UTILISING BIOMETRICS FOR TRANSPARENT USER AUTHENTICATION ON MOBILE DEVICES

Sevasti Karatzouni, Nathan L. Clarke and Steven M. Furnell

Network Research Group, University of Plymouth, Plymouth, United Kingdom
info@network-research-group.org

ABSTRACT

Mobile devices have become a ubiquitous computing device, with over a third of the world's population now owning a device. The nature of the device has expanded far beyond its original inception as a telephony device, now capable of accessing and storing a wide-variety of information. Given this increased access, the ability to effectively provide security has become increasingly important. Key to these is authentication of the user to the device.

Unfortunately current authentication methods such as the PIN are found to be severely lacking in providing any level of security beyond initial point-of-entry, with the level of protection being provided here arguable insufficient. This paper proposes the application of biometric techniques in a transparent and non-intrusive fashion to enable continuous and user convenient authentication of the user. The proposed mechanisms seek to adapt current classification algorithms in a manner that trades off a small degree of security for larger improves in the robustness and user acceptance of the approach.

KEYWORDS

Biometrics, Authentication, Mobility

1. INTRODUCTION

The increasing capabilities of mobile handsets and networks have enabled the creation of a wide range of data-centric services. The volume of information that can be stored and accessed through mobile devices have become enormous. This has raised significant concerns regarding the sensitivity of the information for both individual and more particularly organisations. A recent study by Gartner reports 80% of organisations' critical information is stored on mobile devices [1]. It can be therefore suggested that providing appropriate protection against unauthorised access to information becomes significantly important.

A significant component of the device security consists of user authentication. The current authentication facility in mobile handsets is primarily achieved by the Personal Identification Number (PIN). Unfortunately PINs, being a secret-knowledge technique, have a number of well documented drawbacks: security relies on the user and therefore bad practices from the latter significantly diminishes the security that PINs provide [2].

An alternative solution towards more robust authentication is biometrics, which as they are based on personal identifiers; they closely relate the authentication credentials to the user and thus are able to provide more robust trust to the authentication decision. Biometrics are beginning to constitute a significant impact on the authentication market and their adoption is increasing every year for a range of industries and applications where authentication and identification of a user is required. Their application has already taken place on mobile handsets and it is estimated that in general mobile biometric solutions are going to contribute $268 million towards total mobile identity and access management market by the year 2011 [3].

To date however, all authentication approaches, including biometric approaches, have focussed upon establishing point-of-entry authentication of the user. Although this is imperative to establish at the beginning of a session, unfortunately no further verification of the user is undertaken until the device is switched off again. With the increasing reliance upon mobile devices, few devices are now actually even switched off, removing any protection point-of-entry solutions offer. The ability to provide non-intrusive authentication in a transparent fashion, without the explicit interaction of the user will assist in establishing the identity of the user throughout the session. Of the three authentication approaches: secret-knowledge, tokens and biometrics, only the latter really provides an effective mechanism to achieve this. Through the careful application of particular biometric techniques it could be possible to not only increase security but do so in a user convenient manner. It is important however to utilise techniques that lend themselves towards transparent application. Although in principal many techniques do the ability to achieve this in practice is somewhat restricted. This paper discusses the issues involved in deploying several key biometric techniques in a transparent fashion and proposes a mechanism to achieve this.

The paper is structured as follows. Section 2 presents a background in biometric authentication with section 3 discussing the application of specific techniques to a mobile device. Section 4 discusses the issues that restrict the envisaged application, examining the modifications required to enable transparency. The conclusions are given in Section 5.

2. BIOMETRIC AUTHENTICATION

Biometrics as defined by the International Biometric Group (IBG) is *the automated use of physiological or behavioural characteristics to determine or verify identity* [4]. The operation of biometrics is based on a process of establishing the level of similarity between two samples: a reference template stored in the system that was acquired during enrolment and a new acquired sample provided by the user each time that authentication must take place. A typical biometric system is illustrated in Figure 1.

