Acceptance of subscriber authentication methods for mobile telephony devices

N.L.Clarke, S.M.Furnell, P.M.Rodwell and P.L.Reynolds

Abstract

Mobile phones are now an accepted part of everyday life, with users becoming more reliant on the services that they can provide. In the vast majority of systems, the only security to prevent unauthorised use of the handset is a four digit Personal Identification Number (PIN). This paper presents the findings of a survey into the opinions of subscribers regarding the need for security in mobile devices, their use of current methods, and their attitudes towards alternative approaches that could be employed in the future. It is concluded that, although the need for security is understood and appreciated, the current PIN-based approach is under-utilised and can, therefore, be considered to provide inadequate protection in many cases. Surveyed users responded positively towards alternative methods of authentication, such as fingerprint scanning and voice verification. Based upon these findings, the paper concludes that a non-intrusive, and possibly hybrid, method of authentication (using a combination of techniques) would best satisfy the needs of future subscribers.

Keywords

Authentication, Mobile, GSM, UMTS, Biometrics.

Introduction

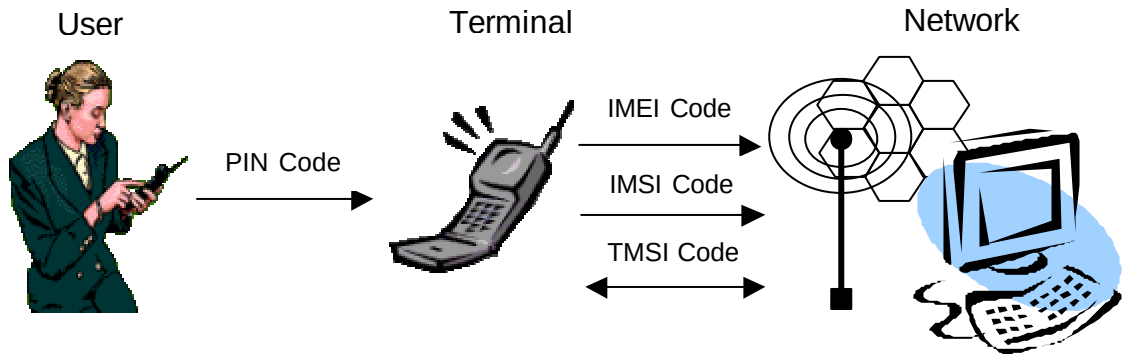
The mobile phone market has witnessed phenomenal growth in recent years, such that the phone itself is now regarded as an essential everyday item by millions of people. Indeed, cellular subscribers currently total around 479.5 million worldwide, a 56.87% growth on the previous year, with forecasts for the end of 2003 estimating that the number of subscribers will be in the region of 1.073 billion [1].

In addition to increasing subscribers, the capabilities of the phones themselves will also improve. With the introduction of third generation mobile devices, part of the ITU IMT-2000 initiative [2], a broadband service of up to 2Mbps will be on offer, providing the potential for true multimedia services [3]. As the technology advances, the range of potential services also expands. Whereas the first generation analogue phones of the 1980s were purely aimed at the provision of voice telephony services, the arrival of second generation (digital) phones in the early 1990s ushered in basic data services such as SMS (Short Message Service) text messaging. In more recent years, devices supporting the Wireless Application Protocol (WAP) have facilitated limited Internet access, and the emergence of faster access technologies, such as GPRS (General Packet Radio Service) and UMTS (Universal Mobile Telecommunications System), will hasten the convergence of the mobile phone with Personal Digital Assistant (PDA) devices. This, in turn, will significantly increase the range of in-built and network-based applications of the device, thus also increasing the range of potentially sensitive and private information that the devices will hold.

As the sensitivity of information stored on a mobile device increases, the need for effective security also increases. The 3rd Generation Partnership Project (3GPP), who provide the technical specifications and regulations for UMTS, have recognised the need for secure data communications and produced appropriate standards [4]. However, security over the air interface is only one aspect of the problem, and it is also important to ensure appropriate protection of the device against unauthorised access. Current mobile handsets do incorporate some level of protection in this respect, but it is fairly rudimentary, and as the need for security increases there is the potential to incorporate more advanced methods. At this stage, however, questions remain about the security measures that customers would expect, and tolerate, to protect their personal information. This paper considers the need for security on mobile handsets, end-user attitudes towards current authentication measures, and their views in relation to future service opportunities and the consequent security requirements that these will impose.

