Internet Engineering Task Force
IP Security Working Group
Internet Draft
Expires in six months

R. Pereira
TimeStep Corporation

February 11, 1998

# Extended Authentication Within ISAKMP/Oakley
<draft-ietf-ipsec-isakmp-xauth-01.txt>

## Status of this Memo



## Abstract

This document describes a method for using existing unidirectional authentication mechanisms such as RADIUS, SecureID, and OTP with ISAKMP.

Table of Contents



## 1. Introduction

The following technique allows IPSec's ISAKMP/Oakley protocol to support extended authentication mechanisms like two-factor authentication, challenge/response and other remote access unidirectional authentication methods.

These authentication mechanisms have a large deployment in remote access applications and many IT departments have requirements for these unidirectional authentication mechanisms.

## 1.1 Extended Authentication

Two-factor authentication and challenge/response schemes like SDI's SecureID and RADIUS are forms of authentication that allow a gateway, firewall, or network access server to offload the user administration and authentication to a central management server. IPSec's ISAKMP/Oakley protocol supports certificates (RSA & DSS), shared-secret, and Kerberos as authentication methods, but since the authentication methods described within this document are only unidirectional authentication methods (client to a gateway/firewall), they cannot be used by themselves, but must be used in-conjunction 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 a secured ISAKMP message. The

gateway/firewall would then use either the appropriate protocol

(RADIUS, SecureID, OTP) to authenticate the user. This allows the authentication server to be within the private network that the gateway/firewall is protecting.

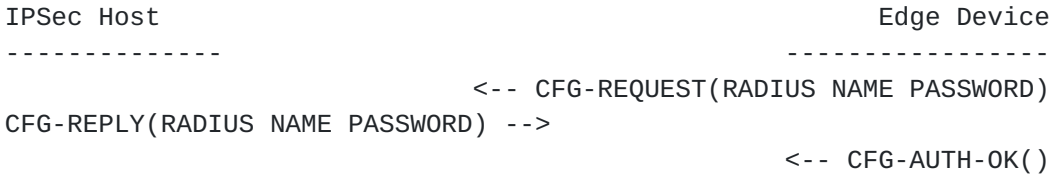
### 1.2 Specification of Requirements

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. Authentication Types

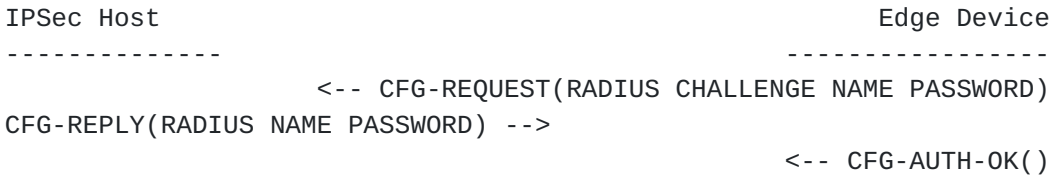
### 2.1 Simple Authentication

Where a user name and password are required for authentication.



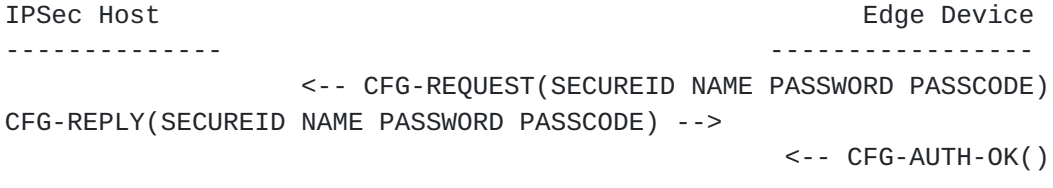

### 2.2 Challenge/Response

Where a challenge from the gateway/firewall must be incorporated with the reply. This makes each reply different.




### 2.3 Two-Factor Authentication

This authentication method combines something the user knows (their password) and something that the user has (a token card).




