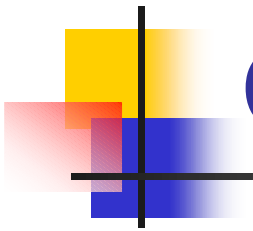
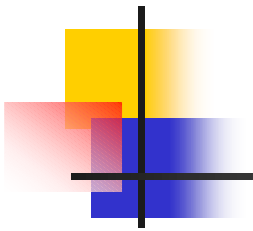
IGMP Security Problem Statement and Requirements

Brian Coan, Telcordia
Haixiang He, Nortel
Brian Weis, Cisco



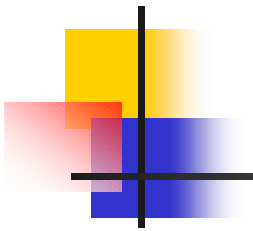
Outline

- Describe attacks against IGMP
- Outline goals for securing IGMP
- Identify requirements which meet these goals
- Propose an execution plan for GSEC WG



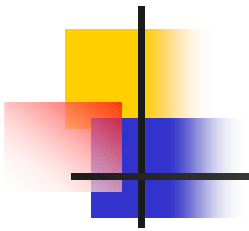
IGMP Attacks

- Local Subnet Attacks
  - IGMPv3 specification has a very good summary
  - Local attacks can cause problems to hosts and routers
  - Waste subnet bandwidth as well as hosts and routers' resources
  - This is a message authentication issue



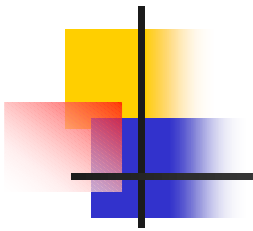
IGMP Attacks

- Subnet Attack Types
  - Off subnet attacks: use router alert mechanism and/or forwarding restriction proposed in IGMPv3
  - Local subnet IGMP message attacks: authenticate local IGMP messages
  - Packet flooding attacks: outside the scope of IGMP security



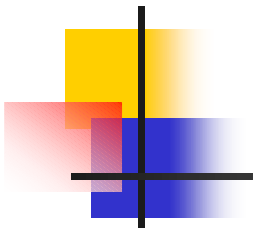
IGMP Attacks

- Internet Multicast Infrastructure Attacks
  - Pull multicast distribution tree all the way from the branch point to the subnet
  - Create useless routing or forwarding states even if there is no traffic
  - Waste bandwidth and router resources
  - Leak multicast traffic (even encrypted) in some scenarios
  - This is an access control (authorization) issue



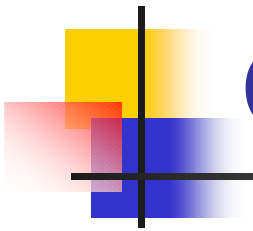
IGMP Attacks

- Intra-domain attacks
  - Receivers and senders are in the same domain.
  - Easy to enforce access control and prevent the attack.
- Inter-domain attacks
  - Receivers and senders are NOT in the same domains
  - Multicast tree can cross receivers' domain, senders' domain and transit domains
  - Access control is not easy and may require routing protocol participation



Where Secure IGMP Fits

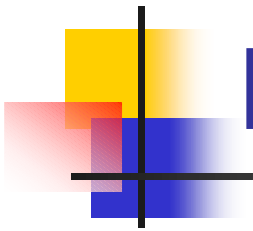
- Big Picture
  - End-to-end crypto
  - Secure multicast routing protocol
  - Secure IGMP
- Secure multicast routing protocol alone or secure IGMP alone is not enough. Both should be secure.



