MSEC Working Group
Internet-Draft
Expires: August 21, 2006

B. Weis
S. Rowles
Cisco Systems
February 17, 2006

Updates to the Group Domain of Interpretation (GDOI) draft-weis-gdoi-update-00

Status of this Memo

Copyright Notice

Abstract

This memo describes additional updates to the Group Domain of Interpretation (GDOI) [RFC3547] . It provides clarification where the original text is unclear. It also includes a discussion of algorithm agility within GDOI, and proposes several new algorithm attribute values.

Table of Contents

1. Introduction

The Group Domain of Interpretation (GDOI) is a group key management protocol fitting into the Multicast Security Group Key Management Architecture [RFC4046]. GDOI is used to disseminate policy and corresponding secrets to a group of participants. GDOI is implemented on hosts and intermediate systems to protect group IP communication (e.g., IP multicast packets) by encapsulating them with the IP Encapsulating Security Payload (ESP) [RFC4303] packets. However, implementation experience has revealed some inconsistencies in RFC 3547 needing clarification. It also defines some additional GDOI algorithm attributes which are useful to GDOI applications.

Algorithm agility, the ability to add new algorithms to namespaces, is an important consideration for any protocol. This memo analyzes the state of algorithm agility within GDOI, and proposes some changes based upon that analysis. In particular, methods for fully supporting the SHA-256 algorithm [FIPS.180-2.2002] as an alternative to SHA-1 and MD5 are described.

1.1. Requirements notation

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 [RFC2119].

2. Cryptographic Algorithm agility

Algorithm agility was a goal during the development of GDOI, and RFC 3547 generally provides the ability to add new algorithms as necessary. However, further analysis has shown that there are places where algorithm agility is not complete. This section discusses the use cryptographic algorithms within GDOI, puts out variances in algorithm agility, and proposes clarifications without changing any payload formats within the protocol.

Recent published attacks on the SHA-1 algorithm motivate its replacement as a cryptographic hash algorithm. The ability for GDOI to move to the SHA-256 hash algorithm is explicitly discussed. Later sections on this document propose some enhancements to the GDOI protocol to provide for an easier means of supporting this and additional hash functions.

2.1. Phase 1 protocol

GDOI is a "phase 2" protocol protected by a "phase 1" protocol. The Phase 1 protocol defined in RFC 3547 is an IKEv1 Phase 1 protocol (Main Mode or Aggressive Mode). The Phase 1 protocol provides confidentiality via an encryption cipher. It also provides message integrity via a pseudo random function ("prf") (described in Section 4 of [RFC2409], which is usually a hash algorithm using the HMAC [RFC2104] construction. IKEv1 negotiates which encryption ciphers and hash algorithms are to be used.

IKEv1 cipher algorithms come from the "Encryption Algorithm" list in the IANA IPsec registry [IPSEC-REG], and the hash algorithms come from the "Hash Algorithm" list in the same registry. The IANA IPsec registry currently includes the SHA2-256, which is intended to be the SHA-256 hash algorithm.

2.2. GROUPKEY-PUSH signature

The GROUPKEY-PUSH message is protected by both an encryption cipher and a digital signature for message integrity. The encryption cipher is described by the IANA GDOI registry as the KEK_ALGORITHM attribute [GDOI-REG]. The digital signature comprises both a hash algorithm defined by the GDOI SIG_HASH_ALGORITHM attribute and a public key signature algorithm defined by the SIG_ALGORITHM attribute. This memo adds the SHA-256 algorithm to the SIG_HASH_ALGORITHM attribute in a later section.

2.3. IPsec TEK Integrity HMAC algorithms

IPsec SAs are distributed by GDOI. An IPsec ESP SA can include an

encryption cipher for confidentiality and an algorithm for packet authentication. The encryption ciphers are defined by the IPsec ESP Transform Identifiers defined in the IANA ISAKMP registry [ISAKMP-REG]. The packet authentication method is distributed via an "Authentication Algorithm" SA attribute. SHA-256 may be chosen as the authentication algorithm with HMAC-SHA2-256. Similarly, an IPsec AH SA is defined by choosing AH_SHA2-256 as the "AH Transform Identifier".

2.4. Certificate Payload

Messages in the GROUPKEY-PULL and GROUPKEY-PUSH protocols may include a Certificate Payload (CERT). Digital signatures, and the algorithm agility thereof, are outside the scope of this memo.

