FireMarking:Android アプリケーションの セキュリティ指向サジェスションシステム

加藤 邦章 (1210017)

北陸先端科学技術大学院大学 情報科学研究科

2015 年 3 月 20 日

キーワード: Android、セキュリティ.

Android ユーザから Android マルウェアが原因とされる被害報告は年々増えている。G Data 社のレポートでは、ユーザにとって迷惑な行為をするアプリケーションによる被害が増加していると述べている。McAfee 社のレポートでは、正規のアプリケーションやサービスの脆弱性を悪用して、アプリケーションストアやセキュリティ製品の監視網を欺くマルウェアが増え、現在のマーケットのセキュリティレベルでは脅威を阻止できないと警告している。その他、シマンテック社のレポートでは、マルウェアによる被害拡大は、ユーザの意識に問題があると説明している。

この 3 つのレポートから、 Android マルウェアによる被害の拡大の原因は、次の 2 つであると考える。それは、ユーザは十分な情報に基づいた意思決定によって、アプリケーションをインストールしているわけではないことと、Android マーケットはマーケット運営者によって、適切に管理されているわけではないことである。本研究では、これらの問題を解決するため、第 3 者の視点で Android マーケットを分析して、マーケットや公開されているアプリケーションの利用リスクを示すセキュリティ指向サジェスションシステム、FireMarker を提案する。

前述の 2 つの問題と Android セキュリティに関する既存研究から、FireMarker の利用者を Android アプリケーション操作により生じる情報を欲する Binarian、Android マーケットの傾向分析を行う Analyst、マーケットやアプリケーションの有用な情報を得たい End-user に分けた。彼らの要求を推測し、それを満たすための条件を議論した。その結果、FireMarker には、次の 3 つの条件があると考えられる。1 つ目の条件は、短時間で大量のアプリケー

ションから情報を集めるために、複数のマシンや Android 端末を制御できること、2 つ目の条件は、アプリケーションを操作した時に生じる情報を取得するために、アプリケーション操作の自動化が可能なこと、3 つ目の条件は、ユーザにマーケットやアプリケーションの利用リスクを示すために、情報を解析、評価して、結果を可視化することである。これらの条件を満たすため、FireMarker は Android マーケットを調査し、その傾向を数値化する MarketDrone と、集めた情報を利用して、ユーザにマーケット及びアプリケーションの利用リスクを示す FireMarking の 2 つから構成されるシステムとして設計した。

MarketDrone は各マーケットからアプリケーションをダウンロードする Crawler、複数のマシン、複数の Android 端末を利用して、アプリケーション操作時に生じるシステムログやトラフィックを収集する Dispatcher、その結果を基にマーケットの傾向を数値化する Filter、前述の 3 つのモジュールを統合し、自動化する Controller から構成される。そして、FireMarking は MarketDrone が出力した情報を用いて、マーケット及びアプリケーションの利用リスクを測る。

本研究では FireMarker の設計のうち、MarketDrone の Crawler、Dispatcher、Filter を次のように実装した。Crawler は、APKTOP という Android マーケットをクロールするツールとして実装した。Dispatcher は、情報収集の処理速度を追求した設計パターン A と可用性を重視した設計パターン B を考案し実装した。Filter は、アプリケーションのシステムログを用いて強制終了や管理者権限の要求するアプリケーションを特定する。また、トラフィックからは、FQDN を種類別に分ける。さらに、トラフィックから HTTP 通信を抽出し、広告に関する通信を行うアプリケーションを特定するツールとして実装した。

次にこれらを用いて、APKTOP と既存のクローラを用いてアプリケーションを集めた OperaMobileStore を調査する実験を行った。その結果、APKTOP からはアドウェアを持つ 4 つのアプリケーションを発見し、OperaMobileStore からはアドウェアを持つ 8 つのアプリケーションを発見した。さらに、両方のマーケットで日本で行った実験にも関わらず、エストニアやロシア、中国など日本以外の広告を表示するアプリケーションを発見した。その他にも、APKTOP からトロイの木馬であるアプリケーションを特定した。実験結果から FireMarker は、APKTOP と OperaMobileStore を比べた時、ユーザにとって安全なマーケットは OperaMobileStore である、と示した。

最後に、実験によって明らかになった課題を今後の展開としてまとめ、その解決方法について議論した。その議論の中で、実験結果から各アプリケーションの利用リスクを評価する手法、マーケットの利用リスクを測る方法を提案した。FireMarker によって、Binarian

は提案する手法を大量のアプリケーションを使って、検証することができる。また、調査したマーケットの情報をデータベースに保存しアクセスできるようにすれば、実験のデータセットとして利用することができる。さらに、Analyst は各マーケットごとの情報を入手し、強制終了するアプリケーションや管理者権限を要求するアプリケーションの数、FQDN の種類、迷惑な広告を表示させるアプリケーション数などの情報を入手することができる。その結果、彼らはマーケットの動向を容易に調べることができる。さらに、End-user は FireMarker によって、アプリケーションインストール時に利用するマーケットの安全性を確かめることができる。その結果、マーケットの安全性を考慮した意思決定により、アプリケーションを使うか否か決めることができる。以上をもって、本研究は Android マルウェア被害の拡大の原因とする 2 つの問題を解決した。