Perceptions of User Authentication on Mobile Devices

S.Karatzouni[1], S.M.Furnell[1,3], N.L.Clarke[1] and R.A.Botha[2]

[1] Network Research Group, School of Computing, Communications & Electronics, University of Plymouth, Plymouth, UK
[2] Centre for Information Security Studies, School of Information and Communication Technology, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
[3] School of Computer and Information Science, Edith Cowan University, Perth, Australia

Abstract

The increasing range of data and services accessible from mobile devices, such as cellphones and PDAs, leads to questions about the adequacy of security provision, particularly in relation to authentication of the user. In this context, this paper describes the findings from a focus group that was conducted to examine four research questions: whether users recognise a need for security on their current devices; how they perceive the current authentication facilities, and whether they use them; whether they envisage a need for greater security provision in the future; and their perceptions of alternative authentication methods and the ways in which they could operate. The overall results showed that users envisage a need for enhanced security as their usage of the device changes to incorporate more sensitive functions. Furthermore, from the options discussion, a preference towards the use of biometric authentication was expressed by the majority of the participants.

Keywords: *Security, authentication, mobile, cellphone, PDA.*

Introduction

Mobile devices such as cellphones and PDAs are becoming more sophisticated tools, with data processing, storage and communication capabilities getting closer to the functionality of desktop computers. As a consequence, the information that can be accessed through and stored on them is becoming more sensitive. This has already been witnessed with other forms of mobile device (e.g. laptops) and as a result they now represent a recognised area of risk. For example, 53% of respondents in Ernst & Young's Global Information Security Survey 2005 identified mobile computing as the issue that raises the major security concerns (Ernst & Young, 2005). Furthermore, in another survey amongst 2,035 IT professionals, 80% of respondents identified their main security fear as employees misplacing or losing the device, as well as not using appropriate security settings (Red Herring, 2006). Against this background, a concern can be raised regarding the ability of current security measures to safeguard the device. Significant amongst these is the user authentication method, which for current phones and PDAs is principally achieved by the use of Personal Identification Numbers (PINs). However, questions can be raised about whether this method will remain sufficient, and (if not) what methods users may be willing to tolerate in its place.

The purpose of this research was to assess views and attitudes regarding the authentication requirements on mobile devices. In order to achieve that, a focus group

was conducted, in order to provide a forum for users to express and exchange their perspectives. The next section presents the objectives and methodology of the research. This is followed by the main discussion, relating to the results obtained, leading to overall conclusions in the final section.

Research objectives and investigative methodology

The focus group was conducted in September 2006, and lasted around 100 minutes. The composition of the participant group is outlined in Table 1, including a mixture of end-users, representatives from the mobile industry, researchers in the area, and representatives from the educational technology and university perspectives. In addition to these, invitations had also been issued to other industry-based representatives, but unfortunately (despite some initial follow-up) these did not lead to final participation.

Participant	Background / Basis for inclusion
1	Representative from a UK mobile network operator.
2	Creator of a web resource that tracks mobile technologies and trends
3	Project student, addressing public understanding of biometrics
4	Project student, conducting user trials and evaluation of biometrics
5	Academic, active in the mobile security domain
6	Learning technologist, commencing research into educational uses of mobile devices
7	Psychologist, with research interests in use of mobile technologies
8	Representative from university ICT department, responsible for campus deployment of mobile devices.
9	Academic with interest in human factors of technology.
10	Male mobile phone user
11	Female mobile phone user
12	Female mobile phone user

Table 1 : Summary of focus group participants

All of the participants were regular end-users of mobile devices, and in many cases conversant with the features and facilities of smartphone devices. As such, they were able to offer perspectives with firsthand knowledge of the more advanced features and facilities that are likely to become the baseline standard in a few years.

A number of research questions were created to form the framework of the discussion, addressing the main areas of interest around the objectives of this research on user authentication. A list of the question as well as a brief justification behind them follows.

1. *Do participants recognise a need for security on their current devices?*

   This question aims to investigate whether users consider their current usage of mobile devices to merit protection, with particular emphasis being given to whether or not user authentication is an important requirement. The general expectation, based upon prior survey work (Clarke *et al*. 2002; Clarke and Furnell, 2005) was that many participants would not view their own need for security to be particularly high.

