# MarketDrone: Androidアプリケーションケーションの動的解析フレームワーク

加藤 邦章 [1] 高野 祐輝 [4,3] 三浦 良介 [4,3] 太田 悟史 [5,1] 篠田 陽一 [2]

[1] 北陸先端科学技術大学院大学 情報科学研究科
[2] 北陸先端科学技術大学院大学 情報社会基盤研究センター
[3] 北陸先端科学技術大学院大学 高信頼ネットワークイノベーションセンター
[4] 情報通信研究機構 サイバー攻撃対策総合研究センター
[5] 情報通信研究機構 ネットワークセキュリティ研究所

## 1 はじめに

2008年にAndroid搭載端末が発表されて以来、Androidユーザは急増している。それに伴い、Androidマルウェアは増え続けている。Androidマルウェアは多数のAndroidマーケットに潜んでおり、それを検出するシステムが必要である。既存のシステムは大規模にAndroidアプリケーションを調べられなかった。そこで我々はAndroidマーケットの大規模調査を行うフレームワークMarketDroneを開発した。これは各Androidマーケットからアプリケーションをダウンロードして、動的な解析を行い、その結果をユーザに出力するフレームワークである。MarketDroneによって、Androidアプリケーションの動的な評価を行うことができるだけでなく、各Androidマーケットの傾向やリスクを知ることができる。本稿はMarketDroneの設計と実装について説明する。次に、MarketDroneの有効性を示すため行ったAndroidマーケットAPKTOPの大規模調査とその結果について述べる。

## 2 MarketDroneの設計と実装

Androidマーケットを調査する際、次の作業を行う必要がある。まず、あるAndroidマーケットから、取得可能なアプリケーションを全て収集する。次に、収集したすべてのアプリケーションの動作から出力されるシステムログやトラフィック等のデータを記録する。最後に記録したデータを解析し、結果をエンドユーザに向けて出力する。我々はこれら一連の作業を統合的に行い、作業を自動化することを目指す。それゆえ、MarketDroneはCrawler、Logger、Analyzerの3コンポーネントと各コンポーネントを統合制御するAutomaterの4機能を持つフレームワークとして設計した(図1)。

次に各コンポーネントについて説明する。Crawlerは複数のAndroidマーケットクローラの集合からなるコンポーネントとした。複数のクローラの集合としたのは、各Androidマーケットのページ構造が異なるためである。現在までに我々は、事前登録や認証を必要としないAndroidマーケット、APKTOPのクローラを開発した。

Loggerは Androidデバイス/エミュレータを複数台を制御し、アプリケーションの実行中に出力されるシステムログやトラフィックを記録するコンポーネントとした。(図2)。Loggerは多数のアプリケーションからシステムログやトラフィック、画面遷移を記録するため、複数のAndroidデバイス/エミュレータを制御するようにした。また、Loggerが行うアプリケーションの実行は、ユーザがアプリケーションを開始させるアイコンを押し、起動30秒後終了するパターンを再現した。複数端末及びAndroidアプリケーションの起動制御は、adb [1] を利用して、実装した。

Analyzerはシステムログやトラフィック等を入力すると、データを抽出、HTTP通信の解析やシステムログの分析を行い、結果を出力するコンポーネントとした。ユーザのアプリ操作から得られる情報はトラフィックやシステムログ、画面遷移と多岐に渡るため、Analyzerは複数の解析システムを備え、高い拡張性を持つよう、実装した。今回我々はAndroidアプリケーションのHTTP通信のうち、多数のアプリケーションで表示される広告について調べるため、Adblockフィルタを利用した解析システムadcheckerを開発し、Analyzerに組み込んだ。

Automaterは Crawler、Logger、Analyzerの3つを統合制御するものとした。今回は3コンポーネントの開発を優先したため、Automaterは実装していない。

## 3 Androidマーケットの大規模調査

MarketDroneの有効性を示すために、我々はAPKTOPを対象としたAndroidマーケットの大規模調査を行った。手順は、初めにAPKTOPの無料で取得可能なアプリケーションを全て収集した。次に収集したアプリケーションを動かして、出力されるトラフィックを記録した。最後に記録したトラフィックからHTTP

