08.06.2004 Martin Schiele, 699440

The Group Domain of Interpretation,

An ISAKMP DOI for secure group communication

1. Introduction

This document presents an ISAMKP Domain of Interpretation (DOI) for group key management called the "Group Domain of Interpretation" (GDOI). In this group key management model, the GDOI protocol is run between a group member and a "group controller/key server" (GCKS), which establishes security associations among authorized group members. GDOI is a group security association management protocol: All GDOI messages are used to create, maintain, or delete security associations for a group. These security associations protect one or more key-encrypting keys (KEK), traffic-encrypting keys (TEK), or data shared by group members for multicast and groups security applications.

2. Recap of ISAKMP

To be able to understand what GDOI really is, one has to know something about ISAKMP, since GDOI depends on ISAKMP in many aspects.

ISAKMP is an abbreviation for Internet Security Association and Key Management Protocol. This protocol negotiates and manages security associations between entities, providing secure connection between two parties. Roughly you can devide this protocol into two phases. In phase 1, entities decide how to protect further communication. This is achieved by several techniques described in RFC 2408. Phase 2 is where the exchanges of GDOI take place. GDOI is a domain of interpretation which is a metalanguage to define payloads.

3. How GDOI works

3.1. General review

GDOI is a "phase 2" protocol which must be protected by a "phase 1" protocol. The "phase 1" protocol can be any protocol which provides peer authentication, confidentiality and message integrity. In RFC 3547 the use of ISAKMP is specified. Therefore this abstract will refer to the use of ISAKMP.

3.2. New payloads

In reference to ISAKMP, GDOI introduces six new payloads:

1) GDOI Security Association

2) SA KEK which follows the Security Association payload

3) SA TEK which follows the Security Association payload

4) Key Download Array (KD)

5) Sequence number (SEQ)

6) Proof of Possession (POP)

The Security Association payload is defined in RFC 2408. For the GDOI, it is used by the GCKS to assert security attributes for both Re-key and Data-security Security Associations.

The SA KEK payload contains security attributes for the KEK method for a group and parameters specific to the Groupkey-Pull operation.

The SA TEK payload contains security attributes for a single TEK associated with a group.

The Key Download payload contains group keys for the group specified in the Security Association payload. These key download payloads can have several security attributes applied to them based upon the security policy of the group as defined by the associated Security Association payload.

The Sequence Number Payload (SEQ) provides an anti-replay protection for Groupkey-Push messages. It's use is similar to the Sequence Number field defined in the IPsec ESP protocol RFC 2406.

The Proof of Possession payload is used as part of group membership authorization during a GDOI exchange.

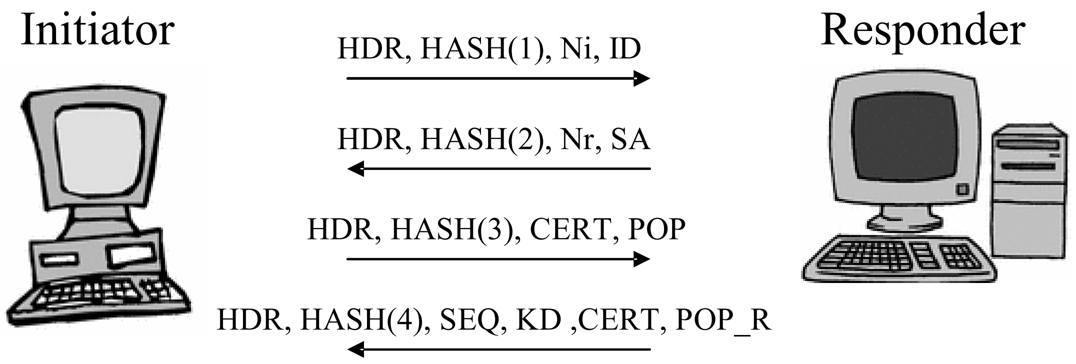
3.3. Phase 2 exchanges

Also there are two phase 2 exchanges: Groupkey-Pull and Groupkey-Push.
Groupkey-Pull is initiated by a group member and downloads keys for a groups "Re-Key" and/or "Data-Security" Security Association. Re-Key includes a KEK common to the group, Data-Security includes a TEK to encrypt or decrypt traffic.
A Groupkey-Push is performed by the GCKS and creates or updates "Re-Keys" or "Data-Security" Security Associations. It is „pushed“ from the GCKS to the members.

