Three IGMP Security Architectures

Mark Baugher, Cisco
Thomas Hardjono, Verisign
Annelies Van Moffaert, Alcatel
Brian Weis, Cisco

Scope

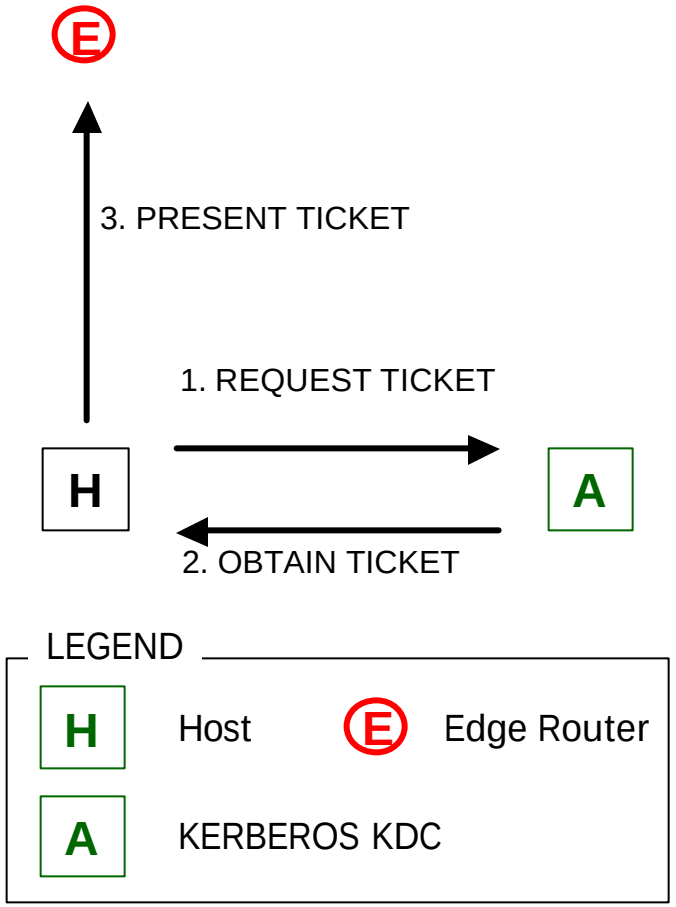
- There is an IGMP security problem
  - Who's authorized to have what role
- There is an IGMP QoS problem
  - Matching capacity with authorization

We're only addressing the security problem!

The Three Architectures

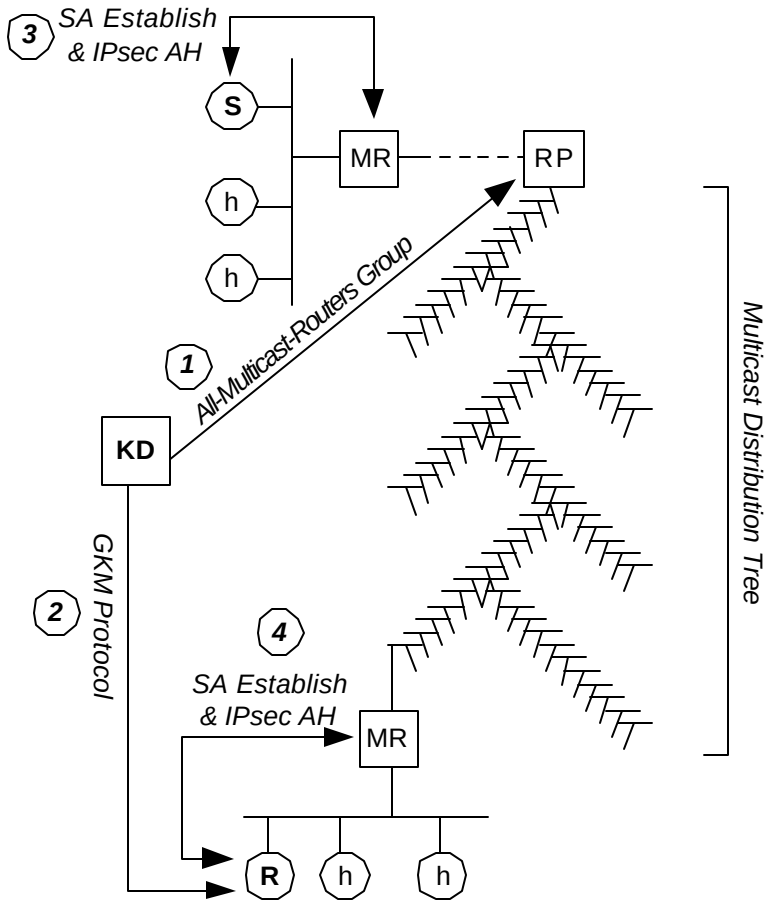
- HASM (Hierarchical Application-Level Secure Multicast)
  - **draft-coan-hasm-00.txt**
- SMRAC (Simple Multicast Receiver Access Control)
  - **draft-irtf-gsec-smrac-00.txt**
- IGMP Message Authentication
  - **draft-irtf-gsec-igmpv3-security-issues-01.txt**

