Analyse automatique de logiciels malveillants au niveau matériel

AHMA

anr agence nationale de la recherche

Appel : AAPG

Année : 2018

Instrument : JCJC

Contact : damien.marion@irisa.fr

COORDINATEUR : Annelie Heuser **PARTENAIRES : CNRS, IRISA**

Résumé :
À l'heure où l'Internet des objets (IoT) est au cœur de l'infrastructure de nos vies quotidienne. Nous proposons une nouvelle méthode robuste et non intrusive basée l'analyse des canaux auxiliaires permettant de sécuriser leur fonctionnement.

CONTEXTE ET OBJECTIFS

L'IoT n'est qu'à ses début, mais compte déjà plus de 40 milliards d'appareils connectés en 2021 et l'on estime que leur nombre atteindra 125 milliards d'ici 2030.

Ces objets, le plus souvent faiblement sécurisé sont des cibles de choix pour des attaques à base de logiciels malveillants (Mirain, Gonnacry...).

Nous avons développé un framework d'acquisition et d'analyse automatisé, non intrusif et indétectable par les logiciels malveillant : *https://github.com/ahma-hub*.

MÉTHODOLOGIE ET RÉSULTATS

Analyse des canaux auxiliaires. Tout système électronique produit des fuites physique résiduelles lors de son fonctionnement. Notre approche se base sur l'analyse de ces productions résiduelles, appelée canaux auxiliaires, afin de détecter la présence d'un logiciel malveillant sur le système. Notre étude c'est concentré sur des fuites électromagnétique.

Fig. 1 : Équipement d'acquisition de fuite électromagnétique.

Apprentissage automatique. Les fuites d'information électromagnétique sont soumises à notre framework. Avant tout, nous utilisons des méthodes de pré-traitement sur ces données pour réduire la quantité de bruit qu'elles contiennent. Notre framework emploie ensuite différents algorithmes d'apprentissage automatique, supervisés et non supervisés, afin de déterminer, si les données mesurées sont issues d'un système infecté ou sain.

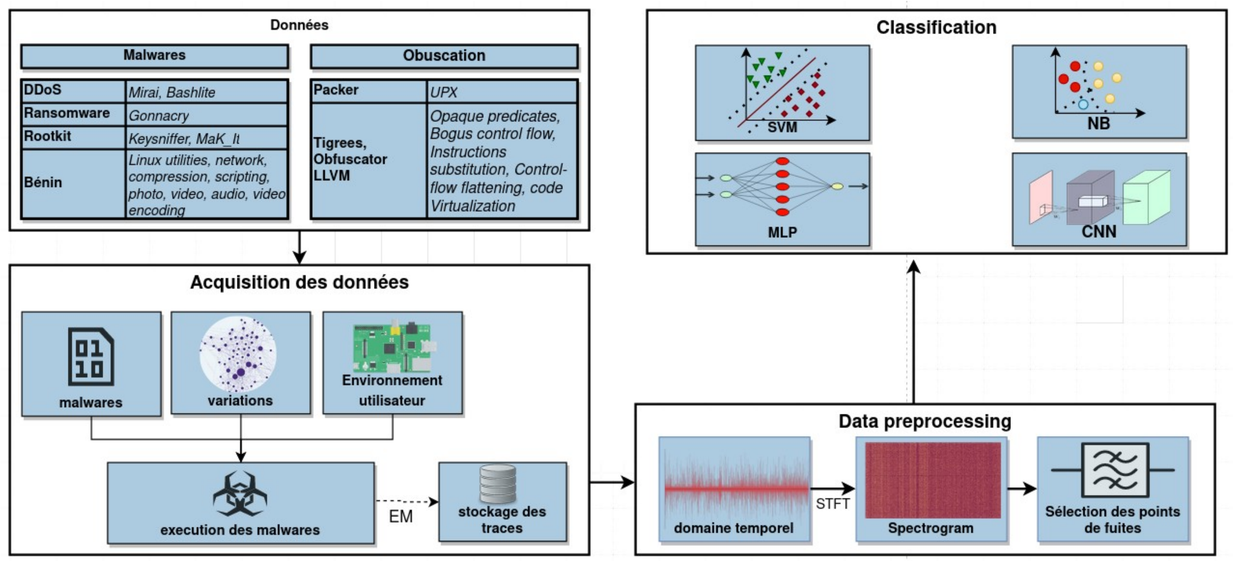

Fig. 2 : Étapes du framework AHMA .

Résultats majeurs du projet :

- Publication d'un article dans la conférence internationale ACSAC-2021 (rang A)
- Framework et donnés publié :
  - https://github.com/ahma-hub.
- Rayonnement médiatique :
  - *Detecting evasive malware on IOT devices using electromagnetic emanations*. The Hacker News, 03/01/2022.
  - *Raspberry Pi Can Detect Malware Using Electromagnetic Waves, Say Researchers*. Indian Times, 16/01/022.
  - *On peut détecter des malwares avec précision grâce... aux ondes électromagnétiques* . 01 net, 16/01/2022.

cnrs UMR IRISA