Transparent Handwriting Verification for Mobile Devices

N.L. Clarke and A.R. Mekala

Network Research Group, University of Plymouth, Plymouth, UK
e-mail: info@network-research-group.org

Abstract

The popularity of mobile devices and the evolving nature of the services and information they can delivery make them increasingly desirable targets for misuse. The ability to provide effective authentication of the user becomes imperative if protection against misuse of personally and financially sensitive information is to be provided. Traditional measures, such as the PIN, although commensurate with current technology requirements, do not provide the level of security required for third generation mobile devices and beyond. Biometrics do however, when implemented intelligently, offer an alternative and more secure approach. This paper discusses the application of biometrics to a mobile device in a transparent and continuous fashion and the subsequent advantages and disadvantages that are in contention with various biometric techniques. For example, in order to facilitate the use of signature recognition transparently, the system must verify users based upon written words and not signatures. From the experiment conducted it was found that current signature recognition systems could indeed perform successful authentication on written words. Based upon 20 participants an average FAR and FRR of 0% and 1.2% respectively were experienced across 8 common words.

Keywords

User Authentication, Biometrics, Signature Recognition, Mobile Devices

1 Introduction

The ability to communicate and work whilst on the move has given rise to a significant growth in mobile devices. This growth has been fuelled from two contrasting directions. The first is from telephony devices that have always had a wireless network connection, but until recently minimal computational and storage capability, and so were unable to provide the user with many services beyond voice telephony. The second is from devices with reasonable computing power but no (simple) method by which they were able to connect to a network outside of the office environment. Today, however, with the advancement of mobile handsets and wireless networking, mobile devices have both the network access and computing capacity to provide users with a diverse range of services. This can be supported by a strong market growth in mobile devices, up 62% in 2004 on the previous year (Smith, 2004), and with forecasts predicting wireless revenues being worth up to $126bn by 2008 (ARC Group, 2003). The single most successful wireless technology to date has evolved device technology from pure telephony handsets into multimedia multi-functional mobile communication tools. The mobile telecommunications industry has experienced a number of revolutionary and evolutionary steps during its relatively short existence, with a current subscription based of 2 billion users worldwide (GSM World, 2005).

However, with the popularity of mobile devices, increasing functionality and access to personally and financially sensitive information, the requirement for additional and/or advanced authentication mechanisms is argued to be essential. Currently, the most popular access security to date takes the form of the password or PIN, a secret knowledge approach that relies heavily upon 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 a recent study showing that 34% mobile phone users not use a PIN, 45% have never changed their PIN and 26% have shared their PIN with other people (Clarke & Furnell, 2005a).

In addition, mobile handsets only request the PIN at switch on, with the device remaining on for large periods of the day with no protection from misuse. Although this has not been a big issue, as the number of mobile devices capable of advanced services and the availability of some wireless networks is limited, this will not hold true in the future where the majority of mobile devices will be capable of, and have access to, an extensive range of services. A trend which is beginning to be seen with the introduction of 3G networks, smartphones and large solid state storage capabilities. The financial loss to the user in this case would not only be the theft of the device itself, but the services accessed before network access is denied and the personal data stored upon the device.

There are three general categories of user authentication: something you know (e.g. passwords and PINs); something you have (e.g. tokens); and something you are (e.g. biometrics) (Smith, 2002). The aforementioned secret knowledge based approaches has already been shown to inadequate for the future needs of mobile users. The use of token based technology to improve user authentication cannot be completely ruled out with technologies such as Bluetooth enabling the capability for day-to-day devices such as watches and jewellery to be used with modified to provide wireless authentication of the user within a prescribed short distance. However, to date, token based technology has not provided any real level of security for mobile devices, with the SIM card (a token) being left within the mobile handset, removing any security that would exist if the handset and phone were separated and only brought together when the phone was in use. Finally, the ability to authenticate users based upon unique characteristics of the person is an interesting approach as it relies on the technology not the person for reliable security.