HASM



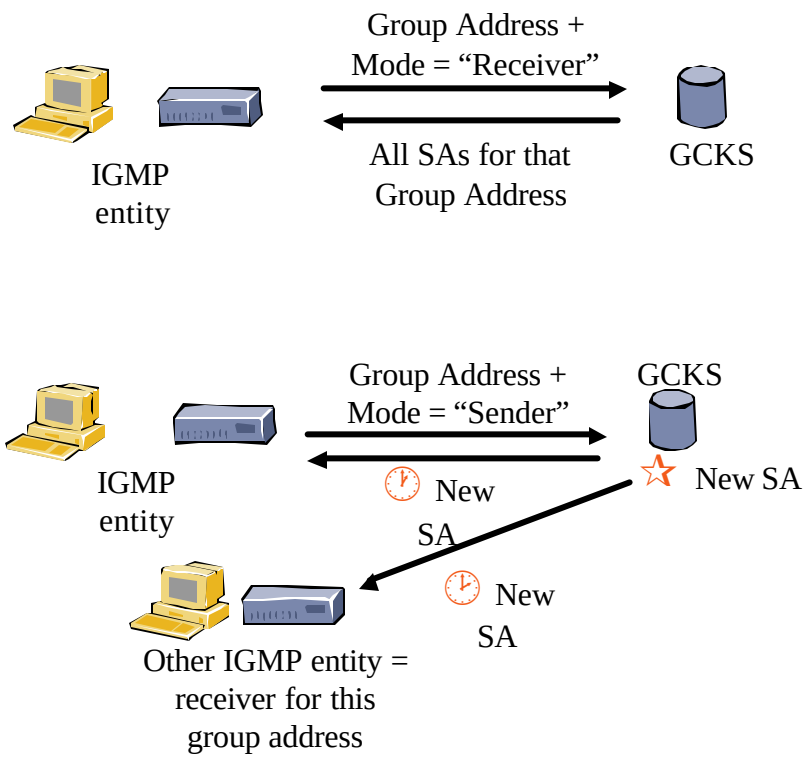
- Four Designs
  0. End-to-end security
  1. Receiver authorization
  2. Sender authorization
  3. Point-to-point, authenticated overlays
- Designs 1 and 2 define IGMP security

SMRAC



- Receiver must obtain Access Token from KD at the same time as initial user-authentication to obtain group-key
- Multicast Router (MR) need only be able to verify authenticity of token (signed by KD)
- KD may use distribution tree to spread valid token-list and KD-certificate

IGMP message authentication



- IPsec AH or ESP
- (G)SA per (Group, Sender)
- Extension of GDOI to set up multi-party SAs
  - contact local GCKS as new "Sender" or "Receiver"
  - GCKS pushes necessary SAs
- Example IGMP GSAs
  - General Queries: Sender={IGMP router}, Receivers={all multicast entities on subnet}
  - Report: Sender=host, Receivers={IGMP routers}

