Internet Engineering Task Force   PANA
Internet Draft   H. Tschofenig
                                            Siemens Corporate Technology

draft-tschofenig-pana-framework-00.txt
9 January 2003
Expires: July 2003

                        PANA Framework Issues

STATUS OF THIS MEMO

   This document is an Internet-Draft and is in full conformance with
   all provisions of Section 10 of RFC2026.

Abstract

This document discusses framework assumptions relevant to activities in
the PANA working group. It is tentative in nature and raises issues
regarding some assumptions made in the group. The aim of this draft is
therefore not to propose solutions instead issues are highlighted which
might require further consideration.

1 Introduction

This document discusses framework assumptions relevant to activities in
the PANA working group. It is tentative in nature and raises issues
regarding some assumptions made in the group. The aim of this draft is
therefore not to propose solutions instead issues are highlighted which
might require further consideration.

The document is organized as follows:

In [Section 2](#) two basic scenarios are described which are differentiated by their authorization procedure – which in this case is about charging. The two scenarios are subscription-based access and alternative means of access. [Section 3](#) then considers a few possible results of a PANA protocol execution. A few examples are listed with increasing order of complexity. In [Section 4](#) a few interesting requirements (in the view of the author) are listed which might influence the outcome of a PANA protocol. The author is aware of the fact that there should be a separation between requirements, analysis and an actual protocol development. However, requirements are not always (or not often) orthogonal and a focus on some requirements (justified or not) might heavily influence the shape of a later protocol design. [Section 5](#) describes some building blocks which might be useful in a future protocol. Some of the building blocks have already (individually) been used in some protocol proposals. The building blocks are roughly aligned in their order of execution – some of them can be omitted without severely effecting the protocol (optional components). In [Section 6](#) a few thoughts on the relationship to mobility protocols (in particular Mobile IP) are presented. Finally in [Section 7](#) some conclusions derived from the previous explanations are given.

[2](#) Basic Scenarios

This section describes two scenarios for network access. The first scenario is traditionally based on a relationship between the user and his home network. The subscribed user uses his credentials in a AAA scenario to dynamically establish a trust relationship between the home network and the visited network.

Note that the term 'user' can also be replaced by some other entity for which the authentication is performed (e.g. a device). The difference between the two is (at the process of authentication and key exchange itself) often marginal since it depends only on the used identifier (e.g. NAI, Kerberos principal name, etc.). The usage of such an identifier after authentication for authorization is often different. Since an identity referring to a user provides some advantages compared to a device, such as additional security, this term is used. The author is, however, aware of the fact that some network access procedures used today are based on device authentication.

[2.1](#) Subscription-based access

Authentication of the user is typically provided to the home network where the user is subscribed and credentials are available. It is typically based on symmetric cryptography. The security relationships are one-to-many, and asymmetric cryptography does not necessarily

provide advantages in key management in such a situation (although it may provide other advantages, of course). In a mobile environment, the performance advantages of symmetric cryptography are also important. The message flow may involve many different visited networks, but an established business relationship (e.g. roaming agreements) between the visited and the home network may be assumed, hence accounting and charging are feasible.

Without roaming the visited network and the home network coincide and the end host is attached to the home network. This procedure simplifies avoiding inter-realm communication. Some ISP scenarios are based on this simplification.

2.2 Alternative means of access

In this scenario the user has no home network and therefore cannot assume such for the purpose of authentication and authorization. Hence authentication, authorization and payment is provided by other means such as pre-paid cards, credit cards and other mechanisms (micro- and macro-payment methods). Which protocol is required for the alternative means of access case depends on the chosen payment protocol. These types of environments are typically found in hot spots.

Additional information about a detailed problem description and protocol exchanges at an abstract level is provided at [1].