Overall Goals

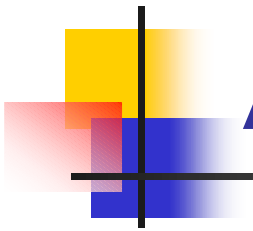
- Define mechanisms to ensure that
  - the extension of a multicast distribution tree to a given subnet can be initiated only by the request of a currently authorized receiver on that subnet
  - only authorized receivers on the subnet can keep the multicast distribution tree current
  - only currently authorized senders are able to introduce data packets onto a multicast distribution tree

Requirement:Local Subnet Protection



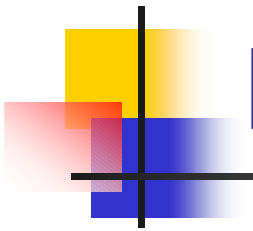
- Solution should consider the benefit vs. cost since local attacks are comparatively easy to trace
- Should consider the protections proposed in IGMPv3 specification
- Should also maintain the multicast model as much as possible

Requirement: Sender Authorization



- In the current multicast model, a sender does not need IGMP to send multicast packet
- A router also does not need IGMP to forward the multicast packet
- A protocol SIMILAR to IGMP can be used to do sender authorization
- This issue will be addressed separately

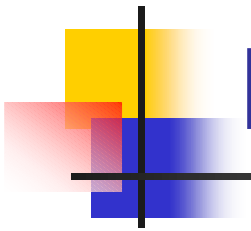
Requirement: Protect Multicast Infrastructure



- Goal: protect the IGMP states maintained by the edge routers
- Why: IGMP States are
  - used to trigger the multicast routing protocol that may cause
    - the delivery of traffic to edge router
    - the creation of upstream routing and forwarding states
  - used to forward traffic downstream

Requirement: Protect Multicast Infrastructure (cont.)

- One authorized (S,G) or (G) subscription within a subnet is enough
- Several levels of authorization are possible:
  - (S,G): A particular source in a particular group
  - (*,G): Any source in a particular group
  - (S, *): A particular source in any group
  - (*, *): Any source in any group
- Intra-domain can be the first step, but Inter-domain issue needs to be addressed by a solution
  - Multiple solutions are possible
  - We will address it in requirement draft



Requirement: Minimality

- Solution must be light-weighted and scalable
- Solution should maintain the multicast model as much as possible
- Solution should minimize the introduction of using new functions

Requirement: Least affect on IGMPv3

- No new requirement that multicast senders participate in IGMP
- Solution is specific to IPv4 (IPv6 is sufficiently different as to warrant a separate analysis)
- IGMPv3 must initially be supported due to popularity of SSM
  - Solution may be implemented based on IGMPv3
  - IGMPv2/v1 can be the next step if they are really matter, but a new mechanism would be required
  - Implementations are allowed to ignore IGMPv2/v1 messages
- The use of IGMP Proxying will not be precluded.

Requirement: Integrity of Messages

- Integrity of IGMPv3 messages is required, preferably with source authentication.
- Confidentiality of IGMPv3 messages is not a requirement -- for either query or report messages
  - IGMP subscriptions can be encrypted but some features such as IGMP switch snooping that can be broken should be considered in a solution

Requirement: Authentication & Authorization

- Receivers and routers may be both authenticated (validation of identity) and authorized (validation of current authority to participate)
  - The granularity of authorization supported will be for an individual receiver to obtain an individual sender's packets from an individual group

Requirement: Key Management Choices

- Both manual and server-based establishment of security associations must be permitted

Requirement: Containment of IGMP messages

- Defenses must be provided against IGMP messages launched from off the subnet as proposed in IGMPv3
  - A router must not forward IGMP queries to another subnet
  - A router must not forward IGMP membership reports
  - A router must not act on IGMP membership reports which do not have a source IP address which belongs to the subnet of the received interface

Proposed GSEC Execution Plan

- Write a draft outlining IGMP security requirements
- Propose receiver authentication and authorization mechanisms based on IGMPv3
- Implement sender authentication mechanisms using another approach, TBD later
  - May be implemented as extension to individual multicasting routing protocols
  - May be accomplished by requiring that all senders use secure IGMP to join a group before they being sending to that group