Biometric Authentication for Mobile Devices

N.L. Clarke[1], S.M. Furnell[1] & P.L. Reynolds[2]

[1]*Network Research Group*
Department of Communication & Electronic Engineering
University of Plymouth, Plymouth
United Kingdom
Email: info@network-research-group.com

[2]*Orange Personal Communications Services Ltd*
Bradley Stoke, Bristol
United Kingdom

ABSTRACT

Mobile devices have found an important place in modern society, with hundreds of millions currently in use. The majority of these use inherently weak authentication mechanisms, based upon passwords and PINs, which can potentially be compromised and thereby allow attackers access to the device and its stored data. A need for stronger authentication is identified and the discussion considers the application of various biometrics to a mobile platform. The feasibility of one such approach, that of keystroke dynamics, is examined, revealing promising results – with individual performances of 0% false rejection rate and 1.3% false acceptance rate being observed. However, higher overall error rates of 15% lead to the proposal of a hybrid, non-intrusive approach to authentication.

Keywords: Mobile Devices, Authentication, Biometrics

INTRODUCTION

The ability to communicate and work whilst on the move has given rise to an explosive growth in mobile devices. Primarily this growth has come out of mobile phone related technologies with worldwide subscribers now in excess of a billion (UMTS Forum, 2002), but it can also be seen that both the use of Personal Desktop Assistants (PDA's), and laptop computers has been growing with popularity (Richardson, 2002; Gibson, 2001). However, this rise in computing mobility could cause a number of security issues, in particular with attackers accessing the data stored on the devices.

The most popular access security to date takes the form of the password or PIN (Personal Identification Number), a secret-knowledge approach that relies heavily on the user to ensure continued validity. For example, the user should not use the default factory settings, tell other people, or write it down. However the poor use of passwords and PINs has been widely documented, with many laptops owners using simple passwords that dictionary attacks can crack in seconds and with many mobile phones and PDA users not even using the security available. Recent surveys have indicated that 44% of mobile phone users do not use the PIN and 25% of PDA users do not a password (Clarke et al., 2002a; Leyden, 2002). Taking a crude comparison with current mobile phone subscribers, this would indicate that some 500 million mobile phones have no access security. Although this is not a particular issue currently with the second generation mobile phones with their

limited storage and computing abilities, this will change with the advent of third generation networks and a convergence of PDA and mobile phone functionality (Giussani, 2001). Mobile phones will be able to store detailed information about friends and family, include digital certificates, bank details and be able to access a wide range of data services through your phone account – ranging from the purchasing of goods to watching movies. Interestingly the same mobile phone survey found that, in contradiction to not using the protection already available with 41% of respondents citing inconvenience, that 81% of respondents wanted more security.

So an alternative means of subscriber authentication is required to replace the secret-knowledge based approaches. It is therefore appropriate to examine the potential of a fundamentally different strategy. From the available techniques, that of token-based authentication and biometric based authentication, only the latter really seems plausible, since tokens would also have to be carried with you along with the device or more commonly left permanently in situ. Biometrics, are based not on what the user *knows*, or what they carry, but who the user *is*, some unique characteristic. After explaining the biometric concept in more detail, this paper considers the techniques that could potentially be deployed on mobile devices, along with a brief example of a practical implementation.

THE NEED FOR AUTHENTICATION ON MOBILE DEVICES

As previously indicated, a large number of mobile devices are currently in use with little or no authentication security. A recent survey into the use of PDAs discovered a third of users who have already had their PDA stolen once still do not use a password, however, one of the cited uses for a PDA by respondents was to store all the passwords and PINs they regularly use for other systems (Leyden, 2002). This highlights two primary issues; firstly, the inherent weaknesses of secret-knowledge based techniques such as the password in that they can be written down in the first place, and secondly the importance of the data being stored on the device. There is a third issue raised concerning user perception and realisation of the security problems. Any person storing sensitive information on a device without securing that device clearly has little comprehension of the associated security issues.

