PANA/GSM Authentication for Internet Access

Paulo S. Pagliusi and Chris J. Mitchell
Information Security Group
Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
P.S.Pagliusi@rhul.ac.uk, C.Mitchell@rhul.ac.uk

August 16, 2003

Abstract

Currently there are no Internet access authentication protocols available that are lightweight, can be carried over arbitrary access networks, and are flexible enough to be used in all the likely future ubiquitous mobility access contexts. This article proposes the PANA/GSM authentication protocol for heterogeneous network access as a step towards filling this gap. A security analysis of the PANA/GSM protocol is also provided. This article aims primarily at contributing to the design of authentication protocols suitable for use in future heterogeneous Internet access environments supporting ubiquitous mobility.

1 Introduction

Currently there are no authentication protocols available that are lightweight, can be carried over arbitrary access networks, and are flexible enough for use with all the various access technologies likely to be deployed to support future ubiquitous mobility. Furthermore, existing access procedures need to be made resistant to Denial-of-Service (DoS) attacks; they also need to provide non-repudiation. The IETF PANA (Protocol for carrying Authentication for Network Access) work aims to provide a protocol [8] that will be a network-layer authentication carrier for access networks that support IP. PANA will be capable of transporting any EAP (Extensible Authentication Protocol) method [4] to enable access authentication. In addition, the EAP/SIM protocol [9] specifies a way of encapsulating the security parameters used by the GSM (Global System for Mobile communication) system [19] within EAP. Once inside EAP, the GSM parameters can thus be carried by PANA. In this paper we present a proposal for combining GSM authentication with EAP/SIM and PANA, which we call PANA/GSM.

The goal of the PANA/GSM protocol is to provide an IP compatible, lightweight, relatively flexible and scalable authentication method that allows a client to be authenticated in a heterogeneous Internet access environment. Section 2 summarises the GSM security services, Section 3 describes the EAP/SIM protocol, and Section 4 explains the PANA protocol. Section 5 then describes the proposed new PANA/GSM authentication scheme. Section 6 analyses the threats to the PANA/GSM protocol, Section 7 considers its advantages and disadvantages and, finally, Sections 8, 9, and 10 present possible further work, conclusions and acknowledgements.

2 GSM Security Services

This section summarises the three GSM air interface security services relevant here, i.e. subscriber identity confidentiality, subscriber identity authentication and data confidentiality. Further details of GSM security can be found in [12, 19]. *Subscriber identity confidentiality* is achieved through the use of temporary identities. Apart from at initial registration, a user is not identified employing his permanent identity, i.e. his IMSI (International Mobile Subscriber Identity), but instead uses a temporary identity known as the TMSI (Temporary Mobile Subscriber Identity). To avoid user traceability, which may lead to the compromise of subscriber identity confidentiality, TMSIs are changed regularly by the visited network (VN) in an 'unlinkable' way. In addition, they are transmitted to the Mobile Station (MS) via an encrypted radio channel.

Subscriber identity authentication is used to authenticate the MS to the VN. This service is based on use of a secret key K_i, shared between the user's Subscriber Identity Module (SIM) and the Authentication Centre (AuC) of the subscriber's home network (HN). For each subscriber, and whenever necessary, the subscriber's HN selects one or more random challenge values *RAND*. Each *RAND* is input to a cryptographic algorithm A3, along with the K_i for that subscriber, and the output is known as *XRES*. A set of pre-calculated (*RAND*, *XRES*) pairs are then supplied to the VN. Whenever the VN wishes to authenticate the MS, it sends it one of the *RAND* values. The MS inputs the *RAND* along with K_i

to algorithm A3, and sends the output, known as *SRES*, back. The VN then compares the received *SRES* with the stored *XRES*, and if they agree the MS is deemed authentic. In order to provide *data confidentiality* between the MS and the VN, an encryption key K_c is also produced at the same time as *XRES*/*SRES* is generated, again as a function of *RAND* and K_i, and using a key generation algorithm A8. The key K_c is passed from the AuC to the VN with the *RAND* and *XRES* values, as part of what is known as an 'authentication triplet' (*RAND*, *XRES*, K_c), and used to encrypt user and signalling data sent between the MS and the VN.

