available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

From desktop to mobile: Examining the security experience

Reinhardt A. Botha[a], *Steven M. Furnell*[b,*], *Nathan L. Clarke*[b]

[a]*Institute for ICT Advancement & School of ICT, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa*
[b]*Centre for Information Security & Network Research, University of Plymouth, Plymouth PL4 8AA, United Kingdom*

ARTICLE INFO

Article history:
Received 25 October 2008
Accepted 4 November 2008

Keywords:
Mobile
Smartphone
User experience
Authentication
Connectivity
Content security

ABSTRACT

The use of mobile devices is becoming more commonplace, with data regularly able to make the transition from desktop systems to pocket and handheld devices such as smartphones and PDAs. However, although these devices may consequently contain or manipulate the same data, their security capabilities are not as mature as those offered in fully-fledged desktop operating systems. This paper explores the availability of security mechanisms from the perspective of a user who is security-aware in the desktop environment and wishes to consider utilising similar protection in a mobile context. Key issues of concern are whether analogous functionality can be found, and if so, whether it is offered in a manner that parallels the desktop experience (i.e. to ensure understanding and usability). The discussion is supported by an examination of the Windows XP and Windows Mobile environments, with specific consideration given to the facilities available for user authentication, secure connectivity, and content protection on the devices. It is concluded that although security aspects receive some attention, the provided means generally suffer from usability issues or limitations that would prevent a user from achieving the same level of protection that they might enjoy in the desktop environment.

1. Introduction

An increasing amount of information is being stored on mobile devices. Indeed, it has been suggested that, in business scenarios, over 80% of new and critical data is now stored in this context (Allen, 2005). In 2005, Gartner predicted that smartphones would be favoured as thin clients for mobile workers (Jones, 2005), and the subsequent quarter-on-quarter growth in smartphone shipments, of 49.8% in Q2 2006 (Cozza et al., 2006) and 44% in Q2 2007 (Cozza et al., 2007), is certainly indicative of their increasing popularity.

Although a broad definition of mobile devices would include laptop computers, the focus of this paper is specifically geared towards pocket and handheld devices such as cellular phones and Personal Digital Assistants (PDAs), with the convergence of these devices into so-called smartphones also being relevant. While not as powerful as desktop or laptop systems, these devices now support a fairly rich set of functionality, with a variety of personal information management features (e.g. contacts, scheduling, etc.), cut-down versions of applications such as word processors and spreadsheets, and Internet connectivity via email, web browsing, and instant messaging. Even at a baseline, the data held on such devices could include contact details of clients and suppliers, or calendar items revealing sensitive business dealings. As such, they can clearly be an asset worthy of protection.

Unfortunately, in addition to their capabilities, mobile devices are by their very nature more vulnerable to threats

* *Corresponding author*. Tel.: +44 1752 586234.
E-mail address: sfurnell@plymouth.ac.uk (S.M. Furnell).
0167-4048/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2008.11.001

such as theft and accidental loss than larger systems in fixed locations. For example, back in 2001, the UK Home Office highlighted the desirability of mobile phones as targets for theft, reporting that over 700,000 handsets had been stolen (Harrington and Mayhew, 2001). Meanwhile, other unofficial reports (Leyden, 2002) put this figure in the region of 1.3 million. In addition, pocket devices are extremely susceptible to loss; a problem that is clearly indicated by the following advice quoted from the London Taxi lost Property site (our emphasis added):

> *"For mobile phones, it is essential that you supply details of the phone make and model, mobile phone service, and either the IMEI number of the phone or your SIM card number. Due to the quantity of mobile phones received, individual mobile phones cannot be identified without this information."* (London Taxi, 2007)

From a security perspective, the significant consideration here is that these devices may contain possible sensitive or valuable information (Chapman, 2007). Of course the risk can be downplayed by arguing that many of these thefts are committed in order to obtain the devices rather than their data. While this may potentially be true for now, the increasing role of the devices as repositories of sensitive information means that opportunities for data exploitation may not be overlooked for long.