The security weaknesses and threats associated with PDAs are important because although the number of devices currently in use is relatively small (in the order of tens of millions), the mobile phone is set to absorb and surpass much of the functionality of current PDA devices. The difference in numbers is from tens of millions of PDAs to hundreds of millions of mobile phones. If authentication mechanisms were left as they currently stand, then the threat posed by attackers would inconvenience users through cost associated with misuse and an almost certain increase in the theft of the devices. For example, the UK Home Office reported some 700,000 mobile phone thefts from subscribers in 2001 and this number can only be set to increase as mobile phones are packed with more technological wizardry (Harrington et al, 2001).

Concerns can also be expressed in relation to laptop computers. For example, the UK Ministry of Defence (MoD) admitted to losing over 600 laptops over a five year period (BBC, 2002), many obviously containing very sensitive information. Although it is likely that many laptops are stolen merely to be resold as a piece of equipment, rather than for the information stored upon them, this cannot be the case it all thefts. Infosecurity reported in May 1999, that 57% of computer crimes involving break-ins on corporate servers were linked to stolen laptops that enabled the breach (Broomfield, 2000).

BIOMETRIC APPROACHES & IMPLEMENTATION

The use of biometrics has existed for hundreds of years in one form or another, whether it is a physical description of a person or perhaps more recently a photograph. Consider for a moment what it is that

actually allows you to recognise a friend in the street or allows you to recognise a family member over the phone. Typically this would be their face and voice respectively, both of which are biometrics. Biometrics are based on unique characteristics of a person, and are typically subdivided into two categories, physiological and behavioural. Physiological biometrics are those based on classifying the person according to some physical attribute, such as their fingerprints, their face and their hand. Behavioural biometrics rely on a unique behaviour of the person such as, their voice and the way in which they write their signature.

Biometrics all work on the basis of comparing the biometric sample against a known template, which is securely acquisitioned from the user when he or she enrolled on the system initially. However this template matching process gives rise to a characteristic performance plot between the two main error rates governing biometrics. The False Acceptance Rate (FAR), or rate at which an impostor is accepted by the system, and the False Rejection Rate (FRR), or rate at which the authorised user is rejected from the system. The error rates share a mutually exclusive relationship as one error rate decreases, the other tends to increase, giving rise to a situation where neither of the error rates are typically both at zero percent (Cope, 1990). Figure 1 illustrates an example of this relationship.

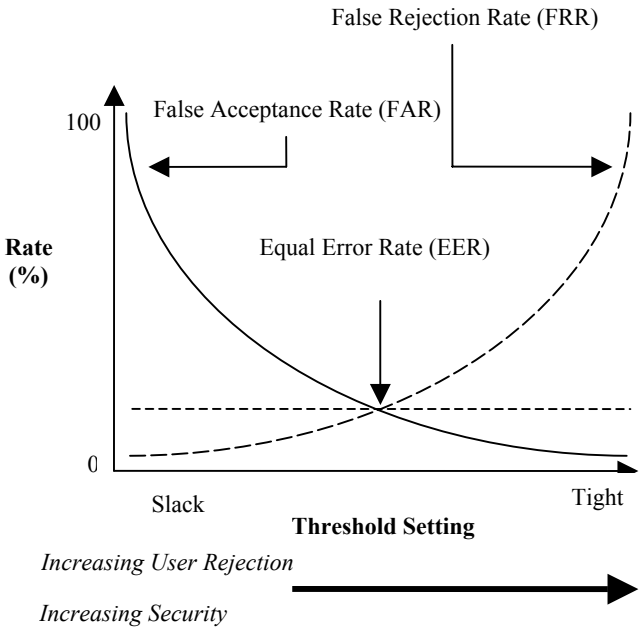


Figure 1 Mutually exclusive relationship between the False Acceptance & False Rejection Rates

This leads to a trade-off situation between high security and low user acceptance (due to fact the authorised user is being rejected a large proportion of the time) and low security and high user acceptance, to which a decision has to made about what threshold setting to set that meets both the security requirements of the device and acceptance levels of users. The point at which the error rates cross is called the Equal Error Rate and is used in industry as a comparative measure between different biometric approaches (Ashbourn, 2000).

