Network Working Group
Internet Draft

A. Yegin
DoCoMo USA Labs
H. Tschofenig
Siemens Corporate Technology
D. Forsberg
Nokia

Expires: August 2004

February 2004

Bootstrapping RFC3118 Delayed DHCP Authentication Using EAP-based Network Access Authentication

<draft-yegin-eap-boot-rfc3118-00.txt>

Status of this Memo

Abstract

DHCP authentication extension (RFC3118) cannot be widely deployed due to lack of an out-of-band key agreement protocol for DHCP clients and servers. This draft outlines how EAP-based network access authentication mechanisms can be used to establish a local trust relation and generate keys that can be used in conjunction with RFC3118.

Table of Contents

1.0 Introduction

EAP [EAP] provides a network access authentication framework by carrying authentication process between the hosts and the access networks. The combination of EAP with a 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 (e.g., EAP-TLS, EAP-SIM) are capable of generating cryptographic keys between the client and the local authentication agent (network access server - NAS) after the successful authentication. These keys are commonly used in conjunction with per-packet security mechanisms (e.g., link-layer ciphering).

DHCP [RFC2131] is a protocol which provides an end host with the configuration parameters. The base DHCP does not include any security mechanism, 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. It does not support roaming clients and assumes out-of band or manual key establishment. These

limitations have been inhibiting widespread deployment of this security mechanism [DHC-THREAT].

It is possible 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 EAP-based access authentication process to bootstrap RFC 3118 for securing DHCP.

The general framework of the mechanism described in this I-D can be outlined as follows:

(1) The client gains network access by utilizing an EAP authentication method that generates session keys. As part of the network access process, the client and the authentication agent (NAS) communicate their intention to create a DHCP security association and exchange the required parameters (e.g., nonce, key ID, etc.) The required information exchange is handled by the EAP lower-layer which also carries EAP.

(2) Although the newly generated DHCP SA is already available to the DHCP client, in case the NAS (acting as a DHCP relay) and the DHCP server are not co-located, the SA parameters need to be communicated to the DHCP server. This requires a protocol exchange, which can be piggybacked with the DHCP signaling.

(3) The DHCP signaling that immediately follows the network access authentication process utilizes RFC3118 to secure the protocol exchange. Both the client and the server rely on the DHCP SA to compute and verify the authentication codes.

This framework requires extensions to the EAP lower-layers (PPP [PPP], IEEE 802.1X [8021X], PANA [PANA]) to carry the supplemental parameters required for the generation of the DHCP SA. Another extension is required to carry the DHCP SA parameters from a DHCP relay to a DHCP server. RFC3118 can be used without any modifications or extensions.

2.0 Terminology

This document uses the following terms:

- DHCP Security Association

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

DHCP SA can be considered as a group security association. The DHCP SA parameters are provided to the DHCP server as soon as the client chooses the server to carry out DHCP. The same DHCP SA can be used by any one of the DHCP servers that are available to the client.

- DHCP Key

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

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

3.0 Overview and Building Blocks

The bootstrapping mechanism requires protocol interaction between the client host (which acts as a DHCP client), the NAS and the DHCP server. A security association will be established between the DHCP server and the DHCP client to protect the DHCP messages.

A DHCP SA is generated based on the EAP SA after a successful EAP authentication. Both the client and the NAS should agree on the generation of a DHCP SA after the EAP SA is created. This involves a handshake between the two and exchange of additional parameters (such as nonce, key ID, etc.). These additional information needs to be carried over the EAP lower-layer that also carries the EAP payloads.

The DHCP SA is ultimately needed by the DHCP client and the DHCP server. On the network side, the DHCP SA information needs to be transferred from the NAS (where it is generated) to the DHCP server (where it will be used). On the client host side, it is transferred from the network access authentication client to the DHCP client.

NAS is always located one IP hop away from the client. If the DHCP server is on the same link, it can be co-located with the NAS. When the NAS and the DHCP server are co-located, an internal mechanism, such as an API, is sufficient for transferring the SA information. 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, the NAS should be co-located with the DHCP relay.

