Heterogeneous Internet Access via PANA/UMTS

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 31, 2004

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 re-used in all the likely future ubiquitous mobility access contexts. This article proposes the PANA/UMTS authentication protocol for heterogeneous network access as a step towards filling this gap. A security analysis of the PANA/UMTS 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.

Keywords: authentication, heterogeneous network access, ubiquitous mobility, UMTS, PANA.

1 Introduction

It is expected that future IP devices will use a variety of network access technologies to support ubiquitous connectivity. For example, one future requirement identified by the SHAMAN[1] Project is to provide flexible security means for accessing heterogeneous mobile networks, including not only UMTS [1], GPRS [10] and GSM [28], but also WLAN [12], Bluetooth[2], and other network technologies. Moreover, "heterogeneous network access control security" received the highest rating value in the list of open research issues for future mobile communication systems produced by the PAMPAS Project [13, p65]. 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 do not provide non-repudiation. In addition to being limited to specific access media (e.g. 802.1aa [15] for IEEE 802 links), some of these protocols are limited to specific network topologies (e.g. PPP [25] for point-to-point links) and are not scalable.

The recent IETF PANA (Protocol for carrying Authentication for Network Access[3]) work aims to provide a protocol [11] that will be a flexible and scalable network-layer authentication carrier for access networks that support IP. PANA will be capable of transporting any EAP (Extensible Authentication Protocol) method [5] to enable access authentication. In addition, the EAP/AKA protocol [2] specifies a way of encapsulating the Universal Mobile Telecommunications System (UMTS) Authentication and Key Agreement (AKA) mechanism [1]

[1] http://www.ist-shaman.org/

[2] www.bluetooth.com

[3] http://www.ietf.org/html.charters/pana-charter.html

within EAP. Once inside EAP, the UMTS parameters can thus be carried by PANA. In this paper we present a proposal for combining UMTS authentication with EAP/AKA and PANA, which we call PANA/UMTS.

The goal of the PANA/UMTS protocol is to provide an IP compatible, lightweight, flexible and scalable authentication method that allows a client to be authenticated in a heterogeneous network access environment. The proposal adapts the security techniques used in UMTS to the PANA structure. The protocol runs between a client device and an agent device in the access network, where the agent may be a client of an AAA (Authentication, Authorization and Accounting) infrastructure, which itself has an interface to the UMTS network.

Section 2 summarises the UMTS network access security feature, Section 3 describes the EAP/AKA protocol, and Section 4 explains the PANA protocol. Section 5 then describes the proposed new PANA/UMTS authentication scheme. Section 6 analyses the threats to the PANA/UMTS protocol, Section 7 considers its advantages and disadvantages and, finally, Sections 8, 9, and 10 present possible further work, conclusions and acknowledgements.

2 UMTS Network Access Security

UMTS is a third generation mobile communication standard developed by 3GPP (Third Generation Partnership Project[4]). UMTS network access security provides users with secure access to UMTS services, protecting in particular the UMTS radio access network (UTRAN). This section summarises the four UMTS network access security features relevant here, i.e. entity authentication, signalling integrity, user traffic confidentiality, and user identity confidentiality. Further details of UMTS security can be found in [1, 4, 28].

UMTS *mutual entity authentication* involves the Mobile Station (MS), the visited network (VN), and the home network (HN); the VN verifies the subscriber's identity by means of a challenge-response mechanism, while the MS checks that the VN has been authorised by the HN. A 128-bit secret key K is shared by the USIM (Universal Subscriber Identity Module) and the HN AuC (Authentication Centre). An authentication vector is produced by the AuC from K and a sequence number, and sent on demand to the VN. The authentication vector contains a random number $RAND$, a network authentication token $AUTN$, an expected result $XRES$, a temporary integrity key IK, and a temporary cipher key CK.

Whenever the VN wishes to authenticate the MS, it sends it one ($RAND$, $AUTN$) pair. The MS verifies $AUTN$, using K and the sequence number in $AUTN$. If this process is successful, the USIM sends RES, computed as a function of K and $RAND$, back to the VN and also computes IK and CK. The VN then compares the received RES with the stored $XRES$, and if they agree the MS is deemed authentic; IK and CK can then be used for connection security, as described below.

Signalling data integrity and origin authentication is provided by computing an integrity check using the 128-bit key IK, shared by the MS and the VN. *User traffic confidentiality* is similarly provided by encrypting traffic using the 128-bit key CK. The user traffic confidentiality feature extends to the Radio Network Controller (RNC), so that microwave links between the Base Stations and the RNC are also protected.