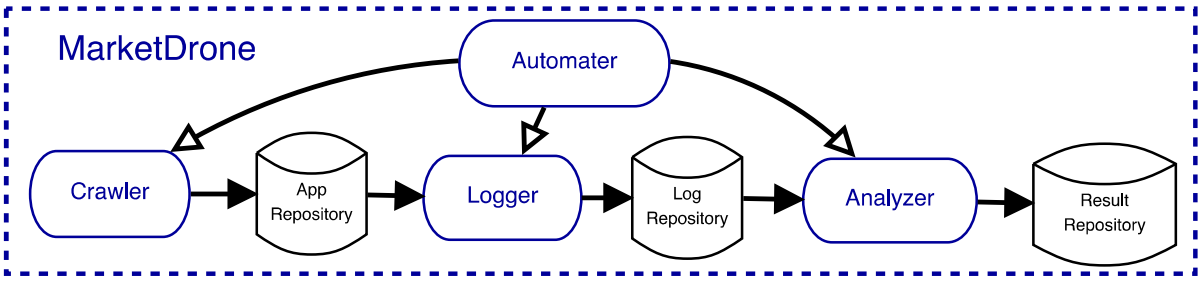


図 1: MarketDrone の構成

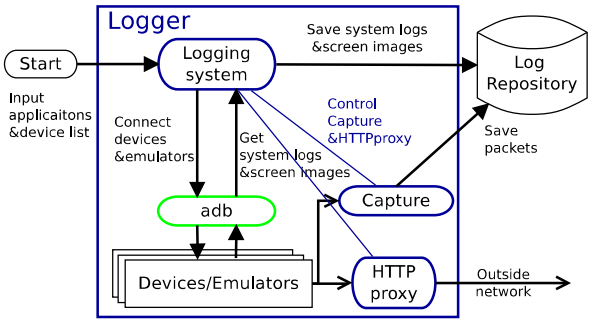


図 2: Logger の構成

表 1: マッチしたフィルタと回数

| Filter | Count | Filter | Count |
|---|---|---|---|
| Japan-2[3] | 9,444 | Russia[5] | 233 |
| General[2] | 5,490 | China[2] | 224 |
| Japan-1[6] | 3,372 | Malware[4] | 35 |
| Privacy[2] | 1,342 | Germany[2] | 5 |
| Estonia[2] | 1,292 | Lithuania[2] | 3 |
| Annoyance[2] | 278 | Bulgaria[2] | 2 |
| | | 合計 | 27,120 |

通信を抽出し、広告について解析を行った。これら手順は MarketDrone を使って行った。MarketDrone は APKTOP から 26,691 アプリケーションを収集し、そのうち、22,146 アプリケーションからトラフィックの取得に成功した。このトラフィックから述べ 81,675 ものURL を抽出でき、解析した結果、Adblock フィルタのパターンにマッチした回数は 21,720 回であった。

表 1 は Adblock フィルタ別にマッチした回数をまとめたものである。我々は表 1 中の Malware フィルタにマッチしたパターンを使い、いくつか危険が高い通信を行ったアプリケーションを特定した。さらに我々は特定したアプリケーションのうち 1 つと同パッケージ名を持つものを APKTOP 及び GooglePlay で調査し、APKTOP に 3 つ、GooglePlay に 1 つ発見した。これから、危険性が高い通信を行ったアプリケーションは、正規アプリケーションに悪意ある広告機能に差し替えられたリパッケージアプリケーションでありうることを示した。

## 4 おわりに

本稿は Android マーケットを調査し、利用リスクを示すことが、ユーザのアプリケーション利用機会を増やし、ユーザの利益になると主張した。そこで我々は Android マーケットを大規模調査するためのフレームワーク MarketDrone を開発した。MarketDrone の有効性を示すために、APKTOP に大規模調査を行った。全アプリケーションの 88%にあたる 22,146 アプリケーションから抽出したのべ 81,675 ものURL から、Adblock の Malware フィルタにマッチした通信を 35 回確認した。そのマッチしたパターンから、いくつか危険性が高い通信を発したアプリケーションを特定した。特定したものと同パッケージ名を持つアプリケーションは APKTOP だけでなく、GooglePlay にもあったことから、正規アプリケーションに悪意ある広告機能に差し替えられたリパッケージアプリケーションである可能性を示した。

以上から、Android マーケットの大規模調査を行う MarketDrone は、APKTOP の傾向の一部を明らかにしたことで、その有効性を示した。今後は複数の Android マーケットに対して大規模調査を行いたい。

## 参考文献

[1] Android Debugger Bridge. http://developer.android.com/tools/help/adb.html.

[2] EasyList. https://easylist.adblockplus.org/en/.

[3] adblock-plus-japanese-filter. https://code.google.com/p/adblock-plus-japanese-filter/.

[4] MalwareDomains. http://www.malwaredomains.com/?page_id=2.

[5] ruadlist. https://code.google.com/p/ruadlist/.

[6] 豆腐フィルタ. http://tofukko.r.ribbon.to/abp.html.