In the first scenario the visited network is given the assurance that the indicated user is registered to a given home network and that the home network provides a guarantee that the generated cost are covered. In the second scenario the payment mechanism has to provide the assurance that the end host is able to pay for the consumed resources. Note that this does not necessarily require user authentication. But it will typically require the transmission of payment-related confidential data prior to completed authorization. This may imply that the establishment of a security association is necessary to protect the sending of this data before the user credential can be verified. This in

turn may necessitate the use of asymmetric cryptography to establish a
unilaterally authenticated tunnel.

3 Possible objectives of executing a PANA protocol

The execution of a PANA protocol is done for a particular purpose. We
try to list a few possible goals:

3.1 Transport of EAP messages

EAP is a container for a number of authentication and key exchange
protocol messages. In the past different transport mechanisms have been

proposed to exchange the EAP payloads between the end host and the AAA
attendant. For several link layers (e.g. IEEE 802) a transport mechanism
for EAP payloads has been standardized. But no such link layer
independent transport mechanism for EAP payloads is available although
it would clearly be very desirable. As a minimum, this would enable EAP-
based entity authentication independent of the link layer. Since the
selection of a transport mechanism seems to be an almost religious issue
it seems to be hard to agree on a particular mechanism. Especially the
different usage scenarios (wired, wireless, mobility, etc.) add
constraints. Nevertheless, it is seen as necessary that PANA comes up
with at least link layer independent transport mechanism for EAP
payloads.

3.2 Installation of filter rules

Installations of filter rules provides packet filtering behavior in
addition to entity authentication. The controlled/uncontrolled packet
forwarding, which was already described in the expired draft [2],
provides this functionality. Depending on the location of the EP(s) and
the PAA a protocol might be required to communicate the filter rules
from the PAA to the EP(s). A number of protocols have been investigated
in the Midcom working group for exactly this purpose. Since these
protocols are outside the scope of PANA only their relationship to the
Midcom working group is of interest; namely how to provide the
information which filter rules to install at which device.

The Midcom protocols would enable the use of temporary filter rules. The
purpose of installing such temporary filter rules is to prevent a threat
where an end host looses connectivity (for various reasons such as

mobility) and an adversary is able to reuse the installed filter rules to transmit data traffic. Additionally a threat exists whereby an adversary uses IP spoofing to inject packets on behalf of someone else. The soft-state principle (i.e. installing filter rules which automatically time out after some time) is important to prevent stale state and possibly denial of service attacks. A more detailed threat description can be found in [3] and with a slightly different focus in [4]. Some of the threats described in the latter document are also applicable in this context.

The requirement for disconnect indication aims to address these threats. Various mechanisms are possible such as limiting the lifetime of the filter rules (and possibly requiring continuous refreshes to keep them in place), requiring continuous re-authentication and at the other extreme requiring each packet to be protected. A small comment about the relationship to existing work in the Midcom wg is given in Section A.

3.3 Session key distribution

Most EAP methods also provide the ability to establish a session key. Session key derivation in EAP is still under discussion but it is worth mentioning that the corresponding draft for carrying session keys via the AAA infrastructure already exist. Protection for session keys delivered in Diameter are provided by CMS [5]. The goal of session key distribution is to provide the end host and the AAA attendant with a unique and fresh session key after a successful AAA exchange (and in this context based on a successful EAP authentication). The session key for the AAA attendant is therefore most likely provided by the AAA infrastructure whereas the end host obtains the session as a result of the EAP authentication and key exchange procedure. As an alternative to this procedure it is possible to establish a session key before client authentication takes place. This approach is chosen by PANA over TLS [6] and by the Secure Network Access Authentication proposal [7]. Care has to be taken in these scenarios, however, to avoid man-in-the-middle attacks.

Recent activities try to create a common framework for key derivation which is described in [8] and might also be applicable for this context. The key derivation and key transport procedure defined for EAP aims to provide session keys for link layer devices (see Section 1 of [8] with [9] and [10] as an example) but might also serve the purpose of creating

the pre-requisites for network layer protection (for example IPsec). One
building block, which is missing in this context, is a (generic)
mechanism for negotiation of algorithms and parameters, e.g. IPsec
security association parameters.

