Multicast Security Group Key Management Architecture

draft-ietf-msec-gkmarch-07.txt

Internet Security

Tobias Engelbrecht

Agenda

- Introduction
- Requirements of a GKMP
- Design of the GKMA
- Rekey Protocol
- Group Security Association
- Security Considerations

Introduction

- Defines a common architecture and design for group key-management protocols (GKMP)

- Examples:
  - video broadcast
  - multicast file transfers

Requirements of a Group Key Management Protocol (GKMP)

Requirements of a GKMP

- A group key management protocol (GKMP)
  - supports protected communication between members of a secure group
  - helps to ensure that only members of a secure group gain access to group data (by gaining access to group keys) and can authenticate group data.

Requirements of a GKMP

- Members receive security associations (SA)
- The group owner may define and enforce group membership, key management, data security and other policies
- Keys have a predetermined lifetime
- Key material should be delivered securely to the members of the group

Requirements of a GKMP

- The key-management protocol should be secure against replay and DoS attacks
- The protocol should facilitate addition and removal of group members
- The key management protocol should provide a mechanism to securely recover from a compromise of the key material
- …

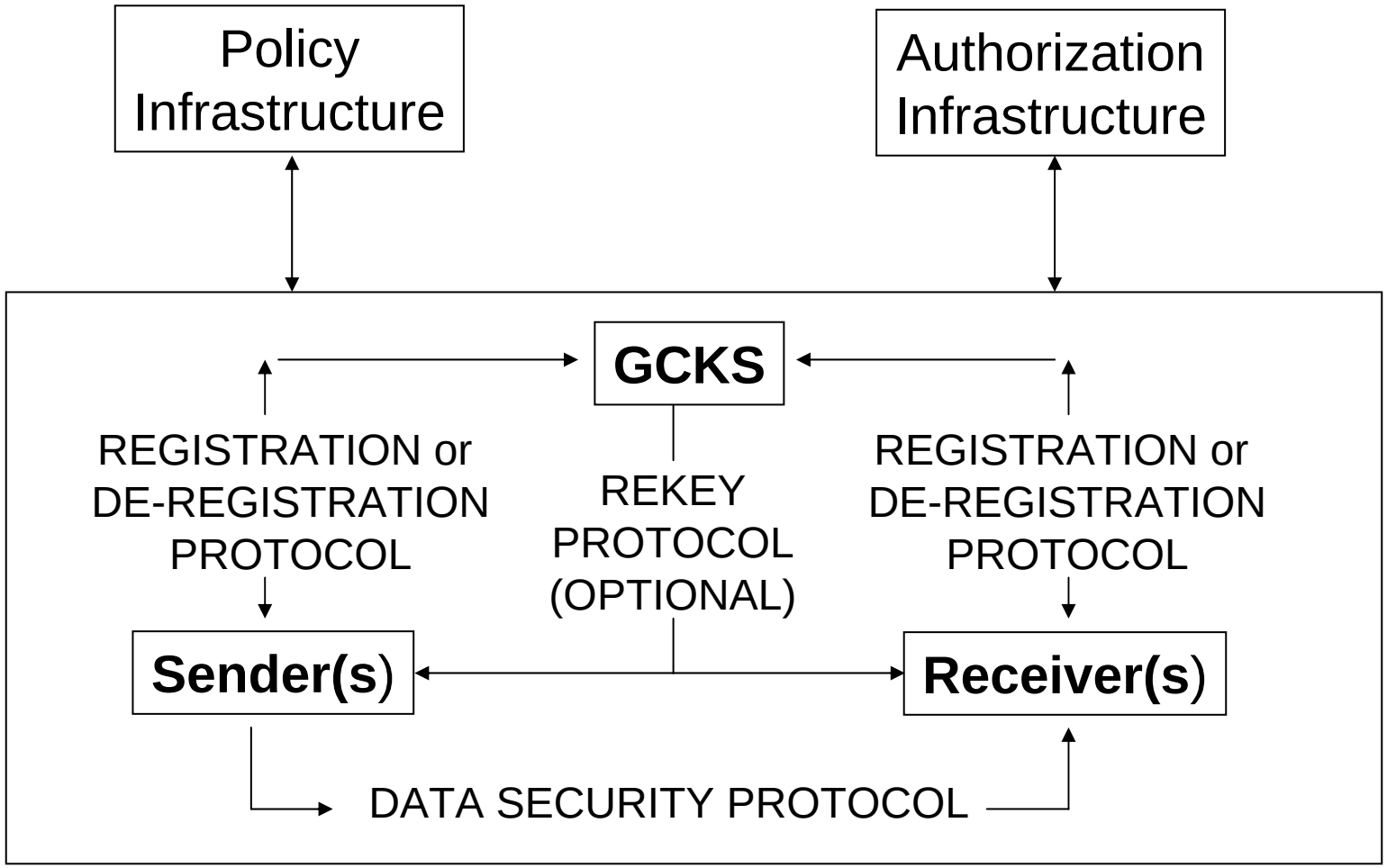
Design of the Group Key Management Architecture (GKMA)