[DS02] enables transmission of AAA-related RADIUS attributes from a DHCP relay to a DHCP server in the form of relay agent information options. DHCP SA is generated at the end of the AAA process, and therefore it can be provided to the DHCP server in a sub-option carried along with other AAA-related information. Confidentiality, replay, and integrity protection of this exchange MUST be provided. [RD03] proposes IPsec protection of the DHCP messages exchanged between the DHCP relay and the DHCP server. DHCP objects (protected with IPsec) can therefore be used to communicate the necessary parameters.

Two different deployment scenarios are illustrated in Figure 1.

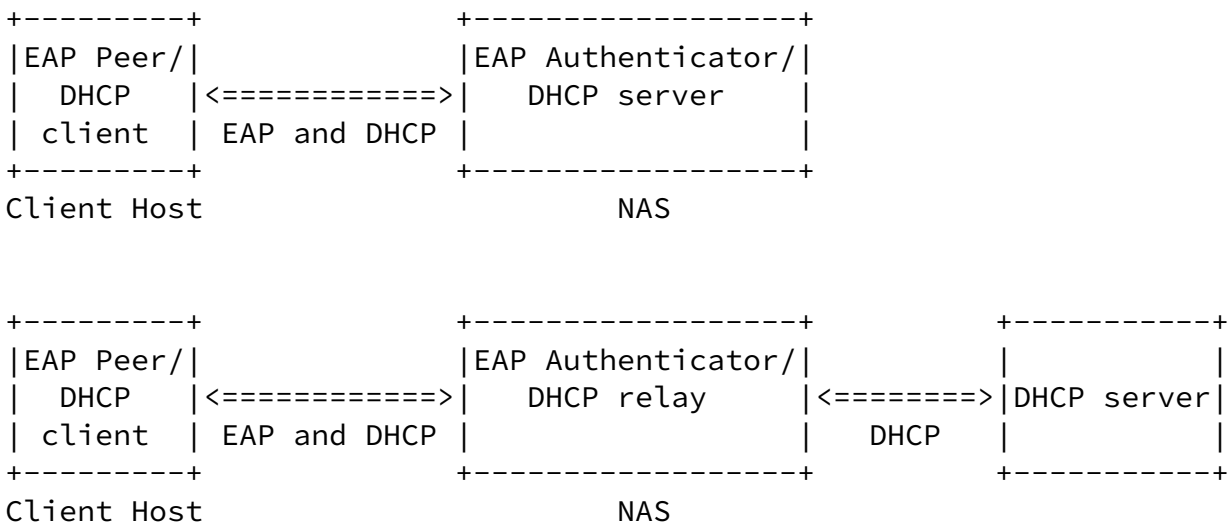


Figure 1: Protocols and end points.

When the DHCP SA information is received by the DHCP server and client, it can be used along with RFC3118 to protect DHCP messages against various security threats. This draft provides the guidelines regarding how the RFC3118 protocol fields should be filled in based

on the DHCP SA.

4.0 Building DHCP SA

DHCP SA is created at the end of the EAP-based access authentication process. This section describes extensions to the EAP lower-layers for exchanging the additional information, and the process of generating the DHCP SA.

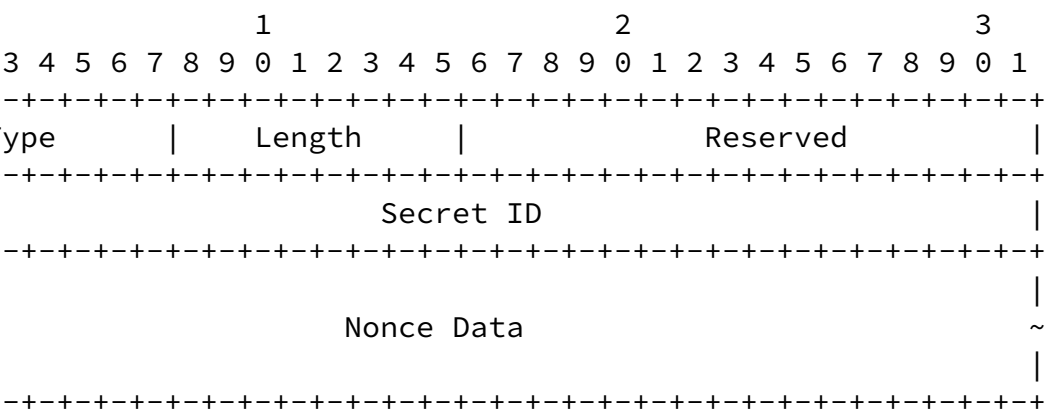
4.1. 802.1X

TBD

4.2. PPP

A new IPCP configuration option is defined in order to bootstrap DHCP SA between the PPP peers. Each end of the link must separately request this option for mutual establishment of DHCP SA. Only one side sending the option will not produce any state.

