ABSTRACT

Possible attacks on mobile smart devices demand higher security for applications handling payments or sensitive information. The introduction of a tamper-proof area on future generations of mobile devices, called Trusted Execution Environment (TEE), is being implemented. Before devices with embedded TEEs can be deployed to the public, investigations on usability aspects of Trusted User Interfaces (TUI) are needed. This article describes the process we have followed at gathering requirements, prototyping and testing suitable designs for TUIs in combination with a touch-screen biometric system. At the end, we present relevant findings of a pilot study that we have conducted using an Experience Sampling Method (ESM) as part of our ongoing work.

Categories and Subject Descriptors
H.5.2 [Information Interfaces and Presentation]: Input devices and strategies

General Terms
Human Factors, Design, Security

Keywords
Usable Security, Secure Mobile UIs, Trusted Executing Environment, Biometrics, Experience Sampling Method

1. INTRODUCTION

Recent previous studies conducted by us and others have shown that users of mobile phones can be identified by the way they swipe their finger on mobile touch-screens [2, 5, 17, 38]. This type of behavioural biometrics in combination with graphical passwords can be used as a two-factor authentication mechanism towards existing mobile devices.

Not only can mobile devices become more secure with this approach, but also the usability and memorability aspects of graphical passwords can be exploited to provide a more seamless authentication experience than the use of PINs and passwords on small touch-screen keyboards.

Simultaneously, investigations for deploying a so called Trusted Execution Environments (TEE) embedded in future mobile devices are currently ongoing [19, 20, 29, 41, 42]. The use of such TEE would provide portable smart phones with yet one more level of security. Thus, a three-factor authentication can be achieved with the combination of a secret graphical password (something the user knows), a trusted mobile device (something the user possesses) and the users’ behavioural biometrics (how the user acts).

However, it has been recognized that human factors play an important role on the acceptability and usability of security and biometrics systems [14, 15, 21, 30]. Therefore, in order to successfully deploy trusted environments and introduce behavioural biometric mechanisms on mobile devices it is necessary to study and analyze the users’ acceptance and perception of these approaches.

In this paper we present our initial investigations on the design of usable mobile Trusted User Interfaces (TUI) that allow users to interact with the protected information accessible from within the TEE. Also, we explore the impact on users’ satisfaction and comprehension when employing one kind of recall-based graphical password enhanced with biometrics, namely Android’s unlock patterns, as a mechanism for authenticating into this secure environment and also as a method for providing informed consent and electronic signing.

Using Experience Sampling Method (ESM) [27] as our methodological approach we developed an Android application that could capture the opinions of users as they performed a series of fictitious online transaction in situ. We report the relevant findings of a pilot study that has been carried out using this method over a one week period.

The paper is structured as follows. Section 2 presents background information on mobile authentication mechanisms, the TEE and the ESM. Section 3 describes the creation of mobile e-commerce transactions scenarios and the setup of our experiments. Section 4 presents preliminary findings from a pilot study. Finally, Section 5 ends the paper with conclusions and descriptions of future work.
2. BACKGROUND

With the increased use of mobile devices and the large amounts of important information that we store in these devices, appropriate mechanisms to guard their contents are needed. Currently, most of the solutions for authenticating users into their mobile devices are based on the same mechanisms used for authenticating users into desktop computers, which do not scale well for mobile environments or do not meet appropriate security levels. These include 4-digit PIN codes, text-based passwords or external hardware devices.

2.1 Authentication approaches in mobile devices

Previous studies have shown users’ concerns with current authentication methods [24] and their interest to have more secure methods for protecting the information contained in their mobile devices [6]. Other studies also indicate that users are not willing to trade convenience for perceived increased security at the moment of authentication [43], and also that providing increased levels of security might result in negative perceptions of the interface [31]. It is also known that people tend to choose weaker, shorter and repetitive passwords, since typing on touch-screen keyboards becomes more cumbersome and slower than in regular keyboards [22], and because individuals’ ability to recall multiple numbers and strings is limited [1, 46].

