Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 6, 2009

M. Behringer
F. Le Faucheur
Cisco Systems Inc
June 4, 2009

Applicability of Keying Methods for RSVP Security
draft-ietf-tsvwg-rsvp-security-groupkeying-05.txt

Status of this Memo

Copyright Notice

Abstract

The Resource reSerVation Protocol (RSVP) allows hop-by-hop authentication of RSVP neighbors. This requires messages to be cryptographically protected using a shared secret between participating

Stephen Kent 11/30/09 9:36 PM
Comment: Shared secrets generally are not used for signatures. These messages require authentication and integrity security services, but not digital signatures per se.

Stephen Kent 11/30/09 9:35 PM
Deleted: signed

nodes. This document compares group keying for RSVP with per-neighbor or per-interface keying, and discusses the associated key provisioning methods as well as applicability and limitations of these approaches. The document also discusses applicability of group keying to RSVP encryption.

Stephen Kent 11/30/09 9:36 PM
Deleted:

Stephen Kent 11/30/09 9:36 PM
Deleted: present

Table of Contents

1. Introduction and Problem Statement

The Resource reSerVation Protocol [RFC2205] allows hop-by-hop authentication of RSVP neighbors, as specified in [RFC2747]. In this mode, an integrity object is attached to each RSVP message to transmit a keyed message digest. This message digest allows the recipient to verify the identity of the RSVP node that sent the message, and to validate the integrity of the message. Through the inclusion of a sequence number in the scope of the digest, the digest also offers replay protection.

[RFC2747] does not dictate how the key for the integrity operation is derived. Currently, most implementations of RSVP use a statically configured key, per interface or per neighbor. However, to manually configure a key per router pair across an entire network is operationally hard, especially when key changes are to be performed on a regular basis. Effectively, many users of RSVP therefore resort to using the same key throughout their RSVP network, and they change it rarely if ever, because of the operational burden. [RFC3562] however recommends regular key changes, at least every 90 days.

This document discusses a variety of keying methods and their applicability to different RSVP deployment environments, for both message integrity and encryption. It does not recommend any particular method or protocol (e.g., RSVP authentication versus IPsec AH), but is meant as a comparative guide to understand where each RSVP keying method is best deployed, and its limitations. Furthermore, it discusses how RSVP hop by hop authentication is impacted in the presence of non-RSVP nodes, or subverted nodes, in the reservation path.

The document "RSVP Security Properties" ([RFC4230]) provides an overview of RSVP security, including RSVP Cryptographic Authentication [RFC2747], but does not discuss key management. It states that "RFC 2205 assumes that security associations are already available". The present document focuses specifically on key management with different key types, including group keys. Therefore this document complements [RFC4230].

2. The RSVP Hop-by-Hop Trust Model

Many protocol security mechanisms used in networks require and use per peer authentication. Each hop authenticates its neighbor with a shared key or certificate. This is also the model used for RSVP. Trust in this model is transitive. Each RSVP node trusts explicitly only its RSVP next hop peers, through the message digest contained in the INTEGRITY object. The next hop RSVP speaker in turn trusts its

Stephen Kent 11/30/09 2:29 PM
Deleted: authenticity

Stephen Kent 11/30/09 2:30 PM
Deleted: for

Stephen Kent 11/30/09 9:42 PM
Comment: This RFC deals with a different protocol, so the recommended key change interval is not necessarily applicable here, especially for a multicast security association.

Stephen Kent 11/30/09 9:42 PM
Deleted: e

Stephen Kent 11/30/09 9:42 PM
Deleted: present

Stephen Kent 11/30/09 2:32 PM
Deleted: the various

Stephen Kent 11/30/09 2:32 PM
Comment: Why is encryption mentioned here? All of the prior discussion focused on integrity and authentication.

Stephen Kent 11/30/09 9:43 PM
Comment: That's not true. In later sections of this document IPsec is, for the most part, rejected and the RSVP INTEGRITY object is recommended.

Stephen Kent 11/30/09 2:32 PM
Deleted: line

own peers and so on. See also the document "RSVP security properties" [RFC4230] for more background.

The keys used for protecting RSVP messages can, in particular, be group keys (for example distributed via GDOI [RFC3547], as discussed in [I-D.weis-gdoi-mac-tek]). If a group key is used, the authentication granularity becomes group membership, not (individual) peer authentication.

Stephen Kent 11/30/09 2:34 PM
Deleted: generating

Stephen Kent 11/30/09 2:34 PM
Deleted: the

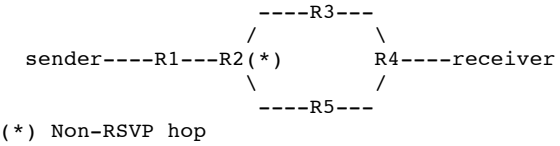
The trust an RSVP node has to another RSVP node has an explicit and an implicit component. Explicitly the node trusts the other node to maintain the RSVP messages intact or confidential, depending on whether authentication or encryption (or both) are used. This means only that the message has not been altered or seen by another, non-trusted node. Implicitly each node trusts each other node with which it has a trust relationship established via the mechanisms here to adhere to the protocol specifications laid out by the various standards. Note that in any group keying scheme like GDOI a node trusts all the other members of the group (because the authentication is now group membership, as noted above).

