Journal of Trust Management
a SpringerOpen Journal

RESEARCH Open Access

Understanding user perceptions of transparent authentication on a mobile device

Heather Crawford[1*] and Karen Renaud[2]

*Correspondence:
hcrawford@fit.edu
[1]Department of Computer Sciences and Cybersecurity, Florida Institute of Technology, 150 W. University Blvd., Melbourne, FL 32901, USA
Full list of author information is available at the end of the article

Abstract

Due to the frequency with which smartphone owners use their devices, effortful authentication methods such as passwords and PINs are not an effective choice for smartphone authentication. Past research has offered solutions such as graphical passwords, biometrics and password hardening techniques. However, these solutions still require the user to authenticate frequently, which may become increasingly frustrating over time. Transparent authentication has been suggested as an alternative to such effortful solutions. It utilizes readily available behavioral biometrics to provide a method that runs in the background without requiring explicit user interaction. In this manner, transparent authentication delivers a less effortful solution with which the owner does not need to engage as frequently. We expand the current research into transparent authentication by surveying the user, an important stakeholder, regarding their opinions towards transparent authentication on a smartphone. We asked 30 participants to complete a series of tasks on a smartphone that was ostensibly protected with varying degrees of transparent authentication. We then surveyed participants regarding their opinions of transparent authentication, their opinions of the sensitivity of tasks and data on smartphones, and their perception of the level of protection provided to the data and apps on the device. We found that 90% of those surveyed would consider using transparent authentication on their mobile device should it become available. Furthermore, participants had widely varying opinions of the sensitivity of the experiment's tasks, showing that a more granular method of smartphone security is justified. Interestingly, we found that the complete removal of security barriers, which is commonly cited as a goal in authentication research, does not align with the opinions of our participants. Instead, we found that having a few barriers to device and data access aided the user in building a mental model of the on-device security provided by transparent authentication. These results provide a valuable understanding to inform development of transparent authentication on smartphones since they provide a glimpse into the needs and wants of the end user.

Keywords: Usability; Usable security; Authentication; Transparent; Mobile

Introduction

The popularity of mobile devices is undeniable. According to the International Data Corporation (IDC), more smartphones were sold in 2012 than desktop and laptop computers combined [1]. Their popularity may be attributed in part to their increasing functionality – technological advances in computing have allowed smartphones to become increasingly powerful, which in turn supports greater functionality. Smartphones

offer a wide range of capabilities, such as email account access, news updates, access to the Internet and device location via GPS. As a result of their increased (and increasing) functionality, smartphones are able to access and store personally identifying information. Potentially private data such as medical details, sensitive business information, personal pictures and voicemails have been recovered from mobile devices, despite being deleted [2]. This confirms that users do indeed store these kinds of data on their devices.

The sensitivity and amount of information stored on smartphones underscores the need for an effective, flexible method of managing device access. Historically, passwords (including sketched varieties) and PINs have been used to protect smartphones from unauthorized access, but they are easily cracked or weakened through sharing, reuse or using weak secrets [3,4]. The cumbersome nature and unpopularity of repeatedly typing a password on a mobile device has led users to avoid accessing business data on their mobile devices [5]. Furthermore, such secret knowledge techniques provide *point-of-entry* security: once the secret has been entered, the user has access to all on-device services and data.

A better method for providing mobile device security would be to use the data-rich interactions a user has with their device to create a pattern which acts as a baseline to support comparison with users in order to verify that the current user is the owner. Such authentication, which may be based on behavioral biometrics such as keystroke dynamics and speaker verification, allow for *transparent, continuous authentication* that runs in the background as the user goes about using their device as usual. With transparent authentication, the user is no longer required to explicitly authenticate because the uniqueness in their device interactions provides the basis for authentication decisions. The biometric information may be gathered via the rich set of input sensors that characterize modern mobile devices, such as microphones, keyboards, screen-based touch input and gyroscopes. These multimedia-based sensors have the benefit of familiarity to the user since they are already used for a variety of on-device functions. The rich and potentially seamless nature of sensor-based biometric data provides transparent authentication with the possibility of providing a more granular approach to application and data access by thresholding tasks. This scheme implies that the device maintains an ongoing level of confidence that the current user is also its owner, referred to as *device confidence*. It is continuously updated based on biometric matches and non-matches. If device confidence is above a defined certainty level, called *task confidence*, then the task (or data access) is allowed; otherwise it is denied.

Transparent authentication has the following benefits over traditional methods:

Effortless: Since the behavioral biometrics are gathered in the background during regular device use, the user does not need to interrupt their tasks to authenticate.
Fine-grained access control: Traditional authentication mechanisms allows for point-of-entry authentication; once the user has provided the correct shared secret, all data and functionality on the device is accessible. Transparent authentication has the capability of providing access control on a per-task or per-data basis.
Continuous: The utilized behavioral biometrics may be selected to take advantage of the most frequently performed tasks such as typing or speaking. In this way, there is a rich source of information used to authenticate, which supports a continuous authentication

model. More information about transparent authentication on mobile devices can be gained from these publications [6,7].

Transparent authentication may elicit concerns regarding privacy, among others, that could lead users to reject it due to its utilization of behavioral biometrics [8]. In order for transparent authentication to gain support, users will have to accept it and consent to have the mechanism installed on their device, potentially barring their legitimate access to their own applications and services. The user is an important stakeholder in the implementation of transparent authentication; thus, their opinions and needs must be considered early in the design process to encourage acceptance. In this paper, we present the findings of a study carried out to determine whether transparent, continuous authentication is likely to be accepted by users. Finally, we elicit initial impressions regarding the use of transparent authentication on a mobile device as an alternative to traditional access control.

Study goals

Alternative authentication methods have been widely researched over the last decade [9-12], but rarely deployed outside a lab setting. In general, researchers might not fully understand how or if users will use, bypass or accept new security mechanisms. Feasibility studies demonstrate that behavioral biometrics show potential as the basis for the decision–making in a transparent authentication system [13,14]. The outstanding question is whether mobile device users would choose to use such a method to protect their devices and data.

Our study has two purposes: (1) to determine whether the participants feel a transparent authentication method on a mobile device provides adequate security, and, if so, whether they would consider using it on their own mobile devices; (2) to elicit user opinions and suggestions to inform the design of a mobile device transparent authentication mechanism. Our study was designed to answer the following related research questions:

- What are the participant's opinions of, and reactions to, using a transparent authentication method on a mobile device?
- What is the participant's perceived level of security while using a mobile device that employs transparent authentication?
- How do participants react to barriers blocking them from completing their intended tasks?

These questions are intended to examine *user opinions* of a possible transparent authentication mechanism, and not the security provision of such a mechanism. The security provision can be carried out once a prototype system has been made available.

Background and literature review

Smartphone authentication

Mobile devices are rapidly changing the landscape for interactive computing. The technology provided by Google Android, Apple iOS, Blackberry, and Microsoft Windows Phone has enabled smartphones and tablets to become the computing device of choice for mobile workers. The success of these devices, and the applications that run on them, is largely due to the multitude of sensors embedded in them. These sensors, such as

the microphone, camera, gyroscope and accelerometer, not only provide information to applications but the sensed information can also be leveraged to facilitate continuous authentication by taking advantage of the unique patterns that exist in the user's interaction with the device.

Despite the range of interactions available due to mobile device sensors, passwords and PINs remain commonplace authentication methods due to their familiarity, ease of use and the existence of code libraries, widgets and development toolkits that support them as authenticators. The availability of development tools that support password use is bolstered by corporate policies that mandate password use on mobile devices that store or access corporate information, despite studies that have shown that these policies can produce passwords that are less secure than expected [15]. Such policies often dictate the length and required characters in a password, but do not allow for alternative authentication methods. Interestingly, corporate password policies have been shown to negatively impact employee productivity due to their strict, inflexible nature [16]. Identifying the issues and limitations of passwords with respect to mobile devices may provide information for corporations, enabling updates to their corporate policies to include authentication alternatives.

While passwords and PINs may be a commonly used means of authentication on mobile devices due to their simplicity and familiarity, studies have shown that they are often slow and cumbersome to type on a soft keyboard [17,18]. Add to this the commonality of mistakes when typing on a mobile device keyboard [19,20] and it becomes clear that passwords and PINs are not the most effective means of authentication for mobile devices. Bao *et al.* performed a user study into the use of passwords as an authenticator on mobile devices, and found that users find passwords on mobiles so cumbersome and slow that they avoided accessing data on their devices unless necessary [5].

Passwords and PINs have the benefit of being familiar to users, as well as being easy to use and implement, even in legacy systems. In order to retain these benefits, research has been performed to attempt to strengthen passwords and PINs rather than replacing them. Vibrapass uses haptic interaction with a separate mobile device to improve the secrecy of entering a password or PIN into an easily observed public terminal, such as an ATM [21]. The mobile device, which is linked to the terminal during the interaction, vibrates to indicate that the user should enter an incorrect secret (i.e., an incorrect character in a password or PIN), while lack of vibration indicates that a correct entry is expected. Their study showed that the system was acceptable to users with about half the characters as incorrect secrets, while providing a higher security level. Such a system could easily be used for password and PIN entry on a mobile device, as was studied by Bianchi *et al.* in creating the Phone Lock method [22]. Phone Lock takes advantage of smartphone sensors to add non-visual audio and haptic cues, such as spoken numbers audible via earphones and vibrations linked to numbers, to PINs of various lengths. Their goal is to provide a PIN entry mechanism that is resistant to shoulder-surfing attacks, but retains the familiarity and ease-of-use attributed to PINs. Their results showed that the users were significantly faster entering the PIN via audio rather than vibration cues, and that the error rate remained insignificantly different between the two modalities [22]. These methods provide valuable insight into how passwords and PINs may be strengthened by using sensor information, but are not necessarily useful for transparent authentication. It may be argued that these methods are *more* invasive than simple passwords or

PINs because they require additional knowledge or interaction as the price for increased security.

