available at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Advanced user authentication for mobile devices

*N.L. Clarke, S.M. Furnell**

Network Research Group, School of Computing, Communication and Electronic, University of Plymouth, Drake Circus, Plymouth PL4 8AA, UK

ARTICLE INFO

Article history:
Received 22 August 2005
Revised 22 August 2006
Accepted 22 August 2006

Keywords:
Keystroke analysis
User authentication
Biometrics
Mobility
Composite authentication

ABSTRACT

As mobile devices continue to evolve in terms of the capabilities and services offered, so they introduce additional demands in terms of security. An issue that has traditionally been poorly served is user authentication, with the majority of devices relying upon problematic secret knowledge approaches. This paper proposes the use of more advanced biometric methods as an alternative. After considering the general range of available techniques and their applicability to mobile devices, the discussion focuses upon the concept of keystroke analysis. Results of a practical evaluation are presented based upon the entry of both telephone numbers and text messages on a mobile phone. The findings reveal the technique to have promise for certain users with average error rates below 5%. The paper then proceeds to explain how the accuracy could be further improved by incorporating keystroke analysis within a composite authentication mechanism that utilises a portfolio of authentication techniques to provide robust, accurate and transparent authentication of the user.

1. Introduction

Mobile devices such as cellular phones and Personal Digital Assistants (PDAs) are now allowing access to an increasing range of data-centric services. Users of such devices can now pay for products using micro-payments, surf the Internet, buy and sell stocks, transfer money and manage bank accounts. In order to enable delivery of such services, mobile devices have become increasingly powerful: phone handsets in particular have evolved from relatively basic terminals, that would handle analogue telephony communications, to digital handsets capable of providing a host of data-centric services, turning the handset into a multimedia, multi-purpose, mobile communications tool, providing much of the functionality of today's PDAs.

With more applications being accessible, and more data being stored, it can be argued that users are now carrying devices that require correspondingly greater levels of protection. Specifically, the reasons for this will include:

1. More technologically advanced mobile handsets – future handsets will be far more advanced than current mobile phones, increasingly incorporating much of the functionality of PDAs, MP3 players, and other portable devices. As such, they will be more expensive and attractive to thieves, resulting in a financial loss to the subscriber.
2. Availability of data services – cellular and wireless networks will provide the user with the ability to download and purchase a whole range of data services and products that would be charged to the subscriber's account. Theft and misuse of the handset would result in financial loss for the subscriber.
3. Sensitive Information – devices will store much more information than current handsets. Proposed applications could result in a whole range of personal, financial and medical information being held, alongside records of business and personal communications conducted by the user (e.g. via emails and multimedia messages). As a simple example of how such evolution has already occurred we need only

* *Corresponding author*. Tel.: +44 1752 233521; fax: +44 1752 233520.
E-mail address: info@network-research-group.org (S.M. Furnell).
0167-4048/$ – see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2006.08.008

consider the contact list on a typical handset. Whereas devices a few years ago would simply hold names and phone numbers, current devices can store full home and business address details for each contact, as well as multiple phone numbers, date of birth and other family information (e.g. names of spouses and children). As such, the compromise of the device would reveal a far greater degree of personal data.

The increasing requirement for protection is evidenced by a survey of 230 business professionals, which found that 81% considered the information on their PDA was either somewhat or extremely valuable. As a result, 70% were interested in having a security system for their PDA, with 69% willing to pay more for a PDA with security than one without (Shaw, 2004). With this in mind, it is relevant to consider the degree to which related security measures are already provided and utilised. Currently, the most widely deployed authentication methods are passwords and PINs (Personal Identification Numbers) – secret knowledge approaches that relies heavily upon the user to ensure continued validity. For example, the user should not use the default factory settings, share their details with others, or write the information down. However, the poor use of passwords and PINs has been widely documented (Denning, 1999), and many mobile users do not even use the security which is available. For example, a survey assessing authentication and security practices on mobile handsets found that 34% of the 297 respondents did not use any PIN security (Clarke, 2004). In addition, even for those respondents who did use the PIN at switch-on only, 85% would leave their handset on for more than 10 h a day, thereby mitigating any security the PIN might provide. Interestingly however, it would appear users do have an appreciation of security, with 85% of respondents in favour of additional security for their mobile device. These findings introduce an interesting and somewhat contradictory view of security, with users willing to adopt new security but not willing to utilise current functionality.

It is widely recognised that authentication can be achieved by utilising one or more of three fundamental approaches: something the user *knows* (password); something the user *has* (token) and something the user *is* (biometric) (Nanavati et al., 2002). The downside of the first approach has already been highlighted, with the use of PINs found to be somewhat lacking in practice. Similarly to secret knowledge techniques, token based approaches fundamentally rely upon the user to remember something to ensure security, with the token needing to be physically present in order to access the device. However, it is considered that this does not lend itself particularly well to the mobile device context either. The most likely scenario is that users would simply leave the token within the mobile handset for convenience. Indeed, this is the case with the Subscriber Identity Module (SIM) in mobile handsets, which already exists as a token and could be physically removed from a phone when not in use. Users typically do not do this because it is inconvenient, and increases the risk of losing or damaging the SIM card. In contrast to the other methods, the third approach to authentication does not rely upon the user to remember anything – it just requires them to be themselves. Such techniques are collectively known as biometrics, and it is here that the most suitable alternatives for going beyond the PIN can be found.

This paper introduces the concept of advanced user authentication for mobile devices through the application of biometrics in a composite, transparent and continuous fashion. This is supported by a study into the feasibility of one particular biometric that lends itself to mobile devices, enabling an increase in the security that can be provided by a device. The main discussion begins by considering biometric technology in more detail, describing particular techniques that lend themselves to mobile devices and the levels of performance that can be typically expected. Section 3 presents a formal study into the application of one such biometric upon a mobile handset. The study looks into authenticating users by the way in which they enter a telephone number or write a text message using a biometric called keystroke analysis. Given the wide variety of mobile devices that exist, with different hardware configurations and processing capabilities, it is clear that no single authentication technique would be suitable for all situations. Rather it would be far more appropriate to provide a suite of authentication techniques that could provide an overall authentication approach for mobile devices. Section 4 describes how such an approach can be achieved, fulfilling the objectives of a more secure, transparent and continuous authentication mechanism. The paper concludes by discussing further areas of work currently underway by the authors.

2. An overview of biometric authentication

The identification and verification of individuals based upon 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. However, the definition of biometrics within the IT community is somewhat broader than just requiring a unique human characteristic(s) and describes the process as an automated method of determining or verifying the identity of a person (Kung et al., 2005). Biometric approaches are typically subdivided into two categories, physiological and behavioural. Physiological biometrics classify a person according to some physical attribute, such as their fingerprints, facial features, or iris patterns. Conversely, behavioural biometrics attempt to characterise the way in which an individual does things, such as speak, type, or sign their name.

The first stage in any biometric system is enrolment, where a reliable sample from the user is acquired. It is essential during this stage the users identity is confirmed, as it is this sample that all subsequent authentications will be compared against. The subsequent comparison stage (which occurs during each authentication attempt) gives rise to a measure of similarity between the sample taken at enrolment (called the template) and the new sample. This process subsequently has the potential for two categories of error: the False Acceptance Rate (FAR), denoting the degree to which impostors are accepted by the system, and the False Rejection Rate (FRR), indicating the likelihood of authorised users being denied access. The error rates tend to share a mutually exclusive relationship giving rise to a situation where neither of the error