The next section provides an overview to the most common biometrics that could be implemented within a mobile terminal, indicating what the unique characteristic the technique attempts to classify users upon and how the biometric is obtained. For more general information on any of the approaches discussed here, consult Nanavati et al. (2002) and Smith (2001).

PHYSIOLOGICAL BIOMETRIC

- Fingerprint Recognition

The most commonly deployed biometric, with a mature and proven technology. The fingerprint comprises of ridges and valleys that form distinctive patterns, such as loops, swirls and arches. The ridges and valleys are characterised by discontinuous and irregularities known as *minutiae* – these are the distinctive features on which most fingerprint technologies are based. In order for the fingerprint image to be captured a specialist reader is required

.

- Facial Recognition

This utilises the distinctive features of the human face in order to authenticate a user. The features often used are those which change very little over time, such as the upper ridges of the eye sockets, areas around the cheekbones, sides of the mouth, nose shape and the relative position of these features relative to each other. The facial image itself can be generated from any static camera or video system that is able to generate image of sufficient quality, such as web camera.

- Iris Scanning

Iris scan technology works by utilising the distinctive features of the human iris and has the potential to be one of the most successful biometrics (Harrison, 2001). Iris recognition requires the acquisition of a high-resolution image of the eye, illuminated by an infrared imager, in order to effectively map the details of the iris. The device to capture this image can vary from a desktop camera to a dedicated camera for integration into physical access units. The main distinctive feature used for authentication is known as the *trabecular meshwork*, although other features are also used, such as furrows, freckles and the corona.

BEHAVIOURAL BIOMETRICS

- Voiceprint Recognition

Voiceprint recognition as the name would imply authenticates person by their vocal characteristics. The authentication can in principle be achieved both text dependently – where the user speaks a predefined word or sentence – and text independently where authentication is not dependent on the word(s) you speak, although, the latter is obviously a more difficult task to achieve successfully. Voiceprint recognition is similar to facial recognition and keystroke dynamics it that it can leverage existing hardware on the device, although some manufacturers do specify or provide a particular microphone that is calibrated with its authentication algorithm.

- Signature Recognition

This is achieved through using the distinctive aspects of a human signature to authenticate users. There are two underlying processes to signature recognition – static – where the completed signature is compared to a template version and authentication is given dependent on the comparison, or more comprehensively – dynamically – where behavioural components such as the speed, pressure and stroke order are also taken into account, hence making it less susceptible to forgery. The majority of signature-scan systems therefore use an electronic tablet that can record the dynamics of writing.

- Keystroke Dynamics

Keystroke dynamics is a technique that authenticates a person by the way in which they type on keyboards/keypads. The typical distinguishing characteristic is the latency between successive keystrokes. Similar to signature recognition, keystroke dynamics can be achieved using static and dynamic approaches, with the former being the easier. Static authentication involves the user entering a predefined keyword such as their username/password, whereas dynamic authentication is text

independent and will authenticate a user given any sequence of text. Since no additional hardware is required this has been a favoured technique, with much research on the subject since the 1980's (Gaines, 1980) but the performance of such a technique is comparatively weak against fingerprint and facial recognition systems, with currently only one commercially available product based on the static mode of authentication (Biopassword, 2002).

- Service Utilisation

This technique is achieved by monitoring the distinctive way in which a person interacts with a device. Measured factors could include the time and type of calls dialled (long distance, local, premium rate numbers for instance), SMS text messages sent to whom and when, and web pages visited over a period of time. The longer the period the more precise the technique becomes. The unique pattern(s) in a person's behaviour can be identified using a branch of artificial intelligence referred to as data mining (Singh et al., 2001). This is a comparatively new method of behavioural biometric and consequently has no commercial product to date.

The survey by Clarke et al. (2002a) also indicated that users wanted more security for their current second generation phones which in itself indicates user's awareness of security issues, and were prepared to use biometrics to achieve the desired level of security. Figure 2 illustrates user's responses towards some of the techniques previously described, considering their application to a mobile phone environment.