Alternatives to passwords and PINS

Graphical passwords [9,23], gestures and screen interaction [24-27] and biometric authentication [28,29], among others, are emerging as viable alternatives to passwords and PINs as smartphone authenticators. Biometrics, in particular, have seen much research interest in terms of authentication, likely due to the range of sensors available on modern mobile devices. Since more than one sensor is usually available, research has focused on using the fusion of multiple biometrics to downplay any limitations that a single biometric may have. For instance, Hazen *et al.* have studied a method that fuses facial and speech recognition [30]; their results show that error rates can be reduced by up to 90% when compared to the error rates for each individual biometric. Trewin *et al.* compared three biometric modalities (face, voice and gestures) to the use of passwords as authenticators on mobile devices in terms of the effects of each on the time, effort, number of errors and task disruption [29]. Their study showed that the biometric modalities facilitated speedier authentication as compared to password entry. Their results enforce the idea that user frustration with password and PIN-based authentication on smartphones provides a possibility for a change in authentication modality, but that a high level of usability must be achieved and maintained to encourage user acceptance of the new method.

Transparent authentication

Both secret knowledge-based methods and the methods suggested to strengthen them require the user to explicitly authenticate prior to using their device. This effortful authentication is unsuited to the mobile device environment, which is characterized by a bursty use pattern – the smartphone is used very frequently but for short periods of time [31,32]. Generally, with each new interaction the user must re-authenticate, which may become frustrating or annoying to the device owner. The purpose of transparent authentication is to remove the barriers often caused by security tasks – a user rarely picks up a device with the intention of performing security measures. Instead, the user has some other task to accomplish, and authentication is a barrier that must be overcome in order to achieve their intended task.

Research into the area of transparent authentication has begun to gain attention as mobile devices become increasingly ubiquitous, store increasingly private information, and as the shortcomings of passwords and PINs on these devices becomes abundantly clear. Hocking *et al.* have introduced a transparent authentication method called Authentication Aura, in which the user is authenticated by polling the area around the device to determine whether known devices associated with the owner are in close proximity [33]. Their results show that such initial polling can reduce the number of explicit authentication requests by up to 74%, which significantly reduced user frustration with authentication. Similarly, De Luca *et al.* have studied a transparent authentication method that is based on patterns in how the user interacts with the touch screen on a mobile device [25]. Their study found that adding such a behavioral biometric to password use increased security and made the device more resistant to attacks. Clarke *et al.* have performed significant research into transparent authentication, both in terms of assessing

frameworks and prototypes [34] and possible biometrics for use in transparent authentication, such as facial recognition [35] and keystroke dynamics [36]. Karatzouni *et al.* have expanded upon the work of Clarke *et al.* to assess user opinions of both current authentication methods and transparent methods [37]. They found that users envisage a need for increased security on mobile devices due to the nature of the data kept on them, and that biometrics and transparent authentication were feasible replacements for traditional authentication methods. These results show that user privacy, and how they perceive the risks to their personal information, is an important consideration in deploying a transparent authentication method.

User privacy on smartphones

Frequent pop-ups and warnings desensitize the user to the risks they are accepting, particularly if no immediate negative consequences are seen as a result [38]. Therefore, a warning system that uses fewer warnings may help increase security on smartphones. Furthermore, users are confused by permission warning systems such as those used by Android [39,40], in which the user is notified about the particular services an app wishes to access for each app installed. Apps that provide fine-grained privacy control have been examined and found useful in managing app permissions [41], but allowing the user to remove Android permissions statically has been found to cause instability in app functionality [42]. Centralized permission systems, such as those used by the Apple App Store in which the app and its use are governed by a centralized body, remove the burden of judging an app's need for access to potentially private or sensitive information. While this seems to be a positive benefit, it may be the case that the body making the ultimate decision has different sensitivities regarding what is private, offensive or potentially risky. Research has been performed to examine this gap between the user and the decision-making body's concerns regarding smartphone privacy and security, as summarized in the following sections.

Smartphone user privacy concerns

Building upon research that shows privacy and security are concerns to mobile device owners, recent work has identified some of the specific threats that concern users. Chin *et al.* found that users are more concerned about privacy on their smartphones compared to their laptops [43]. They report that users are significantly less willing to perform tasks such as making purchases and accessing their bank accounts or medical records on their mobile devices. They found no significant difference, however, when the users were asked about sharing photos and viewing work-related email on their smartphones versus laptops [43].

Similarly, Felt *et al.* surveyed 3115 smartphone users about 99 selected risks associated with their smartphone and ranked them according to the number of users who would be "very upset" if the risk occurred [44]. They found that the warnings presented to users upon installing an app in both Android and iOS do not correspond to user concerns regarding privacy and security on mobile devices.

Mobile devices, when compared to desktop and laptop computers, have been shown to have different needs in terms of privacy and security [45]. Many smartphones have two types of mobile device PINs [46,47]; the handset PIN, which protects the handset itself and the data stored in its memory from unauthorized use, and the SIM PIN, which

protects the use of, and data stored on, the SIM. Kowalski and Goldstein found that most users did not understand the difference between (and the existence of) the SIM and handset PINs [48]. They further found that only 32% of users in their study were aware of the SIM PIN, and none of them chose to use it. Similarly, Botha *et al.* distinguish between SIM and handset PINs and recognize that these are simply point-of-entry security mechanisms that have limited ability to provide content security [49]. They also found that PIN entry on mobile platforms may be tedious and annoying to the owner because "mobile users may simply wish to take the device out of their pocket to check a schedule entry and could therefore find that entering the password takes longer than the task itself". ([49], p.3). These findings suggest the need for a more nuanced and effortless mechanism for mobile devices.

User opinions of transparent authentication

Biometrics are one way of providing transparent authentication. Jones *et al.* performed a survey of respondents to determine what, if any, technologies were familiar and acceptable to respondents as a potential authenticator [50]. They found that biometrics such as fingerprints were nearly as acceptable to users as passwords (67% for fingerprints compared to 70% for passwords), but that smart cards, other tokens and biometrics such as iris and retina scans were far less acceptable (32%, 27% and 44%, respectively).

In order to determine the current (at the time) use of authentication on mobile devices, Clarke and Furnell conducted a survey of 297 mobile device owners to determine mobile device use frequency, the type of authentication they used, and their attitudes toward future authentication options [46]. They found that 83% of respondents favored the use of biometrics-based authentication. They further found that approximately 33% of respondents did not use a password or PIN at all.

As a follow-up study, Clarke *et al.* performed an evaluation of a behavioral biometrics-based transparent authentication framework called Non-Intrusive and Continuous Authentication (NICA) [6]. Their evaluation found that 92% of the 27 participants reported that the NICA prototype provided a more secure environment when compared to other forms of authentication such as passwords and PINs.

Our study builds upon research in mobile authentication, behavioral biometrics and transparent authentication by determining whether users might accept transparent authentication on smartphones, what their attitudes are towards the use of behavioral biometrics to authenticate themselves on a smartphone, and what their opinions are towards having a more granular (rather than binary) approach to smartphone authentication and security.

Research design and methodology

We performed a lab-based, between-groups study ([51], p. 74) in which 30 participants were asked to complete seven tasks using an Apple iPhone provided by the experimenter. The seven tasks were divided into three security levels (Low, Medium, and High) that represented the level of device confidence the device must have before the task is allowed. *Device confidence* is a term that defines the certainty the device has that its current user is also the device owner. Each participant was randomly assigned to one of three groups that determined the level of transparent authentication they experienced. After the participant completed the tasks, we asked them a series of questions in a semi-structured

interview about their experiences with the transparent authentication mechanism, their general impressions of, and perceived needs for, smartphone security. Figure 1 depicts the interplay between the different aspects of the experimental setup.

Our study was designed with three main constraints in mind. First, we intended to elicit information about the users' opinions of the *privacy and security* provided by the mobile device, rather than their opinions of the functionality of or applications on the device. Second, because the users were given an iPhone, we made it clear that the device itself was unimportant to their opinions and that a similar security method may be available for Android or Blackberry devices. Finally, since our study did not make use of a real transparent authentication method on the provided device, we had to be very careful to maintain the impression that one was there, even in the face of questions from participants.

We obtained IRB permission to perform the study prior to its start. All personally identifying information was coded to protect the identity of the participant, and all interviews, which were recorded with the participant's permission, were deleted after transcription.

Participants

The 30 participants ranged in age from 20 to 58 years (median = 26.5, mean = 29.4). 60% of the respondents were Android users with various handset models, 13% were iPhone users, 10% used a Blackberry and the remaining 17% used a feature phone (e.g., non-smart phone). 17% of the participants were female and 83% were male. Participants were recruited in August and September 2012 using convenience sampling methods, through a combination of email invitations and requests for participation to university classes. Participants were not required to own or use a smartphone, and were paid an honorarium for their time.

