IETF PANA Working Group
Internet Draft

H. Tschofenig
Siemens
Corporate Technology

A. Yegin
DoCoMo USA Labs

D. Forsberg
Nokia

Document:
draft-tschofenig-pana-bootstrap-rfc3118-00.txt
Expires: December 2003 June 2003

Bootstrapping RFC3118 Delayed authentication using PANA
<draft-tschofenig-pana-bootstrap-rfc3118-00.txt>

Status of this Memo

Abstract

PANA provides network access authentication and uses the Extensible Authentication Protocol (EAP) to carry different authentication methods. The combination of EAP with an AAA architecture allows authentication and authorization of a roaming user to an access network.

DHCP is a protocol which provides an end host with configuration parameters. Without proper security for DHCP an adversary can mount a number of attacks.

It seems to be reasonable to use the authentication and key exchange procedure executed during the network access authentication to bootstrap a security association for DHCP.

Table of Contents

1. Introduction

PANA [PANA] provides network access authentication by carrying Extensible Authentication Protocol (EAP) between the hosts and the access networks. The combination of EAP with an AAA architecture allows authentication and authorization of a roaming user to an access network. A successful authentication between a client and the network produces a dynamically created trust relation between the two. Various EAP authentication methods are capable of generating

cryptographic keys (e.g., shared secrets) between the client and the authentication agent after successful authentication.

DHCP [RFC2131] is a protocol which provides an end host with configuration parameters. The base DHCP does not include any security mechanisms, hence it is vulnerable to a number of security threats. Security considerations section of RFC 2131 identifies this protocol as "quite insecure" and lists various security threats.

RFC 3118 is the DHCP authentication protocol which defines how to authenticate various DHCP messages. This protocol extension does not support roaming clients and assumes the availability of an out-of band shared secret between the client and the DHCP server. These limitations have been inhibiting widespread deployment of this security mechanism.

It seems to be reasonable to use the authentication and key exchange procedure executed during the network access authentication to bootstrap a security association for DHCP. The trust relation created during the access authentication process can be used with RFC 3118 to provide security for DHCP. This document defines how to use PANA to bootstrap RFC 3118 for securing DHCP.

PANA protocol allows clients to use this protocol even before they are assigned an IP address. A PANA client (PaC) can use the unspecified IP address as its source address during this phase.

PANA thereby offers a split between the two protocols:

- Authentication and key exchange
  (provided by PANA and EAP in particular)
- DHCP message protection by generating the required shared secrets
  for RFC 3118.

Instead of adding EAP support to DHCP itself (which requires modifications to the DHCP protocol due to the nature of EAP messaging) we separate the two protocols. We call this procedure bootstrapping RFC 3118.

This document is organized as follows. Section 2 describes new terms. Section 3 gives an overview of the basic communication and describes the building blocks. Requirements are presented in Section 4. The details of the established parameters for the DHCP SA are listed in Section 5. Processing details and payload formats are illustrated in Section 6. A short message flow describes the protocol interaction in Section 7. Finally in Section 8 additional security considerations are discussed.

2. Terminology

This document uses the following term:

- DHCP security association

To secure DHCP messages a number of parameters including the key that is shared between the PaC (DHCP client) and the DHCP server have to be established. These parameters are collectively referred as DHCP security association (or in short DHCP SA).

- DHCP Key

This term refers to the fresh and unique session key dynamically established between the DHCP client (PaC) and the DHCP server. This key is used to protect DHCP messages as described in [RFC3118].

Further PANA related terms can be found in [PY+02].

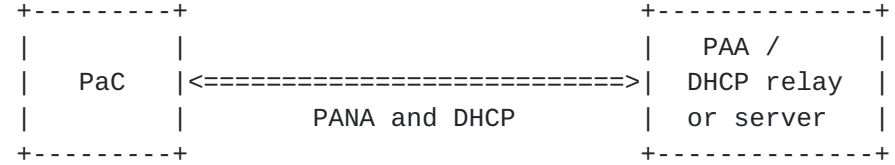
In this document, the key words "MAY", "MUST, "MUST NOT", OPTIONAL","RECOMMENDED "SHOULD", and "SHOULD NOT", are to be interpreted as described in [RFC2119].