Design of the Group Key Management Architecture (GKMA)

- The goal of a GKMP is to securely provide the group members with an up-to-date data security association (Data SA)

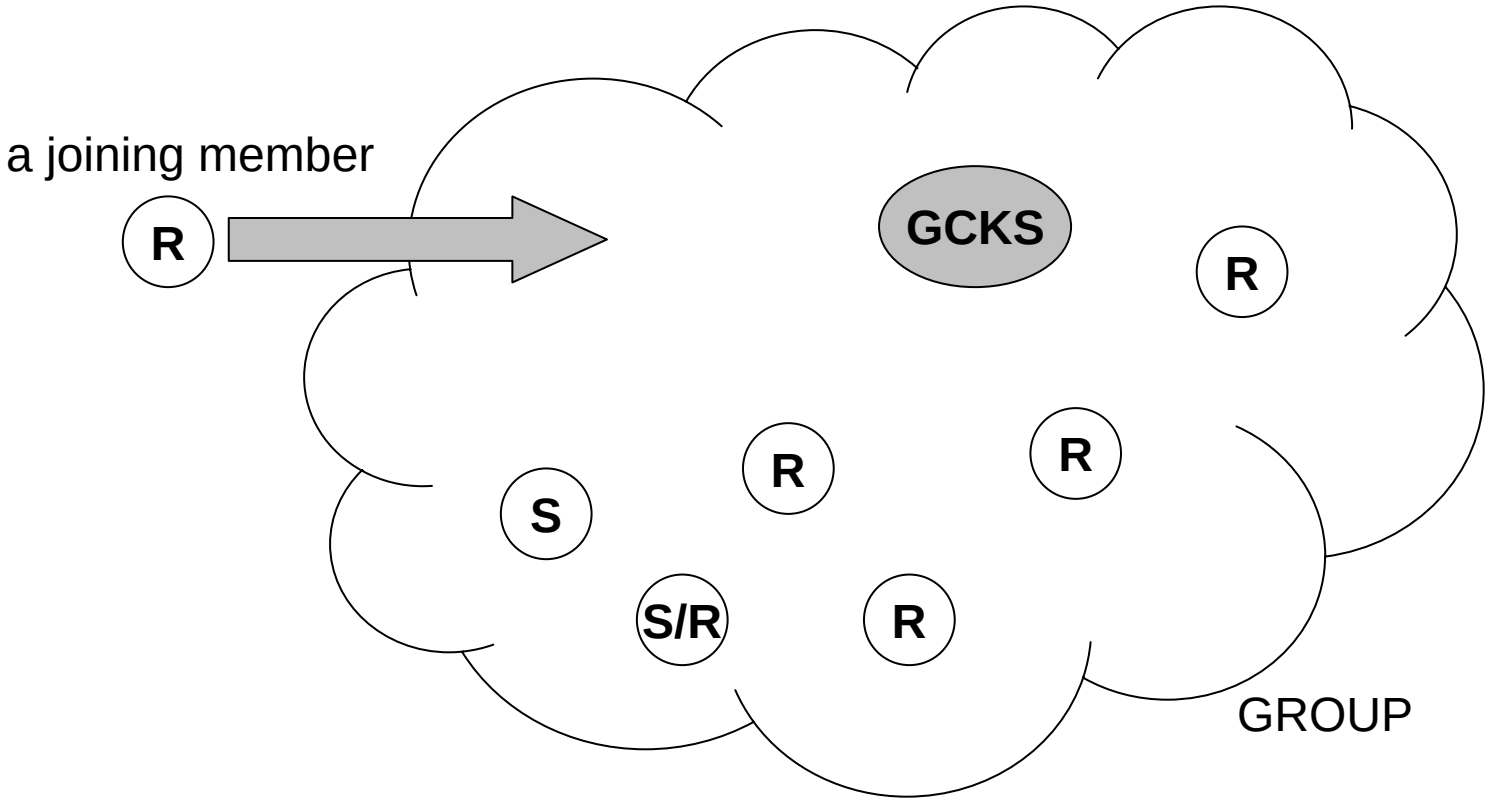
- GKMA Protocols
  - De- / Registration Protocol
  - Rekey Protocol

