---- English version below -----

Offre de Thèse au sein du CEA Grenoble

DOMAINE DE RECHERCHE

Cybersécurité : hardware et software / Défis technologiques

INTITULÉ DU SUJET

Méthodes d'apprentissage profond non supervisé pour les attaques par canaux auxiliaires

RÉSUMÉ DU SUJET

Les produits sécurisés grâce à des mécanismes cryptographiques embarqués, par exemple les cartes à puce, peuvent être vulnérables aux attaques par canaux auxiliaires. Ces attaques se basent sur l'observation de certaines quantités physiques mesurées pendant l'activité du dispositif, comme la consommation de puissance, le rayonnement électromagnétique, le temps écoulé, … dont la variation provoque une fuite d'information. Ces fuites d'information, dûment analysées, peuvent permettre à un attaquant de remonter à des données sensibles, comme les clés secrètes des algorithmes cryptographiques, et donc de mettre en défaut la sécurité du dispositif.

Pour l'analyse des fuites d'information, récoltés sous forme de grandes bases de données de signaux de grande taille, les méthodes d'apprentissage profond sont aujourd'hui devenues incontournables. Depuis 2016 le sujet intéresse de plus en plus les chercheurs du domaine de la sécurité embarquée, qui constatent surtout l'efficacité de ces méthodes d'attaque dans le cadre des attaques profilées. Dans ce contexte l'attaquant a à disposition une base de données complètement maitrisée lui permettant une phase d'entrainement supervisé. Il s'agit du contexte le plus favorable pour l'attaquant.

Pour la mise en place de véritables attaques sur le terrain, ainsi que de plus en plus dans le cadre d'évaluation de systèmes sécurisés complexes, ce scenario n'est pas envisageable. Dans le vaste état de l'art des attaques non-supervisées les méthodes d'apprentissage automatique sont apparues depuis une dizaine d'années, les algorithmes de clustering en étant une partie qui a suscité beaucoup d'intérêt.

Aujourd'hui, le domaine de l'apprentissage profond fait évoluer les algorithmes de clustering, en s'appuient notamment sur les méthodes d' « embedding », c'est-à-dire de représentation des données dans un espace qui privilégie certaines relations « utiles ». Le domaine d'application principale de ces techniques est aujourd'hui la représentation des mots pour l'analyse des langages naturels : une représentation utile immergera les mots dans un espace où les mots du même champ sémantique sont à une faible distance.

L'objectif de cette thèse est étudier les techniques de « deep embeddings », évaluer leur adéquation avec les scénarios d'attaques non-supervisés, notamment dans le cadre des algorithmes

cryptographiques asymétriques à clé publique, formaliser une stratégie d'attaque performante basée sur ces techniques et en analyser en profondeur les propriétés.

FORMATION NIVEAU MASTER RECOMMANDÉ

Mathématiques appliquées, Machine Learning, Cryptologie, Informatique

INFORMATIONS PRATIQUES

Département Systèmes (LETI)
Service Sécurité des Systèmes Electroniques et des Composants
Centre d'Evaluation de la Sécurité des Systèmes d'Information
Centre : Grenoble
Date souhaitée pour le début de la thèse : 01/09/2020

PERSONNE À CONTACTER PAR LE CANDIDAT

Eleonora CAGLI
eleonora.cagli@cea.fr

CEA Grenoble
DRT/LETI/DSYS/SSSEC/CESTI
17 rue des Martyrs
38054 Grenoble

Téléphone : +33 4 38 78 31 31

UNIVERSITÉ / ÉCOLE DOCTORALE

Université de Lyon
Sciences, Ingénierie, Santé (EDSIS)

DIRECTEUR DE THÈSE

Lilian BOSSUET - https://perso.univ-st-etienne.fr/bl16388h/

---- English version -----

PhD position at CEA Grenoble

RECHERCHE DOMAIN

Cybersecurity : hardware and software / Technologic challenges

TITLE

Unsupervised deep learning methods for side-channel attacks

SUMMARY

Secure components exploiting embedded cryptographic mechanisms, for instance smart cards, may be vulnerable to the side-channel attacks. Such attacks are based onto the observation of some physical features measured during the device activity, such as power consumption, electromagnetic irradiation, execution time… the variation of these quantity may provoke an information leakage. A deep analysis of the leakage may lead an attacker to retrieve sensitive information, for instance the secret keys of the embedded cryptographic algorithms, and so to break the device security.

In order to analyze the leakages, which are typically collected as high-dimensional signals big datasets, the deep-learning methods are nowadays a privileged tool. Since 2016, the interest of embedded security researchers toward this topic grows very fast, especially because of the efficiency of these methods in the context of profiled attacks. In this context, the attacker has access to a second dataset, over which he has complete knowledge. This second dataset allows him to perform a preliminary supervised training phase. This context is the most advantageous for the attacker.

To setup the attacks on the field, for instance in the context of complex secure systems evaluation, this scenario is not available. In the wide state-of-the-art concerning non-supervised attacks, machine-learning techniques appeared about ten years ago. In particular clustering methods attracted considerable interest.

Today, the deep-learning research makes clustering algorithms evolve, in particular through “embedding” techniques. These techniques aim at represent data into a space that enhances certain “useful” relations among data. The principal application domain of these techniques today is the representation of words for the natural language analysis: a useful representation should embed words into a space where words belonging to the same semantic field are close to each other.

The goal of this research is studying “deep embedding” techniques, evaluating their suitability for non-profiled attack scenarios, in particular in the context of public key cryptographic algorithms, formalizing an efficient deep-clustering-based attack strategy and deeply analyzing its properties.

FORMATION NIVEAU MASTER RECOMMANDÉ

Applied Mathematics, Machine Learning, Cryptology, Informatics

PRATIC INFORMATIONS

Département Systèmes (LETI)
Service Sécurité des Systèmes Electroniques et des Composants
Centre d'Evaluation de la Sécurité des Systèmes d'Information
Centre : Grenoble
PhD begging date : 01/09/2020

IN ORDER TO CANDIDATE PLEASE CONTACT

Eleonora CAGLI
eleonora.cagli@cea.fr

CEA Grenoble
DRT/LETI/DSYS/SSSEC/CESTI
17 rue des Martyrs
38054 Grenoble

Téléphone : +33 4 38 78 31 31

UNIVERSITÉ / ÉCOLE DOCTORALE

Université de Lyon
Sciences, Ingénierie, Santé (EDSIS)

PhD SUPERVISOR

Lilian BOSSUET - https://perso.univ-st-etienne.fr/bl16388h/