Some mechanisms allow for another request of the passcode;

```
IPSec Host                                          Edge Device
--------------                                     -----------------
                  <-- CFG-REQUEST(SECUREID NAME PASSWORD PASSCODE)
CFG-REPLY(SECUREID NAME PASSWORD PASSCODE) -->
                  <-- CFG-REQUEST(SECUREID NAME PASSWORD PASSCODE)
CFG-REPLY(SECUREID NAME PASSWORD PASSCODE) -->
                                                    <-- CFG-AUTH-OK()
```

### 2.4 One-Time-Password

Similar to the Challenge/Response method, this method allows authentication that is secure against passive attacks based on replaying captured passwords.

```
IPSec Host                                          Edge Device
--------------                                     -----------------
                       <-- CFG-REQUEST(OTP CHALLENGE NAME PASSWORD)
CFG-REPLY(TOP NAME PASSWORD) -->
                                                    <-- CFG-AUTH-OK()
```

## 3. Interaction with ISAKMP

This protocol utilizes the mechanisms described in ISAKMP-Config [Pereira97] to accomplish its request/reply transaction through ISAKMP.

An edge device (gateway or firewall) may request extended authentication from a IPSec host (end-node), thus forcing the host to respond with its extended authentication credentials. The edge device will then respond with a failed or passed message.

Example:

```
IPSec Host                                          Edge Device
--------------                                     -----------------
                  <-- CFG-REQUEST(SECUREID NAME PASSWORD PASSCODE)
CFG-REPLY(SECUREID NAME PASSWORD PASSCODE) -->
                                                  <-- CFG-AUTH-FAILED()
```

When the edge device requests extended authentication, it will specify the type of extra authentication and any parameters required for it. These parameters MAY be the attributes that it requires for authentication or they MAY be information required for the IPSec host's reply (eg. challenge string).

The last message, is simply a reply back from the gateway/firewall denoting failure or passing. The replay MAY have some textual

information describing the reason for the failure or success. The

gateway/firewall may also request another authentication, like Secure ID's next PIN request, where the user is required to enter the next passcode to further verify the user.

### 3.1 Exchanges

ISAKMP-Config sets forth some guidelines on where these exchanges may take place. This document will add on to those guidelines in relation to extended authentication exchanges.

As described in the last section, the edge device requests extended authentication. This MUST be supported at least in these three places:

[1] ISAKMP Main Mode in the responder's second message - if the client's ID is not relevant to decide whether or not to request extended authentication.

[2] ISAKMP Main Mode in the responder's third message - if the client's ID is relevant in deciding whether or not to request extended authentication.

[3] ISAKMP Aggressive mode in the responder's first message - if identity protection is not required for ISAKMP.

The main reason that only the above three places are valid are because the client's reply MUST be secured since it will carry sensitive information like passwords.

In the case of Aggressive Mode, ISAKMP-Config [Pereira97] denotes that the response be sent in an encrypted InfoMode ISAKMP message after the Aggressive Mode is done and an ISAKMP SA exists between the two peers.

The extended authentication exchange MAY also be used in Quick Mode, but for inter-operability's sake, the methods listed above MUST be supported.

## 4. Extensions to ISAKMP-Config

The following are extensions to the ISAKMP-Config [Pereira97] specification to support Extended Authentication.

### 4.1 NOTIFY Types

| Type | Value |
|---|---|
| ISAKMP_CFG_REQUEST | ( as defined in [Pereira97] ) |
| ISAKMP_CFG_REPLY | ( as defined in [Pereira97] ) |
| ISAKMP_CFG_AUTH_OK | 105 |
| ISAKMP_CFG_AUTH_FAILED | 106 |

- o ISAKMP_CFG_REQUEST - This message is sent from an edge device to an IPSec host trying to request extended authentication. Attributes that it requires sent back in the reply MUST be included with a length of zero (0). Attributes required for the authentication reply, such as a challenge string MUST be included with the proper values filled in.

- o ISAKMP_CFG_REPLY - This message MUST contain the authentication attributes that were requested by the edge device filled in.

- o ISAKMP_CFG_AUTH_OK - This message MAY contain a textual message in the XAUTH_MESSAGE attribute.

- o ISAKMP_CFG_AUTH_FAILED - This message MAY contain a textual message in the XAUTH_MESSAGE attribute.

### 4.2 Attributes

| Attribute | Value | Type |
|---|---|---|
| XAUTH_TYPE | 101 | Basic |
| XUATH_USER_NAME | 102 | Variable ASCII string |
| XAUTH_USER_PASSWORD | 103 | Variable ASCII string |
| XAUTH_PASSCODE | 104 | Variable ASCII string |
| XAUTH_MESSAGE | 105 | Variable ASCII string |
| XAUTH_CHALLENGE | 106 | Variable ASCII string |
| XAUTH_DOMAIN | 107 | Variable ASCII string |

- o XAUTH_TYPE - The type of extended authentication requested whose values are described in the next section. This is a mandatory attribute for the ISAKMP_CFG_REQUEST and ISAKMP_CFG_REPLY messages.

