УДК 004.056
П. Луговський; І. Фалендиш
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИБІР ІНФОРМАТИВНИХ ОЗНАК ДЛЯ ЗАДАЧІ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ANDROID

UDC 004.056
P. Lugovskyi; I. Falendysh

SELECTION OF INFORMATIVE FEATURES FOR THE TASK OF ANDROID MALWARE DETECTION

Шкідливе програмне забезпечення для Android – це будь-яке шкідливе програмне забезпечення або код, призначений для завдання шкоди мобільному пристрою користувача Android, наприклад, віруси, трояни, програми-вимагачі, рекламне, шпигунське та інше. Таке шкідливе програмне забезпечення може бути завантажене або встановлене з різних джерел. Після проникнення шкідливого програмного забезпечення на мобільний телефон користувача Android, воно може виконати різні шкідливі дії, такі як крадіжка та продаж конфіденційної інформації, шпигунство за активністю на телефоні (наприклад, текстовими повідомленнями, дзвінками тощо) або вимагання викупу.

Загалом методи виявлення шкідливого програмного забезпечення діляться на три великі групи: статичні, динамічні та гібридні [1]. Як показує дослідження [2], методи машинного навчання виявились дуже перспективними для виявлення шкідливого програмного забезпечення для Android, оскільки вони можуть розпізнавати складні шаблони даних і навчатися на великих масивах даних. Алгоритми машинного навчання ідеально підходять для виявлення шкідливого програмного забезпечення для Android.

Вибір інформативних і незалежних ознак є вирішальним елементом ефективних алгоритмів розпізнавання образів, класифікації та регресії, а ознаки, як правило, є числовими. У нашому дослідженні з виявлення шкідливого програмного забезпечення для Android за допомогою динамічного методу ML на рівні API (Application Programming Interface), інтерфейс прикладного програмування було обрано як ознаку для навчання моделей машинного навчання, які будуть використані для класифікації того чи іншого додатка Android як шкідливого програмного забезпечення чи ні. Наприклад, якщо під час роботи мобільного додатку було викликано один API, то для цього API буде зазначено значення один для ознаки, що стосується цього додатку, або ж буде надано значення нуль. Специфікація API - це детальний опис, який допомагає розробнику використовувати такий інтерфейс для виконання певних вимог або функцій.

Інженерія ознак полягає у визначенні ознак для кращого представлення цільової задачі, яку розв’язує машинне навчання, і подальшого підвищення його точності. Зазвичай для цього використовуються знання з певної галузі або автоматизовані методи для вилучення, вибору або побудови правильних ознак. Для цього сценарію використання для виявлення шкідливого програмного забезпечення на Android ключовим фактором досягнення високої точності є вибір ознак, який, по суті, є вибором API в підході.

Література

1. Ashawa, Moses & Morris, Sarah. (2019). Analysis of Android Malware Detection Techniques: A Systematic Review. International Journal of Cyber-Security and Digital Forensics. No. 8. P. 177-187. 10.17781/P002605.
2. Chowdhury, Naseef & Haque, Ahshanul & Soliman, Hamdy & Hossen, Mohammad Sahinur & Ahmed, Imtiaz & Fatima, Tanjim. (2023). Android Malware Detection using Machine learning: A Review. 10.36227/techrxiv.22580881.v1.