This paper introduces the concept of user authentication for mobile devices using biometrics. However key to this concept are a number of factors designed to ensure security is increased beyond point-of-entry and performed in such a manner as to minimise inconvenience to the user. Section 2 discusses the need for transparent and continuous authentication and the different types of biometric technique that would be appropriate within a mobile device context. One such technique, that of Signature Recognition, is further explored in section 3, with an experiment into its application on a mobile phone being discussed in sections 4 and 5. The paper concludes by discussing the experimental findings and suggesting further areas of research.

2 Biometric Authentication for Mobile Device

The use of biometrics, or specifically unique human characteristics, 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 biometric characteristics. Biometrics can be divided into two categories based upon the underlying characteristic they are using: physiological; and behavioural (Ashbourn 2000). Physiological biometrics are those using characteristics based upon a physical aspect of the body, such as a fingerprint, face, iris or retina. Behavioural biometrics utilise the unique way in which humans behaviour to characterise and authenticate us. Characteristics such as the way in which we speak, type and sign our name.

The term biometrics has recently been hard to avoid with numerous articles and papers being published regarding the use of the technology in passwords and identification cards (Furnell & Clarke, 2005; Fussell, 2005). However, their use in that context is fundamentally different to that being introduced in this paper. In fact, whereas the biometric passport and UK ID scheme seek to utilise highly discriminate biometric techniques such as fingerprints and iris, this study looks to deploy some of the less discriminate approaches, trading off a level of security for usability. Although the use of biometrics within nationalised contexts is somewhat controversial, the use of biometrics on mobile devices, from the aforementioned survey, suggests 83% of respondents were in favour of biometric authentication (Clarke & Furnell, 2005a).

2.1 Transparent & Continuous Authentication

People are often the key factor and inhibitor in many security controls, where the successful interaction of the user is required in order for the control to operate effectively. As such this research project sought to remove as much explicit security interaction from the user as possible but also achieving the following objectives:

- to increase the authentication security beyond secret-knowledge based approaches;
- to provide transparent authentication of the user (within limits) to remove the inconvenience factor from authentication;
- to provide continuous or periodic authentication of the user, so that confidence in the identity of the user can be maintained during usage of the device rather than simply at switch on;
- to provide an architecture that would function (to one extent or another) across the complete range of mobile devices, taking into account the differing hardware configurations, processing capabilities, and varying levels of network connectivity.

An authentication system built upon this would provide a more secure and user friendly environment within which users could operate. The architecture developed to solve this was the Intelligent Authentication Management System (IAMS). The system is designed to capture a wide variety of biometric characteristics during a users normal device interaction and continuously maintain a confidence level in the identity of the user. The level of confidence determining which resources and services a user can access. With a high level the user is given open access to all key resources and services, with the level of access diminishing with the confidence. The user is able to intrusively authenticate themselves to obtain access to a service or resource they currently do not have the confidence to access. Figure 1 below illustrates a device centric architecture for IAMS. The complete architecture and research methodology is beyond the scope of this paper but can be found in Clarke & Furnell (2005b).

