Poster: Fine-Grained Locking System for Data and Applications in Smartphones

Ildar Muslukhov, Yazan Boshmaf and Konstantin Beznosov
Electrical and Computer Engineering
University of British Columbia
2332 Main Mall,Vancouver, Canada
Email: {ildarm, boshmaf, beznosov}@ece.ubc.ca

Cynthia Kuo and Jonathan Lester
Nokia Research Center
Palo Alto, California, USA
Email: {cynthia.kuo, jonathan.lester}@nokia.com

I. Introduction

Smartphones have become truly ubiquitous devices and it is hard to imagine our daily life without them. Today's modern smartphones offer a diverse set of services and rich functionalities, which include gaming, web browsing, emails, GPS navigation, voice search and high definition video. Such rich functionalities attracted a large number of smartphone owners (referred to as users), and as a result, smartphones overtook laptops and desktops in terms of the number of sold items per year [1]. Such success, however, made these devices an attractive target by adversaries, and consequently lead to a growth in the number of malware types on smartphones [5]. The number of lost, misused, stolen or damaged smartphones has also increased over the years [2]. Moreover, adoption of smartphones by companies has created new attack vectors on the corporate data, where sensitive and confidential data are at a greater risk due to the higher mobility of smartphones [3].

A lot of attention has been paid from the research community to the malware threats to data in smartphones [7]. Still, there has been little attention paid to the physical threats, such as theft, loss, damage or malicious use of the device by an adversary. The aforementioned threats might lead to the highly probable risks of an unauthorized data access or data loss. Symantec reports that in 96% of cases when a smartphone is lost, a person who finds it tries to access sensitive data such as social networking applications, emails, pictures, passwords, and banking applications [8]. Furthermore, recent research shows that users do store sensitive data, such as personal pictures, passwords (both in clear and in password managers), email and SMS messages. However, around half of them do not use a locking system (with a PIN-code, Draw-a-Secret or a password) [9]. The participants of the aforementioned study justified their decision not to use a locking system by the necessity to have an instant access to non-sensitive data and applications in their smartphones. Futhermore, results of this study suggest that a locking system should consider sensitivity of separate data items, because sensitivity depends on the content of a data item, which means that an application could contain sensitive and non-sensitive data.

Recent studies show that Authentication Methods (AMs) that are based on a PIN-code or Draw-a-Secret (DAS) do not provide an adequate protection against an adversary who has physical access to the device and who can observe smartphone users. For instance, De Luca et al. [6] showed that most of the users do not protect PIN-codes from eavesdroppers when accessing ATM machines, Zakaria et al. [12] showed that one attempt is enough to capture a DAS authentication secret, and Raguram et al. [11] presented surveillance tools that allows an adversary to capture what users type into smartphones from reflections of the smartphone's display off other objects in the environment, such as sun glasses.

Diverse and dynamic environments where smartphones are being used today make the problem of data protection harder. Oulasvirta et al. [10] showed that users' interactions with smartphones are usually very short in length and users are frequently distracted (every four seconds) from their smartphones by many external factors, e.g., necessity to look where a users is walking or maintaining a conversation with a friend. Lack of attention makes AMs more vulnerable to eavesdropping attacks, because users do not check whether they are being observed. Furthermore, short nature of users' interactions with smartphones forces security tools to compete for users' attention with primary tasks on smartphones, such as sending messages or browsing.

In this poster, we present the design of the study that aims to address the aforementioned limitations of existing smartphone locking systems. In particular, we aim to design and evaluate a system that allows users to lock data items within applications and applications' functionalities. We then present the study design that aims to evaluate the efficiency and the effectiveness of the proposed locking system.

II. Our Approach

There are several ways to improve security of the smartphone locking system against an adversary who is able to observe a user during an authentication process and get a physical access to the victim's smartphone. For instance, AMs based on "something you are" could be used, such as finger print scanner or face recognition. These methods, however, require smartphones to have special hardware and are easy to circumvent [4]. Alternatively, AMs based on "something you have" can be used instead, as they are highly usable and do not require a user to remember and type a secret or password. This is often achieved by employing a hardware token (e.g., NFC or RFID) that allows users to lock and unlock a smartphone on the basis of users' proximity to the device. Still, such an approach requires users to take care of yet another device. Moreover, the hardware token can be still stolen with the smartphone itself.

AMs which are based on a secret knowledge, i.e., "something you know", are very common in smartphones. The resistance of these AMs to eavesdropping attacks could be improved in two ways. First, the frequency of the authentication prompts could be reduced, which might lead to the increase in the time needed for an adversary to get an authentication secret. Second, a stronger AM, e.g., alpha numeric password, could be used. Unfortunately a small user interface in smartphones makes it hard to type long and complex passwords, and thus, if such AM is used it could impede adoption of the locking system. On the other hand, less frequent authentication prompts might potentially convince users to use a stronger "something you know" AMs.