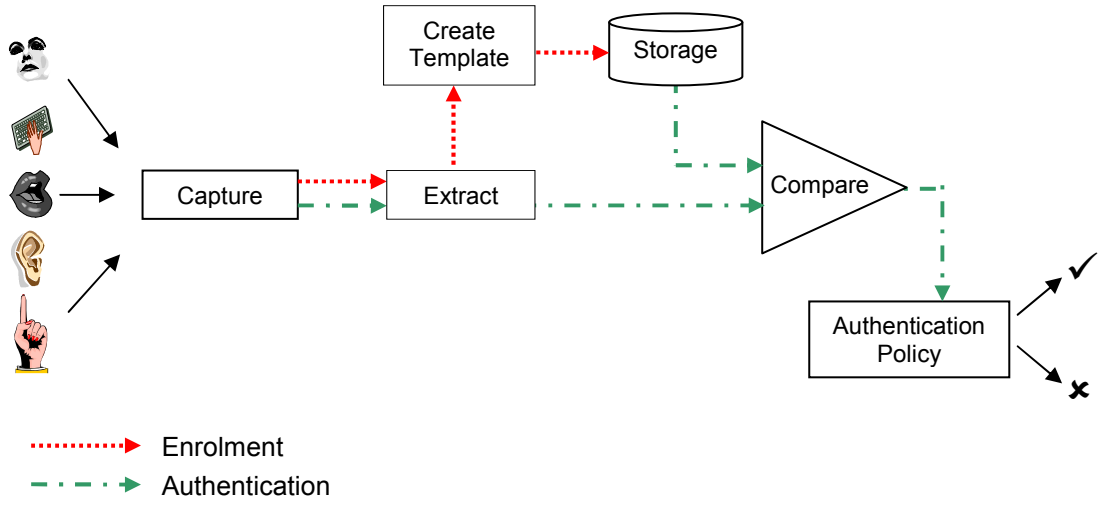

Figure 1. A typical biometric system

Each time a new sample is fed into the system the distinct features are extracted and then subsequently compared to the reference template. This extraction differs per technique in order to preserve privacy of the stored information, as well as to improve performance. Even though biometrics can be provide more robust security, the result of the comparison is a function of

similarity between the two samples and as such can lead towards two principle error rates that affect the performance of the system:

- *False Rejection Rate (FRR)*, which corresponds to the rate at which a legitimate user is falsely being denied access to the system, and
- *False Acceptance Rate (FAR)*, which represents the rate at which an impostor getting accepted by the system

Although biometric performance is the outcome of a number of factors such the feature extraction, the algorithms used to perform the comparison and also environmental conditions, the principal contribution towards good performance is the distinctiveness of the characteristics utilised. This distinctiveness varies amongst the different biometric techniques; especially between behavioural and physiological biometrics as the latter tend to be much more distinct than their behavioural counterparts. An overview of a number of biometrics of interest follows addressing the above issues as well as presenting how each technique operates.

2.1. Face Recognition

The facial structure carries a distinct geometry which can be utilised to discriminate between users. There are different ways that face recognition is performed. Traditional approaches make use of distances formed between specific key points of the face such as the points of the eyes, of the side of mouth and the nose etc [5, 6]. Though more recent techniques tend to examine the holistic view of the face's geometry concurrently utilising a number of characteristic attributes [7]. Although that makes them more demanding in terms of processing, it at the same time makes them more efficient. In all the above techniques the representation of the face is 2-dimensional which appears to be very sensitive to varying illumination, posing or facial expressions [8]. More recent research has focussed upon 3D representations in order to improve tolerance to the aforementioned variations.

2.2. Voice Verification

Voice verification seeks to differentiate between people based on their way of speech. Voice scanning is looking to extract discriminative information from a person's voice by examining the dynamics of his speech. In that way, the technique does not rely only on the sound of a word or phrase that someone could closely replicate, but it takes under consideration the overall dynamics which can not be rendered by mimicking the voice of the legitimate user. Voice verification can operate in three fashions:

- Text – dependent : the user is authenticated based on predefined keywords
- Text – prompt : the used is authenticated based on a challenge scenario
- Text – independent : the user is authenticated regardless what they say

Although all three have been extensively researched only the two first have been applied successfully.

2.3. Signature Verification

This technique utilises the uniqueness of a persons signature to verify a user's identity. Although its first application was to only look at the final result of the user's signature, newer approaches utilise other characteristics in conjunction to improve against forgery. As such a number of dynamics on the user's handwriting are taken into consideration; for example, pressure, speed, direction and the number of the strokes [5, 9]. In that way even if the final result appears to have the same signature characteristics in regards to actual image of the

signature, the dynamics that would be involved can not be counterfeit and as such the measurements would be substantially different. Most of systems nowadays utilised the dynamic approach of the technique.