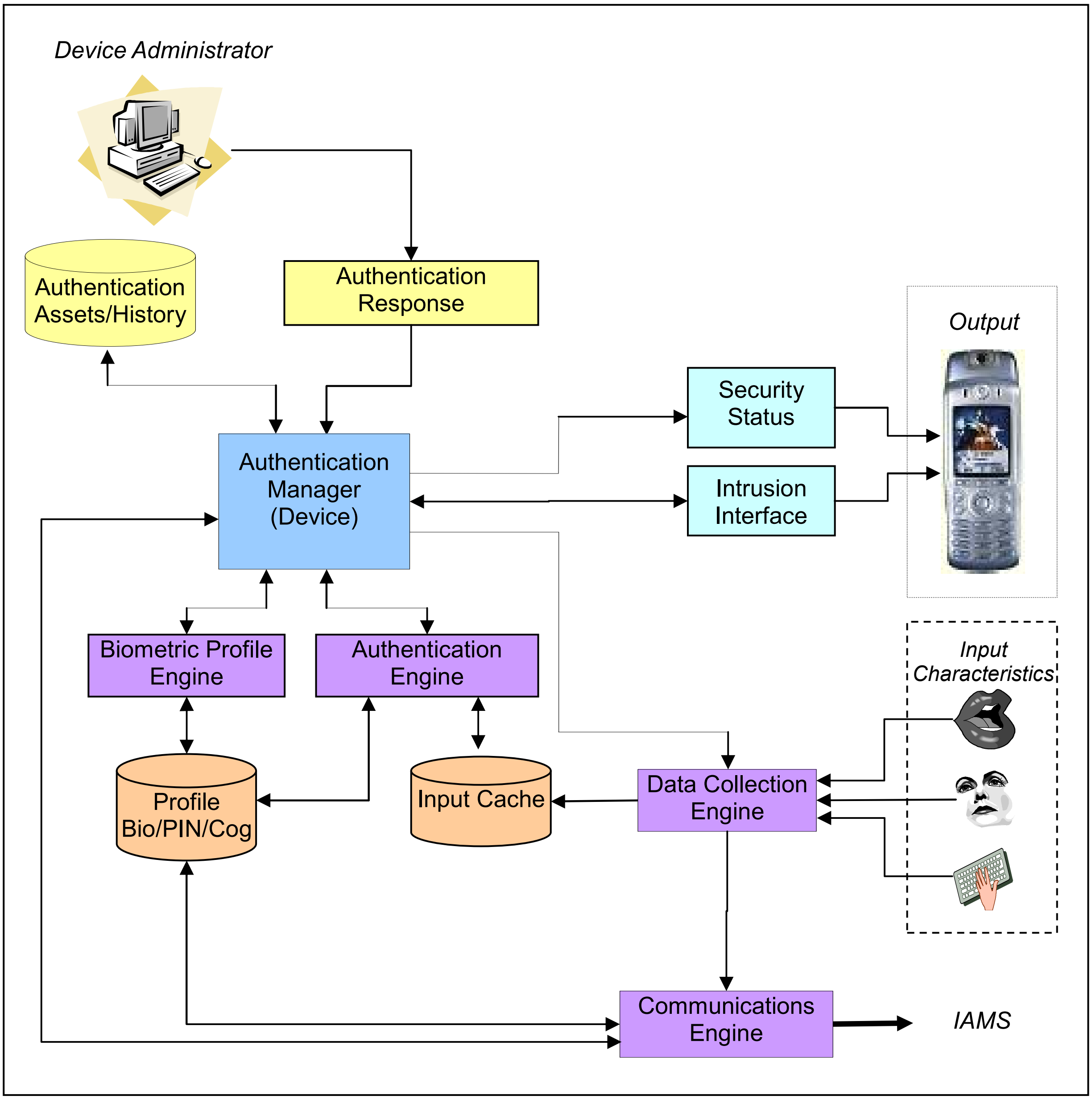

Figure 1: IAMS: Device Centric Architecture

2.2 Biometric Approaches Applicable to Mobile Devices

When considering the hardware and form factor of a mobile device, a number of biometric techniques are found to be more applicable for deployment than others. For instance, in its present form it would not be possible to deploy a hand geometry technique as the equipment used to create the image is both bulky, expensive and requires the hand to be spread flat on a surface rather than simply to be holding a device. However, various other options could be viable. The inclusion of a camera for video calling – a standard service for third generation networks – would permit the use of facial recognition. Given sufficient picture clarity, iris scanning could also be utilised. The microphone, present for telephony services, would open the potential for voice verification, and the keypad would allow a keystroke analysis technique to be applied. For handsets or PDAs without a keypad, a touch sensitive screen is usually provided as the human-computer interface, where signature recognition could subsequently be utilised.

