Automated hardware malware analysis
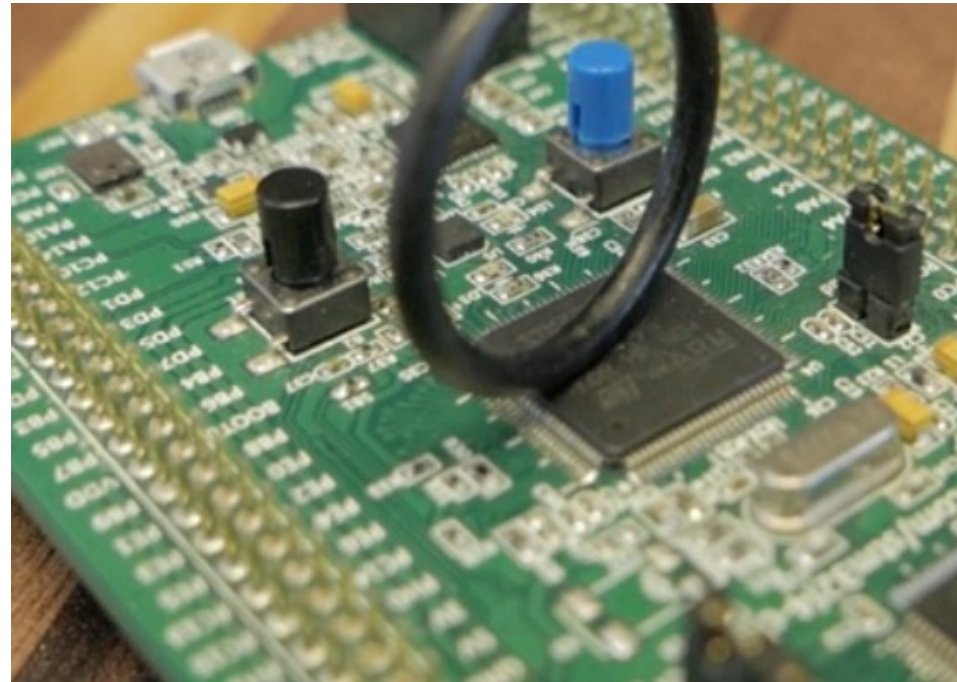
Matthieu Mastio　　　　　　　　**17/05/2019**