Given this functionality, which cannot be used by all EAP methods, the
question remains for what purpose these keys should be used (key
derivation) and where these keys have to be delivered (i.e. key
transport). Additionally the corresponding security association has to
be created which might either require third-party or two-party algorithm
and parameter negotiation. The difference between them has influence on
the performance similar to in-band vs. out-of-band protocols discussed
in other areas.

Additionally it should be mentioned that local re-authentication can be
provided when a session key is distributed and known to the local AAA
server. This local re-authentication might even use a different
authentication mechanism. In some scenarios such a procedure might
provide some performance advantages. Draft [11] describes some issues in
this context.

3.4 Providing secure network access

To grant access only for authenticated hosts/users can also be
accomplished by per-packet authentication. This prevents threats caused
by IP spoofing or threats which are caused due to mobility and a missing

disconnect indication. Such a per-packet authentication behavior
(including integrity protection) might also be of interest in a QoS
based environment with different QoS treated flows. The ability of
EAP/AAA to distribute session keys to establish an IPsec security
association between the end host and the first IP hop comes is an
example for this. In comparison to installed filter rules per-packet
authentication provides a more secure ability to associate each
individual IP packet with an authenticated user or host (which is
especially interesting for accounting but also of interest for
preventing unauthorized traffic to enter the network).

Another good reason for establishing such a security association is to
provide security for the first hop independently of the underlying link
layer technologies against various attacks on the wireless link.
Although there are good reasons for additionally providing link-layer

protection (at least for link layer signaling messages) there are many
reasons for providing the protection (possibly in addition) at the
network layer. The different arguments have already been extensively
discussed in various communities and will not be repeated in this
document.

A number of dead peer detection mechanisms have been proposed for
detecting 'disconnected' hosts which might be of interest for
performance reasons. The interested reader might want to take a look at
[12] as one promising proposal. There are, however, a number of other
proposals.

It is worth mentioning that an IPsec security association might be
useful for a number of other reasons such as micro-mobility, QoS
signaling, context transfer and other protocols.

3.5 Providing secure address configuration

There was often the discussion with what pre-requisites a PANA protocol
should start. Currently it is assumed that PANA is invoked after IP
address assignment (see [13]). There are, however, some threats which
address unprotected configuration messages in both stateful and
stateless address autoconfiguration. It is worth to mention that this
issue is still in discussion.

In addition to the discussion of how to protect the address
configuration procedure it might be necessary to consider how to obtain
some other configuration information like DNS servers etc. Since the
relationship to work done in the IPsec remote access working group is
apparent it might also be of interest to investigate secure address
bootstrapping mechanisms in this area. For securing address
configuration procedures [14] and [15] have been proposed.

It has to be clarified whether secure address configuration is
considered by the working group.

4 Discussion of PANA assumptions

This section aims to review some of the assumptions which appeared in
the PANA environment, and their implications. It is important to note
that certain assumption (e.g. the necessity of user identity

confidentiality) has far-reaching implications on the mechanisms
available to satisfy these assumptions.

   User identity confidentiality:

        Recently there has been an increased interest to keep the
        identity used during the authentication process confidential.
        It is important to make this requirement more precise. The
        distinction between protection of the user identity against
        passive attacks, i.e. eavesdropping, and active attacks, i.e.
        modification or insertion of data, is crucial. For short, we
        call the two different requirements active or passive user
        identity confidentiality. Passive user identity
        confidentiality can be provided by both, symmetric and
        asymmetric cryptographic methods, whereas active user identity
        confidentiality typically requires the use of asymmetric
        cryptographic methods. Furthermore, it must be decided for
        which peer (initiator or responder) active or passive user
        identity confidentiality is required. Providing active user
        identity protection for the initiator and the responder is not
        possible (see e.g. the discussion around IKEv2.