When considering which biometrics to implement within a mobile device, one must consider all the factors; of cost, accuracy, intrusiveness and effort, in addition to user preference. Table 1 illustrates how these key factors vary for different biometric techniques with a specific focus on their applicability within a mobile device, based upon the following criteria:

- Given the already high cost of hardware, the cost factor has been converted into whether a device would already normally or potentially contain the hardware required to capture the biometric sample – based upon products currently on the market. Hardware that can be utilised for a multitude of applications is arguably a far better use of resources and is more likely to be included within the device on a wider scale.
- A (subjective) accuracy category has been assigned to each of the biometrics. Given techniques with no empirical data on performance, a performance indication is included based upon the potential uniqueness of the technique.
- Also, each of the techniques have been assigned to either an intrusive or non-intrusive category. This factor describes the practical intrusiveness and subsequent effort required in using the biometric. A non-intrusive label is assigned to a technique which has at least the potential to be implemented within a mobile device where the capture and subsequent authentication of the user can be performed without the knowledge of it occurring, for example, the use of facial recognition whilst the user is in a video conference. This would remove any effort required by the user to authenticate themself. It does not consider how intrusive the technique is perceived to be by the user. Conversely, an intrusive technique is one where a user is explicitly asked or required to present a sample.

Biometric Technique	**Sample acquisition capability as standard?**	**Accuracy**	**Non-Intrusive?**
Ear shape Recognition	✗	High	✓
Facial Recognition	✓	High	✓
Fingerprint Recognition	✗	Very High	✗
Hand Geometry	✗	Very High	✗
Signature Recognition	✓	Medium	✓
Iris Scanning	✗	Very High	✗
Keystroke Analysis	✓	Medium	✓
Service Utilisation	✓	Low	✓
Voiceprint Verification	✓	High	✓

Table 1: Applicability of Biometric Techniques for Mobile Devices

Given the apparent disparity identified between users wanting more authentication security, but not currently using what is available, and the relatively high inconvenience factor experienced by users, the use of transparent authentication using biometrics would solve both the technological requirement for a more secure authentication mechanism and the user's need to remove any inconvenience from the authentication process. Unfortunately, biometric approaches with excellent accuracy are also the intrusive techniques. A compromise between the level of security provided by a technique and the inconvenience to the user is required. This pattern can be seen to continue, with techniques such as service utilisation and keystroke analysis having very good non-intrusive potential but with lower accuracy rates. However, a number of techniques can be identified as appropriate for deployment on mobile devices in general, as illustrated in figure 2.

This selection is based upon the hardware available on mobile devices and the possible non-intrusiveness of its application. It does not take into account other factors, such as the computational and storage requirements of the techniques. The reason for this is two-fold. Mobile devices are increasing in their computing power and storage capacity on an almost yearly basis, with devices of today already being comparable to basic desktop computers of three or four years ago. Therefore, in all likelihood, mobile devices of the future will not have problems processing the data required for enrolment and authentication. In the short-term, the widespread use of wireless networking technologies would permit the use of a client-server topology for authentication – where the server is given responsibility for the computationally intensive tasks and storage of biometric templates.

Further analysis illustrates their potential for use within mobile devices under different circumstances. As previously described, facial recognition can be used on mobile handsets, however, with the proviso of a front-facing camera, PDAs and laptop computers could also utilise this technique. Keystroke Analysis could be deployed on all categories of device to perform transparent authentication whilst the user is entering text messages, scheduling a meeting, or typing a document. Signature recognition could be used as a user is entering words using the transcriber function of PDA or the notepad function of a tablet PC. Voice verification has the potential to be deployed on all three devices with the presence of a microphone. However, its greatest application would be in telephony, where dynamic authentication of the user can take place during a normal telephone call. Service utilisation also has the potential to monitor behavioural patterns on all categories of device, flagging possible misuse when the user deviates from their typical routine.

In practice however, many of these techniques do not currently have the functionality to be deployed in this manner. In fact, only facial recognition could be used *"as-is"*, with all the remaining techniques requiring varying degrees of modification or development. Keystroke analysis, although commercially available for static-based authentication on PC keyboards, currently has no dynamic-based approach – although this technique has been thoroughly researched (Leggett et al., 1991; Napier et al., 1995). Of more concern is the applicability of keystroke analysis on a mobile handset or PDA, where the keypad or thumb sized keyboard represents a different tactile environment with which the user must interact. Preliminary studies by the author have supported this (Clarke et al., 2003; Clarke et al., 2004). Signature recognition has been developed commercially to provide intrusive authentication of the user based upon a signature, but not on general words signed through transcriber. Speaker verification has also been developed for static (and pseudo-dynamic) authentication, but does not currently perform dynamic authentication of the user. Finally, although service utilisation techniques have been applied within fraud detection scenarios, their use as a real-time authentication technique is undocumented. It is clear therefore, that the majority of techniques require at least adaptation, if not a complete feasibility study before practical implementation of the technique can occur.

