Non-Intrusive Subscriber Authentication for 3G Mobile Systems

Nathan Clarke, Paul Dowland, Dr Steven Furnell, Prof Paul Reynolds and Philip Redwell
Network Research Group, Department of Communication and Electronic Engineering, University of Plymouth, UK

Abstract
Mobile phones are now an accepted part of everyday life, with users becoming more reliant on the services that they can provide. In the vast majority of systems, the only security to be built into the handset is a Personal Identification Number (PIN). Although this may be argued to be commensurate with the requirements of current mobile applications, it is considered that the extended range of services that will be accessible through future third generation (3G) devices will increase the need for stronger methods. The need for stronger security is also highlighted by the increasing commoditisation of advanced subscriber authentication techniques and the relatively low cost of a mobile handset. A survey of 161 mobile subscribers was conducted to assess their attitudes towards the security available in current second generation devices, and their likely acceptance of more advanced methods. Most respondents acknowledged the benefits of improved security techniques and architectures designed for mobile systems; users were aware of potential solutions as the basis for achieving a transparent, non-intrusive method of authentication that does not disrupt the user's activity unless an anomaly is suspected. The viability of the concept will be illustrated by presenting details of a practical keystroke analysis system, which has been implemented to authenticate users on a modified mobile handset. The results observed from this prototype implementation will be discussed.

Subscriber Security Requirements for 3G Systems
The subscriber security provisions in current second generation mobile networks, such as GSM, are relatively limited, with the vast majority of devices using an on-card Personal Identification Number (PIN) based method. However, it can be argued that the level of security needs to be commensurate with the requirements of the device, so the potential consequences from theft or impostor access can be broadly categorised as financial loss (which the legitimate user can limit by reporting the theft of his phone and getting it blocked by the operator) and breach of personal privacy, due to the impostor gaining access to all of the phone's content and activities. If you have got your phone stolen, it is acknowledged that this is a fairly minimal amount of information, the disclosure of which would not normally be considered highly sensitive. Stored text messages may potentially have more significance, but would not generally represent a significant body of information. By contrast, the proposed services third generation (3G) networks demand a more secure subscriber-based authentication system in order to protect personal information in the event of masquerade attacks. The primary reason for this is the hastening convergence of mobile devices with Personal Digital Assistant (PDA) devices, and the subsequent expansion in the range of possible services enabled as a result. The potential consequences of a masquerade will therefore, become far more severe owing to the additional and more private information that these hybrid devices will store.

A Survey of Current Mobile Subscribers
A survey was conducted to determine the attitudes of mobile users in relation to their use of existing PIN-based security, and their views about potential future methods. The survey was distributed to a broad range of mobile phone users, and a total of 161 responses completed both on paper and on line. Although 89% of respondents knew about the PIN facility, only 55% of them actually used it. The survey showed that 76% of respondents had phones with only a single level of security (all power on). Of those users that had the facility to PIN protect the phone in standby mode, only 36% actually used it. Other key findings included:

- 11% of respondents did not even know about the PIN facility. This equates to a 56.6 million subscribers worldwide.
- 44% of respondents did not use the PIN facility, 66% gave the reason as being too inconvenient.
- Providing additional levels of security does not necessarily mean that a subscriber would use them, as evidence from those users who did not use the PIN to lock phones in standby.
- 43% of respondents, 44% had 98% confidence in the protection offered by the PIN facility, believing their phone is still at risk even with the facility active.

Respondents did, however, recognise the need for security, with 81% believing it would be unacceptable without increased security services. As for the form that such security would take, subscribers were asked to comment upon the acceptability of a range of biometric measures, and the results were as shown in the graph below.

An Architectural Framework for Authentication
Authentication could most usefully be handled within a flexible security framework, which is able to identify and cater to the needs of each user. A survey reveals that the level of security expected will vary from user to user, depending on the activities they are performing. This is illustrated by presenting details of a practical keystroke analysis system, which has been implemented to authenticate users on a modified mobile handset. The results observed from this prototype implementation will be discussed.

Summary
The capabilities of 3G mobile systems will open up a range of new service opportunities and, as a consequence, have introduced new requirements for security. The survey findings indicated a weakness of the current provisions, in that the authentication technology is optional and, therefore, often unused. However, whilst non-intrusive security techniques have received mixed reactions from users, their potential has yet to be fully realised. Given that many respondents were unsure about what other types of technology would be available to them, it could be assumed that a non-intrusive method of authentication may prove to be more acceptable and widely used by handset users. Visible architectural frameworks can be specified to support this, and appropriate biometric measures can be identified to comply with the underlying authentication methods.


