A Study on Machine Learning Based Detection of Android Malware and Stego Images

January 2022

Hiroya Kato

別表５
(3)

主　論　文　要　旨

No.1

報告番号	㊙ 乙 第　　号	氏　名	加藤 広野

主 論 文 題 名：

A Study on Machine Learning Based Detection of Android Malware and Stego Images
(機械学習に基づいた Android マルウェアとステゴ画像の検知に関する研究)

（内容の要旨）

インターネット技術の向上に伴い、非常に便利な生活が実現しつつある一方で、電子ファイルやスマートフォンアプリなどのデジタルメディアを悪用した攻撃が重大なサイバーセキュリティ脅威となっている。既存のウイルス対策ソフトにより、既知の攻撃の検出は実用化されているが、多様化した全ての脅威に対処できるわけではない。攻撃の存在を確認することで、ユーザは被害を防ぐことができ、攻撃への対処や分析が行われやすいことから、デジタルメディアにおける脅威の検知技術は、サイバーセキュリティ分野において、最も重要な研究領域の一つになっている。

本論文では、検知技術が活躍する領域の中でも、利用者や被害の多さの観点から、Android マルウェアと、画像に悪性プログラムなどを人間の目には知覚できない微細なシグナルとして埋め込み、密かに攻撃を行うことが可能なステゴ画像の検知について扱う。これらの検知対象に対し、効果的な機械学習に基づいた検知法や未解決の課題への対策を提案する。実データを用いた分析や計算機シミュレーションを通して、提案方式の有効性や欠点および今後の展望を示す。

本論文の構成を以下に示す。

第 1 章では、デジタルメディアにおけるサイバーセキュリティ脅威の検知の重要性および、当該技術が用いられる領域を概観し、本研究の目的と位置付けを明確にする。

第 2 章では、本研究で想定する攻撃モデルや関連する従来研究について述べ、その問題点を述べる。

第 3 章では、SSL（Secure Sockets Layer）サーバ証明書の認証レベルに着目した Android マルウェア検知法を提案する。実データセットを用いた評価を行い、提案方式は、従来方式が検知できないマルウェアを検知し、検知精度を向上できることを示す。

第 4 章では、パーミッションペアの構成比に着目した Android マルウェア検知法を提案する。実データセットを用いた評価を行い、提案方式は、従来方式と比較して、検知結果の解釈を容易にし、学習時間および検知精度に関して優れているため、より実運用に向いていることを示す。

第 5 章では、シグナル埋め込み前に縮小リサイズが施されたステゴ画像への対策を提案する。本提案では、近年のシグナルの埋め込み手法を画像に複数回適用した場合、連続して同様の箇所に埋め込む傾向を利用し、シグナルを強調することで、学習を促進する。実データセットを用いたシミュレーションを行い、提案方式は、従来方式と比較して、縮小リサイズ後に作成されたステゴ画像の検知精度を向上可能であることを示す。

第 6 章は結論であり、本論文の内容を総括している。

別表６
（３）

Keio University

Thesis Abstract

No.

Registration Number	☑ "KOU" □ "OTSU" No. *Office use only	Name	Hiroya Kato

Thesis Title

A Study on Machine Learning Based Detection of Android Malware and Stego Images

Thesis Summary

Along with the development of Internet technologies, they have brought us a considerably convenient life. Meanwhile, attacks via digital media such as electronic files and smartphone applications become serious cyber security threats. Although detecting known attacks is realized by using existing anti-virus software, such a defense is not applicable to all threats because of their diversity. By knowing the existence of attacks, users can avoid damage. Furthermore, it is easy to deal with attacks and analyze them. Thus, detection of the threats in digital media is one of the most important research domains in cyber security.

In this dissertation, I deal with the Android malware (malicious software) and stego images which can stealthily carry out attacks by embedding malicious programs as unperceivable signals. For these detection targets, I propose effective machine learning based detection schemes. Through data analysis and computer simulation, I show their effectiveness, limitations and future prospects.

The outline of this dissertation is as follows:

Chapter 1 deals with the importance of detection of cyber security threats in digital media, and I summarize the fields to which this technique is applied. Furthermore, I clarify the purpose and role of this dissertation.

Chapter 2 deals with attack model, the related work, and the shortcomings.

In chapter 3, I propose an Android malware detection scheme based on level of SSL (Secure Sockets Layer) server certificate. By computer simulation with real datasets, I demonstrate that the proposed scheme can detect malware samples which are not detected by the previous scheme and improve the detection accuracy.

In chapter 4, I propose an Android malware detection based on composition ratio of permission pairs. By evaluation with real datasets, I show that the proposed scheme helps human to easily understand detection results and is superior to conventional ones in terms of training time and detection accuracy, which means this scheme is suitable for practical use.

In chapter 5, I propose a countermeasure against stego images to which downsampling is applied before embedding. I utilize the fact that recent embedding methods tend to embed signals in almost the same pixels when they are applied to images multiple times, which makes signals noticeable. Through computer simulation with real image datasets, I prove that the proposed scheme can improve detection accuracy of the resized stego images compared with conventional ones.

Chapter 6 concludes this dissertation and summarizes the contribution of this work.