3. Overview and Building Blocks

Based on the PANA protocol interaction this bootstrapping protocol requires protocol interaction between the PaC (which acts as DHCP client), the PANA Authentication Agent (PAA) and the DHCP server. A security association will be established between the DHCP server and the DHCP client to protect DHCP messages.

PAA is located one IP hop away from the PaC. If the DHCP server is on the same link, it can be co-located with the PAA. When PAA and DHCP server are co-located, an internal mechanism, such as an API, is sufficient for inter-process communication. If the DHCP server is multiple hops away from the DHCP client, then there must be a DHCP relay on the same link as the client. In that case, PAA will be co-located with the DHCP relay. The required parameters can be communicated to the DHCP server using the DHCP relay agent information options [DS02]. For the purpose of confidentiality protection IPsec protection can be applied as described in [SL+03].

The protocol interaction is illustrated in Figure 1.



Legend:

PaC - PANA Client
PAA - PANA Authentication Agent

Figure 1: DHCP Protocol Bootstrapping

The following building blocks have been identified:

3.1 PaC <-> PAA Communication

Additional payloads are required within PANA as indicated with (A) in Figure 1. These payloads therefore provide the following functionality:

a) Capability indication

A capability describes a certain functionality which is either supported or not. In order to trigger an action or to obtain a certain kind of data item it is necessary to execute some message exchanges. This message exchange allows both entities to learn commonly supported functionality.

b) Trigger message

A trigger message allows one entity (either PaC or PAA) to request a certain action to be executed. For this protocol a trigger message sent by the PaC causes the PAA to create the DHCP security association for support with [RFC3118].

Section 6 describes the message payloads for the additional objects required in PANA the usage with this bootstrapping protocol.

3.2 PAA <-> DHCP Communication

If the PAA and the DHCP server are co-located then only an API call is required for transferring the necessary information from the PAA to the software modules of the DHCP server. If the PAA and the DHCP server are not co-located then an additional protocol is needed to transport the security parameters from the PAA to the DHCP server. [WH+02] points to the importance of this communication as: "Key distribution is not merely a data transport operation; it is also a mechanism for building transitive trust;". Indeed the trust relationship between the PaC and the PAA, which was dynamically established during network access authentication, is used to extend the trust relationship to the DHCP server. The PAA, which is co-located with the DHCP Relay, and the DHCP server trust each other

and both entities belong to the same administrative domain as the PAA.

Security sensitive information has to be exchanged (such as session keys) between the DHCP relay (PAA) and the DHCP server. This protocol is not part of PANA but the security implications must be considered.

Two different protocols have been suggest in the past to support key transport: Radius and Diameter

In order to secure the key transport key wrap mechanisms for Diameter and for Radius have been specified (see [CFB02] and [RFC2548]). The protection mechanism for key transport for Diameter applies application level security mechanisms based on CMS whereas Radius uses lower-layer security mechanisms such as IPsec.

In this context another approach might be possible: [DS02] allows a DHCP relay to add information which is then sent to the DHCP server. [SL+03] proposes IPsec protection of the DHCP messages exchanged between the DHCP relay and the DHCP server. DHCP objects itself (protected with IPsec) can therefore be used to communicate the necessary parameters.

Further work is required to
(a) select one protocol which provides adequate security for the key transport
(b) specify object payloads to carry the parameters between the PAA and the DHCP server.

3.3 Key Derivation

As a result of the EAP authentication and key exchange method a Master Session Key (MSK) is established which is used to establish a PANA security association. The key derivation procedure for establishing this PANA SA is defined in [PANA]. Another security association for usage with DHCP according to [RFC3118] needs to be established. A discussion of the required parameters for the security association is given in Section 5 and the key derivation function is provided in Section 6.2

Since different bootstrapping applications need different keys it is necessary to derive these keys from the session key provided by the EAP method.

4. Requirements

The following requirements regarding protocol design and deployment have to be met:

- The DHCP protocol as defined in [RFC2131] MUST NOT be modified.

- The security mechanism defined in [RFC3118] MUST NOT be modified. Instead it will be used as a basis for bootstrapping the security with the help of PANA.

- The key derivation procedure MUST establish a unique and fresh session key for the usage with [RFC3118]. The session key MUST never be used again in another protocol run or with another DHCP server.