Stephen Kent 11/30/09 2:36 PM
Deleted: is

The RSVP protocol can operate in the presence of a non-RSVP router in the path from the sender to the receiver. The non-RSVP hop will ignore the RSVP message and just pass it along. The next RSVP node can then process the RSVP message. For RSVP authentication or encryption to work in this case, the key used for computing the RSVP message digest needs to be shared by the two RSVP neighbors, even if they are not IP neighbors. However, in the presence of non-RSVP hops, while an RSVP node always knows the next IP hop before forwarding an RSVP Message, it does not always know the RSVP next hop. In fact, part of the role of a Path message is precisely to discover the RSVP next hop (and to dynamically re-discover it when it changes, for example because of a routing change). Thus, the presence of non-RSVP hops impacts operation of RSVP authentication or encryption and may influence the selection of keying approaches.

Stephen Kent 11/30/09 9:54 PM
Comment: Both 2747 and 4230 discuss the use of a handshake to recover from a crash or a restart. Doesn't this handshake allows a sender to determine the identity of the receiver in situations when one or more non-RSVP routers appear along the path?

Figure 1 illustrates this scenario. R2 in this picture does not participate in RSVP, the other nodes do. In this case, R2 will pass on any RSVP messages unchanged, and will ignore them.



(*) Non-RSVP hop

Figure 1: A non-RSVP Node in the path

This creates a challenge for RSVP authentication and encryption. In the presence of a non-RSVP hop, with some RSVP messages such as a

PATH message, an RSVP router does not know the RSVP next hop for that message at the time of forwarding it. For example, in Figure 1, R1 knows that the next IP hop for a Path message addressed to the receiver is R2, but it does necessarily not know if the RSVP next hop is R3 or R5.

This means that per interface and per neighbor keys cannot easily be used in the presence of non-RSVP routers on the path between senders and receivers.

By contrast, group keying will naturally work in the presence of non-RSVP routers. Referring back to Figure 1, with group keying, R1 would use the group key to protect a Path message addressed to the receiver and forwards it to R2. Being a non-RSVP node, R2 will ignore and forward the Path message to R3 or R5 depending on the current shortest path as determined by routing. Whether it is R3 or R5, the RSVP router that receives the Path message will be able to authenticate it successfully using the group key.

3. Applicability of Key Types for RSVP

3.1. Interface-based and neighbor-based keys

Most current RSVP authentication implementations support interface-based RSVP keys. When the interface is point-to-point (and therefore an RSVP router has only a single RSVP neighbor on each interface), this is equivalent to neighbor-based keys in the sense that a different key is used for each neighbor. However, when the interface is multipoint, all RSVP speakers on a given subnet have to share the same key in this model, which makes it unsuitable for deployment scenarios where different trust groups share a subnet, for example Internet exchange points. In such cases, neighbor-based keys are required.

With neighbor-based keys, each RSVP key is bound to an interface plus a neighbor on that interface. It allows for the existence of different trust groups on a single interface and subnet. (This assumes that layer-2 security is correctly implemented to prevent layer-2 attacks.)

Per-interface and per-neighbor keys can be used within a single security domain. As mentioned above, per-interface keys are only applicable when all the nodes reachable on the specific interface belong to the same security domain.

These key types can also be used between security domains, since they are specific to a particular interface or neighbor. Again, interface

Stephen Kent 11/30/09 9:55 PM
Comment: Discuss how this problem does or does not interact with the use of sequence numbers for anti-replay.

Stephen Kent 11/30/09 2:40 PM
Comment: Note that this is a result of choosing to use symmetric keying for authentication. If public-key techniques were employed, this would not be a problem, i.e., a message could be signed without knowledge of the identity of the next RSVP hop.

Stephen Kent 11/30/09 2:40 PM
Deleted: sign

Stephen Kent 11/30/09 2:40 PM
Deleted: with

Stephen Kent 11/30/09 2:46 PM
Comment: Why use these terms at the beginning of the section, then switch to per-interface and per-neighbor later?

Stephen Kent 11/30/09 2:40 PM
Deleted:

Stephen Kent 11/30/09 2:41 PM
Deleted: only

Stephen Kent 11/30/09 2:41 PM
Deleted:

Stephen Kent 11/30/09 2:41 PM
Comment: Define a "trust group"

Stephen Kent 11/30/09 9:56 PM
Deleted: a

Stephen Kent 11/30/09 2:42 PM
Deleted:

Stephen Kent 11/30/09 2:42 PM
Deleted:

Stephen Kent 11/30/09 2:42 PM
Deleted: an

Stephen Kent 11/30/09 2:43 PM
Deleted: distinction

Stephen Kent 11/30/09 2:43 PM
Deleted: Assuming

Stephen Kent 11/30/09 2:44 PM
Comment: What layer 2 security is needed. It's not clear from this sentence.

Stephen Kent 11/30/09 2:44 PM
Deleted:

Stephen Kent 11/30/09 2:44 PM
Deleted:

Stephen Kent 11/30/09 2:44 PM
Comment: Is a security domain the same as a trust group? Define this term.

Stephen Kent 11/30/09 2:44 PM
Deleted:

Stephen Kent 11/30/09 2:45 PM
Comment: Trust group?

level keys can be deployed safely only when all the reachable neighbors on the interface belong to the same security domain.

As discussed in the previous section, per-neighbor and per-interface keys can not be used in the presence of non-RSVP hops.

3.2. Group keys

In the case of group keys, all members of a group of RSVP nodes share the same key. This implies that a node uses the same key regardless of the next RSVP hop that will process the message (within the group of nodes sharing the particular key). It also implies that a node will use the same key on the receiving as on the sending side (when exchanging RSVP messages within the group).

Group keys apply naturally to intra-domain RSVP authentication, since all RSVP nodes implicitly trust each other. Using group keys, they extend this trust to the group key server. This is represented in Figure 2.