Subscriber authentication in mobile systems

At the time of writing, the dominant mobile network standard is GSM (Global System for Mobile communications), which accounts for 63% of the global cellular market [1]. The authentication security that the GSM networks currently provide is focused between the terminal devices and the network, as shown in Figure 1, with a number of checks being made to ensure that the handset is permitted to use the network, has not been reported stolen etc. By contrast, the security between the terminal and the subscriber is currently quite rudimentary, with subscriber authentication based upon the use of a Personal Identification Number (PIN).



PIN – Personal Identification Number
IMEI – International Mobile Equipment Identifier
IMSI – International Mobile Subscriber Identifier
TMSI – Temporary Mobile Subscriber Identifier

Figure 1 : User - Terminal – Network Security Processes

For the majority of mobile phones, the PIN is the only form of authentication required in order for a user to be able to access the device. The authentication process will typically only allow the user to enter the number incorrectly a finite number of times (typically three) before the Subscriber Identity Module (SIM) within the phone becomes locked and requires a special

unlock password (PUK) from the network service provider. In this way, brute force attacks on the PIN code (where every combination is systematically tried) are avoided. However, the security here assumes two things: firstly, that the PIN facility is activated, and secondly, that the user has not compromised its protection (e.g. by not changing it from the factory default, by writing it down, or by telling someone else) in the many that frequently occurs with other knowledge-based authentication approaches, such as passwords [5].

If the PIN facility is enabled, it may (depending on the make/model of phone) provide two levels of authentication. All phones can be configured to request the PIN when they are switched on (normally only allowing emergency calls in its absence). Some models also allow locking of the keypad when switched on, requiring PIN re-entry before each use. As such, the PIN is capable of providing protection, and to date it has generally been regarded as providing sufficient security, given that the information held on the devices is relatively limited (e.g. telephone numbers, simple text messages, etc.), and thus of little value to a thief. Therefore the main threat comes through unauthorised usage of the phone, which only exists in a finite window before the phone is reported stolen and subsequently disabled by the network operator. Recently, with the advent of WAP-enabled second-generation phones, there has been a movement towards the storage of more sensitive material. For example, some handsets contain a credit card reader that is able to make transactions over WAP-enabled web sites. Although this still requires a PIN identification before use, it does pose the question of how far we can rely on PIN codes, how secure they are, and how secure users believe them to be.

Whereas PIN-based authentication relies on something the user *knows*, an alternative method is authentication via something the user *is*, a domain more commonly referred to as biometrics. There are two categories of biometric authentication [6]:

- Physiological biometrics, based upon bodily characteristics (e.g. fingerprint analysis, facial recognition, iris scanning and ear geometry).

- Behavioural biometrics, based upon the way people do things (e.g. voice print, typing style).

Much research has gone into developing these techniques into practical systems, and they are already employed as alternative authentication methods in desktop PC environments - for example, 9% of the respondents to the 2001 CSI/FBI Computer Crime and Security Survey claimed to use biometric security technologies [7]. In addition, there is already evidence of their application within the mobile domain. The Sagem MC959 handset, for example, incorporates a fingerprint recognition system into the back panel [8]. When considering the application of biometrics, in the context of mobile handsets, appropriate thought needs to be given to the practicality of the technique. It is noticeable, for example, that physiological techniques generally require additional hardware, such as the fingerprint scanner, to be added, whereas behavioural techniques do not. Implementation of behavioural techniques can be achieved through software only. Clearly, for mass-market devices, component cost is a major consideration, and handset prices are already subsided by network operators in many countries in order to keep the cost down for the consumer. However another major consideration to take into account is how the subscribers actually feel about security. Customers in today's world dictate the success or failure of a product, so their attitudes and opinions are important factors to take into consideration.

A survey of subscriber attitudes towards mobile security

A survey was conducted to assess the attitudes and opinions of current mobile subscribers towards authentication on their phones. To this end, a questionnaire was devised that assessed the following aspects:

- how the phone is used (e.g. voice communications, text messages etc.) and how subscribers would like to use their phones in the future. This gauges the level to which additional security is necessary - if the phone is used purely for voice communications then the need for increasing security is questionable.
- users opinions about the current form of authentication, the PIN.
- whether users believe there is a need for increasing security, and if so how would they like to see a solution implemented.