In view of these threats, it is reasonable to suggest that security is an increasingly important consideration. Moreover, the fact that mobile devices now store and access comparable data and services to desktop systems implies that similar security provisions ought to be available. Indeed, some users will already utilise security on their desktop, and will be keen to parallel this on their mobile devices. Unfortunately, however, the reality of their experience may currently be quite different, with obstacles posed by mechanisms that are presenting in a different way, or indeed by functionality that is absent entirely. This raises fundamental problems. If the security features are not available, then data will be receiving less protection in a fundamentally more vulnerable location. If the features exist, but are not presented in a comparable manner, then it may mean that users cannot easily transfer their security skills from the desktop.

This paper examines the differences in security mechanisms between desktops and mobile devices that users may encounter when attempting to perform the same core tasks. This is explored from three perspectives: identification and authentication, network connectivity, and content security. Key aspects of each are examined from the perspective of a desktop user looking for the related features in a mobile context. The evaluation enables conclusions to be drawn regarding the security features that exist, and the consequent similarity of the end-user experience between current desktop and mobile systems.

2. Comparing the security experience in desktop and mobile environments

In spite of their fundamental difference in physical form factor, mobile devices can facilitate access to much of the same data, and many of the same services and applications, as their desktop counterparts. As such, a baseline argument for cognate security is easy to make. However, a notable difference is the context in which certain security features are being used. One of the most distinguishing differences between smartphones and desktop computers is that the former is a personal device, typically used by one person, whereas the desktop PC is quite often shared between various users. However, the aforementioned problems of loss and theft can render mobile devices vulnerable to unauthorized use. The need for identification and authentication is therefore different than in the desktop world. This represents the first aspect for a detailed discussion.

Furthermore, the user of the mobile phone is often more responsible for its configuration (especially if it is a private purchase), whereas desktop computers are often controlled (in work settings at least) by administrators. Not only may typical users not be knowledgeable about the various options for connectivity, but they also could find configuring the communication channels challenging due to their lack of experience in configuring desktop environments. As a consequence, the second aspect of the discussion deals with connectivity issues.

Finally, the mobile device, like a desktop, may store valuable information. However, the higher risk of physical loss and the use of removable media may yield a higher priority on protecting content by means other than controlling access to the device. As such, the final area in the discussion is focused upon content security.

Due to the wide prevalence of Microsoft Windows on the desktop and its increasing popularity on mobile devices, our descriptions are based upon consideration of Microsoft Windows Mobile 6 Professional Edition, as contrasted against Windows XP (and accompanying applications) on the desktop. The logic here is that users would reasonably expect a higher degree of similar functionality than with operating systems from different providers. Although Windows Vista is available, XP was selected on the basis that it is the most prevalent desktop version at the time of writing, and hence the most likely baseline against which users' security expectations would be established. Version 6 of Windows Mobile was selected over the (currently) more popular version 5 on the basis that it represented the latest state-of-art in mobile OS and includes a number of security-related improvements over its predecessor. The Professional Edition was preferred over the Standard Edition as it targets PDA-style devices rather than those with a cellphone form factor. We argue that users would expect more of a desktop-like experience in this context, as the displays are often larger, and the devices often have mini-keyboards in addition to stylus-based input.

3. User authentication

The nature of user authentication on mobile devices has remained largely unchanged since their inception, with the vast majority of devices relying upon point-of-entry protection via a Personal Identification Number (PIN). In this respect, the underlying principle is similar to that on most desktop systems, with both relying upon secret-knowledge authentication approaches. However, a fundamental difference on the mobile

device is that the user may encounter multiple mechanisms, in order to lock different aspects of functionality. Specifically, when used on devices supporting telephony, Windows Mobile handsets support two distinct authentication mechanisms: one to protect the mobile device, and another to protect the user's SIM (Subscriber Identification Module). The device-level authentication provides the frontline protection when the handset is switched on, and therefore regulates access to applications and the majority of the user's stored data (the exception being any data, such as contact details, which the user may have stored on the SIM). The use of SIM-level authentication aims to safeguard against the unauthorized use of the user's cellular network account, recognizing that the card could otherwise simply be removed from a protected device and used in an unprotected one. If enabled, the SIM-level PIN effectively governs the ability to make voice calls and use network services via cellular data connections.