Research by the authors is currently underway looking at the application issues of many of these biometric techniques. It is the focus of this paper to address the applicability of signature recognition to a mobile device.

3 Signature Recognition

The handwritten signature precedes the concept of biometrics as it is defined today and has been used as a mechanism for legally binding a person to an agreement written on paper. It is this widespread and acknowledged use of signatures for verifying authenticity that makes it an appropriate technology for deployment, as it is able to minimise usability and privacy concerns.

The underlying mechanism of signature verification can operate in one of two methods: static verification or dynamic verification (Woodward et al., 2003). Under a static mode, a new signature is compared with a known stored sample in terms of its finished appearance, a process similar to the traditional human process. The dynamic mode however, can incorporate a number of additional attributes such as pressure, the speed of strokes, the direction of the stokes and the number of stokes, and authenticate the user more on how the signature was written rather than merely its appearance (Gupta & McCabe, 1997).

4 Methodology

The eventual application of signature recognition technology to handwriting verification would ideally monitor a user's natural behaviour and interaction with the device. However, the objective at this stage of the research was to test the feasibility of applying the technology to the written word. In addition, in order to provide a means of comparison in terms of performance, two investigations were performed:

- A control experiment where participants would utilise the technology as it was designed for, and sign their name in a normal fashion.
- A feasibility experiment where participants would be given a number of commonly used words (within a mobile device context) and the signature recognition technology would be applied to them.

The signature recognition technology selected for use in this research was a commercially available product named PDALok (2006). This was selected because it utilises the dynamic signature method, which was felt would be more appropriate and successful in this context, and because it functioned on a PDA, thereby providing a similar tactile environment in which a user would actually be using the technology.

Word #	Word
1	Bye
2	Love
3	Hello
4	Sorry
5	Meeting
6	Thank you
7	Beautiful
8	Congratulations

Table 2: Words Captured

Twenty people participated in this study, with each user acting in turn as the authorised user with the remaining taking the position of impostor. The users collectively were given an hour to train and identify with the system before the experiment proceeded. In the control experiment each authorised user would enrol upon the system requiring six signature repetitions. Once enrolled, the authorised user would then authenticate themselves a total of

10 times (in two 5 authenticate sessions). Each impostor would then be given the opportunity twice to sign in using the authorised users name against the authorised user's template, giving 38 impostor attempts. The feasibility experiment duplicated this process and applied it to 8 words. The words, as illustrated in Table 2, were selected in 4 bands varying in length. It was hypothesised that the longer the word the more secure in would be and thus have an effect upon the security this approach could provide. Words 1-2 are short words, 3-4 slightly longer, 5-6 longer again and 7-8 the longest.

The experiments were performed using a Toshiba Pocket PC using an unmodified version PDALok in a normal fashion.

5 Results

The performance of signature recognition within control experiment was excellent, with a 0% false acceptance rate (FAR – the rate at which an unauthorised user is accepted on to the system) and a good false rejection rate (FRR – the rate at which an authorised user is rejected from his own system) of 3.5%. Surprisingly, however, the performance of the feasibility experiment surpassed that of the control experiment, performing on average with a FAR and FRR of 0 and 1.2% respectively.

Taking a more detailed examination of the results, figure 2 illustrates the FRR for each user in the control experiment. 14 users experience 0% FAR and FRR, with user 10 performing the worst with a FRR of 20%.