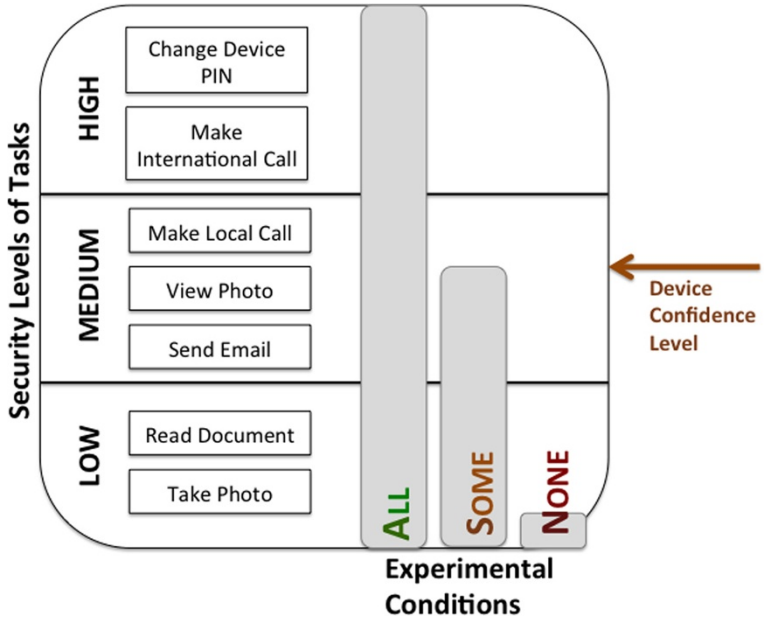

Figure 1 Interplay between the tasks, their security levels, the confidence level of the device and the confidence level of the authentication mechanism.

On their own devices, 27% of participants used a 4-digit PIN, with the same percentage using a sketched password. 30% used no security method, and the remaining 16% used another method, such as encryption and passwords.

Apparatus and materials

Participants used an Apple iPhone 4 with iOS version 5.1.1 during the experiment. It was pre-loaded with the study application and preset with the participant's randomly assigned category and a starting device confidence of "Low". This made it possible to remove potential confounding effects of different operating system versions, and the presence of current applications and stored data on the device. It also limited potential interference from other applications on the participant's own device. The experimenter recorded the interviews using the Voice Memo application on another iPhone. Afterwards, participants were asked a series of questions in a semi-structured interview. The study was conducted in an on-campus meeting room, with one participant and one experimenter per interview; each session lasted 60 to 90 minutes.

Methods

The study began with a short demographic-style questionnaire. The participant was then given an introduction to transparent authentication, introduced to the Apple iPhone and told that a transparent authentication method was running on the device. Transparent authentication was described to the participant as a method that works in the background and allows or disallows access to apps and services such as WiFi or 3G by using the way the device is used to determine if the current user is the legitimate device owner. They were told that the biometrics used were how you speak (voice) and how you type (keystroke dynamics), and that as more and more of these were gathered, the device would become increasingly certain as to who was using the device. Participants were also told that, due to study constraints, no biometrics had been pre-gathered about them so the study would start with a device confidence of Low. Finally, they were told to use a challenge question to explicitly authenticate where they felt it was needed (i.e., if they thought it might help them complete a task).

The participant was told how to turn off or override the transparent authentication mechanism should they wish to at any point during the experiment. This was implemented via a Settings button that popped up a view that asked the participant to confirm that they wanted to turn off security. The transparent authentication could be turned on via the same set of steps. The ability to turn off transparent authentication was provided to build a mental model of the intended transparent authentication method, although the actual working of the application depended on the category to which the participant had been assigned. Each participant began the study with a combination of a "Low" security level and whichever category they had been randomly allocated to.

Upon launching the study application, the participant was prompted via an alert box to set the answer to their challenge question, as a backup to the transparent authentication method. If a task was not allowed because device confidence was lower than the required task confidence, the participant was notified via an alert that stated the required task confidence and the current device confidence, and asked if the participant wanted to answer their challenge question. If the participant said yes (and answered it correctly), the device confidence was increased by one level (i.e., from Low to Medium or Medium to High).

After providing a baseline answer to the challenge question, the participant saw the main "Tasks" screen. All participants completed the tasks in the same order. The order of the tasks were from low to high security, and dictated whether or not explicit authentication was required.

Tasks

Participants completed seven tasks that were classified into one of three security levels: Low, Medium and High based on the general level of privacy or sensitivity a particular task warranted. The task security required a matching device confidence level for the participant to be able to carry them out. The transparent authentication mechanism needs to have that level of confidence that the participant is indeed the authorized device owner. Since the experiment does not last long enough for the participant to build up a device confidence of sufficient level, the device confidence was initially set to "Low" and the participant was instructed to assume that it was based on previous interaction with the device.

The tasks were chosen to represent commonly-used mobile device functionality, as well as for their familiarity to participants. Since one of the study goals was to determine how easy or difficult each task was for the participants, by selecting familiar tasks we hoped that an observed increase in task difficulty could be attributed to additional steps required by the underlying security provision. Participants were reminded that the purpose of the study was to assess their impressions of the security features of the transparent authentication method as described to them, and not their ability to achieve the tasks, nor the user interface of the application itself.

The tasks given to each participant are detailed below.

Low security tasks

Read Document: The participant was asked to open and read the contents of an ostensibly private document from a list. The document titles, such as "PasswordList", "PrivateThoughts" and "BankStatement", were chosen to create a sense of privacy; while the documents did not actually belong to the participant, they were asked to assume that they did. This task was intended to determine whether assigning security levels by *task* was a realistic way of mapping device confidence to device functionality, since we expected that different participants would prefer to have the ability to place documents at different security levels.

Take Photo: The participant was asked to use the mobile device to take a photo of a diagram on a whiteboard in the study locale. Taking a photo on a device may not be a high-security task since it is unlikely to cause the device owner undue concern since the photos can simply be deleted. Exceptions exist, especially in cases of applications where a photo can be immediately uploaded to social networking sites, for example. However, it is envisaged that the ability to view photos rather than take them would fall under a higher security level; this task was included to test this assumption.

Medium security tasks

Send Email: The participant was asked to send an email to a particular email address, with text provided by the experimenter. The text was intended to be somewhat private to give the participant a feeling that they would want to prevent others from seeing it. This

task was used to provide a way for the user to type during the study in order to provide a biometric match or non-match based on their typing pattern. No biometric classification was actually performed; either match or non-match was randomly selected after typing. After the task was completed, the participant was told whether their keystroke dynamics biometric was a match or non-match and the device confidence level was adjusted up or down accordingly.

View Photo: The participant was asked to view a photo, generally the one of the diagram that had been taken in the "Take Photo" task. This task was intended to get the participant thinking about viewing photos versus taking photos and the security ramifications of others viewing their (potentially private) photos.

Make Local Call: The participant was asked to dial a local phone number provided by the experimenter and leave a message of a private nature. The financial aspect of making a call was of interest in this task; the assumption was that a local call would have a lower fee associated with it compared to a long distance call. This task also allowed the participant to speak and thus (theoretically) provide a biometric sample. The participant was informed whether their speaker verification biometric was a match or a non-match, with the accompanying adjustment of the device confidence level.

High security tasks

Make International Call: The participant was asked to dial a long-distance telephone number and leave a message provided by the experimenter. Dialing a long-distance call may have a high cost associated with it compared to making a local call, which allowed us to explore participant opinions on financial risks. This task also allowed another speaker verification match or non-match, much like as described for the Make Local Call task.

Change Device PIN: The participant was asked to change the device PIN. This task was included to assess how participants perceive the value of the PIN mechanism and the security it provides.

Each participant was allocated randomly to one of three categories, which affected their ability to complete the tasks. The participant was able to perform the tasks firstly based on the current device confidence and secondly on their pre-set category, as described below:

None: Participants were unable to complete any task, regardless of their current device confidence. This category is intended to assess the level of frustration seen in a seemingly broken authentication method – one that prevents task completion. This category tested whether the participant would choose to turn off or override the mechanism in frustration. This level of authentication mimics the first stages of using a transparent method, when the device owner has not yet provided sufficient biometric samples to create a baseline for future comparison.

All: Participants were able to complete *all* on-device tasks regardless of device confidence. This category tested whether the participant becomes distrustful of the security provided, since they are neither challenged nor denied access to data or device functionality. This level is meant to mimic the situation in which the mobile device user suspects the security method is malfunctioning and allowing full access to all users.

Some: Participants were able to complete the tasks that were at their current or lower device confidence only. As such, the application compared the current device confidence to that of their current task, and allowed access if the task level was lower than

or equal to the current device confidence. The participant could raise the device confidence by answering their challenge question or by having a matching keystroke or speaker biometric result. This category mimics the real design and use of a transparent authentication method, where the current device confidence is matched to a pre-chosen task authentication level.

The participants were asked to attempt all tasks on the device via the custom designed application and in the same order. Observations were recorded throughout. In particular, the number of times the challenge question was used per task was recorded, as was the number of times the transparent authentication method was deactivated. These values were expected to vary depending on category. Those in the "All" category, for instance, should not have needed to turn off security or answer the challenge question. The participants in the "None" category, however, may have overridden the mechanism by using the challenge question several times before turning off the mechanism altogether. Once the participants had completed all tasks, they were asked a series of questions about their experience in a semi-structured interview (see Appendix A for interview questions). Interview questions explored candidate attitudes towards mobile phone security in general and attempted to gauge initial impressions about the acceptability of a transparent authentication mechanism controlling access on a mobile device.

The participants were debriefed after the interview: they were told that no transparent authentication mechanism had actually been running on the device and that none of their details had actually been collected. They were informed of the three participant categories, and to which category they had been allocated.

