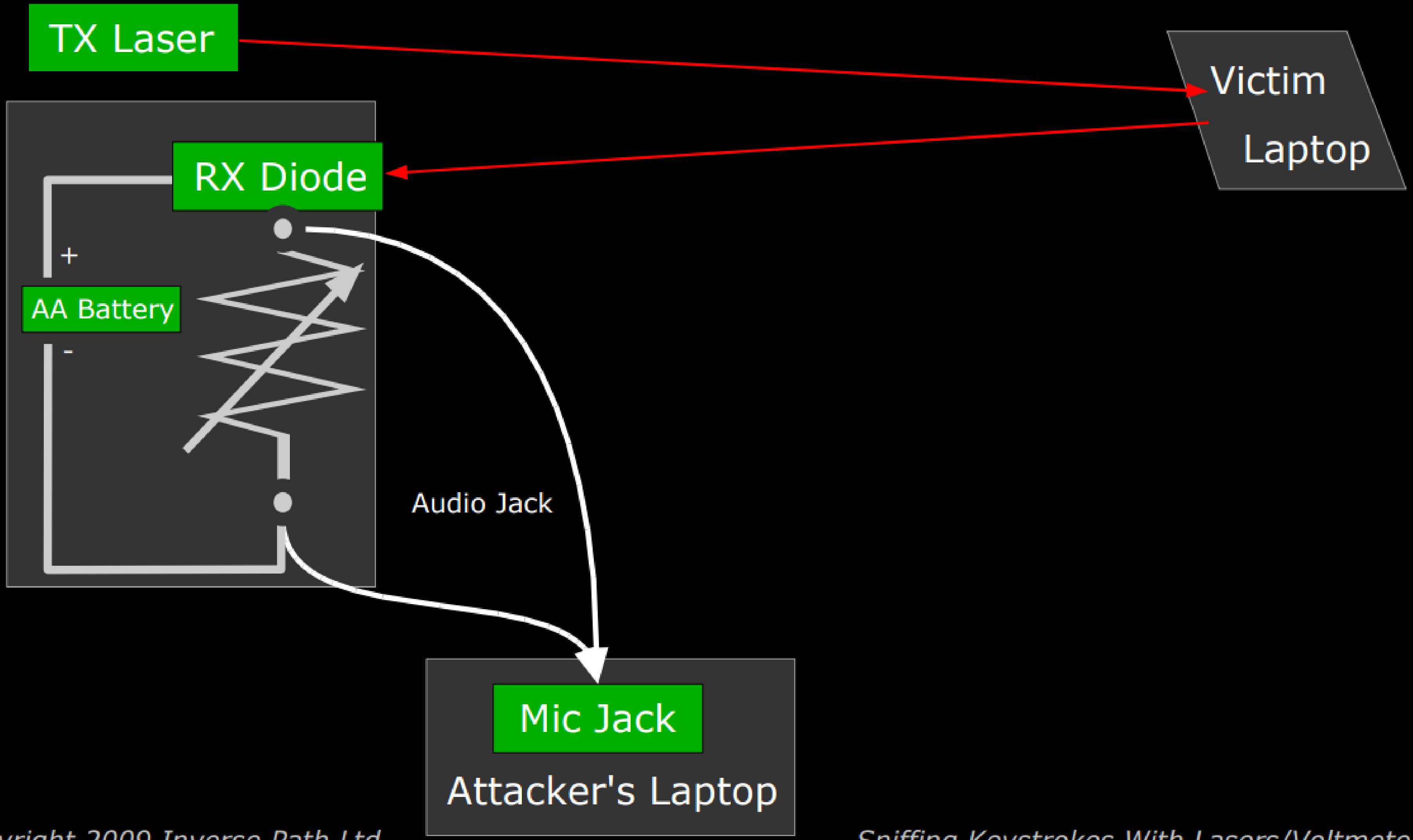

HLT
MUL
FMUL
ADD
MEM
NOP
HLT
MUL
FMUL
ADD
MEM
NOP
HLT

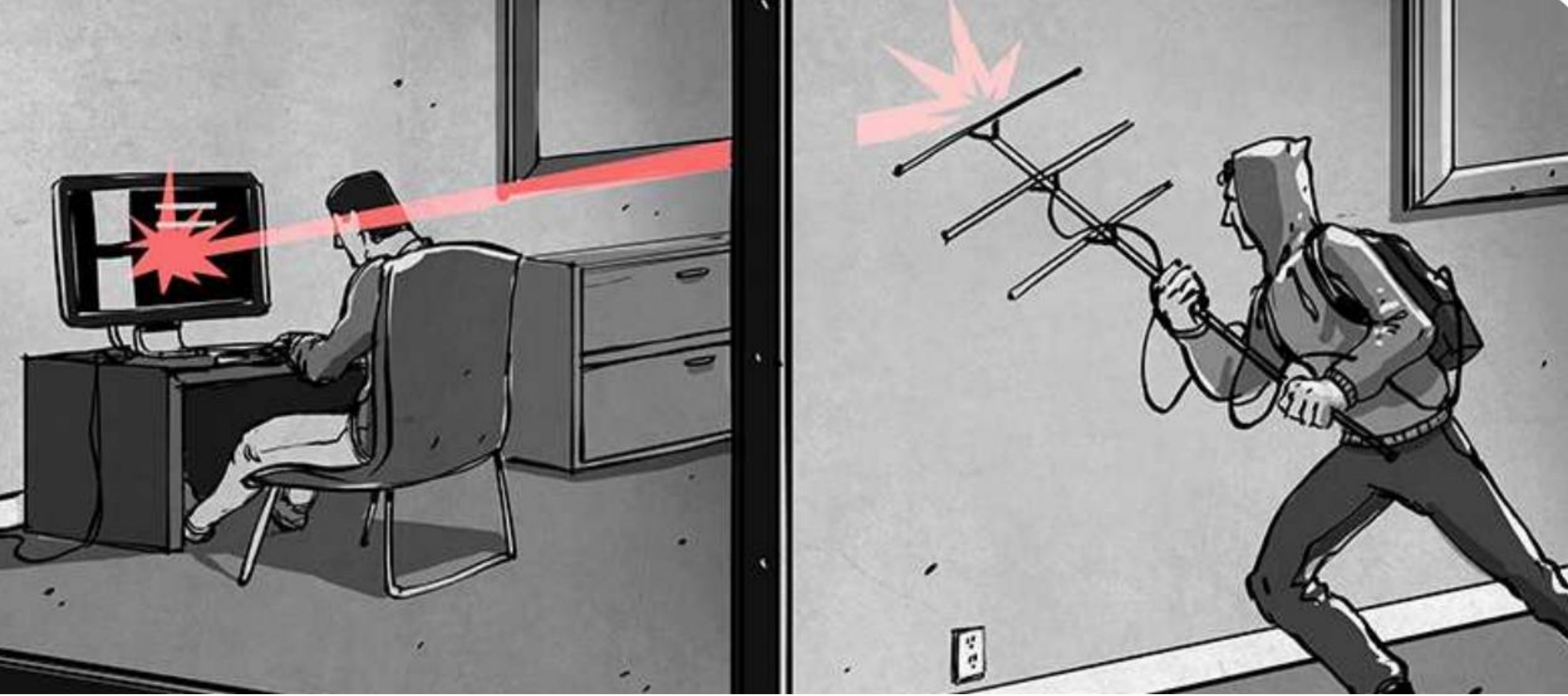

HLT
MUL
FMUL
ADD
MEM
NOP
HLT
