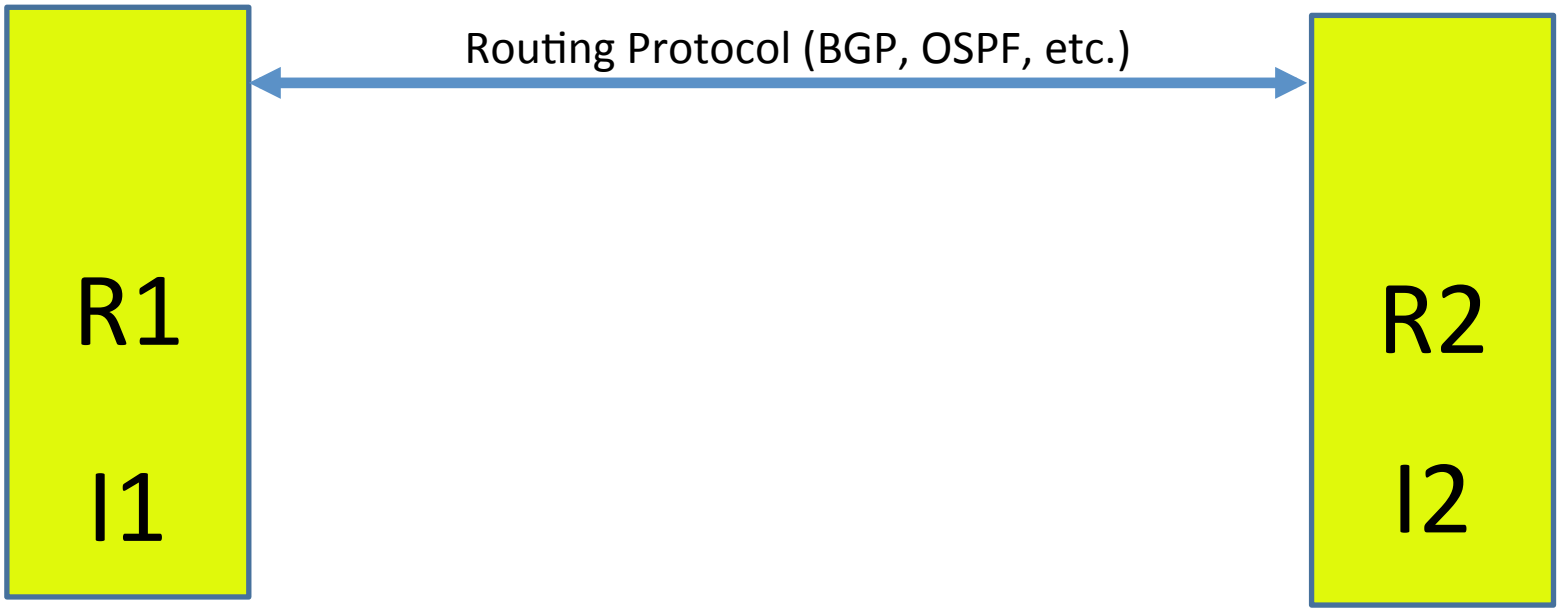
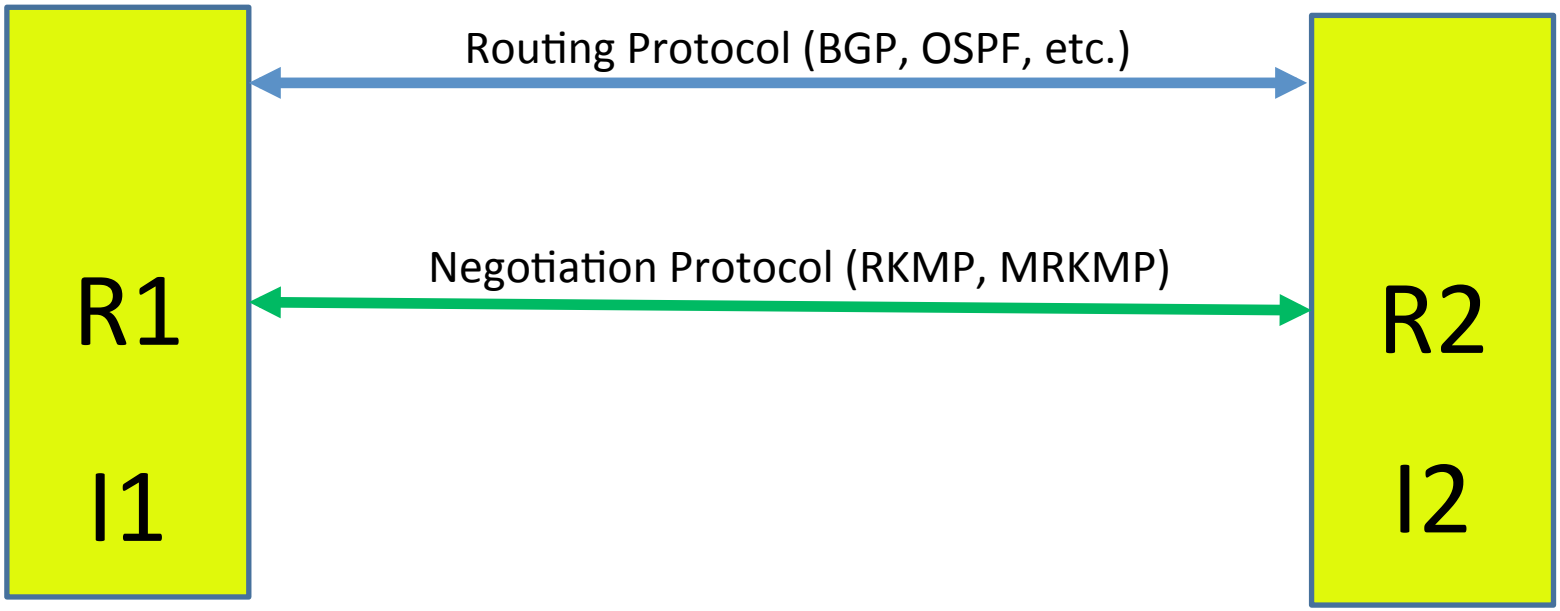
Authentication, Authorization and Policy Management for Routing Protocols

