Internet Engineering Task Force R. Pereira
IP Security Working Group TimeStep Corporation
Internet Draft
Expires in six months
November 21, 1997

Extended Authentication Within ISAKMP/Oakley
<draft-ietf-ipsec-isakmp-xauth-00.doc>

Status of this Memo

This document is a submission to the IETF Internet Protocol Security (IPSECond) Working Group. Comments are solicited and should be addressed to the working group mailing list (ipsec@tis.com) 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 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."

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), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

Distribution of this memo is unlimited.

Abstract

This document describes a method for utilizing authentication mechanisms that are either unidirectional in nature or that work with the base ISAKMP authentication mechanisms.

Table of Contents

1. Introduction

The following technique allows IPSec's ISAKMP/Oakley protocol to support extended authentication mechanisms like SDI's SecureID and RADIUS [RADIUS].

1.1 Specification of Requirements

The keywords "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", and "MAY" that appear in this document are to be interpreted as described in [Bradner97].

2. Extended Authentication

Secure-ID smart cards and RADIUS are forms of authentication that allow a gateway, firewall, or network access server to offload the user administration to a central server. IPSec's ISAKMP/Oakley protocol supports certificates (RSA & DSS), shared-secret, and Kerberos as authentication methods, but since Secure-ID and RADIUS are only unidirectional authentication methods (client to a gateway/firewall), they must be used inconjunction with the other standard authentication methods.

The technique described within this document utilizes ISAKMP to transfer the user's authentication information (name, password) to the gateway/firewall in an encrypted message during the authentication exchange in phase 1. The gateway/firewall would then use either the RADIUS or SecureID transport protocol to authenticate the user. This allows a RADIUS or SecureID ACE server to be within the network (Red Side) that the gateway/firewall is protecting.

While this document specifies both SecureID and RADIUS, it does not preclude any other extended authentication mechanism from being used (eg. TACACS [Finseth93]).

3. Interaction with ISAKMP

By utilizing a NOTIFY payload, the gateway (responder) can request extended authentication from the client (initiator). The client then must respond with its extended authentication credentials in the next exchange. The gateway will then respond with a failure or passed message.

```
Initiator                 Responder
--------------            -----------------
                    <--   NOTIFY(XAUTH_SECUREID | XAUTH_RADIUS )
NOTIFY(XAUTH_AUTH)  -->
                    <--   NOTIFY(XAUTH_OK | XAUTH_BAD)
```

SecureID might also return a "get next" error code, where the user must enter the next passcode. An example of such is as follows:

```
Initiator              Responder
--------------         -----------------
                   <-- NOTIFY(XAUTH_SECUREID)
NOTIFY(XAUTH_AUTH) -->
                   <-- NOTIFY(XAUTH_OK | XAUTH_BAD |XAUTH_SECUREID)
NOTIFY(XAUTH_AUTH) -->
                   <-- NOTIFY(XAUTH_OK | XAUTH_BAD)
```

3.1 ISAKMP Main Mode

The following is an example of Main Mode with an authentication method of RSA signatures plus an extended authentication of RADIUS.

```
Initiator                      Responder
----------                     -----------
HDR, SA                    -->
                           <-- HDR, SA
HDR, KE, Ni                -->
                           <-- HDR, KE, Nr
HDR*, IDii, [CERT,] SIG_I  -->
                           <-- HDR*, IDir, [CERT,] SIG_R, NOTIFY(1)
HDR*, NOTIFY(2)            -->
                           <-- HDR*, NOTIFY(3)
```

```
NOTIFY(1) = NOTIFY(XAUTH_RADIUS)
NOTIFY(2) = NOTIFY(XAUTH_AUTH(user, password))
```

```
   NOTIFY(3) = NOTIFY(XAUTH_OK | XAUTH_BAD('bad password'))
```

While the extended authentication exchange MAY happen anywhere in a ISAKMP exchange, the user s password MUST be sent over securely. Thus Aggressive Mode MUST NOT be used.

The stipulation above only allows us two choices of placement in Main Mode. One as in the above example, and the other, one exchange previous, where the gateway requests extended authentication when sending over its DH key and nonce. The method shown in the example is preferable, since it allows a lookup on the ID payload for a cross-reference.

The extended authentication exchange MAY also be used in Quick Mode, but for interpretability's sake, the method displayed in the example above MUST be supported.

3.2 ISAKMP NOTIFY Types

NOTIFY Type	Value
XAUTH_AUTH	8200
XAUTH_OK	8201
XAUTH_BAD	8202
XAUTH_SECUREID	8203
XAUTH_RADIUS	8204

XAUTH_SECUREID and XAUTH_RADIUS contains no data, while XAUTH_OK and XAUTH_BAD MAY contain a text message in the data. This text message SHOULD be displayed to the user.

XAUTH_AUTH contains the user's credential attributes in the data. For RADIUS, it MUST include the user's name and password attributes (in any order). For SecureID, it MUST include the user's name, PIN and passcode attributes (in any order).

3.3 ISAKMP Extended Authentication Attributes

Attribute	Value	Type
User Name	65051	Variable
User Password/P.I.N.	65052	Variable
Secure ID password	65052	Variable

All of the above attributes are ASCII text strings. The User Name MAY be any unique identifier of the user such as a login name, an email address, or a X.500 DN.

4. RADIUS Extended Authentication

RADIUS [RADIUS] uses a user id and password to authenticate a client.

A RADIUS server requires a shared-secret between it and any host authenticating with so as to encrypt the user's password. This shared-secret is the responsibility of the gateway.

Usually the RADIUS server will require the user name and password. But it might also require optional information about the client such as its IP address (NAS-IP-ADDRESS) or its identifier (NAS-IDENTIFIER) and the port that the user is coming in on (NAS-PORT). Again, this is the responsibility of the gateway since it is authenticating on behalf of the client.

Access-Challenge messages are NOT supported.

5. SecureID Extended Authentication

SecureID uses smart cards to generate a 'passcode' to authenticate the user. This passcode combined with the user's password provides stronger authentication than just passwords.

6. Security Considerations

Care should be taken when sending sensitive information over public networks such as the Internet. Thus the user's password should never be sent in the clear.

7. References

[Bradner97] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

[Finseth93] Finseth, C., "An Access Control Protocol, Sometimes Called TACACS", RFC1492, 1993.

[RADIUS] Rigney, C., Rubens, A., Simpson, W., Willens, S., "Remote Authentication Dial In User Service (RADIUS) ", RFC2138, 1997.

8. Editor's Address

Roy Pereira
<rpereira@timestep.com>
TimeStep Corporation
+1 (613) 599-3610 x 4808

The IPSec working group can be contacted via the IPSec working group's mailing list (ipsec@tis.com) or through its chairs:

Robert Moskowitz
rgm@chrysler.com
Chrysler Corporation

Theodore Y. Ts o
tytso@MIT.EDU
Massachusetts Institute of Technology