[Short Paper] An Approach to Address Physical Threats to Smartphones

Ildar Muslukhov, Yazan Boshmaf, Hyoungshick Kim and Konstantin Beznosov
The University of British Columbia
2332 Main Mall
Vancouver, BC, Canada
{ildarm,boshmaf,hyoung, beznosov}
@ece.ubc.ca

Cynthia Kuo and Jonathan Lester
Nokia Research Center
P.O. Box 1212
Palo Alto, CA, USA
{cynthia.kuo,
jonathan.lester}@nokia.com

ABSTRACT

In this paper we discuss a problem of data protection against the physical threats of loss and theft. We highlight the current challenges and propose a heuristic approach based on users' smartphone use patterns to address them. Anomaly detection might be effectively used for at least an additional measure with the existing authentication methods to enhance usability and security against the physical threats.

1. INTRODUCTION

Smartphones are highly popular today. In fact, in 2011 smartphones have outpaced personal computers (PCs) in the number of sold items per year [1]. One way to explain such success is by great flexibility and rich functionalities of modern smartphones. Moreover, users are able to extend smartphones' functionalities with thousands third party applications. Additionally, large storage capacities of modern smartphones made information access "on the go" much easier and faster. However, such data could be both confidential (e.g., password list, business related documents or bank statements) or sensitive (e.g., photos of family and kids, personal messages)[1]. Unfortunately, the combination of a small physical size of modern smartphones and the ease of carrying around big amounts of data creates risks to confidentiality for *sensitive* data.

Malware threats in smartphones are similar to that in PCs, since both platforms (i.e., smartphones and PCs) use sophisticated operating system (OS) today, the same notion of applications and storage. That is why it is not surprising, that malware, similar to what we have seen in desktop environments, is already moving to smartphones platforms [4].

However, everything changes when we consider factors that are specific to smartphones. First, physical size of smartphones, which not only impacts the usability of the device, but also makes it easier to lose or steal it [2]. Second, the high mobility of the devices, only makes it easer to steal the device or lose it [9]. Third, the limited user interface (i.e., small screen and keyboard) impacts security of the smartphones significantly by forcing users to employ usable, but weak authentication methods [11], which are highly vulnerable to shoulder surfing attacks [6, 14, 15]. Finally, Oulasvirta et al. [12] showed that users are distracted frequently during use of a smartphone, which significantly limits the amount of attention users are able to devote to security in smartphones. This makes eavesdropping attacks much easier, since users are not paying attention whether someone is observing them, while they are typing their credentials.

Users tend to have higher concerns with some types of sensitive data they store on a smartphone when such data are revealed to someone who knows them [11]. Someone who knows a victim (or an "insider") could be his friend, colleague, or a family member. Such an adversary would have more chances to observe how the victim uses his device, thus more chances to eavesdrop an authentication process. Additionally, an "insider" adversary have more chances of getting physical access to the device, without being noticed. Considering the aforementioned abilities of the "insider" type of adversaries in the combination with the lack of smartphone users' attention and the use of weak authentication methods, such as PIN-codes and Draw-a-Secret (DAS), makes smartphones users highly vulnerable to confidentiality breaches, especially when an adversary is able to get a physical access to the device and is able to eavesdrop authentication credentials.

On the other hand, in case of an adversary who does not know the victim (or a "stranger"), users still showed higher concerns for other types of data (e.g., contact details or GPS saved tracks). The use of a locking system with a limited number of wrong attempts based on PIN-codes or DAS might be effective against a pure random attacker who picked up a lost smartphone. However, our study [11] shows that 20% of users that stored sensitive data on their smartphones decided not to use any locking system because of the usability problems of existing locking systems. To make matters worse, a determined adversary can capture the authentication secrets (e.g., PIN or graphical password) first

[1]Throughout this paper we refer to such data as being *sensitive* for brevity.

Symposium on Usable Privacy and Security (SOUPS) 2012, July 11-13, 2012, Washington, DC, USA.

without significant effort – Zakaria et al. [15] showed that one attempt is often enough for an adversary to steal an authentication secret. That is, we need to consider alternative security systems that people might prefer by minimizing the burden of memorizing and/or requiring secrets on the user.

Even though a lot of attention have been paid to malware threats in smartphones lately [3, 5, 7], no or little attention have been paid to physical threats, such as theft and loss.

