A CONCEPTUAL SECURITY FRAMEWORK TO SUPPORT CONTINUOUS SUBSCRIBER AUTHENTICATION IN THIRD GENERATION MOBILE NETWORKS

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

KEYWORDS
UMTS, Continuous Authentication, Security, RM-ODP.

ABSTRACT

This paper discusses a conceptual framework addressing the issue of continuous subscriber authentication for 3rd generation mobile networks, based upon the International Telecommunications Union Reference Model for Open Distributed Processing (RM-ODP). Security provisions within current 2nd generation mobile networks such as GSM, are primarily aimed at secure communications through data encryption and *terminal* authentication via use of a smart card (SIM). Proposed services of the Universal Mobile Telecommunications System (UMTS) demand a more secure subscriber based authentication system, in order to protect personal information in the event of masquerade attack. Any authentication technique will be an integral part of an overall real-time security framework in order to offer continuous protection. In exercising the first three viewpoints of the RM-ODP, a summation of key security issues and a conceptual framework presented.

INTRODUCTION

It is not difficult to see that we are currently in the middle of a mobile communications revolution. From the appearance of mobile communication devices in school playgrounds, to more abstract applications of the technology, such as GSM equipped clothing (Philips, 1999). Owing to its circuit switched nature and a limited bandwidth of only 9.6kbit/s, it is recognised that the current GSM air interface is only *practically* suitable for voice telephony, text messaging and rudimentary data services. However, the next few years will witness the evolution of GSM technologies into a wireless Internet of advanced packet switched data services exhibited by the General Packet Radio Service (GPRS) and Enhanced Data rates for GSM Evolution (EDGE) standards; culminating sometime in the next few years in 3rd Generation (3G) networks. Proposed by the International Telecommunications Union (ITU) initiative, IMT-2000, 3G mobile communications for Europe will come under the banner of UMTS (UMTS Forum, 2000). The proposed increases in bandwidth available will enable service providers to support significantly wider application scenarios than voice and the rudimentary data services of current cellular networks. This expansion of services, especially data services and the subsequent increase in personal and private data, will demand a parallel and corresponding increase in the level of protection provided by the terminal devices and the associated network operators.

This paper will introduce and justifying one of the most important of these security requirements; enhanced subscriber authentication; proceeding to discuss key issues pertaining to a conceptual security framework capable of supporting alternative advanced authentication techniques, in addition to the principle of non-intrusive and continuous monitoring. Although this paper does not discuss any specific continuous authentication mechanisms, the bias is towards biometrics, owing to its inherent suitability to non-intrusive application. (Biometrics Consortium, 2000).

The framework discussed in this paper takes a top-down approach to the problem, introducing and discussing the relevant issues through the use of the ITU Reference Model for Open Distributed Processing (RM-ODP).

ENHANCED AUTHENTICATION - A 3RD GENERATION REQUIREMENT

When considering the proposed services of UMTS (Cox, 1997), and the nature of future 3G devices, we realise that a more secure subscriber-based authentication system is essential in order to protect personal information in the event of masquerade attack (3GPP, 1999). A primary reason for this is the hastening convergence of mobile devices with Personal Digital Assistant (PDA) type devices, and the subsequent expansion in the range of possible services enabled as a consequence. In spite of the impoverished Man-Machine Interface (MMI), inherent to these devices (Nielsen, 1999), there is still a growing trend towards Internet style services through developments like the Wireless Application Protocol (WAP), Europe and I-Mode, Asia. The potential consequences, therefore, of masquerade attacks are far more severe owing to the additional and more personal information that these mobile/PDA devices are now storing and exchanging:

- financial details facilitating m-commerce
- electronic certificates for digital signatures
- full contact details of family and associates
- commercially sensitive miscellaneous information (e.g. scheduler/notepad files)

A key aspect of any proposed security framework is the balance of storage and distribution of the sensitive subscriber signature data within the communications device (handset) and across 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. In order to support true personal mobility, where a subscriber may register with any terminal interface (fixed or mobile) in order to access services, profiles need to be distributable throughout the network. The subscriber's profile could theoretically be accessed from any point within any compliant network in order to authenticate access to valid subscribed services. In such a network-centric monitoring solution, security details would be collected on the terminal and then securely transmitted and securely stored within the network for remote analysis.