- It MUST be ensured that only the intended parties have access to the session key. Hence the key transport between the PAA and the DHCP server MUST be authenticated, integrity, replay and confidentiality protected. The security mechanism used to protect the transport of the session key between the PAA and the DHCP server MUST have an adequate key strength. Section 5.4 of [AS03] offers a description of issues concerning key wrapping.

- The DHCP server MUST ensure that only authorized nodes are allowed to install keying material for subsequent DHCP message protection.

- The established DHCP security association MUST provide data origin authentication, integrity protection and replay protection. A non-goal of this draft is to provide confidentiality protection for DHCP messages.

- The session key between the PaC and the DHCP server becomes active immediately when the PAA returns a PANA message indicating the successful completion of the bootstrapping procedure. The lifetime of the session key at the DHCP is limited to the indicated lifetime. The session key MUST NOT be used beyond that lifetime. Key confirmation of the established session key between the PaC and the DHCP server is provided by exchanging the first DHCP messages.

- Key Naming

The derived session key (DHCP key) MUST be bound to a particular session between the particular PaC and a DHCP server. It MUST be possible for the two peers (PaC and DHCP server) to verify that each other is indeed the intended recipients of the distributed session key.

5. Security parameters for RFC 3118

5.1 Authentication Option of RFC 3118

[RFC3118] defines two security protocols with a newly defined authentication option:

- Configuration token
- Delayed authentication

The generic format of the authentication option is defined in Section 2 of [RFC3118] and contains the following fields:

- Code (8 bits)
- Length (8 bits)
- Protocol (8 bits)
- Algorithm (8 bits)
- Replay Detection Method - RDM (8 bits)
- Replay Detection (64 bits)
- Authentication Information (variable length)

5.1.1 Code Field

The value for the Code field of this authentication option is fixed. Since the value for this field is known in advance it does not need to be communicated.

5.1.2 Length Field

The Length field indicates the length of the authentication option payload. Since the value for this field can be computed it does not need to be communicated.

5.1.3 Protocol Field

[RFC3118] defines two values for the Protocol field - zero and one. A value of zero indicates the usage of the configuration token authentication option.

As described in Section 4 of [RFC3118] the configuration token only provides weak entity authentication. Hence the usage is inappropriate. This authentication option will not be considered for the purpose of bootstrapping.

A value of one in the Protocol field in the authentication option indicates the Delayed authentication. The usage of this option is subsequently assumed in this document.

Since the value for this field is known in advance it does not need to be communicated.

5.1.4 Algorithm Field

[RFC3118] only defines the usage of HMAC-MD5 (value 1 in the Algorithm field). This document assumes that HMAC-MD5 is used to protect DHCP messages.

Since the value for this field is known in advance it does not need to be communicated.

5.1.5 Replay Detection Method (RDM) Field

The value of zero for the RDM name space is assigned to use a monotonically increasing value.

Since the value for this field is known in advance it does not need to be communicated.

5.1.6 Replay Detection Field

This field contains the value which is used for replay protection and it MUST be monotonically increasing according to the provided replay detection method.

An initial value must, however, be set. In case of bootstrapping with PANA an initial value of zero is used. The length of 64 bits (and a start-value of zero) ensure that a sequence number roll-over is very unlikely to occur.

Since the value for this field is known in advance it does not need to be communicated.

5.1.7 Authentication Information Field

The content of this field depends on the type of message where the authentication option is used. Section 5.2 of [RFC3118] does not provide content for the DHCPDISCOVER and the DHCPINFORM message. Hence for these messages no additional considerations need to be specified in this document.

For a DHCPOFFER, DHCPREQUEST or DHCPACK message the content of the Authentication Information field is given as:

- Secret ID (32 bits)
- HMAC-MD5 (128 bits)

The Secret ID is chosen by the PAA to prevent collisions.

HMAC-MD5 is the output of the key message digest computation. Note that not all fields of the DHCP message are protected as described in [RFC3118].

5.2 Lifetime of the DHCP security association

The lifetime of the DHCP security association has to be limited to prevent the DHCP from storing state information over a long time.

The lifetime SHOULD be set to exceed the DHCP lease time. Since access control implemented with the help of packet filters or cryptographic data protection has to be associated somehow with the accounting system it is a policy decision for the network to specify a particular lifetime.

The DHCP server, the PAA, the Enforcement Point (EP) and the AAA server should be aware (directly or indirectly) of the lifetime.

