

The Group Domain of Interpretation

An ISAKMP DOI for secure group communication

Martin Schiele



Agenda

- Introduction
- Recap of ISAKMP
- How GDOI works
- Security considerations
- Conclusion



Introduction

- GDOI
 - is an ISAKMP DOI for group key management
 - manages group security associations which are used by IPSec or other data security protocols running at the IP or application layers
 - protects key-encrypting keys (KEK), traffic-encrypting keys (TEK), or data shared by group members



Recap of ISAKMP

- Internet Security Association and Key Management Protocol
- Negotiates and manages Security Associations between entities
- Provides secure connection between two parties
- There are two Phases:
 - 1st: Entities decide security for following phases
 - 2nd: An exchange which is explained in this presentation



How GDOI works

- Must be protected by a Phase 1 security association established by ISAKMP
- The GDOI protocol is run between a Group member and a Group Controller/Key Server (GCKS)
- The GCKS establishes Security Associations among authorized group members



How GDOI works

- According to ISAKMP there are six new Payloads:
 - GDOI Security Association (GDOI SA)
 - Security Association KEK (SA_KEK)
 - Security Association TEK (SA_TEK)
 - Key Download Array (KD)
 - Sequence Number (SEQ)
 - Proof of Possession (POP)



How GDOI works

- Two Phase 2 exchanges:
 - Groupkey-Pull:
 - 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
 - Groupkey-Push:
 - Creates or updates „Re-Keys“ or „Data-Security“ Security Associations
 - Is „pushed“ from the GCKS to the members



Groupkey-Pull

- Is used to establish Security Associations at the member for a particular group
- The Security Associations include authentication keys, encryption keys, cryptographic policies and attributes
- „Pull“ behavior since the member initiates the retrieval of these Security Associations
- There may be multiple exchanges for a given Phase 1 Security Association



Groupkey-Pull

- Authorization
 - Two alternatives:
 - Phase 1 identity can be used
 - A new identity can be passed in the Groupkey-Pull request:
 - The new identity could be specific to the group and use a certificate that is signed by the group owner
 - The Proof-of-Possession payload validates that the holder possesses the secret key



Groupkey-Pull

Phase 1 protected: each transaction contains an ISAKMP header that uses Phase 1 cookies

Nonce payload, identity payload



Validates that the database contains group information for that identifier

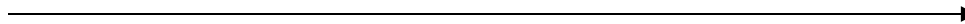
Initiator (Member)

SA KEK, SA TEK payloads



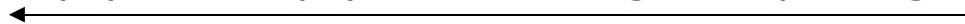
Interprets the SA. If the policies are acceptable (cryptographic protocols are supported) the protocol is continued

POP payload constructed according to SAs



Validates POP signature

SEQ payload, KD payload containing corresponding Keys





Groupkey-Push

- Control information sent securely using group communication
- Typically IP-multicast distribution, but can also be „pushed“ using unicast
- 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
 - Denies access of removed members to new keys and new members to old keys



Groupkey-Push

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



Groupkey-Push

- Group members receiving the Groupkey-Push message:
 - match the cookie pair of the ISAKMP header to an existing SA
 - validate the form of the datagram
 - validate the SEQ
 - process the Security Association and Key Download Array payloads



How GDOI works

- To handle Groupkey-Pull and Groupkey-Push in detail, knowledge of “bitlevel stuff” is necessary!
- All the Payloads are exactly described in RFC 3547



Security Considerations

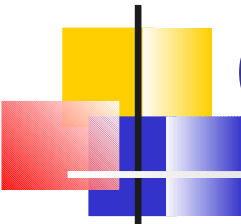
- GDOI is a Security Association management protocol for groups of senders and receivers
- It provides:
 - authentication of entities
 - confidentiality of key management messages
- Uses practices against, man-in-the-middle, connection hijacking, replay, reflection and denial-of-service attacks
- GDOI assumes that:
 - the network is not secure
 - the host computer is secure
 - the members can be trusted
- The security of GDOI is as good as the degree of which the members can be trusted to protect authenticators and keys