        Because of the involved entities in an EAP/AAA message
        exchange it furthermore has to be investigated against which
        entities this protection has to be provided (outsiders or
        network nodes) and whether one should mandate identity
        protection for a protocol in all environments. It should be
        considered that pseudonyms or temporal identities, which are
        also used to provide user identity confidentiality, might
        require a different protection. Additionally there are
        scenarios (for example described in [16] and in [3]) where the
        connection between the end host and the access network is a
        point-to-point link which makes eavesdropping quite difficult.
        It should also be noted that elaborate user identity
        protection schemes at higher layers are quite useless when the
        user identity can be inferred from lower layer identities,
        e.g. IP addresses or MAC addresses (like in IEEE 802.11). We
        conclude that the cost of implementing a particular form of
        user identity protection in the intended environment should be
        carefully considered.

H. Tschofenig   [Page 7]

Internet Draft   9 January 2003

        Ideally as a user it might be desirable to provide some form

of identity protection which only allows the home network to learn the identity during authentication. In case of alternative means of access described in [Section 2](#) a pre-paid service might not require user identity confidentiality since the identity is temporary.

Tunneling Approach:

Support for legacy authentication mechanisms is often mentioned as a justification for proposing TLS-based tunneling approaches (in addition to user identity confidentiality). Apart from the question what to call a legacy authentication protocol it should be considered whether replacing the legacy mechanisms which may not satisfy all desired security requirements with a better mechanisms is preferable, given the time horizon of the PANA working group.

Although this property is not a requirement it has some implications for a PANA protocol. The following issues might be of interest:

- At which entity should the tunnel be terminated?

- How should the end host decide where to terminate the tunnel?

- Which protocol should be used to provide the tunnel?

- What are the performance implications caused by the tunnel?

- Why is it necessary to provide protection for all EAP methods although only a few would benefit from the established tunnel?

- Is the chosen tunnel approach secure against man-in-the-middle attacks (see also below)?

On the other hand some protection of information exchanged between the PaC and the PAA might be desirable such as EAP messages other than those carrying authentication and key exchange protocol payloads and content outside these EAP messages (e.g. device identifier or filter rules, Mobile IP related information, etc.).

If the tunnel is terminated in the access network then in a global roaming case a public key infrastructure is introduced since the end host must be able to authenticate the access

network based on the certificate received during the access
network to end host authentication. Additionally the end host
must be able to authorize the certificate of the access
network as one of a 'valid' access network provider. If the
certificate validation is not possible then an adversary could
impersonate an access network to act as a man-in-the-middle
adversary. As an alternative to a tunnel approach, one could
use mutual public key-based authentication executed between
the end host and the attached access network (e.g. TLS with
mutual authentication), but this would require the
distribution of certificates to clients, which would be much
more costly than simply having certificates for servers.

Disconnect indication:

Disconnect indication allows the to detect whenever an end
host has lost connectivity. As discussed in [Section 3](#) the
properties of the useful mechanisms might show considerable
differences. Hence it might be interesting to determine
whether this property is really required and whether a
timer/lifetime negotiation is required. Periodic re-
authentication, dead peer detection mechanisms, secure
heartbeat (i.e. a challenge/response) protocol and others
might require a negotiation of timers/lifetime is required to
avoid an inappropriate large number (or low number) of
protocol exchanges.

[5](#) Building Blocks

This section tries to list some of the possible building blocks which
might be required for a more advanced protocol. Which of these are
relevant for PANA is subject for further study. The individual parts
have been discussed at various sections.

Discovery of the PAA: In order to exchange the EAP payloads between
the PaC and the PAA it is necessary to discover the entity by
some mechanism. Using the first IP hop (default router) as the
PAA might simplify this discovery procedure.

Negotiation of authentication mechanisms: EAP supports a number of
different EAP methods and therefore it might be required to
agree on a specific mechanism. An unprotected negotiation
mechanism is supported in EAP. A secure negotiation procedure
for the GSS-API methods, which is also supported in EAP, is
described in [[17](#)].

EAP message transport: Finally EAP messages have to be exchanged
        between the various nodes using an agreed transport mechanism.