W. Atwood, R. Bangalore Somanatha
Concordia University/CSE
S. Hartman
Painless Security
D. Zhang
Huawei

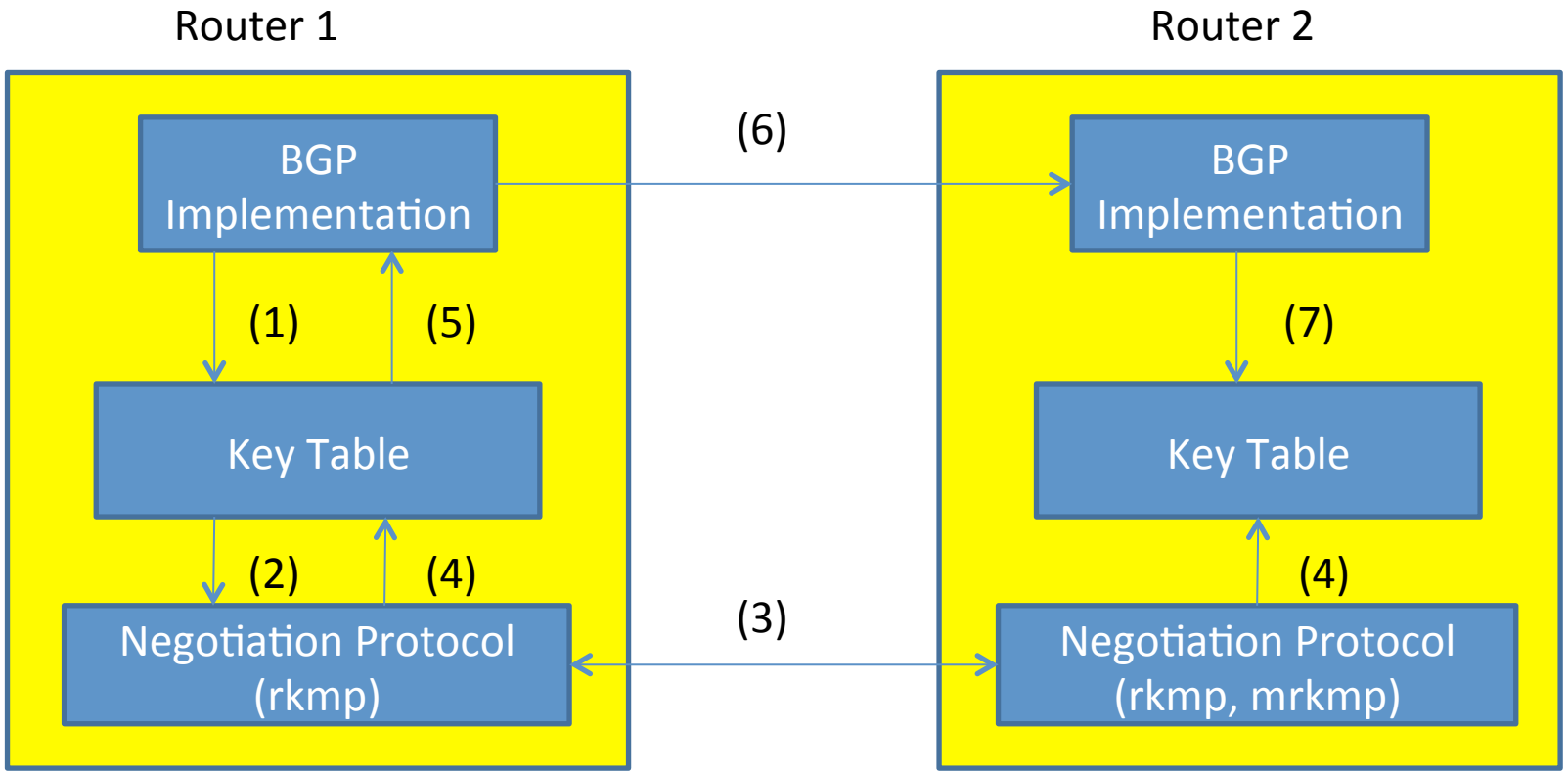
Motivation



Motivation (2)



Motivation (3)



Problem Statement

- Negotiation protocols need something like the crypto table to provide authentication and authorization
- Provide database to configure the negotiation protocol
- Propose management approach that ensures that the keying material for the routing protocol exchanges is distributed only to the appropriate routers.

Out of scope

- We are not concerned with the contents of the exchanged Routing Protocol messages; this is the responsibility of the Routing Protocol specification documents.
- We are also not concerned with the validity of the Routing Protocol messages themselves.

Routing Authentication Policy Database (1)

- This specification introduces a new conceptual database, called RAPD.
- The RAPD serves the following purposes:
  - Is automated key management expected for a particular routing protocol peer or group
  - What identity and credentials are used to authenticate to a remote key-management peer
  - What identities and credentials are accepted when a remote peer authenticates to us
  - Is a particular peer authorized for a particular routing protocol
  - What parameters and transforms are used for a particular security association
  - What key management protocols does this router need to participate in and on what interfaces