3 EAP/SIM Method

The EAP/SIM method [9] is an EAP mechanism for authentication and session key distribution that uses the GSM SIM [19]. It involves a client acting on behalf of a user, an authenticating party, and an EAP server [4]. The EAP server, which typically belongs to the user's home Internet AAA network, is able to obtain authentication triplets from the subscriber's HN AuC. The EAP/SIM packet format and the use of attributes are specified in section 7 of [9]. Either the IMSI or the TMSI can be employed as part of the user identifier. Section 5 of [9] describes user identity management.

In EAP/SIM multiple *RAND* challenges are used to generate several K_c keys, which are combined to generate a 'more secure' key than can be obtained from individual GSM triplets. In EAP/SIM authentication, a Master Key (*MK*) is first derived using the hash function SHA-1 [11] from a combination of the user's identity, n GSM confidentiality keys K_c (n = 1, 2 or 3), the *NONCE_MT* random number freshly generate by the EAP client, and other relevant context information, e.g. the identifier of the EAP/SIM version in use. Keys derived from the *MK* are subsequently used to generate temporary session keys for authentication, encryption, and IV-generation. This includes the EAP/SIM Master Session Key (*MSK*) for encryption of the traffic between the client and the network, the authentication key to be used with the Message Authentication Code attribute (AT_MAC), and the encryption key to be used with the data encryption attribute. EAP/SIM enhances GSM authentication by accompanying the *RAND* challenges and other messages with a *MAC* in order to provide mutual authentication. Finally, EAP/SIM includes optional identity privacy support, and an optional re-authentication procedure.

4 PANA Carrier Mechanism

This section briefly introduces the draft PANA protocol [8], a link-layer agnostic transport for EAP to enable client-to-network access authentication. PANA runs between a PaC (PANA Client) and a PAA (PANA Authentication Agent) situated in the access network, where the PAA may optionally be a client of an AAA infrastructure. PANA carries any authentication mechanism that can be specified as an EAP method (e.g. EAP/SIM), and can be used on any link that supports IP. The header of every PANA packet contains two sequence numbers to provide ordered delivery of EAP messages: one transmitted sequence number (tseq), and one received sequence number (rseq). The payload of any PANA message consists of zero or more Attribute Value Pairs (AVPs), e.g. a cookie AVP used for making an initial handshake robust against 'blind DoS attacks' [8], a MAC AVP protecting the integrity of a PANA message, or an EAP AVP that transports an EAP payload.

Two important features of PANA, namely the security association (SA) and re-authentication, are now described. Once the EAP method has completed, a session key (e.g. the EAP/SIM *MSK*) is shared by the PaC and the PAA. The session key is provided to the PaC as part of the EAP key exchange process, and the PAA can obtain the session key from the EAP server via the AAA infrastructure (if used). PANA SA establishment based on the EAP session key is required where no physical or link layer security is available. Two types of re-authentication (or fast reconnection) are supported by PANA. The first type enters the chosen EAP method (e.g. EAP/SIM) at the authentication phase, where the initial handshake phase can be omitted. The second type is based on a single protected PANA message exchange without entering the authentication phase.

5 PANA/GSM Protocol

The PANA/GSM method proposed here involves three entities, namely the *PaC* (also referred to here as the *client*, *user* or *subscriber*), the *PAA* (*authenticating party*) and the *EAP server*. The *PaC* is associated with a network device and a set of GSM credentials stored in a SIM, where these credentials are used to prove the PaC identity for network access. A possible implementation of the PaC would be an Internet access device (e.g. a laptop) with a PC card inserted in the PCMCIA[1] socket, where the PC card is itself equipped with a GSM-enabled SIM card.

The *PAA* authenticates the GSM credentials provided by the PaC and grants network access. In the context of this document, the *EAP server* is implemented on the AAA server and has an interface to the GSM network, operating as a *gateway* between the Internet AAA network and the GSM authentication infrastructure. The PAA is thus an

[1] Personal Computer Memory Card International Association (www.pcmcia.org/).

AAA client that communicates with the user's EAP server through an AAA protocol supporting EAP (e.g. Diameter EAP [10]). PANA/GSM also involves a further entity, namely the EP (Enforcement Point), which applies per-packet enforcement policies (i.e. filters) to the traffic of the PaC's devices.