The PaC can at any time trigger a new bootstrapping protocol run to establish a new security association with the DHCP server.

6. Processing Details and Payloads

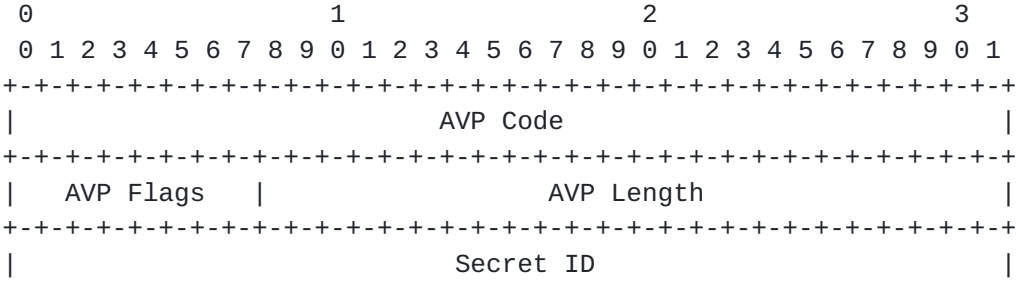
This section defines the necessary extensions for PANA and a key derivation procedure.

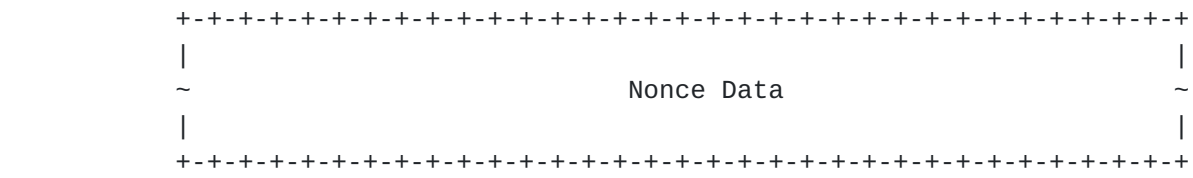
6.1 Capability Indication and Trigger Message

A new PANA AVP is defined in order to bootstrap DHCP SA between the PaC and PAA. DHCP-AVP is included in the PANA_success message if PAA is offering DHCP SA bootstrapping service. If the PaC wants to proceed with creating DHCP SA at the end of the PANA authentication, it MUST include DHCP-AVP in its PANA_success_ack message.

Absence of this AVP in the PANA_success message sent by PAA indicates unavailability of this additional service. In that case, PaC MUST NOT include DHCP-AVP in its response, and PAA MUST ignore if it receives this AVP. When this AVP is received by PaC, it may or may not include the AVP in its response depending on its desire to create DHCP SA. DHCP SA can be created as soon as each entity has received and sent one DHCP-AVP.

The detailed DHCP-AVP format is presented below.



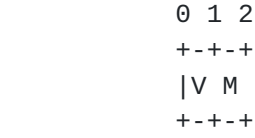


AVP Code

TBD

AVP Flags

The AVP Flags field is eight bits. The following bits are assigned:



M(andatory)

- The 'M' Bit, known as the Mandatory bit, indicates whether support of the AVP is required. This bit is not set in DHCP-AVP.

V(endor)

- The 'V' bit, known as the Vendor-Specific bit, indicates whether the optional Vendor-Id field is present in the AVP header. This bit is not set in DHCP-AVP.

r(eserved)

- These flag bits are reserved for future use, and MUST be set to zero, and ignored by the receiver.

AVP Length

The AVP Length field is three octets, and indicates the number of octets in this AVP including the AVP Code, AVP Length, AVP Flags, and the AVP data.

Secret ID

32 bit value that identifies the DHCP Key produced as a result of the bootstrapping process. This value is determined by PAA and

sent to PaC. PAA determines this value by randomly picking a number from the available session ID pool. If PaC's response does not contain DHCP-AVP then this value is returned to the available identifiers pool.
Otherwise, it is allocated to the PaC until DHCP SA expires. PaC MUST set this field to all 0s in its response.

Nonce Data (variable length)

Contains the random data generated by the transmitting entity. This field contains Nonce_PaC when the AVP is sent by PaC, and Nonce_DHCP when the AVP is sent by PAA. Nonce value MUST be randomly chosen and MUST be at least 128 bits in size. Nonce values MUST NOT be reused.