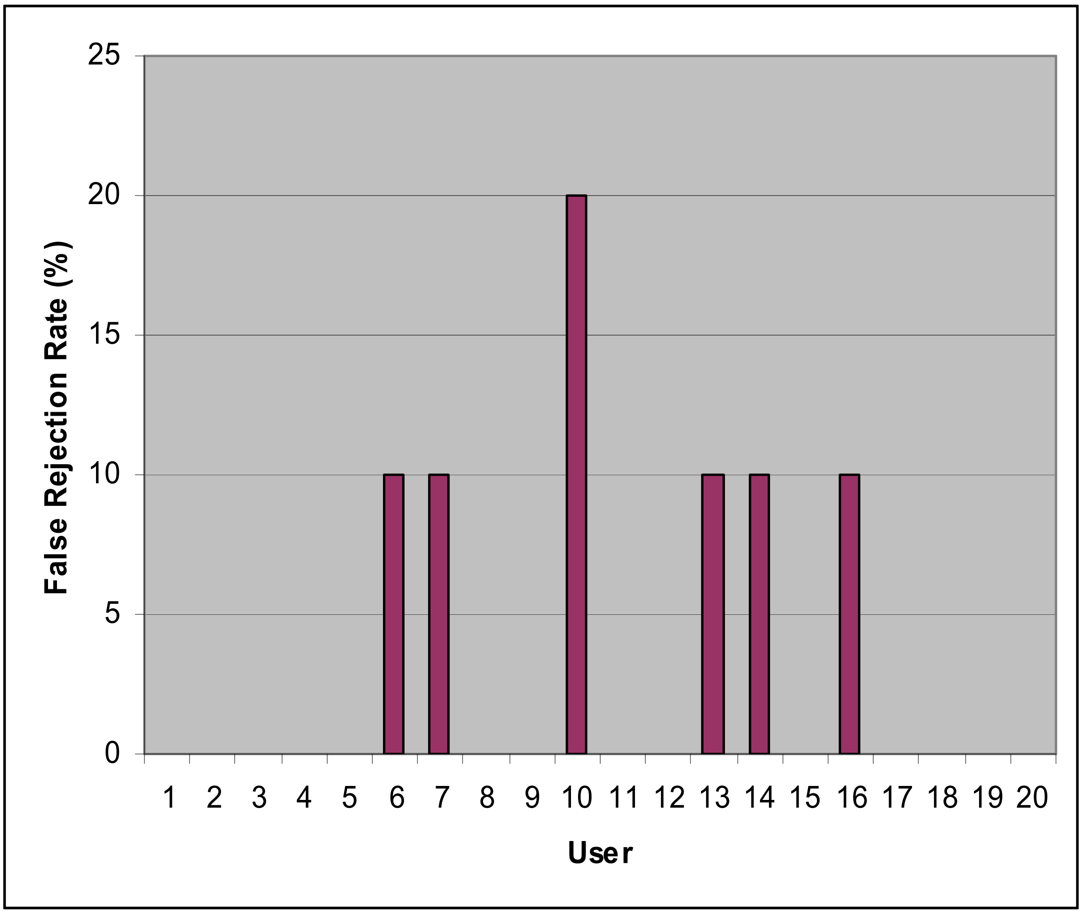

Figure 2: Users FRR in the Control Experiment

Figure 3 illustrates the average FRR across all 8 words for all the participants in the feasibility experiment. 13 participants achieved 0% FAR and FRR, with user 8 performing worst with a FRR of 8.8%.