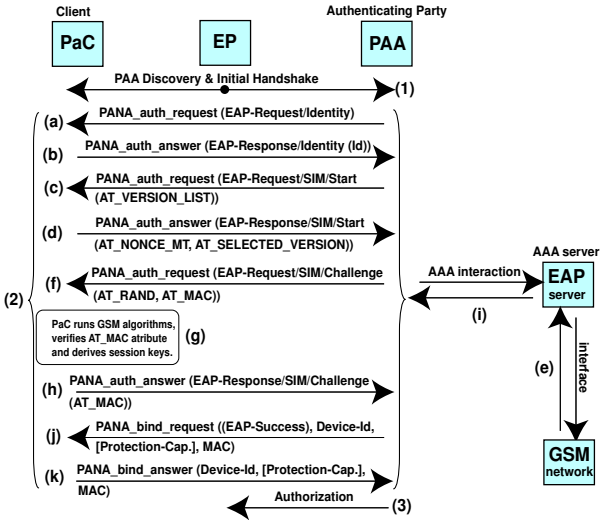

Figure 1: **PANA/GSM full authentication procedure**. The name of each message is shown, followed by the contents of the message in round brackets; square brackets are used to denote optional fields.

Figure 1 shows the PANA/GSM authentication procedure, which has three main phases: (1) Discovery and initial handshake, (2) Authentication, and (3) Authorization. In the *Discovery* phase, an IP address for the PAA is identified, and a PANA/GSM session is established between the PaC and the PAA, following the PANA model. In the *Authentication* phase, the main focus of this article and further explained below, EAP/SIM messages encapsulated in PANA/GSM are exchanged between the PaC and the PAA. At the end of this phase, a PANA SA is established, including the provision of a shared secret EAP/SIM session key (MSK); we call this the PANA/GSM SA. During the *Authorization* phase, a separate protocol is used between the PAA and the EP to manage PaC network access control. After this phase, the established PANA/GSM session as well as the PANA/GSM SA is deleted, following the PANA standard.

During the *Authentication* phase, the first PANA_auth_request message (a) issued by the PAA carries an EAP-Request/Identity payload. The PaC responds (b) with a PANA_auth_answer, which carries an EAP-Response/Identity payload including the user identifier *Id*. After that, an EAP-Request/SIM/START packet with the list of EAP/SIM versions supported by the PAA is transported in a PANA_auth_request (c). The PaC responds (d) with a message carrying the EAP-Response/SIM/Start payload, which includes the $NONCE\_MT$ random number chosen by the PaC, and the EAP/SIM version selected by the PaC. After receiving the EAP-Response/SIM/Start payload from the PAA by means of an AAA interaction, the EAP server obtains the GSM triplets from the home operator's AuC on the GSM network (e). From the triplets, the EAP server derives the keying material, as specified in section 3.

The next message issued by the PAA encapsulates an EAP-Request/SIM/Challenge payload, which contains the n $RAND$ challenges and a MAC attribute to protect the challenges (f). On receipt of this message, the PaC runs the GSM authentication algorithm and calculates a copy of the MAC, verifies that the calculated MAC equals the received MAC, and derives the EAP/SIM session keys (g). Since the $RAND$ challenges given to a PaC are accompanied by the AT_MAC, and since the PaC's $NONCE\_MT$ value contributes to AT_MAC, the PaC is able to verify that the EAP/SIM message is fresh (not a replay) and that the sender possesses valid GSM triplets for the user (the EAP server is forbidden to reuse old triplets).

If all checks out, the PaC responds (h) with a PANA_auth_answer encapsulating the EAP-Response/SIM/Challenge containing the AT_MAC attribute, which is the output of a keyed MAC function using as input the EAP/SIM payload concatenated with the PaC's *SRES* response values. After receiving the EAP-Response/SIM/Challenge payload from the PAA through an AAA interaction, the EAP server verifies that the MAC value is correct and sends back (i) the EAP-Success packet, which indicates that the authentication was successful and also carries derived keying material.

Finally the PAA encapsulates the EAP-Success packet in a PANA_bind_request message sent to the PaC (j), and receives back an acknowledgement through a PANA_bind_answer (k). Both PANA_bind messages are protected by a MAC AVP; they may also optionally contain a Protection-Capability AVP to indicate if link-layer or network-layer encryption should be initiated after PANA/GSM. They are also used to bind device identifiers of the PaC and the PAA to the PANA/GSM SA established at the end of the authentication phase.

