# Research for a new solution for the detection of malwares in IoT/IIoT devices

**POLYCHRONOU Nikolaos-foivos**, THEVENON Pierre-henri, PUYS Maxime,
Univ. Grenoble Alpes, CEA-Leti, Minatech Campus, F-38054 Grenoble, France
BEROULLE Vincent
Univ. Grenoble Alpes, Grenoble INP, LCIS, 26000 Valence, France

## Résumé

*Internet of Things (IoT) and Industrial IoT (IIoT) devices share a big part in the market of computational devices. These mostly low cost devices lack security features, which makes them vulnerable to multiple malware families. There exist solutions for the detection of malware in IoT/IIoT systems. However, these solutions have multiple disadvantages, and hardware or software vendors do not finally use them to protect their systems.*

*This thesis aims to study the disadvantages of the proposed solutions, and propose a new solution that can be implemented in resource constraint environments such as the IoT devices.*

## 1 Malware detection

In the literature, we can find three basic ideas for the detection of malware. These categories are antimalware, Control/Data Flow Integrity (CFI). Hardware Performance Counters (HPCs) based solutions. Antimalware relies in comparing the signatures of files or code with known malware signatures. This method can only detect malware after the malwares infected multiple devices and we store their signatures. CFI verifies that the execution path complies with the statically computed control-flow graph. This solution introduces memory overhead due to the need to store the control flow graphs and performance overhead due to the need to verify each branch instruction before execution. HPC-based solutions extract information from special core resisters that count events specific to the hardware components. Monitoring the values of these special core registers and by using Machine Learning (ML) we can learn the execution patterns of malware and normal applications, as we can see in figure 1 the execution trace of the Rowhammer attack.

### a. Thesis contributions

During our thesis, we experimented with different malware families. In the beginning of this thesis, we focus on Software Attacks Targeting Hardware Vulnerabilities (SATHV). This set of attacks includes attacks such as Cache Side Channel (CSCA), Meltdown, Spectre, Rowhammer, Direct Memory Access attacks. These attacks are particularly dangerous as the can be performed from software and by using a side channel they can extract sensitive information. For example, CSCA is used to find the secret byte of an AES OpenSSL implementation. Meltdown can be used to read private information that a normal program is restricted to access. Due to the severity of the aforementioned attacks, and to address limitations of proposed SOTA techniques, we experimented with the development of a new detection mechanism. We proposed a detection mechanism implemented in software [1,2] to detect SATHV. MaDMAN relies in a simple ML algorithm to detect SATHV. As MaDMAN is implemented in software, which makes MaDMAN vulnerable to software attacks, the future works focuses in the implementation of MaDMAN in hardware. Moreover, MaDMAN targets to secure resource constraint environments. For our future work, we study the integration of MaDMAN in hardware, with the goal of minimizing the resource usage, memory overhead, and energy consumption.

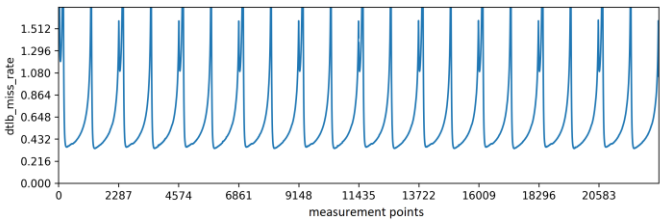


**Figure 1 Rowhammer attack execution trace**

## References

[1] Polychronou, Nikolaos Foivos, et al. "MaDMAN: Detection of Software Attacks Targeting Hardware Vulnerabilities." 2021 24th Euromicro Conference on Digital System Design (DSD). IEEE, 2021.

[2] POLYCHRONOU, Nikolaos Foivos, et al. "Securing iot/iiot from software attacks targeting hardware vulnerabilities." 2021 19th IEEE International New Circuits and Systems Conference (NEWCAS). IEEE, 2021.