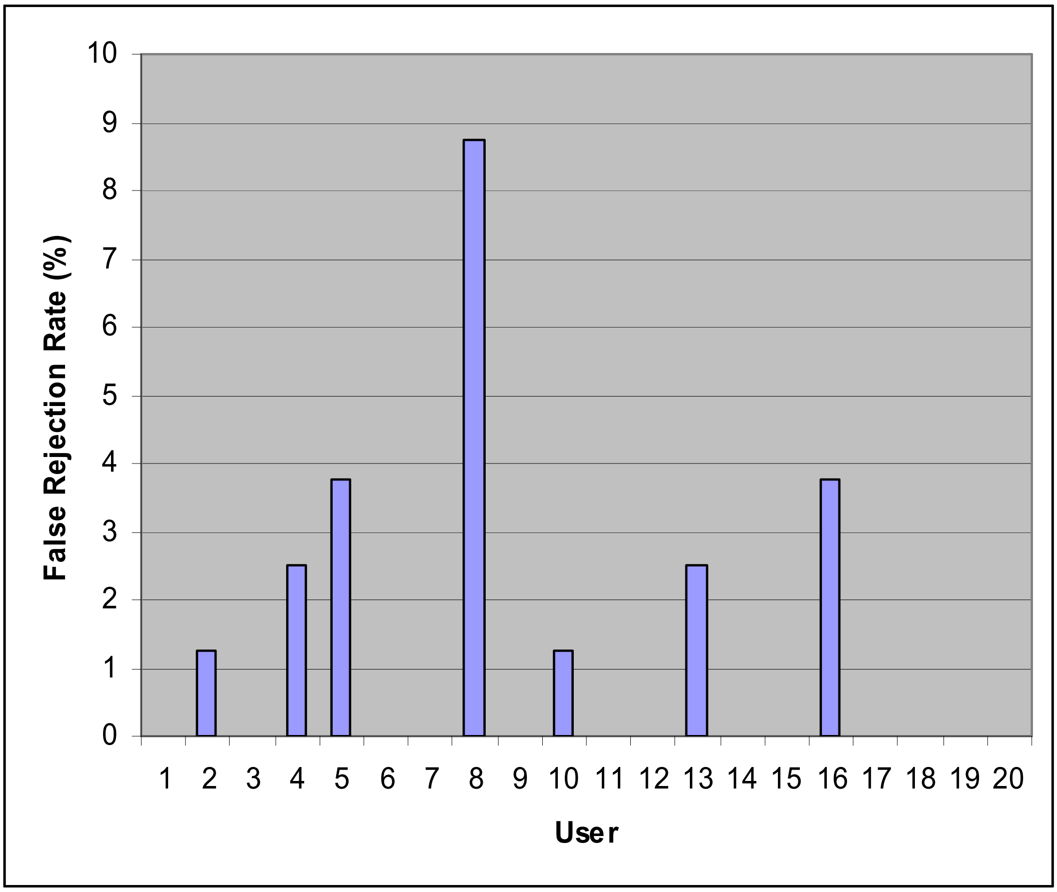

Figure 3: Users FRR in the Feasibility Experiment

Analysing the performance of the signature recognition technology against each of the words, as illustrated in table 3, shows that the length of the word did not play a factor in security, as the technique can already provide an adequate level, but rather has an effect on the FRR and subsequent usability of the approach, with longer words having a greater FRR. From this result it is suggested that enough discriminatory information is contained within small words without requiring a user to sign longer words.

Word #	Word	FRR (%)	FAR (%)
1	Bye	0	0
2	Love	0.5	0
3	Hello	1	0
4	Sorry	0	0
5	Meeting	1.5	0
6	Thank you	2.5	0
7	Beautiful	1.5	0
8	Congratulations	2.5	0
	Average	**1.19**	**0**

Table 3: Performance of Individual Words in Feasibility Experiment

Although a larger population of participants would have been ideal, the overall performance results were based on 8298 samples as detailed below:

- Control Exp: FRR: 20 participants each signing 10 times: 200 samples
  FAR: 19 participants each signing 2 x 19: 722 samples

- Feasibility Exp: FRR: 20 participants, 10 times, 8 words: 1600 samples
  FAR: 19 participants, 2 each, 19, 8 words: 5776 samples

6 Discussion

The overall performance of the signature recognition technology has been excellent with a false acceptance rate of 0% and a marginal false rejection rate. These results also raise a couple of additional interesting points. A signature recognition system is equally able to perform with handwritten words as inputs as it is with signature based input. Although the control experiment performance was poorer than that of the feasibility experiment, it is suggested that this likely has more to do with the reduced number of sample points in the control experiment than that of the feasibility experiment, with the FRR in the control experiment actually only accounting for 8 false rejections.