From the user perspective the fact that two mechanisms are available can be a source of confusion, as they frequently fail to realize that they have two distinct assets requiring protection (i.e. SIM and device). Further confusion can be introduced by the fact that the mechanisms vary in style. While the SIM protection always takes the form of a 4–6 digit PIN number, the style of the device-level authentication is user configurable, and can be either a PIN or password (see Fig. 1). Additionally, there may also be a further level of protection, referred to as PIN2, which is able to safeguard against unauthorized modification of network settings, such as fixed dialing or call barring.

For the device-level protection, the password clearly represents the stronger option, and is more likely to parallel the authentication mechanism used on the desktop (thus allowing a user taking data from one location to the other to afford it equivalent protection). However, this overlooks one of the significant differences in how desktop and mobile devices may be used. Whereas a user sitting at a desktop is likely to tolerate the entry of a password (on the basis that they are likely to be using the system for some time), 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. As such, the authentication method needs to be compatible with the likely frequency and duration of use of the device. The problem is that this is difficult to predict on the mobile device (e.g. there will be other contexts in which the user will access the device for long periods and perform more sensitive tasks).

As a partial consequence of the above, authentication does not appear to be as widely employed on mobile devices as it is on the desktop. For example, a survey of 297 cellphone users, conducted by Clarke and Furnell (2005), found that 34% did not use any PIN security at all. A subsequent focus group study, conducted by Karatzouni et al. (2007), revealed similar findings, with many participants initially believing that they did not have anything of value to protect on their mobile device, as well as citing the inconvenience of the method as the reason they did not use it.

Even if it has been enabled, another potential weakness of user authentication in the mobile context is the one-off nature of the process. Although re-authentication after a period of inactivity has been widely accepted by users on desktop systems, the use of such features on mobile devices is not widespread, with the survey reporting that just 18% of users utilized standby PIN protection (again indicating the perceived inconvenience of the approach). Given that mobile devices are increasingly being left on, it is imperative that a user's identity be confirmed periodically. Research has proposed solutions that enable transparent authentication of the user (Clarke and Furnell, 2007; Mazhelis and Puuronen, 2007), but such concepts have not to date been realized within practical systems.

Rannenberg (2004) indicates that the SIM infrastructure inherent to cellular networks provides an identity management platform that can enable several application oriented innovations. Although we agree with that observation, one must point out that, while this can successfully identify the SIM card that was used, there is no guarentee that it was being used by its genuine owner. This emphasises the need to have better identification and authentication on mobile devices; however, usability and user acceptance issues leaves us far from a clear answer. To complicate matters, the cellular network is by no means the only network that a mobile user may connect to. With this in mind, the next section investigates issues relating to secure connectivity in more depth.

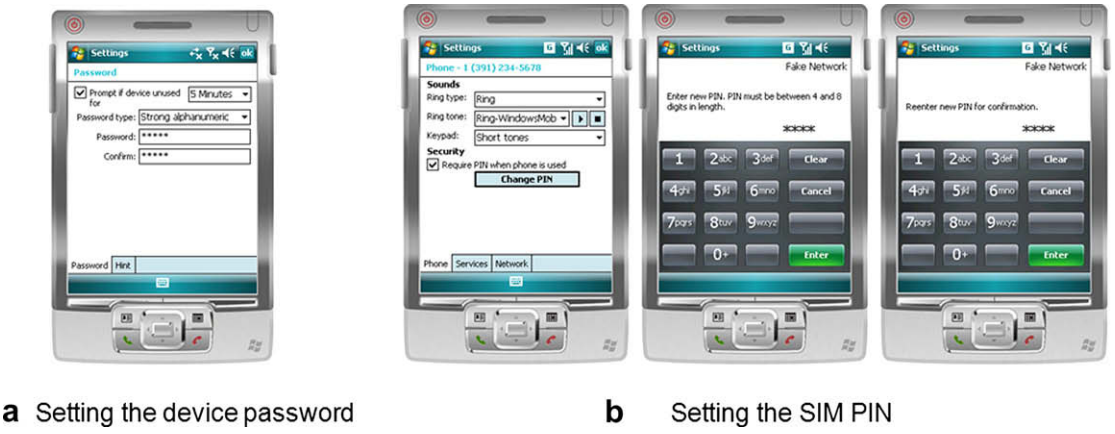

Fig. 1 – Different interaction styles for basic security settings.