The detailed DHCP-SA Configuration Option is presented below.



Type

TBD

Length

>=24

Reserved

A 16-bit value reserved for future use. It MUST be initialized to zero by the sender, and ignored by the receiver.

Secret ID

32 bit value that identifies the DHCP Key produced as a result of the bootstrapping process. This value is determined by the NAS and sent to the client. The NAS determines this value by randomly picking a number from the available secret ID pool. If the client does not request DHCP-SA configuration option, this value is returned to the available identifiers pool. Otherwise, it is allocated to the client until the DHCP SA expires. The client MUST set this field to all 0s in its own request.

Nonce Data (variable length)

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

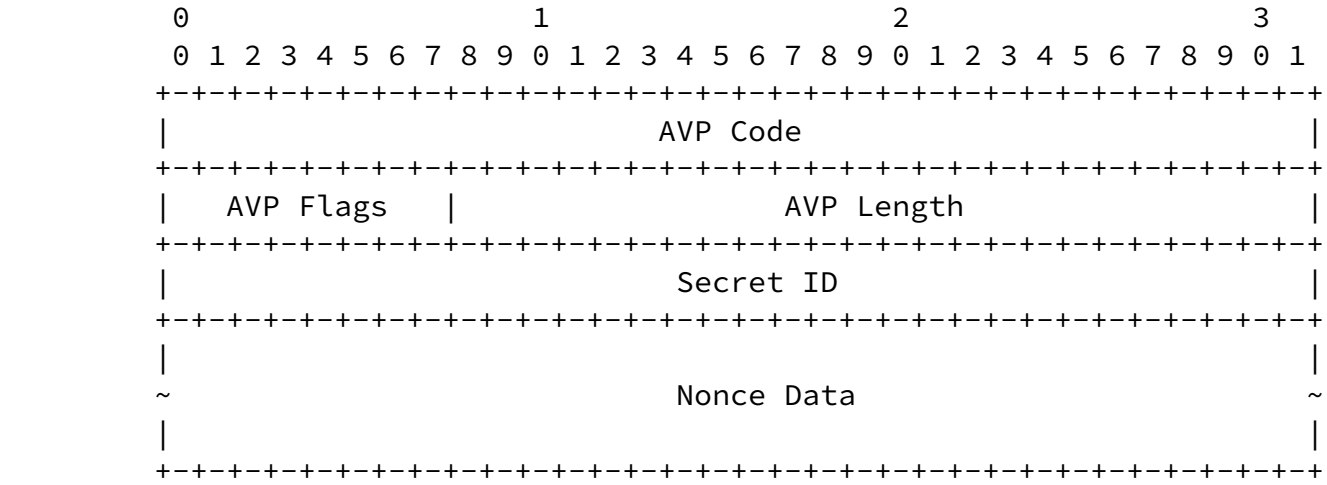
4.3. PANA

A new PANA AVP is defined in order to bootstrap DHCP SA. The DHCP-AVP is included in the PANA-Bind-Request message if PAA (NAS) 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-Bind-Answer message.

Absence of this AVP in the PANA-Bind-Request message sent by the PAA indicates unavailability of this additional service. In that case,

PaC MUST NOT include DHCP-AVP in its response, and PAA MUST ignore received DHCP-AVP. When this AVP is received by the PaC, it may or may not include the AVP in its response depending on its desire to create a DHCP SA. A 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.

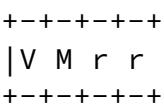


AVP Code

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 AVP data.

Secret ID

A 32-bit value that identifies the DHCP Key produced as a result of the bootstrapping process. This value is determined by the PAA and sent to the PaC. The PAA determines this value by randomly picking a number from the available secret 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 the DHCP SA expires. The 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 the Nonce_client value when the AVP is sent by PaC, and the Nonce_NAS value 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.

