IP Secure Remote Access Working Group
INTERNET-DRAFT
draft-ietf-ipsec-isakmp-hybrid-auth-04.txt
Expires January, 2001

M. Litvin, R. Shamir, T. Zegman
Check Point Software

July, 2000

A Hybrid Authentication Mode for IKE
<draft-ietf-ipsec-isakmp-hybrid-auth-04.txt>

Status of this Memo

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

This document is a submission to the IETF Internet Protocol Secure Remote Access (IPSRA) Working Group. Comments are solicited and should be addressed to the working group mailing list (ietf-ipsra@vpnc.org) or to the editor.

This document is an Internet-Draft. Internet Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working Groups. Note that other groups may also distribute working documents as Internet Drafts.

Internet-Drafts draft documents are valid for a maximum of six months and may be updated, replaced, or made obsolete by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

To learn the current status of any Internet-Draft, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ftp.ietf.org (US East Coast), or ftp.isi.edu (US West Coast).

1. Abstract

This document describes a set of new authentication methods to be used within Phase 1 of the Internet Key Exchange (IKE). The proposed methods assume an asymmetry between the authenticating entities. One entity, typically an Edge Device (e.g. firewall), authenticates using standard public key techniques (in signature mode), while the other

entity, typically a remote User, authenticates using challenge response techniques. These authentication methods are used to establish, at the end of Phase 1, an IKE SA which is unidirectionally authenticated. To make this IKE bi-directionally authenticated, this Phase 1 is immediately followed by an X-Auth Exchange [XAUTH]. The X-Auth Exchange is used to authenticate the remote User. The use of these authentication methods is referred to as Hybrid Authentication mode.

This proposal is designed to provide a solution for environments where a legacy authentication system exists, yet a full public key infrastructure is not deployed.

1.1 Reader Prerequisites

It is assumed that the reader is familiar with the terms and concepts described in "Extended Authentication Within ISAKMP/Oakley" [XAUTH] and "The ISAKMP Configuration Method" [IKECFG].

1.2 Changes from previous version

1.2.1 Version 4.0 Authentication method numbers were assigned by IANA without altering their values.

1.2.2 Version 3.0

Draft was renamed and reposted under the IPSRA working group.

1.2.3 Version 2.0

The authentication methods numbers are now taken from the private use range.

Mutual authentication within Phase 1 is now discussed in [XAUTH].

Added clarification on the use of DSS signatures.

Added clarification on the content of ID payloads sent by the Client during Phase 1.

Changed the semantics of the authentication methods so that they will correspond to similar authentication methods defined in [XAUTH].

1.2.4 Version 1.0

The draft was extensively modified since the last version. The most important change is the breaking down of authentication into two

stages. The first stage is used to authenticate the Edge Device and is based on Phase 1 Exchange, while the latter authenticates the Client and is based on a Transaction Exchange [IKECFG] with the mechanism described in [XAUTH].

2. Discussion

2.1 Background

Several authentication methods are currently defined within IKE [IKE]. These methods use either a secret which is shared by the authenticating entities ("pre-shared key" method), or public key cryptography ("digital signature" mode, "public key encryption" mode, "revised public key encryption mode"). Legacy authentication systems, such as Security Dynamics' SecurID and Axent's OmniGuard/Defender, are not addressed in the current standard.

Legacy authentication systems are already deployed in many organizations. These organizations may not wish to deploy a public-key infrastructure in the near future. Furthermore, even if an organization decides to deploy a public key infrastructure, the deployment can take a considerable amount of time. Within the transition period, organizations may wish to continue using their legacy authentication systems.

2.2 Design considerations

The currently defined IKE authentication methods share two properties: the authentication is mutual (both participants authenticate each other); and symmetric (both participants use the same method for authentication). Mutual authentication is important not only for mere identification but also to prevent man in the middle attacks.

In client-server like implementations of IKE, where one of the participants in the IKE is a User, while the other is an Edge Device (e.g. firewall), it is not always possible to preserve symmetric authentication. For example, a User can use an OmniGuard/Defender token to answer an authentication challenge, but cannot issue an OmniGuard/Defender authentication challenge to the firewall, since she cannot check the firewall's response.

When designing an IKE authentication method that addresses legacy authentication systems, it is necessary to preserve the mutual authentication property of IKE, while its symmetric nature may be violated.

