Internet Draft
draft-hoffman-sla-00.txt
December 17, 2002
Expires in six months

Dan Harkins
Derrell Piper
Paul Hoffman

Secure Legacy Authentication (SLA) for IKEv2

Status of this memo

Abstract

SLA is a new IKEv2 exchange that reuses most of the features of the IKEv2 Initial (Phase 1) exchange but allows for legacy authentication that is not susceptible to man-in-the-middle attacks. It has a flexible number of messages based on the type of authentication being used, and is extensible for new authentication mechanisms. SLA will work with remote access configuration in the same way as IKEv2's Initial exchange.

Introduction

This document is *not* meant to become an RFC. Instead, if the IPsec WG agrees, it should be part of the IKEv2 RFC. The next version of this draft can be specified as changes to the IKEv2 document.

It is possible that the format of the tag-length-value attributes will change to match those that are currently in XAUTH. If that happens, all of the usage examples from XAUTH can bin incorporated. This would increase code-reuse for folks who already have done XAUTH.

1. Exchange overview

Re-use of IKEv2 code is an important goal for SLA. SLA's messages are very similar to those in IKEv2's Initial exchange. The resulting key material is derived in the same fashion as IKEv2, and SLA uses the same denial-of-service protection as IKEv2's Initial exchange. Because SLA has a different exchange number than IKEv2's Initial exchange, there is

no ambiguity for either party about whether or not legacy authentication will be used.

The SLA protocol is based on earlier proposals for secure legacy authentication such as Hybrid and CRACK. In SLA, the authentication of each side happens very differently. The responder (who is usually a security gateway) authenticates itself to the initiator first using standard IKEv2 authentication methods. After that, the initiator (who is usually a remote access client) authenticates itself to the responder using a legacy authentication mechanism such as username-password, SecurID token, and so on.

In this description, "message N" is the last message in the exchange. Because the number of messages is variable, there is no specified number for the message.

A quick summary of the exchange is:

- Message 1 is the same as the IKEv2 message 1.

- Message 2 is the same as the IKEv2 message 2 except that it includes the responder's authentication payload. This allows the remote access client to authenticate the responder before engaging in sensitive legacy authentication.

- Message 3 is the same as the IKEv2 message 3 except that the identification payload and the authentication payload are replaced by the first challenge/response payload, which identifies the initiator and the legacy authentication mechanism being used.

- Messages 4 through N-1 consist of the legacy authentication steps. Each message consists of a single challenge/response payload.

- The last message, N, always comes from the responder, and it includes a challenge/response payload that states that the authentication is complete. It also contains the SAr2, TSi, and TSr payloads from IKEv2 message 4.

2. Exchange details

All information not defined here is assumed to be the same as for the IKEv2 Initial exchange. Messages 1 and 2 are:

```
       Initiator                          Responder
      -----------                        -----------
       HDR, SAi1, KEi, Ni        -->

                                 <--    HDR, SAr1, KEr, Nr, AUTH
```

The responder's AUTH payload is computed over all of message 1 concatenated with all of message 2. Because the contents of the AUTH payload cannot be known when creating the concatenation, a dummy AUTH payload is constructed which consists of the payload header that would have been used (including a correct length field), but with each octet of the contents set to 0x00.

The client MUST both verify the signature as being valid for the gateway's public key as well as verify that the signed exchange matches the actual data sent by the client in the first message.

Message 3 is:

```
       HDR*, CHRE,
             SAi2, TSi, TSr  -->
```

Message 4 through message N-1 have the format:

```
                     HDR*, CHRE
```

This is the challenge/response message described in section 3. The contents of the CHRE payloads is specific to the legacy authentication method chosen.

Message N is the last message, and MUST come from the responder. If the responder successfully authenticates the initiator, message N is:

```
                                  <--    HDR*, CHRE,
                                               SAr2, TSi, TSr
```

If the responder does not successfully authenticate the initiator, message N is:

```
                                  <--    HDR*, CHRE
```

In either case, the CHRE in message N MUST contain the SLA_T_FIN attribute to tell the initiator whether or not the authentication succeeded.