MUL
FMUL
ADD
MEM
NOP
HLT


HLT
MUL
FMUL
ADD
MEM
NOP
HLT
MUL
FMUL
ADD
MEM
NOP
HLT

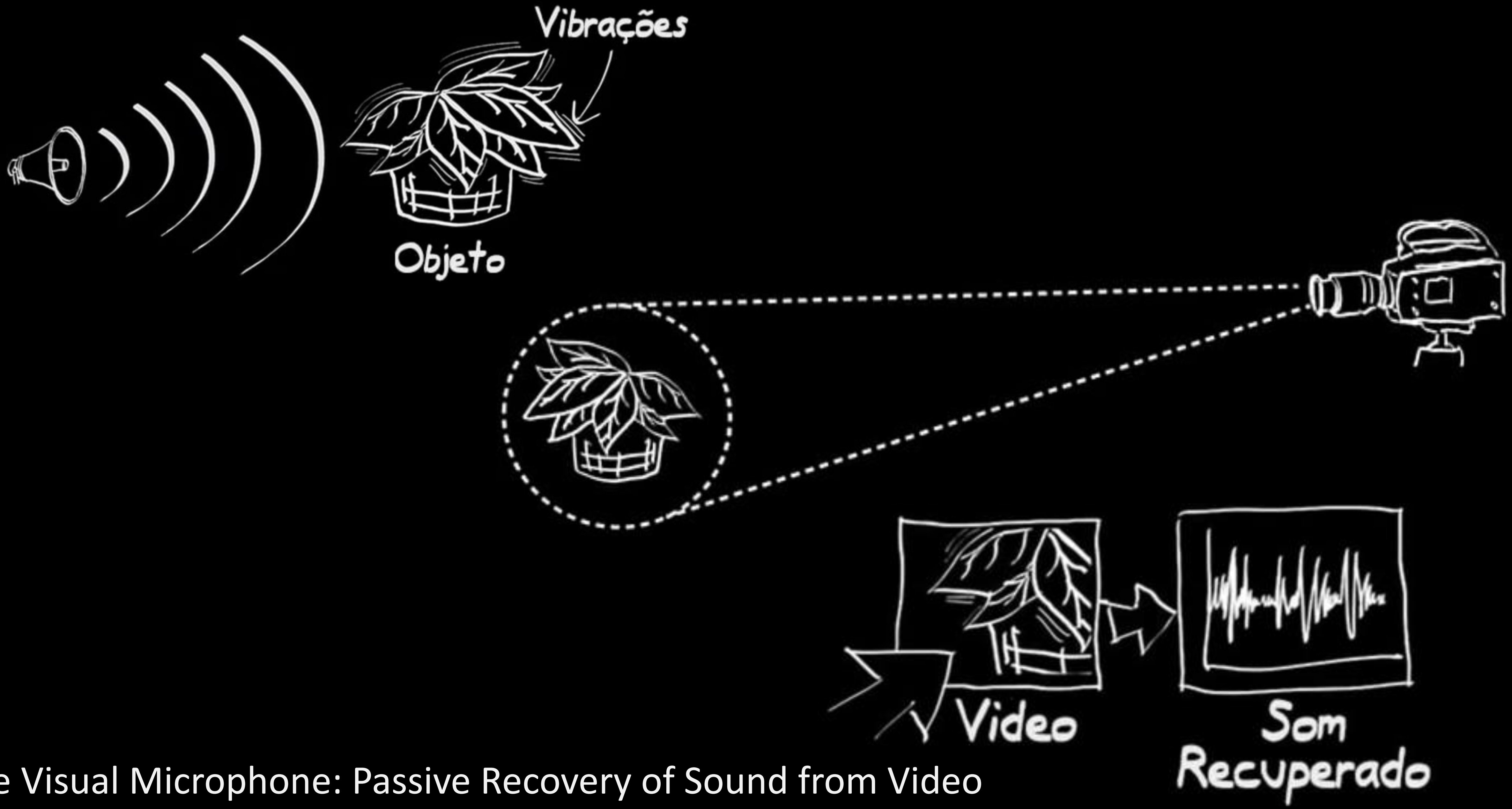
Sniffing Keystrokes With Lasers/Voltmeters

