講演番号： 25

Android アプリにおけるリパッケージング検出法の検討

A－7　　Study of repackaging detection techniques for Android apps

前原　一樹†　宮保　憲治†
Kazuki Maehara†　Noriharu MIYAHO†
† 東京電機大学　情報環境学部
† School of Information Environment, Tokyo Denki University

1. はじめに

Android にマルウェアを仕込む際に使用される技術の一つとして，正規のアプリに悪性コードを埋め込んだアプリを作成する「リパッケージング」という手法がある．改変された Android アプリ（以下，リパッケージアプリと呼称）を，リソース情報を使用して検出する方法が検討されている[1]．

しかし，リパッケージアプリは，元となったアプリがなければ，見つけ出すことは困難である．そこで，本稿では，検出できたリパッケージアプリの署名情報を用いて，他のリパッケージアプリを検出する手法を提案する．

2. 提案手法

図 1 に提案手法の概要を示す．図 1 に示すように，GooglePlay アプリ（以下，GP アプリと略称）と ThirdParty アプリ（以下，TP アプリと略称）からそれぞれ，リソース情報を取出し，同じリソースの保有割合を計算する．次に，閾値を越えた類似度を持つペアを検出する．検出したサードパーティのアプリから署名情報を取出し，署名情報（e.g. 所有者名）と類似する署名を持つアプリがあれば，そのアプリを検出する．この方法を採用する理由は以下の通り．

1. リパッケージアプリ製作者の作成する他のアプリは信用できない
2. 正規アプリ1つに，リパッケージングを行うよりも複数行う方が，より多くのユーザに被害を与えることができる

検出したアプリの署名情報をブラックリストとして登録することにより，さらにアプリを収集した際には，疑わしいアプリを早期に発見することができる．

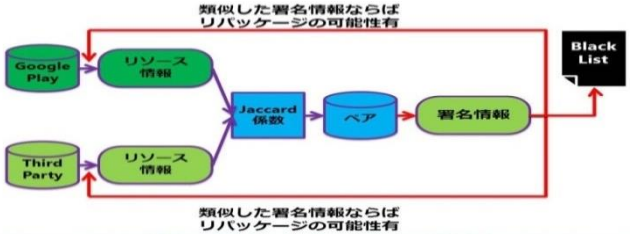

図 1 署名情報による検出法

3. 基礎実験の方法

リパッケージの可能性があるアプリ検出に関わる基礎実験を行った．表 1 に本実験で使用した検体を記す．同じリソースが使用されている割合（以下，類似度と呼称）が，0.5 を超えたペアの TP アプリに対し，署名情報を取出し，類似した署名情報をもつアプリを検出する．署名情報は，所有者名，シリアル番号，開始日時，MD5 を用いた．

表 1 本実験の検体

マーケット	検体数(個)	署名検証検体	収集期間
GooglePlay	1,002	10,633	2014 年
ThirdParty	12,816	0	2015/8～10
合計	13,818	10,633	

4. 基礎実験の結果

図 2 に示す類似度とペア数割合の関係から，類似度が 0.5 未満である割合が，全ペアの約 99.99% 以上であることが分かった．この結果は，類似度 0.5 以上のペアの検出は稀であり，リパッケージアプリの可能性があることを示す．GP アプリとの類似度が 0.5 以上の TP アプリの署名情報を用い，本実験の検体を検索した結果，表 2 に示すように，同じ署名情報を持つ他のアプリが検出された．検出したアプリに対し，VirusTotal で確認した結果，一部の検体に対し，VirusTotal で悪性と判断できた．

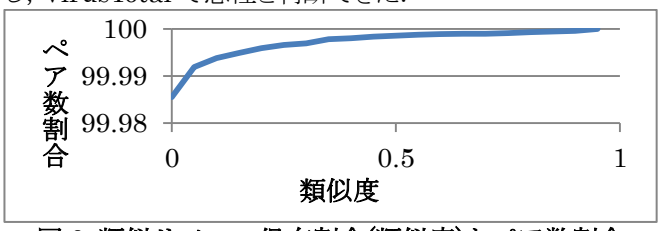

図 2 類似リソース保有割合(類似度)とペア数割合

表 2　実験結果（一部）

所有者名	VirusTotal	GP アプリ	TP アプリ
cht	検知あり	0	17
zhangjiazhi	検知なし	1	1

5. 今後の課題

本検討では，類似した署名情報を持つアプリを検出しただけであり，検出したアプリが真にリパッケージアプリであるか，あるいは単に類似したアプリであるかどうかの検証は行っていない．今後は，検出したアプリが，リパッケージアプリであるかどうかの検証と，元となったアプリを発見する手法を検討する必要がある．

6. 参考文献

[1] 石井悠太，渡邉卓弥，秋山満昭，森達哉，「正規アプリに類似した Android アプリの実態解明」，電子情報通信学会技術研究報告，Vol.114，No.489，pp.187-192，2015