2.1 Error codes

Errors are indicated with IKEv2 Notify exchanges. They are:

REFUSE-TO-DO-SLA
: Responder unwilling to do SLA (after message 1)

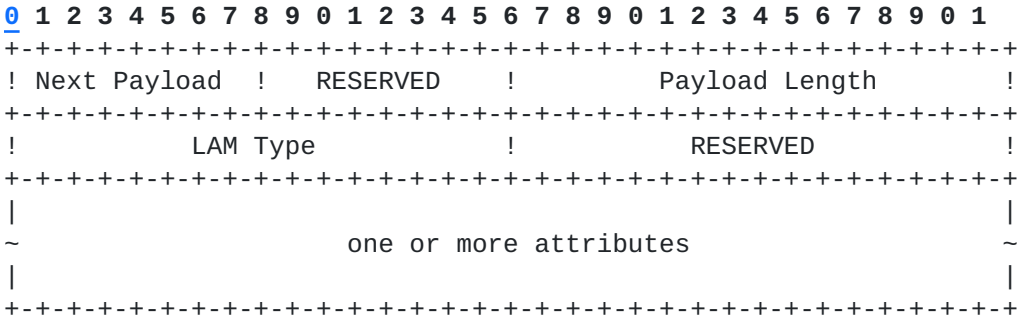
REFUSE-TO-GO-FORWARD
: Initiator (after message 2) cannot or does not want to continue the exchange. This may be due to the initiator not being able to validate the signature on the AUTH in message 2, the initiator not liking SAr1 or KEr, and so on.

3. The Challenge/Response Payload (CHRE)

The Challenge/Response payload is used to convey a challenge from the responder to the initiator and is used by the initiator to respond to a challenge from the responder. The Challenge/Response payload contains attributes denoting specific information conveyed from the initiator to the responder and back. The actual legacy authentication method will

determine the contents of this payload at the various points in the exchange.

This payload consists of the IKEv2 generic header and a payload-specific body whose length is not fixed. The body consists of one or more attributes, described below. The "Payload Length" in the generic header includes the length of the header itself. All fields labeled "RESERVED" MUST be filled with zero (0) prior to sending and each party to the exchange MUST verify that value on all payloads it is sent.



The payload type for this payload is [[TBA]].

The LAM Type field denotes the legacy authentication method associated with the exchange. The LAM Type must be set in all CHRE payloads in an exchange. The LAM Type is selected by the initiator and MUST be set in every CHRE payload to the same value throughout the exchange.

3.1 LAM Types

Different legacy authentication methods are denoted by unique LAM type identifiers in the Challenge/Response payloads.

If the responder is not configured to support the requested LAM type while processing the initiator's first CHRE payload, the responder MUST terminate the exchange and MUST respond with an IKEv2 Notify of type NO-PROPOSAL-CHOSEN.

A conformant responder MUST support at least one of the specified LAM Types. A responder MAY support more than one LAM Type and it's assumed that the choice of which LAM Types are supported is implementation-specific and determined from local policy configuration, perhaps on a per-user basis based on the content of the first CHRE payload and its associated attributes.

The legacy authentication methods are:

LAM Type Identifier	Value
RESERVED	0
SLA_PASSWORD	1
SLA_OTP	2
SLA_CHALLENGE_RESPONSE	3
SLA_SECURID	4
<unassigned>	5-32767
<private use>	32768-65535

This table will be maintained by IANA. Additional LAM types MAY be defined. Such definitions MUST be in standards-track RFCs and registered with IANA.

SLA_PASSWORD
: A simple username/password mechanism. It is used for any simple host-based password or one-way hash mechanism. It also useful for proxy-based password authentication schemes.