Several mechanisms have been proposed but further
investigation for the suitability might be required. Some
issues to consider are at least reliable message delivery with
fragmentation support. Fragmentation might for example be
required for some public key based authentication mechanisms.
In Section 4.5 of [13] congestion control is also mentioned as
a feature which must be supported.

Session key distribution and transport: As described in Section 3
it might be desirable to distribute a session key for
subsequent link layer or network layer protection. Session key
distribution within the Diameter protocol is already described
in [18]. Please note that Jesse Walker et. al. have recently
raised some concerns regarding the current description of the
key distribution in [19]. Various drafts mention the
possibility to provide key distribution to link layer devices.

Session key derivation:

EAP methods sometimes provide their own key derivation
procedure whereas others provide no key derivation at all.
Since the key derivation procedure heavily depends on the
protocol for which the session keys are used. Since the key
derivation procedure heavily depends on the protocol for which
the session keys are used it is beneficial to have a generic
session key derivation. Such a framework and many issues
associated with it are explained in [8]. If session key
derivation is only relevant for EAP methods then no further
actions need to be taken. If PANA defines additional
mechanisms or specific session key transport mechanisms then
further thoughts are required. In case of the tunneling
approach the man-in-the-middle attack problems discovered by
V. Niemi, K. Nyberg and N. Asokan, which are described in
[20], might require that the session keys of the two phases
are cryptographically combined as a possible solution to the
problem. Note, however, that EAP methods that do not
distribute a session key, which is particularly true for some
legacy authentication mechanisms, cannot be fixed by this
mechanism. From the problem description we can conclude that

the tunneling approaches introduced insecurity even for
previously secure authentication protocols (when used in this
environment). In Appendix B a small discussion of the
implications of the tunneling approaches is given. In a
recently published IETF draft [21] J. Puthenkulam et. al. also
describe the man-iin-the-middle attack in detail.

A few members in the CFGR working group are currently
investigating approaches for creating a unified session key

derivation framework. A previously published proposal by
Blumenthal [22] serves as one interesting input document.

SA establishment/negotiation: Distributing a session key is
    unfortunately not sufficient for providing link layer or
    network layer protection. Instead a security association is
    required with information about algorithms and corresponding
    parameters. These parameters need to be negotiated.

Filter rule installation: To allow network access after a
    successful authentication and authorization step filter rules
    might either be installed locally (via an API call, CLI, etc.)
    or first need to be send to the corresponding device(s).

6 Mobility Implications

Mobility places some constraints on signaling protocols executed
(roundtrips, latency, etc.) and on how to combine different protocols
(in-band signaling) to be even more efficient. Mobile IP ([23] and [24])
is an example of such a protocol where signaling messages are
transmitted immediately after roaming. Hence it was logical step to
combine the network access procedures using AAA (which are also executed
immediately after roaming) with mobility signaling. [25] explains such a
procedure for Mobile IP (IPv4) and [26]/[27] envision a similar approach
for IPv6.

Although these proposals use a custom security mechanisms for
authentication, key exchange and for protection of protecting of the
mobility payloads [27] mentions the use of EAP. Replacing the custom
security mechanism with EAP would allow different authentication and key
exchange protocols to be used. Since the payloads used by Mobile IP,
which are ideally carried with the same messages (i.e. in-band), must be

protected, the following issues require further thoughts:

- How are Mobile IP payloads protected? Using the custom security protection defined in ([2] or [27]) the MIP payloads are simply included by the keyed message digest calculation among other fields. If EAP is used instead of this custom security mechanism, which key is used for the protection of the payloads?

- Is the above scheme of payload protecting extensible to all EAP methods? For the author it seems that this is not fully the case if we consider secure password based protocols. These protocols require that the message payloads where the password is cryptographically applied is not vulnerable to dictionary attacks. This is mainly achieved by either encrypting the password with a random component or vice versa. If known plaintext (e.g. Mobile IP parameter) is encrypted with the

password then this property is destroyed.

- Which other payloads (apart from Mobile IP) would benefit from in-band signaling in AAA (and also require protection)?