2.4. Keystroke Analysis

Keystroke analysis is a biometric that tries to discriminate between users based on the way they type in a keyboard. Two features of the overall keystroke dynamics are traditionally utilised as they appear to carry more discriminative information. These are:

- Inter-key Latency: the interval between two successive keystrokes
- Hold Time: the interval between pressing and releasing a key

The technique has not reached the performance of other mainly physiological characteristics, however it has been thoroughly researched as its nature enables authentication to be performed with great transparency to the user. A downside that exists is with respect to the large amount of training data that the technique requires in order to classify between users, however given time to collect this issue is reduced. Keystroke analysis although had been extensively researched for regular keyboards it was not until recently that was assessed for keypads deployed in handsets where the tactile environment differs. The performance of the technique on mobile handsets has showed promising results by research undertaken by the authors in the past [10, 11].

3. BIOMETRICS FOR MOBILE DEVICES

There are a range of biometric techniques currently that have the potential to be utilised within a mobile context but each of them has certain trade-off in terms of cost and performance as well in regards to the option to operate transparently. Table 1 lists techniques that their application is feasible on a mobile device as well as a number of criteria important for their selection.

Table 1. Potential biometric techniques for mobile devices

Biometric technique	Sample acquisition capability as standard?	Accuracy	Non-intrusive?
Ear shape recognition	×	High	✓
Facial recognition	✓	High	✓
Fingerprint recognition	×	Very high	×
Handwriting recognition	✓	Medium	✓
Iris scanning	×	Very high	×
Keystroke analysis	✓	Medium	✓
Service utilization	✓	Low	✓
Voice verification	✓	High	✓
Gait verification	×	Unknown	✓

It can be seen that techniques that share the highest accuracy are at the same time more intrusive to the user. As such there will always be a trade-off and a balance to be sought towards satisfying both aspects of security and convenience. However there are a number of techniques that can operate transparently without further hardware requirements which can significantly reduce cost. Furthermore the aim of achieving transparent authentication imposes the requirement for approaches that are based on the regular use of the device so that no explicit interaction is required. In that basis the techniques to utilise should be also based on integrated

hardware in current and future devices, which is used during normal usage of the device. As such feasible examples of techniques that this might be achieved by - based on current capabilities of the devices, are:

- *Voice Verification*: Capture voice samples during a voice call.
- *Face Recognition*: Utilise the front camera of the handset during a video conference call or furthermore capture snapshots during a normal interaction of the user with his phone as their will be facing the front of their phone.
- *Signature Recognition*: Capture samples while a user utilises an editor in order for example to keep notes.
- *Keystroke analysis*: Capture samples while a user is typing text messages or writing a document.
- *Service Utilization:* Monitor the interaction of the user with the device based for instance on application use, frequency and timing of use etc. (Service utilisation has not yet be developed as an explicit biometric yet)

However, the effective application of the above techniques is not simple in the manner desired, as issues arise when looking to apply them in a mobile environment and moreover transparently.

4. EFFECTIVE APPLICATION ISSUES

Even though the biometric techniques discussed previously have a number of real world applications, their application in the envisaged manner within a mobile environment is restricted due to the way that the sample is captured and how the classification algorithms are implemented. Furthermore, although the nature of the approaches has the potential for transparency, current implementations of them are based on well defined point-of-entry conditions. The following sections will examine the issues that restrict their application and also the methods by which the techniques can be adapted to transparent application.

4.1. Face Recognition

The use of the technique to date has typically focussed upon very well defined environments, with controls on the illumination, facial orientation and distance from the capture device. In a mobile device these conditions are far more variable with authentication needing to take place under a wide-variety of different environmental conditions. The implementation of the technique in a transparent fashion will only seek to complicate these requirements further. The user will not be explicitly asked to pose as the sample is captured and could suffer from a number of bad variables such as poor lighting due to time of day or location, having a significant difference in facial orientation as the user is looking away from the mobile device.