4. Dealing with connectivity

A Windows Mobile 6 device can offer several forms of connectivity, encompassing personal, local and wide area networking. Security-relevant considerations can be found, to varying degrees, at each of these levels.

At the personal area level, the functionality is typically offered via infrared (IR) and Bluetooth communications. The only tangible configuration option for IR communication is to be found under the 'Beam' setting, which in turn has only one option – 'Receive all incoming beams' – which can be toggled on or off. Although it is explained in the Help system, what is not made at all apparent from the interface-level presentation of this option is that it relates to both IR and Bluetooth beams, and there is no facility to configure the different routes independently. Some level of control can be achieved by using other settings to turn Bluetooth on or off (such that the 'beam' setting will then only apply to IR), there is still no means to be receptive to Bluetooth beams without IR being active at the same time.

The use of these connectivity options leads to a relevant observation about the visibility of information for the user; specifically, that there is no indication on the Title bar to show that IR or Bluetooth connectivity is enabled (although this is to some extent handset-dependent, as some may flash a light to signify that Bluetooth is active). It would certainly be relevant to have a reminder, as there are implications from both security (especially if the device is set in 'discoverable' mode) and power management perspectives.

At the local networking level, most devices now provide connectivity via wireless LAN. Given that mobile users may frequently find themselves in unfamiliar surroundings, and uncertain about which networks may be legitimately available to them, an important consideration is how much the device tells them about the networks in the vicinity (e.g. in order to guard against inadvertent trespassing on unprotected private networks, or simply mistaken attempts to connect to the wrong networks). In earlier versions of Windows Mobile users searching for wireless networks were simply presented with a list of SSIDs and an indication of whether the associated networks were within range or not. What was notably lacking was an indication of whether the available networks were open or secured, requiring the user to bring up its properties and then move to the 'Network Key' tab order to find the details. This extra step not only added a level of inconvenience, but it also required the user to actively go *looking* for the security status. However, given that some users may not *know* that they ought to do this, they may simply see that a network is listed as 'Available' and assume that it is permissible for them to use it (and then be confused as to why they cannot actually connect). This aspect has been notably improved in the current version of Windows Mobile, and the user now receives an upfront indication of the security status of any available networks. As such, this is one area in which the user will now have a similar experience as with the desktop version of the operating system.

For devices supporting cellular network access, there are also opportunities for wide area data communications. However there is little for the user to configure in terms of security. Essentially, the options relate to GPRS security settings, allowing the user to select whether PAP or CHAP authentication should be used (both of which are briefly explained in the Help system). Beyond this, the security on the cellular network (e.g. device-level authentication of the handset) is handled transparently from the user perspective.

The availability of such a range of connectivity options is likely to be in marked contrast to the user's experience on the desktop; raising a consequent question about their ability to choose the appropriate method and to assess the risks associated with it. Although it can be argued that some of the shortcomings are inherent factors of the network type rather than the concern of the Mobile OS, the lack of consistency from the user interface perspective does not aid the situation. Moreover, the environment is to some extent characterised by limited configurability and a lack of accompanying help. Indeed, the level of help available for security topics is rather variable, and several security-related settings (e.g. LEAP settings for WLAN authentication; Passkeys in Bluetooth partnerships) are not adequately explained. The combination of these factors does not bode well for the novice user's experience.