It is therefore up to the working group to decide whether PANA should be designed in such an extensible way to include these (and possibly other) parameters. Mobility (especially seamless mobility) clearly places some performance restrictions to a PANA protocol. Hence it might not be able to run an 'arbitrary' number of roundtrip between the end host and a possibly far distant home network before transmitting mobility related signaling messages.

[7] Conclusion

This draft aims to show the relationship to other protocols which are relevant for PANA. It therefore tries to address the question what the result of a PANA protocol exchange should be. In the past there has been some confusion about the working direction of the group. In Section 3 possible outcomes of a PANA protocol execution are presented with various degrees of complexity. Depending on the focus of the group the working group may try to achieve (the given list might):

- Pure EAP message transport

- EAP message transport with installation of filter rules

- Full secure network access protocol

The working group seems to focus on EAP as a container for authentication and key exchange protocols. Hence similar protocols such as SASL are not considered in this document.

It is possible that a single protocol (without optional components) might not completely fit in all environments.

8 Security Considerations

This document addresses a number of security issues but no protocol is proposed. Hence as such no separate security considerations are presented.

9 Acknowledgements

I would like to thank (in alphabetical order) Wolfgang Buecker, Jorge Cuellar, Guenther Horn, Dirk Kroeselberg, Yoshihiro Ohba and Basavaraj Patil for their comments to this document. Additionally I would like to thank all members of the EU funded project Shaman for their fruitful

discussions. I would like to particularly thank the following WP1 Shaman members: Krister Boman, Fredrik Lindholm, Valtteri Niemi, Kaisa Nyberg, Chris Mitchell, Scarlet Schwiderski-Grosche, Heiko Knospe, Tobias Martin, Joachim Schaaf, Peter Windirsch and Peter Howard.

Finally, I would like to thank Alper Yegin for encouraging me to write this document and for his comments.

A Relationship to filter rule installation

The goal of establishing filter rules at some devices seems to be similar to the activities in the Midcom working group. Hence it might be of interest to look at some of the proposals and additionally at drafts published in this context such as TIST [28], which is based on RSVP, or a more recent approach CASP-Midcom [29], which reuses the same ideas based on the CASP protocol [30]. These two proposals allow an end host to communicate filter rules to devices (more or less) along the data path. A mechanism for discovering these devices is also provided by

these proposals. There are, however, differences between the work done in the Midcom and the NSIS group and the considerations made for PANA. First, filter rules are installed for particular message flows only (typically described by a 5-tuple) and not to grant entire network access. Additionally at least [28] has no means to transport EAP messages and in [29] only the basic idea is mentioned without elaborating the details. Second, for these two protocols there must be a mechanism to restrict the filter rule installation only at the edge devices or within the local network only. Without such a mechanism the messages travel towards the given destination address. Ideas for such a scoped/localized signaling message exchange are already considered but not fully investigated. Additionally it must be mentioned that the signaling procedure in these two protocols is heavily based on the assumption of topology insensitivity. This also causes filter rules to be uni-directional.

B Tunneling Implications

In Section 5 the man-in-the-middle attack is described in context of the session key derivation and tunneling approaches. As a solution of the problem the documents [20] and [21] suggest to cryptographically bind the session keys of the two phases, the TLS session key and the session key deriving from the EAP method, to each other. Afterwards the knowledge of this derived session key has to be proven either implicitly or explicitly. In case of an implicit binding the combined session key is used to protect the communication between the two end points. This approach obviously requires that the derived session key is used afterwards for data protection. In order to provide the knowledge of a combined session key for an explicit binding an additional message exchange is required. In Section 4 of [20] an example of such a

cryptographic explicit binding is described which is based on a keyed message digest. Since these tunneling approaches have been introduced to protect legacy authentication mechanisms, which in some cases do not derive a session key as part of the authentication process, the question remains how such a cryptographic binding can be established in these cases. In [20] a 'binding agent' is introduced which combines the session of the tunnel (for example the TLS established session key) and the long-term secret used for the EAP method in case that no session key is created.

