ASPeCT – Securing the future for mobile communications

Nigel Jefferies

Vodafone Ltd, The Courtyard, 2-4 London Road, Newbury, Berks RG14 1JX, UK

Abstract

In this paper, we summarize the objectives and results of the ACTS ASPeCT project, and assess its contribution to the development of a secure third-generation mobile communications system.

The Objectives of the Project

The mobile telecommunications world continues to transform itself as increasing numbers of services are being offered to a growing number of users by more and more operators. It is essential for the continuing success of this process that the evolving security requirements of users and service providers are addressed in an appropriate and timely way. The aim of ACTS project AC095 ASPeCT (Advanced Security for Personal Communication Technologies) was to ensure that this could happen by implementing and running trials of advanced security features to prove their feasibility and acceptability. The project ran from September 1995 until January 1999 with the partners listed in Table 1, representing operators, manufacturers of terminals, smart cards, network and other equipment, and academic institutions.

Full partners	Associate Partners
Vodafone Ltd (Coordinator)	Haines Watts Consulting
Siemens Atea	Lernout & Hauspie
Giesecke & Devrient	Swisscom
Panafon	
Royal Holloway, University of London	
Siemens AG	
K.U. Leuven	

Table 1: ASPeCT partners

The general objective of the project was:

- to study the feasibility and acceptability of new and advanced security features in existing and future personal communication networks, based on trials and demonstrations.

Further to this, the detailed objectives of this project were to investigate, implement and test in trials, solutions in the following areas:

- migration from existing mobile telecommunications systems to UMTS;
- fraud detection in UMTS;
- trusted third parties for end-to-end services in UMTS;
- capabilities of future USIMs;
- the security and integrity of billing in UMTS.

The project produced significant results in each of these areas. After reviewing the background to security for third-generation mobile systems, we will review each of these.

Security in Mobile Communications Networks

For obvious reasons of practicality and limited resources, the project could not encompass all envisaged communications networks. Therefore ASPeCT focused on the security aspects related to a particular system, namely UMTS as being standardised by 3GPP and ETSI. The results of the project provided useful input to this standardisation process during the project's lifetime.

Existing personal communications networks were taken into account solely from the point of view of migration towards UMTS. Concrete solutions were developed in this project for UMTS only. However, the application of some of the results to other systems is also possible.

Furthermore, as indicated in the objectives, the project concentrated its efforts on a subset of the security features in UMTS. These were the ones that are new and advanced, in the sense that they have no analogue in existing systems and are expected to be crucial for the success of UMTS.

Existing mobile and cordless telecommunications networks, such as those conforming to the ETSI GSM and DECT standards, already provide certain essential security features, primarily designed to address the vulnerability of the air interface. One of the most fundamental problems that will be faced by operators of existing networks will be to evolve the current security features towards the more sophisticated and all-embracing set of security features likely to be necessary for UMTS/3GPP networks. This will, in particular, raise questions about the possible functionality that can be provided by existing and future User Service Identity Modules (USIMs) - the smart card application for access to UMTS/3GPP networks.

A further problem is posed by the ever-present threat of fraud, which second-generation security features have only partly addressed. New techniques for detecting fraudulent behaviour will need to be brought into use, following the lead currently being set by large financial organisations.

Totally new, and in particular end-to-end, security features are required to address many new application domains for mobile telecommunications networks; the possible ramifications for European business are immense, and the likely end-to-end security requirements are wide-ranging.

Disputes about bills, often connected with cases of fraud, have increasingly become a problem for users, service providers and network operators with serious economic and legal implications for all parties involved. Therefore, features guaranteeing the security and integrity of billing that help to settle these disputes are urgently needed. Although the issue of the security and integrity of billing is of concern to many other systems, UMTS is a good candidate to implement corresponding measures as the users are equipped with a security module (the USIM) and the design of UMTS can still be influenced.

Results of the ASPeCT project

The ASPeCT project has made significant contributions to enhancing the security of the next generation of mobile communications systems in a number of areas, as was intended in the project's original objectives. It is worth reviewing these briefly to get an idea for what the project has achieved, and how the results will be carried forward. The project can be divided into three main areas: work focussing on authentication and the USIM, work to do with trusted third parties and their use to support a secure billing protocol for value-added services, and work on the detection of fraud in mobile systems.