by Andrea Barisani and Daniele Bianco

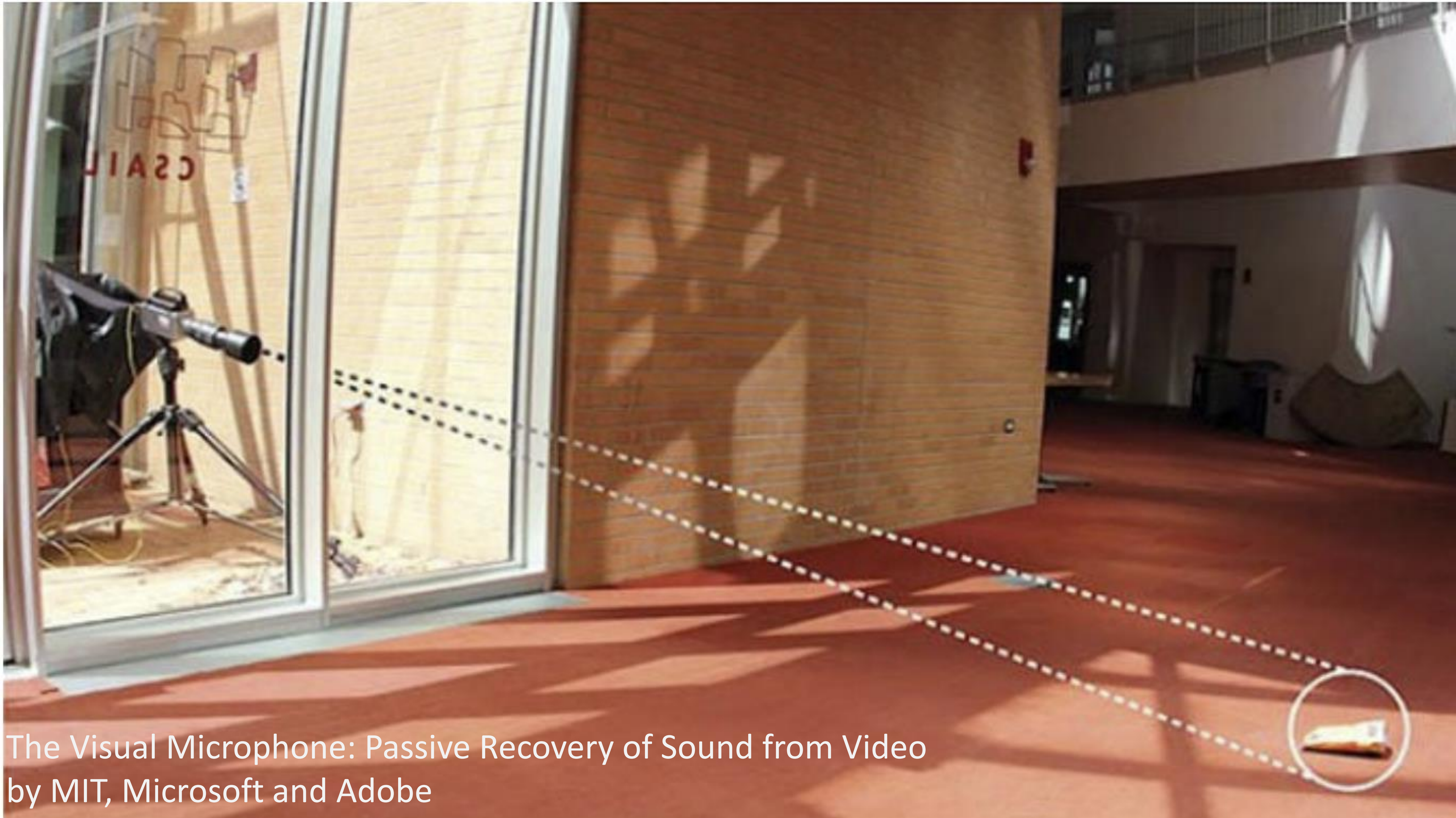

TX Laser
Victim
Laptop
RX Diode
+
AA Battery
-
Audio Jack
Mic Jack
Attacker's Laptop



TEMPEST attacks against AES by Craig Ramsay



The Visual Microphone: Passive Recovery of Sound from Video
by MIT, Microsoft and Adobe



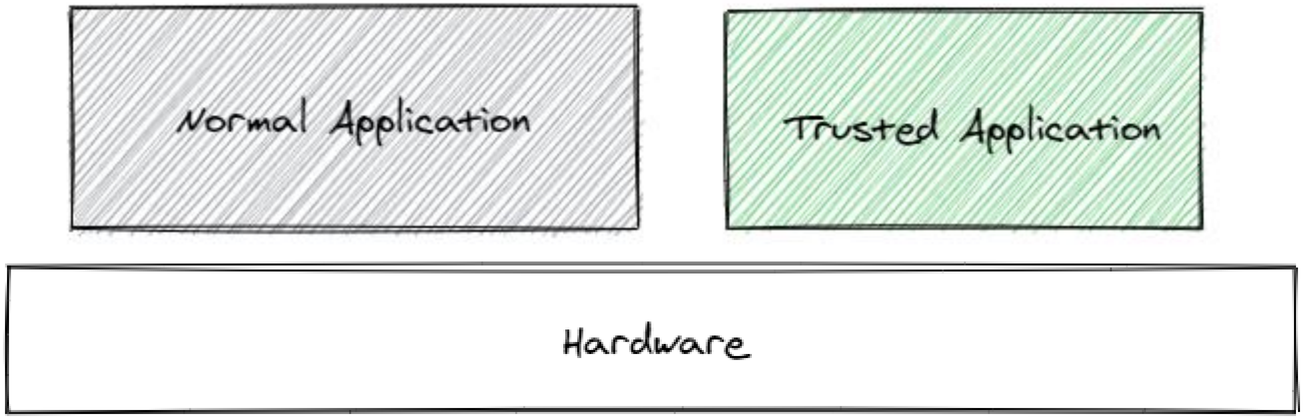
The Visual Microphone: Passive Recovery of Sound from Video
by MIT, Microsoft and Adobe