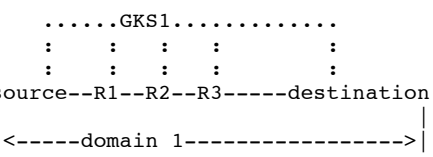


Figure 2: Group Key Server within a single security domain

A single group key cannot normally be used to cover multiple security domains, because by definition the different domains do not trust each other. They would therefore not be willing to trust the same group key server. For a single group key to be used in several security domains, there is a need for a single group key server, which is trusted by both sides. While this is theoretically possible, in practice it is unlikely that there is a single such entity trusted by both domains. Figure 3 illustrates this setup.

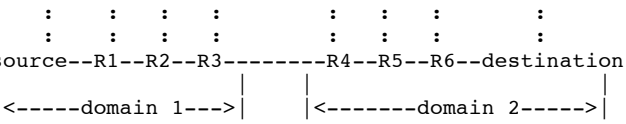


Figure 3: A Single Group Key Server across security domains

A more practical approach for RSVP operation across security domains,

Stephen Kent 11/30/09 2:45 PM
Deleted: only

Stephen Kent 11/30/09 2:45 PM
Comment: Trust group?

Stephen Kent 11/30/09 2:46 PM
Deleted:

Stephen Kent 11/30/09 2:46 PM
Deleted:

Stephen Kent 11/30/09 2:47 PM
Deleted: Here

Stephen Kent 11/30/09 2:47 PM
Comment: Are members of the same trust group?

Stephen Kent 11/30/09 2:48 PM
Comment: Trust domains?

is to use a separate group key server for each security domain, and to use per-interface or per-neighbor keys between the two domains. Figure 4 shows this setup.

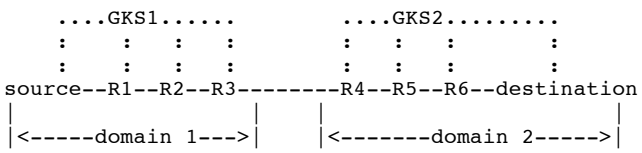


Figure 4: A group Key Server per security domain

As discussed in Section 2, group keying can be used in the presence of non-RSVP hops.

4. Key Provisioning Methods for RSVP

4.1. Static Key Provisioning

The simplest way to implement RSVP authentication is to use static, preconfigured keys. Static keying can be used with interface-based keys, neighbor-based keys or group keys.

However, such static key provisioning is expensive on the operational side, since no secure automated mechanism can be used, and initial provisioning as well as key updates require configuration. This method is therefore mostly useful for small deployments, where key changes can be carried out manually, or for deployments with automated configuration tools that support key changes.

Static key provisioning is therefore not an ideal model in a large network.

Often, the number of interconnection points across two domains where RSVP is allowed to transit is relatively small and well controlled. Also, the different domains may not be in a position to use an infrastructure trusted by both domains to update keys on both sides. Thus, manually configured keys may be applicable to inter-domain RSVP authentication.

Since it is not feasible to carry out a key change at the exact same time in communicating RSVP nodes, some grace period needs to be implemented during which an RSVP node will accept both the old and the new key. Otherwise, RSVP operation would suffer interruptions. (Note that also with dynamic keying approaches there can be a grace period where two keys are valid at the same time; however, the grace period in

Stephen Kent 11/30/09 2:49 PM
Deleted:

Stephen Kent 11/30/09 2:49 PM
Deleted:

Stephen Kent 11/30/09 2:49 PM
Deleted: authentication

Stephen Kent 11/30/09 2:49 PM
Deleted: -

Stephen Kent 11/30/09 2:49 PM
Deleted: s

Stephen Kent 11/30/09 9:59 PM
Comment: Manual is probably the preferred term here, but I any case you need to define the term first.

Stephen Kent 11/30/09 2:50 PM
Deleted:

Stephen Kent 11/30/09 2:50 PM
Deleted:

Stephen Kent 11/30/09 10:00 PM
Comment: You should define what you mean by static key provisioning

Stephen Kent 11/30/09 2:51 PM
Comment: Used to do what?

Stephen Kent 11/30/09 10:00 PM
Comment: What sort of configuration problems arise here?

Stephen Kent 11/30/09 2:53 PM
Comment: The preceding sentence said there were no such tools!

Stephen Kent 11/30/09 2:52 PM
Deleted: which

Stephen Kent 11/30/09 2:53 PM
Comment: Security or trust?

Stephen Kent 11/30/09 2:55 PM
Comment: Is “manually configured” the same as “static” ? the former is a clearer term and I suggest you use it instead of static, if you view them as equivalent terms.

Stephen Kent 11/30/09 2:55 PM
Deleted: the

Stephen Kent 11/30/09 2:55 PM
Deleted: on

Stephen Kent 11/30/09 2:55 PM
Deleted: both

Stephen Kent 11/30/09 2:55 PM
Deleted: sides

manual keying tends to be significantly longer than with dynamic key rollover schemes.)

4.2. Dynamic Keying

4.2.1. Neighbor-based and Interface-Based Key Negotiation

To avoid the problem of manual key provisioning and updates in static key deployments, key negotiation between RSVP neighbors could be used to derive either interface-based or neighbor-based keys. However, existing key negotiation protocols such as IKEv1 [RFC2409] or IKEv2 [RFC4306] may not be appropriate in all environments because of the relative complexity of the protocols and related operations.