Final public reports from the project [1,2] contain a detailed exposition of the main results.

UMTS authentication and the USIM

The authentication framework

In view of the continuing uncertainty during the project's lifetime regarding the evolution from GSM to UMTS, the original objective of securing the evolution and migration between the generations was refocussed. The project worked on achieving a flexible protocol, which

allowed maximum choice of authentication algorithm and permitted negotiation on dynamic roaming agreements as well.
The principle objective of the ASPeCT authentication framework is to provide a flexible procedure for user-network authentication allowing a number of different mechanisms and algorithms to be incorporated, with the ability to migrate smoothly from one mechanism to another. This framework allows the authentication capabilities of USIMs, network operators (NOs) and service providers (SPs) to be taken into consideration for the selection of the mechanism to be used. A list of capability classes (including the mechanisms supported) is maintained so that the different entities can permit the negotiation of the mechanisms to be used.

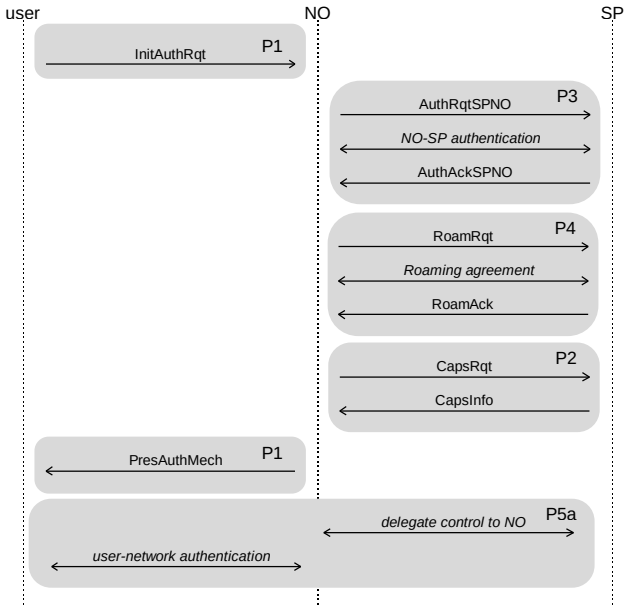

Figure 1: Operational scenario for 'User not registered, no roaming agreement'

To facilitate roaming in a network with many NOs and SPs, roaming agreements should be set up dynamically as required. A roaming agreement would be requested after an initial authentication request sent by the user/terminal to an NO visited for the first time. A prerequisite is that the SP and NO involved have authenticated each other. This will be carried out using a globally agreed mechanism to ensure that all NOs and SPs have the capability to authenticate each other. Flexibility to change mechanisms is not a crucial factor. NO-SP authentication also permits the SP to delegate user-NO authentication to the NO.
The Authentication Capability Class (ACC) identifies the particular authentication mechanisms supported by the USIM. Each respective mechanism has a unique identifier, so visited NOs can immediately identify whether they can support a particular ACC; unknown mechanisms would be defined by the respective SP upon request from the NO.
As an example, the operational scenario is shown in Figure 1 where a user, not registered in the network, initiates authentication and no roaming agreement exists between the NO and the user's SP.

Public-key authentication for UMTS

A new protocol was developed in ASPeCT for authentication between user and network; it was particularly designed to fit the performance constraints of mobile networks. Its design exploits the advances in two fields: Crypto-controller smart cards (which have a co-processor which efficiently supports public-key cryptographic mechanisms) and elliptic-curve cryptosystems (which permit the use of smaller cryptographic parameters). The new protocol was successfully implemented and tested in ASPeCT. This included showing that UMTS and GSM applications can coexist on a single smart card.

Speech-based verification of users

Biometric demonstrations showed that speaker recognition could be used to authenticate users to their smart cards, with the support of the terminal. The techniques were reported in [4]. Since then, the vocal part of the demonstration has been enhanced and shown in public at the IS&N 98 conference in Antwerp, Belgium.