SOFTWARE-BASED SIDE CHANNELS

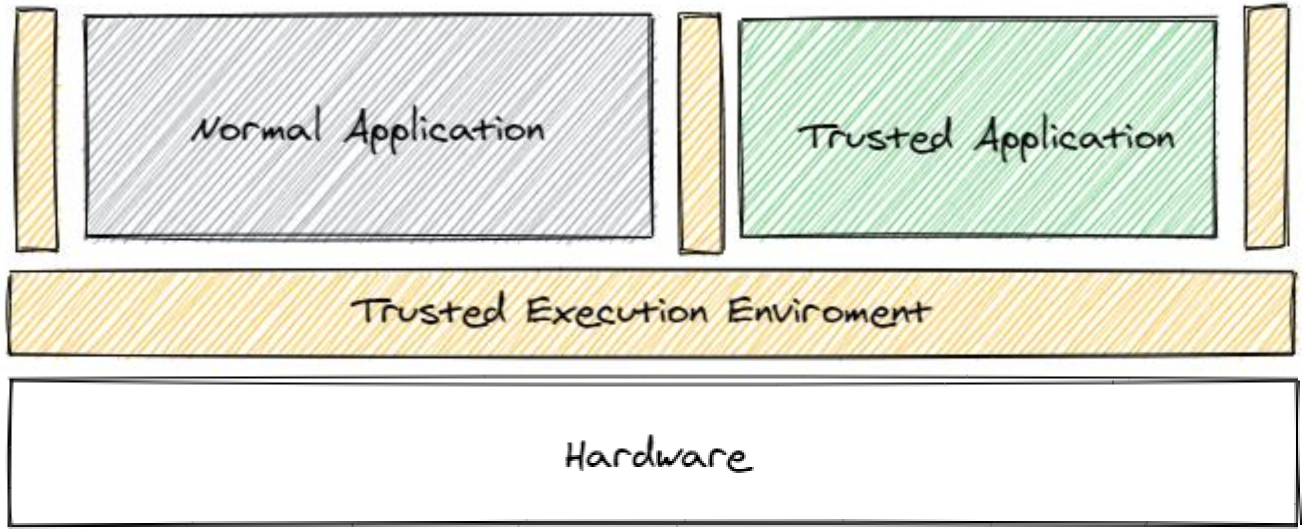
SOFTWARE SIDE CHANNELS

Hardware

SOFTWARE SIDE CHANNELS

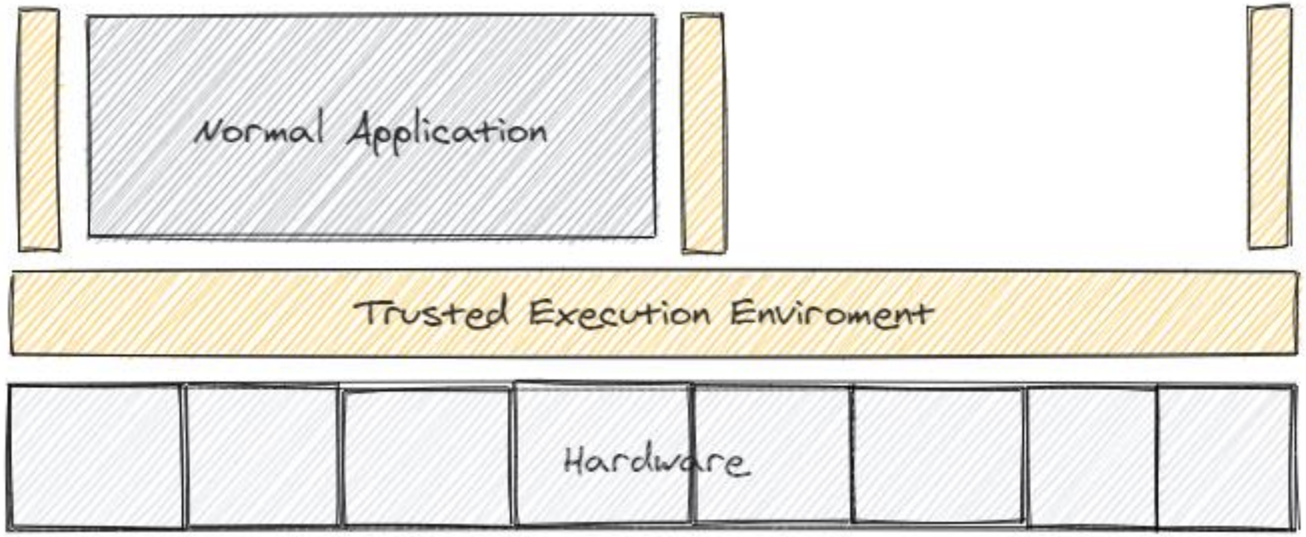


SOFTWARE SIDE CHANNELS

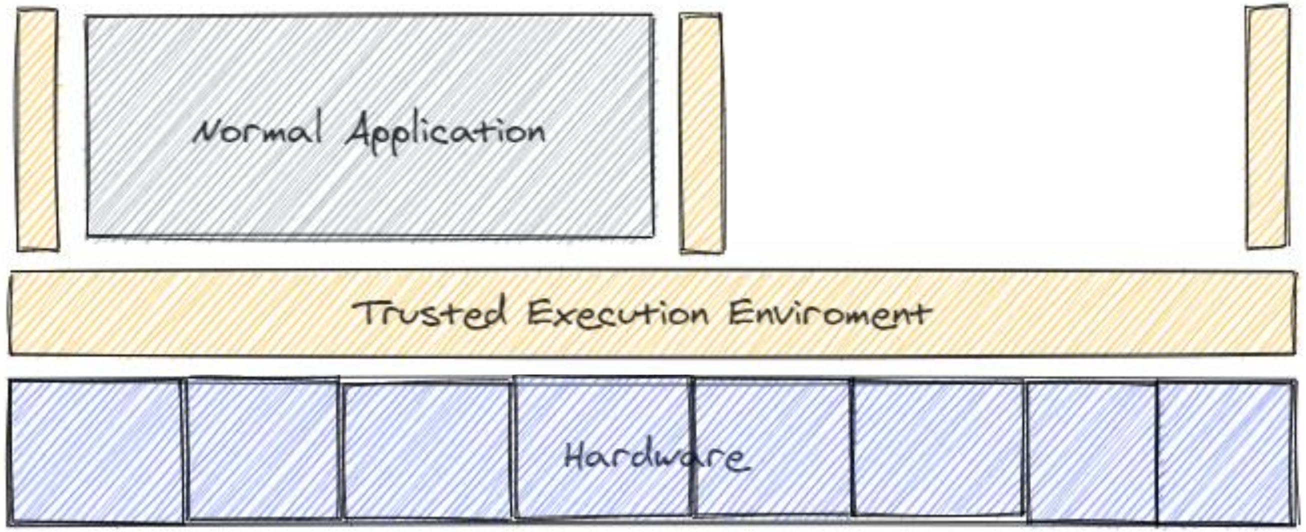


SOFTWARE SIDE CHANNELS

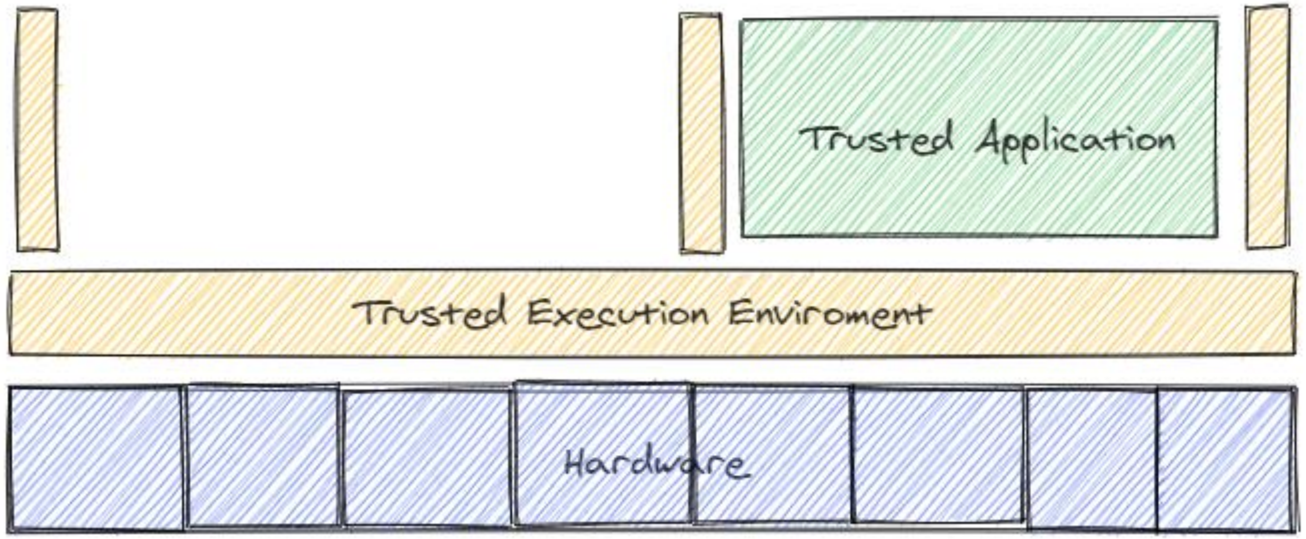
SOFTWARE SIDE CHANNELS



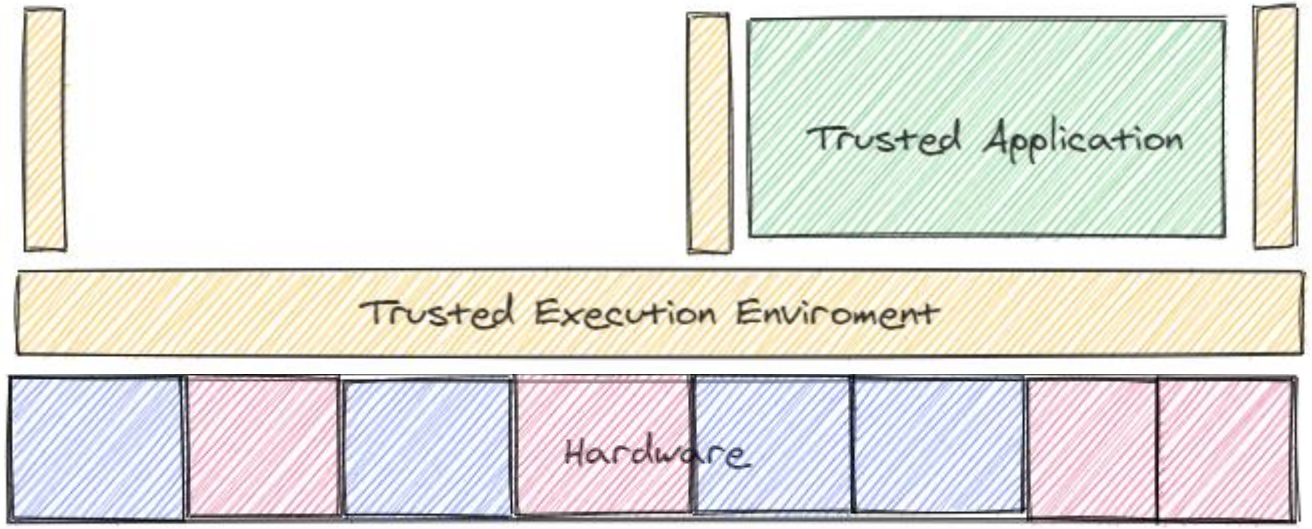
SOFTWARE SIDE CHANNELS



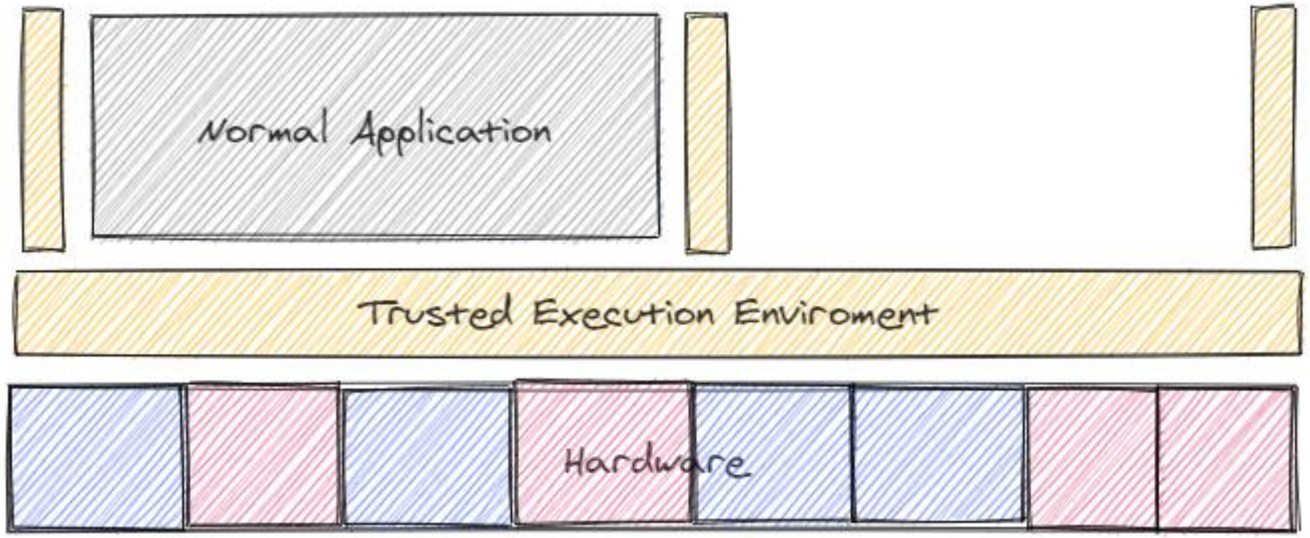
SOFTWARE SIDE CHANNELS



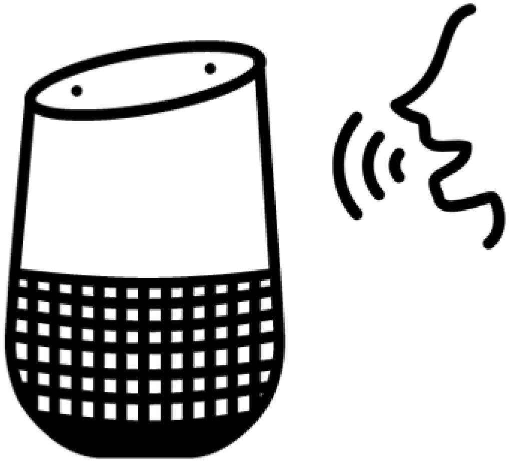
SOFTWARE SIDE CHANNELS

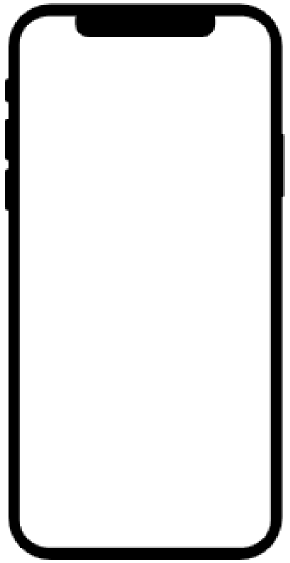


SOFTWARE SIDE CHANNELS

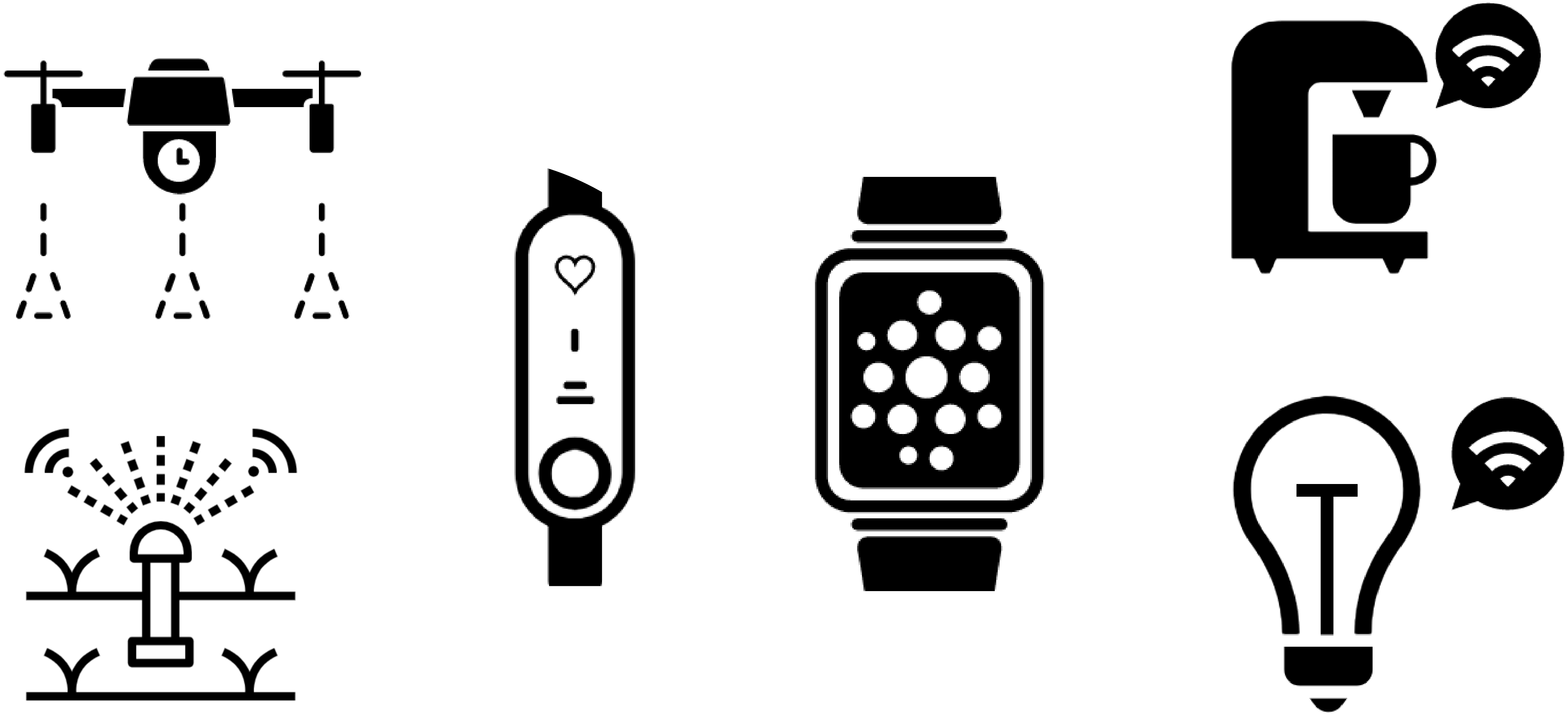


High-end devices