Security Considerations, ISAKMP Phase 1

- Authentication
 - Provided via pre-shared Keys or Public Key encryption
- Confidentiality
 - GDOI relies on Phase 1 Diffie-Hellman exchange to achieve confidentiality
- Man-in-the-Middle attack protection
 - If successful it would foil entity authentication of one or more entities during key establishment
 - GDOI relies on Phase 1 authentication to protect against these attacks

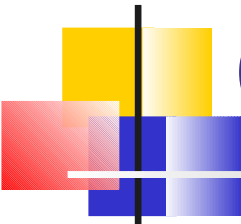
Security Considerations, ISAKMP Phase 1

- Replay/Reflection attack protection
 - If successful the attacker gains information from subsequent messages
 - GDOI relies on Phase 1 nonce mechanism a hash-based message authentication
- Denial-of-Service protection
 - Attacker sends messages to GDOI entities to cause unneeded message authentication operations
 - GDOI relies on 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



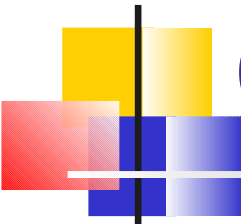
Security Considerations, Groupkey-Pull

- Is a Phase 2 protocol under protection of Phase 1
- Authentication is not required since Phase 1 has previously authenticated the peer
- Confidentiality is provided by Phase 1
- Authorization
 - The POP payload enables authorization



Security Considerations, Groupkey-Pull

- Man-in-the-Middle attack protection
 - Message authentication includes a secret only known by the group member and the GCKS
 - Therefore an attacker would not be able to change messages undetected
- Replay/Reflection attack protection
 - Implementations should keep a record of recently received messages that have already been processed
 - This enables an early discard of replayed messages
- Denial-of-Service attack protection
 - The group member and GCKS exchange nonce values which are included in subsequent hash payload calculations
 - Group members and GCKS do not perform any computationally expensive task before receiving a hash with its own nonce included



Security Considerations, Groupkey-Push

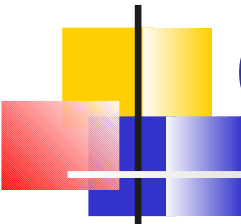
- Is a single message to all group members
- Authentication
 - The message is digitally signed using the private key of the GCKS
- Confidentiality
 - The GCKS encrypts the message with a key that was established in prior Groupkey-Pull exchanges

Security Considerations, Groupkey-Push

- Man-in-the-Middle attack protection
 - The combination of authentication and confidentiality prevents Man-in-the-Middle attacks
- Replay/Reflection attack protection
 - The message has an increasing sequential number (SEQ)
 - A group member would recognize a replayed message by comparing the SEQ to a sliding Window
 - Implementations should keep a record of recently received messages that have already been processed
 - This enables an early discard of replayed messages

Security Considerations, Groupkey-Push

- Denial-of-Service attack protection
 - Phase 1 techniques are used as a weak form of protection
 - 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 becouse with weak cryptographic methods GCKS impersonations would be possible and thus GCKS message source authentication be impossible
 - Least cryptographic methods are performed first
 - The sequence number is checked against the sliding window
 - Generally only a group member can evectivelyly deploy a denial of service attack



Security Considerations, Groupkey-Push

- Forward Access Control
 - If changes in group membership and in TEKs or KEKs are performed in one message, Forward Access Control is not ensured
 - To provide complete Forward Access Control two messages have to be sent, the first changing the group membership, the second changing the policies



Conclusion

- GDOI Applications
 - All secure multicast applications including video broadcast and multicast file transfer
 - 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 asymmetric 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



Sources

- RFC 3547: The Group Domain of Interpretation
- The depth of the World Wide Web



End of Presentation

Thank you for your Attention