Having considered the security in relation to the networking technologies themselves, it is also relevant to consider what users may encounter in relation to their subsequent communications. One of the primary applications here is, of course, the Internet Explorer browser, and it quickly becomes apparent that the more limited nature of the browsing experience has implications from the security perspective. For example, those used to security and privacy options in a standard desktop browser will find a vastly reduced set available in the mobile context. So, whereas Internet Explorer 7 includes over 45 configurable options (via the 'custom' security settings), the mobile incarnation of the browser offers only 3 related settings. This contrast is illustrated in Fig. 2. Of course, much of the explanation for this relates to the fact that the mobile browser itself does not support many of the features that would otherwise introduce security risks (e.g. scripting and ActiveX). Nevertheless, there is a lack of coverage in the Help system to explain to users how their vulnerability (i.e. exposure to threats) when web browsing may differ in the mobile context.

Having flagged this significant difference, it should be noted that there are certain things that work as a desktop user would expect. For example, the mobile browser supports https secure sessions, and presents associated warnings to the user if certificates are not valid. Moreover, the Help system includes relevant entries to provide an overview of certificates, and how to view and delete them. Meanwhile, in terms of connection security, support is also offered for establishing VPN connections (albeit with the location of this functionality making the assumption that the user will only wish to do this in relation to 'work' networks).

Having established that the experience with the connectivity-related aspects is rather mixed, the discussion now proceeds to consider the security available to protect content held on the device.

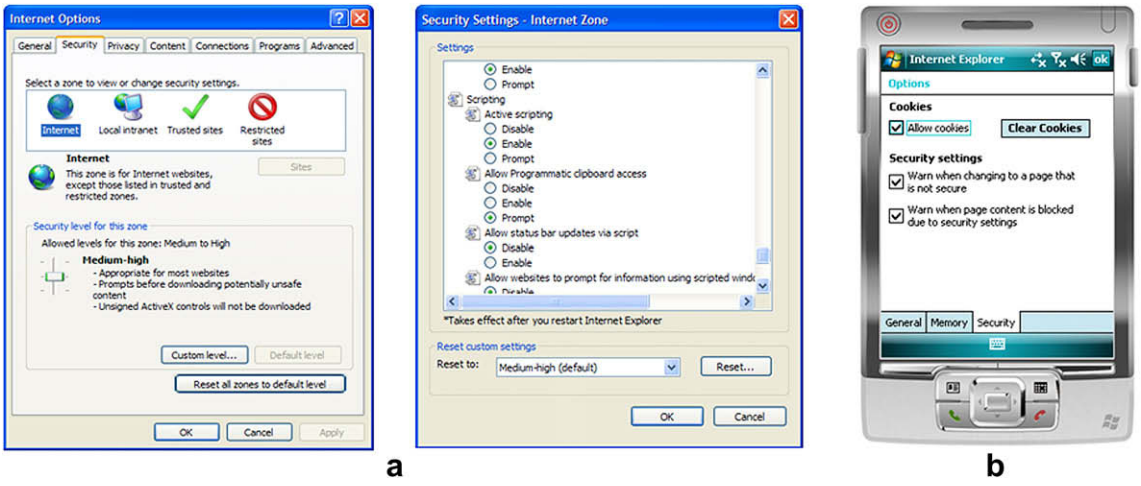

Fig. 2 – Contrasting the security options in desktop versus mobile web browsers.

5. Content security

Early generations of cell phones and PDAs had relatively little storage capability, with the consequence that their potential to store sensitive data was limited. The situation today is dramatically different, increasing the likelihood that data will be created with, or transferred onto, mobile devices. However, the related protection of such content is another area in which a marked contrast to the desktop experience can be observed, in the sense that the mobile versions of the software may not support the application-level security features that are to be found in their desktop counterparts. A good example of this is provided by Word Mobile, which allows documents to be taken from the desktop and then viewed (and to some extent manipulated) on the mobile device. However, a notable constraint of the mobile application is its lack of support for password-protected documents. Attempting to use Word Mobile to open a document that has been password-protected in the desktop version of Word yields the result shown in Fig. 3. Word Mobile is unable to open a password-protected document created on Word on the desktop. It follows that users cannot transfer this element of good practice from the desktop to the mobile. Furthermore, if they genuinely need to access the content on their mobile device, they are obliged to remove the protection first (resulting in sensitive data being stored with less security in a more vulnerable location). The lack of document-level protection effectively means that access to private information must rely solely upon the device-level authentication process to provide frontline safeguard against unauthorized access.

