ダミーデータを用いたAndroidの端末情報の保護

綿谷　彰*，高橋　健一，川村　尚生，菅原　一孔
（鳥取大学大学院工学研究科情報エレクトロニクス専攻）

Using Dummy Data for the Protection of Information in Android

Akira Wataya, Kenichi Takahashi, Takao Kawamura and Kazunori Sugahara
(Department of Information and Electronics, Graduate School of Engineering Tottori University)

1. はじめに

近年，スマートフォンと呼ばれる高機能携帯電話が急速に発展している．Android はスマートフォン向けのオープンプラットフォームの1つであり，個人や企業が自由に利便性の高いアプリケーションを開発できることで知られている．また，開発したアプリケーションはGoogle Playと呼ばれるアプリケーション配信サービスを通じて自由に公開可能であり，年間数十万のアプリケーションが公開され，爆発的な増加をみせている．このような利点がある反面，Android 端末の位置情報や端末情報を標的としたマルウェアの存在が問題となっている．携帯端末であるAndroid端末は，PCなどの端末と比較して利用頻度が多く，位置情報やアドレス帳など，より多くの個人情報が保存されている．

Android では,セキュリティモデルとしてパーミッション機構が採用されている[1]. パーミッション機構では，マニフェストファイルにアプリケーションが保有するパーミッションが宣言され，宣言されたパーミッションがアプリケーションをインストールする際に提示される．マルウェアも例外ではなく，マルウェアとして動作するために必要なパーミッションを提示する．また 2012 年 2 月の米国カリフォルニア州での合意[2]では，Google や Apple などアプリケーション配布を事業とする主要 6 社に対し，アプリケーション配布サイトにおいて，各アプリケーションの説明ページの中に「プライバシーポリシー」との見出しのリンクを設置することが求められた．プライバシーポリシーでは，アプリケーションがユーザの端末からどのような情報を収集しようとするのかが記述される．しかし調査[3]によれば，すべてのアプリケーションにプライバシーポリシーが設置されているわけでないことやプライバシーポリシーの記述にアプリケーション間で差異があることが報告されている．

これらの Android を取り巻くセキュリティ環境で，パーミッションの知識が乏しいユーザが，個人情報をマルウェアから守ることは難しい．そこで本稿では，正規アプリケーションを装ったマルウェアの端末情報取得を防ぐために，アプリケーションに渡す情報をダミーデータとし，ユーザの個人情報を保護する手法を提案する．

2. 関連研究

小松ら[4]は，アプリケーションの危険性をインストール時に掲示することでユーザの判断を補助するシステムを提案している．アプリケーションの危険性は，パーミッションの組み合わせや特定のパーミッションに重みを付加することで判断している．しかし，ユーザはそのパーミッションが Android 上でいつ使用されるかを特定できない．また，危険性の精度もパーミッションの組み合わせによる可能性を示しているに過ぎず，実際にそのような危険性があるのかはわからない．

坂下ら[5]は,アプリケーションのソースコードを静的解析することで，アプリケーションのパーミッションの利用目的をユーザに可視化することを提案している．しかし，可視化されたとしても，その結果をユーザが判定する必要があり，既存のパーミッション機構のユーザ負担と対して変わらない．

渡邊ら[6]は，アプリケーションが情報の取得や漏洩に関わる動作を行うとき，それをユーザに通知し，実行の可否を選択させる動的制御機構を実現している．これにより，ユーザはパーミッション利用時を特定することができる．しかし，選択後の動作については言及されていない．

3. 提案手法

マルウェアは携帯端末上では正規のアプリケーションを装って悪さをするスパイウェアのようなものが多い．正規のアプリケーションはパーミッション機構を通して，端末情報が格納されている Android のメソッドにアクセスし情報を取得する． 同様に，マルウェアもそのパーミッション機構を利用し，端末情報が格納されているメソッドにアクセスし情報を取得する．そのため，ユーザが端末上の動作だけでマルウェアであるかどうかを判断することは難しい．

そこで，アプリケーションが取得しようとする端末情報をダミーデータ化する．アプリケーションが端末情報を取得する際に，アプリケーションが要求する情報をダ

ミーデータとすることで重要な個人情報の漏洩を防ぐ．ダミーデータが外部へ送信されたとしても，端末のユーザの個人情報とは別物であるため，ユーザに危害が加わることはない．実装イメージを図 1 に示す．