6 Security Analysis

In this section, security threats to the proposed PANA/GSM protocol are considered.

6.1 Mutual Authentication and Triplet Exposure

PANA/GSM provides mutual authentication via the EAP/SIM mechanisms. The PaC believes that the PAA is authentic because the network can calculate a correct AT_MAC value from the *RAND* challenges in the challenge request. The PAA believes that the PaC is genuine because the *MAC* computed from the *SRES* response values is correct. Moreover, PANA/GSM validates the EAP AVP through its PANA message validity check scheme. However, to calculate a correct AT_MAC in order to impersonate a valid PAA to the PaC, it is enough to know the *RAND* and K_c values from n GSM triplets of the subscriber. Given physical access to the SIM card, it is easy to obtain any number of GSM triplets. Another way to obtain triplets is to mount an attack on the PaC platform via a virus or other malicious software. The PaC thus needs to be protected against triplet querying attacks by malicious software. Moreover, if the same SIM credentials are also used for GSM traffic, the triplets could be revealed in the GSM network – see subsection 6.7. Care should be taken not to compromise the K_c keys used in PANA/GSM to attackers when they are transmitted between entities, or handled outside a protected environment.

6.2 Minimal Trust Relationship

The use of triplets is a GSM feature that permits delegation of authentication as well as cipher key distribution from the HN to the VN through a minimal trust relationship between operators. That is, the HN does not need to reveal the most sensitive information, such as K_i, to any intermediate entity in the VN. Another benefit of this scheme is that subsequent authentications do not require additional round trips with the HN, and this gives a major performance advantage. This kind of technique can be useful in providing heterogeneous network access supporting ubiquitous mobility. In particular, such an approach may be very valuable in the scenario where a user's access device wishes to access the Internet via different multiple access media and network interfaces, leading to the use of a number of network operators.

6.3 User Identity Confidentiality

PANA/GSM includes user identity confidentiality support, which protects the privacy of the user identity against *passive* attacks (e.g. eavesdropping). But the mechanism cannot be used on the first connection with a given PAA, when the permanent user identity needs to be sent in clear. In this case, an *active* attacker that impersonates the access network may learn the subscriber's permanent identity. However, the PaC can refuse to send the cleartext permanent user identity to the PAA if it believes that the access network should be able to recognize its pseudonym. If user identity confidentiality is required and the PaC and PAA cannot guarantee that the pseudonym will be maintained reliably, then an external security mechanism may be used to provide additional protection. Nevertheless, this kind of tunnelling mechanism can itself introduce new security vulnerabilities, as described in subsection 6.5.

6.4 Session Key Derivation

PANA/GSM key derivation combines several GSM triplets in order to derive stronger keying material and stronger AT_MAC values. The actual strength of the resulting keys depends, among other things, on the operator-specific authentication algorithms, the strength of the K_i key, and the quality of the *RAND* challenges. At no point does PANA/GSM require the keys K_c or the derived *SRES* values to be communicated. A passive eavesdropper can learn n different *RAND* values and the corresponding AT_MAC and may be able to link this information to the user identity. An active attacker that impersonates a GSM subscriber could easily obtain n different *RAND* values and the corresponding AT_MAC values from the EAP server for any given user identity. However, as long as the cryptographic functions used are sufficiently robust, this should not enable the attacker to deduce the correct *SRES* and K_c values.

6.5 Man-in-the-Middle Attacks

Care has to be taken to avoid man-in-the-middle attacks arising when tunnelling is used, e.g. when using PEAP [13], or when EAP/SIM is part of a sequence of EAP methods. Such vulnerabilities can arise (see, for example, Asokan et al. [3]) even when the authentication protocols used at the various 'levels' are in themselves secure. When such attacks are successfully carried out, the attacker acts as an intermediary between a PaC victim and a legitimate PAA. This allows the attacker to authenticate successfully to the PAA, as well as to obtain access to the network. As a solution to the problem, Asokan et al. [3] and Puthenkulam et al. [16] suggest cryptographically binding the session keys of the two phases, i.e. binding together the tunnel session key and the *MSK* derived from the EAP/SIM method.