Many graphical password schemes have been suggested as a way to improve memorability and usability at the moment of authentication [7]. The Android’s mobile operating system introduced a recall-based graphical password commonly known as unlock pattern as an approach for locking the screen of mobile devices. Contrary to PIN codes and text-based passwords, unlock patterns take advantage of users’ ability to remember images better than numbers [33], and of their motor memory [44] created by repeatedly moving their finger in a similar fashion several times. Moreover, unlock patterns do not force users to type in small touch-screen keyboards and they do not require any additional hardware. Figure 3(b) shows an example of an unlock pattern.

However, weaknesses of Android unlock patterns have been identified, such as their small password space (low entropy) and their vulnerability to smudge attacks [4] and shoulder-surfing attacks [16, 45] (but which also threatens PIN codes and passwords [36]). Nevertheless, it has been shown that enhancing unlock patterns with biometric characteristics is a promising approach towards rising the security level of this type of graphical password while at the same time retaining its usability benefits [2, 17].

2.1.1 Using biometrics in mobile devices

Several attempts have been made for introducing behavioural biometric schemes into mobile devices with varying degrees of security and usability performances.

Common approaches include the studies on users’ typing rhythms on the device’s keyboard, as presented in [12, 11, 28, 32, 34, 47] and others. More unobtrusive approaches of continuous authentication include gait biometrics [9, 18, 23, 35], the unique way a person moves her hand to her ear when answering a phone call [13], identifying users through their routine behaviours [39], and more.

Recently, touch-screen biometrics have also been explored as a possible authentication mechanism. Our initial research work in this area, presented in [2], considers two biometric features applied to Android unlock patterns of 6 dots, namely the time the user’s finger is inside a dot (finger-in-dot) and the time the user’s finger travels between two dots (finger-in-between-dots).

The performance of biometric systems is often compared in terms of different error metrics, so called False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate. FAR represents the probability that an intruder is wrongly identified as a legitimate user, commonly used as a measure of the system’s security. FRR is the probability that a legitimate user is wrongly identified as an intruder, used as a measure of the system’s usability. EER is the point where FAR and FRR are equal. Depending on the level of security or usability required by a certain application, the FAR and FRR probabilities can be traded-off (the smaller FAR provides a greater FRR, meaning greater security and decreased usability, and vice versa). Using a Random Forest machine learning classifier [10] and without any other analytical enhancements to the data, the results in [2] indicate that a FAR of 10% provides a FRR of approximately 11.08%, giving an EER of 10.39%. This analysis was done considering three different lock patterns, suggesting that users can be identified to this rate regardless of the pattern they draw. Also, these results show that unlock patterns can provide greater security than 5 digit PIN codes and become a two-factor authentication mechanism [2].

Similarly, the work in [17] tested the performance of an unlock pattern biometric system in a long-term real world study. They asked participants to draw predefined 5-dot unlock patterns one time a day over a period of 21 days. An email reminder was sent everyday to each participant over that period. The biometric features measured included the X- and Y-coordinates, pressure, size, time and speed. Using a Dynamic Time Warping classifier (DTW) [25], a FAR of 21% and FRR of 19% were obtained.

Furthermore, a commercial solution has been attempted, as presented in [5], but the performance metrics are not publicly available, neither are results presented of testing under real conditions.

Although these results do not yet provide optimal performance, they are a promising indication that individuals can be recognized by the way they draw an unlock pattern on a touch-screen. More studies are needed on the effect of the relation of contexts in which the unlock patterns are drawn and their performance. Also, on the user experience of this type of authentication. These challenges are being tackled by our current work.

2.2 Trusted Execution Environment (TEE)

In general terms, a Trusted Execution Environment (TEE) is a technology that offers a standardized way to provide trust and security services to common mobile applications that are run on the normal application environment of the device, so called “Rich OS”.

The TEE provides a privileged execution environment in the mobile device, which is separate from the ordinary execution environment running common applications. From within this privileged environment, or TEE, it is possible to control access to peripherals and/or data storage. To make this possible, the TEE provides services to Rich OS applications through a TEE client API.

