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.

MASTER OF SCIENCE RECOMMENDED

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 starting 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/