Non-Intrusive Subscriber Authentication for 3G Mobile Systems

Nathan Clarke, Paul Dowland, Dr Steven Furnell, Prof Paul Reynolds and Philip Rodwell
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 prevent unauthorised use of 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 research relates to the investigation, design, and evaluation of advanced subscriber authentication techniques, suited to application within the context 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 to support emerging applications. These results support the conceptual design of a user authentication architecture for 3G mobile systems, using the concepts of biometrics 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 relying upon Personal Identification Number (PIN) based methods. However, it can be argued that the level of security here is commensurate with the requirements of the devices, as 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 the phone and getting it blocked by the operator) and breach of personal privacy, due to the impostor gaining access to contact details and text messages held on the device. However, it is acknowledged that this is a fairly limited 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:

- financial details enabling mobile electronic commerce transactions
- electronic certificates for digital signatures
- full contact details of family and associates
- commercially sensitive miscellaneous information (e.g. scheduler/notepad files)
- medical records as a result of telemedicine or teleconsultations.

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 56% of them actually used it. The survey showed that 76% of respondents had phones with only a single level of security (at power on). Of those users that had the facility to PIN protect the phone in standby mode, only 36% used it. Other key findings included:

- 11% of respondents did not even know about the PIN facility. Scaled up this could represent up to 52.8 million subscribers worldwide.
- Of the 44% of respondents who did not use the PIN facility, 65% gave the reason as being its inconvenience.
- Providing additional levels of security does not necessarily mean that a subscriber will actually use them, as evidenced by those users who did not use the PIN to lock phones in standby.
- A large number of respondents, 41%, have little 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 either *good* or *very good* to have increased security. As for the form that such security would take, subscribers were asked to comment upon the acceptablity of a range of biometric measures, and the results were as shown in the graph below.

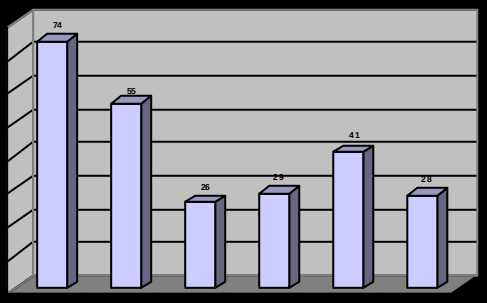


Figure 1: Acceptability of biometric authentication options

88% of users wanted to be able to access additional data services, such as m-commerce, video conferencing and web browsing from their devices – highlighting the need to better authentication in future devices.

One of the stated requirements for secure 3G service provision is that it should be possible for service providers to "authenticate users at the start of, and during, service delivery" (3GPP, 1999). Authentication *during* service delivery represents a departure from the standard approach in 2G systems and again implies the need for some form of transparent measure to avoid disrupting a subscriber's legitimate activity. Options for achieving this may be related to periodic or continuous supervision of subscriber activity, utilising profiling techniques or biometric monitoring.

Of the respondents who indicated that they would like more security, 63% also felt that the a continuous technique during normal phone use would be a good idea. Obviously some authentication methods lend themselves to this much better than others, and it would be important from the user acceptance perspective to ensure that chosen method(s) could be applied in a non-intrusive manner.

An Architectural Framework for Authentication

Authentication could most usefully be handled within a flexible security framework, which is able to intelligently monitor the available characteristics based upon the current activity of the subscriber. For example, voice verification could be utilised during a voice call, but during an e-commerce transaction it could be replaced by other characteristics that are more appropriate to the context, such as keystroke analysis. The monitoring system would determine which characteristics, from those available on the terminal, should be assessed at any given time and then pass on the relevant data for analysis. The analysis itself could be network or terminal-based. However, to avoid traffic overhead, the latter approach may be preferable. The terminal could then securely send the results to a network-based monitoring agent for access decisions (the involvement of the network level ensures that the network operator / service provider is kept aware of potential compromise). In this scenario, the network ultimately remains in control of the security and could request re-sampling by the terminal if the authentication results were inconclusive. Such an arrangement is illustrated in the figures below. The approach would be non-intrusive in the sense that the terminal user would be unaware of the security system unless compromise was suspected.

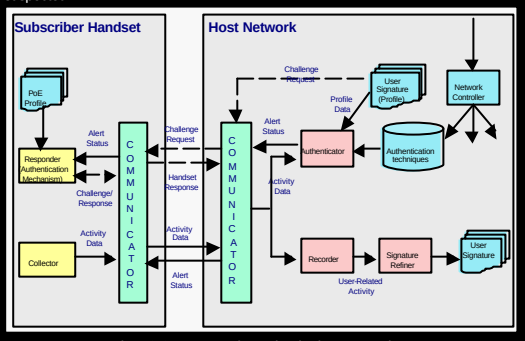


Figure 2: Components of an Authentication Framework

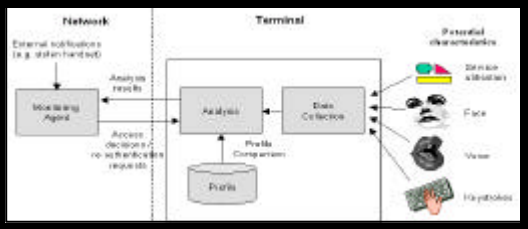
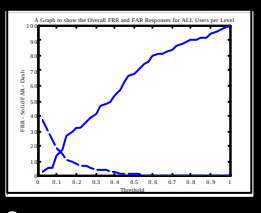


Figure 3: Potential Subscriber Monitoring Scenario

An Example Biometric

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

The study involved 16 test subjects, with neural networks 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.



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

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

Summary

The capabilities of 3G mobile systems will open up a range of new service opportunities and, as a consequence, will impose 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, subscribers have shown the desire for additional security, and have responded positively towards a number of alternative techniques. Given that many respondents do not use the current security techniques that are available to them, it can be assumed that a non-intrusive method of authentication may prove to be most acceptable and widely utilised by end users. Viable architectural frameworks can be specified to support this, and appropriate biometric measures can be identified to provide the underlying authentication methods.

Clarke, N.L, Furnell S.M, Rodwell , P.M. and Reynolds, P.L. 2001. " Acceptance of subscriber authentication methods for mobile telephony devices", to appear in *Computers & Security*.

Furnell, S.M, Illingworth , H.M, Katsikas, S.K, Reynolds, P.L. and P.W.Sanders. 1997."A comprehensive authentication and supervision architecture fornetworked multimedia systems", *Proceedings of IFIP CMS '97*, Athens, Greece, 22-23 September 1997, pp227-238.

Furnell, S.M, Dowland, P.S, Illingworth , H.M. and P.L.Reynolds. 2000. " Authentication and supervision: A survey of user attitudes", *Computers & Security*, vol. 19, no. 6, pp529-539.

Rodwell, P.M, Furnell, S.M. and Reynolds, P.L. 2000."Non-intrusive security requirements for third generation mobile systems", *Proceedings of PG Net 2000– 1st Annual Postgraduate Symposium on the Convergence of Telecommunications,Networking and Broadcasting*, Liverpool, UK, 19-20 June 2000, pp7-12.

Rodwell, P.M, Furnell, S.M. and Reynolds, P.L. 2001. "A Conceptual Security Framework to support Continuous Subscriber Authentication in Third Generation Mobile Networks", *Proceedings of Euromedia 2001*, Valencia, Spain, 18-20 April 2001. pp135-138.

orange tm

http://www.plymouth.ac.uk/nrg