2.5. POP Hash Function

The GDOI Proof of Possession (POP) payload may be included in the GROUPKEY-PULL protocol. It contains a digital signature over the hash of some nonces, which provides the current possession of the peer. The digital signature algorithm is defined as the "POP Algorithm" in the IANA GDOI registry [GDOI-REG]. However, identity of the hash algorithm to create the signed data was omitted in RFC 3547. This memo remedies this omission in a clarification section below.

3. RFC 3547 Clarification

3.1. SA Payload

The units of the SIG_KEY_LENGTH value was unspecified in RFC 3547. The value is the length of the keys in bits.

The GDOI_PROTO_IPSEC_ESP attribute is sometimes referred to by the truncated name PROTO_IPSEC_ESP.

RFC3547 explicitly specifies that if a KEK cipher requires an IV, then the IV MUST precede the key in the KEK_ALGORITHM_KEY KD payload attribute. However, it should be noted that this IV length is not included in the KEK_KEY_LEN SA payload attribute sent in the SA payload. The KEK_KEY_LEN includes only the actual length of the cipher key.

The Group Controller/Key Server (GCKS) adds the KEK_KEY_LEN attribute to the SA payload when distributing KEK policy to group members. The group member verifies whether or not it has the capability of using a cipher key of that size. If the cipher definition includes a fixed key length (e.g., KEK_ALG_3DES), the group member can make its decision solely using KEK_ALGORITHM attribute and does not need the KEK_KEY_LEN attribute. Sending the KEK_KEY_LEN attribute in the SA payload is OPTIONAL if the KEK cipher has a fixed key length.

3.2. SIG Payload

The GROUPKEY-PUSH message SIG payload is further clarified here; the SIG payload is a signature of the entire GROUPKEY-PUSH message (not including the SIG payload) before it's been encrypted. The HASH is taken over the string 'rekey', the GROUPKEY-PUSH HDR, SEQ, SA, KD, and optionally the CERT payload. After the SIG payload is created using the signature of the above hash, the current KEK encryption key encrypts all the payloads following the GROUPKEY-PUSH HDR.

3.3. SEQ Payload

Each GROUPKEY-PUSH message contains a sequence number, which provides anti-replay protection for a KEK. Thus, the GCKS returns a SEQ payload in the GROUPKEY-PULL exchange only if a KEK attribute also exists in the SA payload.

A KEK sequence number is associated with a single SPI (i.e., the single set of cookie pair values sent in a GROUPKEY-PUSH ISAKMP HDR). When a new KEK is distributed by a GCKS, it contains a new SPI and resets the sequence number.

When a SEQ payload is included in the GROUPKEY-PULL exchange, it includes the most recently used sequence number for the group. At the conclusion of a GROUPKEY-PULL exchange, the initiating group member MUST NOT accept any rekey message with both the KEK attribute SPI value and a sequence number less than or equal to the one received during the GROUPKEY-PULL. When the first group member initiates a GROUPKEY-PULL exchange, the GCKS provides a Sequence Number of zero, since no GROUPKEY-PUSH messages have yet been sent. Note the sequence number increments only with GROUPKEY-PUSH messages. The GROUKEY-PULL exchange distributes the current sequence number to the group member.

The sequence number resets to one with a new KEK attribute, as described in section 5.6 of RFC 3547: "Thus the first packet sent for a given Rekey SA will have a Sequence Number of 1". The sequence number increments with each successive rekey.

3.4. POP Payload

RFC 3547 defines the Proof of Possession (POP) payload, which contains a digital signature over a hash. Some RFC 3537 text erroneously describes it as a "prf()".

RFC 3547 omitted including a GDOI SA attribute in which the hash function type could be passed between the GCKS and the group member. This results in no method for the hash algorithm to be specified within the GDOI protocol. To remedy this omission, the hash algorithm passed in the SIG_HASH_ALGORITHM MUST be also used as the POP hash algorithm.

Receivers of the POP payload need the sender's public key in order to validate the POP. RFC 3547 does not provide for passing of the POP signature key. Indeed, the public key will usually come from a certificate in the CERT payload. However, if a CERT payload is not sent with a POP payload, or if the CERT is an attribute cert (not containing a public key), then the distribution of the public key is outside of the scope of this standard.