Low-end devices



PhD MAIN GOALS

This work aims at understanding and mitigating microarchitectural side-channels on low-end IoT devices.

Goal 1

- Build **knowledge** over the main class of **microarchitectural attacks** and existing countermeasures, as well as develop a **threat model for low-end IoT** devices.

PhD MAIN GOALS

This work aims at understanding and mitigating microarchitectural side-channels on low-end IoT devices.

Goal 1

- Build **knowledge** over the main class of **microarchitectural attacks** and existing countermeasures, as well as develop a **threat model for low-end IoT** devices.

Goal 2

- Understanding which **microarchitectural side-channels** affecting Intel and Arm high-end computing platforms may **span to existing low-end MCUs**.

PhD MAIN GOALS

This work aims at understanding and mitigating microarchitectural side-channels on low-end IoT devices.

Goal 1

- Build **knowledge** over the main class of **microarchitectural attacks** and existing countermeasures, as well as develop a **threat model for low-end IoT** devices.

Goal 2

- Understanding which **microarchitectural side-channels** affecting Intel and Arm high-end computing platforms may **span to existing low-end MCUs**.

Goal 3

- Unveiling new software-based microarchitectural attacks for low-end MCUs.

PhD MAIN GOALS

This work aims at understanding and mitigating microarchitectural side-channels on low-end IoT devices.

Goal 1

- Build **knowledge** over the main class of **microarchitectural attacks** and existing countermeasures, as well as develop a **threat model for low-end IoT** devices.

Goal 2

- Understanding which **microarchitectural side-channels** affecting Intel and Arm high-end computing platforms may **span to existing low-end MCUs**.

Goal 3

- Unveiling new software-based microarchitectural attacks for low-end MCUs.

Goal 4

- Designing and implementing **mitigation mechanisms** for single- and multi-core MCUs by (i) exploring commercial off-the-shelf **(COTS) hardware components** and (ii) by exploring modern free and **open processor architectures** (i.e, RISC-V).

PROPOSTA DE DISSERTAÇÃO

Tema: Desenvolvimento de uma ferramenta para automatização, benchmark e análise de canais microarquiteturais em dispositivos low-end.

Area: Segurança

Vão adquirir conhecimento em:

- Ataques Microarquiteturais (e.g., cache side channel..)
- Microarquiteturas de computadores (cache, MPU, TZ...etc)
- Modelos de ameaça (aka threat models)
- Arquiteturas de segurança (i.e., TEEs)
- Vão ter de lidar com várias placas, o que vos vai dar traquejo no geral.

THANKS!

Cristiano Rodrigues

cris96r@gmail.com