Vol.2013-SPT-7 No.12
2013/11/11

「"Little Brothers Watching You:" Raising Awareness of Data Leaks on Smartphones」の報告

可児　潤也[†1]

本稿では、SOUPS2013 にて発表された「"Little Brothers Watching You:" Raising Awareness of Data Leaks on Smartphones」[1]の紹介を行う。この論文では、スマートフォン上でのデータの漏えいに対する意識の向上について述べられている。今日のスマートフォンアプリでは、アプリによってプライバシセンシティブな情報が端末から送信されることについての十分なフィードバックが提供されていない。Balebako らは、位置情報を収集しサードパーティに送信する二つの有名なゲームアプリに関して、ユーザがどのような誤解を持っているか研究室実験を通じて調査した。その後、Balebako らが開発した二種類のインタフェース：通知機構と可視化機構を利用した実験を通して、被験者がスマホアプリのデータ送信に関して認知し得た利点と懸念について報告する。また、どの程度ユーザの意識が高まり、これらの機構がどの程度有用であるかを考察しまとめる。

Report of “"Little Brothers Watching You:" Raising Awareness of Data Leaks on Smartphones”

JUNYA KANI [†1]

I would report about ““Little Brothers Watching You:” Raising Awareness of Data Leaks on Smartphones“. This study reports about raising awareness of data leaks on smartphones. Today's smartphone applications fail to provide sufficient feedback about which privacy-sensitive information is leaving the phone. Through a qualitative lab study, Balebako et al. first discuss misconceptions that smartphone users currently have with respect to two popular game applications that frequently collect the phone's current location and share it with multiple third parties. They then report on participants' perceived benefits and concerns regarding data sharing with smartphone applications after using two types of interfaces that Balebako et al. developed: the notifications and the visualization. They conclude with a discussion on how heightened awareness of users and usable controls.

1. はじめに

ユーザは、スマートフォン上での自分のプライバシの保護について懸念を持っている[2][3]。しかし、一般的な既存のインタフェースでは、送信先、送信の頻度、および送信の目的といったデータ送信に関する情報をユーザに認知させることができない。また、ユーザがアプリケーション（以下、アプリ）や送信される情報の種類を比較できるように、端末から送信される情報を分かりやすくまとめた形で提供してもいない。そのような情報がない状態で、ユーザがスマホからのデータ送信に対し、最適な決定を下すことは難しいと言えよう。

Balebako らは、ユーザの Android アプリ上で起こるプライバシ漏えいの意識を改善させることを目的とする「プライバシリーク」と名づけたスマートフォン上で動作するアプリケーションを提示する。半構造化インタビューを通して、まず参加者のデータ送信に関する理解度の調査を行った。その後、プライバシリークに対する反応と理解度の変化を調査した。

†1 静岡大学大学院情報学研究科
Graduate school of Infomatics, Shizuoka University.

2. 関連研究

ユーザがどの程度、スマホアプリのプライバシについて、またセキュリティリスクについて理解しているか、いくつかの研究で調査されている[4][5]。Balebako らは、ユーザの理解の欠如により深く入り込んだ調査を行った。

また、セキュリティとプライバシの問題に対し、ユーザに通知するためのツール、それらのデータの管理を提供するツールが提案されている [6][7][8][9][10]。しかし、既存研究の多くは、ユーザの理解には焦点を当てていない。Balebako らは提案した通知インタフェースがユーザの要求と期待に応えているかどうか調査を行った。

3. プライバシリーク

Balebako らは、ユーザの Android アプリ上で起こるプライバシ漏えいの意識を改善させることを目的とする「プライバシリーク」と名づけたスマートフォン上で動作するアプリケーションを提案する。Balebako らのプロトタイプは TaintDroid[11]上のプラットフォームで構築される。TaintDroid は、プライバシセンシティブなデータが Android アプリによって端末から送信されるかどうかを判断することができる。本アプリは、ユーザに送信されるデータの頻度と送信先を 2 つの方式で認識させる：

(a) 可視化機構は、どのアプリから、何の情報が、何度送信されたのかをグリッドレイアウトでまとめられた形で見ることができる。
(b) JIT（ジャストインタイム）通知機構は、データが送られた瞬間にユーザに通知する。Balebako らのプロトタイプでは、端末からプライバシセンシティブなデータが送信されようとした際に、バイブレーションと水が落ちるような音が鳴る。また、通知エリアにアイコンとショートテキスト通知が表示される。