Analysis

The independent variable for this study is the level of transparent authentication the user sees: a high level (the "None" category), a moderate level (the "Some" category) or a low level (the "All" category). The dependent variables were their subjective perceptions of transparent authentication and their subjective beliefs about the security level provided by a transparent authentication method. These were measured using ordinal-answer questions (i.e., Likert scale questions) as well as a semi-structured interview. The recordings were transcribed for analysis purposes. We thus had three kinds of data to inform our analysis:

1. Transcribed interviews;
2. Data recorded by the application about what the participants actually did; and
3. Demographic data from the applicants.

We analyzed the data quantitatively and qualitatively. The demographic and descriptive data was charted and analyzed in order to ensure that we understood what the participants did during the experiment. The interview transcripts were analysed using the Grounded Theory approach ([52], p. 101) to elicit themes in the answers. We worked first through the transcripts of the interviews line by line, coding the data. This process was repeated to ensure that all codes had been identified. The codes were then grouped into themes.

Statistical significance of the ordinal data was determined initially using the Kruskal-Wallis test. This test was chosen for its applicability to non-parametric data with three or

more independent participant categories. In cases where the Kruskal-Wallis test indicated statistical significance, the inter-category significance was tested in a pairwise manner using the Mann-Whitney test, which is suitable for use on non-parametric data where there are two independent groups.

Results

No participants withdrew, and each participant was paid £6 for their time. The final themes that emerged from the qualitative analysis are discussed below.

The first theme, *basis for security level choice*, provides an insight into user perceptions when choosing security levels. The second theme, *security as a barrier*, answers the questions about the helpful nature of removing security barriers, and whether they use or override transparent authentication and why. Questions regarding perceived security are answered by the final theme, *user perceptions of authentication*.

Theme 1: basis for security level choice

Participants expressed concerns regarding data and functionality on current mobile devices, and expressed the desire to protect them. One reason given for not using an access control mechanism on their own devices was the inconvenience of having repeatedly to enter a password or PIN. This confirms the arguments of [31,32] about the impact of the bursty usage pattern on the inconvenience imposed by current access control mechanisms that require authentication at each use.

Figure 2 depicts the participant responses for the required security confidence level for each experimental task, grouped into *High, Medium* and *Low* as an aggregate of the three participant categories.

All participants, regardless of category, considered "Change Device PIN" a high security task. This result indicates that changing PINs was considered a "meta-security" task, in that use of a PIN controls access to device data, functionality and settings as well as providing point-of-entry access control. Some participants noted that control over the device and its functionality belongs to the person who knows the PIN. One participant referred to a PIN-locked device as a "brick": essentially useless.

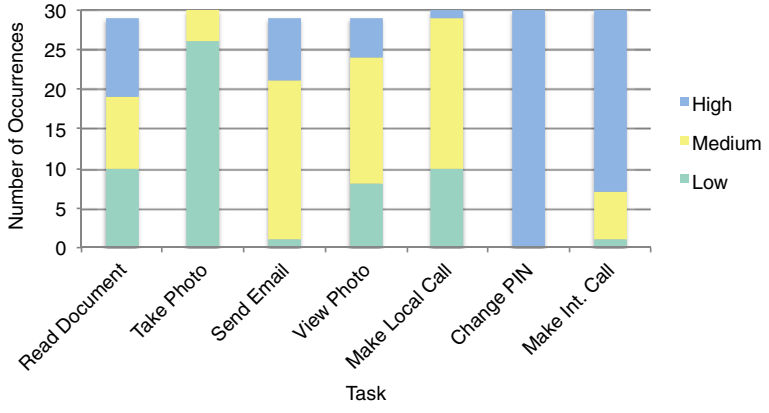

Figure 2 Participant choices for task security level.

Participants did not consider the "Take a Photo" task to be high security. Taking a photo adds data to the device rather than editing or exposing existing data, and is easily deleted by the device owner. Therefore, this task is not a source of data leakage or privacy concerns to the participants in our study.

The "Read Document" task had a relatively even split between high, medium, and low security. This shows the link between the *contents* or *subject* of the document and the preferred level of security. Participants preferred to have the ability to assign a more fine-grained security level based on the sensitivity of each document's contents, rather than based on the meta-task. When they were required to choose an overall level, many participants chose the higher security level with the intention of better protecting any private or sensitive information that might reside in one of the documents. A clear distinction was made between personal and business-related documents: the former were referred to using the terms "personal" or "private", which denote a sense of ownership. Work-related documents, on the other hand, were referred to as "sensitive" and "dangerous", which imply that the participant understood that there was some risk associated with their being exposed, but this does not suggest a sense of ownership.

The differences between the preferred security levels per task reveal a number of considerations that participants implicitly took into account to determine the sensitivity of a given task. Some major themes emerged during the analysis of the responses. When participants were asked why they chose a particular security level for the task in question, responses fell into one of the following categories.

Perceived risks

The study participants cited the following risks that affected the levels to which they allocated the tasks:

Data Loss or Exposure: This risk is strongly linked to data ownership. For example, participants drew a clear distinction between loss of personal data as opposed to work–related data. Loss of personal data, they considered, implied loss of reputation or "face" that could be difficult to overcome in the device owner's social circles. Loss of business data, on the other hand, could result in loss of a job and professional reputation.

Impersonation: The risk of impersonation was a strong theme, particularly with respect to sending email. The anticipated severity ranged from pranks by friends who may send a false email to a mutual friend, to more serious examples that included sending negative or derogatory email to the owner's boss, or using the owner's email as a way of "doing evil things" or committing fraud.

Financial Loss: This risk was prevalent when discussing making telephone calls, both international and local. The perceived risk of financial loss was directly proportional to the chosen security level. For instance, international calls were considered more expensive than local calls, and thus were assigned a higher security level. Thus, associating financial loss with a particular task makes it more likely that device owners would be prepared to perform specific actions in order to protect the data or to authorise the task.

Embarrassment (Misinterpretation of Actions): Strongly related to impersonation and loss of reputation, embarrassment was a risk factor that was associated with many of the tasks. Participants were particularly concerned with embarrassing or compromising photos and other images, as opposed to emails, text messages, or documents. The

embarrassment risk was not in the subject of the photo itself, but with the risk that others may see it, or perhaps pass it onto mutual friends via email or MMS.

Identity Theft and Fraud: Identity theft differs from impersonation in that the latter is single instance and ID theft encompasses multiple instances and has much more serious consequences due to the importance of identity in transactions such as banking.

Damage control after data compromise: Once a person's identity is stolen, it can take a significant amount of time to reclaim the identity and to rebuild reputation and credibility including aspects such as credit ratings and credit card ownership. In less far-reaching situations, there is an aspect of damage control linked to the embarrassment and reputation risks, since time and effort must go into rebuilding status in both social and professional spheres.

Access to some data or tasks may imply access to others: Coupling of tasks and data access is common on mobile devices. For instance, access to email probably permits access to the device owner's address book. It was unclear to many study participants whether protecting one task implied protection of all associated tasks or data, so they tended to assign a higher required security level in these cases.

Data/task sensitivity

If a task or data were considered sensitive, personal or private, the participants in all three categories felt that the device confidence level required to access the task or data should be higher than that of a non-sensitive task or data. This expressed desire to protect themselves is understandable, yet we found that many of the participants did not consider their own on-device data either important or sensitive. Many expressed the belief that there was little data of value on their device. They were also generally uninformed about how much data their own device actually held at the time of the experiment.

Control over device & data

Device owners expressed a strong need to control physical access to their own device and the data it contained. Some participants achieved this simply by keeping the device on their person all the time.

> "…it never really leaves my pocket…"

Techniques such as supervision and physical possession of the device were used to ease security concerns. Device sharing was cited as a motivation for assigning security levels according to perceived data sensitivity. Participants stated that implementing public and private folders or memory locations would allow them to share their device without risking sensitive data exposure. Such sharing was done in a very controlled fashion: participants supervised device use and considered this non-negotiable.

The sense of control over the device and data extended to the choice of security mechanism. When asked whether they would consider using a transparent authentication method on their own mobile device, 90% of the participants answered in the affirmative, at least on a trial basis. The participants stated that they would "play around with" the method to "see how it worked". Such a statement shows the owner's desire to know how the security provisions work, and this applies equally to a transparent method. They clearly wanted to have control over its operation and access to data. Furthermore, our interpretation suggested that they might well also want to understand how intrusive

the security provision will be before committing to its use. Reasons advanced for why they would subsequently remove such a transparent authentication mechanism included annoyance, too-frequent explicit authentication requests, or if they believed the method was not restricting access with sufficiently rigour: "allowed anybody to access my stuff". Interestingly, many participants stated that their feeling of device and data security was enhanced by barriers existing to control data access, even though some considered such barriers annoying and frustrating.

One participant suggested that since biometric usage data was already on the device, it would be a positive benefit to the device owner to have this data used to enhance security provision:

> "In the past people might have raised concerns about storing that kind of information [keystrokes and voice] on a mobile device, but ...if it's already on there, why not use it to provide additional security? It's practically already recording your voice, and it's already recording what you're typing and things like that, so, I'm not sure the objection of storing that information on a mobile device is valid."

Theme 2: security as a barrier

There was a clear theme of security being a barrier, or hurdle, that emerged from the analysis. Participants seemed somewhat conflicted about this. On the one hand the perceived access control delivered by said barrier gave them a sense of security. On the other hand, these barriers sometimes prevented them from accessing their own data and device functionality. Many stated that they would remove access control software if it got "too annoying", or required them to explicitly authenticate too often, something that they considered would be "frustrating".