The survey was distributed as hard copies to a wide range of people, with one proviso – in order to be able to offer a valid opinion, the respondents had to be current or past users of mobile phones. A total of 138 paper-based copies where returned. An on-line version was also created, achieving another 23 responses. Thus, a final total of 161 responses were obtained, and the results are analysed in the sections that follow.

General

The survey was not aimed at any specific age group or gender, the hope being to obtain a good cross section of users. As shown in Figure 2 below, 53.5% of respondents were in the 17-24 age group. Although at first glance this figure does not suggest a particularly representative sample, it is actually a fair reflection of mobile phone ownership in the UK, where the survey was focused. Recent market research studies have illustrated that teenagers now account for a significant proportion of phone purchases, particular in relation to pre-pay phone options [9]. With this in mind, the predominance of younger respondents in this study is less surprising, and serves to make the results a more accurate reflection of typical subscriber attitudes.

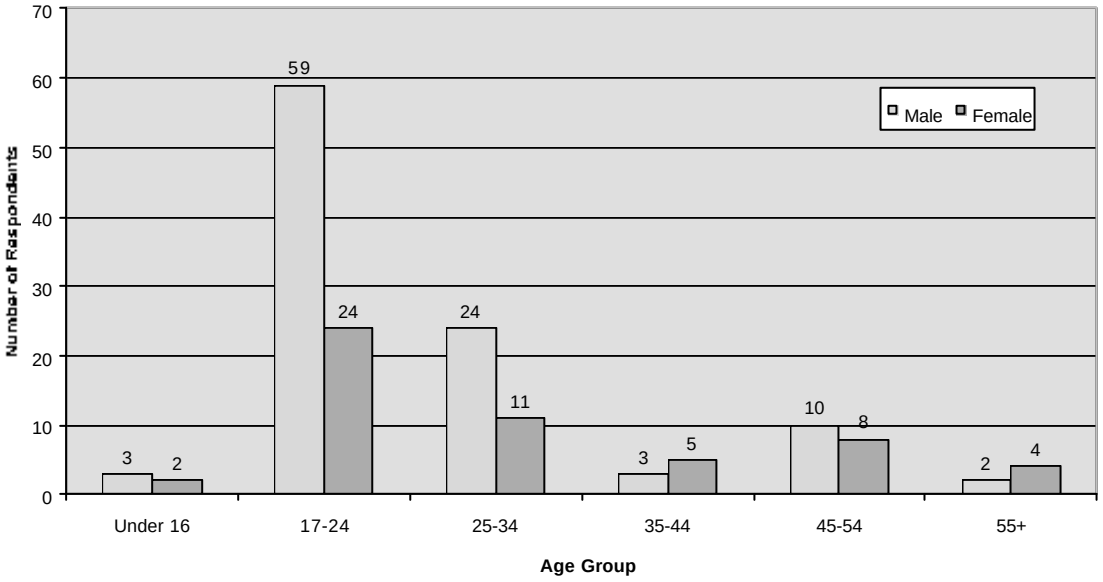


Figure 2 : Gender and age split in the respondent group

The desire to remain contactable is apparent from how long respondents leave their handsets switched on. 57% of those questioned said they kept their phone switched on for greater than ten hours a day, with 19% claiming between six and ten hours, and the percentage descending in order to 11% for less than one hour a day. These findings have a couple of implications:

- The need to leave the phone on comes in part from the need to stay in touch. So is the mobile phone the users principle means of doing this? Those switching on for less than one hour are likely to be users who only switch on when they wish to use the phone themselves. Thus either do not wish to be kept in contact with or have another principle means of communication, for instance a landline phone. Those leaving their phones on for a long period of time are likely to consider their phones to be there major means of contact, showing a possible long-term commitment towards the use of mobile phones.

- With the large number of respondents leaving their phone on, this could have implications for security, especially those who do not have or do not use a PIN facility to lock their keypad on standby.

Different phone manufacturer's, although providing a range of different phones, often keep the same software functionality, i.e. Nokia and its proprietary menu system. Nokia and Motorola's use of the PIN is no different in principle. However, whereas Motorola provides the facility to lock the keypad whilst on standby, Nokia however does not. In this particular sample, 57% of respondents are Nokia owners, of whom 96% leave their phone on for more than one hour a day, and 87% leave it on for more than six hours a day. This results in a significant number of unlocked phones on stand-by mode for long periods of time every day, leaving them with effectively no defence from un-authorised use if lost or accidentally left unattended.

