(d) 情報

Android のパーミッション機構に関する研究の一考察

Investigation on Permission Mechanism of Android

綿谷 彰 † 高橋 健一 † 川村 尚生 † 菅原 一孔 †

Akira Wataya † Kenichi Takahashi † Takao Kawamura † Kazunori Sugahara †

† 鳥取大学大学院 工学研究科 情報エレクトロニクス専攻

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. 中でも, Android スマートフォンが急速な普及をみせている. Android はスマートフォン向けオープンプラットフォームの１つであり, 誰も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, Android Market 上に公開可能であり, 爆発的な増加をみせている.

しかし, このような利点がある反面, Android 端末を標的としたマルウェアの存在が問題となっている. 実際, Android 端末の位置情報や端末情報を狙ったマルウェア, SNS を悪用して不当にユーザから金銭を得ようとするマルウェアなどが報告されている [1][2]. 例えばマルウェアによる以下の被害が報告されている.

- IMEI, IMSI をサーバに受信
- 送受信される SMS メッセージを外部サーバに送信
- プレミアム SMS の番号への送信
- GPS ロケーションのアップデート
- 電話番号, 連絡先リストをサーバに送信
- 写真撮影とアップロード

携帯端末である Android 端末は, PC などの端末よりも利用頻度が多く, 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. このような情報の漏洩は, ユーザが犯罪に巻き込まれる可能性を高める.

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 [3]. パーミッションは, アプリケーション開発時に開発者の判断でマニフェストファイルに使用が宣言され, 宣言されたパーミッションはユーザ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要求する. しかし, パーミション機構によるセキュリティモデルはユーザに対する依存度が高く, セキュリティとしての確実性に問題を抱えている. 本稿では, パーミッション機構に対する研究の調査, 考察を行う.

2 パーミッション機構に関する研究

文献 [4][5][6] では, パーミッションの組み合わせからアプリケーションの危険性を判断することが提案されている. Enck ら [4] は, インストール時にアプリケーションが要求するパーミッションの組み合わせから推測される危険性をユーザに提示することを提案している. しかし, 対象としている危険性の範囲が狭い. Shin ら [5] は, パーミッション機構の欠点を指摘し, 不正に重要なパーミッションを取得できることを示し, その解決策を議論している. 松戸ら [6] は, パーミッションの組み合わせに基づいた危険性検知と危険性提示を行うことで, 危険性の判断を支援することを提案している. この提案では, パーミッションの組み合わせから起こりうる事態をアイコンを用いてユーザに示すことで, アプリケーションインストールの危険性を理解することを補助する. しかし, ユーザはパーミッションが Android 上でいつ利用されたかを特定できない. また, 危険性検知の精度についても言及されていない. Nauman ら [7] は, アプリケーションインストール後にアプリケーションに与えたパーミッションをユーザが変更できる仕組みを提案している. しかし, ユーザにパーミッションの知識が必要となる. 川端ら [8] は, Android 端末の機能や情報を扱う API へのフックポイントを設けて, アプリケーション実行時に割り込み処理を行うことでアプリケーションのリアルタイム動的制御を実現している. これにより, ユーザはパーミッションの利用時を特定することができ, ユーザは利用時に動的に承認を与えることができる. しかし, パーミッションによる起こりうる危険性をユーザが理解することは難しい.

3 考察

各研究からパーミッション機構の問題は大きく 3 つに分類できる.

問題 1. ユーザはアプリケーションインストール時に, そのアプリケーションが要求しているパーミッションから動作を予測しなければならない.

問題 2. ユーザはアプリケーション動作時に, パーミッション利用のタイミングはわからないため位置情報などの個人の機密情報が外部に送信されていても気が付くことができない.

問題 3. パーミッション機構によるセキュリティはユーザの自己判断に頼る部分が大きいため, ユーザに対してわかりやすいパーミッションの解説方法など, 新し

いユーザインタフェースの考案が必要である．

表 1: 各研究の問題への対応

研究一覧	問題 1	問題 2	問題 3
Enck['09]	○	×	×
松戸 ['12]	○	×	○
Shin['10]	○	×	×
Nauman['10]	×	○	×
川端 ['11]	×	○	×

表 1 から, どの研究も 3 つの問題を同時に解決できていないことがわかる．

4 提案手法

Android では, 必要以上にパーミッションを要求し, 情報漏洩を引き起こす不正アプリケーションが存在する．また, パーミッションを目的以上に要求する正規アプリケーションも存在する．そのため, 不正なアプリケーションのみを判別することは困難である．そこで, 我々は Android をターゲットにするマルウェアに対して, システム側で対策するのには限界があると考え, ユーザを補助するために, 外部との通信を可視化する．例えば, あるアプリケーションが位置情報を送信する際に, 送信先と位置情報を送信することをユーザに提示する．そして, 位置情報を送信することで自宅が特定されてしまうなどの危険性をユーザに警告する．警告は, API への割り込み処理を利用し, Android の送信動作に割り込むことで実現する．図 1 は, 警告のポップアップのイメージである．

図 1: 警告のイメージ

これにより, ユーザはアプリケーションが実際にパーミッションを使用した時間を把握することができる．また, アプリケーション起動時の動作とそれから推測される危険性をユーザに提示する．ユーザに具体的な危険例を提示することで, アプリケーションの動作をユーザに知らせることができる．問題 3 を解決するには, ユーザの理解しやすいインタフェースの提案を行わなければならない．既存の研究では, アイコンなどのユーザインタフェースが用いられている．ユーザに危険性やパーミッション機構などの専門知識を正確に伝えるには, 情報量を少なくし端的に伝えることのできるデザインでなければならない．今後の課題として, そのデザインを考えることが上げられる．

5 まとめ

本稿では, Android のパーミッション機構によるセキュリティの研究に対して問題点を指摘し, 解決案を提案した．今後, 具体的な実装を進めていく必要がある．

参考文献

[1] McAfee 脅威レポート, 2012 年第 2 四半期 . http://www.mcafee.com/japan/media/mcafeeb2b/international/japan/pdf/threatreport/threatreport12q2.pdf.

[2] McAfee 最新ウイルス一覧. http://www.mcafee.com/japan/security/latest.asp.

[3] Android Developers. http://developer.android.com.

[4] Enck William, Ontang Machigar, and McDaniel Patrick. On Lightweight Mobile Phone Application Certification. *Proc. of 16th ACM Conference on Computer and Communications Security, pp.235-245*, 2009.

[5] 松戸隆幸, 児玉英一郎, 王家宏, 高田豊雄. Android OS 上でのアプリケーション導入時におけるセキュリティ助言システムの提案. CSEC, 2012-CSEC-56, No.12 pp.1-7, 2012.

[6] Shin Wook, Kwak Sanghoon, Kiyomoto Shinsaku, Kiyomoto Shinsaku, Fukushima Kazuhide, and Tanaka Toshiaki. A Small but Non-negligible Flaw in the Android Permission Scheme. *Proc. of IEEE International Symposium on Policies for Distributed Systems and Networks(POLICY), pp.107-110*, 2010.

[7] M.Nauman, S.Khan, and X.Zhang. Extending Android Permission Model and Enforcement with User-defined Runtime Constraints. *5th ACM Symposium on Information, Computer and Communications Security, pp.328-332*, 2010.

[8] AndroidOS における機能や情報へのアクセス制御機構の提案. 川端 秀明, 磯原 隆将, 竹森 敬祐, 窪田 歩, 可児 潤也, 上松 晴信, 西垣正勝. Computer Security Symposium , 2011, No.3 pp.161-166, 2011.