Non-intrusive security requirements for third generation mobile systems

P.M.Rodwell[†], S.M.Furnell[†] and P.L.Reynolds[‡]

[†] Centre for Communications, Networks and Information Systems, Department of Communication and Electronic Engineering, University of Plymouth, Plymouth, United Kingdom
[‡] Orange Personal Communications Services Ltd, St James Court, Great Park Road, Bradley Stoke, Bristol, United Kingdom

Abstract

The next few years will witness the emergence of third generation mobile technologies, such as the Universal Mobile Telecommunications System (UMTS). The increased bandwidth available will enable the support of significantly wider application scenarios than the voice telephony and basic data services of current networks. This expansion of services will also demand a corresponding increase in the level of protection provided by the devices and network operators. This paper considers the security requirements of UMTS, with particular focus upon subscriber authentication techniques, comparing them against the more basic measures that have been considered satisfactory within second-generation systems such as GSM.

1 Introduction

The world wide market for mobile phone technologies has experienced dramatic growth in recent years. Statistics from October 1999 indicated that there were 376.5 million subscribers (with a growth of 52.5% having been experienced in the previous twelve months) and the forecast market by 2003 will exceed one billion (Intekom, 1999). The mobile technologies themselves have already evolved from the voice-only analogue systems of the mid to late 1980s, to the current second generation (2G) systems, introduced in the early 1990s. These systems, based upon digital technology, have enabled mobile data links, albeit at rather limited rates (e.g. 9.6 Kbit/s). Second generation networks are currently being enhanced with a range of data-oriented developments, designed to increase both the capacity of the air interface (e.g. the General Packet Radio Service, GPRS) and the range of mobile data services (e.g. the Wireless Application Protocol, WAP). However, by 2001, it is expected that these technologies will begin to be superseded by third generation (3G) systems such as UMTS, the Universal Mobile Telecommunications System (UMTS Forum, 1998).

UMTS aims to provide a complete, global system and offer a broadband service of up to 2 Mbit/s. This increased capacity will facilitate a fundamental improvement in mobile services, offering the potential for true multimedia capabilities. As such, UMTS is seen as the natural evolutionary path for both subscribers and operators, and a competitive market can already be seen to exist. At the time of writing, the auction of five UMTS licenses in the UK have all attracted bids in excess of £3.5 billion from new and existing network operators (Rushe and Oldfield, 2000).

As service opportunities advance, so to do the requirements to protect subscribers and network operators from the possible effects of fraud and unauthorised use. This paper considers the security requirements for 3G systems, comparing them to the established security practices utilised within 2G networks. Specific requirements are considered from the subscriber perspective, leading to the identification of a requirement for non-intrusive methods that do not impede legitimate activity.

2 Security in second generation systems

The most widespread 2G system is the Global System for Mobile Communications (GSM) (Mouly and Pautet, 1992), which, by September 1999, accounted for 344 operational networks across 127 countries (GSM Association, 1999). Security provision in GSM networks is largely geared towards secure communication (i.e. radio interface encryption) and terminal-based authentication. The latter is achieved via the combination of the Subscriber Identity Module (SIM) and the International Mobile Equipment Identifier (IMEI). The SIM holds the subscriber's personal information, such as contact numbers and text messages that have been sent and received. The SIM also contains the International Mobile Subscriber Identity (IMSI), enabling the subscriber to be uniquely identified, irrespective of the handset into which their SIM may be placed. The terminal itself can be uniquely identified via the IMEI number. This can be used in conjunction with the operator's Equipment Identity Register (EIR) database to determine the status of a device. This status will indicate that the terminal is either white-listed (i.e. allowed to access the network), grey-listed (i.e. under observation for possible problems) or black-listed (i.e. not permitted to connect to the network as it has been reported as stolen or is not of an approved type). This provides a good level of access control between the terminal devices themselves and the network.