Furthermore, within the TEE framework it is possible to build trusted applications that can interact with the display
and the touch-screen, effectively creating a so called Trusted User Interface (TUI). The TUI enables trusted applications to securely capture users’ consent that cannot be circumvented by an attacker.

2.3 Experience Sampling for data collection

In order to study the user experience of a usable TUI and of unlock pattern biometrics we consider the Experience Sampling Method (ESM). ESM allows researchers to capture the experience in situ of certain cohorts of users [27, 37]. One of its purposes is to minimize retrospective bias by asking participants to produce accurate accounts of their actions, surrounding contexts, emotional states and opinions as they unveil in their natural environment.

Traditionally, applying this method requires participants to record a dairy description of their momentary experiences and surrounding environments as they go on with their daily activities. Nowadays, the use of smart phones allows for more sophisticated ways of capturing those experiences and contexts, and collecting data quicker and more efficiently. Also, participants can be signalled to record their experience in an easy way.

More detailed descriptions on the way we implemented the ESM is given in Section 3.2.2.

3. EXPERIMENTAL APPROACH

The aim of our investigations is to create a better understanding of the experience of users as they carry out a mobile transaction, assuming that their sensitive information is stored on the mobile device (accessible by unlocking the TEE), and that an unlock pattern mechanism enhanced with biometrics can be used to grant them access to the TEE and to electronically sign transactions.

In order to accomplish this we have carried out two main activities: defining requirements for a secure usable TUI through e-commerce scenarios and evaluating these scenarios under real use contexts. The following sections describe the approach taken within these two activities.

3.1 Defining mobile e-commerce scenarios

In order to conceive user-friendly interfaces for the TEE, we generated a series of e-commerce scenarios resembling the steps that a user would take when engaging on an online transaction with the use of a mobile device, and we tested those scenarios with paper prototypes, depicted in Figure 1. The functional and usability requirements for these scenarios were discussed iteratively with industry partners of the U-PrIM research project, including members of a well-known Scandinavian banking institution (Nordea Bank in Denmark) and a world leader organization in digital security (Gemalto). Their domain expertise from previous studies provided valuable insights into the behaviour of users when performing Internet banking, users’ mental models with regards to online transactions, the different security requirements, the specifications of a TUI, the technological limitations, and other aspects relevant for the construction of our scenarios.

From their feedback and discussions important requirements for designing usable TUIs were identified, some of which are presented in the following points:

A.1 Users should be able to recognize that they are acting in a secure environment in their device. The TUI’s interface elements, themes and layouts should help users understand the moments at which they are acting in the TEE as opposed to other application.

A.2 Users should know and feel that the information accessible via the TUI is secured. The interface should convey to users the notion that the credentials, keys and other information accessible only from the TUI is safe and cannot be attacked (i.e., cannot be affected by malware).

A.3 Users should be guided through the transaction with as little burden as possible, as long as security and privacy requirements are met. During mobile transactions, the interface should be kept clean and convey only the information necessary for the transaction, offering more convenience and effectiveness to users. Display reasonable default values when appropriate.

A.4 Users should be able to securely provide informed consent. The interface elements should make users aware of the information that is about to be sent and on what they are agreeing to. Also, the signing mechanism should provide high assurance that the right user is performing the transaction.

A.5 Users actions should be mapped to the elements in the user interface. Our approach suggests the use of touch-screen biometrics not only as a way to authenticate towards the TEE containing users’ credentials, but also as a way to enable electronic signing of transactions. However, it is crucial that the interface helps users understand that these give two different outcomes.

Moreover, from our discussions and the literature specializing on the human factors that influence biometric systems, we considered the following points as important in our approach of using touch-screen biometrics as a method for authentication into the TEE:

B.1 Biometrics should be handled under the user’s control. For privacy and security reasons, the user’s biometric template should be stored locally on the device and

under the user’s control [40]. All the matching of the template against an authentication attempt should be calculated on the device.