3.5. TEK Integrity Key

Regarding the integrity key pushed to the member, the SHA1 keys will consist of 160 bits, SHA256 keys will consist of 256 bits, and MD5 keys will consist of 128 bits.

3.6. PFS

RFC 3547 provides an OPTIONAL additional protection for the KD payload during a GROUPKEY-PULL exchange called Perfect Forward

Secrecy (PFS). If the GCKS and group member exchange KE payloads containing Diffie-Hellman public keys, the GCKS encrypts the KD payload with a secret obtained from the Diffie-Hellman shared number. This encryption precedes the encryption of the entire GROUPKEY-PULL message.

The purpose of PFS in GDOI is to more carefully protect the keying material passed from the GCKS to the group member. If a passive attacker captures the GROUPKEY-PULL exchange and performs an offline attack of the IKE Phase 1 confidentiality keys, it may eventually discover them. If PFS is not used, the attacker can immediately use the recovered keys to decrypt data packets and GROUPKEY-PUSH messages, either live or stored. Thus, the IKE Phase 1 keys are critical to the long-term confidentiality of the group. PFS was added as an additional mechanism to hinder a passive attacker by requiring it to perform an additional cryptanalysis to recover the Diffie-Hellman shared number computed by the GCKS and group member.

RFC 3547 Section 3.2.1 says "The GCKS responder will xor the DH secret with the KD payload and send it to the member Initiator, which recovers the KD by repeating this operation as in the Oakley IEXTKEY procedure [RFC2412]". However, the IEXTKEY procedure does not xor the DH shared secret with an entire payload, and the DH shared secret is not likely to be long enough to cover the entire payload. Therefore, the following amended procedure MUST be used for PFS.

1. The leftmost bits in the DH shared secret are used as an encryption key. The encryption key algorithm described in the KEK_ALGORITHM attribute is used.

2. The new key is used to encrypt the KD payload. Note that the length of the KD payload may be larger due to cipher block padding. If so, the KD payload length must be modified to reflect the actual length of the ciphertext.

3.7. GCKS Authorization

Meadows and Pavlovic have published a paper [MP04] describing a means by which a rogue GDOI device (i.e., GCKS or group member) can gain access to a group for which it is not a group member. The rogue devices perpetrates a man-in-the-middle attack, which can occur if the following conditions are true:

1. The rogue GDOI participant convinces an authorized member of the group (i.e., victim group member) that it is a key server for that group.

2. The victim group member, victim GCKS, and rogue group member all share IKEv1 authentication credentials.

3. The victim GCKS does not properly verify that the IKEv1 authentication credentials used to protect a GROUPKEY-PULL protocol are authorized to be join the group.

The actual attack is too detailed to explain in this memo, but it is important to recognize that it can be perpetrated whether or not the group policy requires the use of CERT and POP payloads. In all cases, the attack can be stopped when the authorized GCKS performs authorization based on the IKEv1 authentication credentials. A GDOI key server SHOULD perform one of the following authorization checks:

1. If the use of CERT and POP payloads are not mandated in group policy, the GCKS SHOULD maintain an list of authorized group members for each group, where the group member identity is its IKEv1 authentication credentials. The authorization check SHOULD be made after receipt of the ID payload containing a group id the group member is requesting to join.

2. If the CERT and POP payloads are used for authorization, the GCKS SHOULD verify that the identify in the CERT payload refers to the same identity in the IKEv1 authentication credentials. This stops a group member from authenticating to the GCKS with its own credential, yet including another group member's credentials and proof-of-possession in the CERT and POP payloads.

Additionally, a GDOI group member SHOULD be configured with policy describing which IKEv1 identities are authorized to act as GCKS for a group.

3.8. Minimum defined attributes

Minimum attributes that must be sent as part of an SA KEK: KEK_ALGORITHM, KEK_KEY_LENGTH (if the cipher definition includes a variable length key), KEK_KEY_LIFETIME, SIG_HASH_ALGORITHM (except for DSA based algorithms), SIG_ALGORITHM.

RFC 3547 states that all mandatory IPsec DOI attributes are mandatory in GDOI_PROTO_IPSEC_ESP. However, no such list of mandatory IPsec DOI attributes can be found in RFC 2407. This memo requires that the following attributes MUST be supported by an RFC 3547 implementation supporting the GDOI_PROTO_IPSEC_ESP SA TEK: SA Life Type, SA Life Duration, Encapsulation Mode, Authentication Algorithm (if the ESP transform includes authentication).