Relatively little attention is paid to the authentication of the person using the handset or their access to services. Authentication of the subscriber to the terminal is normally achieved via a Personal Identification Number (PIN), which is also held in the SIM. This is a facility that the subscriber must enable on the handset before any protection is provided and, assuming they have done this, the level of protection can still vary between devices. On some systems, the PIN will only be invoked when the handset is first switched on, whereas on others the subscriber also has the option to put the device into a 'locked' state whilst it is still in standby mode (requiring PIN entry before further actions are possible).

Having said this, PIN protection can generally be considered commensurate with the level of risk associated with unauthorised use. Unless the terminal is lost/stolen (in which case the subscriber would be expected to report it and access would be denied by the operator), the window of opportunity for unauthorised use by an impostor who has breached the PIN would be relatively brief, with relatively contained potential consequences.

3 Requirements for security in third generation devices

The proposed services of UMTS (Cox, 1997) demand a more secure subscriber-based authentication system in order to protect personal information in the event of masquerade attacks. On a typical second-generation handset, the consequences from theft or impostor access can be broadly grouped into two categories:

- financial loss, as a result of the thief making calls at the legitimate subscriber's expense (depending upon the policy of the operator, these losses may not be passed on to the subscriber once the handset is reported as stolen).

- breach of personal privacy, as a result of the names of the subscribers' contacts and their phone numbers being held within the SIM card. 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.

When considering the nature of a 3G device, however, the potential consequences become more severe. The reason for this is that we are likely to witness convergence with Personal Digital Assistant (PDA) type devices and an expansion in the range of possible services that can be accessed. As such, a device might also store:

- financial details to enable mobile commerce payments;
- electronic certificates for digital signatures;
- full contact details of friends and associates;
- miscellaneous information of a commercially sensitive or private nature (e.g. entered into scheduler or notepad applications).

The need for security within UMTS has already been recognised and relevant standards work is progressing in a number of areas, including (3GPP, 2000):

- definition of a UMTS security architecture and specification of underlying elements;
- detailing of security requirements for UMTS service provision (e.g. user access, billing fraud control) and physical network elements (e.g. user identity module, core network and interfaces to non-UMTS networks);
- requirements specification of cryptographic algorithms;
- development of security guidelines.

Aspects such as these will inform the implementation of UMTS networks and services by the international community.

One significant consideration is whether security monitoring should reside within the subscriber's terminal or within the network. Compared to GSM, UMTS does not share the concept of a home network – the 'universal' aspect suggested in the name is based upon roaming between operators to suit the service required. This indicates a need for security to be focused within the handset, as to rely on it within the network will only be as strong as the weakest link (in terms of operators). However, a counter-argument is that UMTS also supports personal mobility, where a subscriber may register with any terminal (fixed or mobile) in order to access services. In this scenario, the subscriber's profile would need to be accessed from the network in order to determine valid services. A terminal-based approach has the advantages that the confidentiality of security details is in the hands of the subscriber, as opposed to being held by the network operator. In addition, authentication and supervision may be performed without imposing any network traffic overhead and independently of link/bandwidth availability. With network-centric monitoring, details would need to be collected on the terminal and then transmitted for remote analysis. A hybrid approach is likely to represent the most appropriate solution.

In addition to terminal and network security, certain services, such as e-commerce, may also incorporate their own security safeguards in addition to the standard facilities within the network and the terminal. This can already be seen to be the case with current e-commerce web sites, which typically require supplementary identification and authentication via their own usernames and passwords before the user is permitted to make purchases.

4 Non-intrusive security options

Even in 2G systems, PIN codes do not represent an ideal form of subscriber authentication. Their use can be criticised in a similar manner to traditional passwords in desktop IT systems, in that subscribers may introduce vulnerabilities by sharing them with other people or writing them down (Jobusch and Oldehoeft, 1989). In addition, PINs can be considered to be intrusive, as they require specific actions from the subscriber in order to authenticate themselves. Where a subscriber wishes to make a relatively quick call or mobile-based transaction, the need to firstly enter a PIN can be considered a hindrance. As a consequence, many subscribers do not make use of the facility to lock their handsets between transactions (leaving them in a vulnerable state if lost or stolen). Ideally, there is a requirement for non-intrusive or transparent protection measures, such that the provision of security does not unduly interrupt or inconvenience the legitimate subscriber.