In order to overcome the above issue of transparency and thus improve the tolerance of the technique to variations, two options are available. Firstly to undertaken research looking to improve the classification algorithms and remove the dependence upon these factors. Secondly, look to adapt current classification algorithms in a fashion that achieves transparency. This research proposes to opt for the latter choice, as research into improving classification algorithms has and will continue to take place and designing a process that adapts existing approaches rather than designing a single mechanism provides more flexibility. Unfortunately, when looking to adapt currently algorithms, the process is essentially trading with the FAR and

FRR of the system: typically trading less security (higher FAR) in favour of a higher level of robustness and user acceptance (lower FRR).

The proposed method of adapting existing algorithms is to move away from a one-to-one comparison of an image with a template, and replace the template with a series of images that represent various facial orientations of the authorised user. In this way, existing pattern classification algorithms can still be applied, however the approach should overall be more resilient to changes in facial orientation. As under this proposed mechanism, each sample will effectively be compared to a series of images stored within the template, the number of verifications performed will increase. This will therefore introduce an increased likelihood that an impostor is accepted by an appropriate similarity with at least one of the series of images. Under this proposed system, the FAR will only ever be as good as the original FAR of the algorithm being used, with more realistically an increase in the FAR being experienced (as illustrated in equation 1). Conversely however, under this proposed system the FRR will at worst equal that of the previous FRR, but more realistically will be lower (as illustrated in equation 2).

$$FAR_{new} \geq FAR_{old} \qquad \text{(Equation 1)}$$

$$FRR_{new} \leq FRR_{old} \qquad \text{(Equation 2)}$$

The advantage of trading of the FAR and FRR in facial recognition is two fold:

1. Facial recognition approaches have quite distinct characteristics and experience good levels of performance in terms of FAR and FRR. Indeed, facial recognition systems are often used in identification systems as well as verification systems. The use of them for verification does not require such distinctiveness.
2. The relationship between the FAR and FRR is not linear but non-linear, with small changes in the FAR typically resulting in larger changes in the FRR.

It is therefore possible to take advantage of these properties to provide a little less security for a larger improvement in the robustness and usability of the approach.

4.2. Voice Verification

Although voice verification can be performed using one of three types of input, the only effective solutions to date have been based on the text-dependent and text-prompted inputs. Unfortunately neither of these approaches can offer transparency to the verification process as the user would be required to repeat predefined or real-time generated words prompted from the system. The text independent approach is the ideal solution to the issue of achieving transparency, enabling the system to analyse the voice of the user while they use voice applications and extract the distinct features regardless of what the user says. However, to date this technique has not managed two achieve satisfactory classification results as the inputs into the classification algorithm tend to be too variable.

Similarly to the proposed mechanism for facial recognition, it is not the purpose of this solution to further the research being undertaken within the voice verification domain, of which there is much. Instead through modifying the method by which existing algorithms are used the objective of transparency can be achieved. The solution proposes to utilise the combination of three existing technologies:

1. Voice Verification – Text-dependent mode. To perform voice verification on single static phrases or words.

2. Voice Recognition. To perform recognition of the words being spoken.

3. Database. To provide a mechanism of indexing and storing the words and voice templates.

The use of voice recognition would enable recognition of the spoken word/phrase and can subsequently index them in a database of words spoken. Given a carefully designed enrolment process, the database of indexed words would be sufficiently large for a text-dependent voice verification approach to then be applied to the static word. The process of enrolment and verification is illustrated in Figure 2 and Figure 3.

