The Use of Group Key Management in Internet Standards

Brian Weis
Distinguished Engineer, Cisco Systems
IETF MSEC WG Co-Chair
IEEE 802.1 Security TG Contributor

NIST Key Management Workshop
June 8-9, 2009

Introduction

- There has been an increasing realization in standards bodies that some applications require the use of group security (i.e., typically 3 or more entities sharing the same keying material)
  - When more than two systems need to share the same keying material, pair-wise Key Management (KM) methods are not sufficient
  - This talk discusses current group key management methods that have been defined in standards to deal with various group security scenarios

Agenda

- Overview of Group Key Management (GKM)
- Unique requirements of GKM
- Examples of Internet Standard GKM

Overview of Group Key Management

- There exists a large body of research, spanning several decades
- GKM methods can be broadly classified as either
  - Contributory (E.g., CLIQUES)
    - Group members use Group Diffie-Hellman to independently derive group keying material
  - Centralized (E.g., RFC 3547 (GDOI))
    - Group members register to a trusted third party (group controller/key server) and are given group keying material

Overview of Group Key Management

- Standards groups have concentrated on centralized GKM, because such methods best meet the needs of Internet group applications.
  - Maintaining separate roles of group controllers and group members is more practical for most applications
    - Authorization is straightforward
    - Revocation of group members is relatively easy
  - Centralized methods typically uses existing KM framework components
  - The contributory method do not scale as well to large numbers of group methods

Group Security Standards History

1997

- Hugh Harney & Carl Mukenhirn (Sparta) published a pair of IETF RFCs describing the GKMP protocol (RFC 2093, RFC 2094)
- Wallner, Harder, and Agee (NSA) published the first draft of an individual titled "Key Management for Multicast: Issues and Architectures" (RFC 2627)

1998

- The IETF IPsec WG became interested in defining how to secure IP multicast traffic, but the WG consensus was that this topic was believed to be an area not mature enough for standardization
- The Secure Multicast Research Group (SMuG) IRTF WG was formed to better describe the security requirements and use cases, and to create a reference framework.

2001

- The IETF MSEC WG was formed to focus on securing traffic of media broadcast applications
- The IETF AVT WG accepts a work item to develop a Secure RTP profile of RTP, recognizing that some RTP applications use IP multicast (RFC 3711)

Group Security Standards History

2004

- The IEEE 802.11i group publishes a wireless security method that includes distribution of a group key for protecting broadcast PDUs
- The IEEE 802.1 security task force begins development of key agreement methods for MACsec (IEEE 802.1X-REV)

2007-present

- The IETF focus has shifted from large multicast media broadcast applications to a wider range of Internet group security use cases
  - Conference bridged media applications
  - Internet signaling applications where communication is point-to-point but the identity of the recipient is not known in advance
  - Interior Routing Protocol security

MSEC WG

- Architecture documents:

  RFC 3740: The Multicast Group Security Architecture

  RFC 4046: Multicast Security (MSEC) Group Key Management Architecture

  RFC 5374: Multicast Extensions to the Security Architecture for the Internet Protocol
- GKM documents:

  RFC 3547: The Group Domain of Interpretation (GDOI)

  RFC 3830: MIKEY: Multimedia Internet KEYing

  RFC 4535: GSAKMP: Group Secure Association Key Management Protocol

Centralized GKM (RFC 3740)

Two protocol flows:

- Registration: provide a group member (GM) with current group policy & keying material
  - Mutual authentication of a group member (GM) and group controller (GC)
  - Authorization (GC authorizes GM, GM may authorize GC)
  - Create a strong secure channel (encrypted for confidentiality and including a MAC for data integrity), in which current group policy & keying material is downloaded to GM
  - GC uses a centralized policy to determine key usage

Note: there is a tight binding between authentication/authorization and the willingness of the GC to transport keys

Centralized GKM (RFC 3740)

- Rekey: efficiently provide updates for group policy & keying material to GM
  - GC multicasts updates to group policy and keys to all GMs
  - Updates are encrypted for confidentiality & signed for both data integrity and source origin authentication
  - GMs can be efficiently revoked when a Group Membership algorithm such as LKH is included in group policy (RFC 2627)

Note: GC depends on an implicit authentication/authorization, whereby only GMs given the confidentiality keys can continue to participate in the group

Key Transport

- Download of group keying material is a key transport operation
- Note that group keying material is distributed along with policy
  - Both policy and keying material has the requirement to be protected by strong authenticated encryption
- It could be useful for a KM framework to include this capability. One way to do so would be to allow authenticated encryption as a way to “wrap” keys.
  - This allows existing KM framework components to be used.

The Use of Confidentiality and Data Integrity as a Key Transport Method

- Use of recommended confidentiality and data integrity algorithms can meet or exceed the security of AES key wrap or public key encryption
- For example, use of 128-bit AES-GCM or AES-CCM to protect a GKM protocol provides
  - Strength of 128 bits
  - Use of a dynamic IV
- These attributes meet or exceed the strength of other key transport methods.

Key Derivation

- In a centralized GKM the GC unilaterally choose session keying material
  - One method is to use a strong RNG (e.g., as described in FIPS 140-2 Annex C)
  - In other cases, it is derived from a master key.
    - SP 800-108 recommends key derivation methods from a master key, which could be a useful part of a GKM framework

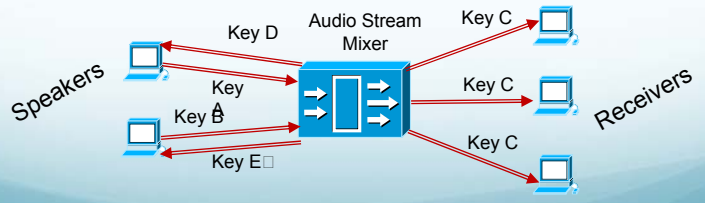
Examples of Internet Standards GKM

GKM is useful in a variety of applications, at various layers of the network stack. We discuss a few examples.