Mobile phone usage - present and future

Unsurprisingly, results indicate that the vast majority use their mobile phone for talking. More interestingly, however, 90% of respondents regularly use text messages as a means of communication. Figure 3 illustrates these findings, in addition to responses for a range of other current services. The other services are newer, and from the responses have not been adopted as widely at present. A possible discrepancy in the data exists surrounding the use of the email service. Although this service is currently available on only a small proportion of handsets, 64% responded 'yes' or 'no' to the question of whether they used the facility. It is considered likely that many respondents who answered 'no' were doing so because their phone does not offer them the option (and, therefore, they should ideally have selected the 'not available' option on the questionnaire). This hypothesis also applies to the use of WAP services. However, it is valid to note the proportion of users that do use their phone for WAP and email services stands at 6% and 9% respectively, indicating an emerging acceptance and use of advanced data services.

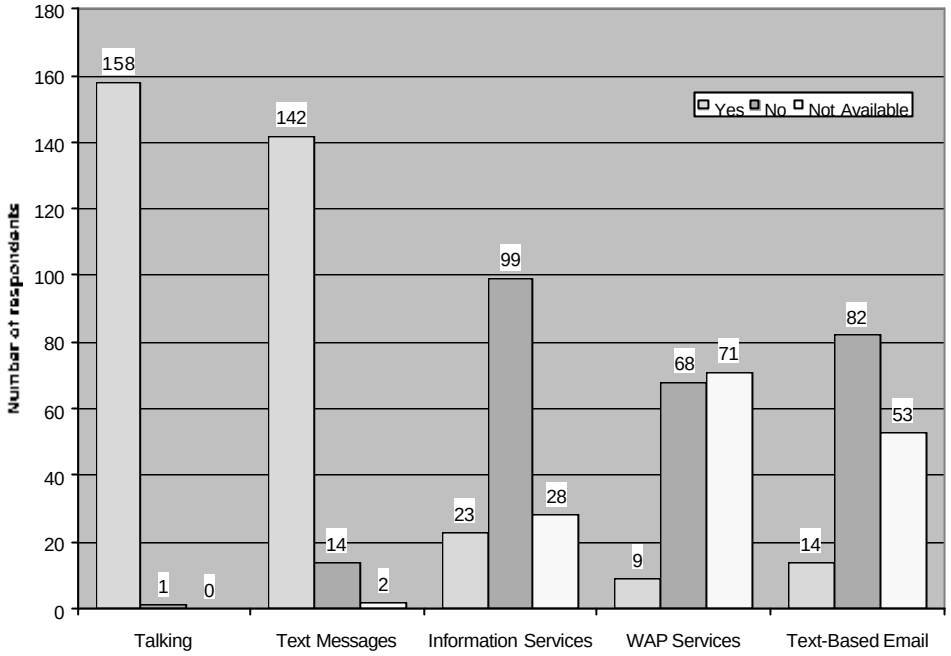


Figure 3 : Services used by respondents

Respondents were also asked whether they would consider using a small range of other services that are likely to be offered by future mobile handsets. The questionnaire specifically suggested the options 'video conferencing', 'online shopping', 'World Wide Web', 'Downloading music' and 'Personal Organiser', as well as offering respondents the option to suggest other ideas that would interest them. The results strongly suggested that the adoption of advanced mobile service is likely to continue, with 40% looking to use video conferencing, 43% interested in online shopping, 58% desiring mobile web access, 53% wishing to download music, and 73% wanting an integrated personal organiser. Although the latter would not necessarily involve communication between phones and the network, the data stored in personal organisers could well contain sensitive information such as bank account details etc. The additional services that were suggested by respondents included 'digital money', 'radio', and 'global positioning system' – all of which are very likely to emerge in combination with telephony handsets. Overall, it is also worth noticing that 88% of respondents did want to use some form of additional service.

Usefulness of current security

As previously discussed, the primary method of user authentication for mobile phones is the PIN, which is able to provide up to two levels of security. Although 89% of respondents knew about the PIN facility, only 56% of them use it in either form. The survey shows that 76% of respondents had phones with only one level of security (at power on). Of those users that did have both levels of security, only 46% of them used the second level on a regularly basis. Asking whether the respondents feel entering a PIN number is inconvenient, 41% responded 'yes' with the same percentage also expressing doubts about the level of protection the PIN can provide. Although the results are not conclusive enough to put an argument for or against the usefulness of the PIN facility, there are a number of significant points that can be drawn from the data:

- 11% of respondents did not know about the PIN facility. On the face of it, this is a relatively small percentage, but on a worldwide scale that accounts for 52.8 million subscribers who do not even know that security is available.