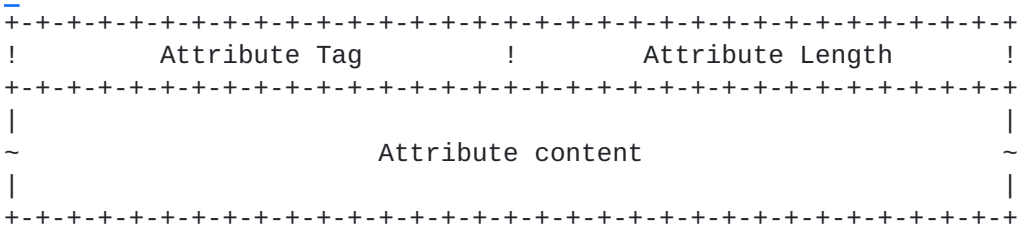
SLA_OTP
: A one-time password mechanism. It is useful for the S/KEY [Hal95] and OTP [HM96] schemes.

SLA_CHALLENGE_RESPONSE
: A token-based challenge/response mechanism. It's useful for a wide variety of cryptographic tokens, typically based on DES.

SLA_SECURID
: A SecurID-like mechanism. It's useful for the RSA SecurID system. The SLA_SECURID closely resembles SLA_CHALLENGE_RESPONSE.

3.2 LAM Attributes

The Challenge/Response payload contains attributes used to convey information between the initiator and the responder authenticating the initiator. Attributes have the structure:



The attribute length is specified in octets.

Attribute name	Attribute tag
RESERVED	0
SLA_T_USERNAME	1
SLA_T_SECRET	2
SLA_T_DOMAIN	3
SLA_T_PIN	4
SLA_T_CHALLENGE	5
SLA_T_MESSAGE	6
SLA_T_FIN	7

This table will be maintained by IANA. Additional LAM attributes MAY be defined. Such definitions MUST be in standards-track RFCs and registered with IANA.

SLA_T_USERNAME
: The initiator user identity that's requesting authentication. The

syntax and format of SLA_T_USERNAME is specific to each LAM type.

SLA_T_SECRET
: Secret information the initiator sends in an attempt to authenticate, for instance a password or passcode. The syntax and format of SLA_T_SECRET is specific to each LAM type.

SLA_T_DOMAIN
: The domain or realm the initiator is requesting authentication credentials within. The syntax and format of SLA_T_DOMAIN is specific to each LAM type.

SLA_T_PIN
: The initiator's PIN. The syntax and format of SLA_PIN is specific to each LAM type.

SLA_T_CHALLENGE
: Any challenge the responder may choose to issue to the initiator. The syntax and format of SLA_T_CHALLENGE is specific to each LAM type.

SLA_T_MESSAGE
: An ASCII string to be displayed to the user upon receipt of the corresponding CHRE payload. SLA_T_MESSAGE is valid for all LAM types. Upon receipt, the contents of SLA_T_MESSAGES SHOULD be displayed to the initiator user, typically along with the CHRE challenge.

SLA_T_FIN
: The responder's response to the authentication exchange at all critical decision points specific to each LAM type. The following table defines the values for SLA_T_FIN:

Finish Types	Value
RESERVED	0
SLA_FIN_SUCCESS	1
SLA_FIN_MORE	2

SLA_FIN_SUCCESS indicates the responder has successfully authenticated the initiator. This value successfully terminates the SLA exchange. This value is legal for all LAM types.

SLA_FIN_MORE indicates the responder requires an additional round-trip to authentication the initiator. This is only legal for LAM types which define its use. It MUST NOT be used unless defined in the corresponding LAM profile.

4. Legacy Authentication Method (LAM) Profiles

Each defined LAM type uses the CHRE payload and LAM attributes in a different manner. This section profiles the acceptable use of each for the defined LAM types and details the list of acceptable attributes for each profile.

In the profiles, the CHRE payloads are numbered. Thus, CHRE1 is the CHRE payload in message 3 of the SLA exchange, CHRE2 is the CHRE payload in message 4, and so on.

4.1 LAM Profiles: Password

The Password profile supports legacy operating system (OS) authentication along with proxy-based password authentication protocols.

The password exchange consists of exactly two CHRE payloads:

- The CHRE1 payload contains the initiator's username as a SLA_T_USERNAME attribute and a password as a SLA_T_SECRET attribute. The format of the initiator password is dictated by the corresponding host OS or proxy authentication server and may be either plaintext or binary.