6.2 Key Derivation

This section describes the key derivation procedure which allows to establish a DHCP security association. The key derivation procedure is reused from IKE [RFC2409]. The character '|' denotes concatenation.

DHCP Key = HMAC-MD5(MSK, const | Session ID | Nonce_PaC | Nonce_DHCP | DHCP-Server-Identity)

The values of have the following meaning:

- MSK

The Master Session Key (MSK) is provided by the EAP method as part of the PANA/EAP protocol execution.

- const

This is a string constant. The value of the const parameter is set to "PANA DHCP Bootstrapping".

- Session ID

This value is a 128-bit value as defined in the PANA protocol [PANA]. This value identifiers a particular session of a client.

- Nonce_PaC

This random number is provided by the PaC and exchanged within the PANA protocol.

- Nonce_DHCP

This random number is provided by the PAA/DHCP server and exchanged with the PANA protocol.

- DHCP-Server-Identity

The DHCP-Server-Identity field contains the IP address of the DHCP to which the session keys will be sent.

- DHCP Key

This session key is 128-bit in length and used as the session key for securing DHCP messages. Figure 1 of [EAP-Key] refers to this derived key as Transient Session Keys (TSKs).

7. Example message flow

This section describes some basic PANA message flows which use DHCP bootstrapping.

Figure 2 depicts a message flow which enables DHCP bootstrapping. The PANA message flow starts with a discovery of the PAA, followed by network access authentication. Finally, after the authentication is successful a PANA security association is established which protects subsequent messages such as the DHCP-AVP. The DHCP-AVP payload contains parameters described in Section 6. As a summary, it indicates that the network supports bootstrapping and provides the necessary parameter if requested by the PaC.

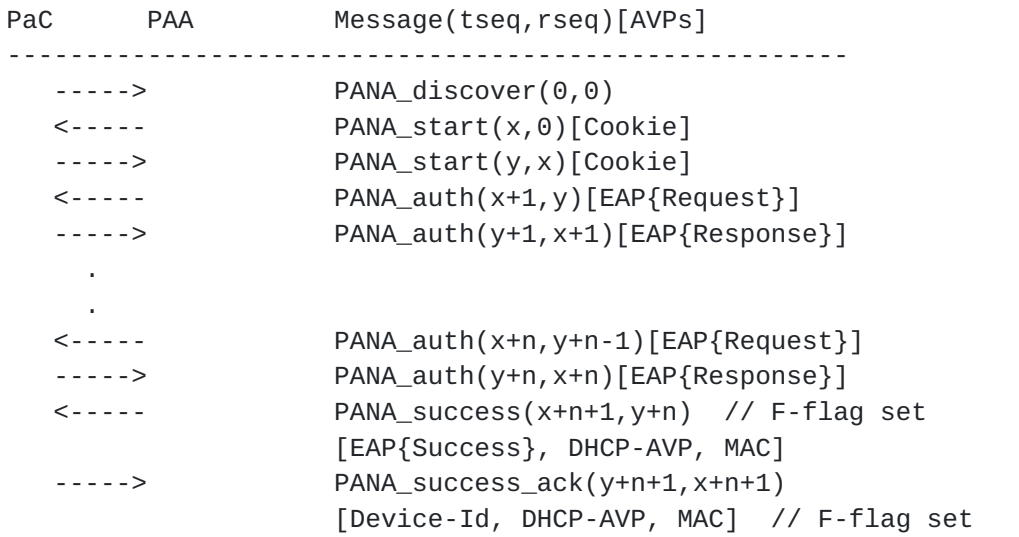


Figure 2: Message flow for PANA DHCP bootstrapping

8. Security Considerations

This document describes a mechanism for dynamically establishing a security association to protect DHCP signaling messages.

PANA uses EAP to support a number of authentication and key exchange protocols. With the functionality of EAP this document therefore supports DHCP security for roaming users.

This document separates the different security mechanisms in a clean way:

a) The appropriate EAP method for a certain scenario, environment or architecture can be chosen. The security properties heavily depend on the chosen EAP method.

b) PANA carries EAP messages and provides additional security. The security features of PANA are described in [PANA].

c) The security mechanism in [RFC3118] is reused for providing authentication, integrity and replay protection.