The "Some" category had a large number of explicit authentication requests, as shown in Figure 3. This stands to reason since this category had the least access to tasks out of all categories when transparent authentication was enabled. The "None" category also had a large number of explicit authentication uses because they too saw its use as a means of accomplishing their task. It was expected that they would quickly learn that using explicit authentication did not allow them to complete the tasks. This assumption held for all but one participant, who felt that repeatedly entering the challenge question was providing the mechanism with keystroke biometric information. The differences between

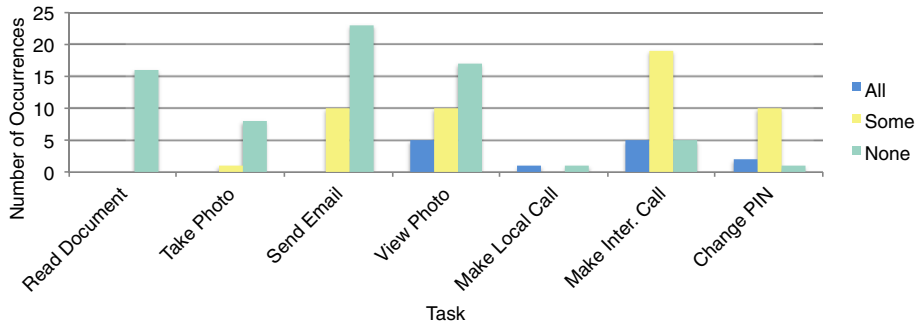

Figure 3 Per-task frequency of explicit authentication use for each of the seven tasks, divided by participant category.

the "Some" and "None" groups and supporting comments show that the device owner's threshold for interruption is relatively low. They also reinforce the "security as a barrier" mental model, and confirm that their usual tasks are the main goal when using a mobile device.

To determine the effect of barriers on security provision, the participants in all categories were able to disable transparent authentication. Figure 4 shows the frequency with which participants disabled transparent authentication on a per-task basis. The "Some" category participants did not disable transparent authentication at all. Their mental model matched the actual operation of transparent authentication; therefore they were able to complete all tasks using explicit authentication and biometric matches only. The "All" category members chose to disable transparent authentication before the tasks that required higher device confidence. The "None" category disabled transparent authentication frequently for the first task, and increasingly less with subsequent tasks. Participants in the "None" group chose to disable transparent authentication permanently early in the experiment, which suggests that task completion might well trump precaution, especially when security becomes intrusive and overly arduous.

The theme of security as a barrier is strongly supported by the behavioral recording data. Explicit authentication requests force the user to stop the task they intend to complete and resume it once authentication is complete. The perceived level of frustration with such interruptions was cited as a major reason that participants in this study would consider disabling a transparent authentication method on their device.

One of the main reasons for the amount of frustration felt when security provision was seen as a barrier was lack of access to the data on the device. Figure 5 shows the participants' perceived levels of data protection provided by transparent authentication, per category. Participants in the "All" category thought the data was poorly protected since they indicated an answer higher than neutral in only two cases. This category had the fewest security barriers with which to contend. Conversely, many of the "None" category members, who had the most security barriers, considered the data very or somewhat well protected. The "Some" category members ranged somewhere between the "All" and "None" extremes. They had a moderate number of security barriers, and largely considered the data either somewhat protected or not protected, but never very well protected.

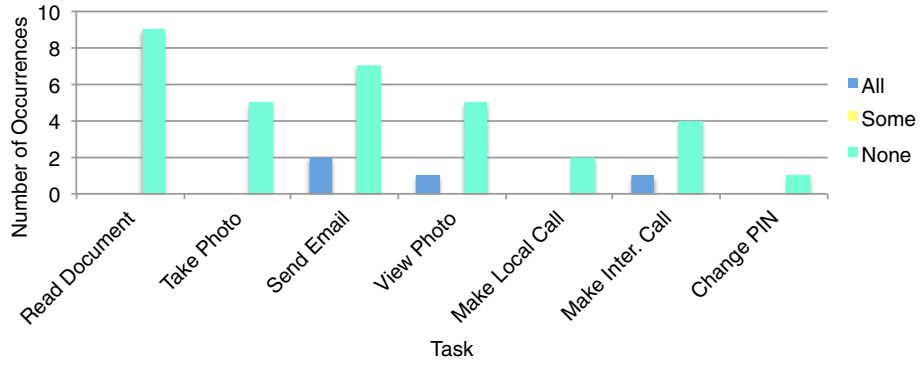

Figure 4 Per-task frequency of disabling transparent authentication for each of the seven tasks by participant category.

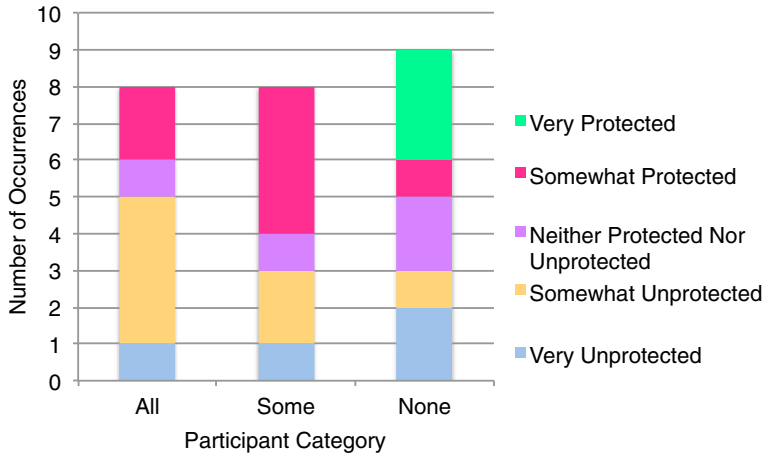

Figure 5 Perceptions of data protection provided by transparent authentication. Each category had 10 participants; some declined to provide a specific value, as shown by the shorter bars.

Theme 3: perceptions of authentication

The participants seemed to believe that "something is better than nothing" in terms of security provision. This, however, does not explain the actions of those participants who chose to use no security at all on their own device. Other things, perhaps the barriers provided by explicit authentication methods, discourage them from using security on their devices even though they seem to believe that it is useful. This theme can also be seen in the previously stated opinions on PIN use. Participants saw the PIN as a powerful overarching security method for protecting the functionality and data on their own device. It seemed, however, that the other side of the coin, not being able to access their own data, outweighed the need for this barrier being put in the way of potential thieves. The barrier was too uni-dimensional: it offered the same obstacle to intruder and legitimate user.

When they had expressed their opinion of their own device's access control offerings, including whether they used it or not, we asked them directly about whether they thought transparent authentication would be an attractive alternative. Figures 6 and 7 show participant opinions on transparent authentication provision compared to either their current mobile device security method (Figure 6) or to no security at all (Figure 7). These figures show that the majority of participants felt that the security provided by transparent authentication was at least as good as what they currently use on their own device, and much better than no security at all. This feeling of a secure environment may encourage users to adopt transparent authentication as an alternative to traditional passwords and PINs.

The overwhelming majority of the participants would consider using a transparent authentication method. However, the participants offered several areas of improvement for transparent authentication, as follows:

1. Assign required device confidence on a per-task or per-folder basis, in addition to by task or application. Have pre-set values that can be changed by owner to reduce initial setup effort.
2. Minimize the number of explicit authentication interruptions as much as possible as these are considered frustrating and intrusive.

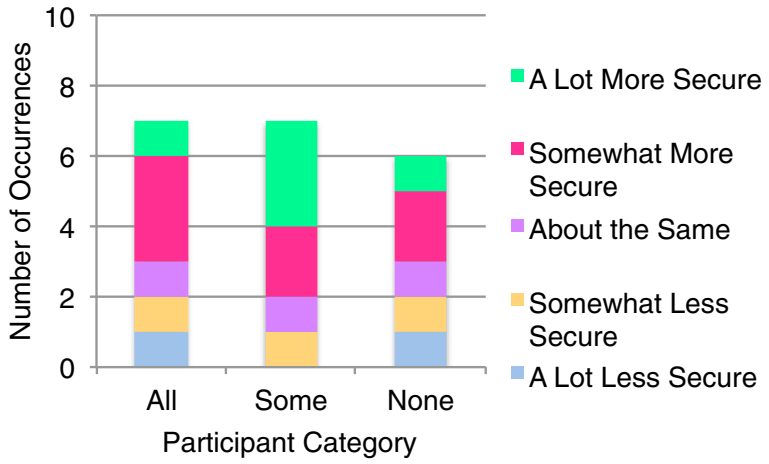

Figure 6 Security provision of transparent authentication compared to owner's current method. Each category had 10 participants; some declined to provide a specific value, as shown by the shorter bars.

3. Keep the owner's data on the owner's device. Do not share it with others, or remove it from the device in order to implement a security mechanism.
4. Minimize effort for frequent tasks. This can be managed by allowing the device owner to select a lower device confidence for tasks that are accessed frequently.