4.2.2. Dynamic Group Key Distribution

With this approach, group keys are dynamically distributed among a set of RSVP routers. For example, [I-D.weis-gdoi-mac-tek] describes a mechanism to distribute group keys to a group of RSVP speakers, using GDOI [RFC3547]. In this solution, a key server authenticates each of the RSVP nodes independently, and then distributes a group key to the entire group.

5. Specific Cases Supporting use of Group Keying

5.1. RSVP Notify Messages

[RFC3473] introduces the Notify message and allows such messages to be sent in a non-hop-by-hop fashion. As discussed in the Security Considerations section of [RFC3473], this can interfere with RSVP's hop-by-hop integrity and authentication model. [RFC3473] describes how standard IPsec based integrity and authentication can be used to protect Notify messages. We observe that, alternatively, in some environments, group keying may allow use of regular RSVP authentication ([RFC2747]) for protection of non-hop-by-hop Notify messages. For example, this may be applicable to controlled environments where nodes invoking notification requests are known to belong to the same key group as nodes generating Notify messages.

5.2. RSVP-TE and GMPLS

Use of RSVP authentication for RSVP-TE [RFC3209] and for RSVP-TE Fast Reroute [RFC4090] deserves additional considerations.

With the facility backup method of Fast Reroute, a backup tunnel from the Point of Local Repair (PLR) to the Merge Point (MP) is used to protect Label Switched Paths (protected LSPs) against the failure of

Stephen Kent 11/30/09 10:02 PM
Comment: This is a very vague criticism. You need to be more specific in dismissing these protocols. Also, what about the TLS handshake for key negotiation, which has recently been adopted for key management with SRTP?

Stephen Kent 11/30/09 10:04 PM
Comment: And is this authentication based on initial, manual provisioning of keys? If so, then it has some of the same problems you ascribed to other key management methods above. If not, explain how the group key server authenticates the group members and distributes the group key to them. This description of GDOI sweeps these issues under the rug!

Stephen Kent 11/30/09 2:58 PM
Comment: And this is much less complex because???

Stephen Kent 11/30/09 3:00 PM
Deleted: Notify

Stephen Kent 11/30/09 3:01 PM
Comment: If this section assumes use of group keying it should say so up front. Otherwise this last sentence seems out of place.

Stephen Kent 11/30/09 3:02 PM
Comment: This one example is pretty minimal. A more generic description of the circumstances where this is true is needed.

a facility (e.g., a router) located between the PLR and the MP. During the failure of the facility, the PLR redirects a protected LSP inside the backup tunnel and as a result, the PLR and MP then need to exchange RSVP control messages between each other (e.g., for the maintenance of the protected LSP). Some of the RSVP messages between the PLR and MP are sent over the backup tunnel (e.g., a Path message from PLR to MP) while some are directly addressed to the RSVP node (e.g., a Resv message from MP to PLR). During the rerouted period, the PLR and the MP effectively become RSVP neighbors, while they may not be directly connected to each other and thus do not behave as RSVP neighbors in the absence of failure. This point is raised in the Security Considerations section of [RFC4090] that says: "Note that the facility backup method requires that a PLR and its selected merge point trust RSVP messages received from each other." We observe that such environments may benefit from group keying. A group key can be used among a set of routers enabled for Fast Reroute thereby easily ensuring that PLR and MP authenticate messages from each other can be authenticated, without requiring prior specific configuration of keys, or activation of key update mechanism, for every possible pair of PLR and MP.

Where RSVP-TE or RSVP-TE Fast Reroute is deployed across AS boundaries (see [RFC4216]), the considerations presented above in section 3.1 and 3.2 apply, such that per-interface or per-neighbor keys can be used between two RSVP neighbors in different ASes (independently of the keying method used by the RSVP router to talk to the RSVP routers in the same AS).

[RFC4875] specifies protocol extensions for support of Point-to-Multipoint (P2MP) RSVP-TE. In its Security Considerations section, [RFC4875] points out that RSVP message integrity mechanisms for hop-by-hop RSVP signaling apply to the hop-by-hop P2MP RSVP-TE signaling. In turn, we observe that the analyses in this document of keying methods apply equally to P2MP RSVP-TE for the hop-by-hop signaling.

[RFC4206] defines LSP Hierarchy with GMPLS TE and uses non-hop-by-hop signaling. Because it reuses LSP Hierarchy procedures for some of its operations, P2MP RSVP-TE also uses non-hop-by-hop signaling. Both LSP hierarchy and P2MP RSVP-TE rely on the security mechanisms defined in [RFC3473] and [RFC4206] for non hop-by-hop RSVP-TE signaling. We note that the observation in Section 3.1 of this document about use of group keying for protection of non-hop-by-hop messages apply to protection of non-hop-by-hop signaling for LSP Hierarchy and P2MP RSVP- TE.

Stephen Kent 11/30/09 3:04 PM
Deleted: :

Stephen Kent 11/30/09 3:05 PM
Deleted: a

Stephen Kent 11/30/09 3:04 PM
Deleted: a

Stephen Kent 11/30/09 3:04 PM
Comment: There are a lot of instances of "e.g." in this paragraph. Are they all examples, or should some of them be "i.e."?