2. *How do participants perceive the current authentication facilities, and do they use them?*

   The intention here is to focus participants' attention specifically towards the PIN-based techniques that are dominant upon current devices, exploring opinions about the general nature of the method the extent to which they are used in practice. The investigators' expectations here were again partially informed by the earlier research, such that it was anticipated that many participants would not be using the current facilities at all (in part based upon their reasoning from question 1).

3. *Do participants envisage a need for greater security provision in the future?*

   Anticipating that some participants would be unlikely to prioritise a need for authentication based upon their current usage of the device, this question asks them to consider the range of emerging and future applications of mobile devices that may interest them. From this, they are asked to reassess their views on the requirement for authentication, in view of the increased sensitivity of data or services that may then be involved.

4. *How do participants perceive the potential alternative methods of authentication and the ways in which they could operate?*

   Assuming that the preceding question would highlight a requirement for further protection, this question aims to elicit opinions about alternative mechanisms (such as token and biometric approaches), and methods of applying them.

Although some expectations had been formed as a result of previous research, the participants were not led towards any particular viewpoints during the discussion of each question (nonetheless, the conclusions drawn from the first two questions proved to be generally as anticipated, thus justifying the progression towards the subsequent discussion issues). A discussion guide was formed and followed during the session that would provide the background and the context for the research questions to be answered. The session was video recorded in order to capture any non-verbal information that could provide further input (i.e. reactions to a certain view) or help to quantitative appraisal of answers (i.e. show of hands as an answer).

Focus Group Results

The focus group session began with some background discussion about the participants' use of their mobile devices, with consideration specifically directed towards mobile phones and PDAs, rather than laptops or single-function devices such as media players. This section begins with brief comments in relation to this usage, before proceeding to discussion of the main findings, based around the research questions. It should be noted that, due to overlaps in the related discussions, research questions 1 and 2 are discussed within a single subsection, whereas the extent of discussion arising from question 4 has led to it being split over two subsections. All of the sections are supported by direct quotes from the participants in order to

evidence the views expressed. In all cases, the quotes are exactly as spoken, although in some cases segments have been omitted for brevity (denoted by '…') and in other cases the authors have added wording in brackets in order to provide clarification.

Background of attendees on the use of mobile devices

The majority of participants indicated that their usage of mobile devices had not changed in recent years, and focused mainly upon traditional functionality such as telephony and text messaging. Even where some considered a mobile device as a necessity to their everyday lives, the main driver tended to be communication.

> *"If I left the house without it I would feel a little bit naked. It's like you can't get in touch with people"*

> *"A lot of people are using it more and more. I'm aware of that…but personally…for me it's just a communication tool…that's it"*

> *"I never actually use any of the features, I just text and that's it … Occasionally I use the camera phone feature a bit"*

Although some participants stated that they had used services such as downloading content (e.g. ringtones) or video conferencing, this was mainly for experience's sake rather than an ongoing usage. Nevertheless a minority (mainly owning high-end devices) used them for accessing e-mail or browsing the web on a more regular basis, including in a business context:

> *"I mean if I had to lose this [device] at this point in time … I would be completely lost, because I run my diary, I basically run everything that I do with this kind of thing"*

The potential for greater adoption of services was also identified by some attendees, suggesting that the usage of the device is likely to change in the future.

Current need for security and use of the available security mechanisms

Surveys have repeatedly reported that although users store a great amount of sensitive information on their devices, little attention is given to protecting them using the available security mechanisms (Pointsec, 2005; Kucan, 2003). It was therefore important to see how users assess their own security requirements based on their use of their device.

The main discovery was that participants did not feel at risk as their usage was limited to services that do not involve storage or access of highly sensitive information.