A further content-related risk with the mobile device is that files will often be stored on removable media (such as SD cards) rather than solely in the device memory. This is essentially unprotected by the authentication method applied to the device, in the sense that (unless further measures are applied) an attacker could simply remove the card and read it in another device. As a consequence, devices offer the option to store files on cards in an encrypted form – representing an additional feature in Windows Mobile 6 when compared to earlier versions of the OS (Microsoft, 2007b). This at least ensures that the removable media cannot be read on other devices. As can be seen from Fig. 4 this is an easy activity with the consequences of the action spelled out clearly. This may provide an adequate measure if the actual storage media is lost. However, it could be argued that a greater level of granularity would be desirable here. For example, given that the card itself is removable media (and therefore inherently offers the flexibility to be used in other devices), it would be preferable for the user to be able to apply security selectively to sensitive files rather than as a blanket judgment across the whole set. Of course, the effectiveness of this measure (even with more granularity) relies upon adequate user

Fig. 3 – Word and password-protected documents.

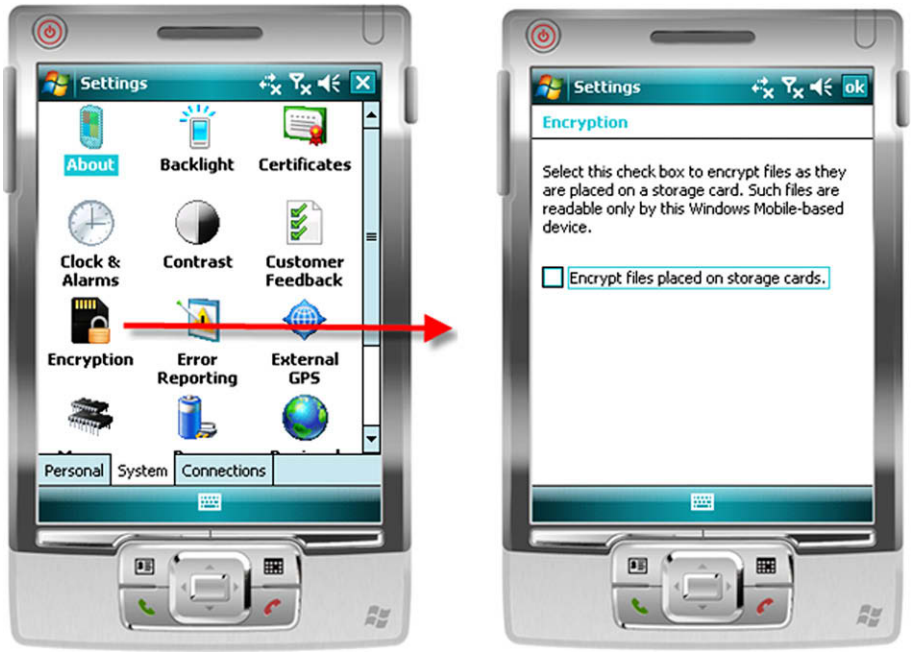

Fig. 4 – Storage card encryption feature in Windows Mobile 6.

authentication on the device, which the earlier discussion has established may not be the case.

For the future, Digital Rights Management is heralded as the answer to protecting document-based content irrespective of its whereabouts. This functionality is supported through a standard API provided by Windows Mobile 6. However, this would require applications that are sensitive to the DRM protected content, as well as a FDRM server implementation (Microsoft, 2007a). Since Digital Rights Management as an enterprise solution is still in its infancy we do not consider it here further in the context of mobile devices, other than noting that the support for it is promising. It is arguable, however, how much of the functionality was built-in to protect business documents versus the drive to protect entertainment resources such as music and video.