Stephen Kent 11/30/09 3:06 PM
Deleted:

Stephen Kent 11/30/09 3:06 PM
Deleted:

Stephen Kent 11/30/09 3:07 PM
Deleted: s

Stephen Kent 11/30/09 3:07 PM
Deleted: c

Stephen Kent 11/30/09 3:07 PM
Deleted: considerations

Stephen Kent 11/30/09 3:07 PM
Deleted: on

Stephen Kent 11/30/09 3:08 PM
Deleted: s

6. Applicability of IPsec for RSVP

6.1. General Considerations Using IPsec

The discussions about the various keying methods in this document are also applicable when using IPsec to protect RSVP. Note that [RFC2747] states in section 1.2 that IPsec is not an optimal choice to protect RSVP. The key argument is that an IPsec SA and an RSVP SA are not based on the same parameters. However, when using group keying, IPsec can be used to protect RSVP. The potential issues and solutions using group keying are:

- [RFC2747] specifies in Section 4.2, bullet 3, that both the key identifier and the sending system address are used to uniquely determine the key. In a group keying scenario it would be necessary to either store a list of senders to do this, or to not use the sending system address to determine the key. Both methods are valid, and one of the two approaches must be chosen. The pros and cons are beyond the scope of this document.
- Anti-replay protection in a group keying scenario requires some changes to the way [RFC2747] defines anti-replay. Possible solutions are discussed in detail in [I-D.weis-gdoi-mac-tek]). For example, when using counter-based methods with various senders in a single SA, the same counter may be received more than once, this conflicts with [RFC2747], which states that each counter value may be accepted only once. Time based approaches are a solution for group keying scenarios.

The document "The Multicast Group Security Architecture" [RFC3740] defines in detail a "Group Security Association" (GSA). This definition is also applicable in the context discussed here, and allows the use of IPsec for RSVP. The existing GDOI standard [RFC3547] contains all relevant policy options to secure RSVP with IPsec, and no extensions are necessary. An example GDOI policy would be to encrypt all packets of the RSVP protocol itself (IP protocol 46). A router implementing GDOI and IPsec protocols is therefore able to implement RSVP encryption.

6.2. Using ESP

In both tunnel mode and transport mode, ESP does not protect the header (in tunnel mode the outer header). This is an issue with group keying when using ESP to secure RSVP packets: the packet header could be modified by a man-in-the-middle attack, replacing the destination address with another RSVP router in the network. This router will receive the packet, use the group key to decrypt the encapsulated packet, and then act on the RSVP packet. This way an attacker cannot create new reservations or affect existing ones, but

Stephen Kent 11/30/09 3:09 PM
Deleted: s

Stephen Kent 11/30/09 3:10 PM
Comment: Since this section purports to talk, about IPsec, I would expect to see references to RFC 4301 and its discussion of how SAs are identified in a multicast environment.

Stephen Kent 11/30/09 3:11 PM
Comment: MUST?

Stephen Kent 11/30/09 3:11 PM
Deleted: only

Stephen Kent 11/30/09 10:12 PM
Comment: This statement seems to conflict with the assertion in 6.2 that ESP is has a vulnerability when used with group keying in the RSVP environment. RFC 3547 describes a key management protocol for use with ESP, not AH, so the comment about this RFC specifying all the "policy options to secure RSVP with IPsec" is misleading at best.

Stephen Kent 11/30/09 3:15 PM
Comment: Are you discussing use of IPsec, or of just the AH or ESP protocols? IPsec is defined in RFC 4301 and it requires defining an IPsec boundary, use of the SDP and SAD, etc.

Stephen Kent 11/30/09 3:13 PM
Comment: Why is encryption cited here, when almost everywhere else only integrity and authentication are discussed?

Stephen Kent 11/30/09 3:15 PM
Deleted: IPsec

Stephen Kent 11/30/09 3:15 PM
Deleted: the

Stephen Kent 11/30/09 3:18 PM
Comment: Decrypt? Are you ruling out use of ESP-NULL? Also, the recipient of a tunneled packet checks the inner header against the SAD cache (RFC 4301) so this attack would not work.

Stephen Kent 11/30/09 10:16 PM
Comment: What info from the packet does the receiver use to determine the source? If the packet were protected using ESP in tunnel mode, normal IPsec processing calls for the receiver to discard the outer header and pay attention to only the inner header. A MITM could not modify that header undetectably.

he can "re-direct" reservations to parts of the network off the actual reservation path, thereby potentially denying resources to other applications on that part of the network.

6.3. Using AH

The INTEGRITY object defined by [RFC2747] provides integrity protection for RSVP also in a group keying context, as discussed above. AH [RFC4302] is an alternative method to provide integrity protection for RSVP packets.

The RSVP INTEGRITY object protects the entire RSVP message, but does not protect the IP header of the packet nor the IP options (in IPv4) or extension headers (in IPv6).

AH tunnel mode (transport mode is not applicable, see section 6.5) protects the entire original IP packet, including the IP header of the original IP packet ("inner header"), IP options or extension headers, plus the entire RSVP packet. It also protects the immutable fields of the outer header.

The difference between the two schemes in terms of covered fields is therefore whether the IP header and IP options or extension headers of the original IP packet are protected (as is the case with AH) or not (as is the case with the INTEGRITY object). Also, AH covers the immutable fields of the outer header.

As described in the next section, IPsec tunnel mode can not be applied for RSVP traffic in the presence of non-RSVP nodes; therefore the security associations in both cases, AH and INTEGRITY object, are between the same RSVP neighbors. From a keying point of view both approaches are therefore comparable. This document focuses on keying approaches only; a general security comparison of these approaches is outside the scope of this document.

6.4. Applicability of Tunnel Mode

IPsec tunnel mode encapsulates the original packet, prepending a new IP header plus an ESP or AH sub-header. The entire original packet plus the ESP/AH sub-header is secured. In the case of ESP the new, outer IP header however is not cryptographically secured in this process. This leads to the problem described in Section 6.2. AH tunnel mode also secures the outer header, and is therefore not subject to these man-in-the-middle attacks.

