Analyse automatique de logiciel malveillant au niveau matériel

Automated Hardware Malware Analysis

Soumission: Début de projet

1 Details of the project

- **le nom et l'acronyme du projet**: AHMA, Automated Hardware Malware Analysis
- **l'identité et l'affiliation du porteur** : Annelie Heuser, CNRS researcher, Univ Rennes 1, Inria, CNRS, IRISA, Rennes
- **le consortium** : Univ Rennes 1, Inria, CNRS, IRISA, Rennes
  positions funded by the project: 1 PostDoc, 1 PhD student
- **l'instrument de financement** : ANR JCJC
- **les dates de début et de fin de projet** : scientific start of the project: March 2019, duration: 42 month
- **la plage de TRL associée aux innovations** : 3-4 (proof-of-concept will be experimentally demonstrated using a prototype)

2 Summary

The Internet of Things (IoT) will influence the majority of our daily life's infrastructure. While efficiency and diffusion of IoT are increasing, security threats are becoming a far-reaching problem. Here we are particularly concentrating on ensuring the security of IoT nodes against malware threats, which may seriously disrupt daily life and economic activity or even reveal privacy critical data of users. As state-of-the-art software monitoring techniques (static or dynamic) can still be circumvented by sophisticated attackers, we propose an automated hardware malware analysis (AHMA) framework that is non-intrusive and cannot easily be controlled or hidden by the malware attacker. AHMA uses side-channel information of the underlying hardware IoT device to detect if a device is infected by malware (mutated or even unknown) or in its typical running state. Our novel framework is of high importance and impact for industries, and thus for users benefiting from increasing protection.

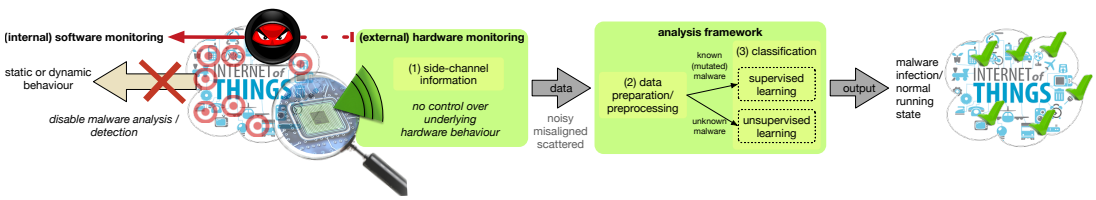

Figure 1: Overview of AHMA framework

The talk will be given in French.