Quantitative analysis

We analysed the information gathered by the application itself while the participants used it, in order to determine whether there were differences between the different experimental groups. Table 1 shows the frequency of explicit authentication use per task; the majority of explicit authentication use occurred from participants in the "Some" and "None" groups. This is an expected result since they were the groups that experienced the most barriers when attempting to complete tasks. It can be argued that the "Some" group should see the most explicit authentication use because its use actually helped the

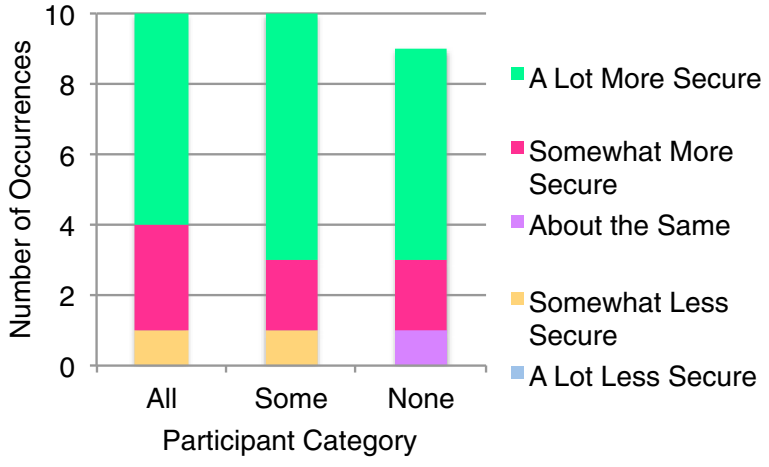

Figure 7 Security provision of transparent authentication compared to no security. Each category had 10 participants; some declined to provide a specific value, as shown by the shorter bars.

Table 1 Total number of explicit authentication attempts per experimental group (All, Some and None) for each task

Task	Group			ρ Value
	All	Some	None	
Read document	0	0	16	$<$ **0.0001**
Take photo	0	1	8	**0.0436**
Send email	0	10	23	**0.0008**
View photo	5	10	17	0.1290
Make local call	1	0	1	0.5958
Change device PIN	2	10	1	**0.0009**
Make international call	5	19	5	$<$ **0.0001**
Totals	13	50	71	
Median	1	10	8	
Mode	0	10	1	
Std. Dev.	2.27	7.13	8.61	

The last column shows statistical significance calculated using the Kruskal-Wallis test. $\rho < 0.05$ are significant (bolded values).

participants to complete their tasks, where the use in the "None" group was not reinforced by being able to then complete the task. Table 1 shows that the "None" group (71 instances, median = 8, mode = 1, SD = 8.61) actually had more instances of explicit authentication use than the "Some" group (50 instances, median = 10, mode = 10, SD = 7.13). However, this result is affected by the contribution of one study participant who misunderstood the function of the challenge question. During the semi-structured interview, the participant stated that they chose to enter their answer repeatedly because they thought that their typing biometrics were being sampled and that task access would be granted when the mechanism had "enough" biometric information. This had the result of artificially increasing the total number of explicit authentication requests seen for the "None" group. This participant's data is included in this analysis rather than being removed as an outlier because the data the participant contributed in other parts of the study (frequency of turning off transparent authentication, qualitative answers to semi-structured interview questions) showed no such bias, and were valuable in assessing other aspects of the hypotheses that drove this work.

There were significant differences in the frequency of explicit authentication use in all tasks except *View Photo* and *Make Local Call* (see Table 1). The order of the tasks had an effect on these values, since all participants began the study at a Low device confidence, and thus had access to at least the first two tasks as they were Low security. The exception is the "None" category, since they were unable to complete any tasks while the transparent authentication was in operation. The significance in explicit authentication frequency per task can be interpreted as the number of barriers presented to participants in various categories; the "All" category had no barriers at all, the "Some" category had a moderate number, and the "None" category had a large number. It is interesting to note that some participants in the "All" category decided to use the explicit authentication despite having task access without it. This shows that they had a strong mental model of the transparent authentication mechanism, and attempted to work within it.

To determine which categories contained the significant results for frequency of using explicit authentication, pairwise comparisons between the frequency data for the "All",

"Some", and "None" categories were performed using the Mann-Whitney test, as shown in Table 2. The View Photo and Make Local Call tasks have been excluded from Table 2 because there was no indication of statistical significance revealed by the Kruskal-Wallis tests.

Per Table 2, most of the categories were significantly different from each of the other categories in terms of the number of times explicit authentication was used per task (see Table 1 for the per-task frequencies). The exceptions are when comparing "All" and "None" for the *Change PIN* and *Make International Call* tasks, and "All" and "Some" and "Some" and "None" for the *Take Photo* task. These differences show that barriers presented before allowing tasks were significantly more frequent for "Some" and "All". This represents a potentially annoying amount of intrusion into the participants' attempts to complete the assigned tasks, a notion that was supported in the participants' comments.

The total number of times a participant chose to turn off transparent authentication is depicted in Table 3. As is expected, due to the barriers put in place for the "None" group, they had the highest instance of disabling transparent authentication. Thus, task completion was considered more important, at least in the experimental setting, than the security of the device and its data.

Perceiving tasks as the main goal is supported by the significant differences between the "None" and "All" and "None" and "Some" categories for the tasks in Table 4. In both cases, many participants in the "All" category did not feel the need to disable transparent authentication since all tasks were accessible with it enabled. In the "None" category, the only way to complete the tasks was to disable transparent authentication, so the difference between these occurrences is understood. Similarly, there would also be many instances in the "Some" category where disabling transparent authentication aided the participant in completing tasks, therefore explaining the statistically significant differences between

Table 2 Pairwise ρ values calculated using the Mann-Whitney test for number of times explicit authentication was used for the tasks that were significantly different

Task	Group	Participant category		
		All	**Some**	**None**
Read document	All	–	NaN	**< 0.0008**
	Some	–	–	**< 0.0008**
	None	–	–	–
Take photo	All	–	0.3681	**0.0347**
	Some	–	–	0.1224
	None	–	–	–
Send email	All	–	**< 0.00002**	**0.0147**
	Some	–	–	0.7066
	None	–	–	–
Change PIN	All	–	**< 0.0005**	0.5828
	Some	–	–	**< 0.00008**
	None	–	–	–
Make international call	All	–	**0.0012**	1.000
	Some	–	–	**0.0012**
	None	–	–	–

$\rho < 0.05$ are significant (bolded values). The comparison between the "All" and "Some" categories for the *Read Document* task is NaN because there were no occurrences of explicit authentication for either category.

Table 3 Total number of times transparent authentication was turned off per group for each task

Task	Group			ρ Value
	All	Some	None	
Read document	0	0	9	$<$ **0.0001**
Take photo	0	0	5	**0.0030**
Send email	2	0	7	**0.0025**
View photo	1	0	5	**0.0146**
Make local call	0	0	2	0.1260
Change device PIN	0	0	1	0.3679
Make international call	1	0	4	**0.0490**
Totals	4	0	33	
Median	0	0	5	
Mode	0	0	5	
Std. Dev.	0.79	0	2.75	

The last column shows statistical significance calculated using the Kruskal-Wallis test. $\rho < 0.05$ are significant (bolded values).

these occurrences and the "None" category. These results reinforced the finding that disabling transparent authentication, and leaving it off for subsequent tasks, was considered the correct course of action, and that completing the tasks was more important than protecting the information and accessibility of tasks on the device.

Study limitations

The convenience sampling methods used represent a potential source of study bias since the participants were skewed towards technically-minded males that were younger than an unbiased distribution. However, the age of the participants is in-line with the average

Table 4 Pairwise ρ values calculated using the Mann-Whitney test for frequency that transparent authentication was turned off for the tasks that were significantly different

Task	Group	Participant category		
		All	Some	None
Read document	All	–	NaN	**< 0.0001**
	Some	–	–	**< 0.0001**
	None	–	–	–
Take photo	All	–	NaN	**0.0137**
	Some	–	–	**0.0137**
	None	–	–	–
Send email	All	–	0.1675	**0.0318**
	Some	–	–	**0.0016**
	None	–	–	–
View photo	All	–	0.3681	0.0636
	Some	–	–	**0.0137**
	None	–	–	–
Make international call	All	–	0.3681	0.1444
	Some	–	–	**0.0336**
	None	–	–	–

$\rho < 0.05$ are significant. The two NaN values mark cases where both categories had no instances of turning off security.

age of UK mobile device owners [53]. Since this study is introductory in nature, this source of bias can be considered acceptable.

The majority of the data gathered in this study is of a subjective nature; it is the participants' opinions and perceptions and is thus subject to their own beliefs and knowledge. The same study conducted on a larger or differently populated group (as the group sampled here was UK-centric) could well result in a different range of opinions. Asking participants to express opinions is a widely-used mechanism for gauging mental models of particular concepts and, as such, was warranted here. The UK-centric nature of the participants clearly signals the need for a wider ranging study but does not detract from the value of the insights we gained from this study.

Discussion

It is curious that participants, in general, did not feel their data was valuable, were not entirely sure how much data they held, yet were concerned about other people accessing this data. Their expressed preference might be a manifestation of their fear of the unknown [54], a vague sense of being at risk and needing to take action to prevent harm. Perhaps their behavior is rooted in loss aversion, and is not really linked to the actual value of their data. On the other hand, it might be that participants were giving the answers that they think the experimenter might want to hear by claiming that security barriers are desirable, since they were aware of her research speciality.

As imperfect as our findings may be, they do, nevertheless, deliver valuable insights into participants' thought processes. Device owners clearly have a sense of identity associated with their mobile devices, as demonstrated by their unwillingness to allow others to use their devices. That they are frustrated with frequent authentication attempts is also clear. Even if they were demonstrating a social desirability response by claiming a need for authentication their own annoyance with it came across very clearly. Rather than merely being lazy, it became clear that users had very good reasons for their so-called "insecure" behaviors. Security researchers need to consider such rationales when designing security mechanisms, or these will be subverted or discarded if they become too arduous to use.