3.9. Attribute behavour

An GDOI implementation MUST abort if it encounters and attribute or capability that it does not understand.

4. New GDOI Attributes

This section contains new attributes to be are defined as part of GDOI.

4.1. Signature Hash Algorithm

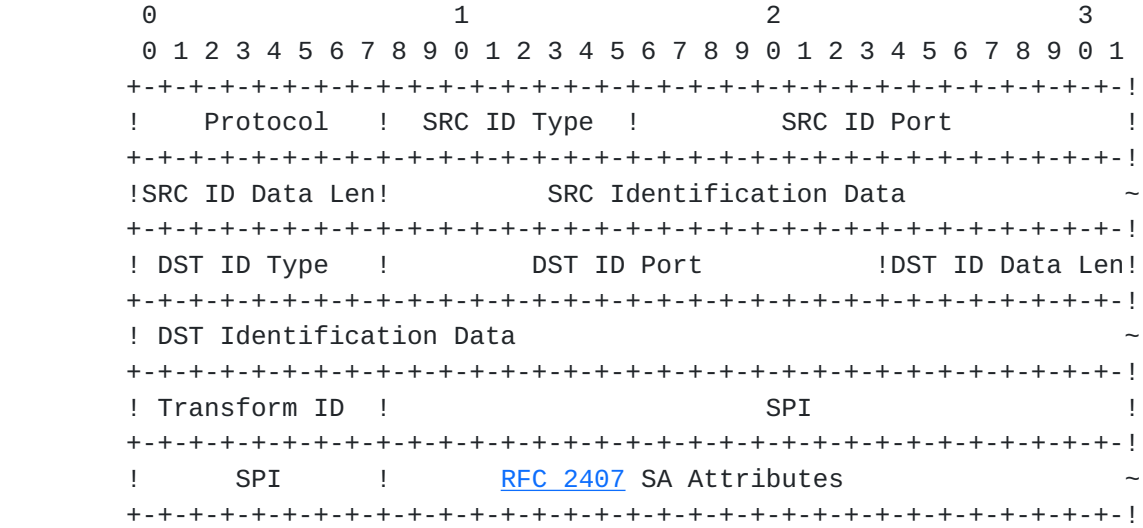
RFC 3547 defines two signature hash algorithms (MD5 and SHA-1). However, steady advances in technology have rendered both hash algorithms to be weak when used as a signature hash algorithm.

The SHA-256 hash algorithm [FIPS.180-2.2002] has been made available by NIST as a replacement for SHA-1, and is its preferred replacement for both MD5 and SHA-1. A new value for the GDOI SIG_HASH_ALGORITHM attribute is defined by this memo to represent the SHA-256 hash algorithm: SIG_HASH_SHA256. Support for SIG_HASH_SHA256 is OPTIONAL.

4.2. Support of AH

RFC3547 only specifies data-security SAs for one security protocol, IPsec ESP. Typically IPsec implementations use ESP and AH IPsec SAs. This document extends the capability of GDOI to support both ESP and AH. The GROUPKEY-PULL mechanism will establish IPsec ESP SAs and IPsec AH SAs. The GROUPKEY-PUSH will refresh the IPsec ESP SAs and the IPsec AH SAs. Support for AH [RFC4302] will come with the introduction of a new SA_TEK Protocol-ID with the name GDOI_PROTO_IPSEC_AH. Support for the GDOI_PROTO_IPSEC_AH SA TEK is OPTIONAL.

The TEK Protocol-Specific payload for AH is as follows:



The SAT Payload fields are defined as follows:

- Protocol (1 octet) -- Value describing an IP protocol ID (e.g., UDP/TCP). A value of zero means that the Protocol field should be ignored.

- SRC ID Type (1 octet) -- Value describing the identity information found in the SRC Identification Data field. Defined values are specified by the IPsec Identification Type section in the IANA ISAKMP Registry [ISAKMP-REG].

- SRC ID Port (2 octets) -- Value specifying a port associated with the source Id. A value of zero means that the SRC ID Port field should be ignored.

- SRC ID Data Len (1 octet) -- Value specifying the length of the SRC Identification Data field.

- SRC Identification Data (variable length) -- Value, as indicated by the SRC ID Type. Set to three bytes of zero for multiple-source multicast groups that use a common TEK for all senders.