REFERENCE MODEL OF OPEN DISTRIBUTED PROCESSING

The Reference Model of Open Distributed Processing (RM-ODP, 1994) was a joint effort by the International Standards Organisation (ISO) and the ITU-T to develop a coordinating framework for the standardisation of open distributed processing (ODP), supporting heterogeneous interworking between systems. The model describes an architecture, integrated into which are distribution, interworking, interoperability and portability. The RM-ODP framework takes a top-down approach, defining five abstract system viewpoints: Enterprise, Information, Computation, Engineering and Technology. The different viewpoints enable one to move progressively away from the conceptual world of user interfaces and enter into the tangible world of the supporting technologies and hardware infrastructures.

Viewpoints

The prescriptive framework, RM-ODP Part-3, proposes five viewpoints decomposing the specification of the ODP system, focusing on the separate concerns. Using the conceptual structures, rules and functions, a fundamental defining framework is generated specifying and bounding the proposed ODP system.

The five viewpoints of the RM-ODP are briefly categorised as follows:

- Enterprise Viewpoint: Purpose, Scope & Policy analysis. Organisational policies and requirement, performative actions.
- Information Viewpoint: Semantics and Information Processing. Required information through the use of Schemas.
- Computational Viewpoint: Functional Decomposition. Functionality of ODP application, object handling.
- Engineering Viewpoint: Infrastructure to support the distribution.
- Technology Viewpoint: Technology required for implementation.

Using this top-down approach, a large and complex system specification can be broken down into smaller, separate and manageable pieces, each focusing on the associated relevant issues to a particular working group.

CONCEPTUAL FRAMEWORK TO SUPPORT CONTINUOUS MOBILE AUTHENTICATION

This section addresses conceptual issues when considering techniques for discrete real-time authentication over a mobile communications network. The discussion covers the first three viewpoints of the *Requirements Analysis* and *Functional Specifications* sections of the RM-ODP schematic, Figure 1.

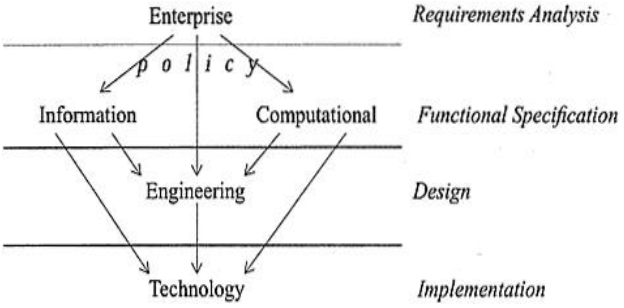

Figure 1: RM-ODP Viewpoints

Low level engineering and hardware infrastructure issues have not been considered at this stage.

Enterprise (Business) Viewpoint

The enterprise viewpoint, addresses the performative actions governing the proposed framework. This is achieved through the use of active and passive *objects*, where an object is any unique entity within the framework; groups of objects or *object communities*, purposefully grouped to achieve a larger goal; and object permissions/prohibitions or *roles of objects*.

Top Level Objects

Under normal operation, there is only one *active* object within the security framework:

- the subscriber.

In the extreme case that the system is unable to resolve a security issue virtually, a human operator could intervene in the decision making process, but essentially and for the majority of the time, the subscriber will be under autonomous control of the network.

The passive objects forming the top of the framework:

- the mobile network *(community)*
- the network interface handset *(community)*
- the subscriber account
- the archived subscriber reference profile
- the handset generated subscriber profile
- subscriber data packets
- subscriber payments (money)

Treating the network and handset as single entities/object communities, negates the need to break them down into their hardware infrastructures. Separate payment objects recognise that some subscribers prefer to pay in advance via tokens rather than contractual schemes. As these objects are not authentication issues, they will not be included in subsequent discussion.

Communities
The primary top-level object communities consist of 'the network, the subscriber account, the subscriber profile' and 'the interface handset, the subscriber authentication profile'; both objects share the data and subscriber objects.