The participants in this study were open to the idea of an alternative mechanism, especially if such a mechanism intruded as little as possible, yet at the same time did provide a measure of protection. However, the sense of identity they associate with their devices means that an transparent mechanism is going to have to treat the behavioral biometric data with respect, and not remove it from the device.

Our main findings are as follows:

Security Barriers Need to be Visible: While removing security barriers such as effortful authentication and warning messages may simplify security provision while limiting user frustration with barrier frequency, this study has shown that removing *all* barriers is probably unwise. Participants indicated that having a few barriers was desirable to show that the security mechanism is working as intended. Barriers also help users build a mental model of the security provided, and may help build user trust that their data and device are adequately protected. To our knowledge, this result is novel.

Secret Knowledge is Problematic: We found that users were fearful of forgetting secret knowledge such as PINs and passwords because they linked that knowledge to the ability to use their device at will. Removing the dependence on remembering a secret, while still

adequately protecting the device functionality and data, may help relieve the user of this fear. This result goes beyond other research that states that users *do* forget passwords and PINs [55] to state that users are *fearful* of forgetting, and thus allow this fear to inform their security provision on their mobile device. We also believe this result is in line with other studies that state the user does not wish to act in an insecure manner, but perhaps chooses to do so to make up for failings in the security provisions afforded them [3].

Biometrics are Acceptable: We found that users were willing to try transparent methods based on biometrics, although they wished to have a period of evaluation before making a final decision. This result is similar to those found by Clarke *et al.* [46], and show that a plausible authentication solution that uses biometrics and is also acceptable to users has not yet been discovered. Furthermore, we found that users are willing to consider trying transparent authentication, as they see a need for alternatives to passwords and PINs. This finding supports similar results reported by Clarke *et al.* in their evaluation of the NICA method [6].

Recommendations

Based on these findings, we recommend the following considerations for those providing an alternative mobile device authentication mechanism:

Use what we have: Mobile devices gather a significant amount of potentially private information about the user and their preferences, such as typing patterns, speech, accelerometer and gyroscope data and to whom and when they call or text. Future authentication methods can use this information as a way of determining who is using the device at a given time via behavioral biometrics such as keystroke dynamics, speaker verification and device use patterns. Since this information is already gathered, users tend to support its use as a potential authenticator.

Respect the mobile device environment: Since mobile devices are characterized by a bursty use pattern in which users access them frequently for short periods of time [31,32] authentication methods should not represent a barrier with each use or it may encourage users to not use security provisions. Mobile devices also have limitations in processor speed and memory, which is one reason for use of easy authentication methods. Alternatives to these easy methods should work in the background, but not overtax processors and memory.

Keep data on-device: Participants reported that they were uncomfortable with personally-identifying information leaving their device. Since this data is already gathered, future authentication methods that use it should process it on the device itself. This has far-reaching privacy implications since the data remains under its owner's control at all times.

Remove *most* barriers, but not *all*: Our study has shown that participants choose not to use provided security methods on their mobile device because they quickly become frustrated with entering authentication details repeatedly. Such barriers to task completion are common in security. Since the mobile device environment is characterized by frequent use, owners are asked to authenticate frequently. Removing some of these barriers may help reduce user frustration with authentication, but removing all barriers may have the effect of changing the user's mental model of the security provided. Participants opined that they would like to test, or experiment with, any new method

before adopting it; this supports the creation of a mental model of security. Therefore, we should give clear signals as to the current state of security on the device, and give feedback in a non-intrusive manner as to the success or failure of authentication methods.

Conclusions and future work

Mobile devices represent a unique environment that is not well-suited to repeated entry of secret knowledge-based authentication methods. Consequently, we require alternative authentication methods that respect both the bursty nature of this environment, as well as the device owner's need for a reliable, non-intrusive authentication method. Respecting both the needs of the user and the limitations of the mobile device environment may lead to methods that are both more usable and more acceptable to device owners.

As a first step towards realizing transparent authentication on mobile devices, we conducted a user study with 30 participants to understand their opinions of transparent mobile device authentication that is based on behavioral biometrics. Our results show that 30% of participants used no security method on their mobile device, despite the opinion that their device stored sensitive information that should be protected. Overall, 73% of study participants felt transparent authentication was more secure than traditional methods such as secret knowledge techniques, although many of them wished to test the new system first before making a final decision on its security provision. Finally, 90% of participants stated that they would consider using a transparent authentication method on their own mobile device, should one be made available to them.

Through our qualitative analysis of interview questions, we found that participants are fearful and distrustful of PINs and other secret knowledge methods, that they often depend on physical proximity to the device to limit unauthorized access, and that having a few barriers helps them feel that the mechanism is working as designed. We recommend that future work in creating alternative authentication methods for mobile devices respect the limitations of the mobile device environment while limiting the effort that a user must make in order to protect their device. Furthermore, we recommend that any method be completely transparent to the user in its workings while providing a clear indication of the current security state of their device at any given time. Finally, we recommend that new authentication methods keep the user's personally identifying information on the device; this respects the owner's privacy and ensures that the authentication mechanism does not empower identity thieves.

Future work

The study reported here has several interesting avenues for future work, as follows:

- Perform a related study on tablets to see whether users express the same concerns on more powerful and functional (but still portable) devices;
- Examine whether putting apps into particular user-chosen security levels reduces the amount of access an application has to potentially private data/functionality. This study examined the feelings of users to other *people* having access to functionality on their device. The difference is that *apps* may also have that functionality and data access. Can we also protect the user from automated data access, access to device functionality that they have accepted due to blanket acceptance of warning messages?

Appendix A: interview questions

- Were you able to complete all the tasks given to you? Why or why not?
- Did you turn off the transparent authentication system? Why or why not?
- Did you use the challenge question feature? Why or why not?
- Assume for a moment that you were placing each task from the study into a security level that you think is most appropriate given how you use your mobile device and how sensitive you think each task is. Use the 3-point Likert scale to assign each task from the study into what level you think it should be in.
- How many security level choices would you like to have? Is Low/Med/High accurate enough, or should there be more choices?
- What did you like about using the transparent authentication system?
- What did you dislike about using the transparent authentication system?
- Would you use a transparent authentication method on your own mobile device? Why or why not?
- Using the 5-point Likert scale, indicate how well protected you thought the data on the device was. 1 is very unprotected, 2 is somewhat unprotected, 3 is neither protected nor unprotected, 4 is somewhat protected and 5 is very protected. Why did you select this level?
- What security mechanism do you currently use on your mobile device?
- When compared to using your usual security mechanism as the sole security method on a mobile device, did you feel that using a transparent authentication method was more secure, less secure, or about the same? Use the Likert scale for this 1 is a lot less secure, 2 is somewhat less secure, 3 is about the same, 4 is somewhat more secure, and 5 is a lot more secure. Why?
- When compared to using no security method at all on a mobile device, did you feel that using a transparent authentication method was more secure, less secure, or about the same? Use the Likert scale for this 1 is a lot less secure, 2 is somewhat less secure, 3 is about the same, 4 is somewhat more secure, and 5 is a lot more secure. Why?

Competing interests
The authors declare that they have no competing interests.

Authors' contributions
The majority of the work was done by the first author (HC), as is expected given that the work presented in this manuscript is a part of the first author's Ph.D. dissertation. HC conceived the study, designed the interview questions, designed and wrote the required mobile device application, undertook all participant meetings and interviews and compiled the first pass of qualitative data analysis. HC also performed all quantitative statistical analysis, including the first draft of the results. KR made suggestions that improved the clarity and neutrality of the interview questions, performed the second pass of qualitative data analysis, and refined the results that are based on both qualitative and quantitative analysis. Both authors wrote parts of, edited and approved the final manuscript.

Author details
[1]Department of Computer Sciences and Cybersecurity, Florida Institute of Technology, 150 W. University Blvd., Melbourne, FL 32901, USA. [2]School of Computing Science, University of Glasgow, Sir Alwyn Williams Building, Lilybank Gardens, Glasgow G12 8QQ, UK.

Received: 26 September 2013 Accepted: 20 March 2014
Published: 3 June 2014

References

1. IDC (2013) Mobility reigns as the smart connected device market rises. Online: http://www.idc.com/getdoc.jsp?containerId=prUS23958513#.UTCkuDd4DIZ. Last checked: August 21, 2013
2. Glisson WB, Storer T, Mayall G, Moug I, Grispos G (2011) Electronic retention: what does your mobile phone reveal about you? Int J Inform Secur 10(6): 337–349
3. Adams A, Sasse MA (1999) Users are not the enemy. Comm ACM 42(12): 40–46