B.2 The enrollment process is crucial for the effectiveness of the biometric system [14, 30]. The interface should guide the users through the enrollment process in an understandable way. The work presented in [2] showed that as few as five enrollment trials are necessary to achieve an $EER \approx 14.08\%$ in an unlock pattern biometric system.

B.3 Users should be aware that their biometrics are being recorded. The interface should inform users when their biometrics are being used. This might have an impact on the way users behave when trying to draw an unlock pattern, perhaps by moving their finger in a more consistent manner, which can influence the FRR of the system.

B.4 Users should have a fall back strategy in case the biometric system fails to identify them. It can be in the interests of the stakeholders supplying a biometric solution to provide their customers with an alternative way of authenticating. However, careful consideration has to be placed on the alternative strategy given, since this can compromise security.

B.5 The decision threshold is dependent on the risk level of the transaction. Lowering the threshold would improve usability, while increasing it would give more security.

B.6 An adapting factor should be considered. In order to adapt to the contextual changes of the user over time, an ageing or adapting factor can be considered, as presented in [3], where the oldest trials are weighted less and newer successful authentication attempts are considered as additional training trials.

3.1.1 Meeting requirements through a User Interface

As a result of our discussions, a series of concrete scenarios were sketched and prototyped using the wireframing tools Axure RP 6 and Balsamiq 2.1 (Figure 2). The scenarios were divided into two main types, low-risk and high-risk transactions, depending on the quantity of the payment or the amount of information to be sent for the transaction taking place (in reality, a risk assessment would be needed to determine the type of transaction). These scenarios envisioned the creation of a secured mobile application that would be offered, for example, by a bank to its customers.

This application would let users securely access their information, such as credentials and encryption keys that are contained securely in the TEE of the device, and use those credentials at the moment of carrying out online transactions. In order to access their credentials the application would ask users to authenticate to the TEE by drawing an unlock pattern.

Biometrics on unlock patterns, as presented in [2], would be employed to verify if the person trying to use the TUI is the legitimate user (Figure 2(b)). At this point a visually contrasting icon is shown to indicate users that their biometrics are being recorded (requirement B.3).

If the user succeeded to authenticate, the application would show a subtle transition to visually indicate to the user that the TEE is being accessed, and a reversed transition would be shown when the user leaves the TEE (requirement A.1). The TUI is made visually distinguishable from other common applications’ interfaces by the choice of colours and layout (requirement A.2).

After authenticating to the TEE, the credentials requested by the service provider would be automatically selected by the application (requirement A.3) as seen in Figure 2(c), but users would be given the opportunity to choose different values if they want to.

By selecting a button reading “Pay & agree” (or “Agree & send” in case no money is involved in the transaction) users would be approving the transaction by agreeing to send the specified payment and/or disclosing the selected credentials (Figure 2(c)). Depending on the transaction, the most relevant information would be placed prominently at the top in the form of a question. The button is placed just below the question with the intention of making users more aware of what they are consenting to (requirement A.4).

Depending on the risk level of the transaction, the strictness level of the of the biometric system would vary by choos-
and the authentication trial.
lates the distance between the mean of the enrollment trials
distance, as presented in [3], which, in simple terms, calcu-
tions electronically was implemented based on a Manhattan
used to authenticate users into the TEE and sign transac-
scenarios of the developed application. The biometric system
Figure 3 shows the look-and-feel of one of the high-risk sce-
low-risk scenarios and six high-risk scenarios were developed.
scenarios discussed in Section 3.1. In total, seven different
enrollment trails.
Participants by storing their fictitious credentials and biometric
One of the modules handled the registration of the test par-
e-commerce scenarios under natural settings.

In order to help users differentiate the action that they
were taking as they draw an unlock pattern, a button at the
bottom of the unlock pattern was displayed reading either
‘Login’ for authenticating to the TEE or ‘Sign’ for signing
the transaction (requirement A.5). Using biometrics in com-
bination with the TEE provides liability towards the bank,
similar to a real paper signature in traditional transactions,
and can serve as high assurance that the person performing
the transaction is who she claims to be.