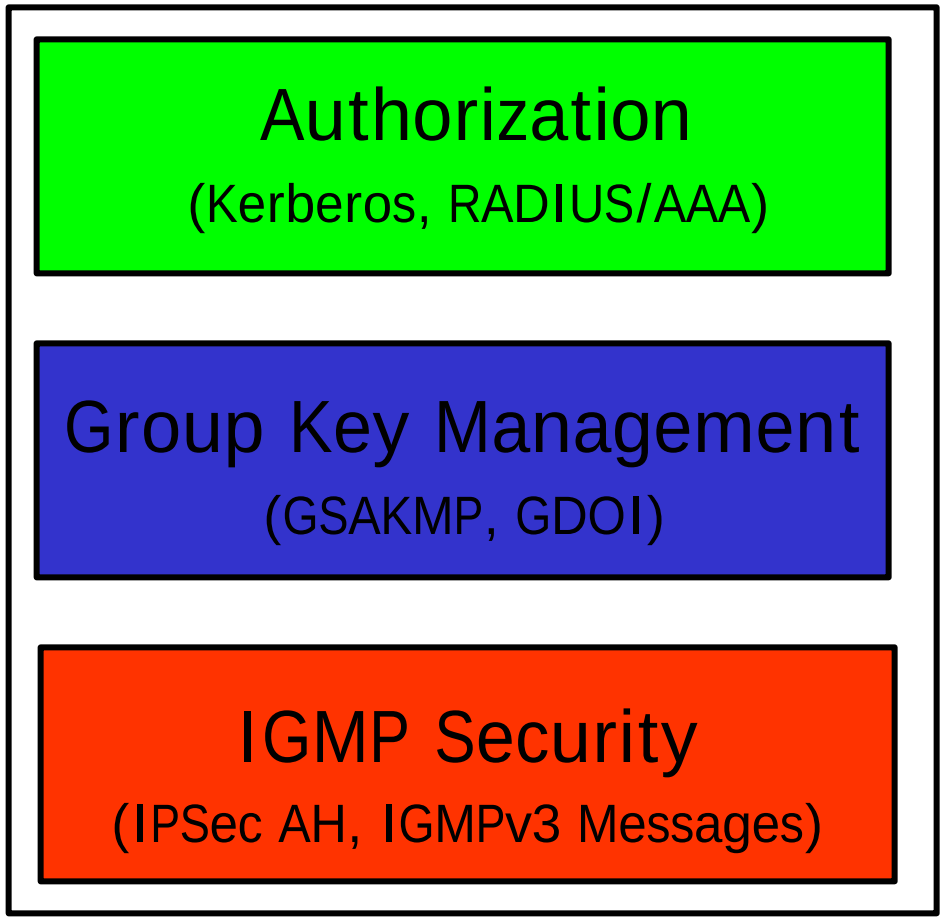
Review of IGMP in the architectures

- HASM
  - Design 1 addresses IGMP security using Kerberos tokens
  - Design 2 adds policy for restricting senders
- SMRAC
  - Adds extensions to IGMPv3 using tokens
- Alcatel
  - Encapsulates IGMPv3 in AH or ESP