- The CHRE2 payload contains a SLA_T_FIN attribute with the value of SLA_FIN_SUCCESS.

The following attributes are defined for Password:

SLA_T_USERNAME (initiator -> responder, required)

SLA_T_USERNAME is sent in the initiator's first CHRE payload and MUST contain the initiator's username which is used as an index key by the host OS or proxy password authentication server.

SLA_T_SECRET (initiator -> responder, required)

SLA_T_SECRET is sent in the initiator's first CHRE payload and MUST contain the initiator's password.

SLA_T_DOMAIN (initiator -> responder, optional)

SLA_T_DOMAIN is sent in the initiator's second message and MAY be used to specify the authentication domain that the initiator is requesting authentication within.

SLA_T_FIN (responder -> initiator, required)

SLA_T_FIN is used to successfully terminate the exchange.

4.2 LAM Profiles: One-Time Password

The OTP profile supports both the S/KEY and OTP one-time password schemes.

The OTP exchange consists of exactly four CHRE payloads.

- The CHRE1 payload contains only any associated attributes such as a username.

- The CHRE2 payload contains the OTP server's challenge text which MUST be displayed to the initiator user.

- The CHRE3 payload contains the initiator's one-time password response.

- The CHRE4 payload contains a SLA_T_FIN attribute with the value of SLA_FIN_SUCCESS.

The following attributes are defined for OTP:

SLA_T_USERNAME (initiator -> responder, required)

SLA_T_USERNAME is sent in the initiator's first CHRE payload and MUST contain the initiator's username which is used as an index key by the OTP server.

SLA_T_CHALLENGE (responder -> initiator, required)

SLA_T_CHALLENGE is sent in the responder's first CHRE payload and MUST contain the OTP challenge to be issued to the initiator.

SLA_T_SECRET (initiator -> responder, required)

SLA_T_SECRET is sent in the initiator's second CHRE payload and contains the initiator's one-time password.

SLA_T_MESSAGE (responder -> initiator, optional)

SLA_T_MESSAGE is optionally sent in any responder message and MAY by used by the responder to provide optional text to be displayed to the user along with any associated challenge text.

SLA_T_FIN (responder -> initiator, required)

SLA_T_FIN is used to successfully terminate the exchange.

4.3 LAM Profiles: Challenge/Response

The Challenge/Response profile supports various token cards that follow a standard challenge/response exchange. The initiator's token card information (the response) depends on the responder's request (the challenge).

The Challenge/Response profile consists of at least two CHRE payloads. If more challenges are required to authenticate this initiator, the CHRE2 payload contain a challenge to the initiator. The initiator would respond with CHRE3, and the responder with CHRE4. This can be repeated until the responder authenticates the initiator (or authentication fails, see below).

When the initiator is using a token that can compute the next expected response without requiring a challenge, the CHRE1 payload contains the initiator's username and expected response. When the initiator does not have an expected response, or has chosen not to use the current one for whatever reason, the CHRE1 payload contains only the initiator's username.

The CHRE2 payload contains the responder's challenge text which MUST be displayed to the initiator user unless the initiator has presented an expected response (as above) in which case this is identical to CHRE4

below.

The CHRE3 payload, when used, contains the initiator's response to the responder challenge.

The CHRE4 payload contains a SLA_T_FIN attribute with the value of SLA_FIN_SUCCESS, or another challenge.

The following attributes are defined for Challenge/Response:

SLA_T_USERNAME (initiator -> responder, required)

SLA_T_USERNAME is sent in the initiator's second message and MUST contain the initiator's username which is used as an index key for authentication by the responder.

SLA_T_SECRET (initiator -> responder, required)

SLA_T_SECRET contains the initiator's response and is sent in the initiator's second message if an anticipated challenge is used, and in the initiator's third message if the initiator is responding to a responder challenge.

SLA_T_PIN (initiator -> responder, optional)

SLA_PIN is optionally sent in any initiator message and MAY by used if the authentication protocol also requires the initiator to provide a PIN.