6. Discussion and conclusion

The investigation has shown that although elements of security are provided on mobile devices, the extent and usability of the implementation are often lacking. This is especially worrying since the devices will routinely operate outside of physically controlled environments and so will be at increased risk of exposure.

Summarising the main findings from the assessment, it can be seen that users face a varied experience in moving from desktop to mobile contexts. In terms of authentication, there is a trade-off between security and usability, in the sense that while mobile devices can support comparably secure password-based authentication, it becomes an inherently less usable safeguard in this context. A possible solution may lie with the use of alternative authentication paradigms, such as biometrics, which have the potential to provide stronger security than a password and can operate in a more convenient manner. However, such measures are not widely available on PDA-style mobile devices at the time of writing. From a connectivity perspective, mobile devices typically support a range of options, some of which may not be directly familiar to the user in the desktop environment. The fact that each type of connectivity has its own security issues and distinct configuration options can represent a conceptual challenge; the user needs to know which networks facilitate which services, and what level of security is available. Finally, in terms of content protection, mobile devices often support reduced levels of security functionality. In some cases, such as with Internet Explorer, this is because the applications themselves support a more restricted range of features, and thus the security measures that one would find on the desktop are simply not relevant. In other cases, such as with document protection, the desired functionality may simply be lacking and users are required to modify their security expectations accordingly. The key thing in both cases is that users need to be aware of the limitations, because they may otherwise simply perceive an inconsistency in their desktop to mobile experience.

It is relevant to note that many of the comments and criticisms raised in the discussion relate to the specific way in which the interface aspects of Windows Mobile have been realized, rather than any usability problems that are unavoidable on a mobile device. As such, a key point to take away is that many of the issues could have been avoided if security (and the user's need to access it effectively) were to have been given greater consideration. Indeed, linked to the problems posed by the interface is the fact that the security-related options in the Professional Edition of the OS were fractured across various settings and applications. By contrast, it is interesting to note that the Standard Edition improves upon this with a 'Security' option on the settings menu, as illustrated in Fig. 5. This groups many of the related

Fig. 5 – Windows Mobile 6 Standard Edition security settings menu.

functions together in one place, and is somewhat analogous to the 'Security Center' on the desktop version of the OS. Even then, however, it does not include any of the options relating to secure connectivity, which again leads to unnecessary separation. Having said this, such problems are far from solved in the desktop environment, with security often being complicated by avoidable usability issues (Furnell et al., 2006; Furnell, 2007).

Even if the security-related functionality is appropriately grouped, the problem may remain that it needs to be managed by end-users. Although a growing number of remote management tools are available that enable administrators to have a greater control of devices when used in a corporate context (i-mate, 2007; SOTI, 2007), this does not assist a large number of users who purchase their own devices and still use them to hold and access sensitive data. As such, the ultimate goal on the mobile device essentially remains the same as on the desktop; to make security available in a manner that the user can understand and use, and at the same time give them an appropriate level of protection and reassurance.

REFERENCES

Allen M. A day in the life of mobile data. Mobile Security, British Computer Society. Available from: http://www.bcs.org/server.php?show=conWebDoc.2774; November 2005.

Clarke NL, Furnell SM. Authenticating mobile phone users using keystroke analysis. International Journal of Information Security 2007;6(1):1–14.

Clarke N, Furnell S. Authentication of users on mobile telephones – a survey of attitudes and practices. Computers & Security 2005;24(7):519–27.

Chapman M. Mobile phone users oblivious to data threats. Available from: http://www.vnunet.com/vnunet/news/2188621/mobile-phone-users-oblivious; 2007.

Cozza R, Liang A, Mitsuyama N, Nguyen TH, De La Vergne HJ. Quarterly statistics: PDAs and smartphones, all regions. Gartner Research Report G00141146, 19 September, 2007.

Cozza R, Mitsuyama N, De La Vergne HJ, Liang A, Nguyen TH. Market trends: smartphones, worldwide, 2006. Gartner Research Report G00143276, 12 September, 2006.

Furnell SM, Jusoh A, Katsabas D. The challenges of understanding and using security: a survey of end-users. Computers & Security 2006;25(1):27–35.