Design of the Group Key Management Architecture (GKMA)



Design of the Group Key Management Architecture (GKMA)

A new member joins the group:



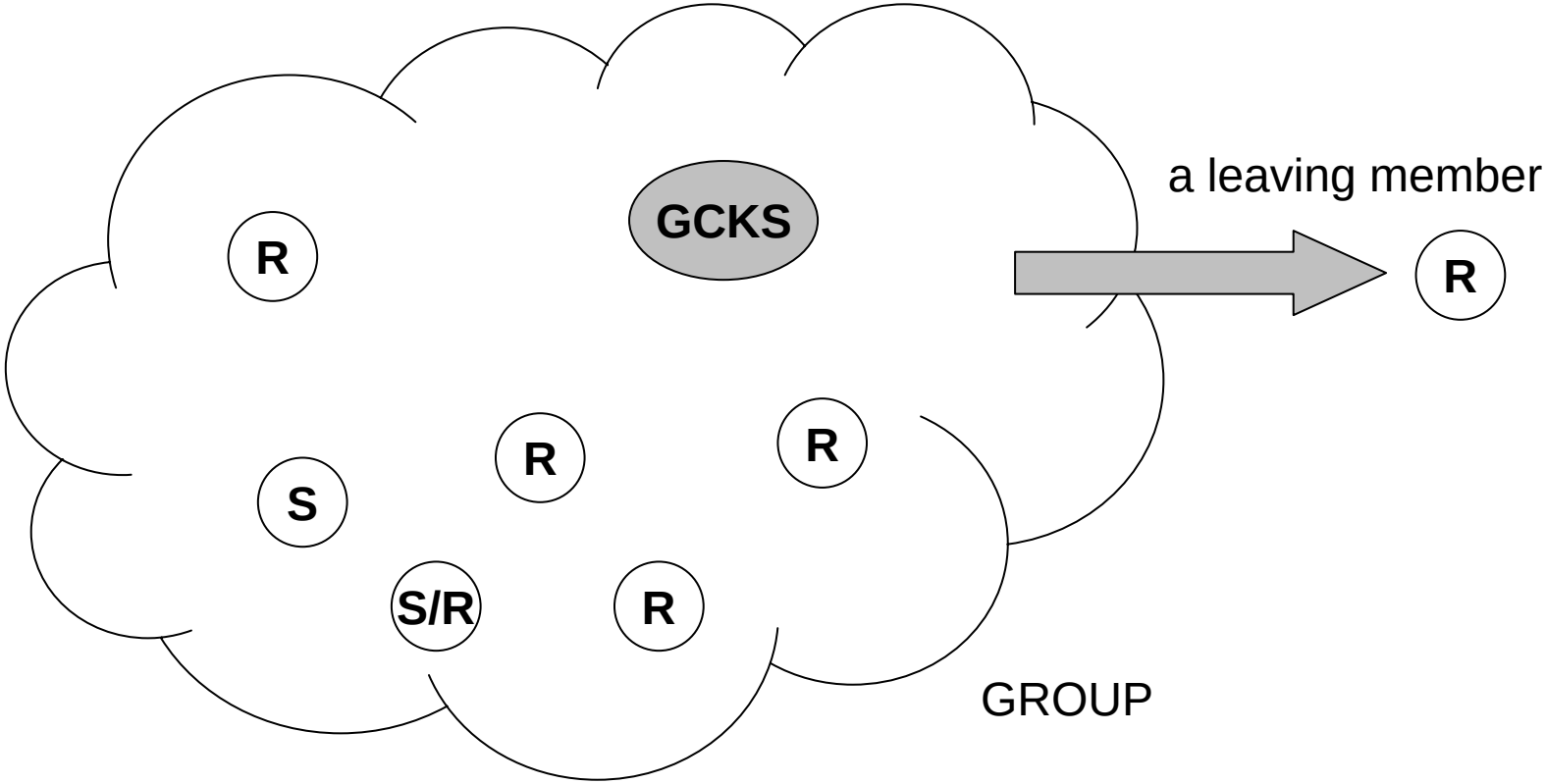
Design of the Group Key Management Architecture (GKMA)