The authentication methods currently defined in IKE all use a six

packet exchange for Main Mode, and a three packet exchange for Aggressive Mode. When defining a new authentication method, which is based on challenge-response authentication, it is not possible to place a limitation on the number of packets that need to be exchanged to authenticate a User. Usually, a simple authentication protocol consists of three messages: a challenge by the Edge Device; a response by the User; and a status message (authentication success/failure) sent by the Edge Device. However, in many cases the protocol consists of more than a single challenge-response (e.g. new PIN mode of SecurID).

Due to these limitation, we divide the authentication process into two stages. In the first stage, Phase 1 Exchange is being utilized to authenticate the Edge Device and to establish an IKE SA. In the second stage, a Transaction Exchange [IKECFG] with the mechanism described in [XAUTH] is used to authenticate the Client. Even though the two stages could have been integrated into a single exchange, we feel that this separation, being based on existing exchanges without modifying them, is easier to implement.

This proposal is suitable for environments where a legacy authentication system is deployed, yet public key cryptography can be used by the Edge Devices. In that case, the situation resembles the way authentication is implemented in the World Wide Web using SSL. The servers use public-key techniques to authenticate themselves to the Users, and establish an encrypted connection. The User can then authenticate herself (or send other identification information, such as a credit card number). The assumption in this mode is that deploying public key for a small number of entities (web servers or Edge Devices) is possible without a full-public key infrastructure deployment.

In some scenarios, security policy on the Edge Device might call for authentication of both the User and the User's Device. In such a case the Phase 1 authentication methods described in [XAUTH] should be used.

2.3 The hybrid authentication mode in a nut-shell

The participants in the hybrid authentication mode are typically a User and an Edge Device. The participants start to negotiate, using either Main Mode or Aggressive Mode, an SA in which the authentication method is of a new type, indicating it is a hybrid authentication method. At the end of Phase 1 the established IKE SA is used by the Edge Device to start a Transaction Exchange [CFG] in order to authenticate the User. Upon the successful completion of the exchange the participants can proceed to use the IKE SA for other purposes (e.g. Quick Mode).

3. Terms and Definitions

3.1 Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [Bra97].

3.2 Definitions

The following terms are used in this document:

Edge Device - Gateway, router or firewall protecting a corporate network.

User - A person trying to gain access to a corporate network protected by an Edge Device.

User's Device - user's device.

Client - Denotes both the User and the User's Device. Used whenever a distinction between the two terms is not necessary.

3.2.1 Authentication Methods Types

The following values relate to hybrid mode authentication. Their use is detailed in following sections. These values were assigned by IANA.

Type	Value
HybridInitRSA	64221
HybridRespRSA	64222
HybridInitDSS	64223
HybridRespDSS	64224

3.3 Notation

This document follows the notations defined in [IKE].

4. Description of the Hybrid Authentication Mode

The hybrid authentication mode is divided into two stages. The first stage is a Phase 1 Exchange used to authenticate the Edge Device. The exchange follows the same structure and rules as described in [IKE] with some exceptions as described in the following sub-sections. The Phase 1 Exchange can use either Aggressive Mode or Main Mode. The

initiator of the Phase 1 Exchange can be either the Client or the Edge Device. The initiator of the following Transaction Exchange MUST be the Edge Device.

The Phase 1 Exchange MUST be immediately followed by a Transaction Exchange whose initiator is the Edge Device. The Transaction Exchange MUST be protected by the IKE SA negotiated in the preceding Phase 1 Exchange. This IKE SA MUST NOT be used for any other exchange before the Transaction Exchange terminates successfully and the User is authenticated. If the User fails to authenticate the IKE SA MUST be discarded.

There are two characteristics that uniquely identify a hybrid authentication method:

The first is the direction of the authentication. The latter determines the authentication method used to authenticate the Edge Device (i.e. RSA or DSA).

For example, HybridInitRSA denotes Hybrid authentication that utilizes RSA signatures in Phase 1 to authenticate the Edge Device. The initiator of the Phase1 exchange is to be authenticated using XAUTH.

4.1 Bidirectional Authentication

For a discussion on how to use Bidirectional authentication together with legacy authentication systems see [XAUTH].