3.2 Evaluating the identified scenarios under realistic contexts of use - Pilot study

Based on the specified requirements and the interface ideas
created on the prototyped scenarios, a mobile application
was developed using Android’s platform [26]. The intention
of the application is to implement a tailored version of
the Experience Sampling Method (ESM), described in Sec-
tion 2.3, suited for capturing the in situ user experience of
e-commerce scenarios under natural settings.

3.2.1 Implementing a ESM mobile application

The application itself consisted of three main modules.
One of the modules handled the registration of the test par-
ticipants by storing their fictitious credentials and biometric
enrollment trails.

Another module consisted on the implementation of the
scenarios discussed in Section 3.1. In total, seven different
low-risk scenarios and six high-risk scenarios were developed.
Figure 3 shows the look-and-feel of one of the high-risk sce-
narios of the developed application. The biometric system
used to authenticate users into the TEE and sign transac-
tions electronically was implemented based on a Manhattan
distance, as presented in [3], which, in simple terms, calcul-
ates the distance between the mean of the enrollment trials
and the authentication trial.

In order to collect opinions and context information from
users as they performed the scenarios, a third module con-
sisted on a questionnaire engine based on the open source
platform Open Data Kit (ODK)2 [8]. ODK provides a set
of tools to perform on-the-field collection of data. We in-
tegrated parts of ODK into our application to be able to
collect the opinions and contexts of test participants after
every time they were signalled to carry through the step of
a transaction scenario. The questions that were asked de-
pended on the risk level of the scenario performed.

3.2.2 In situ user evaluations

A pilot study has been carried out with 21 participants. Par-
ticipates were invited for participation via a Facebook
event, with the prerequisite to own an Android mobile de-
vice. Individuals that agreed on participating were given
a link to download the application and a document with
information about the test.

Recruited participants were 7 females and 14 males with
an average age of 24 years old, all of them coming from
Sweden. 15 participants stated that they lock their phone’s
screen, 8 of them using a PIN code and 7 using an unlock
pattern (none using a password).

During the registration process, these participants were
asked to provide their phone numbers as unique identifiers,
and other personal attributes with the intention of giving a
more personalized experience to the evaluations of the sce-
narios. Then participants were enrolled into the biometric
system by asking them to choose an unlock pattern consist-
ing of at least six dots and to repeat it 10 times. A dialog
was first shown informing participants why this was done
and how to do it (satisfying requirement B.2 presented in
Section 3.1). The participants’ information was saved lo-
ally on their phones, but the biometric data was sent to
a server with the intention of analysing the performance of
this system under different contexts of use (in reality, the
user’s biometrics would always be stored locally on the de-
vice). Due to the relatively small amount of participants
and received trials, an analysis of the performance of the
biometric system is not presented in this paper. At the end,
participants answered a registration questionnaire with de-
mographic information, as well as their habits with mobile

2ODK: Open Data Kit (http://opendatakit.org/)
phones and online shopping.

After registration, participants were instructed to wait for a signal where they would be asked to complete a transaction and answer a questionnaire. Following the guidelines in [27] we used a so called signal-contingent recording approach, in which participants receive a periodic signal or indication when they should perform a given task. We used scheduled SMS messages to signal participants three times a day (morning, afternoon and evening) for a period of one week. Each SMS contained a link that opened the application on a particular scenario.

To motivate participants to send in their responses, they were told that each submitted entry would grant them a ticket in a lottery where they could win movie tickets and smaller prices. In total, 17 SMSs were sent to each participant requesting them to submit a transaction, and a general response rate of 78.15% was obtained.

The questions asked after a transaction was completed were the same for all participants. However, participants did not succeed to login to the TEE due to the biometric system they were presented with slightly different questions. Questions measured participant’s emotional state, their context in which they performed the transaction, their understanding of and satisfaction with the unlock patterns and with the transaction in general, their feeling of security when interacting with the TUI, and others. Furthermore, biometric data was collected in the background along with the devices’ model number, the type of scenario and the number of attempts it took the participant to draw the unlock patterns successfully.

