Network Working Group
Expires May 1997
Internet Draft

S. Mamros
New Oak Communications
November 1997

Pre-Shared Key Extensions for ISAKMP/Oakley

<draft-mamros-pskeyext-00.txt>

Status of this Memo

1. Abstract

The application of IP Security for remote access over the Internet requires that it support ''traditional'' authentication paradigms. This document describes how a traditional username and passphrase-style mechanism can be integrated into the existing pre-shared key authentication mechanism in ISAKMP/Oakley.

2. Introduction

ISAKMP/Oakley [Hark97] provides several authentication methods. Of these, only the pre-shared key authentication method can be made to work in the absence of a public key infrastructure. While it is expected that usage of public key mechanisms will increase substantially in the near future, many sites which want to use IP Security as a tunnelling mechanism for remote access over the Internet may not be able or willing to convert their existing systems to use public key technology right away. Thus, these sites will

need to use pre-shared key authentication in one form or another.

ISAKMP/Oakley provides both Main Mode and Aggressive Mode as the two basic methods for establishing an authenticated key exchange. However, Main Mode using pre-shared key authentication is restricted to using only the IP addresses of the initiator and responder as the means to select a key. Remote access solutions require user-based keying, which means that Aggressive Mode is the only viable method which can be used with pre-shared keys.

The major drawback to Aggressive Mode is that, unlike Main Mode, one cannot protect the identities of the initiator and responder; these must be transmitted in the clear. Another element which must be transmitted in the clear is the responder's hash, designated as HASH_R in [Hark97]. When pre-shared key authentication is being used, HASH_R is derived from a combination of the pre-shared key and the nonces, ISAKMP cookies, and publicly-exchanged Diffie-Hellman values of both the initiator and responder, plus the responder's identity. The only "secret" element among those used to calculate HASH_R is the pre-shared key itself; all of the other elements are transmitted in the clear in the first two messages of Aggressive Mode. The security of HASH_R is thus entirely dependent on the security of the pre-shared key itself, which in turn relies on the effective key length.

The "traditional" method of using a username for identification, and a passphrase for authentication, is still in common use at many sites. Such sites may be tempted to map the username/passphrase directly to the ISAKMP/Oakley pre-shared authentication mechanism, with the username being used for the initiator's identity (designated as IDii in [Hark97]) and the passphrase being employed as the pre-shared key. However, the lack of identity protection in Aggressive Mode, coupled with a relatively small search space for text-based passphrases, makes this approach vulnerable to brute-force searches of the passphrase via analysis of HASH_R.

This document defines an alternate approach through which usernames and passphrases may be used in conjunction with pre-shared key authentication, while providing somewhat better protection for the identity and also expanding the brute-force key space. The method described here employs an additional algorithm for deriving the values used for IDii and the pre-shared key; these values are then used as-is in the standard algorithms defined in [Hark97] for deriving keys and hash values.

3. Terms and Definitions

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [RFC-2119].

4.1. Derivation of Initiator Identity (IDii)

The initiator identity (IDii) is derived by performing a SHA-1 [SHA] hash calculation over the username. Any characters used to terminate or delimit the username string, such as a zero octet, MUST NOT be included in the hash calculation. If the environment in which the username is defined considers usernames to be case-insensitive, any uppercase alphabetical characters (A-Z) in the username MUST be converted to their lowercase equivalents (a-z) before performing the hash calculation.

The initiator places the SHA-1 hash in the Identification Data field of the Identification Payload designated as IDii in its initial message to the responder in Aggressive Mode. The ID Type field MUST be ID_KEY_ID, as defined in [Pip97]. The responder stores a table of SHA-1 hashes mapped to their respective usernames and their corresponsing passphrases.

4.2. Derivation of the Pre-Shared Key

The pre-shared key is derived by using the HMAC algorithm [RFC-2104] in conjunction with the SHA-1 hash algorithm, with the passphrase used as the key and the plaintext username as the "message". In the notation of [Hark97],

```
pre-shared-key = prf(passphrase, username)
```

where the pseudo-random function is HMAC-SHA-1.

As with the IDii derivation described above, terminating and delimiting characters (such as zero octets) MUST NOT be included in the calculation. If usernames are case-insensitive, uppercase alphabetical characters MUST be converted to lowercase before applying this algorithm. However, mixed-case passphrases MUST be supported, and the case of all alphabetic characters in the passphrase MUST be preserved in the calculation. The resulting 160-bit hash value MUST be used in its entirety as the pre-shared key.

5. Security Considerations

The methods described in this document do not purport to be a solution for all of the problems which face any system relying on username/passphrase authentication for security. A weak passphrase can compromise the security of any such system. Also, physical and logical security of the username/passphrase database is crucially important.

The method for deriving IDii does provide some level of identity obfuscation, but it falls short of full identity protection as provided by Main Mode. One can compare the value of IDii with the values used in previous exchanges to determine whether or not the same user initiated a prior exchange. We rely on the collision and reversability resistance and properties of SHA-1 to protect the original username.

The algorithm for deriving the pre-shared key is stronger than using the passphrase as-is for the key only if the plaintext username is not revealed to an attacker. Security administrators may wish to consider the use of different usernames for remote access under this scheme than those which are used for other systems such as electronic mail.

6. References

[Hark97] Harkins, D., Carrel, D., "The resolution of ISAKMP with Oakley", draft-ietf-ipsec-isakmp-oakley-05.txt.

[Pip97] Piper, D., "The Internet IP Security Domain Of Interpretation for ISAKMP", draft-ietf-ipsec-ipsec-doi-06.txt.

[RFC-2104] Krawczyk, H., Bellare, M., and Canetti, R., "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[RFC-2119] Bradner, S., "Key Words for use in RFCs to indicate Requirement Levels", RFC 2119, March 1997.

[SHA] NIST, FIPS PUB 180-1, Secure Hash Standard, April 1995.
http://csrc.nist.gov/fips/fip180-1.txt (ascii)
http://csrc.nist.gov/fips/fip180-1.ps (postscript)

7. Author's Address

Shawn Mamros

New Oak Communications, Inc.
125 **Nagog Park** +1 978 266 1011
Acton, Massachusetts, 01720 smamros@newoak.com