- Of the 44% of respondents who do not use the PIN facility, 65% of them considered it to be inconvenient, thus suggesting a good reason why they do not use it.

- Providing additional levels of security does not necessarily provide the user with additional protection if s/he does not use it through inconvenience. 64% of respondents for whom the ability to PIN-protect the phone between calls is available, still do not use the facility because they find entering the PIN inconvenient.

- A significant proportion of respondents, 41% do not have confidence in the protection the PIN facility provides, indicating users believe their phone is still at risk from misuse even if the PIN facility is in use.

- 52% of female respondents do not use the PIN facility compared to 39% of males.

The survey also asked respondents to comment about issues relating to the compromise of security. When asked to consider compromise by another party, only 11% of users believed that their phone had been used without their permission. The real percentage is likely to be higher, from misuse that has gone undetected. For instance people who may use the phone briefly without the owner's knowledge. Those respondents who answered positively to this question are likely to have had their phone stolen, and thus detected the misuse. The questions also considered compromise of protection arising from the subscribers' own actions. There are several ways in which subscribers may invalidate the PIN security, such as revealing the number to someone else, forgetting it, or writing it down. Table 2 presents a summary of the findings here.

	Yes (%)	No (%)
Forgotten It	17	83
Told Someone Else	26	74
Taken a Written Note Of It	6	94

Table 2 : Respondents who invalidate their PIN protection

Attitudes towards future authentication options

With mobile handset manufacturers and network operators both aiming to provide users with additional services, the need for security is likely to increase. This survey has identified that users are already using data services, and are willing to use future services as and when they become available. It is an encouraging sign that the respondents also recognise the need for security, with 81% believing it would be either good or very good to have more security. Only two respondents thought it would be bad idea. This recognition shows that users are aware of the need for security, and are also possibly worried about their current level of protection. Interestingly, however, the desire for more security shows a downward trend as the respondents' age increases, as shown in Table 3.

Age Group	Responded positively to additional security (%).
Under 16	100
17-24	89
25-34	72
35-44	66
45-54	68
55 or older	42

Table 3 : Respondents opinions on having additional security

Having established that respondents were generally accepting of additional authentication measures, the survey proceeded to assess their preferences for the forms that it could take. Having determined that PIN-based protection is problematic, it is considered that other authentication methods based upon something the user *knows* (e.g. passwords) would be equally under-utilised or inconvenient. The implication of this is that the most sensible route for improving authentication is to base the approach upon a biometric technique (the other option for authentication, basing it upon something the user *has*, is likely to offer little advantage, as the phone itself is something the user has, and any supplementary authentication token would be likely to be kept with the device). With this in mind, the survey respondents were presented with a range of biometric authentication options and asked to indicate which of them would be preferable to the PIN. The biometrics offered as options were as follows: fingerprint recognition, voice print recognition, ear geometry, facial recognition, iris scanning, and typing style All of these techniques have been the focus of previous research, and some are already widely recognised as commercial products in the domains of physical access control and desktop computing [10]. Techniques such as ear geometry (in which the subscriber would be identified by the physical shape of their ear) and typing style (in which authentication would be based upon characteristic inter-keystroke latencies observed when subscribers dial numbers or otherwise interact with the keypad) are less recognised in the marketplace, but are considered particularly suited to non-intrusive application in a telephony context. The respondents' opinions in relation to the techniques are illustrated in Figure 4.