3.3.1 Groupkey-Pull

The Groupkey-Pull is used to establish Security Associations at the member for a particular group. It is initiated by a member of a group and therfore has "pull" behavior since the member initiates the retrieval of Security Associations. The Security Associations include authentication keys, encryption keys, cryptographic policies and attributes. There my be multiple Groupkey-Pull exchanges for a given phase 1 Security Association.

The exchange is phase 1 protected. Each transaction has a ISAKMP header (HDR) that uses phase 1 cookies.



To construct the first GDOI message the initiator chooses Ni and creates a nonce payload, builds an identity payload including the group identifier, and generates HASH(1).
The GCKS (responder) passively listens for incoming requests from group members.
The Phase 1 authenticates the group member and sets up the secure session.

Upon receipt of the first GDOI message the GCKS validates HASH(1), extracts the Ni and group identifier in the ID payload. It verifies that it's database contains the group information for the group identifier.

The GCKS constructs the second GDOI message, including a nonce Nr, and the policy for the group in an Security Association payload, followed by SA TEK payloads for traffic Security Associations, and SA KEK policy, if the group controller will be sending Re-key messages to the group. HASH(2) is generated using these values.

Upon receipt of the second GDOI message, the initiator validates HASH(2), extracts the nonce Nr, and interprets the SA payload. If the policy in the SA payload is acceptable (e.g., the security protocol and cryptographic protocols can be supported by the initiator), the initiator continues the protocol. If the group policy uses certificates for authorization, the initiator generates a hash including Ni and Nr and signs it. This becomes the contents of the POP payload. If necessary, a CERT payload is constructed which holds the public key corresponding to the private key used to sign the POP payload.

The initiator constructs the third GDOI message by including the CERT and POP payloads (if needed) and creating HASH(3).

Upon receipt of the third GDOI message the GCKS validates HASH(3). If the initiator sent CERT and POP payloads, the POP signature is validated.

The GCKS constructs the fourth GDOI message, including the SEQ payload, if the GCKS sends rekey messages, the KD payload containing keys corresponding to policies previously sent in the SA TEK and SA KEK payloads, and the CERT and POP payloads.

Upon receipt of the fourth GDOI message, the initiator validates HASH(4). If the responder sent CERT and POP_R payloads, the POP signature is validated. If SEQ payload is present, the sequence number in the SEQ payload must be checked against any previously received sequence number for this group. If it is less than the previously received number, it should be considered stale and ignored. This could happen if two Groupkey-Pull messages happened in parallel, and the sequence number changed between the times the results of two Groupkey-Pull messages were returned from the GCKS.

The initiator interprets the KD key packets. For TEKs, once the keys and policy are matched, the initiator is ready to send or receive packets matching the TEK policy. If policy and keys had been previously received for this TEK policy, the initiator may decide instead to ignore this TEK policy in case it is stale. If this group has a KEK, the KEK policy and keys are marked as ready for use.

3.3.2. Groupkey-Push

The Groupkey-Push control information is sent securely using group communication. Typically it is an IP-multicast distribution, but it can also be "pushed" using unicast. The message replaces a KEK Security Association and/or creates a new Data-Security Association. Logical Key Hierachy (LKH) is supported to provide forward and backward access control. This denies access of removed members to new keys and new members to old keys.

The GCKS may initiate a Rekey message for several reasons: If group membership has changed or keys are due to expire. The GCKS sends an ISAKMP header with the correct cookie pair, a SEQ, Security Association and Key Download Array (KD) payloads. SA_KEK is sent if KEK or group membership has changed, SA_TEK if there are new traffic-encrypting keys. All payloads are encrypted using the current key-encrypting key.

Group members receiving the Groupkey-Push message match the cookie pair of the ISAKMP header to an existing Security Association. Then the form of the datagram sent by the GCKS and the Sequence Number are validated. If they are valid, the receiver processes the Security Association and Key Download Array payloads.