> *"As a general user who is only using it for personal use, there's no data on there that I class that sensitive"*

> *"I use this [Pocket PC] just for access to the exchange server and nothing else…So the issue of security hasn't arisen with this yet, but probably will do at some stage"*

> *"I think it depends from which context you are using it in, cause the security you are going to need in it, is going to depend on the sensitivity of the data…the only thing that I got that is sensitive is friends' phone numbers and address details"*

As participants did not generally recognise a current security requirement it was interesting to assess how they perceived the nature and adequacy of current authentication methods. Today's mobile devices are mainly protected by the use of PINs. However, previous research has suggested that users often perceive these to be an insufficient and inconvenient method, and consequently do not use them (Clarke *et al*. 2002; Clarke and Furnell, 2005). Similar views were also expressed by the participants, as only a third of them claimed to use PIN protection at switch on and only one used a PIN in standby mode. Meanwhile, the rest did not use any protection at all. Some based their decision not to do so on the fact that they did not perceive their current usage would pose any concern (which follows from the views in the previous section):

> *"Passwords and that kind of stuff, I've just never done it. I think the thing is with me that obviously because I just text and I don't do anything else, from a sensitive point of view there is no information that I perceive is valuable enough to be worth worrying about"*

> *"I'm not sure that anybody would want to steal my information, I don't perceive myself to be that important"*

However, even those that did make use of the mechanism expressed concern as to the level of security that it could provide in some contexts:

> *"I suppose for accidental loss or whatever, that will be fine because people are not going to guess your keyword or your PIN code or whatever. However PIN codes and things are limited ... basically something that can be attacked in numerous ways"*

Although the sensitivity of information played a role, other comments mentioned traditional downsides of PINs such as forgetting them, and a viewpoint from many participants was that the PIN can only protect them if their phone is switched off (i.e. if someone acquired the device when already switched on they would find no requirement for reauthentication). The following comments were typical in relation to PINs:

> *" I think any security that is going [to] lock me out every now and then…is the reason I don't use PINs now cause I always forget my PIN…*

> *"I never turn my phone off so if I lost it, it would be on anyway"*

> *"I've used them before. It's simple to use, it's just…I don't see any point using it myself cause I never turn my phone off"*

These views underline the fact that PIN-based point-of-entry authentication is perceived to provide limited protection. A further factor that may have influenced attitudes towards security and use of current facilities was the fact that none of the participants had experienced a security incident:

> *"No, that's probably why I'm not so that worried about the security. I've never actually lost my phone, only ever dropped it when I'm drunk and reset it and things like that but never lost the phone"*

As such, it was perhaps not surprising to find that the general view was negative when asked about paying more for a device in order to increase security. The following comments were typical, suggesting that even if they considered paying, the protection itself was not the direct driver:

> *"No, not even for a second"*

> *"Well I don't know. If my phone had a fingerprint scanner on it, I'd think that was cool so yeah I'd pay more".*

Overall, therefore, it was clear that participants did not currently perceive a significant need to protect their devices. Even though this view was basically formed due to the limited usage of their devices, it was also partially informed by attitudes towards PIN-based authentication, which participants felt was not sufficient (and thus making use of it would hardly add any further protection for their devices).

Perceptions of future security requirements and responsibility

As the participants' limited security requirements were expected, an objective was to assess how future adoption of more sensitive services might affect their opinions. The majority certainly agreed that using more data-centric and sensitive services would increase their desire for protection:

> *"If you are using it from a business context, obviously you know the more important the data then the stronger security is going to be needed."*

> *"Although I don't use my phone for an awful lot more than texting at the moment, as phones get more sophisticated and easy to use etc ... I'm going to start using it for mobile banking or whatever the nature of the data that I'm gonna be using is going to become more sensitive definitely"*

Another aspect that was highlighted was the fact that stronger security would desirable in certain uses of the phone, as the danger of misuse would be increased.

> *"For example, if I make a local call ... maybe I'm not that worried ... But certainly when I want to start dialling international numbers or something maybe I do want to make sure that it's stronger authenticated. Maybe when I start to accessing documents that sit in a*

specific area of my device which is business documents then I want to be authenticated"

This view came in agreement with previous work by some of the authors that has suggested that linking the level of security to the service access would be a way of enhancing protection based on the sensitivity of the data (Clarke and Furnell, 2006). From this perspective, the question was explicitly posed as to whether it would be desirable to have distinct levels of security in order to be authenticated depending upon the service or data use. The general thought was that it could be a positive way to enhance security, but only if that was applied in a manner that maintained convenience:

"I don't want to have strong security for texting, but I do want to have some security for mobile banking, so different levels of security definitely would be the way to do it"

"It depends how you put it. How many levels? I would be happy with one or two. Right now I'm using my phone. Do I want to enter a text message? All right, next level. Do I want to browse the Internet? Another level . . . one level or two levels would be fine. But getting it too far, it would be 'all right which level do I need? I need access 3 or access 5?"