6.6 Service Theft and Dictionary Attacks

PANA/GSM does not specify any mechanism for preventing service theft. Therefore an attacker can gain unauthorized access to the network by stealing service from another user, spoofing both the IP and

MAC addresses of a legitimate PaC to gain unauthorized access. In a non-shared medium, service theft can be prevented by simple IP address and MAC address filters. In shared links, filters are not sufficient to prevent service theft as they can easily be spoofed (as described by Parthasarathy [14]). A recent draft [15] describes how an IPsec[2] SA can be established to secure the link between the PaC and the EP, which can be used to prevent service theft in the access network. Because PANA/GSM is not a password protocol, it is not vulnerable to dictionary attacks, assuming that the pre-shared secret is not derived from a weak password.

6.7 Credential Reuse

PANA/GSM cannot prevent attacks in the GSM networks. If the same SIM credentials are also used in GSM, it is possible to mount attacks via the GSM air interface. A passive attacker can eavesdrop on GSM traffic and obtain (*RAND*, *SRES*) pairs. He can then use a brute force attack to obtain separately the 64-bit K_c keys used to encrypt the GSM data. If the attacker can obtain n K_c keys, where $1 \leq n \leq 3$, he can then impersonate a valid network to a PANA/GSM client. An active attacker can mount a "false GSM base station (BS) attack", replaying previously seen *RAND* challenges to obtain *SRES* values (see [12] for further details). He can then use a brute force attack to obtain the K_c keys. If successful, the attacker can impersonate a valid network or decrypt previously seen traffic. However, it should be noted that these attacks are not possible if the SIM credentials used in PANA/GSM are not shared in the GSM network. It should also be noted that performing a brute force search for a 64-bit key is a non-trivial task that could not be performed in real time; moreover, it is unlikely to be worth the effort of performing such a search just to steal network access.

6.8 Integrity, Replay Protection and Confidentiality

The protection of signalling message exchanges through the PANA/GSM SA prevents an opponent from acting as a man-in-the-middle adversary, from session hijacking, from injecting packets, from replaying messages, and from modifying the content of the exchanged packets. Also, as with all PANA methods, in PANA/GSM an integrity object is defined, supporting data-origin authentication, replay protection based on sequence numbers, and integrity protection based on a keyed message digest. Moreover, some EAP/SIM attributes are used to provide integrity, replay protection, and confidentiality for EAP/SIM payloads, except for the EAP/SIM/Start round trip. However, in this latter case the protocol values are protected by a later PANA/GSM exchange.

[2] http://www.ietf.org/html.charters/ipsec-charter.html

6.9 Negotiation Attacks, Fast Reconnection and Randomness

EAP method downgrading attacks might be possible, because PANA/GSM does not protect the EAP method negotiation, especially if the user employs the EAP/GSM identifier with other EAP methods. However, the EAP document [4] describes how to avoid attacks that negotiate the least secure EAP method from among a set. If a peer needs to make use of different EAP authentication methods, then distinct identifiers should be employed, each of which identifies exactly one authentication method. In any case, some protection against such an attack can be offered by repeating the list of supported EAP methods protected with the PANA/GSM SA. PANA/GSM does not support cipher suite negotiation, but includes an EAP/SIM version negotiation procedure (see section 3). PANA/GSM supports two types of fast reconnection; since fast reconnection does not involve the entire AAA communication, it gives performance benefits. A PANA/GSM implementation needs to use a good source of randomness to generate the random numbers required in the protocol.

6.10 Denial-of-service Attacks

PANA/GSM sequence numbers and cookies provide resistance against blind resource consumption DoS attacks as described in [8]. But PANA/GSM does not protect the EAP/SIM method exchange itself. Since in particular the PAA is not allowed to discard packets, and packets have to be stored or forwarded to an AAA infrastructure, a risk of DoS attacks remains. Also PANA/GSM adopts the EAP/SIM mechanism that is not a tunnelling method. Hence an adversary can both eavesdrop on the EAP/SIM payloads and inject arbitrary messages which might confuse both the PaC and the PAA. In physically insecure networks, an attacker may mount DoS attacks by sending false PANA/GSM success or failure indications. However, the attacker cannot force the PaC or the PAA to believe successful authentication has occurred when mutual authentication has failed or has not happened yet. The PANA/GSM protocol also enables both the PaC and the PAA to transmit a tear-down message [8]. This message causes state removal, a stop to the accounting procedure, and removes the installed packet filters. Thus such a message needs to be protected to prevent an adversary from deleting state information and thereby causing DoS attacks.