4. FINDINGS FROM THE PILOT STUDY

From the collected information interesting conclusions can be drawn. The following paragraphs list some of the relevant findings of this pilot study:

The performance of the biometric system affects users’ satisfaction with unlock patterns, but not the overall feeling of security of the transaction. A Pearson correlation 2-tailed test revealed a significant negative relationship between the number of attempts at drawing their unlock pattern before successful biometric verification and users’ satisfaction with this kind of graphical password, $r(279) = -0.468, p < .001$; but no significant relationship was found with the perceived level of security of the transaction overall, $r(242) = -0.030, p = .640$. This implies that the usability of the unlock pattern mechanism is separated from the users’ perception of security of the rest of the application.

Participants understood that there’s a difference between using unlock patterns for authenticating and for electronic signing. From the responses to the question “Why do you think you had to enter your pattern again?” 94% of the responses correctly stated that the second pattern was used to sign a transaction and as an extra security step to assure that it was them signing the transaction. One explanation for this positive result is the use of the buttons with the labels ‘Sign’ and an information dialog shown to participants at the beginning of the application. However, this needs to be further explored.

Participant’s surroundings has no effect on the performance of the unlock patterns biometric system.

Their surroundings at the moment of carrying out a transaction were categorized as being either at home or in some kind of more social context. A 2-tailed t-test revealed that there’s no statistically significant difference between these two surroundings, $t(211) = -1.025, p = .307$. However, this doesn’t take other factors into consideration, such as their activity, their emotional state, etc.

Unlock patterns exhibited good memorability. In case users forgot their unlock pattern (which was chosen by themselves), they were given the chance to display it via a menu option. The application recorded every time this option was selected as an indication that the user had forgotten the pattern (requirement B.4). Only two participants asked to be reminded of their unlock pattern in a total of four occasions, accounting for only 1.4% of all the completed scenarios. This is an indication that users are able to remember unlock patterns in general.

Unlock patterns are preferred over PINs and strong passwords. Participants were asked if they would have preferred to use a PIN-code or strong password when carrying out a transaction, and 65.6% of their responses indicated they would not have preferred those methods. To check if the difference between their ‘no’ and ‘yes’ responses were not given by chance a chi-square test was performed, where $\chi^2(1) = 44.021, p < .001$.

Responsiveness time of the biometric system was acceptable. Although not measured empirically, it was observed that executing biometric verification on the device using a Manhattan detector [3] at the moment of carrying out a transaction does not impact the performance of the device negatively.

5. IMPLICATIONS AND FUTURE WORK

This article presented some identified requirements for developing a TUI and for securing it with touch-screen biometrics. Findings indicate that the proposed solution is well understood by users, but that efficient security mechanisms are needed to provide a good overall experience of the transaction. Our findings also support the idea that applying biometrics to graphical mechanisms for mobile authentication is worth exploring further, based on their usability, memorability and security benefits, but that performance needs improvement. Moreover, it is important to display informative interface elements at every step of a mobile transactions, since they can serve as helpful indicators of the actions a user is a about to take. A graphical TUI should make users aware of the conditions of each particular transaction and the information to be transferred at that specific moment.

From the preliminary findings and other lessons learned from the pilot study presented here, we plan to refine the application and run a formal round of testing over a longer period of time with a larger sample of participants spread over different locations. Some of the research questions that we want to address in our future testing rounds include: Do users understand what is being sent?, How are the biometrics of unlock patterns affected by the contexts of use?, Do users understand that biometric data are stored locally in a secure way under their control and that the biometric authentication is done with their device (and not with service providers)?, What is their approach if they fail to authenticate?, and others.
The evaluations being carried out have the purpose of providing us with more insights into the user experience of secure mobile transactions.

6. ACKNOWLEDGMENTS

This work is part of the U-PrIM project being funded by the Swedish Knowledge Foundation (KK-stiftelsen). We want to thank Patrick Bours, Loba van Heugten, Ernst Jöranger, Tobias Pulls and John-Sören Pettersson for their contributions and help in the project thus far.

7. REFERENCES