If the PAA and the DHCP server are co-located then the session keys and the security parameters are transferred locally (via an API call). Some security protocols already exercise similar methodology to separate functionality.

If the PAA and the DHCP server are not co-located then there is some similarity to the requirements and issues discussed with the EAP Keying Framework (see [AS03]). Figure 3 is taken from Section 4.5 of [AS03] and adjusted accordingly. A major different to [AS03] is that the communication between the PAA and DHCP server takes place between the same administrative domain. Hence the security issues described in [WH+03] are much less problematic.

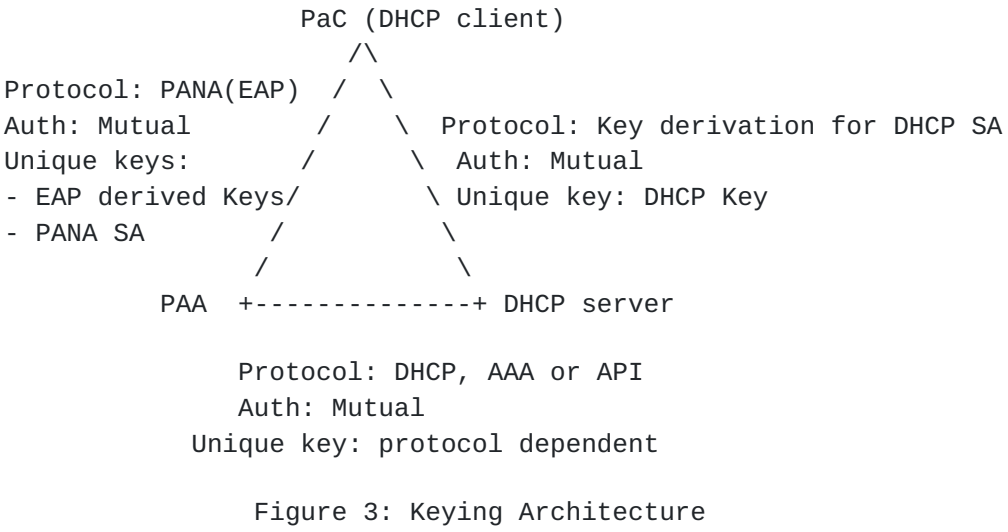


Figure 3: Keying Architecture

Figure 3 describes the participating entities and the protocol executed between them. It must be ensured that the derived session key between the PaC and the DHCP server is fresh and unique.

The key transport mechanism, which is used to carry the session key between the PAA and DHCP server, must provide the following functionality:

- Confidentiality protection
- Replay protection
- Integrity protection

Furthermore it is necessary that the two parties (DHCP server and the PAA) authorize the establishment of the DHCP security association.

Russ Housley recently (at the 56th IETF) presented a list of recommendations for key management protocols which describe requirements for an acceptable solution. Although the presentation focused on NASREQ some issues might also applicable in our context. We will address the presented issues briefly:

- Algorithm independence

Our proposal bootstraps a DHCP security association based on RFC 3118 where only a single integrity algorithm (namely HMAC-MD5) is proposed which is mandatory to implement.

- Establish strong, fresh session keys (Maintain algorithm independence)

PANA relies on EAP to provide strong and fresh session keys for each initial authentication and key exchange protocol run. Furthermore the key derivation function provided in Section 6.2 contains random numbers provided by the PaC and the PAA which additionally add randomness to the generated key.

- Include replay detection mechanism

Replay protection is provided by the PANA protocol itself and by including random numbers for the key derivation procedure which aims to provide a fresh and unique session key between the PaC (DHCP client) and the DHCP server.

Furthermore, the key transport mechanism between the PAA and the DHCP server must also provide replay protection (in addition to confidentiality protection).

- Authenticate all parties

Authentication between the PaC and the PAA is provided by the PANA protocol which utilizes EAP. After establishing a PANA security association key confirmation of this PANA SA is provided.

Key confirmation between the PaC and the DHCP server is provided with the first protected DHCP messages exchanged.

- Perform authorization

Authorization for network access is provided during the PANA exchange. The authorization procedure for DHCP bootstrapping is executed by the PAA after the PaC requests bootstrapping.

The PAA might reject a request for bootstrapping based on local policies.