4. 調査手法

Balebako らは、19 人の参加者に対し研究室実験を行った。調査は以下の順序に構造化されており、3 つのパートからなる: 1）参加者は 2 つのゲーム（Toss it と Angry bird）をプライバシリークのない状態でプレイし、ゲームについてと端末から送信されるデータについての質問に答える。2）参加者は同じゲームをプライバシリークの有効な状態でプレイし、同様の質問に答える。3）プライバシリークの有用性、データの管理について、そして要求されるデータ送信の認識についてインタビューされる。

5. 初期理解

第１パートのインタビュー内で、参加者は２つのゲームを 3-7 分プレイした。その後、情報を送信した両ゲームのうちどちらが、いつ、なぜ、何のデータが端末から送信されたかを尋ねられた。参加者の認識レベルは大きく３つのグループに分けられることが分かった。

グループ１：端末からデータが送信されることを考えたこともなかった。

グループ２：データがアプリ開発者のもとだけに、アプリ改善のために送られていると信じていた。

グループ３：データがマーケティングに使われていることを理解していたが、データ送信の頻度や、データの送信先までは理解しきれていなかった。

6. プライバシリーク基礎実験

第２パートのインタビューは可視化機構を見た後に行われた。この結果、データは参加者あたり平均で 29 回送信されており、参加者はデータ送信の頻度に驚いていた。また、全体的に参加者はプライバシリークプロトタイプに肯定的であり、「プライバシリークによって提供される情報は有用である」、「プライバシリークのようなアプリをインストールしたい」などのコメントがあった。

JIT 条件で調査を受けた 10 人の参加者は、可視化機構に加えて JIT 通知機構を経験した。この 10 人の参加者のうち 8 人は、「プライバシリークによって提供された情報は正確か」という質問に肯定的に答えていた。音情報や触感情報、また可視化情報のフィードバックを組み合わせることで情報の信頼性を強めることができることが分かった。

7. まとめ

Balebako らは、ユーザのデータ送信に関する理解についての知見を報告した。ほとんどの参加者は、送信されるデータの頻度とデータの送信先を認識していなかった。今後 Balebako らは、スマホアプリを利用するにあたってのプライバシ漏えいに対するユーザの意識を改善することのできるツールとインタフェース、またスマホアプリにおけるユーザが不要なデータ共有を防ぐことを助けることのできる有効な制御メカニズムを調査し続ける。

参考文献

1) Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, Carolyn Nguyen: "Little Brothers Watching You:" Raising Awareness of Data Leaks on Smartphones, In Proc. of SOUPS, 2013
2) M. Bohmer, B. Hecht, J. Schoning, A. Kruger, and G. Bauer. Falling asleep with angry birds, facebook and kindle: a large scale study on mobile application usage. In Proc. of MobileHCI, 2011.
3) J. L. Boyles, A. Smith, and M. Madden. Privacy and data management on mobile devices. Pew Internet and American Life Project, Aug. 2012.
4) A. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner. Android permissions: User attention, comprehension, and behavior. In Proc. of SOUPS, 2012.
5) P. Kelley, S. Consolvo, L. Cranor, J. Jung, N. Sadeh, and D. Wetherall. A conundrum of permissions: Installing applications on an android smartphone. In Proc. of USEC, 2012.
6) S. Consolvo, J. Jung, B. Greenstein, P. Powledge, G. Maganis, and D. Avrahami. The Wi-Fi privacy ticker: improving awareness & control of personal information exposure on wi-fi. In Proc. of Ubicomp, 2010.
7) L. Cranor, P. Guduru, and M. Arjula. User interfaces for privacy agents. TOCHI, 13(2):135{178, 2006.
8) P. G. Kelley, L. Cesca, J. Bresee, and L. F. Cranor. Standardizing privacy notices: an online study of the nutrition label approach. In Proc. of CHI, 2010.
9) A. Felt, S. Egelman, M. Finifter, D. Akhawe, and D. Wagner. How to ask for permission. In Proc. of HotSec, 2012.
10) P. Hornyack, S. Han, J. Jung, S. Schechter, and D. Wetherall. These aren't the droids you're looking for: retrofitting android to protect data from imperious applications. In Proc. of CCS, 2011.
11) W. Enck, P. Gilbert, B. Chun, L. Cox, J. Jung, P. McDaniel, and A. Sheth. Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones. In Proc. of OSDI, 2010.