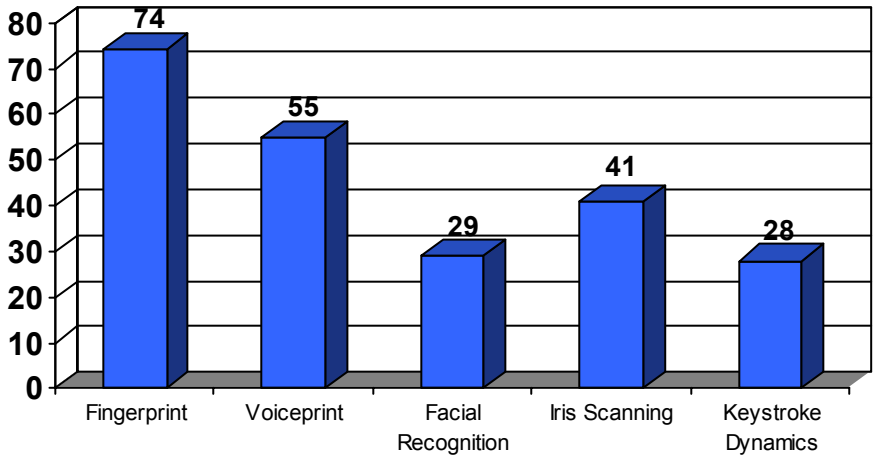


Figure 2 User's Biometric Preferences

The extent to which the biometrics previously described can be used within a mobile terminal device depends largely on the available hardware. It is unlikely, due mainly to cost, that many users will be willing to buy the additional hardware unless there are other real tangible benefits to be gained, such as a camera –which can be used for facial recognition but also take holiday pictures for instance. The only time where it would be conceivable for additional security-specific hardware purchases would be when the cost associated with the hardware is relatively small in comparison to the device to which it is protecting. This is likely to discount mobile handsets and PDAs as they are not likely to be expensive enough, but perhaps not laptops, where the upper boundary resides around $3700 ($6600 AUD). Otherwise it can be generally held true that the only biometric approaches available are those that can be easily (and cheaply) implemented on current devices. Typical biometric approaches that can be implemented on current mobile devices are given in table 1. This is by no means a definitive list as many devices differ in their hardware specifications. For instance some Acer laptops now have fingerprint recognition built into the system (Thornton, 2001) and some PDAs do not currently have the expandability to include a camera.

Mobile Phone	PDA	Laptop
➢ Voice Recognition via in-built microphone ➢ Keystroke Dynamics via scaled-down keyboard ➢ Facial Recognition via add-on or built-in camera ➢ Iris Recognition via add-on or built-in camera	➢ Voice Recognition via in-built microphone ➢ Facial Recognition via add-on camera ➢ Iris Recognition via add-on camera ➢ Signature Recognition via touch sensitive display	➢ Keystroke Dynamics via keyboard ➢ Fingerprint Scanner (via optional PCMCIA slot) ➢ Facial Recognition via in-built camera ➢ Iris Recognition via in-built camera

Table 1 Applicable Biometric for Mobile Devices

MOBILE BIOMETRICS IN PRACTICE

Keystroke dynamics is of particular interest as the approach has a number of advantages over other biometrics that make it useful as an authentication technique for mobile devices, mainly, the lack of additional hardware required and the ability to implement a solution completely transparently to the user, therefore resolving any issues of user inconvenience (the issues of convenience and intrusiveness are discussed in the following section). Although it is recognised that many PDAs do not have keyboards or keypads, a general market trend of late has seen the introduction of either add-on keyboards or scaled down versions (HP, 2002; HandSpring, 2002) to which keystroke dynamics can be applied. Of course no single biometric approach will encompass all mobile devices due to the differing hardware configurations, but the authentication mechanism proposed in this paper will take this into account.