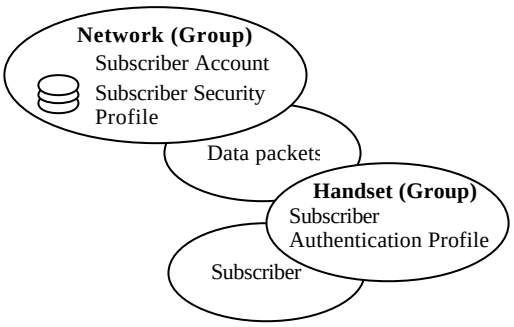

Figure 2: The Enterprise Objects

Roles of Objects
Identifying the rules bounding the objects within the conceptual framework through:

- Permissions - What *CAN* be done
- Obligations - What *MUST* be done
- Prohibitions - What *MUST-NOT* be done.

Permissions:
A subscriber can choose to:

- access their network account at any time.
- change their network interface handset.
- terminate their account at any time.

The network can choose to:

- issue an authentication challenge at any time.
- maintain more than one profile for each subscriber.

Obligations:
A user:

- must have a valid network account.
- must continuously satisfy authentication.
- must sufficiently fund their network access.

The network:

- must automatically act on authentication failure.
- must provide suitable protection of subscriber profiles; under legislation like the EU Data Protection Directive (Lloyd, 1996).

Prohibitions:
A subscriber:

- can only access *their* account.
- cannot initiate authentication profile changes.
- cannot bypass authentication.
- authentication profile cannot be artificially generated by any casual/non dedicated means.

Information Viewpoint
This viewpoint presents the schemas involved with handling the state and structure of the pre-defined data object schemas at particular times:

- Static - state of an object at a particular time.
- Invariant - restricts state/structure at all times.
- Dynamic - defines permitted state changes.

Static schemas

- At Point-Of-Entry, any user is unauthenticated.
- At network defined intervals, fixed or system variable, authentication is transparently requested.

Invariant schemas

- Continuous authentication is always active.
- The network handset must be authenticated to access the network.

Dynamic schemas
A subscriber:

- state change - authenticated to unauthenticated.
- profile is permitted to change over time; e.g. with age, health, behaviour etc.
- is permitted to change their handset(s) over time without affecting archived profiles.

Computational Viewpoint
This view specifies the functional interactions between system objects at a low level. From this viewpoint, it can be argued that the required authentication may exist at several levels, as illustrated in Figure 3.

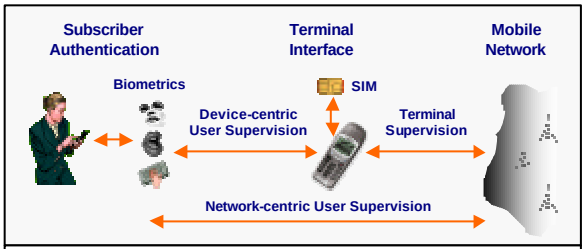

Figure 3: Mobility Authentication

It is considered that a suitable framework for achieving this is not dissimilar to previous security work carried out in the area of real-time network monitoring; i.e. The Intrusion Monitoring System (IMS), (Furnell, S.M., Dowland, P., 2000). Building on this work, it can be demonstrated that with suitable modifications, the IMS can be remodelled to meet the requirements of a continuous authentication system for mobile applications, where a detected anomaly is represented by a failed subscriber authentication. Considering the architecture in a purely authentication-based role (i.e. where misfeasor abuse is not considered), a suitable conceptual structure is shown in Figure 4.