4.4. Computing DHCP SA

The key derivation procedure is reused from IKE [RFC2409]. The character '|' denotes concatenation.

```
DHCP Key = HMAC-MD5(AAA-key, const | Secret ID | Nonce_client |
                    Nonce_NAS)
```

The values have the following meaning:

- AAA-key:

  A key derived by the EAP peer and EAP (authentication) server and transported to the authenticator (NAS) at the end of the successful network access AAA.

- const:

  This is a string constant. The value of the const parameter is set to "EAP RFC3118 Bootstrapping".

- Secret ID:

  The unique identifier of the DHCP key as carried by the EAP lower-layer protocol extension.

- Nonce_client:

  This random number is provided by the client and carried by the EAP lower-layer protocol extension.

- Nonce_NAS:

  This random number is provided by the NAS and carried by the EAP lower-layer protocol.

- 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 a Transient Session Key (TSK).

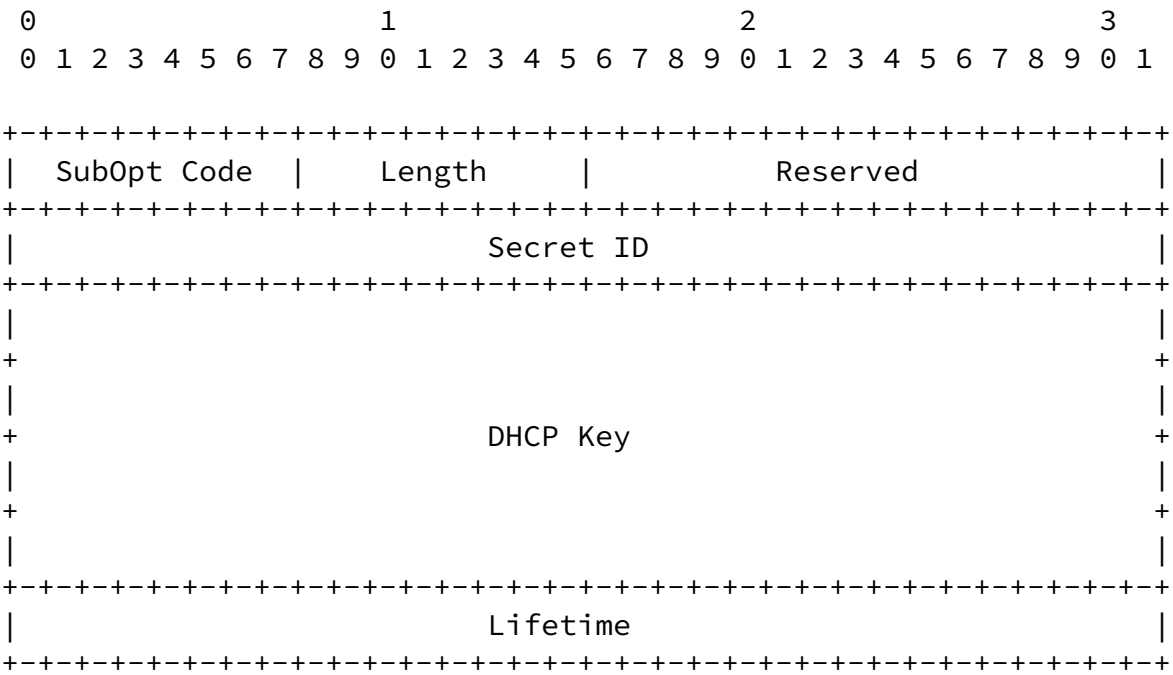
The lifetime of the DHCP security association has to be limited to prevent the DHCP server from storing state information indefinitely. The lifetime of the DHCP SA should be set to the lifetime of the network access service. The client host, NAS, and the DHCP server should be (directly or indirectly) aware of this lifetime at the end of a network access AAA.

The PaC can at any time trigger a new bootstrapping protocol run to establish a new security association with the DHCP server. The IP address lease time SHOULD be limited by the DHCP SA lifetime.

5.0 Delivering DHCP SA

When the NAS and the DHCP server are not co-located, the DHCP SA information is carried from the NAS (DHCP relay) to the DHCP server in a DHCP relay agent info option. This sub-option can be included along with the RADIUS attributes sub-option that is carried after the network access authentication.

The format of the DHCP SA sub-option is:



SubOpt Code

TBD

Length

This value is set to 26.

Reserved

A 16-bit value reserved for future use. It MUST be initialized to zero by the sender, and ignored by the receiver.