The idea of using their device to access more sensitive information led some participants to reassess the possibility to pay for additional security:

"When you start becoming more aware about stuff [dangers/threats] like that, you start realizing what you are doing with the phone as well. I think then you realize, actually I like the idea of [a network operator] providing higher security and I'll pay for that"

Nevertheless there was also the view that the even future would impose more fears, there would be an expectation of security provision from the side of the services that are being offered, rather than the device itself:

"The type of data that I use my mobile phone with, and will use in the future, won't be very different from the one that I use in my PC anyway. It will just be a different access device. So I expect, if I'm going to be using data that are sensitive from a personal level, it will only be with services that I expect to be secure anyway. I wouldn't necessarily pay extra for that because that is their whole point of existence"

Proceeding from this, it was interesting to see who participants generally considered to be responsible to provide security in the first place. Faced with this question, less than a third felt that it should be their own responsibility to ensure the security of their device. In terms of accessing services, the responsibility for security was felt to lie with a service provider (in order to secure the access and the data), rather than looking to protect the device itself in a more robust way:

> *"But then you are accessing bank accounts details that you're just using the mobile or whatever device you are using to access something somewhere else so the security is there…Responsibility for bank details should be with the banks, so they look after your confidential detail and security for your own device should be yourself"*

The idea of making the network provider responsible for securing access to services and information was not viewed positively, again reflecting the fact that participants would prefer a distinction in the different roles.

> *"Not only you are trusting them with your password details but also that implies that they are never going to make a mistake, that they are never not going to pass your username and password on to somebody else. If I'm going to authenticate myself and log myself into a particular server, I actually want control of that. As much as I hate passwords, I want to have control over who I login with"*

> *"Having my network provider say 'Oh don't worry, we'll authenticate you to the bank', that's something that I want them separately. You just give me network access, I'll deal with the bank, don't worry about it"*

Given that most of the participants would prefer additional protection to be on their side rather than relying on the provider, it is relevant to consider the form(s) that this could take. As such, the next discussion topic proceeded to consider alternative authentication methods.

Views & attitudes towards alternative methods of user authentication

As alternatives to the PIN, participants were asked to consider two approaches – tokens and biometrics - and the way that they could be applied in the context of mobile phones.

Participants were not receptive to using tokens. Considering the device to be a token itself, the idea of needing to have something else to access it was not well-received:

> *"My first opinion would be that is just something else to lose…you still have the same issues with the token, because somebody could pinch the token, or I would lose it more likely"*

> *"It's also the annoyance. Unless it's something you wear all the time… if I want to make a phone call I also have to take my watch or my key ring or whatever"*

Unlike tokens, there was relatively high acceptance of the potential to use biometric techniques. As previous work has shown, users are starting to be more open to biometric techniques and consider their use in order to enhance security (Clarke *et al*. 2002). When the participants were asked which biometrics they would like to see implemented on mobile handsets and would be more willing to use, the majority

agreed that fingerprints would be adequate enough to safeguard the device, while at the same time seeming convenient:

> *"Personally I'd use fingerprint, it's easy…"*

> *"I think fingerprint recognition would be fine on a phone…the average person who's gonna steal this, even if they do know how to fake the latex and so how to fake the finger, why would they bother? Just to break into somebody's mobile phone?"*

Others were more open to techniques that could be linked to their normal use of the device or be derived from the features already existing on the device.

> *"There's a Korean phone that does facial recognition. I don't know how successful it is"*

> *"Voice as well…obviously when you are talking"*

Despite the fact that different kinds of biometrics were suggested by the attendees, fingerprint scanning was the most popular. As the technique is one of the most well-known biometrics, the question was posed as to whether this preference was linked to the greater knowledge of the technique in comparison with other approaches. The responses were mixed, with the general view being that it is just more convenient than other options. However, one participant also observed that it is a matter of culture, as many of us feel familiar with fingerprinting as a result of seeing it used in crime movies and the like. It was conjectured that other approaches would achieve similar acceptance on mobile devices if they were similarly familiar from other contexts:

> *"If ... in order to get into the school, you needed to have your iris scanned then it would be like: 'All right, I had my iris scanned all my life, I don't mind really'"*

In respect to the fingerprint versus other techniques, an argument that was made was the fact that biometric approaches that could depend on the use of the device are not applicable throughout all users as each one differs in their usage. As such biometrics like fingerprints can provide a common solution.