The word length of the handwritten words also raises an interesting result, with the FRR on average getting worse as the length increases. The FAR across all words is excellent. This suggests, given the signature recognition's ability to successful discriminate against impostors, a higher degree of variance is being experienced in the longer words and therefore shorter words would be more appropriate to use in a practical system. This has a subsequent advantage of placing less demand upon the user when performing authentication.

An analysis of the individual users between the control and feasibility experiment identifies 4 users which have a FRR greater than 0%. Although, given the small magnitude of the FRR it is still within acceptable boundaries, it does raise a trend common to all biometric techniques, particularly behavioural based. Within a population, there will always be people who (for whatever reason) are unable to use a particular biometric technique. It is appropriate therefore, if biometrics were to be deployed on a large scale, multiple techniques be utilised in order to reduce the probability of a user not being able to use any of them. Approaches such as IAMS allow for this eventuality.

7 Conclusions & Future Work

The ability of applying dynamic signature recognition to handwriting verification has been excellent, with good results across both the control and feasibility experiment. Its applicability therefore within a transparent and continuous authentication such as IAMS is good, although some work still exists in integrating the technology within existing handwriting recognition software to enable handwriting verification.

From a wider perspective, research is still continuing into the applicability of other non-intrusive biometrics, such as keystroke analysis, facial recognition and service utilisation. The authors are also examining the practicalities of an architecture such as IAMS would represent on mobile devices, giving consideration to factors such as the differing networking environments a device may encounter, usability and scalability.

8 References

Arc Group. 2003. “Mobile Content & Applications 2003”. Arc Group. http://www.3g.co.uk/3GHomeSearch.htm

Ashbourn, J. 2000. Biometrics: Advanced Identity Verification. Springer

Clarke N, Furnell S, Lines B, Reynolds P. 2003. “Using Keystroke Analysis as a mechanism for Subscriber Authentication on Mobile Handsets”. Proceedings of the IFIP SEC 2003 Conference, Athens, Greece, May, pp97-108

Clarke N, Furnell S, Lines B, Reynolds P. 2004. “Application of Keystroke Analysis to Mobile Text Messaging”. Proceedings of the 3rd Security Conference, Las Vegas, USA, 14-15 April, 2004.

Clarke, N., Furnell, S. 2005a. “Authentication of users on mobile telephones – A survey of attitudes and opinions”. Computers & Security, vol.24, no.7, pp.519-527.

Clarke, N., Furnell, S. 2005b. “User Authentication for Mobile Devices: A Composite Approach”. Proceedings of the 6th Australian Information Warfare and Security Conference, Geelong, Australia, pp.48-56.

Furnell, S. and Clarke, N. 2005. “Biometrics – No Silver Bullets”, *Computer Fraud & Security,* August 2005, pp9-14.

Fussell, R. 2005. “Authentication: The Development of Biometric Access Control”. The ISSA

GSM World. 2005. “GSM Subscriber Statistics”. GSMWorld.Com. http://www.gsmworld.com/news/statistics/pdf/gsma_stats_q3_05.pdf

Gupta, G., McCabe, A. 1997. “A Review of Dynamic Handwritten Signature Verification”. James Cook University, Townsville, Australia.

Leggett, J., Williams, G., Usnick, M. 1991. “Dynamic Identity Verification via Keystroke Characteristics”. International Journal of Man-Machine Studies.

Napier, R., Laverty, W., Mahar, D., Henderson, R., Hiron, M., Wagner, M. 1995. “Keyboard User Verification: Toward an Accurate, Efficient and Ecological Valid Algorithm”. International Journal of Human-Computer Studies, vol. 43, pp213-222.

PDALok. 2006. “Biometric Digital Signature”. Romsey Associates Ltd. http://www.pdalok.com/default.htm

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

Smith, T. 2004. “PDA, Smartphone Sales Rocket in Europe”. The Register. www.theregister.co.uk/2004/04/20/euro_q1_pda_sales/print.html.

Woodward, J., Orlans, N., Higgins, P. (2003). Biometrics. Identity Assurance in the Information Age. McGraw-Hill.