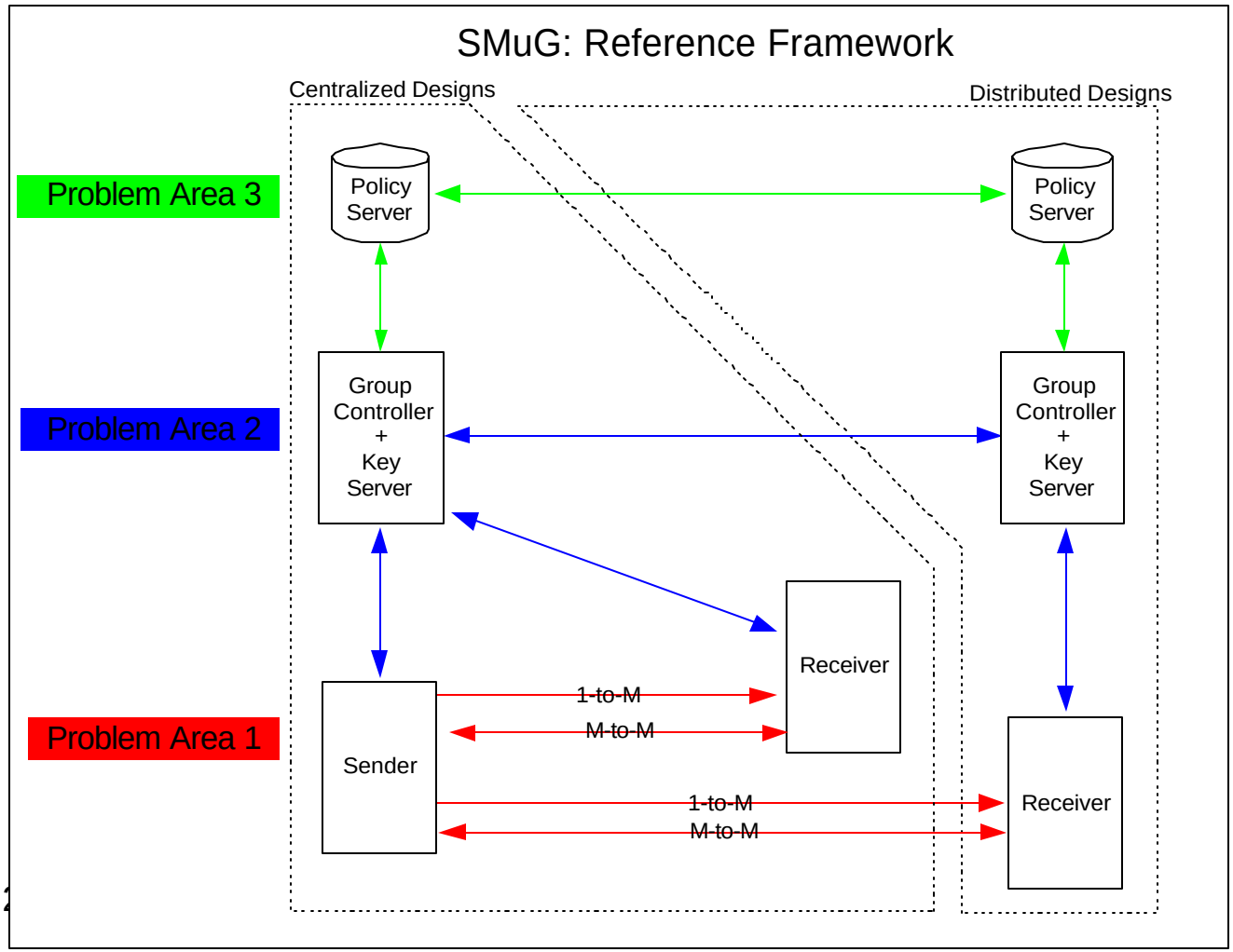
Proposed work agenda

- Focus on IGMPv3 (receivers)
- Defer sender authorization issues

Secure IGMP Block Diagram



Original SMuG Reference Framework



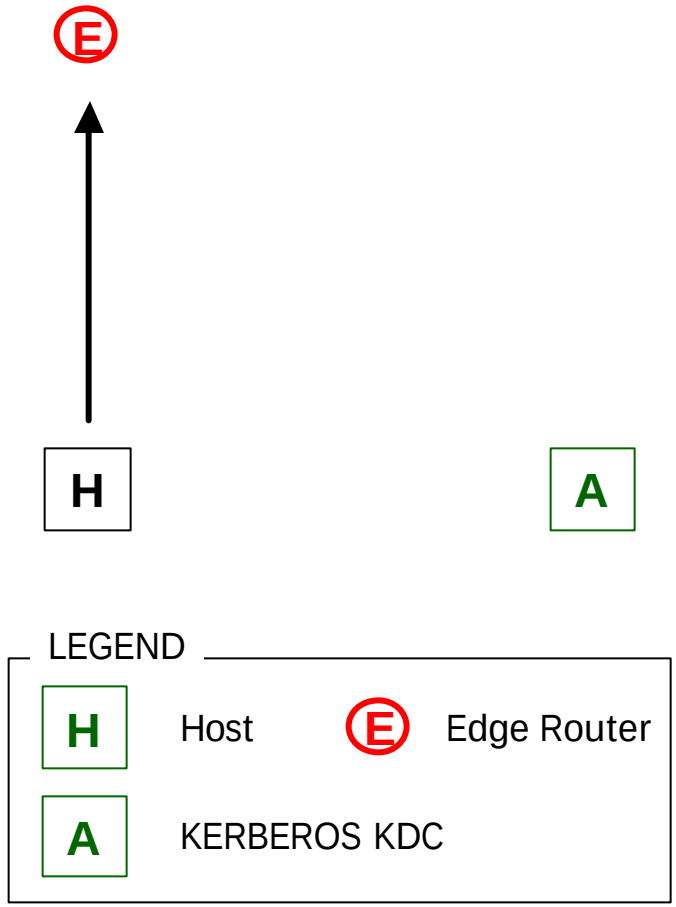
Next steps ....

- GSEC needs to consider which architecture (or parts thereof) satisfy the Secure IGMP requirements
- This will lead to a GSEC IGMP security architecture document

Questions?

