Poster: Towards an app-driven Mobile Authentication Model

Nicholas Micallef, Mike Just, Lynne Baillie, Gunes Kayacik
Interactive and Trustworthy Technologies Group,
Glasgow Caledonian University
{firstname.surname}@gcu.ac.uk

1. INTRODUCTION

By 2013 smart phones are expected to overtake PCs as the main way to access the Web [1]. This means that robust and efficient authentication and access control systems are required since smart phones are increasingly being used to access and store sensitive personal information such as emails and banking transactions. Even before the advent of smart phones, Clarke and Furnell [2] conducted a user study which showed that users of mobile devices expect that a system that can implicitly and continuously perform user authentication in the background without disrupting the normal user-mobile device interaction is the most desired mobile authentication solution. This statement was later confirmed by Jakobsson et al. [3], who state that users of smart phones find that the prompting for passwords is much more annoying than other smart phone limitations such as small screen size and limited network coverage.

But usability is not the only problem with the all-or-nothing authentication model that is currently deployed on mobile devices. Mobile devices are portable devices and might be shared among a larger amount of people in a variety of situations. In Karlson et al. [4] they investigated how and to what extent users share their phone and they concluded that current security mechanisms deployed on our mobile devices do not facilitate sharing. They also reported that users wanted to share their device but without allowing others to delete or modify data. Similarly, Stajano [5] proposed that PDAs should have two modes (public and private) and when the device is handed to another user the private mode should not be accessible. In addition, participants in a study by Hayashi et al. [6] expressed their concern regarding their children misusing their mobile phones and tablets.

Therefore, the aim of this research is to define an authentication model which improves the user experience and facilitates sharing on a mobile device without reducing the security level. To achieve this goal we need to move beyond the current binary security model that offers all-or-nothing access to the phone and make use of background sensors to define passive (in the literature it is also referred to as 'implicit') authentication only in circumstances where authentication is "necessary". Inbuilt sensors include those that collect data in the background, related to acceleration, orientation, light, sound, magnetic field, Wi-Fi, etc. As a first approach, we define which situations require passive authentication according to the level of sensitive personal information that is accessed or stored by each application. The user is only prompted with an explicit authentication mechanism when passive authentication fails.

2. RELATED WORK

Recently researchers started looking into ways in which they could minimize the use of locking mechanisms such as PINs with the aim of finding an optimal balance between security and usability during authentication. Hayashi et al. [7] introduce CASA, a context-aware scalable authentication in which they choose the type of unlock mechanism to use (none, PIN or password) according to a number of passive factors such as user's location. They conducted 2 studies to evaluate the feasibility and users' receptiveness of this authentication model. They report that with this model they were capable of reducing the number of explicit authentications by 68%. They also claim that more than half of their participants preferred to use this authentication model compared to the one that they were previously using. Hayashi et al. [6] also evaluate the impact of making some applications available without the need to unlock the device. They show that this small change can make quite a significant difference in the number of unlocks that a user would have to perform.

Both works from Hayashi et al [6, 7] are very relevant to this research since we share the main goal of finding an optimal balance between security and usability during authentication on mobile devices. When building our model we use the concept of passive factors (also known as implicit factors) which is used in both [7] and [8]. What makes our research different from [7] is that we use these passive factors only on specific occasions rather than each time a user wants to unlock their phone, this is because as defined in [6] most of the applications do not require explicit authentication.

3. AUTHENTICATION MODEL

The main idea behind the authentication model that is being investigated by this research is to reduce the number of unlocks by removing the unlock mechanism which is normally prompted when a user starts a new session on his phone and to passively/implicitly check for authentication only when applications that access or store sensitive personal information are used. Background sensor data will be continuously collected by a separate process. In related work, Hayashi et al. asked users to list the top 20 applications and determine whether they want some or all of the functionality of these applications available when the device is in an unlocked state [6]. In this case, users wanted almost half of the applications to be available when the device is in an unlocked state and the other half available when the device is in a locked state. In the case of our authentication model we decided to classify applications into security levels according to the amount of sensitive personal information that they access and store (refer to Table 1). Sensitive personal information is defined as information that once it is associated with a user's identity then it becomes a potential threat to the user's privacy [9]. The initial classification of applications into these different security levels could be achieved by implementing one of these techniques: (1) User classifies applications ahead of time; (2) Manufacturer or application provider (Google play or apple app store) classify the apps themselves; (3) Application classification is done automatically based upon for example the type of permissions that are used by the app or according to the generic category (e.g. Entertainment) of that particular app.

