Securing Group Management in IPv6 with Cryptographically Generated Addresses (CGA)

Presented by Viban Terence Yuven

(Based on a paper by Claude Castelluccia and Gabriel Montenegro)
Overview

Group Management in IP
- Multicast
- Anycast

Proof-of-Membership Problem

Solution Requirements

CGA Addresses
- CGA and Mobile IPv6
- Group CGA Addresses

Basic Scheme
- Protocol Properties

More Refined Protocol Overview
- Advantages
- Privacy Considerations

Conclusion

Questions
Group Management in IP

- **IP Multicast**
  - a single packet is sent by a source to a Multicast group which is identified by a single IP address.
  - packets are duplicated in the network and delivered to each member of the group
  - useful for group communications
    - games, video/audio conferences
    - files, content distributions

- **IP Anycast**
  - packets sent to an IP Anycast group reach only one member
    - the “closest” one
    - not always the same
  - an anycast address is assigned to a group of interfaces these interfaces reside within a topological region defined by an address prefix
IP Multicast

- A Multicast group is defined by an IP multicast address

```
+----------+----------------+-----------------+
<table>
<thead>
<tr>
<th>8</th>
<th>4</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>11111111</td>
<td>flag</td>
<td>scop</td>
</tr>
<tr>
<td>----------</td>
<td>----------------</td>
<td>-----------------</td>
</tr>
</tbody>
</table>
```

- The model:
  - a host that wants to join a group sends a **MLD message** to its local router
  - the local router then informs the routing fabric of the new member

- A host that wants to receive packets of a given group must explicitly **join** this group
IP Anycast

- An Anycast group is defined by an IP anycast address
  - IP anycast addresses are allocated from the unicast address space
- A host that wants to send packets to an anycast group:
  - use the group’s anycast address as destination address
  - the packets are routed by the network to the “closest” member
- The model:
  - a host that wants to join a group sends a MLD message to its local router...
  - the local router then informs the routing fabric of the new member
Proof-of-Membership Problem

- Both IP Multicast and Anycast suffer from potential DoS attacks
- Anyone can issue a MLD-join message for a multicast or anycast address
  - **Multicast**: a malicious host can overflow the network by adding extra branches in the delivery tree!
  - **Anycast**: a malicious host can redirect the traffic and prevents the legitimate hosts from seeing it!
- The problem is that the (access) routers do not know who is authorized to join each group!
- This is the *proof-of-membership* problem!
Solution Requirements

• The solution should be “light”, i.e. not too computationally expensive.
• The solution should be scalable i.e. able to support a very large number of members per group and a large numbers of groups.
• The solution should support mobile hosts efficiently
  – should provide fast group registration
  – should not assume any pre-established contexts in the routers
• The solution should be end-to-end
  – avoid reliance on global infrastructure such as PKI (Public Key Infrastructure) and TTP (Trusted Third Party).
CGA Addresses

- This proposal relies on Cryptographically Generated Addresses
- A CGA Address is generated from a Public Key
- IPv6 (unicast) address format:
  - prefix (64 bits) + HostID (64 bits) = 128 bits
- IPv6 CGA address, the HostID is generated from a public key (PK)

\[ \text{HostID} = \text{hmac-64} (\text{sha1} (\text{imprint}), \text{sha1} (\text{PK})) \]

- CGA addresses are unique
- A host can prove that it owns a CGA address by proving that it knows the corresponding private key, by signing its packets with it.
- NO infrastructure required: cryptographic relation between address and signature
- a malicious host could only steal a CGA address if:
  - it can find the private key or
  - it can find a public/private key pair that hashes to the target HostID
CGA and Mobile IPv6

• CGA are very useful to solve the *proof-of-ownership* problem and secure redirection protocols such as Mobile IPv6

• In Mobile IPv6, a mobile host (MH):
  – has a Home Address (HoA) in its Home network
  – gets a Care-of Address (CoA) in the visited network
  – informs its Correspond Nodes (CN) of its current CoA by sending a Binding Update (HoA->CoA)

• If the CN and the MH do not have a pre-established secret that binds the HoA with the MH
  – any malicious host could send a Binding Update to redirect someone’s else HoA

• If the HoA is a CGA:
  – a MH can prove that it owns its HoA by including its public key in the BU and by signing the resulting message with its private key
Group CGA Addresses

Two new types of CGA addresses are defined

- **Multicast CGA addresses (M-CGA)**
  - **GroupID = sha1-112(PK)**
  - new S bit in the flag field distinguishes these addresses

- **Anycast CGA addresses (A-CGA)**
  - same format as unicast CGA address i.e.
    - **HostID = hmac-64(sha1(imprint), sha1(PK))**
Basic Scheme

- A group is defined by a group CGA address (M-CGA or A-CGA)
- Any of the group controllers (could be any host, for example the source):
  - generates the group CGA address from a public/private key pair
  - authorizes members to join.