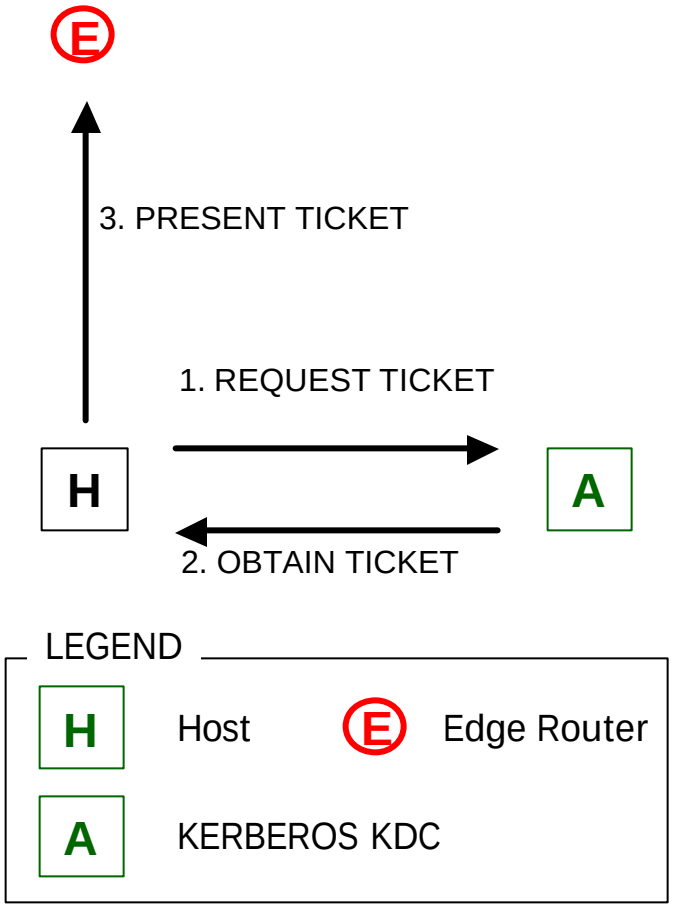
Backup

HASM Design 0



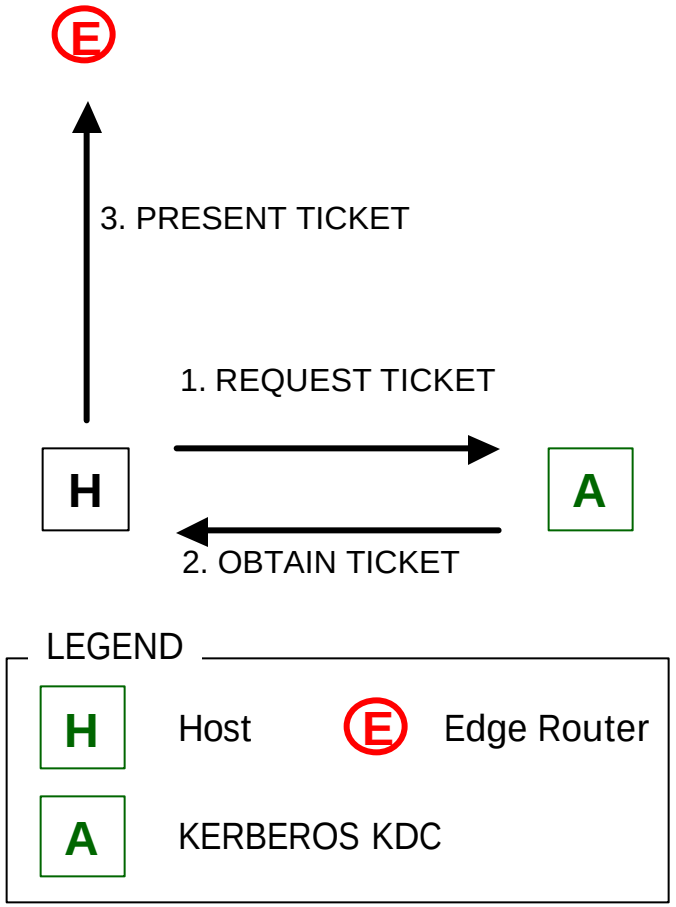
- Based up securing the data plane
  - Using multicast security
- No control plane security

HASM Design 1



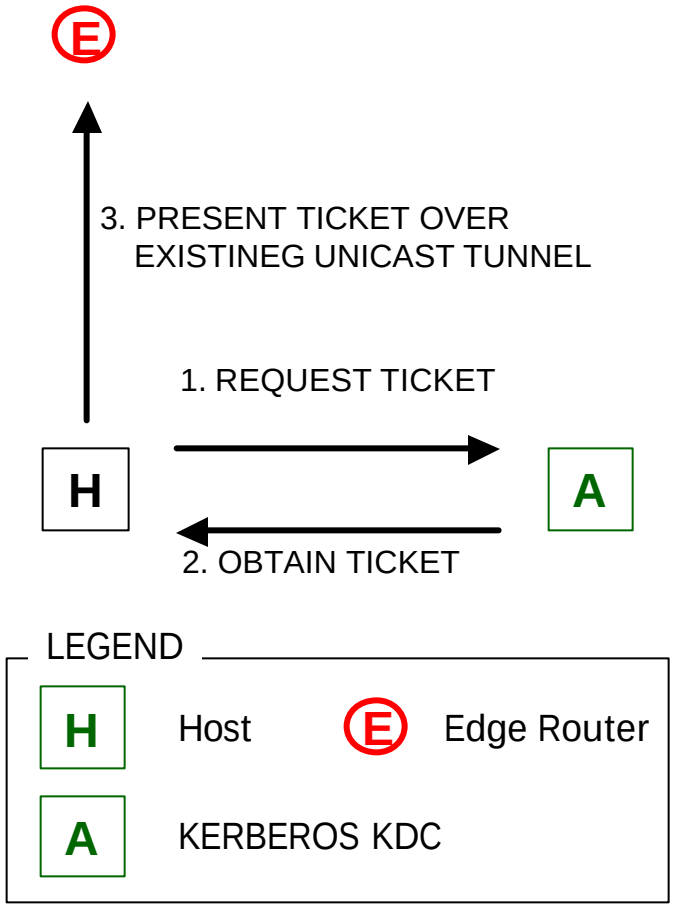
- Works for IGMP
- Receiver-authorized joins
- Uses Kerberos

HASM Design 2



- Outside of IGMP
- Requires new host and router protocol
- Sender-authorized joins
- Uses Kerberos

HASM Design 3



- Experimental
  - Uses unicast tunnels
  - Each tunnel is separately authorized
- New router-host control protocols
- Uses Kerberos for authorization