Finally, UMTS provides *user identity confidentiality* through the use of temporary identities. Apart from at initial registration, a user is not identified employing his permanent identity IMSI (International Mobile Subscriber Identity), but instead uses a temporary identity known as the TMSI (Temporary Mobile Subscriber Identity[5]). To avoid user traceability, which may lead to the compromise of user identity confidentiality, temporary identities are changed regularly in an 'unlinkable' way. In addition, it is

[4] http://www.3gpp.org/

[5] It is TMSI in the circuit switched domain, and P-TMSI in the packet switched domain.

required that any signalling or user data that might reveal the user identity is encrypted when sent across the UTRAN.

3 An EAP Mechanism for Carrying UMTS/AKA

The EAP/AKA protocol [2] is an EAP mechanism for authentication and session key distribution that uses UMTS AKA [1]. It involves a client acting on behalf of a user, an authenticating party and an EAP server. The EAP server is the network element that terminates the EAP protocol [5]. It may be co-located with the authenticating party, although the EAP server is typically implemented on a separate AAA server with whom the authenticating party communicates using an AAA protocol. The EAP server, which normally belongs to the user's home Internet AAA network, is able to obtain authentication vectors from the subscriber's HN AuC.

The EAP/AKA uses two round trips to mutually authenticate the client and the network, and provide them with temporary shared secret keys. The protocol includes exchange of EAP-Request/Response messages of types Identity and AKA. The type AKA also has a subtype field that admits the values: Challenge, Authentication-Reject, Synchronization-Failure, Identity, and Notification. The subtype-specific data is composed of parameters encapsulated in attributes. The EAP/AKA packet format and the use of attributes are specified in Section 6 of [2]. Either the IMSI or the TMSI can be employed as part of the user identifier. Section 4 of [2] describes user identity management.

In the EAP/AKA full authentication procedure, an identity request/ response message pair is first exchanged. Next, the EAP server sends an EAP-Request/AKA-Challenge message. This message contains a random number (AT_RAND), a network authentication token (AT_AUTN), and a Message Authentication Code (AT_MAC) computed on the EAP packet; it may optionally contain encrypted data (AT_ENCR_DATA) for identity confidentiality support. The client runs the AKA algorithm (usually inside a USIM) and verifies $AUTN$ and MAC. If this is successful, the client is talking to a valid EAP server. It then derives the RES and the temporary keys, and sends back the EAP-Response/AKA-Challenge, protected by another AT_MAC. The EAP server then checks the AT_MAC, compares the received RES with the stored $XRES$, and if they agree the user is deemed authentic; the shared temporary keys can now be used.

The EAP/AKA keying material is generated from a Master Key (MK), which is calculated using the hash function SHA-1 [18] from a combination of the user identity, the UMTS integrity key IK, and the UMTS confidentiality key CK. The material derived from the MK is subsequently used to generate the temporary keys. This includes the Master Session Key (MSK) for encryption of the traffic between the client and the network, the encryption key (K_encr) to be used with AT_ENCR_DATA, and the authentication key (K_aut) to be used with AT_MAC. Finally, EAP/AKA includes optional identity privacy support, and an optional re-authentication procedure.

4 Protocol for carrying Authentication for Network Access (PANA)

This section briefly introduces the draft PANA protocol [11], 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/AKA), 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' [11], a MAC AVP, protecting the integrity of a PANA message, or an EAP AVP, which 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/AKA *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/AKA) at the authentication phase, where the initial handshake phase can be omitted. If there is an existing PANA SA, PANA_auth messages carrying the EAP fast reconnection process can be protected with a MAC AVP. The second type is based on a single protected PANA message exchange without entering the authentication phase. If there is an existing PANA SA, both PaC and PAA can send a PANA_reauth_request to the communicating peer and expect the peer to return a PANA_reauth_answer, where both messages are protected with a MAC AVP.

5 PANA/UMTS Authentication Procedure

The PANA/UMTS mechanism proposed here involves three functional entities, namely the *PaC* (also referred to here as the *client*, *user* or *subscriber*), the *PAA* (or *authenticating party*) and the *EAP server*. The *PaC* is associated with a network device and a set of UMTS credentials stored in a USIM that 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[6] socket, equipped with a UMTS-enabled USIM card. There are other possible implementations, e.g. involving the use of a UMTS Mobile Equipment (ME, e.g. mobile phone) equipped with a USIM card and linked to a laptop (e.g. via cable, Bluetooth, infrared or WLAN)[7].