4. Gaw S, Felten EW (2006) Password management strategies for online accounts In: Proceedings of 2nd symposium on usable privacy and security, pp 44–55
5. Bao P, Pierce J, Whittaker S, Zhai S (2011) Smartphone use by non-mobile business users In: Proceedings of the 13th international conference on human computer interaction with mobile devices and services, pp 445–454
6. Clarke N, Karatzouni S, Furnell S (2009) Emerging challenges for security, privacy and trust, Volume 297/2009 of IFIP advances in information and communication technology. chap. Flexible and Transparent User Authentication for Mobile Devices. Springer Boston, pp. 1–12
7. Crawford H, Renaud K, Storer T (2013) A framework for continuous, transparent mobile device authentication. Comput Secur 39, Part B: 127–136
8. Prabhakar S, Pankanti S, Jain AK (2003) Biometric recognition: security and privacy concerns. IEEE Secur Privacy 1(2): 33–42
9. Chiasson S, van Oorschot PC, Biddle R (2007) Graphical password authentication using cued click points. In: Proceedings of the 2007 European symposium on research in computer security, volume 4734/2007 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg, pp 359–374
10. O'Gorman L (2003) Comparing passwords, tokens, and biometrics for user authentication. Proc IEEE 91(12): 2019–2040
11. Patel SN, Pierce JS, Abowd GD (2004) A gesture-based authentication scheme for untrusted public terminals In: Proceedings of the 17th annual ACM symposium on user interface software and technology, pp 157–160
12. Shi E, Niu Y, Jakobsson M, Chow R (2011) Implicit authentication through learning user behavior. In: Burmester M, Tsudik G, Magliveras S (eds) Information security, Volume 6531 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg, pp 99–113
13. Rokita J, Krzyzak A, Suen C (2008) Image analysis and recognition volume 5112 of Lecture Notes in Computer Science. chap. Cell Phones Personal Authentication Systems Using Multimodal Biometrics. Springer Berlin / Heidelberg, pp 1013–1022
14. Snelick R, Indovina M, Yen J, Mink A (2003) Multimodal biometrics: issues in design and testing In: Proceedings of the 5th international conference on multimodal interfaces, pp 68–72
15. Komanduri S, Shay R, Kelley PG, Mazurek ML, Bauer L, Christin N, Cranor LF, Egelman S (2011) Of passwords and people: measuring the effect of password-composition policies In: Proceedings for the SIGCHI conference on human factors in computing systems, pp 2595–2604
16. Inglesant PG, Sasse MA (2010) The true cost of unusable password policies: password use in the wild In: Proceedings of SIGCHI conference on human factors in computing systems, pp 383–392
17. Azenkot S, Zhai S (2012) Touch behavior with different postures on soft smartphone keyboards In: Proceedings of 14th international conference on human computer interaction with mobile devices and services, pp 251–260
18. Hoggan E, Brewster SA, Johnston J (2008) Investigating the effectiveness of tactile feedback for mobile touchscreens In: Proceedings of the SIGCHI conference on human factors in computing systems, pp 1573–1582
19. Allen JM, McFarlin LA, Green T (2008) An in-depth look into the text entry user experience on the iPhone In: Proceedings of the human factors and ergonomics society annual meeting, Volume 52(5): 508–512. SAGE Publications
20. Chen T, Yesilada Y, Harper S (2010) What input errors do you experience? Typing and pointing errors of mobile web users. Int J Hum Comput Stud 68(3): 121–182
21. Luca AD, von Zezschwitz E, Hussmann H (2009) Vibrapass: secure authentication based on shared lies In: Proceedings of the SIGCHI conference on human factors in computing systems, pp 913–916
22. Bianchi A, Oakley I, Kostakos V, Kwon DS (2011) The phone lock: audio and haptic shoulder-surfing resistant pin entry methods for mobile devices In: Proceedings of the 5th international conference on tangible, embedded and embodied interaction, pp 197–200
23. Dunphy P, Heiner AP, Asokan N (2010) A closer look at recognition-based graphical passwords on mobile devices In: Proceedings of the 6th symposium on usable privacy and security, pp 26–38
24. Cai L, Chen H (2011) Touchlogger: inferring keystrokes on touch screen from smartphone motion In: Proceedings of 6th USENIX workshop on Hot Topics in Security (HotSec'11), pp 9–9
25. Luca AD, Hang A, Brudy F Lindner C, Hussmann H (2012) Touch me once and I know it's you!: implicit authentication based on touch screen patterns In: Proceedings for the SIGCHI conference on human factors in computing systems, pp 987–996
26. Frank M, Biedert R, Ma E, Martinovic I, Song D (2012) Touchalytics: on the applicability of touchscreen input as behavioral biometric for continuous authentication In: IEEE transactions on information forensics and security, Volume 8, pp 136–148
27. Uellenbeck S, Dürmuth M, Wolf C, Holz T, Görtz H (2013) Quantifying the security of graphical passwords: the case of android unlock patterns In: Proceedings of the 20th ACM conference on computer and communications security, pp 161–172
28. Allano L, Morris AC, Sellahewa H, Garcia-Salicetti S, Koreman J, Jassim S, Ly-Van B, Wu D, Dorizzi B (2006) Non-intrusive multi-biometrics on a mobile device: a comparison of fusion techniques In: Proceedings of the SPIE conference on biometric technology for human identification III
29. Trewin S, Swart C, Koved L, Martino J, Singh K, Ben-David S (2012) Biometric authentication on a mobile device: a study of user effort, error and task disruption In: Proceedings of the annual computer security applications conference, pp 159–168
30. Hazen T, Weinstein E, Heisele B, Park A, Ming J (2007) Face biometrics for personal identification: multi-sensory multi-modal systems. chap. Multimodal face and speaker identification for mobile devices. Springer
31. Falaki H, Mahajan R, Kandula S, Lymberopoulous D, Govindan R, Estrin D (2010) Diversity in smartphone usage In: Proceedings of the 8th international conference on mobile systems, applications and services, pp 179–194
32. Jo HH, Karsai M, Kertèsz J, Kaski K (2012) Circadian patterns and burstiness in mobile phone communication. New J Phys 14(1): 013055

33. Hocking C, Furnell S, Clarke N, Reynolds P (2013) Cooperative user identity verification using an authentication aura. Comput Secur in press
34. Clarke N, Furnell S (2007) Advanced user authentication for mobil devices. Comput Secur 26(2): 109–119
35. Clarke N, Karatzouni S, Furnell S (2008) Transparent facial recognition for mobile devices In: Proceedings of the 7th international information security conference
36. Clarke N, Furnell S, Lines B, Reynolds P (2003) Keystroke dynamics on a mobile handset: a feasibility study. Inform Manag Comput Secur 11(4): 161–166
37. Karatzouni S, Furnell S, Clarke N, Botha RA (2007) Perceptions of user authentication on mobile devices In: Proceedings of the 2007 ISOneWorld conference. CD Proceedings
38. Stewart DW, Martin IM (1994) Intended and unintended consequences of warning messages: a review and synthesis of empirical research. J Publ Pol Market 13(1): 1–19
39. Felt AP, Ha E, Egelman S, Haney A, Chin E (2012) Android permissions: user attention, comprehension and behavior In: Proceedings of the eighth symposium on usable privacy and security, pp 1–3:14
40. Kelley PG, Consolvo S, Cranor LF, Jung J, Sadeh N, Wetherall D (2012) A conundrum of permissions: installing applications on an android smartphone In: Proceedings of 16th international conference on financial cryptography and data security, pp 68–79
41. Zhou Y, Jiang X, Freeh VW, Zhang X (2011) Taming information-stealing smartphone applications (on android) In: Proceedings of the 4th international conference on trust and trustworthy computing, pp 93–107
42. Kennedy K, Gustafson E, Chen H (2013) Quantifying the effects of removing permissions from android applications In: Proceedings of Mobile Security Technologies (MOST)
43. Chin E, Felt AP, Sekar V, Wagner D (2012) Measuring user confidence in smartphone security and privacy In: Proceedings of the eighth symposium on usable privacy and security, pp 1–1:16
44. Felt AP, Egelman S, Wagner D (2012) I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns In: Proceedings of 2nd ACM workshop on security and privacy in smartphones and mobile devices, pp 33–44
45. Ben-Asher N, Kirschnick N, Sieger H, Meyer J, Ben-Oved A, Möller S (2011) On the need for different security methods on mobile phones In: Proceedings of 13th international conference on human computer interaction with mobile devices and services, pp 465–473
46. Clarke N, Furnell S (2005) Authentication of users on mobile telephones - a survey of attitudes and practices. Comput Secur 24(7): 519–527
47. Herley C, van Oorschot PC, Patrick AS (2009) Passwords: if we're so smart, why are we still using them? In: Proceedings of the 13th international conference on financial cryptography and data security Volume 5628/2009 of Lecture Notes in Computer Science, pp 230–237
48. Kowalski S, Goldstein M (2006) Consumers' awareness of, attitudes towards, and adoption of mobile phone security In: Proceedings of the 20th international symposium on human factors in telecommunication
49. Botha RA, Furnell S, Clarke N (2009) From desktop to mobile: examining the security experience. Comput Secur 28(3–4): 130–137
50. Jones LA, Antòn AI, Earp JB (2007) Towards understanding user perceptions of authentication technologies In: Proceedings of the 2007 ACM workshop on privacy in electronic society, pp 91–98
51. Field A, Hole G (2008) How to design and report experiments. SAGE Publications
52. Strauss A, Corbin JM (1998) Basics of qualitative research: techniques and procedures for developing grounded theory 2nd edition. SAGE Publications
53. The Deloitte Consumer Review (2013) Beyond the Hype: The True Potential of Mobile. Online: Last checked: June 25, 2014 http://www.deloitte.com/assets/Dcom-UnitedKingdom/Local%20Assets/Documents/Industries/Consumer%20Business/uk-cb-consumer-review-edition-5.pdf
54. Cao HH, Han B, Hirshleifer D, Zhang HH (2011) Fear of the unknown familiarity and economic decisions. Rev Finance 15: 173–206
55. Florêncio D, Herley C (2007) A large-scale study of web password habits In: Proceedings of the 16th international conference on World Wide Web (WWW '07), pp 657–666

doi:10.1186/2196-064X-1-7
Cite this article as: Crawford and Renaud: **Understanding user perceptions of transparent authentication on a mobile device.** *Journal of Trust Management* 2014 **1**:7.