GDOI Update
Draft -07

Brian Weis

What Happened?

- Draft -06 completed WG last call prior to Maastricht
  - We discussed updates in Maastricht
  - The chairs were not satisfied that there were enough comments & asked for more
  - Mark Baugher provided a thoughtful review
- Draft -07 was published in October
  - Vincent recently provided some additional comments
  - One practical issue has arisen with SENDER_ID allocation

Summary of changes between draft -06 and draft -07

- Lots of miscellaneous clarification
  - More key terms added
  - Use cases clarified
- A few substantive issues we'll discuss

Authorization

- Section 3.1: “SHOULD” changed to “MUST”:

  “A group member MUST ensure that the Phase 1 identity of the GCKS is an authorized GCKS.”

Rekey signing key

- In Maastricht we had a discussion about the scope of a signing key.

  “A signing key should not be used in more than one context (e.g., used for host authentication and also for message authentication).”

Clarifying LKH Semantics

- GDOI does not include a detailed description of LKH semantics
  - Only that which is necessary for interoperability (e.g., packet formats)
  - GM processing of the key arrays
- Added reference [HD03], which describes generic LKH semantics
  - "*Multicast and Group Security*" by Hardjono and Dondeti.

Counter Mode Keying Material

- Explicitly stated that the keying material downloaded for a TEK might include more than the session key.

  "When an algorithm specification specifies the format of the keying material, the value transported in the KD payload for that key is passed according to that specification. The keying material may contain information besides a key. For example, The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP) [RFC4106] defines a salt value as part of KEYMAT."

New issues

- Vincent's email to the list
  - Security Considerations
  - Backwards Access Control
  - Aborting an exchange
- Practical issue
  - SENDER_ID value distribution

Security Considerations
Trust Levels

Section 7: "The security of GDOI, therefore, is as good as the degree to which group members can be trusted..."

- Comment: “I'd like to know what could happen if one of the GM is compromised.”
  - DoS
  - Can spoof sender traffic

Security Considerations
GROUPKEY_PULL

Section 7.2.4 (Replay/Reflection Attack Protection)

- Comment 1: Freshness method described here is not a replay protection method.
  - Will consider what to do with this text
- Comment 2: “Keeping a record of recently received GROUPKEY-PULL messages is a limited approach.
  - This is within the context of a single IKE phase 1 session
  - IKE Phase 1 protocol is expected to be short lived, so there’s only 4 valid messages to record
  - IKEv1 implementations often use a hash of the message as an “early discard” mechanism

Section 7.2.5 (Denial of Service Protection)

- Comment: Are above methods really sufficient for DoS too, as stated?
  - That’s all that is available in an IKEv1 framework

Security Considerations GROUPKEY_PUSH

Section 7.3.4 (Replay/Reflection Attack Protection for the GROUPKEY_PUSH exchange)

- Comment: Isn't The SEQ mechanism sufficient for detecting replays?
  - Yes, text suggesting keeping track of keep a record of recently received messages can be removed.

Section 7.3.5 (Denial of Service Protection)

- Comment: Rate limiting messages is another good technique
  - OK, we can mention that

Backwards Access Control

Section 1.5.1 describes a method to maintain forward access control (removing the ability for de-authorized GM to see future traffic)

- Question: Why not the same for backwards access control (preventing a new GM from seeing old traffic)?
  - Not seen as a practical requirement, but could be added
  - Synchronization of new keying material between new GM and old GMs is tricky. We can document this though.

Aborting an exchange

- Question: What does a GM do if it does not accept the policy pushed to it?
  - Aborts the protocol. This may result in a KS retransmitting messages until it times out the session
  - GM could send Informational exchange with a Delete payload

SENDER_ID value distribution

- In draft -07 KS allocates a single SENDER_ID value at a time to a GM
  - It can be advantageous to give some GMs two or more SENDER_ID values at a time
    - Higher bandwidth GMs
    - GMs with per-interface SADBs
- The KS is able to deliver multiple SENDER_ID values during registration.
  - But how does the KS know that it should do so??

SENDER_ID value distribution

- Only clean solution is for the GM to *request* multiple SENDER_IDs
  - Requires a new payload (e.g., Notify) to GDOI message 1:

    HDR*, HASH(1), Ni, ID, [N(# SENDER_IDS)]
  - This is a significant change to the message

    Do we need to bump up the minor version #?

    Current text: “Major Version is 1 and Minor Version is 0”

SENDER_ID value distribution

- Can this be cleanly handled by implementations?

  HDR*, HASH(1), Ni, ID, [N(# SENDER_IDS)]

  HASH(1) = prf(SKEYID_a, M-ID | Ni | ID | [N])

- Or is this such a significant change that we need to bump up the ISAKMP HDR minor version #?

Next Steps

- Authors need to resolve the new issues
- Hold a short Working Group Last Call for the new version?