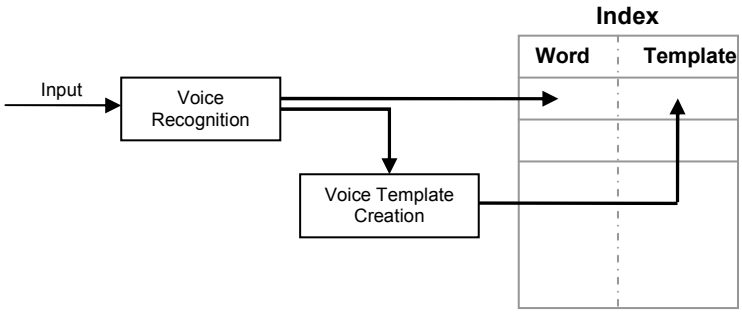

Figure 2. Voice Enrolment Process

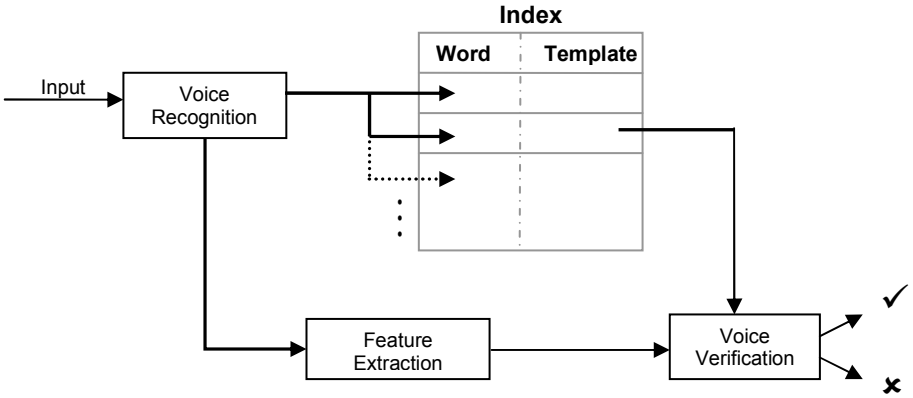

Figure 3. Voice Verification Process

Through applying the algorithms in this manner the system is able to take advantage of strong performance experienced by text-dependent voice verification. The possible disadvantage is the enrolment database of index words not being sufficiently large to enable static classification to take place – none of the phrases spoken in practice appear in the enrolment database. Given the one-to-one verification that takes place (versus a one-to-many) it is not anticipated that the level of security will be affected either positively or negatively, however the transparency and subsequent usability of the approach should improve significantly.

4.3. Signature Recognition

In order to achieve the objective of transparency, a requirement exists to authenticate a user, not based upon their signature (as this would need to be obtained intrusively) but based upon written words a user might scribe using the stylus on the touch-sensitive screen. In essence, it is not signature recognition that is required but handwriting verification.

The move towards dynamic signature classification has assisted in the ability to measure unique characteristics of how a user writes rather than simply the final image. This places less reliance upon the uniqueness of the final signature (and the word in this particular scenario). Therefore, although two written words might appear to look the same (a fairly trivial task) it is highly unlikely there were written in an identical fashion.

Unfortunately, current systems can only deal with simple one-to-one comparisons and in order to achieve transparency, the system would need to be equipped with the ability to verify a user by whichever word they scribed. Implementing a design approach, similar to voice verification, where a database is utilised to index written words during enrolment would assist in providing a dictionary of previously scribed words within which to perform verification.

This approach would also suffer from the same disadvantage as voice, in that a previous sample must be stored in the database for verification to be performed. However, with carefully designed enrolment processes, this problem can be minimised. It will also theoretically not affect the security, however initial prior research undertaken by the authors have already demonstrated good performance of this approach, indeed with it providing better security than when used in its traditional signature recognition mode [12].

4.4. Keystroke Analysis

Keystroke analysis even in a text-dependent mode is one of the weaker forms of biometric authentication, suffering from large variations in typing characteristic leading to worsening levels of security and user inconvenience. Utilising keystroke analysis in text-independent mode has not resulted in performance rates that would be useful in practice. It is therefore necessary to utilise the static (text-dependent) mode of operation and seek to apply current algorithms in a fashion to achieve transparency.

For the transparent use of the technique a similar approaches to the above could be used, by indexing the words typed by the user. Studies in the past have been performed by the authors utilising for reference a number of keywords likely to occur in text messages. The results showed promising results indicating that such approach could be effectively used for achieving transparency [10, 11]. Nevertheless due to the less distinctive nature of keystroke features it is suggested that a large index of words must be utilised and the use of more than one word in each verification in order to further improve the verification decision (as illustrated in **Figure 4**).