One of the stated requirements for secure UMTS 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.

There is already a significant emphasis upon subscriber profiling in order to counter fraud, with operators applying data analysis techniques to network data in order to identify and flag potentially fraudulent transactions (Modisette, 1999). The same principles could be extended to address user authentication (i.e. to prevent masquerade attacks) and anomaly detection. Profiling could encompass factors such as the types of services typically accessed and the times/durations of access in order to construct a model of the subscriber's normal behaviour. Such techniques have been the focus of work in the general IT domain for some time and have been incorporated into network-based intrusion detection systems (Porras and Neumann, 1997).

The features of 3G terminals that will enable more advanced subscriber services will also offer the potential to facilitate more advanced security options. For example, a number of biometric approaches (Cope, 1990) could conceivably be integrated in a non-intrusive manner, depending upon the nature of the mobile device and the service being accessed. Suitable options might include:

- voice verification, for use in traditional voice-telephony scenarios;
- facial recognition, for videophone applications;
- fingerprint recognition, to detect that the correct person is holding the handset (such a technique has already been incorporated into current devices, such as the Sagem MC 959 ID – see www.sagem.com);
- keystroke analysis, enabling verification of identity from keyboard/keypad interactions (Furnell et al. 1996);
- handwriting recognition, in scenarios where the user may interact via a pen and touch-screen combination.

Such information could be gathered to facilitate real-time identity verification, leading to progressive withdrawal of accessible services (e.g. e-commerce transactions, international call capability) as more potential problems are identified. Anomaly detection could also be based upon current activity, matching overall rules that have been determined to suggest anomalous conditions. Significant departures from the subscriber profile could trigger further levels of response, such as total locking of the terminal and initiation of contact with a human intermediary (from the network operator), who could then take further steps to verify the users legitimacy.

It is considered that information such as that listed above could be most usefully 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 (as previously mentioned), 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 figure 1 below. The approach would be non-intrusive in the sense that the terminal user would be unaware of the security system unless compromise is suspected.