Additional work included simulating a microphone swap between training the user and actual use. The robustness of the system against microphone swap was investigated and was found to give rise to a 50% increase in false rejection rate on a single password verification trial.

A study also investigated the feasibility of a split of the algorithm over the terminal and smart card. This would have the advantage of making maximum use of the secure environment on the card, and the superior processing capabilities of the terminal. An investigation of the minimal memory and I/O buffer sizes of the different modules was carried out. A straightforward algorithmic split that is compatible with near future card constraints seems infeasible. More detailed results can be found in [1].

Secure payment for value-added services

Trusted third parties in mobile communications

Extensive investigations have been undertaken into the use of trusted third parties (TTPs) for mobile communications networks. The services that could be provided using TTPs have been assessed. A compact certificate format has been developed, suitable for the mobile environment. A systematic approach to the analysis of key escrow schemes has been developed.

TTPs allow users to establish confidential communication channels with other users, possibly in different countries, whilst being able to satisfy law enforcement requirements at both the national and international level by allowing the recovery of confidentiality keys under appropriate controls - such as an extension of a search warrant.

The ASPeCT TTP provides UMTS users with a mechanism to support end-to-end confidentiality of communications. In our model, two users who wish to communicate with each other make use of the key management services provided by a TTP infrastructure to support the establishment of a shared secret confidentiality key to be used in a symmetric cryptosystem. We assume that each user belongs to a *domain* (perhaps a country) and that they only directly communicate with a *home TTP*, which is a TTP associated with their domain.

An important feature of the mechanism is that some information used to generate the shared secret confidentiality key is escrowed to the TTPs. Thus, the demonstrator offers a mechanism whereby an *interception agent* can obtain the information, which may then be used to decrypt targeted communications.

Key recovery relating to ASPeCT protocols is discussed in more detail in [6].

A payment model for mobile users of value-added services

The micropayment system used in ASPeCT is applied to pay for the provision of valued added services that provide information to the user based on Worldwide Web technology. The novelty is not the payment protocol itself, but the way in which it is integrated with the authentication protocol proposed for the mobile system UMTS and the payment scenario for basic and value added services in UMTS.

ASPeCT has developed a protocol to show how mobile users can pay for access to information services in a flexible, efficient and secure way. The method has potential application to charging for any telecommunications service.

It is expected that the number and variety of value added services (VASs) will greatly increase while current networks are evolving towards UMTS. The charging for today's VASs typically consists of a basic charge for the telecommunication service and a premium for the value added service. Both are usually based on the duration of the call. In the future, more flexible charging schemes for the premium would be desirable. Flexibility relates to the

parameters that determine the charge, to the variety of different possible tariffs and to the ease with which a certain tariff can be changed.
The value of a particular piece of information retrieved by a user from a VAS provider at any one time may be quite small. Therefore, the use of computationally expensive payment mechanisms may not be acceptable. In addition, the scheme has to take into consideration the specific requirements of a mobile telecommunications system. In short, the charging scheme must also be efficient.
The evolution of current mobile systems towards UMTS will see the emergence of many new network operators, service providers and VAS providers. This will have serious implications for the trust relations among them. It will be increasingly important that the charging scheme is secure against cheating, and that parties involved should have the assurance that justified claims relating to charges can be proved and that unjustified claims cannot be successfully made. This is called incontestable charging.
Our approach is via a credit-based micropayment scheme based on tick payments, as described in [5].

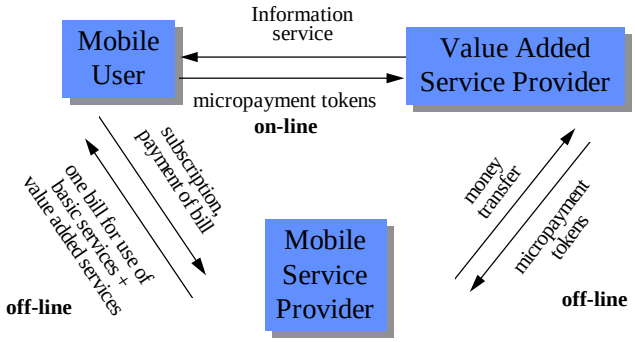

Figure 2: The ASPeCT billing model

In our model (see Figure 2) the user has a subscription with a UMTS service provider. The charge for using a VAS is composed of two parts:

- a basic charge for the provision of the communication link between the user and the VAS provider by the network operator and;
- a premium for the value added, paid to the VASP.