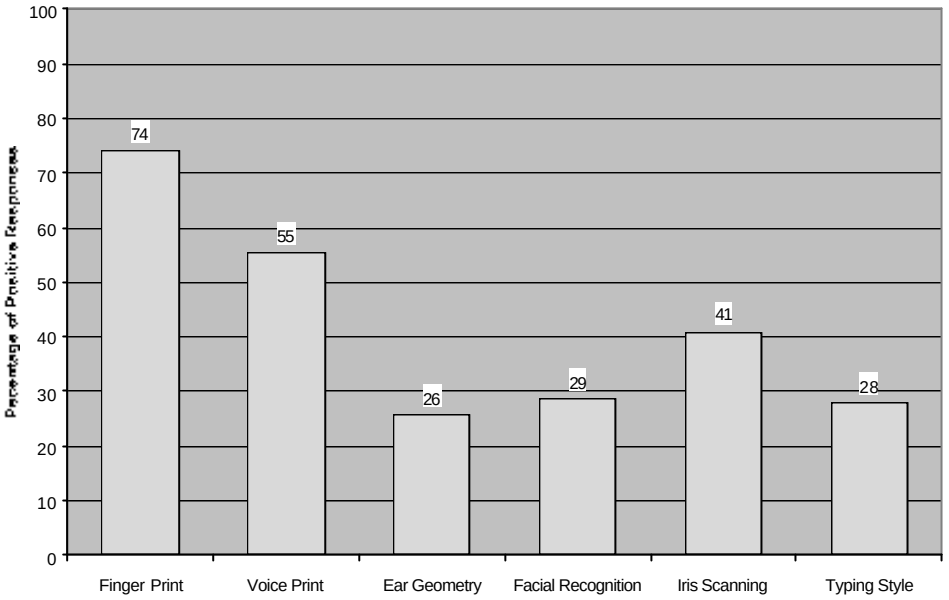


Figure 4 : Positive responses to biometric authentication techniques

The results showed a strong preference towards fingerprint analysis, with approximately three quarters of the respondents selecting this option. Voice print analysis and iris scanning also achieved good scores, albeit significantly lower than fingerprint analysis in both cases. The remaining three techniques were demonstrably less popular, appealing to just over a quarter of respondents in each case. However, any conclusions drawn from these results should be tempered with the observation that the respondents are likely to have responded most positively to those ideas that they have already heard of. Fingerprints have long been known to provide a means of successfully identifying people, and indeed such techniques are already being used in mobile phones. Voice print analysis has also attracted much attention through the media, computer software applications, and also in the phone industry (albeit in the context of voice recognition for dialling numbers, rather than as a means of authentication). It is also fairly easy to understand this authentication technique, as people generally sound different. Techniques such as ear geometry and typing style are newer, and less information is known about them. Although keystroke analysis techniques have been extensively researched for use in PC-based authentication [11,12], it is not a widely advertised or used technique. As for ear geometry, although it is not very difficult to imagine how this technique might possibly work, there are no current implementations on the general market, and knowledge about this technique would, therefore, have been very limited amongst the respondents.

The point, therefore, is not to regard the results as a conclusive attitude towards one technique over another. The key observation that can be made is that all techniques were (to some degree) considered favourably, and that if a technique were to be implemented that was less known about generally, a degree of education and awareness before wide scale adoption.

One advantage of certain biometrics when compared to the PIN is that they offer the potential for authentication to be performed on a continual basis rather than as a one-off judgement. Respondents were, therefore, asked whether they would consider continuous authentication during a call to be acceptable. The results revealed that 41% of respondents considered continuous authentication during a call to be a good idea, while 24% were against the idea, and 35% were indifferent to the idea. However, the actual number of users willing to break

during their call to authenticate themselves is likely to be low, which implies that any continuous authentication method implemented would have to be non-intrusive (without explicit action by the user). Certain authentication techniques will clearly lend themselves to this better than others, for instance voiceprint, as the user would be talking on the phone already. Techniques such as keystroke analysis would not typically be viable during a traditional voice call, but could potentially provide a measure of authentication as each call is initiated, or during the conduct of keypad-oriented, non-voice sessions.

For all authentication techniques, including the PIN, some information needs to be stored so that a comparison is possible with the input data. The final objective of the survey was to establish users opinions on where this profile should be stored – on the phone or in the network. The advantage of storing the profile on the phone is that authentication can then occur completely on the phone, with the result that no personal details are communicated to and from the network, and the network traffic overhead is minimised. However, the disadvantage is that the user is then restricted to being authenticated on the one phone. By having profile information stored on the network, users would be able to login at any network access point, thus enhancing their personal mobility. It would also enable the network operator to monitor the success or failure rates for possible misuse. Where a preference was expressed, the opinions from the survey respondents clearly favoured the profile being held in the handset, with 52% of respondents selecting this option. By contrast, 26% favoured the network, while 20% did not mind and 2% did not understand the question. Given that the respondents were probably not be giving much thought to the issue of the network overheard, it is likely that their preference for the handset-based profile relates to the ability to retain control over their own profile data.