The *PAA* authenticates the UMTS credentials provided by the PaC and grants network access. In the context of this article, the *EAP server* is implemented on the AAA server and has an interface to the UMTS network, operating as a *gateway* between the Internet AAA network and the UMTS AKA infrastructure. The PAA is thus an AAA client that communicates with the user's EAP server through an AAA protocol supporting EAP (e.g. Diameter EAP [14]) and key wrap (e.g. Diameter CMS [7], where this involves encrypting a content-encryption key using a key encrypting key). PANA/UMTS also involves a further entity, namely the EP (Enforcement Point), which may be co-located with the PAA, which applies per-packet enforcement policies (i.e. filters) to the traffic of the PaC's devices.

Figure 1 shows the PANA/UMTS full 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/UMTS session is established between the PaC and the PAA, following the PANA model (see subsection 4.2 of [11]). In the *Authentication* phase, the main focus of this article and further explained below, EAP/AKA messages encapsulated in PANA/UMTS 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/AKA session key (*MSK*); we call this the PANA/UMTS SA. During the *Authorization* phase, a separate protocol is used between the PAA and the EP to manage the PaC network access control. After this phase, the established PANA/UMTS session as well as the

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

[7] An alternative described in [16] is to use USIM Toolkit commands, which enables the USIM to request the ME to open an infrared or Bluetooth channel with the user laptop.

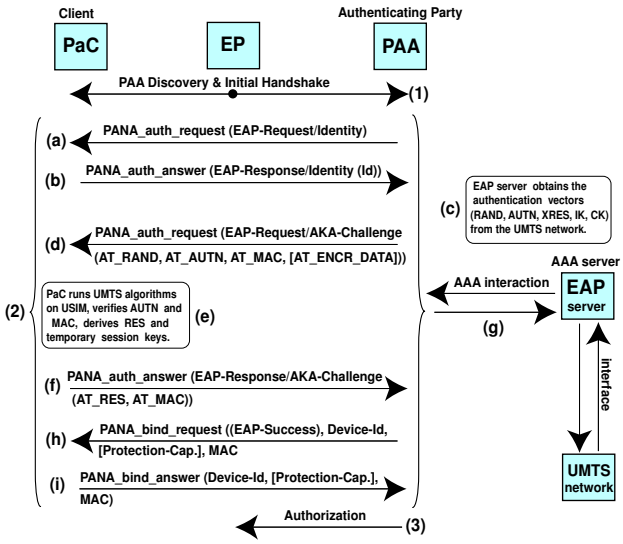

Figure 1: **PANA/UMTS full authentication procedure**. The name of each message is shown, followed by the contents of the message in round brackets. Square brackets are used to denote optional fields.

PANA/UMTS SA is deleted, following the PANA standard (see subsection 4.5 of [11]).

During the *Authentication* phase, the first PANA_auth_request message (a) issued by the PAA encapsulates 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 receiving the user identity from the PAA through an AAA interaction, the EAP server obtains from the UMTS network the user's authentication vector, which is further used for deriving the temporary keys (c).

The next PANA_auth_request message (d) issued by the PAA includes the EAP-Request/AKA-Challenge packet that contains $RAND$, $AUTN$, MAC, and an optional AT_ENCR_DATA (see Section 3). On receipt of this message, the PaC runs the AKA algorithm inside a USIM, calculates a copy of $AUTN$ and MAC, and verifies that these calculated values equal the received ones[8]. After that, it derives RES and the EAP/AKA temporary keying material (e) for further use.

If all checks out, the PaC responds (f) with a PANA_auth_answer message transporting the EAP-Response/AKA-Challenge payload, which includes RES and MAC. After receiving this payload from the PAA by means of an AAA interaction, the EAP server compares the received RES with the stored $XRES$ obtained from the authentication vector; if they agree, the PaC is deemed authentic. As a result, the EAP server sends back (g) the EAP-Success packet, which carries the derived keying material. Finally the PAA encapsulates the EAP-Success packet in a PANA_bind_request message sent to the PaC (h), and receives back an acknowledge through a PANA_bind_answer (i). Both PANA_bind messages are protected by a MAC AVP; they may optionally contain a Protection-Capability AVP to indicate if link-layer or network-layer encryption should be initiated after PANA/UMTS. They are also used for binding device identifiers of the PaC and the PAA, via Device-Id AVP, to the PANA/UMTS SA established at the end of the authentication phase.