> *"I only use it for voice, he [another attendee] only uses it for texting. It's a mobile so one way or another you will have to hold it in your hand to actually use it so fingerprint is the most appropriate from that perspective"*

This view underlines the fact that as no approach fits all needs, whether that is PINs or certain biometrics. Thus instead of providing one solution that some users are not willing to use, having a flexible mechanism that could conform to each user's needs while at the same time fulfilling the different security requirements would be a more appropriate approach. This is again compatible with the previous proposals from the authors (Clarke and Furnell, 2006)

Another issue raised in the discussion of biometrics was that of privacy, which has traditionally been presented as one of the factors that make people cautious about using the technology (Cavoukian, 1999). However, in terms of influencing preference towards certain techniques, privacy was not of much concern for the group. Most attention was given to the lack of accuracy and the excessive effort that biometrics (especially those based upon behaviour) may require, but also in certain techniques that they felt they could be less secure in their application on mobile phone:.

> *"The thing is even though it's a telephony device, the one I would be more uncomfortable using is voice, because anyone else can hear it"*
>
> *"And having any background noise affects voice recognition"*
>
> *"My problem I found is the signature recognition. I didn't like the voice recognition but as we were saying earlier for mobile phones that will be the most acceptable really. But the signature recognition I had problems with. My signature is never the same five times in a row, so I would get locked out of my mobile phone if I did that"*
>
> *"You can see…It's something about seeing an iris…if it went wrong and I was locked out … I'd feel out of control"*

On that basis, although acknowledging the level of security that biometrics can provide, participants would have little tolerance of getting falsely rejected and being locked out of the device:

> *"If it always let me through I'd be prepared to put up with that [false acceptance errors], because it's still a greater level of security that I use now and it's still not bothering me….I'm prepared to let the mistake happen as long it's not for me, as long as I am always let through"*

Transparent & continuous authentication versus traditional point-of-entry methods

With the issue of personal convenience still in mind, participants were asked to consider whether authentication can run in the background without the user having explicit knowledge about when it was taking place or needing to make explicit effort to provide authentication details. This has been suggested not only to overcome issues of intrusiveness that PINs or biometrics such as fingerprints could pose, but also to provide a continuous authentication solution versus the point-of-entry verification of PINs that was attributed a lack of protection by the attendees. Asked how they would feel about such a mechanism, attendees offered varying responses:

> *"I would like it cause if it doesn't interfere with you and there is no different reason anyway so there is no problem is it?"*
>
> *"I don't have a problem with this in a sense that I don't worry about the device monitoring me, but I will probably if something pops out and say 'No, you are not who you say'. Soon as it does that switch it off and then switch it on again"*

"That will be annoying…it would be like 'Oh it thinks it's not me'"

"Will it be a bit like when your battery is lowering gives you a warning? 'Cause how would you know? You make three mistakes or there are three different things in the background"

The negative views were mainly due to fears that false rejections could cause potential inconvenience by interrupting legitimate use of the device. There was also concern that the casual use of a mobile phone would not permit this type of authentication, as it would be difficult to acquire a consistent biometric profile at all times, again raising the issue of rejection rates:

"It's okay if you use it at your desk or something maybe but…I mean the nature of the mobile phone is that you don't generally use it like that. If you are sitting in a train or in a car or you are walking and you want to do something …I can't imagine that the way that I use it that I could be following a pattern. I'd get that three exceptions every five minutes kind of thing…I would feel uncomfortable"

Despite the potential intrusiveness, there was also the view that it would be preferable to have explicit authentication so that the user is always conscious of the procedure:

"I don't like the idea of any form of machinery interacting with me, without me giving it express permission that it may. I just don't like it, full stop"

Nevertheless that was not an issue for the majority of the participants. It was interesting enough that the main issue was usability and convenience, and less the issue of privacy that is often brought up in relation to biometrics. More focus on privacy came when the group was asked to give their opinion on how such an approach should be implemented - specifically in terms of the authentication taking place locally in the device or in the network (and thus where the biometric profile would need to be held):

"My concern is where would the fingerprint, let's say like signature, where would be stored? Would that be stored on the phone, so if somebody stole my phone they have my signature which is signed on the back of your bank cards and my fingerprint obviously? What then can people do with the information…obviously if someone knows how to hack into a phone could they use the information?"