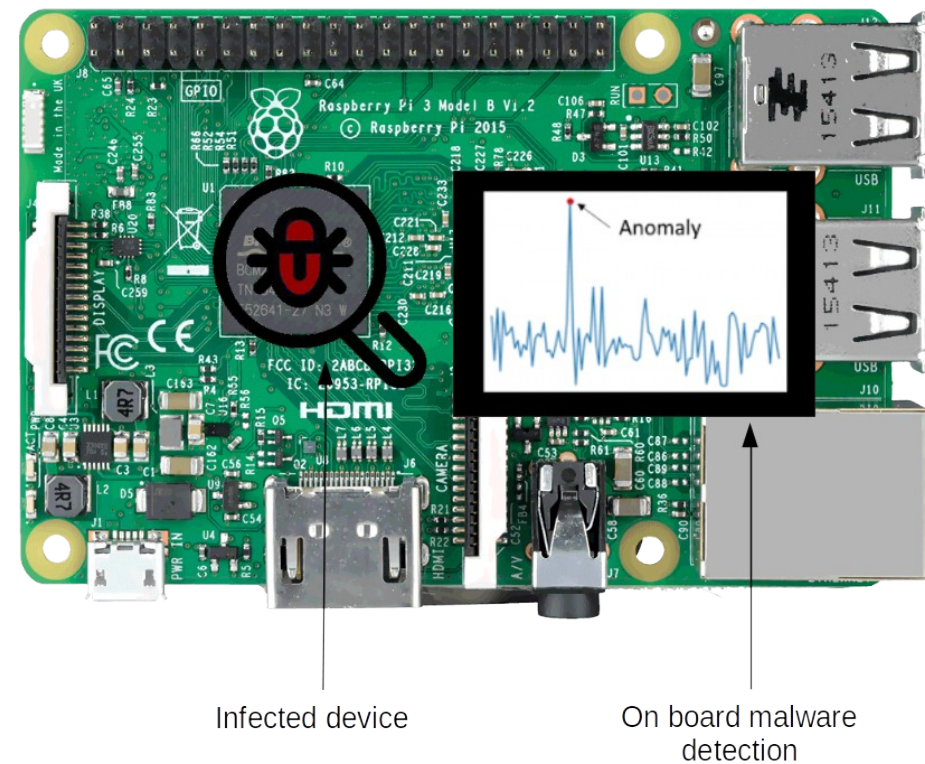
What is side channel analysis?
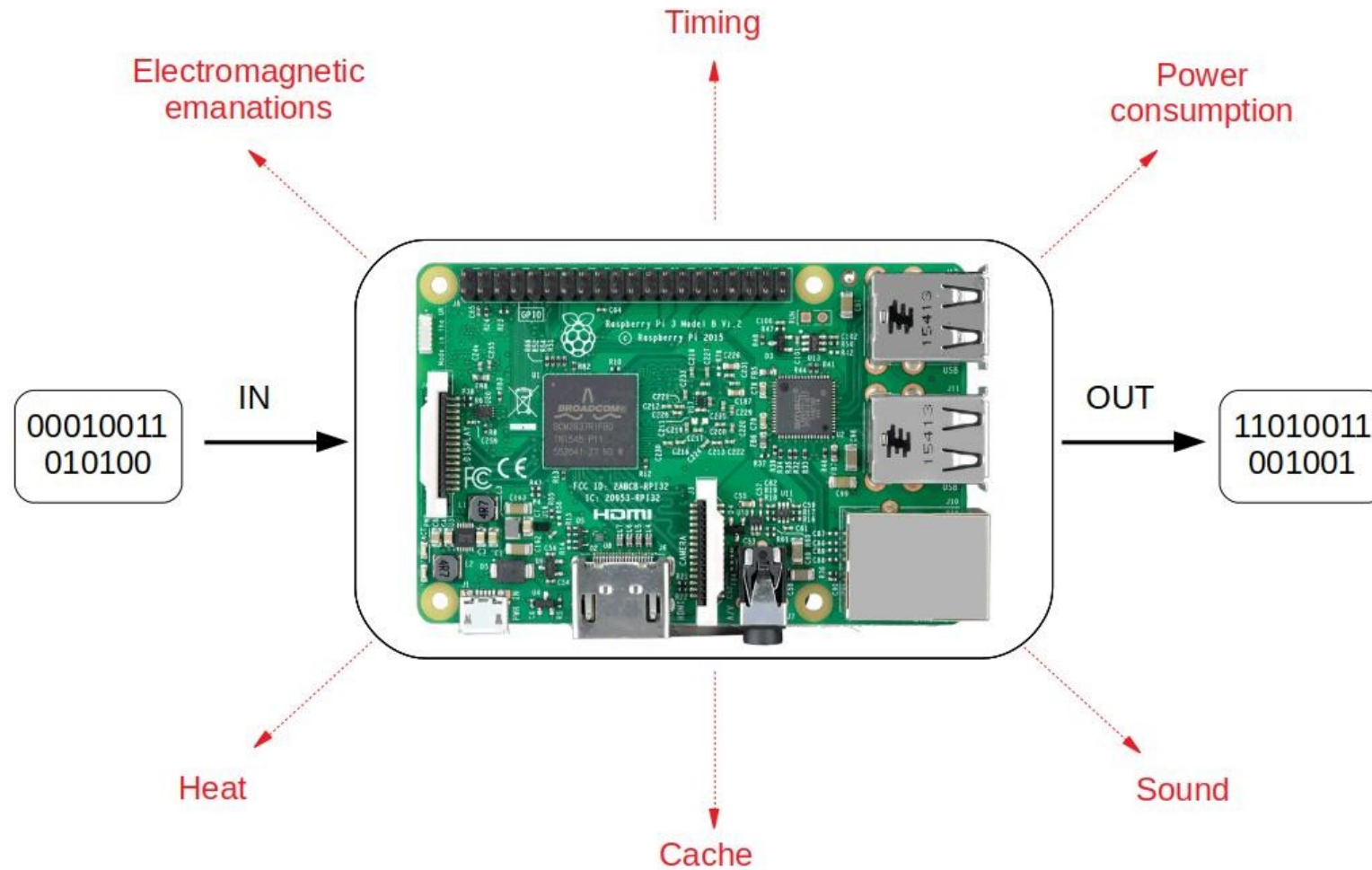
Side-channel attacks