6 Security Analysis

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

6.1 User Identity Confidentiality

PANA/UMTS 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 will have to be sent in clear. In this case, an *active*

[8] If the MAC does not match, the PaC silently ignores the previous message and does not send any authentication results to the PAA. If the $AUTN$ does not match, the PaC then sends back to the PAA an explicit error packet (EAP-Response/AKA-Authentication-Reject) inside a PANA_auth_answer message.

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, such as the Protected Extensible Authentication Protocol (PEAP) [20], may be used to provide additional protection. Nevertheless, this kind of tunnelling mechanism can itself introduce new security vulnerabilities, as described in subsection 6.2.

6.2 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, or when EAP/AKA 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. [23] suggest to cryptographically bind the session keys of the two phases, i.e. to bind together the tunnel session key and the *MSK* derived from the EAP/AKA method. Even when tunnelling or an EAP sequence of methods are not used with PANA/UMTS, user data need to be integrity protected on physically insecure networks to avoid man-in-the-middle attacks and session hijacking.

6.3 Mutual Authentication

PANA/UMTS provides mutual authentication via the UMTS AKA mechanisms. The PaC believes that the PAA is authentic because the network sent correct *MAC* and *AUTN* values. The PAA believes that the PaC is genuine because the received *RES* agrees with the stored *XRES*, and the *MAC* computed on the challenge response is correct. Moreover, PANA/UMTS validates the EAP AVP exchanges through its PANA message validity check scheme (Section 4.1.6 of [11]).

6.4 Key Derivation

PANA/UMTS supports 128-bit key derivation through the EAP/AKA key hierarchy. The temporary keys for protection of the EAP/AKA payloads and the *MSK* are cryptographically separate; i.e. an attacker cannot derive any non-trivial information from *K_encr* or *K_aut* based on the *MSK* or vice versa. An attacker also cannot calculate the pre-shared secret *K* from *IK*, *CK*, *K_encr*, *K_aut* or *MSK*.

6.5 Service Theft, Brute-Force and Dictionary Attacks

PANA/UMTS does not specify any mechanism for preventing service theft. Therefore an attacker can gain unauthorized access to the network by stealing the 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 [21]). A recent draft [22] describes how an IPsec[9] 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.

The effective key length in PANA/UMTS is 128 bits, and there are no known computationally feasible brute-force attacks. Because PANA/UMTS is not a password protocol, it is not vulnerable to dictionary attacks, assuming that the pre-shared secret is not a weak password.

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

6.6 Integrity, Replay Protection and Confidentiality

The protection of signaling packet exchanges through the PANA/ UMTS 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 messages. Also, as with all PANA methods, in PANA/UMTS 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, in PANA/UMTS some attributes are used to provide integrity, replay protection and confidentiality for EAP/AKA payloads. In this case, integrity protection is based on a keyed MAC [17] (i.e. AT_MAC). Confidentiality (AT_ENCR_DATA and AT_IV) is based on the Advanced Encryption Standard (AES) block cipher [19]. On full authentication, replay protection for the EAP/AKA payload is provided by the underlying UMTS AKA scheme, which makes use of the *RAND* and *AUTN* values. For EAP based re-authentication, a counter and a server nonce is used to provide replay protection. The contents of the EAP-Response/Identity payload exchanged by PANA/UMTS are implicitly integrity protected by including them in key derivation.

6.7 Negotiation Attacks, Fast Reconnection and Generation of Random Numbers

EAP method downgrading attacks might be possible because PANA/UMTS does not protect the EAP method negotiation, especially if the user employs the EAP/AKA identifier with other EAP methods. Nevertheless, the EAP document [5] describes a practice to avoid attacks that negotiate the least secure EAP method from among a set. If a particular peer needs to make use of different EAP authentication methods, then distinct identifiers should be employed, each of which identifying exactly one authentication method. Anyway, some protection against such an attack can be offered by repeating the list of supported EAP methods protected with the PANA/UMTS SA.

PANA/UMTS does not support EAP/AKA protocol version negotiation or ciphersuite negotiation.

In line with Section 4, PANA/UMTS supports two types of fast reconnection. Since fast reconnection does not involve the entire AAA communication, it gives performance benefits. A PANA/UMTS implementation needs to use a good source of randomness to generate the random numbers required in the protocol[10].