Protecting RSVP packets with IPsec tunnel mode works with any of the above described keying methods (interface, neighbor or group based), as long as there are no non-RSVP nodes on the path. Note that for

Stephen Kent 11/30/09 3:15 PM
Deleted: IPsec

Stephen Kent 11/30/09 3:18 PM
Deleted: IPsec

Stephen Kent 11/30/09 3:18 PM
Deleted:

Stephen Kent 11/30/09 3:18 PM
Deleted: IPsec

Stephen Kent 11/30/09 10:13 PM
Deleted: appliable

Stephen Kent 11/30/09 3:19 PM
Deleted: IPsec

Stephen Kent 11/30/09 3:21 PM
Comment: If general security considerations are outside the scope, why did you spend so much text in 6.3 discussing them? Most of the text here discussed what AH protects vs. what the RSVP INTEGRITY object protects.

Stephen Kent 11/30/09 3:21 PM
Deleted: tunnel

Stephen Kent 11/30/09 3:22 PM
Comment: But, as I noted in a comment above, that analysis was flawed.

RSVP messages to be visible and considered at each hop, such a tunnel would not cross routers, but each RSVP node would establish a tunnel with each of its peers, effectively leading to link protection.

In the presence of a non-RSVP hop, tunnel mode cannot be applied, because a router upstream from a non-RSVP hop does not know the next RSVP hop, and can thus not apply the correct tunnel header. This is independent of the key type used.

Stephen Kent 11/30/09 3:24 PM
Deleted:

Stephen Kent 11/30/09 10:19 PM
Comment: If the sender knows what destination address to apply in transport mode, then why not apply the same destination address as the outer header? You need to explain this issue in more detail to make it clear to readers.

6.5. Applicability of Transport Mode

IPsec transport mode, as defined in [RFC4303] is not suitable for securing RSVP Path messages, since those messages preserve the original source and destination. [RFC4303] states explicitly that "the use of transport mode by an intermediate system (e.g., a security gateway) is permitted only when applied to packets whose source address (for outbound packets) or destination address (for inbound packets) is an address belonging to the intermediate system itself." This would not be the case for RSVP Path messages.

6.6. Applicability of Tunnel Mode with Address Preservation

The document "Multicast Extensions to the Security Architecture for the Internet Protocol" [RFC5374] defines in section 3.1 a new tunnel mode: Tunnel mode with address preservation. This mode copies the destination and optionally the source address from the inner header to the outer header. Therefore the encapsulated packet will have the same destination address as the original packet, and be normally subject to the same routing decisions. While [RFC5374] is focusing on multicast environments, tunnel mode with address preservation can be used also to protect unicast traffic in conjunction with group keying.

Stephen Kent 11/30/09 10:23 PM
Comment: This RFC defines this mode for use by a security gateway sending traffic on a multicast SA. The authors need to explain how this applies to RSVP; I would expect the nodes to act as end systems, not SGs.

Tunnel mode with address preservation, in conjunction with group keying, allows the use of AH or ESP for protection of RSVP even in cases where non-RSVP nodes have to be traversed. This is because it allows routing of the IPsec protected packet through the non-RSVP nodes in the same way as if it was not IPsec protected.

Stephen Kent 11/30/09 3:30 PM
Comment: IPsec has always allowed the inner and outer headers to be the same, because it allows tunnel mode to be used between end systems. So, what is really different here?

Stephen Kent 11/30/09 3:27 PM
Deleted: IPsec

Stephen Kent 11/30/09 10:24 PM
Comment: Provide details here to explain the key details that make this work.

7. End Host Considerations

Unless RSVP Proxy entities ([I-D.ietf-tsvwg-rsvp-proxy-approaches] are used, RSVP signaling is controlled by end systems and not routers. As discussed in [RFC4230], RSVP allows both user-based security and host-based security. User-based authentication aims at "providing policy based admission control mechanism based on user identities or application." To identify the user or the application,

a policy element called AUTH_DATA, which is contained in the POLICY_DATA object, is created by the RSVP daemon at the user's host and transmitted inside the RSVP message. This way, a user may authenticate to the Policy Decision Point (or directly to the first hop router). Host-based security relies on the same mechanisms as between routers (i.e., the INTEGRITY object) as specified in [RFC2747]. For host-based security, interface-based or neighbor-based keys may be used, however, key management with pre-shared keys can be difficult in a large scale deployment, as described in section 4. In principle an end host can also be part of a group key scheme, such as GDOI. If the end systems are part of the same zone of trust as the network itself, group keying can be extended to include the end systems. If the end systems and the network are in different zones of trust, group keying cannot be used.

8. Applicability to Other Architectures and Protocols

While, so far, this document discusses only RSVP security assuming the traditional RSVP model as defined by [RFC2205] and [RFC2747], the analysis is also applicable to other RSVP deployment models as well as to similar protocols:

- Aggregation of RSVP for IPv4 and IPv6 Reservations [RFC3175]: This scheme defines aggregation of individual RSVP reservations, and discusses use of RSVP authentication for the signaling messages. Group keying is applicable to this scheme, particularly when automatic Deaggregator discovery is used, since in that case, the Aggregator does not know ahead of time which Deaggregator will intercept the initial end-to-end RSVP Path message.
- Generic Aggregate Resource ReSerVation Protocol (RSVP) Reservations [RFC4860]: This document also discusses aggregation of individual RSVP reservations. Here again, group keying applies and is mentioned in the Security Considerations section.
- Aggregation of Resource ReSerVation Protocol (RSVP) Reservations over MPLS TE/DS-TE Tunnels [RFC4804]([RFC4804]): This scheme also defines a form of aggregation of RSVP reservation but this time over MPLS TE Tunnels. Similarly, group keying may be used in such an environment.
- Pre-Congestion Notification (PCN): [I-D.ietf-pcn-architecture] defines an architecture for flow admission and termination based on aggregated pre-congestion information. One deployment model for this architecture is based on IntServ over DiffServ: the DiffServ region is PCN-enabled, RSVP signalling is used end-to-end but the PCN-domain is a single RSVP hop, i.e. only the PCN-boundary-nodes process RSVP messages. In this scenario, RSVP authentication may be required among PCN-boundary-nodes and the considerations about keying approaches discussed earlier in this