Discussion

Although the results have suggested the desire for a greater level of security, this clearly represents something of a contradiction when it is considered alongside the fact that many respondents do not even use the current method that has been provided for them. This suggests that it is the security technique, rather than the concept of security, that users are rejecting, and as such a move towards non-intrusive methods of authentication may provide the protection that users are looking for, but without the associated inconvenience that is currently perceived. Although fingerprint scanning was a favourite technique, it does not necessarily lend itself to non-intrusive implementation, as the user would need to place his/her finger on the scanner. If the scanner were to be placed in a natural area on the phone where a finger would normally be placed to hold the device, then the level of intrusiveness would be arguable. Voiceprint lends itself to both one-off and continuous monitoring of voice communications, but would either lose its non-intrusiveness, or the ability to authenticate, on data communications. Keystroke analysis also lends itself to non-intrusive authentication for one-off monitoring and would be more likely to facilitate continuous monitoring during the utilisation of keypad-oriented services.

Since none of the biometrics discussed can provide non-intrusive authentication for all possible scenarios, and secondly cannot provide 0% false acceptance and false rejection rates, it would seem logical to provide a hybrid model of authentication, using a number of non-intrusive methods as first/second line security, with the PIN (or some other knowledge-based methods) providing a fallback method if needed. Current research is focusing upon the realisation and evaluation of such an approach, and the authors are investigating the application of biometrics in this context. A preliminary investigation of keystroke analysis

has been conducted to assess whether it is possible to authenticate people from the way in which they dial numbers on a standard GSM handset. Although the results are not conclusive at this stage (with false acceptance and false rejection errors of around 15% being observed), it is considered that refinement of the technique may yield better performance. The full results from this element of the investigation will be published in due course.

Conclusions

The survey findings have indicated a weakness of the current security provisions on mobile handsets, in that the authentication technology is optional and, therefore, not used by a large proportion of users. However, subscribers have shown both the need and the desire for additonal security, and have responded positively towards a number of alternative authentication techniques. At the same time, the results showed that many respondents do not use the current security techniques that are available to them. In view of this, it can be assumed that a non-intrusive method of authentication may prove to be most acceptable and widely utilised by end users.

With the introduction of the third generation phones, a range of new services will become available from mobile devices – services that the respondents in the survey indicated that they would be keen to use. In this context, the protection of users' information must become a prime concern, especially when considering the possible sensitivity of the data, and the need for a sucessful transition into a multi-billion dollar m-commerce market. Security is, therefore, essential, and approaches must be employed that subscribers will tolerate and use.

References

[1] Intekom. 2001. *Latest Global & Regional Cellular Statistics*. http://home.intekom.com

[2] ITU. 2001. Full description of the IMT-2000 (International Mobile Telecommunications) initiative located on the ITU (International Telecommunications Union) website at www.itu.int, Radio-Communication (ITU-R) division.

[3] UMTS Forum. 1998. *The Path towards UMTS – Technologies for the Information Society.* Report no. 2. The UMTS Forum. http://www.umts-forum.org/reports.html

[4] 3GPP. 2000. *Terms of Reference: Services and System Aspects – Working Group 3.* TSG SA WG3 – Security. http://www.3gpp.org/TSG/ToR/TSG-SA/sa3-tor.htm

[5] Jobusch, D.L. and Oldehoeft, A.E. 1989. "A Survey of Password Mechanisms: 1", *Computers & Security*, Vol. 8, No. 7: 587-604.

[6] Cope, B.J.B. 1990. "Biometric Systems of Access Control". *Electrotechnology*, April/May: 71-74.

[7] CSI. 2001. '2001 CSI/FBI Computer Crime and Security Survey', *Computer Security Issues & Trends*, vol. VII, no. 1. Computer Security Institute. Spring 2001.

[8] SAGEM. 2000. “SAGEM points a finger at GSM”, Press Release, 24 January 2000. http://www.sagem.com/en/communiques-en/cp-1sem2000-en.htm#mc 959 id empreinte

[9] Miller, S. 2001. “Mobile sales soar, driven by teenage market”, MediaGuardian report, 23 May 2001. http://media.guardian.co.uk/newmedia/story/0,7496,495263,00.html.

[10] Polemi, D. 1997. *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable,* Institute of Communication and Computer Systems, National Technical University of Athens. April 1997.

[11] Legget, J. and Williams, G. 1988. “Verifying identity via keystroke characteristics”, International Journal of Man-Machine Studies, 28.

[12] Joyce, R. and Gupta, G. 1990. “Identity Authentication Based on Keystroke Latencies”, Communications of the ACM, Volume 33, February 1990.