Figure 1: Acceptability of biometric authentication options

Figure 2: Components of the Authentication Framework

Figure 3: Potential subscriber monitoring baseline

An Experimental Biometric
Initial experimental work has been conducted to assess the feasibility of applying keystroke dynamics, within a mobile phone context, to authenticate by assessing their interactions on the keypad (touching profiles of characteristic inter-keyboard survey timings for different parameters). The initial study has utilised two types of keypad input, namely 4-digit PIN codes and standard telephone numbers.

The study involved 16 test subjects, with network/user being trained in an attempt to differentiate between legitimate users and impostors. Data input was collected from a modified mobile phone handset, connected to a PC in order to preserve the tactile context of a mobile device.

Note: Individual networks performed as well as 0% FRR and 1.3% FAR

FAR FRR EER
PIN code
18.1 12.5 15
Varying telephone
36.3 24.3 32
Fixed telephone
16 15 15

The initial study has utilised two types of keypad input, namely 4-digit PIN codes and standard telephone numbers.

The study involved 16 test subjects, with network/user being trained in an attempt to differentiate between legitimate users and impostors. Data input was collected from a modified mobile phone handset, connected to a PC in order to preserve the tactile context of a mobile device.

Note: Individual networks performed as

http://www.plymouth.ac.uk

Computers & Security

Proceedings of IFIP CMS '97

Figure 1: Acceptability of biometric authentication options

Figure 2: Components of the Authentication Framework

Figure 3: Potential subscriber monitoring baseline

An Experimental Biometric
Initial experimental work has been conducted to assess the feasibility of applying keystroke dynamics, within a mobile phone context, to authenticate by assessing their interactions on the keypad (touching profiles of characteristic inter-keyboard survey timings for different parameters). The initial study has utilised two types of keypad input, namely 4-digit PIN codes and standard telephone numbers.

The study involved 16 test subjects, with network/user being trained in an attempt to differentiate between legitimate users and impostors. Data input was collected from a modified mobile phone handset, connected to a PC in order to preserve the tactile context of a mobile device.

Note: Individual networks performed as well as 0% FRR and 1.3% FAR

FAR FRR EER
PIN code
18.1 12.5 15
Varying telephone
36.3 24.3 32
Fixed telephone
16 15 15

The initial study has utilised two types of keypad input, namely 4-digit PIN codes and standard telephone numbers.

The study involved 16 test subjects, with network/user being trained in an attempt to differentiate between legitimate users and impostors. Data input was collected from a modified mobile phone handset, connected to a PC in order to preserve the tactile context of a mobile device.

Note: Individual networks performed as well as 0% FRR and 1.3% FAR

FAR FRR EER
PIN code
18.1 12.5 15
Varying telephone
36.3 24.3 32
Fixed telephone
16 15 15

The initial study has utilised two types of keypad input, namely 4-digit PIN codes and standard telephone numbers.

The study involved 16 test subjects, with network/user being trained in an attempt to differentiate between legitimate users and impostors. Data input was collected from a modified mobile phone handset, connected to a PC in order to preserve the tactile context of a mobile device.

Note: Individual networks performed as well as 0% FRR and 1.3% FAR

FAR FRR EER
PIN code
18.1 12.5 15
Varying telephone
36.3 24.3 32
Fixed telephone
16 15 15

The initial study has utilised two types of keypad input, namely 4-digit PIN codes and standard telephone numbers.

The study involved 16 test subjects, with network/user being trained in an attempt to differentiate between legitimate users and impostors. Data input was collected from a modified mobile phone handset, connected to a PC in order to preserve the tactile context of a mobile device.

Note: Individual networks performed as well as 0% FRR and 1.3% FAR

FAR FRR EER
PIN code
18.1 12.5 15
Varying telephone
36.3 24.3 32
Fixed telephone
16 15 15

The initial study has utilised two types of keypad input, namely 4-digit PIN codes and standard telephone numbers.

The study involved 16 test subjects, with network/user being trained in an attempt to differentiate between legitimate users and impostors. Data input was collected from a modified mobile phone handset, connected to a PC in order to preserve the tactile context of a mobile device.

Note: Individual networks performed as well as 0% FRR and 1.3% FAR

FAR FRR EER
PIN code
18.1 12.5 15
Varying telephone
36.3 24.3 32
Fixed telephone
16 15 15

The initial study has utilised two types of keypad input, namely 4-digit PIN codes and standard telephone numbers.