7 Advantages & Disadvantages

In this section, the PANA/GSM proposal is assessed with respect to how well it addresses security issues arising in future heterogeneous network access scenarios. The main advantages of PANA/GSM in this context are as follows.

- PANA/GSM is implemented using PANA, a flexible and scalable network-layer access authentication protocol. PANA/GSM also derives from the simple, lightweight and robust GSM mobile system.
- PANA/GSM uses the EAP/SIM method, which provides enhancements to GSM including stronger authentication, stronger key agreement and mutual authentication. PANA/GSM is also not vulnerable to dictionary attacks and, with the exception of the PaC first connection to PAA, it provides user identity confidentiality.
- The PANA/GSM SA prevents man-in-the-middle attacks, session hijacking, packet injection, message replay, and content modification of the exchanged PANA/GSM packets. The PANA/GSM integrity object supports data-origin authentication, replay protection based on sequence numbers, and integrity protection.
- PANA/GSM provides ordered delivery of messages with sequence numbers, which, along with cookies, provides resistance against blind DoS attacks. PANA/GSM also provides confidentiality of the EAP/SIM payload.
- PANA/GSM includes an EAP/SIM version negotiation procedure and supports two types of fast reconnection, giving performance benefits. Use of GSM triplets requires a minimal trust relationship between operators, and also gives a performance benefit.

The disadvantages of the proposed PANA/GSM protocol are as follows:

- The PaC first connection to PAA is not protected by the user identity confidentiality mechanism.
- PANA/GSM does not specify any mechanism for preventing service theft or for supporting cipher suite negotiation. On the other hand, because PANA/GSM is just a signalling protocol and does not carry user data traffic, in fact it does not have to formally specify any mechanism for preventing service theft. However, since EAP/SIM has key derivation functionality, it is possible to bootstrap IKEv2 [6] from PANA/GSM to establish a local IPsec tunnel for providing both cipher suite negotiation and service theft prevention.
- There is a risk of DoS attacks through false EAP/SIM Success/Failure indications and tear-down messages. Nevertheless, the EAP document [4] describes a way to discard false success messages, and PANA/GSM supports protected tear-down messages by using a MAC AVP. Thus a false failure message is the only remaining problem. For example, the PANA/GSM protocol does not provide security protection for the initial EAP payload exchange. Integrity protection can only be provided after the PANA/GSM SA has been established. Thus the PaC will accept a PANA_bind_request message carrying a false EAP Failure payload, sent by an attacker impersonating the legitime PAA, in response to (*b*) a PANA_auth_answer message carrying an EAP Response/Identity payload.

8 Further Work

The session key derivation procedure in the current version of PANA/GSM depends heavily on the EAP/SIM protocol. Therefore one interesting alternative may be to adopt one of the unified EAP session key derivation approaches currently being investigated (see, for example, Salowey and Eronen [17]), instead of adopting the existing scheme from EAP/SIM. An analogous scheme to PANA/GSM would be to specify the GPRS GMM [7] and the UMTS AKA [1] authentication protocols as an EAP method (e.g. Buckley et al. [5] and Arkko et al. [2]), enabling their use with PANA. Another interesting new application would be the transport of public key based authentication protocols by EAP (e.g. Tschofenig and Kroeselberg [18]) and PANA.

9 Conclusions

Authentication and key agreement are the central components of secure access procedures for heterogeneous network access supporting ubiquitous mobility. In this paper, we have proposed the PANA/GSM protocol, providing an IP-compatible, lightweight, flexible and scalable method for authenticating a user to an access network. The protocol is based on PANA, a network-layer access authentication protocol carrier, which communicates, via EAP, with an AAA infrastructure interacting with a GSM AuC. PANA/GSM uses the EAP/SIM protocol, which encapsulates GSM parameters in EAP and provides enhancements such as stronger authentication and key agreement as well as mutual authentication.