- DST ID Type (1 octet) -- Value describing the identity information found in the DST Identification Data field. Defined values are specified by the IPsec Identification Type section in the IANA ISAKMP Registry [ISAKMP-REG].

- DST ID Port (1 octet) -- Value describing an IP protocol ID (e.g., UDP/TCP). A value of zero means that the DST Id Port field should be ignored.

- DST ID Port (2 octets) -- Value specifying a port associated with the source Id. A value of zero means that the DST ID Port field should be ignored.

- DST ID Data Len (1 octet) -- Value specifying the length of the DST Identification Data field.

- DST Identification Data (variable length) -- Value, as indicated by the DST ID Type.

- Transform ID (1 octet) -- Value specifying which AH transform is to be used. The list of valid values is defined in the IPsec AH Transform Identifiers section of the IANA ISAKMP Registry [ISAKMP-REG].

- SPI (4 octets) -- Security Parameter Index for AH.

- RFC 2407 Attributes -- AH Attributes from Section 4.5 of [RFC2407]. The GDOI supports all IPsec DOI SA Attributes for

GDOI_PROTO_IPSEC_AH excluding the Group Description, which MUST NOT be sent by a GDOI implementation and is ignored by a GDOI implementation if received. The Authentication Algorithm attribute of the IPsec DOI is group authentication in GDOI. The following RFC 2407 attributes MUST be sent as part of a GDOI_PROTO_IPSEC_AH attribute: SA Life Type, SA Life Duration, Encapsulation Mode.

5. IANA Considerations

The SIG_HASH_ALGORITHM KEK Attribute should be assigned a new Algorithm Type value from the RESERVED space to represent the SHA-256 hash algorithm as defined. The new algorithm name should be SIG_HASH_SHA256.

A new SA_TEK type Protocol-ID type should be assigned from the RESERVED space. The new algorithm id should be called GDOI_PROTO_IPSEC_AH, and refers to the IPsec AH encapsulation.

6. Security Considerations

This memo describes additional clarification and protocol updates to the GDOI protocol. The security considerations in RFC 3547 remain accurate, with the following additions.

- Several minor cryptographic hash algorithm agility issues are resolved, and the stronger SHA-256 cryptographic hash algorithm is added.

- Protocol analysis has revealed a man-in-the-middle attack when the GCKS does not authorize group members based on their IKEv1 authentication credentials. This is true even when a CERT and POP payloads are used for authorization. Although suggested as an option in RFC 3547, a GDOI device (group member or GCKS) SHOULD NOT accept an identity in a CERT payload that does not match the IKEv1 identity used to authenticate the group member.

7. References

7.1. Normative References

[FIPS.180-2.2002]
National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-2, August 2002, <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>.

[GDOI-REG]
Internet Assigned Numbers Authority, "Group Domain of Interpretation (GDOI) Payload Type Values", IANA Registry, December 2004, <http://www.iana.org/assignments/gdoi-payloads>.

[IPSEC-REG]
Internet Assigned Numbers Authority, "Internet Key Exchange (IKE) Attributes IKE Attributes", IANA Registry, December 2005, <http://www.iana.org/assignments/ipsec-registry>.

[ISAKMP-REG]
Internet Assigned Numbers Authority, "Internet Security Association and Key Management Protocol (ISAKMP) Identifiers ISAKMP Attributes", IANA Registry, January 2006, <http://www.iana.org/assignments/isakmp-registry>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2407] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC3547] Baugher, M., Weis, B., Hardjono, T., and H. Harney, "The Group Domain of Interpretation", RFC 3547, July 2003.

[RFC4046] Baugher, M., Canetti, R., Dondeti, L., and F. Lindholm, "Multicast Security (MSEC) Group Key Management Architecture", RFC 4046, April 2005.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)",

RFC 4303, December 2005.

7.2. Informative References

[MP04] Meadows, C. and D. Pavlovic, "Deriving, Attacking, and Defending the GDOI Protocol", ESORICS 2004 pp. 53-72, September 2004.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

Authors' Addresses

Brian Weis
Cisco Systems
170 W. Tasman Drive
San Jose, California 95134-1706
USA

Phone: +1-408-526-4796
Email: bew@cisco.com

Sheela Rowles
Cisco Systems
170 W. Tasman Drive
San Jose, California 95134-1706
USA

Phone: +1-408-527-7677
Email: srowles@cisco.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.