- authorization scheme (off-line)
  - the group manager authorizes the member by disclosing the group pub/priv. Key pair via a secure channel.

- registration scheme (on-line)
  - A host that wants to join the group MUST include the group public key with the MLD join message and sign it with the group private key.
  - The router can verify that the host is authorized to join the group if:
    - the Group CGA was generated from the group PK included in the MLD join message.
    - the signature is valid and therefore the host knows the group private key
    - Router performs a hash and a signature verification
Illustration

GROUP CONTROLLER

Gaddr (Gpub, Gpriv)

1

(Gpub, Gpriv)

HOST

2

(MLDjoin Gaddr) +
Gpub)_{Gpriv}

ROUTER

3

if (Gaddr == hash(Gpub)) { /* Group address generated from PK */
  if (signature is valid) /* the host knows Gpriv */
    accept MLDjoin
    return True;
}

reject MLDjoin;

24.06.2008

Internet Technology
Basic Scheme Protocol Properties

- Pros:
  - registration is *end-to-end*: all authorization information is in MLD message. Routers do not have to contact a TTP.
    - Low registration latency
    - scalable
    - mobile supported
  - no pre-established states are needed in the routers

- Cons:
  - membership revocation not provided
  - key disclosure problem
  - requires a secure channel between group manager and group members!

- another scheme that uses authorization certificates such as SPKI can be used
More Refined Protocol Overview

• Assumptions:
  – a group is defined by a group CGA address (M-CGA or A-CGA)
  – each member also has a (unicast) CGA address
  – group controller (possibly several)
    • generates the group CGA address from a public/private key pair
    • authorizes members to join by issuing certificates

• Authorization management (off-line)
  – a host that is authorized to join a group gets a SPKI certificate from the group controller
  – the certificates contains the group public key, the host CGA address, a validity period and is signed with the group private key.
More Refined Protocol Overview (2)

- **Registration management (On-line)**

- A host that wants to join the group must include its SPKI certificate (signed with the *Group private key* by a group controller) and its *CGA public key* in the MLD message and sign it with its *CGA private key* (the one used to generate its unicast address).

- A router that receives a MLD-join messages will only accept it if:
  - (1) *The host owns its CGA address*:
    - the CGA address contained in the certificate was generated from the host’s *CGA public key*
    - the MLD message’s signature is correct (the requesting host knows the CGA private key and therefore owns the corresponding CGA address).
  - (2) *the MLD-SPKI certificate is valid (CGA has been authorized)*:
    - the group address was generated from the *Group public key*, the validity period is correct, the certificate signature is correct
If (Haddr = hash (Hpub))
  if (signature is valid)
    /* Haddr belongs to the requester */
    If (Gaddr = hash (Gpub))
    /* Group address generated from PK */
    if (certificate signature is valid)
      if (issuer == Gaddr)
        if (subject == Maddr)
          if (date() == 02/04/2002)
            /* cert. Is valid */
            accept MLDjoin
            return ';
        }
    reject MLDjoin;
Advantages

- **Membership expiration supported**
  - each certificate has a validity period field
- **No secure channel required**
  - the certificates are sent from the group controller to the member in clear
- **No private key disclosure risk**
  - the group controller never discloses the group private key
- **Scalable**
  - distributed
  - no TTP required meaning that the routers can verify the authorization directly from the MLD msg
  - No pre-established context required in the routers, therefore well adapted to mobile environments
Privacy Considerations

• *Group Structure Privacy*
  - Routers operate strictly on a need-to-know bases
  - This results not only leads to a huge gain in terms of realiability and overhead but also in terms of privacy
  - Subscriber’s identity could also be configured using IPv6 address privacy extensions to hide the subscriber’s identity

• *Traffic Privacy*
  Traffic encryption by communicating key(s) at induction
  - Group controller generates keys K1 [t1;t2], K2 [t2;t3], ...Kj[tj;tj+1]
  - At induction a host receives a certificate and relevant keys (perhaps encrypted, for example using RSA encryption instead of DSA)
  - Host encrypts with Kj and includes j in plain text
Conclusions

• Handling group membership safely is a thorny problem which can lead to DOS attacks if ignored
• A node must be able to prove that it has the authorization to be a member of any given group
• This solution proposes a certain type of group address for both Multicast and Anycast groups to ensure a fully distributed solution
• When a router receives an MLD report, it can verify that the Multicast Listener is an authorized member of a given group
• In order to do this the router does not need to contact any trusted third party nor does it require any pre-established association with the listeners
• This leads not only to a huge gain in terms of scalability, reliability and overhead, but also in terms of privacy.
Thanks for your attention.

Questions