Secret ID

This is the 32-bit value assigned by the NAS and used to identify the DHCP key.

DHCP Key

128-bit DHCP key computed by the NAS is carried in this field.

Lifetime

The lifetime of the DHCP SA. This Unsigned32 value contains the number of seconds remaining before the DHCP SA is considered expired.

6.0 Using DHCP SA

Once the DHCP SA is in place, it is used along with RFC3118 to secure the DHCP protocol exchange.

[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

The value for the Code field of this authentication option is 90.

- Length

The Length field indicates the length of the authentication option payload.

- Protocol

[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 its usage is not recommended. 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 negotiated between the DHCP client and DHCP server.

- Algorithm

  [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 negotiated. [TBD: Consider future algorithm support]

- Replay Detection Method (RDM)

  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 negotiated.

- Replay Detection

  This field contains the value that is used for replay protection. This value MUST be monotonically increasing according to the provided replay detection method. An initial value must, however, be set. In case of bootstrapping with EAP an initial value of zero is used. The length of 64 bits (and a start-value of zero) ensures that a sequence number rollover is very unlikely to occur.

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

- Authentication Information

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 NAS to prevent collisions. [NOTE: If there are multiple NASes per DHCP server, this identifier space might need to be pre-partitioned among the NASes.]

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].

7.0 Security Considerations

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

If the NAS 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 NAS 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 [AS+03]). Figure 2 is originally taken from Section 4.1 of [AS+03] and extended accordingly. DHCP key is a TSK (Transient Session Key [AS+03]). The key is generated by both the DHCP client and the DHCP relay, and transported from the DHCP relay to the DHCP server. DHCP protocol traffic between the DHCP client and DHCP server is protected using this key.

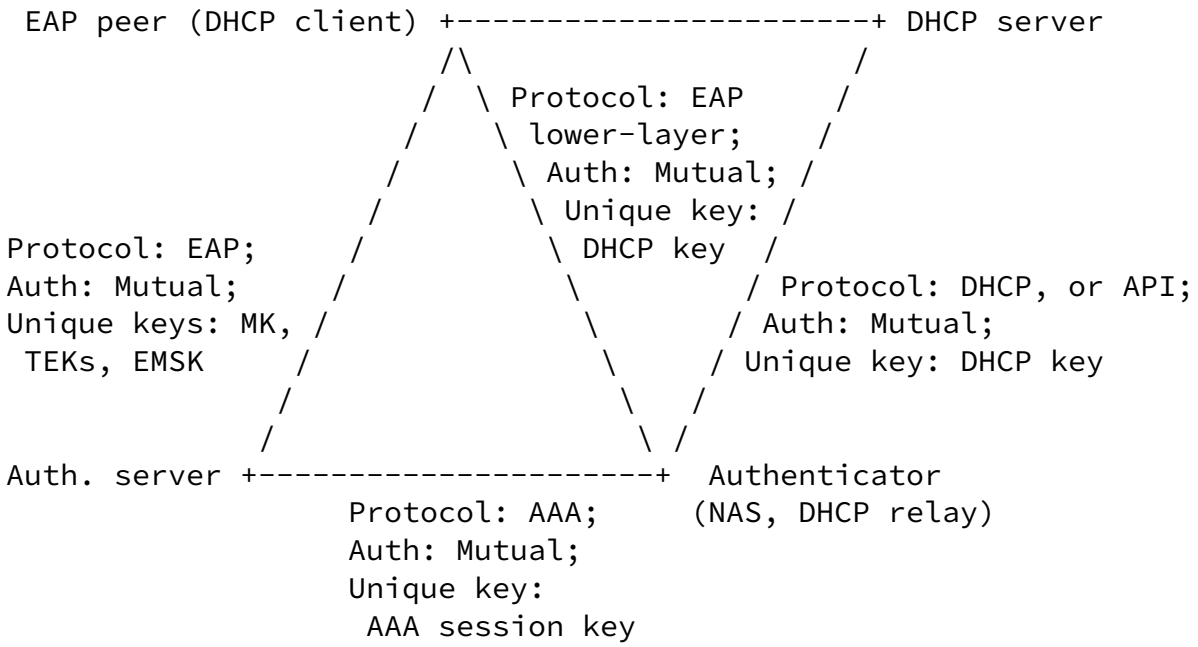


Figure 2: Keying Architecture

Figure 2 describes the participating entities and the protocols executed among them. It must be ensured that the derived session key between the DHCP client and the server is fresh and unique.