Existing tunneling proposals use two different types of tunnels:

Tunnel endpoint identical with EAP end point: With this tunnel the
    EAP endpoint and the tunnel endpoint are co-located. This type
    of tunnel is used with EAP-TTLS [31], PEAP [32] and in PIC
    [33]. If the client authentication mechanism does not create a
    session key then the long-term secret between the user and the
    authentication server (e.g. AAAH) can be used by the binding
    agent to derive a new session key. To securely deliver the
    user's long-term secret to the binding agent might not be a
    serious problem since the endpoints are likely to be in the
    same administrative domain.

Tunnel endpoint not identical with EAP end point: With this tunnel
    the EAP endpoint is not the same as the tunnel end point of
    the tunnel. This type of tunnel is used by the PANA over TLS
    proposal [6] and by the Secure Network Access Authentication
    proposal [7]. In these proposals the tunnel end point is
    established between the PaC and the PAA to protect the EAP
    message exchange between these two nodes. The EAP messages
    exchanged by the protected tunnel are then possibly forwarded
    to a backend server (e.g. to a AAAH server) using a AAA
    infrastructure. If a mobile node roams to a new network then
    the tunnel (i.e. TLS tunnel) is terminated at the PAA and the
    EAP messages travel all the way back to the home AAA server.
    In order to use the same procedure as above the binding agent
    needs to have both keys (the session key established with the
    TLS tunnel and the user's long term secret). It would be
    problematic to transfer the user's long-term secret to the
    visited network where the TLS tunnel terminates. Hence one
    possibility is to transfer the TLS established session key to
    the end point of the EAP method. After the binding agent at
    the AAAH server derives the combined session key it is
    transferred back to the tunnel end point in the visited
    network (i.e. to the PAA) since it might be used to secure the
    data traffic between the PaC and some node in the visited
    network.

C Authors' Address

Hannes Tschofenig
Siemens Corporate Technology

Otto-Hahn-Ring 6
81739 Munich
Germany
EMail: Hannes.Tschofenig@siemens.com

D Bibliography

[1] H. Knospe and S. Schwiderski-Grosche, "Online payment for access to heterogeneous mobile networks," in IST Mobile and Wireless Telecommunications Summit 2002 , 2002.

[2] P. Flykt, C. Perkins, and T. Eklund, "AAA for IPv6 network access," Internet Draft, Internet Engineering Task Force, Mar. 2002. Work in progress.

[3] M. Parthasarathy, "Pana threat analysis and security requirements," internet draft, Internet Engineering Task Force, 2002. Work in progress.

[4] H. Tschofenig, "Nsis threats," internet draft, Internet Engineering Task Force, 2002. Work in progress.

[5] P. Calhoun, S. Farrell, and W. Bulley, "Diameter CMS security application," Internet Draft, Internet Engineering Task Force, Mar. 2002. Work in progress.

[6] Y. Ohba, S. Baba, and S. Das, "Pana over tls," Internet Draft, Internet Engineering Task Force, 2002. Work in progress.

[7] D. Forsberg and J. Rajahalme, "Secure network access authentication (senaa)," Internet Draft, Internet Engineering Task Force, 2002. Work in progress.

[8] B. Aboba, "The EAP session key problem," Internet Draft, Internet Engineering Task Force, Feb. 2002. Work in progress.

[9] I. D. 802.11i/D2, "Draft supplement to standard for telecommunications and information exchange between systems – lan/man specific requirements – part 11: Wireless medium access control (mac) and physical layer (phy) specifications: Specification for enhanced security," tech. rep., 2001.

[10] I. S. 802.11-1997, "Information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications," tech. rep., 1997.

[11] S. Faccin and F. Le, "AAA local security association (LSA): The temporary shared key (TSK)," Internet Draft, Internet Engineering Task Force, July 2001. Work in progress.