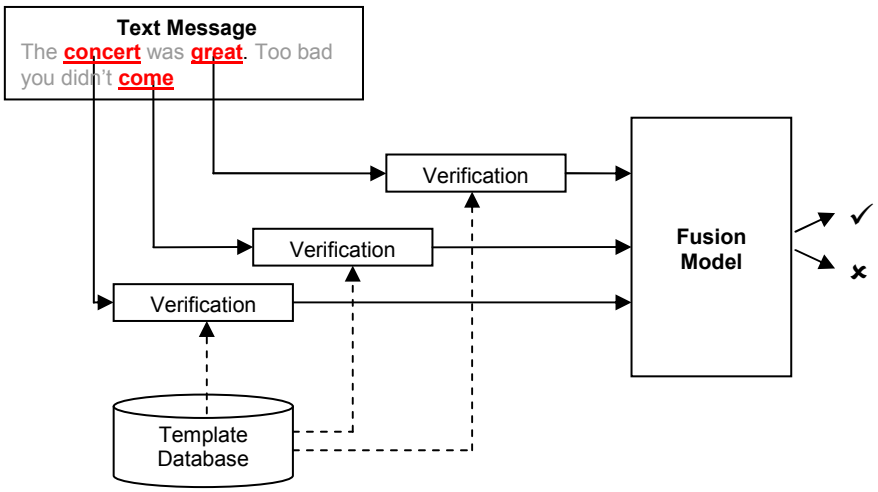

Figure 4. Fusion model for keystroke analysis

The modification proposed to this approach will not negatively affect the security provided, as a one-to-one based verification is still being performed. It should however improve the robustness and importantly achieve transparency.

5. CONCLUSIONS

The changing nature of mobile computing imposes the requirement for enhanced and robust security. Biometrics can address this issue and provide more trust with respect to the user's identity. Furthermore, if implemented correctly they can provide a mechanism to transparently and thus continuously maintain trust of the user.

However, such application is yet restricted due to current implementations and mechanisms have been proposed that focus upon the integration of technology and the use of the more static characteristics. Through the manipulation of security and user convenience, techniques can be applied in a transparent fashion.

Further research is required however to assess to what degree these proposed mechanisms will improve user convenience and importantly at what cost to security.

REFERENCES

[1] Martin, A. (2005) *Tackling mobile security*, SCMagazine, http://scmagazine.com/uk/news/article/520403/tackling-mobile-security

[2] Lemos, R. (2002): "Passwords: The Weakest Link? Hackers can crack most in less than a minute", CNET.com, Available at: http://news.com.com/2009-1001-916719.html

[3] ITWALES (2006) *Mobile security products to be incorporated into handsets by 2011*, http://www.itwales.com/997788.htm

[4] IBG (2007) *Which is the best biometric technology*, International Biometric Group, http://www.biometricgroup.com/reports/public/reports/best_biometric.html

[5] Ashbourn, J. (2000): "Biometrics: Advanced Identity Verification, The Complete Guide", Springer, London, UK, 2000

[6] Yun, W.Y. (2003): "The '123' of Biometric Technology", Information Technology Standards Committee, Available at: http://www.itsc.org.sg/synthesis/2002/biometric.pdf

[7] Chellappa, R., Wilson, C.L., Sirohey, S. (1994): "Human and Machine Recognition of Faces: A Survey", University of Maryland Computer Vision Laboratory. Available at http://lcv.stat.fsu.edu/research/geometrical_representations_of_faces/PAPERS/face_recognition_survey1.pdf

[8] Bronstein, A.M., Bronstein, M.M., Kimmel, R. (2003) *Expression-Invariant 3D Face Recognition*, Proceedings of Audio & Video-based Biometric Person Authentication (AVBPA), Lecture Notes in Computer Science, Vol. 2688, Springer, 2003, pp. 62-69

[9] Gupta, G., McCabe, A. (1997): "A Review of Dynamic Handwritten Signature Verification",James Cook, University, Townsville, Australia

[10] Clarke, N.L., Furnell, SM. (2006): "Authenticating Mobile Phone Users Using Keystroke Analysis", International Journal of Information Security, pp1-14, 2006

[11] Karatzouni S, Clarke NL (2007): "Keystroke Analysis for Thumb-based Keyboards on Mobile Devices", Proceedings of the 22nd IFIP International Information Security Conference (IFIP SEC 2007), Sandton, South Africa, 14-16 May, pp. 253-263

[12] Clarke, N.L., Mekala, A.R. (2006): “Transparent Handwriting Verification for Mobile Devices”, Proceedings of the Sixth International Network Conference (INC2006), Plymouth, UK, 11-14 July, pp277-288, 2006