When group membership is altered using a group management algorithm new SA_TEKs and their associated keys are usually also needed. New Security Associations and keys ensure that members who were denied access can no longer participate in the group.

4. Security considerations

4.1. General overview

GDOI is a Security Association management protocol for groups of senders and receivers. It provides the authentication of entities and confidentiality of key management messages. It uses practices against, man-in-the-middle, connection hijacking, replay, reflection and denial-of-service attacks. GDOI assumes that the network is not secure. It assumes that, although the network may be under the complete control of an attacker, the host computer is secure. Also the members are assumed to be trustable.

The security of GDOI is as good as the degree of which the members can be trusted to protect authenticators and keys.

4.2. ISAKMP phase 1

In phase 1, authentication is provided via pre-shared keys or Public Key encryption. GDOI relies on phase 1 Diffie-Hellman exchange to achieve confidentiality. To defend against Man-in-the-Middle attacks, GDOI relies on phase 1 authentication to protect against these attacks. Replay/Reflection attacks are foiled by the phase 1 nonce mechanism and hash-based message authentication.

Denial-of-Service attack protection is achieved by the phase 1 cookie mechanism to indentify spurious messages prior to cryptographic processings. This is a weak form of protection, since a sophisticated attacker can imitate the cookies.

4.3. Groupkey-Pull

Groupkey-Pull is a phase 2 protocol under protection of phase 1. Authentication is not required since phase 1 has previously authenticated the peer. Confidetiality is provided by phase 1 and the POP payload enables authorization.

Message authentication includes a secret only known by the group member and the GCKS, and therefore an attacker would not be able to change messages undetected, which provides Man-in-the-Middle attack protection.

Replay/Reflection attack protection is performed, since implementations of GDOI should keep a record of recently received messages that have already been processed. This enables an early discard of replayed messages.

The group member and GCKS exchange nonce values which are included in subsequent hash payload calculations. Group members and GCKS do not perform any coputationally expensive task before receiving a hash with its own nonce included. Therfore some protection against Denial-of-Service attacks is achieved.

4.4.Groupkey-Push

Groupkey-Push is a single message to all group members.

Authentication is performed, since the message is digitally signed using the private key of the GCKS.

The GCKS encrypts the message with a key that was established in prior Groupkey-Pull exchanges, which provides confidentiality.

Man-in-the-Middle attack protection is achievd through the combination of authentication and confidentiality.

The increasing sequential Number (SEQ) in the messages provides Replay/ Reflection attack protection. A group member would recognize a replayed message by comparing the SEQ to a sliding window. Implementations of GDOI should keep a record of recently received messages that have already been processed. This enables an early discard of replayed messages.

For Denial-of-Service attack protection, again phase 1 techniques are used as a weak form of protection, but the digital signature used for message authentication can amplify denial of service attacks due to the computational expensive cryptographic operations. This price has to be payed becourse with weak cryptographic methods, GCKS impersonations would be possible and thus, GCKS message source authentication be impossible! To handle this issue, least cryptographic methods are performed first and the Sequence Number is checked against the sliding window. This enables early detection of invalid messages.

Since an attacker needs to know at least a weak valid cryptographic key and a valid Sequence Number, generally only a group member can evectiveliy deploy a Denial-

of-Service attack.
In terms of Forward Access Control it is vital, that changes in group membership and in TEKs or KEKs are not performed in one message. To provide complete Forward Access Control, two messages have to be sent, the first changing group membership and the second changing policy and keys.

5. Conlusion

Typical GDOI Applications would be all secure multicast applications including video broadcast and multicast file transfer, and also unicast applications such as Video-on-Demand. For example a Groupkey-Push message may establish a pairwise IPsec Security Association for a member of a subscription group without the need for key management and costly assymmetric cryptography.
Many Real Time Transport Protocol applications need security above the IP layer. A future RTP security protocol may benefit from using GDOI to establish Security Associations.

Appendix

Sources

- RFC3547, The Group Domain of Interpretaion
- Several more or less helpful sources in the World Wide Web...