[12] G. Huang, S. Beaulieu, and D. Rochefort, "A traffic-based method of detecting dead ike peers," internet draft, Internet Engineering Task Force, 2002. Work in progress.

[13] A. Yegin, R. Penno, et al. , "Protocol for carrying authentication for network access (PANA)requirements and terminology," Internet Draft, Internet Engineering Task Force, July 2002. Work in progress.

[14] B. Patel, B. Aboba, S. Kelly, and V. Gupta, "DHCPv4 configuration of IPSEC tunnel mode," Internet Draft, Internet Engineering Task Force, May 2001. Work in progress.

[15] D. Dukes and R. Pereira, "The ISAKMP configuration method," Internet Draft, Internet Engineering Task Force, Oct. 2001. Work in progress.

[16] Y. Ohba et al. , "Problem space and usage scenarios for PANA," Internet Draft, Internet Engineering Task Force, June 2002. Work in progress.

[17] E. Baize and D. Pinkas, "The simple and protected GSS-API negotiation mechanism," RFC 2478, Internet Engineering Task Force, Dec. 1998.

[18] E. Gustafsson, W. Bulley, A. Rubens, J. Haag, G. Zorn, and D. Spence, "Diameter NASREQ application," Internet Draft, Internet Engineering Task Force, Mar. 2002. Work in progress.

[19] J. Walker, R. Housley, and N. Cam-Winget, "AAA key distribution," Internet Draft, Internet Engineering Task Force, Apr. 2002. Work in progress.

[20] N. Asokan, V. Niemi, and K. Nyberg, "Man-in-the-middle in tunnelled authentication," in http://eprint.iacr.org/2002/163/ , 2002.

[21] J. Puthenkulam, V. Lortz, A. Palekar, D. Simon, and B. Aboba, "The compound authentication binding problem," internet draft, Internet

Engineering Task Force, 2002. Work in progress.

---

[22] U. Blumenthal, "Secure session key generation. creating PRF from
MAC function," Internet Draft, Internet Engineering Task Force, July
2002. Work in progress.

[23] C. Perkins and Ed, "IP mobility support for IPv4," RFC 3220,
Internet Engineering Task Force, Jan. 2002.

[24] D. Johnson, C. Perkins, and J. Arkko, "Mobility support in IPv6,"
Internet Draft, Internet Engineering Task Force, July 2002. Work in
progress.

[25] C. Perkins and E. Gustafsson, "AAA registration keys for mobile
IP," Internet Draft, Internet Engineering Task Force, Mar. 2002. Work
in progress.

[26] F. Dupont et al. , "AAA for mobile IPv6," Internet Draft, Internet
Engineering Task Force, Nov. 2001. Work in progress.

[27] S. Faccin et al. , "Diameter mobile IPv6 application," Internet
Draft, Internet Engineering Task Force, Nov. 2001. Work in progress.

[28] M. Shore, "The TIST (topology-insensitive service traversal)
protocol," Internet Draft, Internet Engineering Task Force, May 2002.
Work in progress.

[29] H. Tschofenig and H. Schulzrinne, "A firewall/nat traversal client
for casp," internet draft, Internet Engineering Task Force, 2002. Work
in progress.

[30] H. Schulzrinne, H. Tschofenig, X. Fu, J. Eisl, and R. Hancock,
"Casp - cross-application signaling protocol," internet draft, Internet
Engineering Task Force, 2002. Work in progress.

[31] P. Funk and S. Blake-Wilson, "EAP tunneled TLS authentication
protocol (EAP-TTLS)," Internet Draft, Internet Engineering Task Force,
Mar. 2002. Work in progress.

[32] H. Andersson, S. Josefsson, G. Zorn, et al. , "Protected
extensible authentication protocol (PEAP)," Internet Draft, Internet
Engineering Task Force, Feb. 2002. Work in progress.

[33] Y. Sheffer, H. Krawczyk, and B. Aboba, "PIC, a pre-IKE credential provisioning protocol," Internet Draft, Internet Engineering Task Force, Feb. 2002. Work in progress.