The key transport mechanism, which is used to carry the session key between the NAS 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 NAS) authorize the establishment of the DHCP security association.

At IETF 56 Russ Housley 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 be also applicable in this context.

- Algorithm independence:

This proposal bootstraps a DHCP security association for 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):

This scheme relies on EAP methods to provide strong and fresh session keys for each initial authentication and key exchange protocol run. Furthermore the key derivation function provided in Section 4.4 contains random numbers provided by the client and the NAS which additionally add randomness to the generated key.

- Replay protection:

Replay protection is provided at different places.

The EAP method executed between the EAP peer and the EAP server MUST provide a replay protection mechanism.

Additionally random numbers and the secret ID are included in the key derivation procedure which aim to provide a fresh and unique session key between the DHCP client and the DHCP server.

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

Finally, the security mechanisms provided in RFC 3118, for which this draft bootstraps the security association, also provides replay protection.

- Authenticate all parties:

Authentication between the EAP peer and the EAP server is based on the used EAP method. After a successful authentication and protocol run, the host and the NAS in the network provide AAA-key

confirmation either based on the 4-way handshake in IEEE 802.11i or based on the protected PANA exchange. DHCP key confirmation between the DHCP client and server is provided with the first protected DHCP message exchange.

- Perform authorization:

Authorization for network access is provided during the EAP exchange. The authorization procedure for DHCP bootstrapping is executed by the NAS before this service is offered to the client. The NAS might choose not to include DHCP-AVP or DHCP SA Configuration Option during network access authorization based on the authorization policies.

- Maintain confidentiality of session keys:

The DHCP session keys are only known to the intended parties (i.e., to the DHCP client, relay [TBD: is that OK?], and server). The EAP protocol itself does not transport keys. The exchanged random numbers which are incorporated into the key derivation function do not need to be kept confidential.

DHCP relay agent information MUST be protected using [RD03] with non-null IPsec encryption.

- Confirm selection of "best" cipher-suite:

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 occur.

- Uniquely name session keys:

The DHCP SA is uniquely identified using a Secret ID (described in [RFC3118] and reused in this document).

- Compromised NAS and DHCP server:

A compromised NAS may leak the DHCP session key and the EAP derived session key (e.g., AAA-key). It will furthermore allow corruption of the DHCP protocol executed between the hosts and the DHCP server since NAS either acts as a DHCP relay or a DHCP server.

A compromised NAS may also allow creation of further DHCP SAs or other known attacks on the DHCP protocol (e.g., address depletion).

A compromised NAS will not be able to modify, replay, inject DHCP messages which use security associations established without the EAP-based bootstrapping mechanism (e.g., manually configured DHCP SAs).

On the other hand, a compromised DHCP server may only leak the DHCP key information. AAA-key will not be compromised in this case.

- Bind key to appropriate context:

The key derivation function described in Section 4.4 includes parameters (such as the secret ID and a constant) which prevents reuse of the established session key for other purposes.

8.0 IANA Considerations

TBD

9.0 Open Issues

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

10.0 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.

[AS+03] Aboba, B., Simon, D., Arkko, J. and H. Levkowetz: "EAP Keying Framework", Internet-Draft, (work in progress), October 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.

[RD03] R. Droms: "Authentication of DHCP Relay Agent Options Using IPsec", Internet-Draft (work in progress), August 2003.

[SE03] J. Salowey and P. Eronen: "EAP Key Derivation for Multiple Applications", Internet-Draft (work in progress), June 2003.

[DHC-THREAT] Hibbs, R., Smith, C., Volz, B., Zohar, M., "Dynamic Host Configuration Protocol for IPv4 (DHCPv4) Threat Analysis", Internet-draft (expired), June 2003.

[8021X] IEEE Standard for Local and Metropolitan Area Networks, "Port-Based Network Access Control", IEEE Std 802.1X-2001.

[PPP] W. Simpson, "The Point-to-Point Protocol (PPP)", RFC 1661 (STD 51), July 1994.

11.0 Acknowledgments

We would like to thank Yoshihiro Ohba and Mohan Parthasarathy for their useful feedback to this work.

12.0 Author's Addresses

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

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