Table 1. Security levels according to usage of sensitive info

	Criteria
Level 1	no access & storage of sensitive personal info
Level 2	partial access & storage of sensitive personal info
Level 3	continuous access & storage of sensitive personal info

Initially we use standard application categories [10] to generically classify applications into these three security levels (as in Table 2). We plan to consider other methods later, such as confirming our choices with users.

Table 2. Generic classification of application categories

Level 1	Level 2	Level 3
Sports, News, Entert, Multimedia, Comics, Games, Lifestyle, Travel, Reference, Themes	Shopping, Productivity, Browser, Health, Tools, Libs & Demos	Finance, Communication, Social, Settings

Each time that an application is accessed the system determines what type of application it is by using the criteria in Table 1. If it is an application from 'Level 1' the system will not perform any type of authentication. If it is an application from 'Level 2' the system will take a couple of passive factors (e.g. location + orientation) from the background sensor data and check whether they follow the usual patterns of that particular user. If the just collected sensor data does not follow the usual patterns the user is asked to authenticate using his preferred active authentication mechanism (PIN, password etc). If it is an application from 'Level 3' the system will take a more detailed set of passive factors (e.g. location + light + noise + orientation) from the background sensor data and check whether they follow the usual patterns of that particular user. If the just collected sensor data do not follow the usual patterns the user is asked to authenticate using his preferred active authentication mechanism. It is important to note that if in the same session a user moves from a 'Level 2' application to a 'Level 3' application and the system would already have authenticated the user explicitly to access the 'Level 2' application then the authentication model would not ask the user to authenticate again.

We hypothesize that with this model we manage to reduce the number of times that the user would need to authenticate in a particular day but at the same time keep an almost similar level of security that the users experienced when using an all-or-nothing security model.

Table 3. Criteria for Authentication decision

	Passive factors
Level 1	No check
Level 2	Passive factors: Location + Orientation
Level 3	Passive factors: Location + Light + Noise + Orientation

4. CONCLUSION AND FUTURE WORK

We are currently finalizing (1) the best way to initially classify the applications using the criteria in Table 1; (2) the analysis of the passive/implicit sensor data to define what passive factors (refer to Table 3) to use to decide whether or not, to ask for active authentication mechanisms when using applications that are classified as 'Level 2' and 'Level 3'. Afterwards, a prototype that implements this authentication model will be deployed so that we can carry out a number of evaluations which will measure the effectiveness of this authentication model from both a usability and security perspective.

5. REFERENCES

[1] Gartner forecast: http://news.cnet.com/8301-1001_3-10434760-92.html

[2] Clarke, N. and Furnell, S. "Authenticating mobile phone users using keystroke analysis". In Information Security Journal, 2006.

[3] Jakobsson, M., Shi, E., Golle, P. and Chow, R. "Implicit authentication for mobile devices". In HotSec'09.

[4] Karlson, A. Bernheim Brush, A. and Schechter, S. "Can I Borrow Your Phone?: Understanding Concerns When Sharing Mobile Phones". In ACM CHI '09.

[5] Stajano, F. "One user, many hats; and, sometimes, no hat– towards a secure yet usable PDA". In Proceeding of Security Protocols Workshop. 2004.

[6] Hayashi, E., Riva, O., Strauss, K.,Bernheim Brush, A. and Schechter, S. "Goldilocks and the two mobile devices: going beyond all-or-nothing access to a device's applications". In ACM SOUPS '12.

[7] Hayashi, E., Das, S., Amini, S., Owusu, E., Han, J., Hong, J., Oakley, I., Perrig, A. and Zhang, J. "CASA: A Framework for Context-Aware Scalable Authentication". In U-PriSM 2012 Workshop.

[8] Gupta, A., Miettinen, M., Asokan, N. and Nagy, M. "Intuitive Security Policy Configuration in Mobile Devices Using Context Profiling". In IEEE SocialCom 2012.

[9] Bettini, C., Sean Wang, X. and Jajodia, S. "Protecting privacy against location-based personal identification". In Springer-Verlag SDM'05.

[10] Böhmer, M., Hecht, B., Schöning, J., Krüger, A. and Bauer, G. "Falling asleep with Angry Birds, Facebook & Kindle: a large scale study on mobile app usage". In ACM MobileHCI'11.