The subscriber enters into contractual relationship with the SP on behalf of the user. Any payment scheme for the protection of the premium has to be run between the user and the VASP. The fact that the network operator need not be involved has the advantage that the implementation of security enhancements to existing VASs requires no modifications to whatever network is providing the connection. The only changes that are necessary are software changes at the end-points of the communication. In this way, the solution is not restricted to UMTS.
The only on-line communication required in the charging procedure is that between the user and the VASP while the service is being provided. The VASP will forward the information proving his claims on the user to the SP (possibly through the NO) off-line who in turn will bill the user, also off-line. The SP will also take care of the payments to NOs providing the connectivity.

Detecting fraud in mobile communication systems

The ASPeCT project demonstrated the feasibility of a solution to the problem of secure billing for the provision of services using the aforementioned authentication protocol to initiate a payment scheme. Major results of the project include the three fraud detection tools based on separate approaches to the problem of detecting and identifying instances and patterns of possible fraudulent behaviour.

- a rule based tool;
- a neural network based tool using supervised learning;
- an unsupervised learning tool utilising neural networks.

A major result of the project is the integration of these three tools, together with a fourth tool using an unsupervised learning approach to B-number analysis, into a combined tool - BRUTUS - with its own monitoring and management GUI. All the tools adopt an approach based on analysis of *user profiles* based on comparison of recent and longer-term behaviour histories derived from toll ticket data. The neural network-based tools use a differential analysis; the rule-based tool also allows absolute analysis against fixed criteria. Further details can be found in [5].
A report has been written with the objective of the determination of the legal rules applying in the various fields of law affected by the use of fraud detection systems by mobile communications operators or service providers, see [3].

The Future

ASPeCT has shown how the major security issues for UMTS can be addressed. The job of ensuring that a viable security architecture is standardized falls to a follow-up project, AC336 USECA, which is discussed in [7].

Conclusion and acknowledgements

Each of the results described has had an impact, whether on public standards, on partners' internal development plans, or on the direction of future research. The true value of ASPeCT's work will only become apparent when mobile communications are used as the standard communications tool for electronic commerce, and users' confidence in the security of the system is founded on a sound technical basis.
The author wishes to thank all the participants in ASPeCT for their contributions.

References

[1] ACTS AC095 ASPeCT deliverable D20, 'Project final report and results of trials', AC095/VOD/W31/DS/P/20/1, January 1999.†

[2] ACTS AC095 ASPeCT deliverable D25, 'Legal aspects of fraud detection', AC095/KUL/W26/DS/P/25/1, December 1998.†

[3] Phil Gosset, Mark Hyland 'Classification, Detection and Prosecution of Fraud on Mobile Networks', presented at ACTS Mobile Summit, Sorrento, Italy, June 1999.

[4] Martine Lapère & Eric Johnson, "User Authentication in Mobile Telecommunication Environment Using Voice Biometrics and Smart Cards", 4th International Conference on Intelligence in Services and Networks, IS&N '97, Lecture Notes in Computer Science, 1238 (1997) 437-444.

[5] E. Lerouge et al. 'Fraud detection in mobile telecommunications networks', presented at ACTS Mobile Summit, Sorrento, Italy, June 1999.

[6] Konstantinos Rantos and Chris Mitchell, 'Key Recovery in ASPeCT Authentication and Initialisation of Payment Protocol', presented at ACTS Mobile Summit, Sorrento, Italy, June 1999.

[7] Bart Vinck, 'A viable security architecture for UMTS', presented at ACTS Mobile Summit, Sorrento, Italy, June 1999.

† available from the project website at http://www.esat.kuleuven.ac.be/cosic/aspect/