2. RISKS AND PHYSICAL THREATS

Sensitive and valuable data that are stored in smartphones have the following risks:

- **Data Loss** - valuable data could be lost.
- **Data Corruption** - valuable data could be corrupted.
- **Unauthorized Data Access** - confidentiality of sensitive data could be breached.

The aforementioned risks originates from the following physical threats:

- **Loss** of the device. Note, that by **loss** we also mean the complete damage of the device, since the later poses only **data loss** risk, when the loss of the device additionally might lead to an **unauthorized data access**.
- **Theft** of the device. Theft of the device might be permanent (e.g., an adversary steals the devices without getting it back) and temporary (an adversary steals the device, but tries to return it without being noticed). Both of these cases could lead to **data loss**, if an adversary deletes valuable data, **data corruption**, if an adversary modifies valuable data, or **unauthorized data access**, if an adversary reads sensitive data.

3. ADVERSARIAL MODEL

We plan to develop better models of the adversary. We may consider not only the adversary's knowledge about a victim but also the limited capability to access the victim's smartphone. We classify our adversaries into the following categories:

- $\mathbf{A}^{\mathbf{unlimited}}_{\mathbf{targeted}}$ - An adversary (e.g., spy) who has accumulated some knowledge about a victim's smartphone use patterns; she can freely access the victim's smartphone without limited time.
- $\mathbf{A}^{\mathbf{limited}}_{\mathbf{targeted}}$ - An adversary (e.g., close family or friend) who has accumulated some knowledge about a victim's smartphone use patterns; she can access the victim's smartphone during a limited time interval.
- $\mathbf{A}^{\mathbf{unlimited}}_{\mathbf{random}}$ - An adversary (e.g., someone who picked up a lost phone) who has no knowledge about a victim's smartphone use patterns; she can freely access the victim's smartphone without limited time.
- $\mathbf{A}^{\mathbf{limited}}_{\mathbf{random}}$ - An adversary (e.g., someone a victim meets for the first time) who has no knowledge about a victim's smartphone use patterns; she can access the victim's smartphone during a limited time interval.

In our adversarial model we assume that all adversaries mentioned above would have at least one of the following objectives:

- **OBJ1** - An adversary wants to read sensitive data.
- **OBJ2** - An adversary wants to delete or corrupt valuable data.

We note that the case when an adversary aims to steal a smartphone for its fiscal value can be considered as a special case of the **OBJ2**, because in this case an adversary will wipe-out all data in the smartphone, leading to deletion of the valuable data in a smartphone. We also do not consider an adversary that tries to get an access to the data directly on the storage card (i.e., we assume that all data on the storage cards are encrypted or the storage physically is not removable).

Physical threats by definition imply that an adversary would be able to get a physical access to the victim's smartphone. Moreover, we assume a knowledgeable adversary who knows what kind of protection system is being used by the victim, and is able to observe how the victim uses his/her smartphone, thus would be able to steal authentication secrets from the PIN-code and Draw-A-Secret (DAS) authentication methods.

Finally, we assume that an adversary is not able to bypass a reference monitor (RM) of the access control system in smartphones. This assumption, however, does not mean that an adversary cannot perform usual users' actions, such as application installation, control network connectivity and resetting the device to the default factory settings, i.e., wiping all data and applications in a smartphone. We also assume that data stored on removable memory cards are encrypted and there are no vulnerabilities in both encryption algorithm and its implementation.

4. OUR APPROACH

In order to address the aforementioned problem of physical threats we suggest to explore anomaly detection methods in data protection system (DPS). The key idea is simple: a trusted process in a mobile phone collects the phone owner's usage patterns and then trains them to build a behavioral model (BHM) of the owner. The constructed model will be used to detect whether a given usage pattern is appropriately generated by the phone owner. In the case of an "anomalous" access request, an appropriate defense action (e.g., authentication prompt or device lock) could be performed. Such an approach would allow users to use their smartphones without a need of frequent authentications, which might improve the usability of the DPS. Additionally, less frequent authentication might convince users to use a stronger authentication method (e.g., longer passwords). However, building and evaluating BHMs is faraway from being a trivial task.