In order to reduce the frequency of authentication prompts, we propose to lock only data and applications' functionalities which are sensitive to the user. Such a locking system requires the following capabilities:

- An access to the list of data items and functionalities within an application in order to allow users to define the protection scope, i.e, what needs to be locked.
- The detection of every access to the locked data or applications' functionalities in order to enforce the appropriate defense actions (e.g., audit record, re-authentication).

We believe it is desirable to implement the proposed locking system as an extension to the mobile OS, so as to avoid breaking existing third party applications. Such an approach, however, might have problems with the visibility of data items and applications' functionalities. For instance, an application might store data in a proprietary format or store it online, so that the locking system would not be able to monitor each data item correctly. This is why we consider two different perspectives in the design of the locking system for data items, applications and applications' functionalities.

OS perspective: First, we plan to extend the Input Output (IO) layer of the Android OS in order to detect when an application gets an access to the data. Additionally, we plan to extend the Graphic User Interface (GUI) libraries and bind them with the IO layer in order to trace which data access is generated by users' interactions with a smartphone. We need the GUI extension, in addition to the IO extension, because we (1) focus on users' access to data, and (2) an access by a user to data items or functionalities would not necessarily generate an IO operation or an IO operation might be triggered without users' interactions. Moreover, the GUI extension will allow us to detect when particular features of the applications are being used. We also plan to investigate the visibility of applications' data items and their functionalities to the OS for the configuration purposes.

In order to evaluate the effectiveness of the proposed locking system, we plan to use the top 30-50 third party applications from the categories which were identified as sensitive in the previous study [9], such as social networking applications, email clients, GPS routes tracking systems. Users' interactions will be simulated with the aforementioned applications on the OS with the prototype of the proposed locking system. During such interactions we plan to measure how many data accesses the proposed locking system would be able to detected. Finally, we plan to evaluate the efficiency of the proposed system by measuring the introduced overheads.

Third Party Applications Perspective: In the case of applications with hidden data or functionalities, we plan to propose an API that will allow third party applications to (a) report the list of its data items and functionalities, (b) check whether a data item or functionality is locked by a user, and (c) report when the locked data item or application's functionality is accessed by a user. We plan to perform a case study on several open source mobile applications in order to evaluate the proposed API on the amount of changes required, i.e., the number of additional lines of codes.

References

[1] Gartner highlights key predictions for it organizations and users in 2010 and beyond. http://www.gartner.com/it/page.jsp?id=1278413. last accessed August 18, 2011.

[2] Lost and found: The challenges of finding your lost or stolen phone. http://blog.mylookout.com/2011/07/lost-and-found-the-challenges-of-finding-your-lost-or-stolen-phone/. last accessed August 18, 2011.

[3] 2010: Anual study: Global cost of a data breach. http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon, 2011.

[4] John Callaham. Galaxy nexus android 4.0 face unlock broken by picture. http://www.neowin.net/news/galaxy-nexus-android-40-face-unlock-broken-by-picture. last accessed March 4, 2012.

[5] Eric Chien. The motivations of recent android malware. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/motivations_of_recent_android_malware.pdf, 2011.

[6] Alexander De Luca, Marc Langheinrich, and Heinrich Hussmann. Towards understanding atm security: a field study of real world atm use. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 16:1–16:10, New York, NY, USA, 2010. ACM.

[7] William Enck, Peter Gilbert, Byung-Gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N. Sheth. Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones. In *Proceedings of the 9th USENIX conference on Operating systems design and implementation*, OSDI'10, pages 1–6, Berkeley, CA, USA, 2010. USENIX Association.

[8] Symantec Inc. Webview. http://www.symantec.com/about/news/resources/presskits/detail.jsp?pkid=symantec-smartphone-honey-stick-project, 2012.

[9] Ildar Muslukhov, Yazan Boshmaf, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov. Understanding users' requirements for data protection in smartphones. In *Workshop on Secure Data Management on Smartphones and Mobiles*, 2012.

[10] Antti Oulasvirta, Sakari Tamminen, Virpi Roto, and Jaana Kuorelahti. Interaction in 4-second bursts: the fragmented nature of attentional resources in mobile hci. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, CHI '05, pages 919–928, New York, NY, USA, 2005. ACM.

[11] Rahul Raguram, Andrew M. White, Dibyendusekhar Goswami, Fabian Monrose, and Jan-Michael Frahm. ispy: automatic reconstruction of typed input from compromising reflections. In *Proceedings of the 18th ACM conference on Computer and communications security*, CCS '11, pages 527–536, New York, NY, USA, 2011. ACM.

[12] Nur Haryani Zakaria, David Griffiths, Sacha Brostoff, and Jeff Yan. Shoulder surfing defence for recall-based graphical passwords. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11, pages 6:1–6:12, New York, NY, USA, 2011. ACM.