- o XAUTH_USER_NAME - The user name MAY be any unique identifier of the user such as a login name, an email address, or a X.500 Distinguished Name.

- o XAUTH_USER_PASSWORD - The user's password.

- o XAUTH_PASSCODE - A token card's passcode. This SHOULD only be used when the password attribute is also used.

- o XAUTH_MESSAGE - A textual message from an edge device to an IPSec host. This message SHOULD be displayed to the user to notify them of the reason why authentication failed or succeed.

- o XAUTH_CHALLENGE - A challenge string sent from the edge device to the IPSec host for it to include in its calculation of a password or passcode. This attribute SHOULD only be sent in a ISAKMP_CFG_REQUEST message.

- o XAUTH_DOMAIN - The domain to be authenticated in. This value will have different meaning depending on the authentication type.

### 4.3 Authentication Types

| Value | Authentication Required |
|---|---|
| 0 | Generic |
| 1 | RADIUS |
| 2 | OTP |
| 3 | NT Domain |
| 4 | Unix Login |
| 5 | SDI SecureID |
| 6 | AXENT Defender |
| 7 | LeeMah InfoCard |
| 8 | ActiveCard |
| 9 | Secure Computing Enigma (DES Gold) |
| 10 | TACACS |
| 11 | TACACS+ |
| 12 | S/KEY |
| 13 | NDS (Netware Directory Services) |

- o Generic - A catch-all type that allows for future extensibility and a generic mechanism to request authentication information. This method allows for any type of extended authentication.

- o RADIUS - A RADIUS [Radius97] server requires a user name and a password, but since RADIUS may be proxying for another type of authentication method, both the request and the reply MAY be like any of the other extended authentication types.

- o OTP - One-Time-Passwords as defined in [Opt96] uses a challenge string to request a certain generated password. The request SHOULD contain a user name, password and a challenge string

while the reply MUST contain the user name and the generated password. The challenge string is formatted as defined in [Metz97].

- NT Domain - This authentication type provides for user authentication by login into a Windows NT(r) domain. The request SHOULD contain empty user name, password and domain attributes. The reply MUST contain all of these attributes filled in. The domain attribute is optional for both messages, and SHOULD NOT be included in the reply if it isn t included in the request.

- Unix Login - Much like the NT Domain authentication type, but this will authenticate the user to a Unix(r) workstation.

- SDI SecureID, AXENT Defender, LeeMah InfoCard, ActiceCard, Enigma/DES Gold - All of these (and others) use smart cards to generate a 'passcode' to authenticate the user. This passcode combined with the user's password provides stronger authentication than just passwords. The response MUST include the user name, user password and the token card's passcode. This authentication type MIGHT also include a challenge string in the request.

- TACACS - Defined in [Tacacs93], this authentication protocol was the precursor to RADIUS, thus the same rules apply.

- TACACS+ - Defined in [Tacacs+97], this authentication protocol is an updated version of the original TACACS protocol, thus the same rules apply.

- S/KEY - This one-time-password scheme defined in [Skey95] was the precursor to OTP, thus the same rules apply.

- NDS - Much like the NT Domain authentication type, but this will authenticate the user to a NetWare Directory server.

## 5. Security Considerations

Care should be taken when sending sensitive information over public networks such as the Internet. A user's password should never be sent in the clear and when sent encrypted, the destination MUST have been previously authenticated. The use of ISAKMP-Config [Pereira97] plus further guidelines outlined in this document address these issues.

## 6. References

[Bradner97] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", RFC2119

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

[Radius97] C. Rigney, A. Rubens, W. Simpson, S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC2138

[Pereira97] R. Pereira, "The ISAKMP Configuration Method", draft-ietf-ipsec-isakmp-cfg-02

[Opt96] N. Haller, C. Metz, "A One-Time Password System", RFC1938

[Skey95] N. Haller, "The S/KEY One-Time Password System", RFC1760

[Tacacs93] C. Finseth, "An Access Control Protocol, Sometimes Called TACACS", RFC1492

[Tacacs+97] D. Carrel, L. Grant, "The TACACS+ Protocol Version 1.77", draft-grant-tacacs-01.txt

[Metz97] C. Metz, "OTP Extended Responses", RFC 2243

## 7. 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
rgm3@icsa.net
ICSA

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