4.2 Unidirectional Authentication

If the Client's side is not to be authenticated during the Phase 1 Exchange, the Phase 1 Exchange is slightly modified in the following manner:

The signature payload sent by the Client SIG_I (or SIG_R) is replaced with HASH_I (HASH_R), where HASH_I (HASH_R) contains the hash of the data that would have otherwise be signed in SIG_I (SIG_R). Note however that even if the Edge Device uses a signature scheme tied to a particular hash algorithm (i.e. DSS with SHA), the negotiated prf or the HMAC version of the negotiated hash function MUST be used by the Client when computing HASH_I (HASH_R).

If a certificate request payload is sent from the Edge Device the Client MUST respond with an empty certificate payload, i.e. with a

certificate payload whose Certificate Data field has zero length.

The ID payload sent by the Client SHOULD be left empty (i.e. with an empty Identification Data field and with an ID type of zero) thus providing identity protection for the Client even if Aggressive Mode is used.

Examples:

Main Mode with hybrid authentication, Client initiator:

```
     Initiator                          Responder
    ----------                         -----------
     HDR, SA                    -->

                                <--     HDR, SA

     HDR, KE, Ni                -->

                                <--     HDR, KE, Nr

     HDR*, IDii, HASH_I         -->

                                <--     HDR*, IDir, [ CERT, ]
                                              SIG_R

                            XAUTH-Exchange
```

Aggressive Mode hybrid authentication, Edge Device initiator:

```
     Initiator                          Responder
    -----------                        -----------
     HDR, SA, KE, Ni, IDii      -->

                                <--     HDR, SA, KE, Nr, IDir,
                                             HASH_R

       HDR, [ CERT, ] SIG_I       -->

                            XAUTH-Exchange
```

5. Implementation hints

Since the Edge Device always initiates the Transaction Exchange, when a Client initiates the Phase 1 Exchange, the authentication methods included in the Client's proposal should be either HybridInitRSA or HybridInitDSS, whereas if the Edge Device is the initiator of the Phase 1 Exchange the authentication methods included in the Edge Device's proposal should be either HybridRespRSA or HybridRespDSS.

6. Security Considerations

This document describes a protocol to be used to establish an IKE SA. The level of security the protocol provides, relies among other things, on the strength of the authentication mechanism used to authenticate the Client.

While pre-shared key authentication for mobile users can be done only in Aggressive Mode, thus revealing the identity of the User, these proposed methods provide, when used in conjunction with Aggressive Mode, User's identity protection and when used in conjunction with Main Mode, provide identity protection for both parties.

While the authors greatly discourage the use of fixed passwords, these methods have another advantage over the pre-shared key method: The password is not prone to offline dictionary attacks, since the password is encrypted using a derivative of the Diffie-Hellman shared key. Only the participants in the IKE protocol know the shared key.

NB: When using standard IKE authentication methods both parties can (and must) detect man-in-the-middle attacks. When one uses hybrid authentication to establish unidirectional authenticated IKE SA's, only the Client can (and must) detect these kinds of attacks.

This proposal does not provide protection against denial of service attacks in which an attacker, impersonating a User, repeatedly tries to authenticate, eventually causing the User's account to be revoked. Nonetheless, this kind of weakness is inherent to challenge-response techniques and should not be considered a weakness of this protocol but of the authentication methods it utilizes.

7. Acknowledgements

The authors would like to thank Roy Pereira, Tim Jenkins, Paul Kierstead and Stephen Kent for their comments and contributions to this document.

8. References

[Bra97] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", RFC2119

[IKE] D. Harkins, D. Carrel, "The Internet Key Exchange (IKE)", RFC2409

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

[IKECFG] R. Pereira, S. Anand, B. Patel, "The ISAKMP Configuration Method", draft-ietf-ipsec-isakmp-mode-cfg-05.txt

[XAUTH] R. Pereira, S. Beaulieu, "Extended Authentication Within ISAKMP/Oakley", draft-ietf-ipsec-isakmp-xauth-06.txt

Author Addresses:

Moshe Litvin <moshe@checkpoint.com>
Check Point
3A Jabotinsky St.
Ramat-Gan 52520
ISRAEL

Roy Shamir <roy@checkpoint.com>
Check Point
3A Jabotinsky St.
Ramat-Gan 52520
ISRAEL

Tamir Zegman <zegman@checkpoint.com>
Check Point
3A Jabotinsky St.
Ramat-Gan 52520
ISRAEL

Full Copyright Statement: