Security Issues in PIM-SM

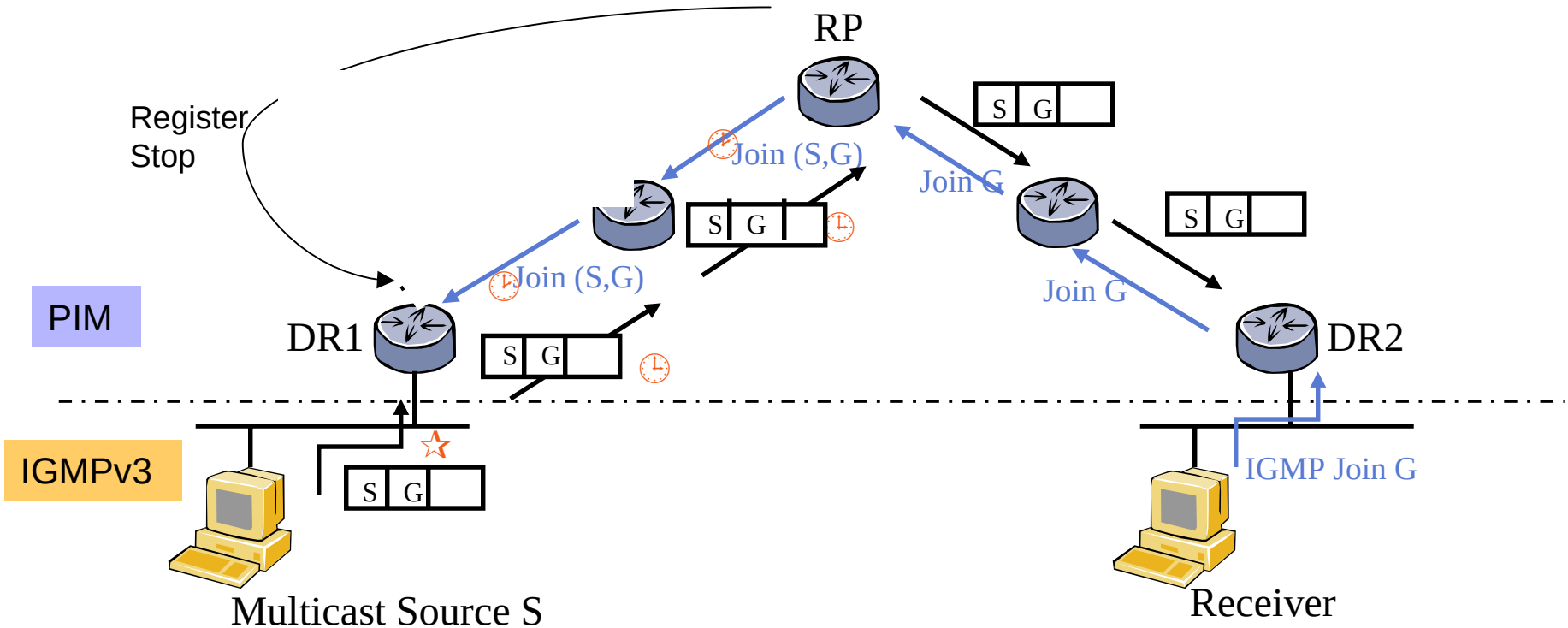
IRTF, GSEC meeting,
Minneapolis 19-03-'02

Olivier Paridaens
Annelies Van Moffaert

PIM-SM: Protocol Overview

Draft-ietf-pim-sm-v2-new-05.txt

PIM-SM: Protocol Independent Multicast-Sparse Mode
DR: Designated Router
RP: Rendez-vous Point = Root of multicast tree



PIM-SM Bootstrap mechanism

- How do the PIM routers know the correct RP for every group?
- Bootstrap Router (BSR) periodically sends Bootstrap Messages (BSMs): info to map a range of group addresses to an RP.
- BSM are
  - flooded hop-by-hop throughout the PIM domain
  - IP dest addr = 224.0.0.13, all PIM routers address
  - TTL=1
  - all PIM routers store Bootstrap information

Illustration of C-RP and BSM mechanism

C-RP: Candidate-RP
BSR: BootStrap Router
BSM: BootStrap Message

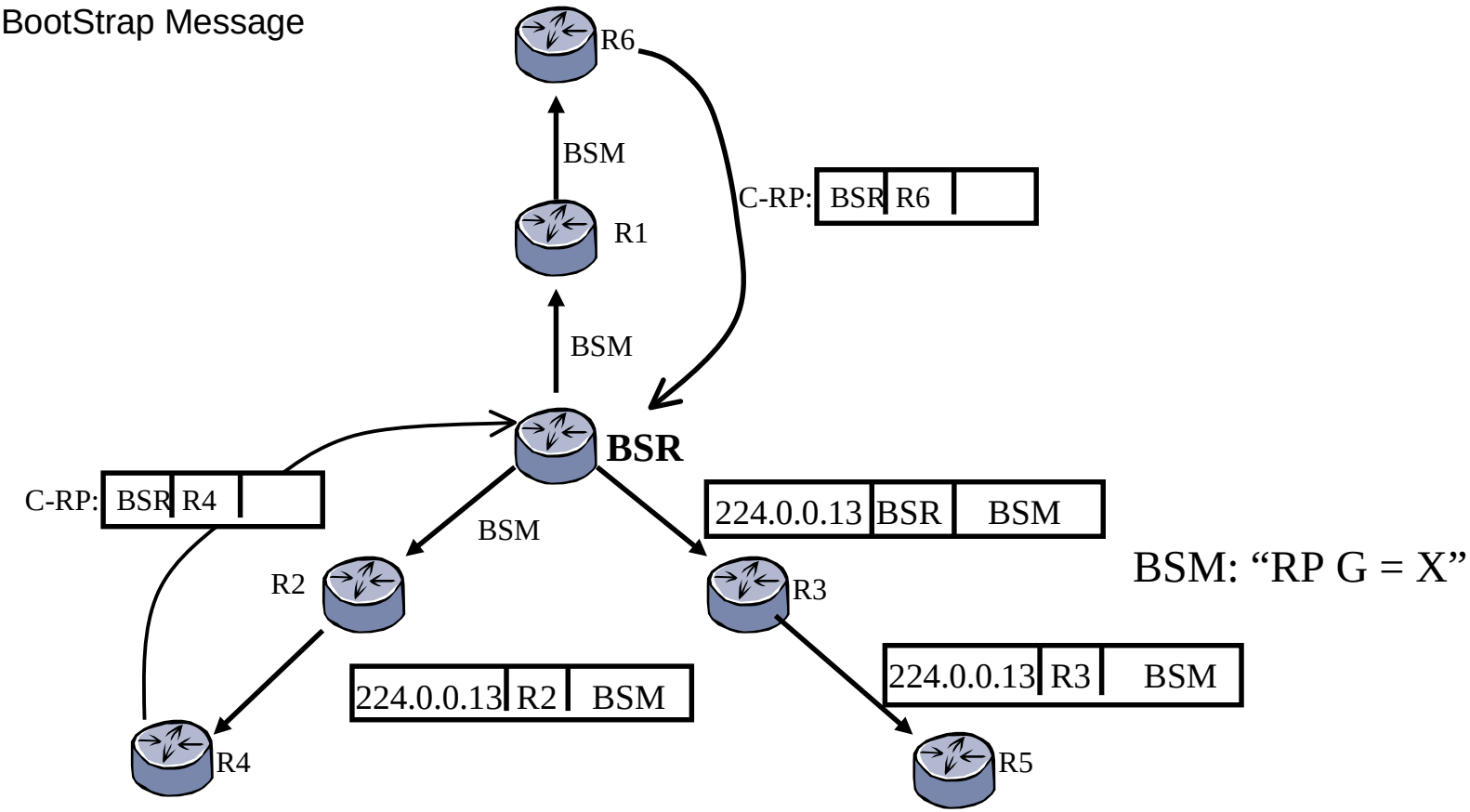
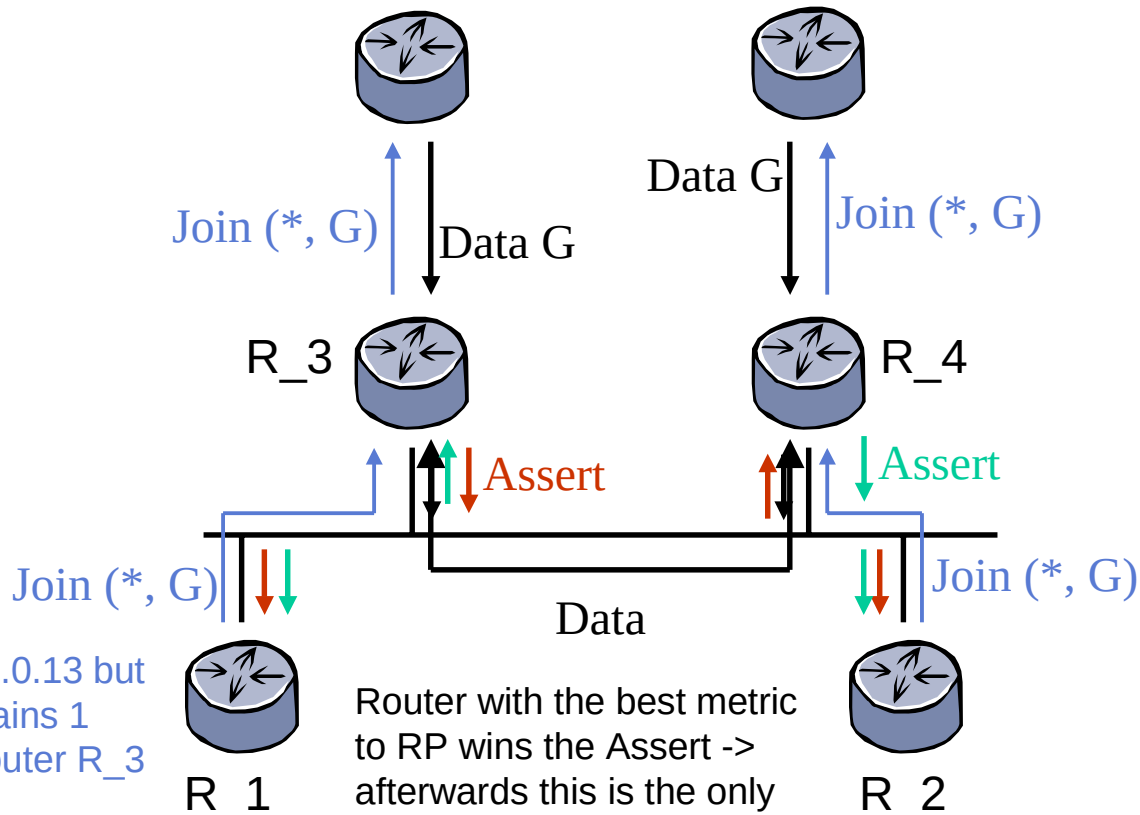


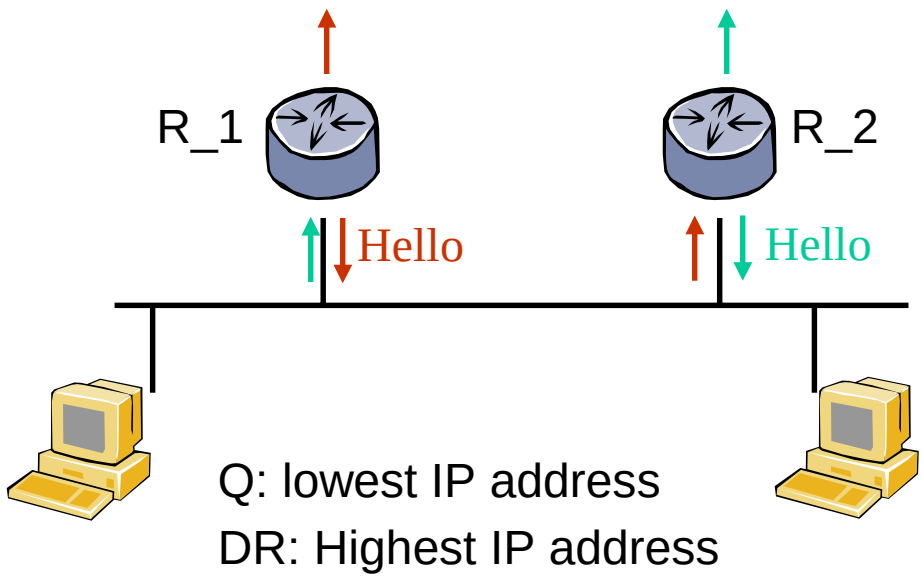
Illustration of Assert mechanism

Assert mechanism prevents duplicate traffic on shared LANs



Hello messages

- Sent by every router to announce itself to its neighbors
- No Join/prunes etc are accepted from routers from which no Hello is received
- Used to decide which PIM router will be DR on a local LAN that connects to internet through >1 PIM router
- Typically DR ≠ Q.



Conclusion from security point of view

- All link-local messages: Join/Prune, Assert, Hello are sent to a multicast address (224.0.0.13) and can be destined for more than 1 PIM router
- Bootstrap messages ensure correct mapping between a range of group addresses and RPs (roots) for these groups. They are relayed hop-by-hop each time as payload of a new IP packet with TTL=1, Dest IP = 224.0.0.13, Source IP = IP of relaying PIM router $\Rightarrow$ IPsec AH cannot provide end-to-end security

Security section in PIM-SM I-D

- Draft-irtf-gsec-pim-sm-security-issues-01.txt
- Draft-ietf-pim-sm-v2-new-05.txt
- Recommends IPsec AH to authenticate PIM-SM control messages
  - Unicast messages (Register, Register Stop)
    - no problem, standard IPsec AH and IKE can be used
  - Link-local messages (Join/Prune, Hello, Assert)
    - described solution ⇒ problems with anti-replay mechanism
  - Bootstrap messages
    - nowhere mentioned in security section

IPsec AH for PIM link-local messages

- Link-local messages (Join/Prune, Hello, Assert)
  - PIM-SM I-D: 1 SA for this group shared by all PIM routers on the link/subnet with SPI = 0
    - >1 sender per SA ⇒ anti-replay mechanism fails
    - Proposed solution: separate SA per sender
  - Sent to IP dest 224.0.0.13 ⇒ SAs are predictable ⇒ SAs can be pre-configured manually
    - E.g. k PIM routers on subnet: R_1,…R_k

Router R_1

Preconfigured SAs for Router R_1			
	IP dest	IP source	Message
Outgoing	224.0.0.13	R_1	Join/Prune, Hello, Assert
Incoming	224.0.0.13	R_2	Join/Prune, Hello, Assert
		…	…
	224.0.0.13	R_k	Join/Prune, Hello, Assert

Authentication of BootStrap Messages

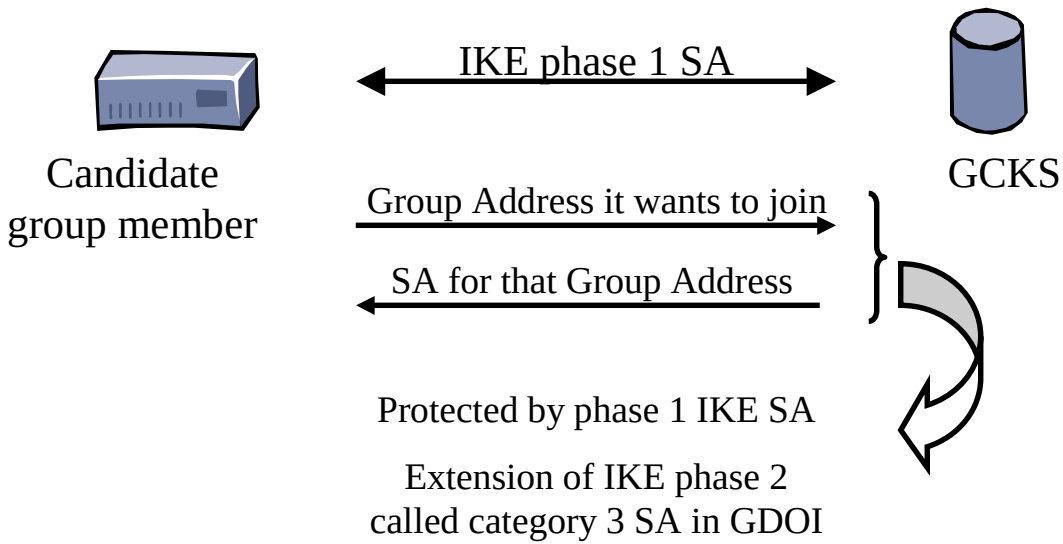
- Authentication of Bootstrap messages is nowhere covered
  - IPsec AH is symmetric key-based ⇒ cannot provide source (=BSR) authentication of Bootstrap Messages (BSMs)
    - digital signatures within Bootstrap messages
    - (TESLA)
  - BSMs are relayed hop-by-hop, every relaying PIM router creates a new IP packet with TTL=1 ⇒ BSR authentication should be done within PIM-SM rather than at IP layer
  - Keying mechanism is required such that all PIM routers have a valid copy of the BSR's public key. Simple Key Management Protocol (SKMP) proposed ideas for this.

SA set-up for link-local messages

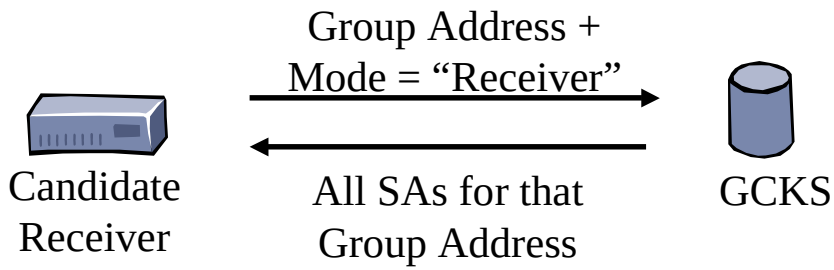
- Automatic configuration of SAs has often advantages (practical, scalable)
- IKE cannot be used to set up SAs that should be shared by more than 2 parties (1 sender, >1 receiver)
- Draft-irtf-gsec-pim-sm-security-issues-01.txt proposes a new mechanism based on an extension of GDOI

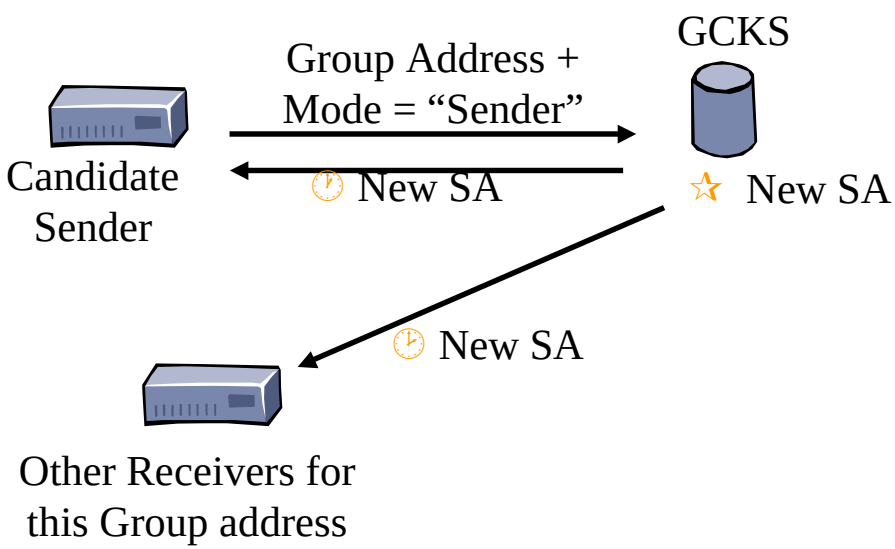
Mechanism to Automatically Set up Multi-party SAs based on GDOI

Group Domain of Interpretation (GDOI)



Proposed extension to GDOI





Example of SAs to protect link-local PIM messages

Booting PIM Router

IKE Phase 1

GCKS

224.0.0.13 + mode = "Receiver"

SA per PIM router on the same link/subnet

Booting PIM Router

IKE Phase 1

GCKS

224.0.0.13 + mode = "Sender"

New SA

☆ GCKS creates New SA

Other PIM Router on same link/subnet

IKE Phase 1

New SA