6.8 Denial-of-service Attacks

PANA/UMTS sequence numbers and cookies provide resistance against blind resource consumption DoS attacks, as described in [11]. But PANA/ UMTS does not protect the EAP/AKA 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/UMTS adopts the EAP/AKA mechanism, which is not a tunnelling method. Hence an adversary can both eavesdrop on EAP/AKA 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/UMTS success or failure indications. However, the attacker cannot force the PaC or the PAA to believe successful authentication has occurred when mutual authentication failed or has not happened yet.

The PANA/UMTS protocol also enables both the PaC and the PAA to transmit a tear-down message [11]. 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.

[10] See [8] for details on generating random numbers for security applications.

6.9 Minimal Trust Relationship and Cipher Key Distribution

The use of authentication vectors is an significant UMTS feature that permits delegation of authentication as well as cipher key distribution from the home to the visited network through a minimal trust relationship between operators. That is, the home network does not need to reveal the information most sensitive, such as K, to any intermediate entity in the visited network. Another benefit with this scheme is that subsequent authentications do not require additional round trips with the home network, and this gives a big performance advantage. This kind of technique encapsulated into EAP/AKA and carried by PANA/UMTS can be useful to address heterogeneous network access supporting ubiquitous mobility. In particular, in the scenario where a user's access device wishes to access the Internet via different multiple access media and network interfaces[11], leading to the use of a number of network operators. In this scenario, if we use PANA/UMTS, the home AAA server can make use of authentication vectors to delegate PaC authentication function to the PAA in the visited network, achieving therefore minimal trust relationship between home and visited network operators as well as performance benefit. Furthermore, the same authentication vectors distribution scheme can include cipher keys to any network access point implementing a PAA, e.g. a NAS (Network Access Server), wishing to establish an encrypted channel with a PaC.

6.10 Mandatory Integrity Protection versus Mutual Authentication

We can imagine a feasible scenario where the interface between the client and the NAS is wireless and the NAS must use a signalling message, such as a start encryption command, to activate the encryption in the air interface. In this case, beyond the use of the authentication vectors material, the introduction of mandatory integrity protection for critical signalling messages in PANA/UMTS through the MAC AVP and the AT_MAC attribute is crucial to avoid the typical masquerading or 'false entity in-the-middle' attack, of which prevention could not be achieved solely by mutual authentication. Thus, the mandatory integrity protection mainly for critical signalling messages is another feature from PANA/UMTS that provides significant contribution for authentication in heterogeneous network access.

[11] E.g. PPP [25], Bluetooth, IEEE 802.1aa [15].

7 Advantages and Disadvantages

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

- PANA/UMTS is implemented using PANA, a flexible and scalable network-layer access authentication protocol. Such a protocol is necessary when link-layer authentication mechanisms are either not available or not able to meet the overall requirements, or when multi-layer authentication is needed.
- PANA/UMTS is based on the EAP/AKA method. This method enables the use of the existing AKA infrastructure in a number of new scenarios involving devices that already contain a USIM. For example, it can be used as a secure PPP authentication method or else in the context of WLANs and IEEE 802.1aa technology, through EAP over wireless. PANA/UMTS is also not vulnerable to brute force or dictionary attacks and, with the exception of the PaC first connection to PAA, it includes user identity confidentiality.
- The PANA/UMTS SA prevents man-in-the-middle attacks, session hijacking, packets injection, message replay and content modification of the subsequent exchanged packets. The

PANA/UMTS integrity object supports data-origin authentication, replay protection based on sequence numbers and integrity protection.

- PANA/UMTS provides ordered delivery of messages with sequence numbers, which along with cookies provides resistance against blind DoS attacks. PANA/UMTS also provides confidentiality of the EAP/ AKA payload based on a block cipher.

- PANA/UMTS supports two types of fast reconnection, resulting in performance benefits. Use of UMTS authentication vectors provides minimal trust relationship between operators and also performance benefit. Adoption of mandatory integrity protection for critical PANA/ UMTS signalling messages avoids masquerading attacks.

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

- Although the PANA/UMTS identity payload is implicitly integrity protected, the PaC first connection to PAA is not benefited by the user identity confidentiality mechanism.

- PANA/UMTS does not specify any mechanism for preventing service theft, either for supporting ciphersuite or EAP/AKA version negotiation. On the other hand, because PANA/UMTS is just a signaling 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/AKA has key derivation functionality, it is possible to bootstrap IKEv2 [9] from PANA/UMTS to establish a local IPsec tunnel for providing both cipher suite negotiation and service theft prevention.

- Risk of DoS attacks through false EAP/AKA Success/Failure indications and tear-down messages. Nevertheless, the EAP document [5] describes a way to discard false success messages, and PANA/UMTS supports protected tear-down messages by using a MAC AVP. Thus False EAP Failure is the only remaining problem. For example, the client will accept false EAP Failure in response to EAP Response/Identity carried by PANA/UMTS.

8 Further Work

The session key derivation procedure in the current version of PANA/UMTS depends heavily on the EAP/AKA 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 [24]), instead of adopting the existing scheme from EAP/AKA, compliant with Section 5 of [26]. An analogous scheme to PANA/UMTS would be to specify the GPRS GMM authentication protocol [10] as an EAP method (e.g. Buckley et al. [6]), enabling its use with PANA. Another interesting new application would be the transport of public key based authentication protocols by EAP (e.g. Tschofenig and Kroeselberg [27]) and PANA.

9 Conclusions

According to the PAMPAS Project [13, p135], "the increasing heterogeneity of the networking environment is one of the long-term trends which requires new security approaches. The main challenges include the investigation and development of unified, secure and convenient authentication mechanisms that can be used in different access networks". 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 new PANA/UMTS protocol, in order to provide 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 a AAA infrastructure interacting with a UMTS AuC. PANA/UMTS is also based

on EAP/AKA, which permits to use the AKA infrastructure in new network scenarios comprising devices equipped with a USIM. PANA/UMTS prevents man-in-the-middle attacks, session hijacking, packets injection, message replay, content modification and blind DoS attacks. It imposes data-origin authentication, replay protection based on sequence numbers and integrity protection. Beyond to support user identity and EAP/AKA payload confidentiality, it uses a 128-bit key length and is not vulnerable to brute-force or dictionary attacks.

The use of authentication vectors in PANA/UMTS provides minimal trust relationship between operators and no additional round trips with the home UMTS network, thereby increasing the likelihood of successful use. The protocol, from the user's point of view, works with a 'standard' UMTS USIM card and requires only an appropriate Internet access device and a USIM card reader, integrated to or separated from that device. The gains of performance due to the two types of fast reconnection, and the gains of security due to the PANA/UMTS SA may make the PANA/UMTS proposal attractive to all the UMTS operators willing to offer to 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] C. W. Blanchard. Wireless security. In R. Temple and J. Regnault, editors, *Internet and wireless security*, chapter 8. Institution of Electrical Engineers, London, UK, 2002.

[5] 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.

[6] 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.

[7] P. Calhoun, S. Farrell, and W. Bulley. Diameter CMS security application. Internet draft (work in progress), Internet Engineering Task Force, March 2002.

[8] D. Eastlake 3rd, S. Crocker, and J. Schiller. Randomness recommendations for security. Request For Comments 1750, Internet Engineering Task Force, December 1994.

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

[10] 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.

[11] 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.

[12] J. T. Geier and J. Geier. *Wireless LANs*. Sams Publishing, Indianapolis, IN, USA, 2nd edition, 2001.

[13] C. Guenther. Pioneering advanced mobile privacy and security (PAMPAS) refined roadmap. Deliverable D03 IST-2001-37763, PAMPAS Project, http://www.pampas.eu.org/, February 2003.

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

[15] Institute of Electrical and Electronics Engineers. *IEEE P802.1aa/D5-2003 DRAFT Standard for Local and Metropolitan Area Networks - Port Based Network Access Control - Amendment 1: Technical and Editorial Corrections*, February 2003.

[16] V. Khu-smith and C. Mitchell. Enhancing e-commerce security using GSM authentication. In *the Proceedings of the EC-Web 2003, 4th International Conference on Electronic Commerce and Web Technologies*, Prague, Czech Republic, September 2003. To be published in the Springer-Verlag LNCS series.

[17] H. Krawczyk, M. Bellare, and R. Canetti. HMAC: Keyed-hashing for message authentication. Request For Comments 2104, Internet Engineering Task Force, February 1997.

[18] 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.

[19] NIST. *Federal Information Processing Standard, Advanced Encryption Standard (AES) (FIPS Publication 197)*. National Institute of Standards and Technology, U.S. Department of Commerce, November 2001.

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

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

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

[23] 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.

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

[25] W. Simpson. The point-to-point protocol (PPP). Request For Comments 1661 (STD 51), Internet Engineering Task Force, July 1994.

[26] H. Tschofenig. PANA framework issues. Internet draft (work in progress), Internet Engineering Task Force, January 2003.

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

[28] 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.