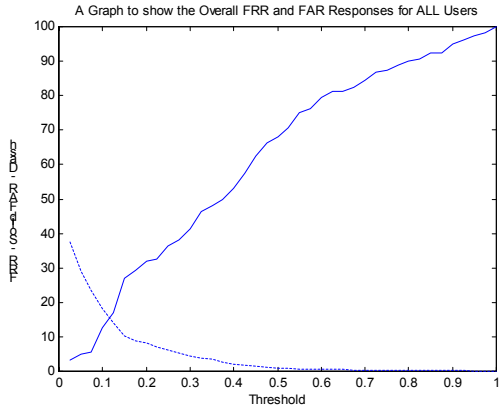
The history of keystroke dynamics dates back over twenty years with many research papers having been published, Joyce et al. (1990), Leggett et al. (1988) and Monrose et al. (1999) to name but a few. However, all studies to date with the exception of Ord (2000) have focussed on the ability to classify users on the basis of their interaction with a keyboard and not a keypad, as is common to mobile phones. To the authors best knowledge there have been no studies involving a mobile phone keypad – Ord's study used the numeric keypad from a computer keyboard, where the location and tactile differences are considered large enough to warrant an independent study. Thus a study was devised to investigate the feasibility of a keystroke dynamics technique on a mobile phone.

From the foundation Ord's study, a series of investigations were designed to examine the feasibility of using keystroke dynamics on a mobile handset (Clarke et al., 2002b). Three experiments were conducted, each involving a total of 16 participants:

1. the entry of a four digit number, analogous to the PINs used on current devices;
2. the entry of a series of varying telephone numbers;
3. the entry of a fixed telephone number.

The first and third investigations required the participants to enter the numeric keystroke sample thirty times, with twenty samples then being used to create a reference profile, and the remaining ten for subsequent testing. The second investigation required a larger number of samples due to the changing nature of the input string, and thus the need to train the authentication system more accurately. Fifty samples were taken, with thirty for training and twenty for testing.

Previous studies have shown neural networks to provide an effective foundation for keystroke analysis (Ord, 2000; Cho et al., 2000) and they have consequently been used in these investigations. The neural network structure is constructed on the feed-forward back-propagation network (Bishop, 1995), best exemplified for pattern recognition techniques.



Investigation	FAR (%)	FRR (%)	EER (%)
PIN Code	18.1	12.5	15
Varying Telephone	36.3	24.3	32
Fixed Telephone	16	15	15

Table 2 Keystroke Dynamics Results

Figure 3 Keystroke Dynamics Performance Chart

The results demonstrate the potential to distinguish authorised users from impostors, although arguably not to any great accuracy. However, the experimental procedure used in this study was performed under controlled conditions, with users all entering the same input data - a condition that is unlikely in the real world. Additionally, the design, and implementation of the neural network used for classification was primitive and un-optimised. Continuation of the study beyond this feasibility stage requires variables such as pre-processing, generalisation, network sensitivity and network configuration to be considered and analysed.

Further development of the technique will also consider other forms of user interaction with mobile handsets, in order to attempt to profile behaviour in different contexts. For instance, the way in which someone types when entering an SMS message is likely to be different to the way in which they enter a telephone number. Some users will use certain applications or functionality on the phone more often than others; will dial certain number more than others; and equally as important will not use or dial certain people or services. All of these factors could potentially be used as discriminating characteristics, leading to a stronger overall verification technique.

CONCLUSIONS

Mobile devices are going through an evolutionary period with the combined ability to have high computer processing on small handheld devices, and the formidable success of the mobile phone industry. Users are no longer chained to their desks and mobility has become an important factor in many people's life. This has left an increasing security problem generally, with a major issue being authentication.

The current form of authentication is a very cheap solution but suffers from a number of inherent weaknesses, such as the lack of and improper use of passwords and PINs. Biometrics are amongst the most powerful authentication tools as they are based on a unique human characteristic.

Biometrics' on mobile devices are also an effective tool for non-intrusive authentication, as different approaches can be implemented whilst the user is interacting with the device. In the context of a mobile phone, voice recognition can be used to authenticate a user whilst they are speaking on the phone, keystroke dynamics whilst they are typing SMS messages and facial recognition when they use video conferencing facilities. Thus a hybrid non-intrusive authentication mechanism utilising the

available biometrics on each mobile device as the underlying authenticator would provide a transparent and secure solution.

REFERENCES

Ashbourn, J. (2000). Biometric. Advanced Identity Verification. The Complete Guide. Springer.

BBC. (2002). MOD Loses 600 Laptops. BBC News Online
http://news.bbc.co.uk/hi/english/uk/newsid_1757000/1757792.stm

Biopassword (2002). www.biopassword.com

Bishop, M. (1995). Neural Networks for Pattern Recognition. Oxford University Press.

Broomfield, S. (2000). It's Not Just a Laptop Anymore!. Information Impacts Magazine. www.cisp.org/imp/february_2000/broomfield/02_00broomfield.htm.

Cho, S., Han, C., Han, D., Kim, H. (2000). Web Based Keystroke Dynamics Identity Verification using Neural Networks. Journal of Organisational Computing & Electronic Commerce, Vol.10, No.4, pp.295-307.

Clarke, N., Furnell, S., Rodwell, P., Reynolds, P. (2002a). Acceptance of Subscriber Authentication for Mobile Telephony Devices. Computers & Security, Vol.21, No.3, pp.220-228.

Clarke, N., Furnell, S., Lines, B., Reynolds, P. (2002b). Subscriber Authentication for Mobile Phones using Keystroke Dynamics. Proceedings of the Third International Network Conference (INC2002), Plymouth, UK, 16-18 July 2002. pp347-356.

Cope, B. (1990). Biometric Systems of Access Control. Electrotechnology, April/May: 71-74.

Gaines, R., Lisowksi, W., Press, S., Shapiro, N. (1980). Authentication by keystroke timing: Some Preliminary Results. Rand Report R-256-NSF. Rand Corporation, Santa Monica, CA.

Gibson, B. (2001). Apple Slips to 8th in US laptop sales. MacCentral Online. http://maccentral.macworld.com

Giussani, B. (2001). Roam – Making Sense of the Wireless Internet. Random House Business Books, London.

HandSpring. (2002). Treo 270. HandSpring. www.handspring.com

Harrington, V., Mayhew P. (2001). Home Office Research Study 235: Mobile Phone Theft. Crown Copyright.

Harrison, L. (2001). Iris Recognition is Best Biometric. The Register. www.theregus.com
Joyce R., Gupta, G. (1990). Identity Authentication Based on Keystroke Latencies. Communications of the ACM. Vol. 39; pp 168-176.

Leggett, J., Williams, G. (1988). Verifying Identity via Keystroke Characteristics. International Journal of Man-Machine Studies, 28.

Leyden, J. (2002). PDAs Make Easy Pickings for Data Thieves. The Register. www.the register.co.uk/content/54/25478.html

Monrose, F., Reiter, M., Wetzel, S. (1999). Password Hardening Based on Keystroke Dynamics. Proceedings of the 6th ACM Computer and Communication Security Conference.

Nanavati, S., Thieme, M., Nanavati, R. (2002). Biometrics. Identity Verification in a Networked World. John Wiley & Sons.

Ord, T. (1999). User Authentication Using Keystroke Analysis with a Numerical Keypad Approach. MSc Thesis, University Of Plymouth, UK.

Richardson, T. (2002). PDA Shipment Growth Slows. The Register. www.theregister.co.uk.

Singh, H., Furnell, S.M., Lines, B. and Dowland, P.S. (2001). Investigating and Evaluating Behavioural Profiling and Intrusion Detection Using Data Mining. Proceedings of International Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security, St. Petersburg, Russia, 21-23 May, 2001.

Smith, R. (2002). Authentication. From Passwords to Public Keys. Addison Wesley

Thornton, C. (2001). Fast laptop includes built-in fingerprint reader. PC World.com. www.pcworld.com/news.

HP. (2002). Targus iPAQ™ Bundle. HP. http://athome.compaq.com/store/default.asp?page=optionCategories&SuperCategoryID=97

UMTS Forum (2002). Long Term Potential Remains High For 3G Mobile Data Services. www.umts-forum.org/reports.html. pp 5.