- Power consumption and electromagnetic emanation (inference of cryptographic keys)

- Acoustic (sounds produced by keyboard to log the typed keys)

- Cache (Spectre,Meltdown)

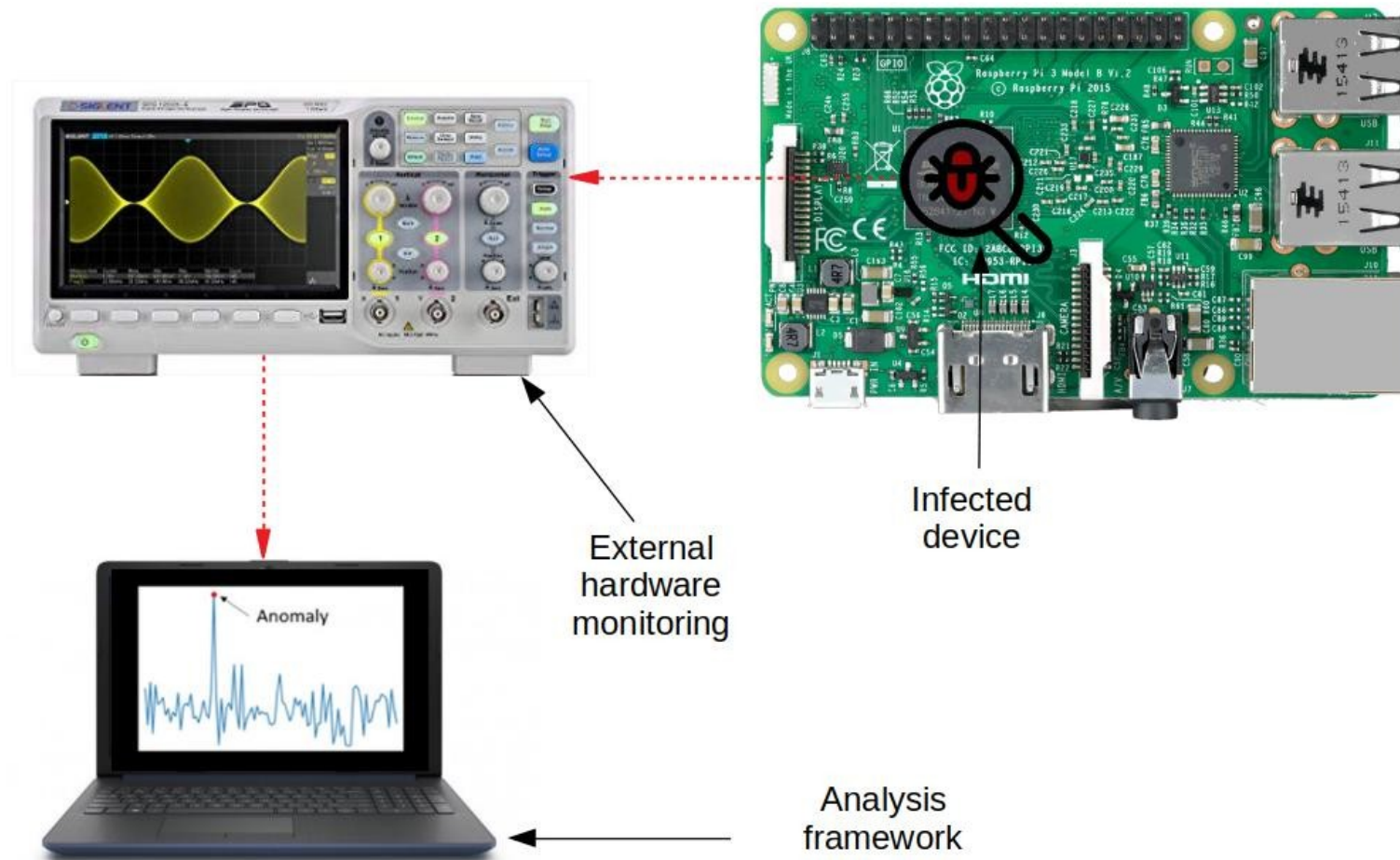# Traditional malware detection
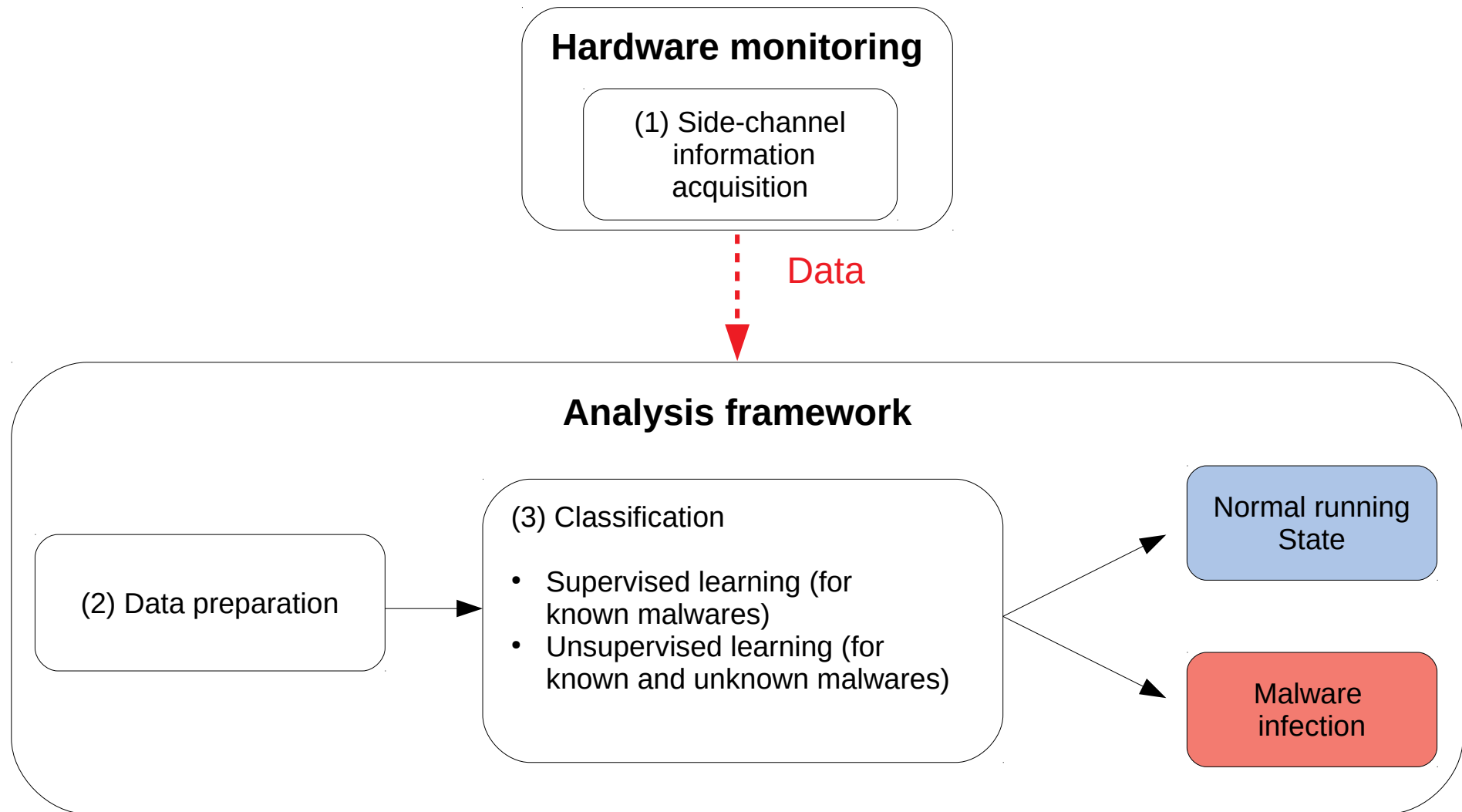
- Signature-based

- Behavior-based

- Specification-based

Anomaly

Infected device

On board malware detection

Side-channel malware detection

External hardware monitoring

Infected device

Anomaly

Analysis framework

AHMA Framework

Hardware monitoring

(1) Side-channel information acquisition

Data

Analysis framework

(2) Data preparation

(3) Classification

- Supervised learning (for known malwares)
- Unsupervised learning (for known and unknown malwares)

Normal running State

Malware infection

Researchers

- Annelie Heusser : *Researcher in TAMIS*

- Duy Phuc Pham : *PhD student in TAMIS*

- Matthieu Mastio : *Post-Doc in TAMIS*

ANR-18-CE39-0001

Any question?

Matthieu Mastio

17/05/2019