First, we need to understand how to successfully build BHMs. In particular, we need to investigate what kind of users' interactions with a smartphone are highly sensitive to users. For example, we can test the possibilities of several features such as finger pressure on the touch screen, email reading/sending patterns, application usage patterns or data access patterns. In addition to these, we may use the physical location of the smartphone (e.g., the changes of network settings and a new GPS position) since an attacker may try to connect through a new WiFi access point in a novel

location. With these collected datasets, we also need to find a proper classification algorithm. So we plan to implement several different classification algorithms such as support vector machine (SVM), Markov chain, neural networks, K-Nearest neighbor and naïve Bayesian and then evaluate their performance (e.g., accuracy) and efficiency (time available for development and training). To show the feasibility of using users' smartphone use patterns, we will compare these results with the existing approaches [8, 10] which used the phone call history or location traces alone.

Second, we need to consider how to evaluate the constructed BHMs since there is no real data about real adversaries' use patterns. So we plan to perform a real-like laboratory experiment as follows: (1) recruit a group of participants for the role of victim (victim group), collect their smartphone usage patterns and build BHMs with the collected patterns; (2) recruit another group of participants for the role of attacker (adversary group), give "shallow" copies of the participants' smartphones in the victim group (by replacing real data with faked ones) to the participants in the adversary group, respectively and ask to get as much sensitive data from the assigned smartphone as possible, while trying to avoid detection. In order to obtain the validity of this experiment, the reward for a participant in the adversary group will be proportional to the information obtained from the assigned smartphone. Also, to simulate the adversaries discussed in Section 3, we measure the time used to obtain the information from the smartphones and the adversaries' knowledge levels will be controlled by instructing the participants in the adversary group on how an assigned victim uses her smartphone.

Finally, once an anomaly is detected (i.e., unusual user behavior) an appropriate defense action should be executed. Such an action could actively interfere with a user (e.g., authentication prompt) or might be passive (e.g., audit record or decoys [13]). The type of an action might depend on many factors: data type, data sensitivity, whether user have a backup copy if such data etc. We assume that a user or a company would select the best possible action for specific set of data, e.g., highly confidential business documents might be destroyed and low level sensitivity photos would trigger addition of an access audit record to the log journal.

It is unclear, however, what such actions should be from users perspective. That is why we plan to conduct a user study in order to understand what kinds of defense methods users would prefer to have in a DPS and how such actions could be supported by modern smartphone platforms.

5. 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] K. Barr, P. Bungale, S. Deasy, V. Gyuris, P. Hung, C. Newell, H. Tuch, and B. Zoppis. The vmware mobile virtualization platform: is that a hypervisor in your pocket? *SIGOPS Oper. Syst. Rev.*, 44:124–135, December 2010.

[4] E. 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.

[5] M. Conti, V. T. N. Nguyen, and B. Crispo. Crepe: context-related policy enforcement for android. In *Proceedings of the 13th international conference on Information security*, ISC'10, pages 331–345, Berlin, Heidelberg, 2011. Springer-Verlag.

[6] A. De Luca, M. Langheinrich, and H. 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] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. 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] M. Jakobsson, E. Shi, P. Golle, and R. Chow. Implicit authentication for mobile devices. In *Proceedings of the 4th USENIX conference on Hot topics in security*, HotSec'09, Berkeley, CA, USA, 2009. USENIX Association.

[9] M. Landman. Managing smart phone security risks. In *2010 Information Security Curriculum Development Conference*, InfoSecCD '10, pages 145–155, New York, NY, USA, 2010. ACM.

[10] F. Li, N. Clarke, M. Papadaki, and P. Dowland. Misuse detection for mobile devices using behaviour profiling. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 1(1):41–53, 2011.

[11] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov. Understanding users' requirements for data protection in smartphones. In *Workshop on Secure Data Management on Smartphones and Mobiles*, 2012.

[12] A. Oulasvirta, S. Tamminen, V. Roto, and J. 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.

[13] N. Provos. A virtual honeypot framework. In *Proceedings of the 13th conference on USENIX Security Symposium - Volume 13*, SSYM'04, pages 1–1, Berkeley, CA, USA, 2004. USENIX Association.

[14] R. Raguram, A. M. White, D. Goswami, F. Monrose, and J.-M. 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.

[15] N. H. Zakaria, D. Griffiths, S. Brostoff, and J. 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.