As seen above the fear of having a device lost or stolen would discourage the idea of keeping the profile on the phone. On the other hand, there was also a view that storing the profile in the network would pose not only issues of control (moving from the user to the provider) but also the issue of who handles that information when it is on the side of the provider. In that context there were negative views about storing profiles in the network:

> *"Would you really want your biometric data stored on the inside of a company that's possibly got people, dodgy people breaking into it already?"*

Aside from trust towards the provider, two more issues were raised by the attendees in respect to the remote storage of the profile. First was the issue of immediacy of access and availability:

> *"Potentially everything can be stored in the network. There is a trade-off between responsiveness and security….Especially if you are not in coverage all period of time and you want to look up someone's name, address or whatever in your address book you haven't got it…There's got to be some balance between security that happens on the network and immediacy you have on the person"*

Similar to the issue of immediate access, participants indicated that they would not like to have explicit interaction with the provider in order to get authenticated. The preference was towards achieving authentication locally.

> *"I'd like to use that information even when I don't interact with the network operator. Because I can certainly use authentication as well, so I can't think that it can be just the network operator"*

Conclusions

This research recorded the views and attitudes of mobile phone users towards security on mobile phones. Most participants in the focus group did not see a significant need for security on their current mobile phones. However, the possibility of using their mobile phones for more than just calls and short messaging was recognized. The members of the focus group that used their mobile phones for more advanced tasks acknowledged that some form of security is important.

This was also reflected in the current use of authentication mechanisms. Most participants either did not use any authentication mechanism, or only used a PIN request at power up time, and were generally concerned with the inconvenience of current mechanisms. However, they were also receptive to the view that future, more sensitive uses of their device would necessitate greater use of security, and were therefore open to the consideration of alternative authentication methods.

Taking into consideration the concerns regarding the convenience of authentication mechanisms, it is not surprising that most participants were positive towards the use of biometrics and specifically fingerprinting. However, some privacy concerns were raised, particularly as to what exactly gets stored and where it gets stored. Others were concerned about being monitored continuously, especially if unaware of the fact.

This research supports the researchers' view that further work towards a comprehensive framework for authentication on mobile devices is indeed necessary. Furthermore it provided valuable insights into user perspectives on these matters.

Acknowledgements

This work has been conducted as part of a 2-year research project, funded by the Eduserv Foundation. Part of this research was also made possible through a grant under the SA/UK Networking agreement administered by the South African National Research Foundation (NRF GUN 2074892).

References

Cavoukian, A. (1999) Privacy and Biometrics, Information & Privacy Commissioner of Ontario, Canada, http://www.ipc.on.ca/images/Resources/pri-biom.pdf

Clarke, N., Furnell, S.M, Rodwell, P.M, Reynolds, P.L (2002) Acceptance of Subscriber Authentication Method for Mobile Telephony Devices, Computers & Security, 21, 3, 220-228

Clarke, N.L., Furnell S.M. (2005) Authentication of Users on Mobile Telephones - A Survey of Attitudes and Practices, Computers & Security, 24, 7, 519-527

Clarke, N.L., Furnell S.M. (2006) A Composite User Authentication Architecture for Mobile Devices, Journal of Information Warfare, vol. 5, no. 2, 11-29

Ernst & Young (2005) *Global Information Security Survey 2005 : Report on the Widening Gap*, http://www.ey.com/global/download.nsf/International/Global_Information_Security_Survey_2005/$file/EY_Global_Information_Security_survey_2005.pdf

Kucan, B. (2003) Stolen PDAs Provide Open Door to Corporate Networks, Help Net Security, 1 August 2003, http://www.net-security.org/article.php?id=533

Red Herring (2006) Mobiles Scream for help: UK-based mobile security company adds security to mobile phones, 2 October 2006. http://www.redherring.com/Article.aspx?a=18907&hed=Mobiles+Scream+for+Help

Pointsec (2005) IT Professionals Turn Blind Eye to Mobile Security as Mobile Survey Reveals Sloppy Handheld Habits, Pointsec News Release, 18 November 2005, http://www.pointsec.com/news/newsreleases/release.cfm?PressId=108