SLA_T_MESSAGE (responder -> initiator, optional)

SLA_MESSAGE is optionally sent in any responder message and MAY by used by the responder to provide optional text to be displayed to the user along with any associated challenge text.

SLA_T_FIN (responder -> initiator, required)

SLA_T_FIN is used to successfully terminate the exchange.

4.4 LAM Profiles: SecurID

The SecurID profile supports the RSA SecurID protocol. With SecurID the initiator will be passing the output of the SecurID card as the body of the CHRE1 payload and its identity as an associated SLA_T_USERNAME attribute. Assuming the initiator and responder are in sync (that is, they are not in "Next Code" mode), the authentication completes with the CHRE2 payload.

For simple SecurID, the CHRE payloads are used as follows:

- The CHRE1 payload contains the initiator's username and the current Passcode displayed by the initiator's SecurID token.

- The CHRE2 payload contains a SLA_T_FIN attribute with the value of SLA_FIN_SUCCESS.

When the initiator and responder clocks are slightly out of sync, the responder will respond with an additional challenge payload to which the initiator MUST respond with another response payload. This is known as "Next Code" mode.

For SecurID with "Next Code", the CHRE payloads are used as follows:

- The CHRE1 payload contains the initiator's username and the current Passcode displayed by the initiator's SecurID token.

- The CHRE2 payload contains a SLA_T_FIN attribute with the value of SLA_FIN_MORE.

- The CHRE3 payload contains the initiator's next Passcode displayed by the initiator's SecurID token.

- The CHRE4 payload contains a SLA_T_FIN attribute with the value of SLA_FIN_SUCCESS.

The following attributes are defined for SecurID:

SLA_T_USERNAME (initiator -> responder, required)

SLA_T_USERNAME is sent in the initiator's second message and MUST contain the initiator's username which is used as an index key by the ACE server.

SLA_T_PIN (initiator -> responder, optional)

SLA_T_PIN is sent in the initiator's second message and MAY be used when the SecurID card is not a PINPAD card.

SLA_T_MESSAGE (responder -> initiator, optional)

SLA_T_MESSAGE is optionally sent in any responder message and MAY by used by the responder to provide optional text to be displayed to the user along with any associated challenge text.

SLA_T_FIN (responder -> initiator, required)

SLA_T_FIN is used to successfully terminate the exchange and to request the initiator continue under "Next Code" mode.

4.5 LAM Profile Matrix

Each of the LAM's supported by IKE Challenge/Response fall into one of the defined LAM profiles. This section details the classification for those methods.

Password
- DIAMETER
- LDAP
- NDS (Netware Directory Services)
- NT Domain
- RADIUS
- TACACS

```
        TACACS+
        UNIX Login

OTP
        OTP
        S/KEY

Challenge/Response
        AXENT Defender
        CheckPoint ActivCard
        CRYPTOCard CRYPTOCard
        Digital Pathways SNK
        LeeMah InfoCard
        Secure Computing SafeWord (Enigma Logic DES Gold)

SecurID
        RSA SecurID
```

5. Additional security considerations

Each legacy authentication mechanism has its own security considerations. Using any particular legacy authentication mechanism exposes the IKEv2 system to the same attacks as the legacy authentication mechanism.

The encrypted channel that results after the the first two messages is secured because the responder signs its Diffie-Hellman public value. The channel is secured from the initiator's perspective because the initiator knows that the responder was the actual source of the Diffie-Hellman public value and is an active party to the exchange. The channel is secured from the responder's perspective because the initiator has proved proof-of-possession of a long-term shared secret and would not have sent its sensitive information if a man-in-the-middle was detected by the initiator.

6. Additional IANA considerations

Create a LAM Type registry from section 3.1.

Create a LAM Attribute registry from section 3.1.

7. Authors' Addresses

Dan Harkins
dharkins@trpz.com

Derrell Piper
ddp@electric-loft.org

Paul Hoffman
paul.hoffman@vpnc.org