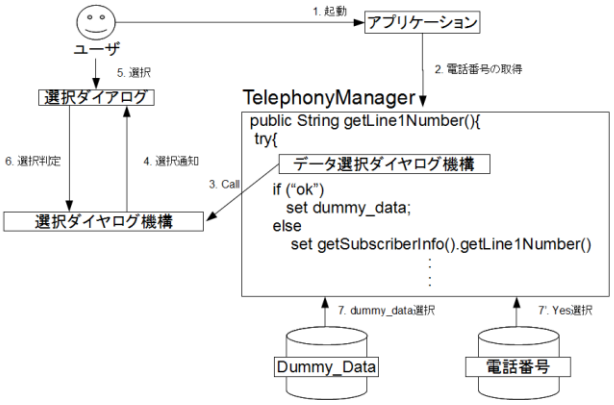

図 1. 実装イメージ

アプリケーションが端末情報を取得するとき，特定のメソッドが呼び出される．例えば，電話番号を取得するときは getLine1Number()が呼び出される．これらのメソッドにデータ選択ダイヤログ機構を設置し，端末画面にダイヤログを表示することで，ユーザにアプリケーションに提供するデータを選択させる．ダイヤログの選択肢は「Yes」と「Dummy」を用意する．「Yes」を選択した場合，端末情報をそのままアプリケーションに提供する．「Dummy」を選択した場合は，要求する端末情報をダミーデータに置き換え，アプリケーションに提供する．「Dummy」を選択することで，アプリケーションへ提供される情報がダミーデータ化されるので，端末情報の漏洩を防ぐことができる．

4. 実験

ダミーデータ化により，アプリケーションがどのように動作するか実験を行った．図 2 にダミーデータ化の 1 例を示す．

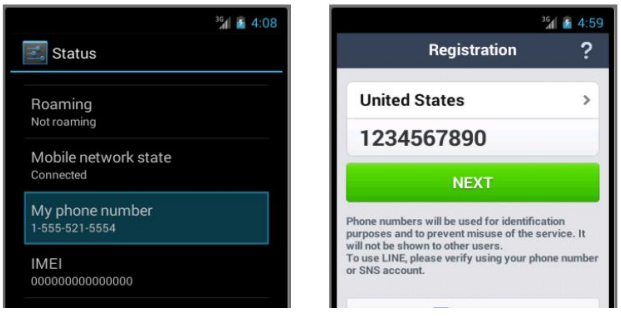

図 2.ダミーデータ化の例:左:端末情報，右:電話番号の取得結果

図 2 より，取得された電話番号は”1234567890”となっており，実際の電話番号ではなくダミーデータ化された電話番号となっていることがわかる．実験では，Google Play 上に存在する 10 個のアプリケーションの動作を確認した(表 1).

表 1. 実験で使用したアプリケーション

アプリケーション名	アプリケーションID
端末情報	com.hkworks.DeviceInfo
端末情報	jp.xeeken.android.deviceinfo
端末情報表示ツール	jp.gr.java_conf.tada
電話情報	br.com.axasoftware.mysimcard
Android端末情報取得Free	jp.android.tool.app.free
MyQR: アドレス帳簡単登録	net.karappo.android.myqr
Menu0	jp.sakura_hoaru.Menu0
電話番号を忘れない。MY電話番号	com.orimagi.myad
My Number	hr.mynumber
LINE	jp.naver.line.android

電話番号を取得・発信するアプリケーションでは，電話番号がダミーデータとなっているため発信することはできなかった．しかし，他はすべて正常に動作することが確認できた．

実験結果から端末情報ではなく，ダミーデータがアプリケーションに提供されたことがわかる．実験では，市場にあるアプリケーションを使用したが，端末情報を取得するプロセスはマルウェアも同様であることから正規のアプリケーションを装ったマルウェアに対して，ダミーデータを用いることは有効であると考えられる．端末情報の代わりにダミーデータがアプリケーション側に，提供されることで，正規のアプリケーションを装ったマルウェアによる情報漏洩を防ぐことができる．

5. 終わりに

本稿では，マルウェアによる情報漏洩に対してダミーデータを用いることを提案した．しかし端末情報をダミーデータに置き換えるだけでは，ユーザは使用しているアプリケーションがマルウェアであるかどうか判断できない．また，ダミーデータのままでは使用できないアプリケーションや携帯機能が存在する．

そこで，ダミーデータでは動かないアプリケーションへ端末情報を提供できる機構として，ダミーデータと端末情報のどちらかをアプリケーションへ提供するかユーザが選択する機構を考案した．今後，端末情報のダミーデータ化を進め，その有効性について調査する．

文 献

(1) Android Developers, http://developer.android.com
(2) 米国カリフォルニア州司法省, Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for User of Mobile Applications, http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy
(3) 市瀬 小夜，高木 浩光，渡辺 創：「スマホアプリにおけるアプリケーション・プライバシーポリシー掲載の国際比較調査」，SCIS2014，The 31st Symposium on Cryptography and Information Security Kagoshima, Japan, Jan 2014
(4) 小松 勇毅，児玉 英一郎，王 家宏，高田 豊雄：「Android OS におけるアプリケーション導入時のユーザ補助システムの提案」，電子情報通信学会技術研究報告，ISEC，情報セキュリティ 113(135)，pp.13-18, (2013)
(5) 坂下 卓弥, 小形 真平, 海谷 治彦, 海尻 賢二:「静的解析による Android パーミッションの利用目的の可視化方法」，電子情報通信学会研究報告，EMM，マルチメディア情報ハイディング・エンリッチメント 113(138), pp.143-149, (2013)
(6) 渡邊 華奈子，大月 勇人，瀧本 栄二，斎藤 彰一，毛利 公一：「Android におけるユーザの意図しない情報の漏洩を防止するパーミッション動的制御」，電子情報通信学会技術研究報告，ISEC，情報セキュリティ 113(135), pp.159-166, (2013)