Furnell SM. Making security usable: are things improving? Computers & Security 2007;26(6):434–43.

Harrington V, Mayhew P. Home office research study 235: mobile phone theft. Crown Copyright; 2001.

i-mate Suite. Advanced management solution for mobile devices. i-mate PLC. Available from: http://www.imatesuite.com/; 2007.

Jones N. Smartphones to be favored as thin clients by mobile workers. Gartner Research Report G00127690, 27 May, 2005.

Karatzouni S, Furnell SF, Clarke NL, Botha RA. Perceptions of user authentication on mobile devices. Proceedings of the 6th Annual ISOneWorld Conference, 11–13 April, 2007, Las Vegas, NV, pp. 55-1–55-13.

Leyden J. Mobile phone theft is far worse than we thought. The Register, http://www.theregister.co.uk/content/archive/24138.html 20 February, 2002 [accessed 09.07.07].

London Taxi. Lost property information, http://www.london-taxi.co.uk/taxi/lost-property.htm; 2007 [accessed 09.07.07].

Mazhelis O, Puuronen S. A framework for behavior-based detection of user substitution in a mobile context. Computers & Security 2007;26(2):154–76.

Microsoft. File-based digital rights management, http://msdn2.microsoft.com/en-us/library/bb446727.aspx; 2007a [accessed 23.10.07].

Microsoft. Microsoft reveals new windows mobile 6 smartphone software, improves world's fastest-growing mobile operating system. Available from: http://www.microsoft.com/presspass/press/2007/feb07/02-11WM6SoftwarePR.mspx; 2007b.

Rannenberg K. Identity management in mobile cellular networks and related applications. Information Security Technical Report 2004;9(1):77–85.

SOTI. SOTI MobiControl V5. SOTI INC. Available from: http://www.soti.net/; 2007.

Reinhardt A. Botha is a professor in the Institute for ICT Advancement and the School of ICT of the Nelson Mandela Metropolitan University, Port Elizabeth, South Africa. He holds a PhD in Computer Science from the Rand Afrikaans University (now University of Johannesburg) in Johannesburg, South Africa. His research interests encompass Information Security, Mobile Computing and IT Service Management.

Steven Furnell heads the Centre for Information Security & Network Research at the University of Plymouth in the United Kingdom, and is an Adjunct Professor with Edith Cowan University in Australia. He specialises in computer security and has been actively researching in the area for fifteen years, with current areas of interest including security management, computer crime, user authentication, and security usability. Prof. Furnell is a Fellow and Branch Chair of the British Computer Society (BCS), and a UK representative in International Federation for Information Processing (IFIP) working groups relating to Information Security Management (of which he is the current chair), Network Security, and Security Education. He is the author of over 190 papers in refereed international journals and conference proceedings, as well as the books Cybercrime: Vandalizing the Information Society (Addison Wesley, 2001) and Computer Insecurity: Risking the System (Springer, 2005). Further details can be found at www.plymouth.ac.uk/cisnr <https://www.cisnr.org/exchweb/bin/redir.asp?URL=https://www.cisnr.org/exchweb/bin/redir.asp?URL=https://www.cisnr.org/exchweb/bin/redir.asp?URL=http://www.plymouth.ac.uk/cisnr>.

Nathan Clarke graduated with a BEng (Hons) degree in Electronic Engineering in 2001 and a PhD in 2004 from the University of Plymouth. He has remained at the institution and is now a senior lecturer in Information Systems Security within the Centre for Information Security and Network Research. Dr Clarke is also an adjunct scholar at Edith Cowan University, Western Australia. His research interests reside in the area of user identity, mobility and intrusion detection; having published 40 papers in international journals and conferences. Dr Clarke is a charted engineer, member of the British Computing Society (BCS), the Institute of Engineering Technology (IET) and a UK representative in the International Federation of Information Processing (IFIP) working groups relating to Information Management Identity Management and Information Security Education. Dr Clarke is the co-chair of an innovative new symposium series on the Human Aspects of Information Security & Awareness (HAISA).