Stephen Kent 11/30/09 3:31 PM
Deleted:

Stephen Kent 11/30/09 3:32 PM
Comment: "pre-shared" is yet another key management term. Why does it appear here first. Is it different from static or manual keying as discussed in prior sections?

Stephen Kent 11/30/09 3:33 PM
Comment: Zone vs. domain vs. group?

Stephen Kent 11/30/09 3:33 PM
Comment: Ibid.

Stephen Kent 11/30/09 3:36 PM
Comment: This is too glib. You may suggest that the analyses presented here apply to these other contexts, but that is far short of being a definitive assertion, especially given some of the errors in the analysis I have identified.

Stephen Kent 11/30/09 3:33 PM
Deleted: only

document apply. In particular, group keying may facilitate operations since the ingress PCN-boundary-node does not necessarily know ahead of time which Egress PCN-boundary-node will intercept and process the initial end-to-end Path message. Note that from the viewpoint of securing end-to-end RSVP, there are a lot of similarities in scenarios involving RSVP Aggregation over aggregate RSVP reservations ([RFC3175], [RFC4860]), RSVP Aggregation over MPLS-TE tunnels ([RFC4804]), and RSVP (Aggregation) over PCN ingress-egress aggregates.

9. Summary

The following table summarizes the various approaches for RSVP keying, and their applicability to various RSVP scenarios. In particular, such keying can be used for RSVP authentication (e.g., using the RSVP INTEGRITY object or AH) and/ or for RSVP encryption (e.g., using ESP in tunnel mode).

	Neighbor/interface based keys	Group keys
Works intra-domain	Yes	Yes
Works inter-domain	Yes	No
Works over non-RSVP hops	No	Yes (1)
Dynamic keying	Yes (IKE)	Yes (e.g., GDOI)

Table 1: Overview of keying approaches and their applicability

(1): RSVP integrity with group keys works over non-RSVP nodes; RSVP encryption with ESP and RSVP authentication with AH work over non-RSVP nodes in 'Tunnel Mode with Address Preservation'; RSVP encryption with ESP & RSVP authentication with AH do not work over non-RSVP nodes in 'Tunnel Mode'.

We also make the following observations:

- All key types can be used statically, or with dynamic key negotiation. This impacts the manageability of the solution, but not the applicability itself.
- For encryption of RSVP messages, IPsec ESP in tunnel mode can be used. There is however a security concern, see Section 6.2.
- There are some special cases in RSVP, like non-RSVP hosts, the "Notify" message (as discussed in Section 5.1), the various RSVP deployment models discussed in Section 8 and MPLS Traffic Engineering and GMPLS discussed in section 5.2 , which would

Stephen Kent 11/30/09 3:36 PM
Deleted: IPsec

Stephen Kent 11/30/09 3:37 PM
Deleted: IPsec

Stephen Kent 11/30/09 3:37 PM
Deleted: managability

Stephen Kent 11/30/09 3:37 PM
Deleted: s

benefit from a group keying approach.

10. Security Considerations

This entire document discusses RSVP security; this section describes a specific security considerations relating to subverted RSVP nodes

10.1. Subverted RSVP Nodes

A subverted node is defined here as an untrusted node, for example because an intruder has gained control over it. Since RSVP authentication is hop-by-hop and not end-to-end, a subverted node in the path breaks the chain of trust. This is to a large extent independent of the type of keying used.

For interface or per-neighbor keying, the subverted node can now introduce fake messages to its neighbors. This can be used in a variety of ways, for example by changing the receiver address in the Path message, or by generating fake Path messages. This allows path states to be created on every RSVP router along any arbitrary path through the RSVP domain. That in itself could result in a form of Denial of Service by allowing exhaustion of some router resources (e.g. memory). The subverted node could also generate fake Resv messages upstream corresponding to valid Path states. In doing so, the subverted node can reserve excessive amounts of bandwidth thereby possibly performing a denial of service attack.

Group keying allows the additional abuse of sending fake RSVP messages to any node in the RSVP domain, not just adjacent RSVP nodes. However, in practice this can be achieved to a large extent also with per neighbor or interface keys, as discussed above. Therefore the impact of subverted nodes on the path is comparable for all keying schemes discussed here (per-interface, per-neighbor, group keys).

11. Acknowledgements

The authors would like to thank everybody who provided feedback on this document. Specific thanks to Bob Briscoe, Hannes Tschofenig, Brian Weis, Ran Atkinson, and Kenneth G. Carlberg.

12. Changes to Previous Version

This section provides a change log. It will be removed in the final document:

12.1. changes from behringer-00 to behringer-01

- New section "Applicability to Other Architectures and Protocols": Goal is to clarify the scope of this document: The idea presented here is also applicable to other architectures (PCN[I-D.ietf-pcn-architecture], RFC3175 and RFC4860, etc.
- Clarified the scope of this document versus RFC4230 (in the introduction, last paragraph).
- Added a section on "End Host Considerations".
- Expanded section 5.5 (RSVP Encryption) to clarify that GDOI contains all necessary mechanisms to do RSVP encrpytion.
- Tried to clarify the "trust to do what?" question raised by Bob Briscoe in a mail on 26 Jul 2007. See the section on trust model.
- Lots of small editorial changes (references, typos, figures, etc).
- Added an Acknowledgements section.