- Maintain confidentiality of session keys

The DHCP session keys are known to the indented parties only i.e. to the PaC, PAA and the DHCP server.

The PANA protocol does not transport keys at all. The exchanged random numbers which are incorporated into the key derivation function do not need to be kept confidential.

The key transport between the PAA and the DHCP server (in case that these two entities are not co-located) must ensure confidentiality of the session keys.

- Confirm selection of "best" ciphersuite

This proposal does not provide confidentiality protection of DHCP signaling messages. Only a single algorithm is offered for integrity protection. Hence no algorithm negotiation and therefore no confirmation of the selection occurs.

- Uniquely name session keys

The session key is uniquely named by including identifiers of the intended parties (DHCP server and PaC) into the key derivation function. Furthermore a constant "PANA DHCP Bootstrapping" is included which prevents usage of this session key for a different bootstrapping application.

- Compromised PAA

A compromised PAA will be able to learn the DHCP session key and the EAP derived session key (e.g. MSK) and the PANA SA. It will

furthermore be able to corrupt the DHCP protocol executed between mobile end hosts and the DHCP server since
- the PAA either itself acts as a DHCP server or
- the PAA acts as a DHCP relay.

A compromised PAA will also be able to create further DHCP SAs or to perform other known attacks on the DHCP protocol (e.g. address depletion).

A compromised PAA will not be able to modify, reply, inject DHCP messages which use security associations established without the PANA bootstrapping protocol (e.g. manually configured DHCP SAs) or DHCP SAs established with PANA before the PAA was compromised.

- Bind key to appropriate context

The key derivation function described in Section 6.2 includes parameters (such as the DHCP server identity and a constant) which prevents reuse of the established session key for other purposes. The key derivation includes the session identifier to associate the key to the context of a certain PANA protocol session and therefore to a particular client.

9. IANA Considerations

TBD

10. Open Issues

This document describes a bootstrapping procedure for [RFC3118]. The same procedure could be applied for [DHCPv6].

It is necessary to describe the details of the capability negotiation within PANA and to define the DHCP object structure which allows communication of the necessary parameters between the PAA and the DHCP server.

11. References

[DHCPv6] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins and M. Carney: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", Internet-Draft, (work in progress), November, 2002.

[PANA] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig and A. Yegin: "Protocol for Carrying Authentication for Network Access (PANA)", Internet-Draft, (work in progress), March, 2003.

[RFC3118] R. Droms and W. Arbaugh: "Authentication for DHCP Messages", RFC 3118, June 2001.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC2408] Maughhan, D., Schertler, M., Schneider, M., and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[PY+02] Penno, R., Yegin, A., Ohba, Y., Tsirtsis, G., Wang, C.: "Protocol for Carrying Authentication for Network Access (PANA) Requirements and Terminology", Internet-Draft, (work in progress), April, 2003.

[DS02] Droms, R. and Schnizlein, J.: "RADIUS Attributes Sub-option for the DHCP Relay Agent Information", Internet-Draft, (work in progress), October, 2002.

[SL+03] Stapp, M. and Lemon, T. and R. Droms: "The Authentication Suboption for the DHCP Relay Agent Option", Internet-Draft, (work in progress), April, 2003.

[AS03] Aboba, B. and Simon, D.: "EAP Keying Framework", Internet-Draft, (work in progress), March 2003.

[RFC2132] Alexander, S. and Droms, R.: "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[RFC2131] R. Droms: "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[WH+03] J. Walker, R. Housley, and N. Cam-Winget, "AAA key distribution", Internet Draft, (work in progress), April 2002.

[RFC2548] Zorn, G., "Microsoft Vendor-Specific RADIUS Attributes", RFC 2548, March 1999.

[CFB02] Calhoun, P., Farrell, S., Bulley, W., "Diameter CMS Security Application", Internet-Draft, (work in progress), March 2002.

12. Acknowledgments

Place your name here.

13. Author's Addresses

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

Alper E. Yegin
DoCoMo USA Labs
181 Metro Drive, Suite 300
San Jose, CA, 95110
USA
Phone: +1 408 451 4743
Email: alper@docomolabs-usa.com

Dan Forsberg
Nokia Research Center
P.O. Box 407
FIN-00045 NOKIA GROUP, Finland
Phone: +358 50 4839470
EMail: dan.forsberg@nokia.com

Full Copyright Statement