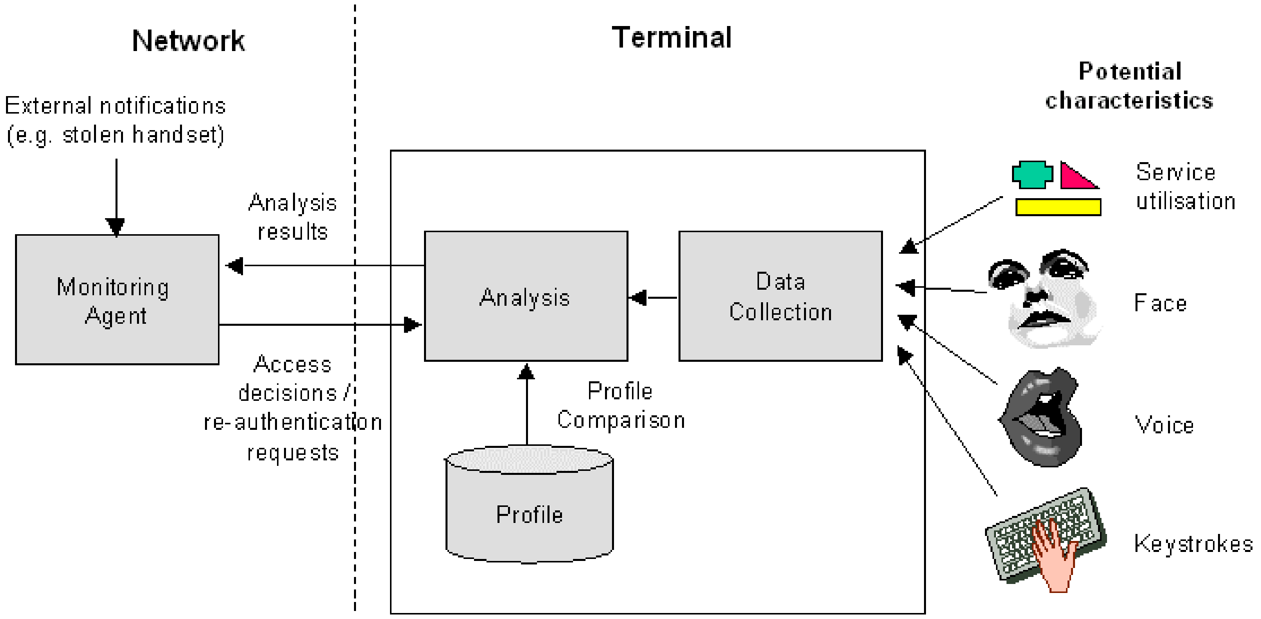

Figure 1: Potential subscriber monitoring scenario

In this scenario, PIN or password-based methods could still be utilised, but would represent a baseline approach, invoked only when other monitoring methods are not able to provide sufficient data for conclusive analysis. The authors are currently in the early stages of a research project addressing these issues.

5 Conclusions

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. This paper has identified the requirement for non-intrusive methods of subscriber authentication and supervision. Further work is required in order to establish an appropriate monitoring framework and the monitoring methods best suited to mobile application. While biometric systems have been evaluated in the context of desktop IT systems, little work has been conducted to assess their effectiveness in the mobile environment. As such, further research is required to determine whether existing methods can be tailored or, indeed, whether new approaches can be identified.

References

3GPP. 1999. *3G Security: Security Threats and Requirements*. 3rd Generation Partnership Project. Technical Specification Group Services and System Aspects. Document 3G TS 21.133 version 3.1.0).

3GPP. 2000. *Terms of Reference: Services and System Aspects – Working Group 3*. TSG SA WG3 – Security. http://www.3gpp.org/TSG/ToR/TSG-SA/sa3-tor.htm

Cope, B.J.B. 1990. "Biometric Systems of Access Control". *Electrotechnology*, April/May: 71-74.

Cox, A. 1997. "New Services for UMTS". *Proceedings of UMTS – The Next Generation of Mobile*, London, UK, 27-29 October 1997.

GSM Association. 1999. "GSM Worldwide Networks on Air". GSM Association, 'GSM World' website. 6 September 1999. http://www.gsmworld.com/membership/networks_on_air.html.

Furnell, S.M.; Green, M.; Hope, S.; Morrissey, J.P. and Reynolds, P.L. 1996. "Non-Intrusive Security Arrangements to support Terminal and Personal Mobility". *Proceedings of EUROMEDIA 96*, London, UK, 19-21 December 1996: 167-171.

Intekom. 1999. "Latest Global & Regional Cellular Statistics - World Cellular Indicators". http://home.intekom.com/cellular/statistics_latest.htm.

Jobusch, D.L. and Oldehoeft, A.E. 1989. "A Survey of Password Mechanisms : Part 1", *Computers & Security*, Vol. 8, No. 7: 587-604.

Modisette, L. 1990. "State-of-the-Art in Preventative Fraud Systems". *Proceedings of The 1999 GSM World Congress – Day 2*. Cannes, France, 23-25 February 1999.

Mouly, M. and Pautet, M. 1992. *The GSM System for Mobile Communications.* Mouly and Pautet, 4 rue Elisee Reclus, F-91120 Palaiseau, France.

Porras, P.A. and Neumann, P.G. 1997. "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances", *Proceedings of 20th National Information Systems Security Conference*, 9 Octber 1997.

Rushe, D. and Oldfield, C. 2000. "The biggest game in town", The Sunday Times, Business Focus, 16 April 2000: 3.

UMTS Forum. 1998. *The Path towards UMTS – Technologies for the Information Society*. Report no. 2. The UMTS Forum. http://www.umts-forum.org/reports.html