12.2. changes from behringer-01 to ietf-00

- various edits to make it clearer that draft-weis-gdoi-for-rsvp is an example of how dynamic group keying could be achieved for RSVP and not necessarily the recommended solution

12.3. changes from ietf-00 to ietf-01

- Significant re-structuring of the entire document, to improve the flow, and provide more consistency in various sections.
- Moved the "Subverted RSVP nodes" discussion into the security considerations section.
- Added a "summary" section.
- Complete re-write of the old section 5.5 (RSVP encryption), and "promotion" to a separate section.
- Changed reference ID.weis-gdoi-for-rsvp to the new draft ID.weis-gdoi-mac-tek
- in several places, explicitly mentioned "encryption" for RSVP (in parallel to authentication).
- Various minor edits.

12.4. changes from ietf-01 to ietf-02

- Re-wrote and re-structured the section on IPsec (section 6).
- Re-wrote the section on RSVP-TE and GMPLS (section 5.2).
- Various editorial changes.

12.5. changes from ietf-02 to ietf-03

- Extension of section 6.3 (Using IPsec AH), to address comments received from Ran Atkinson. Included a comparison of what AH protects vs what the INTEGRITY object protects.

- Added section 6.5 on "tunnel mode with address preservation.
- Some minor edits.

12.6. changes from ietf-03 to ietf-04

- Added below table 1 in note (1) that "RSVP encryption with ESP and RSVP authentication with AH work over non-RSVP nodes in 'Tunnel Mode with Address Preservation'"

12.7. changes from ietf-04 to ietf-05

- Clarified in section 6.3 that IPsec AH also secures the immutable fields of the outer header (comment from Bob Briscoe)
- Simplified in section 2 the comment that trust in group keying extends to all members of the group (deleted the words on "explicit and implicit"). (comment from Brian Weis)
- A number of corrections, re-wordings and clarifications in response to Kenneth Carlberg's email from 2 June 2009

13. Informative References

[I-D.ietf-pcn-architecture]
Eardley, P., "Pre-Congestion Notification (PCN) Architecture", draft-ietf-pcn-architecture-11 (work in progress), April 2009.

[I-D.ietf-tsvwg-rsvp-proxy-approaches]
Faucheur, F., Manner, J., Wing, D., and L. Faucheur, "RSVP Proxy Approaches", draft-ietf-tsvwg-rsvp-proxy-approaches-07 (work in progress), May 2009.

[I-D.weis-gdoi-mac-tek]
Weis, B. and S. Rowles, "GDOI Generic Message Authentication Code Policy", draft-weis-gdoi-mac-tek-00 (work in progress), July 2008.

[RFC2205] Braden, B., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997.

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

[RFC2747] Baker, F., Lindell, B., and M. Talwar, "RSVP Cryptographic Authentication", RFC 2747, January 2000.

[RFC3175] Baker, F., Iturralde, C., Le Faucheur, F., and B. Davie, "Aggregation of RSVP for IPv4 and IPv6 Reservations", RFC 3175, September 2001.

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, December 2001.

[RFC3473] Berger, L., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, January 2003.

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

[RFC3562] Leech, M., "Key Management Considerations for the TCP MD5 Signature Option", RFC 3562, July 2003.

[RFC3740] Hardjono, T. and B. Weis, "The Multicast Group Security Architecture", RFC 3740, March 2004.

[RFC4090] Pan, P., Swallow, G., and A. Atlas, "Fast Reroute Extensions to RSVP-TE for LSP Tunnels", RFC 4090, May 2005.

[RFC4206] Kompella, K. and Y. Rekhter, "Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)", RFC 4206, October 2005.

[RFC4216] Zhang, R. and J. Vasseur, "MPLS Inter-Autonomous System (AS) Traffic Engineering (TE) Requirements", RFC 4216, November 2005.

[RFC4230] Tschofenig, H. and R. Graveman, "RSVP Security Properties", RFC 4230, December 2005.

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

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC4804] Le Faucheur, F., "Aggregation of Resource ReSerVation Protocol (RSVP) Reservations over MPLS TE/DS-TE Tunnels", RFC 4804, February 2007.

[RFC4860] Le Faucheur, F., Davie, B., Bose, P., Christou, C., and M. Davenport, "Generic Aggregate Resource ReSerVation Protocol (RSVP) Reservations", RFC 4860, May 2007.

[RFC4875] Aggarwal, R., Papadimitriou, D., and S. Yasukawa, "Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)", RFC 4875, May 2007.

[RFC5374] Weis, B., Gross, G., and D. Ignjatic, "Multicast Extensions to the Security Architecture for the Internet Protocol", RFC 5374, November 2008.

Authors' Addresses

Michael H. Behringer
Cisco Systems Inc
Village d'Entreprises Green Side
400, Avenue Roumanille, Batiment T 3
Biot - Sophia Antipolis 06410
France

Email: mbehring@cisco.com
URI: http://www.cisco.com

Francois Le Faucheur
Cisco Systems Inc
Village d'Entreprises Green Side
400, Avenue Roumanille, Batiment T 3
Biot - Sophia Antipolis 06410
France

Email: flefauch@cisco.com
URI: http://www.cisco.com