Université de Rennes

Direction de la Recherche et de l'Innovation

Appel à projets - Année 2024

Contrats doctoraux «Ordinaires»

ECOLE DOCTORALE : Matisse **POLE DE RECHERCHE : Mathématique-Numérique**

Unité de recherche d'accueil

Unité de Recherche : IRISA

Equipe : WIDE

Encadrement

Directeur de thèse : Bromberg David **Unité de recherche** : IRISA

Employeur/Établissement d'origine : Université de Rennes 1

HDR : x oui □ non **Nb de thèses en cours** : 4

Mail : david.bromberg@irisa.fr **Tél.** :

Co-directeur de thèse : **Unité de recherche** :

Employeur/Établissement d'origine :

HDR : □ oui □ non **Nb de thèses en cours** :

Mail : **Tél.** :

Sujet

Titre : HELENOS - Resisting to Massive proliferation of new Android malware threats

Mots clés : Android, Security, Malware, ML

Cotutelle internationale (oui/non) : **Si oui, préciser l'établissement et le pays de rattachement** :

Descriptif (15-30 lignes) :
Contexte socioéconomique et scientifique ; Les hypothèses et questions posées ; Les grandes étapes de la thèse et démarche ; Approches méthodologiques et techniques envisagées

Context. Android is now the most used operating system with 863.3 million applications with a rate of more than 50 000 submissions a month. Estimations indicate that more than 75 billions applications were downloaded on the platform in 2016. Consequently, due to its widespread popularity, the Android platform has become a lucrative target for hackers.
Hence Android constitutes one of the first choice platform to propagate malware threats. Infection rate on Android devices is constantly increasing spawned out by a dramatic proliferation of malware. Nowadays there are no satisfactory solutions to stop the proliferation of malware over Android devices. It constitutes a severe threat to any businesses. It may interrupt and disable applications, retrieved and spoofed personal information and identity, access sensitive information, control all applications executing on users' device, and even overcharge users for functionality that's widely available.

Previous work. The last decades, to increase the accuracy of malware detection, a huge amount of classification models based on either machine or deep learning methods have been proposed [1, 2, 3]. In previous works, different test-bed to evaluate the true robustness of anti-malware scanners through the design of benchmarks and key indicators with the use of innovative measurements techniques have emerged[4, 5]. In particular, to automate the robustness evaluation of anti-malware scanners against the steady increase of malware variants, toolchains to generate Android adversarial examples (AAEs) dedicated to Android has demonstrated the strong inability of existing scanners to detect sophisticated malware that have mutated. In other terms, current classification models have difficulties to detect AAEs.

Objective. Our objective is first to evaluate the true robustness of anti-malware scanners. Since we have at our disposal adequate benchmarks and evaluation methodology, the objective of this thesis is to study the implementation of new defense techniques and to evaluate them.
Transformers, a category of attention-based deep learning techniques, have gained substantial recognition in the last years, and have shown to be very effective in various domains such as language modeling, machine translation, audio classification, computer vision, object detection, semantic segmentation, and image classification with Vision Transformers models (ViT) [6, 7].
Accordingly, the purpose of this project is to study how to apply Transformers to the specific case of Android malware detection. Current anti-malware scanners are built around traditional machine learning (ML) algorithms [8, 9]. They usually require intermediate feature extraction phases to allow characterization of the malware, via for instance static code analysis. Particularly, deep expertise in both software engineering and Android code development is required to extract the adequate features to give as input to the machine learning models beforehand.
Transformers have proven to be particularly effective in performing automatic feature learning from structured and non-structured data from various domains potentially paving the way for a substantial improvement in the robustness of scanners. There are different paths to explore : should we rather apply Transformers model on the source code of an application, or its bytecode assembly or directly on its binary ?[10, 11, 12]. Another way to explore could be to project the code of an application to an image and then to analyze this image[13]