In this revised structure, the client is represented by the subscriber handset and several of the modules have been renamed from the original IMS to reflect the more restricted authentication-only role (on the network side, the Archiver function has been removed altogether – reflecting the fact that the system is looking to perform real-time authentication rather than ongoing activity monitoring). The authentication function need not reside

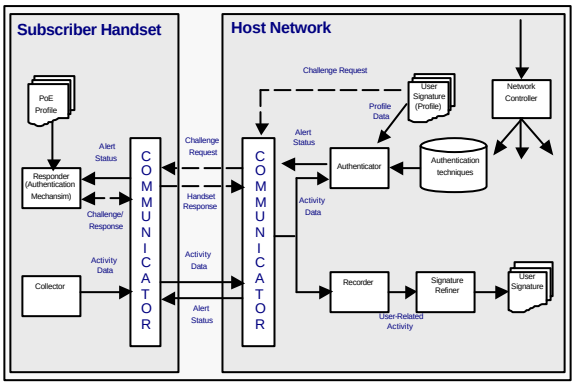

Figure 4: Enhanced Mobile Authentication System

completely within the network. Point of Entry (PoE) authentication in particular could reside in the subscriber terminal, using an appropriate technique as the basis (e.g. the baseline method could still be a PIN, but more advanced methods such as fingerprint recognition could also be used if the handset device was suitably equipped). However, rather than be a completely isolated function within the terminal, it could be linked into the wider network-based monitoring system. For example, the network could be notified of any handset login failures, which would enable its alert status to proceed from an initially higher starting point than it would have otherwise done in the case of a completely successful login at the first attempt. More advanced, ongoing supervision would be network-based and, in this sense, the role of the handset becomes that of collecting relevant authentication data, upon request from the host network, and then responding as instructed when the data has been remotely analysed. It can be seen that the decision making process is retained within the network under the control of the network operator's system; in this case the 'Authenticator' module. This is a fundamental security issue, offering advantages to both the operator and the subscriber: For the operator, it removes control and the possibility of casual authentication tampering from the subscriber handset, for the subscriber, it offers the service of subscriber mobility.

There can be a number of mechanisms in place to trigger the authentication challenge request process:

- a simple chronological time-out.
- significant change of destination tolling.
- change from normal usage profile, i.e. departure from normal calling pattern, etc.
- mobile cell handover, a point of potential system weakness to a system abuser.
- e-commerce transaction.

Any combination of the above should transparently trigger the re-authentication mechanism. In addition, there are other quality-of-service considerations to be addressed:

- network loading issues.
- reception conditions.
- available network bandwidth when roaming.
- remaining life-cycle of existing GSM handsets.

It can be argued that a brick wall lock out is not necessarily the best solution to authentication failure. As mentioned previously, quality of service is critical, and a low False Rejection Rate is fundamental to any continuous authentication scenario. It is advisable to exercise a form of phased service lockout, ranging from basic logging of user activity to a complete system bar.

CONCLUSIONS

This paper introduced and justified the need for improved subscriber authentication within the next generation of mobile communication devices. Through the approach of the ITU RM-ODP, the rules for a conceptual discrete real-time authentication framework have been generally defined and, through on going work on the IMS at the University of Plymouth, a suitable core architecture proposed.

REFERENCES

3GPP. 1999. "3G Security: Security Threats and Requirements." Technical Specification Group Services and System Aspects. Document: 3G TS 21.133 v3.1.0.

Biometric Consortium. 2000. "An introduction to biometrics", The Biometric Consortium, http://www.biometrics.org/html/introduction.html

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

Furnell, S.M., Dowland. "A conceptual architecture for real-time intrusion monitoring", Information Management & Computer Security, vol. 8, no. 2, 65-74.

Lloyd, I. 1996. "An outline of the European Data Protection Directive". *The Journal of Information, Law and Technology*, 1996.

Nielsen, J. 1999. "The Graceful Degradation of Scaleable Internet Services", *Alertbox*, 31 October,. http://www.useit.com/alertbox/991031.html

RM-ODP, 1994. "Reference Model of Open Distributed Processing". Standards: ISO #10746. ITU-T #X.900.

BIOGRAPHY

Philip Rodwell was educated in Communication Engineering at the University of Plymouth, England; where he received his B.Eng. Honours degree in 'Personal Communications and Networks'. The programme included a one-year placement at Philips Consumer Communications, Le Mans, France; where he was part of the DECT team responsible for developing the software for the Xalio range of cordless products. He is currently studying for his PhD within the Network Research Group at the University of Plymouth, researching 'Non-Intrusive Security Systems for 3rd Generation Mobile Networks', in association with Orange PCS, Bristol, England.