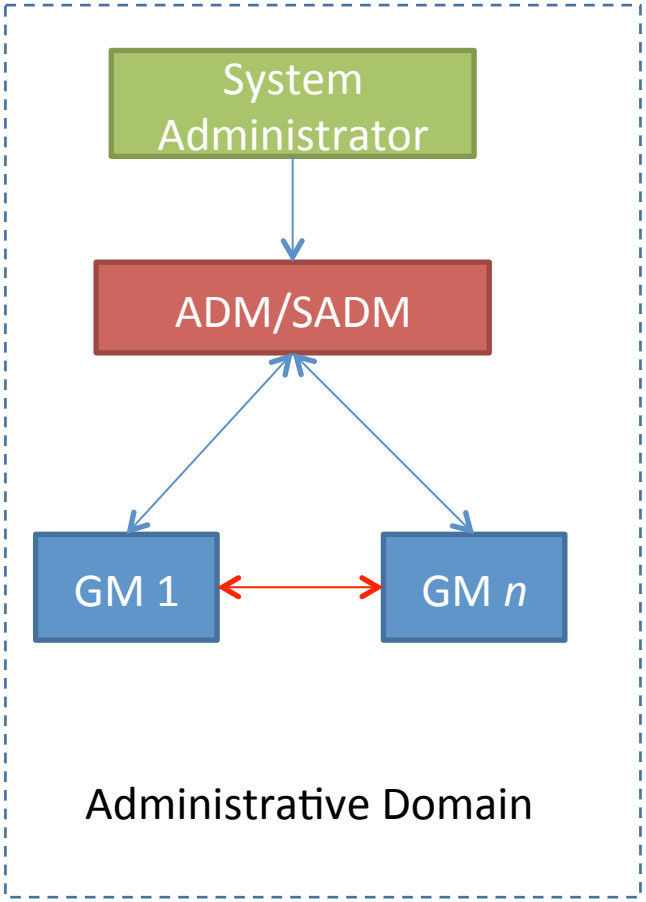
Routing Authentication Policy Database (2)

- According to the key table, routing protocols specify a peer and protocol in order to request a key to send a message. The peer is either the identity of a unicast peer or of a group. The form of the peer identifier is specified by the specific routing protocol in question.
- The peer and protocol are enough to find an existing key.
- As a result, the RAPD needs to be able to locate the appropriate automated key management policy given a peer and protocol. The RAPD is also used by key management applications when a peer attempts to authenticate or request a key. In this instance, the key management application has the IKE identity of the peer.

Routing Authentication Policy Database (3)

- In order to establish an IKE SA, the following information is needed:
  - Identity of the local system to use
  - Identities acceptable for the remote endpoint
  - Credential to use for the local system
  - Lifetime information
  - Acceptable transforms
  - Authentication information for the remote system
- In order to establish a routing SA keyed by an IKE SA, the following information is needed:
  - Peer and protocol
  - Acceptable transforms

System Overview



- For a particular routing protocol, the network is divided into one or more Administrative Domains (AD). An AD is a set of routers with a common policy.
  - System Administrator (SA) This is the human who controls the Administrative Domain.
  - Administrative Domain Manager (ADM) This is the manager for the entire AD. Its role is to distribute the operational policies to the routers within the AD.
  - Standby ADM (SADM) This provides for robustness if the ADM is unavailable.
  - Group Member (GM) Any router within the AD.
- Each router has a unique identity in the context of a particular AD.
- Authorization of a router involves matching the identity of that router against the policy governing the set of permitted neighbors.

System Operations

- The SA interacts with the ADM to set the policies for the AD.
- The ADM establishes a mutually authenticated relationship with each client router, i.e., with each GM in the AD.
- The ADM then pushes the policy definitions to the GMs.
- Based on the policy, each GM establishes a mutually authenticated relationship with each of its authorized neighbors.
- Each GM will then negotiate cryptographic parameters with its neighbors, or distribute the parameters that it generates, depending on the policy in place.

Operations During Router Installation

1. Establish the existence of a new router identity in the AD, using the SA - ADM interface.
2. Define the policy or policies that are applicable to this new identity, using the SA - ADM interface.
3. For the router that will be the first router on the network path between the new router and the ADM, take whatever action is necessary to force the ADM to push revised configuration information to it.
4. At the new router, manually install sufficient policy to allow it to accept its neighbor as part of its authorized neighbor set, and to allow it to know the location of the ADM. Then, force the ADM to push complete configuration information to it.

Operations During Reboots

- A router must store the information concerning its governing policies in a form of storage that persists over a reboot.
- When a router reboots (and especially when a large number of routers reboot due to a power failure and restoration), a router must use the stored information to re-establish its neighbor relationships. This will minimize the likelihood of an apparent denial of service attack on the ADM.
- Once the router has established its neighbor relationships, and after a suitable (random) interval, the router should contact its ADM to refresh its policy database.

Questions?