- Layer 4
  - Conference bridged media applications (SRTP)
- Layer 3
  - Securing multimedia content distributed via IP multicast (ESP)
  - Internet signaling applications where communication is point-to-point but the identity of the recipient is not known in advance (RSVP, ESP)
- Layer 2
  - The use of cryptographic groups that enforce a particular network access security policy on an Ethernet link (IEEE 802.1X-REV)
  - Distribution of wireless broadcast key (IEEE 802.11i)

Conference bridged media applications

- Conference bridges act as a mixer of media streams.
  - They can support many participants, where many of the participants receive the same media stream
  - The mixer's operation can be simplified through the use of group keys.
  - RTP is designed for group oriented point-to-multipoint
  - SRTP is also point-to-multipoint (i.e., needs group keying)

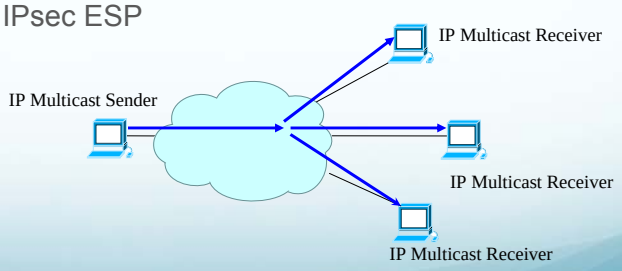


Conference bridged media applications

- Example: DTLS-SRTP Key Transport (KTR)
  - draft-ietf-avt-dtls-srtp-07
  - draft-wing-avt-dtls-srtp-key-transport-03
- Key Transport: Authenticated encryption

Securing multimedia content distributed via IP multicast

- IP packets encrypted and sent via IP multicast
  - IETF Multicast Group Security Architecture (RFC 3740)
    - Few senders, many receivers
    - Encrypted IP multicast packets
  - Data packets are usually RTP protected with SRTP, DTLS-SRTP, or IPsec ESP

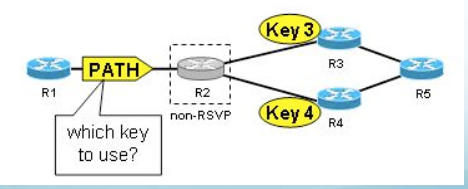


Securing multimedia content distributed via IP multicast

- Example: IPsec and GDOI
  - RFC 4301 & RFC 4374, RFC 3547
- Key Transport: GDOI Authenticated Encryption (allowed by FIPS 140-2 IG)

Internet signaling applications

- In some hop-by-hop applications, communication is point-to-point but the identity of the recipient is not known in advance
  - IP packets maintain host source & destination addrs, but routers along the path process the packet
  - Security associations are hop by hop, where the next hop may be one of a group of routers

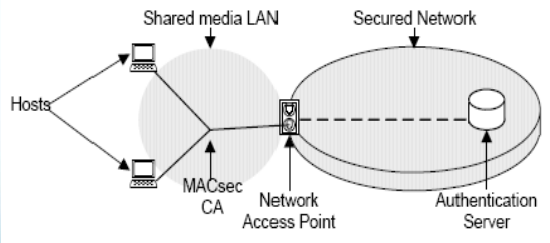


Internet signaling applications

- Example: RSVP and GDOI
  - draft-ietf-tsvwg-rsvp-security-groupkeying-04
  - draft-weis-gdoi-mac-tek-00
- Key Transport: GDOI Authenticated Encryption

IEEE 802.1 frame encryption

- IEEE 802.1AE (MACsec) defines an encryption method between stations on a LAN or LAN segment
  - Common scenario is one or more hosts connected to a bridge port ("Ethernet switch" port) using a shared media

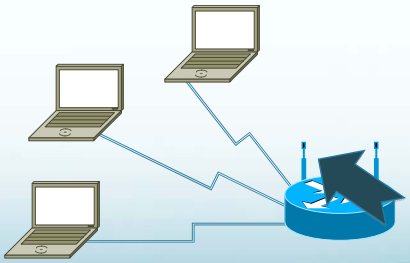


IEEE 802.1 frame encryption

- The draft IEEE 802.1X-REV specification provides GKM as an optional extension to user/device authentication
  - EAPOL-EAP exchange between Authenticator/Supplicant using an EAP method supporting key derivation (e.g., EAP-TLS, EAP-FAST)
  - EAPOL-MKA exchange between Authenticator/Supplicant using pair-wise key distributes a "group CAK"
  - EAPOL-MKA exchange between all hosts and bridge port chooses a key server, which distributes MACsec keys as needed
    - Key Transport: AES Key Wrap

IEEE 802.11i

- An IEEE 802.1X Authenticator using IEEE 802.11i sends multicast and broadcast frames, which need to be secured.
  - Replicating these frame and sending through each pair-wise security association would be wasteful.



IEEE 802.11i

- In addition to pair-wise keys, an IEEE 802.1X Authenticator defines a Group Temporal Key (GTK), used to protect multicast and broadcast frames.
  - This ‘one-to-many’ group key, used only by the station deriving the key
  - Key Transport: AES key wrap

Conclusions

- Centralized GKM applications are essential for many Internet applications
- Centralized GKM can be easily accommodated in a KM framework
  - General authenticated encryption methods can be used for key transport
  - It would be helpful if methods of key derivation described in SP 800-108 were explicitly noted in updates to newer NIST recommendations

For those viewing via webcast, please submit questions for this presentation to kmwquestions@nist.gov