The use of 'triplets' in PANA/GSM requires a minimal trust relationship between operators, and no additional round trips with the home GSM network, thereby increasing the likelihood of successful use. The protocol, from the user's point of view,

works with a 'standard' GSM SIM card and requires only an appropriate Internet access device and a SIM card reader. The gains in performance arising from the two types of fast reconnection, and the gains in security due to the PANA/GSM SA, may make the PANA/GSM proposal attractive to GSM operators wishing to offer their users heterogeneous Internet access in ubiquitous mobility networks.

10 Acknowledgements

The authors would like to acknowledge the many helpful insights and corrections provided by Hannes Tschofenig and Yoshihiro Ohba.

References

[1] 3GPP. *Technical Specification 3GPP TS 33.102 V5.1.0: "Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 5)"*. Third Generation Partnership Project, December 2002.

[2] J. Arkko and H. Haverinen. EAP AKA authentication. Internet draft (work in progress), Internet Engineering Task Force, February 2003.

[3] N. Asokan, V. Niemi, and K. Nyberg. Man-in-the-middle in tunnelled authentication. In *the Proceedings of the 11th International Workshop on Security Protocols*, Cambridge, UK, April 2003. To be published in the Springer-Verlag LNCS series.

[4] L. Blunk, J. Vollbrecht, B. Aboba, J. Carlson, and H. Levkowetz. Extensible authentication protocol (EAP). Internet draft (work in progress), Internet Engineering Task Force, June 2003.

[5] A. Buckley, P. Satarasinghe, V. Alperovich, J. Puthenkulam, J. Walker, and V. Lortz. EAP SIM GMM authentication. Internet draft (work in progress), Internet Engineering Task Force, August 2002.

[6] C. Kaufman (editor). Internet key exchange (IKEv2) protocol. Internet draft (work in progress), Internet Engineering Task Force, May 2003.

[7] ETSI. *GSM Technical Specification GSM 04.08 (ETS 300 940): "Digital cellular telecommunication system (Phase 2+); Mobile radio interface layer 3 specification" (version 7.8.0)*. European Telecommunications Standards Institute, June 2000.

[8] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, and A. Yegin. Protocol for carrying authentication for network access (PANA). Internet draft (work in progress), Internet Engineering Task Force, July 2003.

[9] H. Haverinen and J. Salowey. EAP SIM authentication. Internet draft (work in progress), Internet Engineering Task Force, February 2003.

[10] T. Hiller and G. Zorn. Diameter extensible authentication protocol (EAP) application. Internet draft (work in progress), Internet Engineering Task Force, March 2003.

[11] NIST. *Federal Information Processing Standard, Secure Hash Standard (FIPS Publication 180-1)*. National Institute of Standards and Technology, U.S. Department of Commerce, April 1995.

[12] P. Pagliusi. A contemporary foreword on GSM security. In G. Davida, Y. Frankel, and O. Rees, editors, *Infrastructure Security: International Conference – InfraSec 2002, Proceedings, Lecture Notes in Computer Science 2437*, pages 129–144, Bristol, UK, October 2002. Springer-Verlag.

[13] A. Palekar, D. Simon, G. Zorn, and S. Josefsson. Protected EAP protocol (PEAP). Internet draft (work in progress), Internet Engineering Task Force, March 2003.

[14] M. Parthasarathy. PANA threat analysis and security requirements. Internet draft (work in progress), Internet Engineering Task Force, April 2003.

[15] M. Parthasarathy. Securing the first hop in PANA using IPsec. Internet draft (work in progress), Internet Engineering Task Force, May 2003.

[16] J. Puthenkulam, V. Lortz, A. Palekar, D. Simon, and B. Aboba. The compound authentication binding problem. Internet draft (work in progress), Internet Engineering Task Force, October 2002.

[17] J. Salowey and P. Eronen. EAP key derivation for multiple applications. Internet draft (work in progress), Internet Engineering Task Force, June 2003.

[18] H. Tschofenig and D. Kroeselberg. EAP IKEv2 method. Internet draft (work in progress), Internet Engineering Task Force, June 2003.

[19] M. Walker and T. Wright. Security. In F. Hillebrand, editor, *GSM and UMTS: The Creation of Global Mobile Communication*, chapter 15, pages 385–406. John Wiley & Sons, New York, 2002.