Registration Protocol (RP)

- unicast protocol
- the GCKS and the member authenticates each other
- supplies the member with information to initialize a Data SA and a Rekey SA
- RP must ensure that the transfer is done over a Registration SA

Design of the Group Key Management Architecture (GKMA)

A new member leaves the group:



Design of the Group Key Management Architecture (GKMA)

Rekey Protocol

- multicast / unicast protocol from GCKS to members
- Rekey Messages are protected by the Rekey SA
- Rekey Messages update or change the Data SA and / or the Rekey SA

Design of the Group Key Management Architecture (GKMA)

Rekey Protocol

- Rekey messages are authenticated by
  - Source Authentication
  - Group Based Authentication
- ensures that all members receive the Rekey information in a timely manner

Design of the Group Key Management Architecture (GKMA)

- Group keys
  - key encryption keys (KEKs)
  - traffic encryption keys (TEKs)
- Traffic Protection Keys (TPKs) denote the combination of a TEK and a traffic integrity key
- Registration and / or Rekey Protocol establish the keys

Design of the Group Key Management Architecture (GKMA)

GCKS (Group Controller / Key Server)

- creates KEKs and TPKs
- performs authentication and authorization according to the group policy
- MAY present a credential to the group members signed by the group owner
- runs the Rekey protocol to push Rekey messages

Rekey Protocol

Rekey Protocol

Properties

- to ensure that all members receive the rekey information in a timely manner
- mechanism to re-sync keys
- avoid implosion problems

Rekey Protocol

Transport & Protection

- encrypted with the Group KEK
- authentication with MAC or digital signature
- sequence number protect against replay attacks
- reliable transport

Rekey Protocol

Implosion

- Reasons
  - all members contact the GCKS at the same time
  - packet loss (feedback implosion)
- Solutions
  - a member waits before sending an out-of sync or feedback message
  - a member contacts an other server

Group Security Association (GSA)

Group Security Association (GSA)

- consists of the Registration SA, Rekey SA (optional) and Data SA
- WITHOUT Rekey SA
  - Registration Protocol initializes and updates one or more DATA SA
- WITH Rekey SA
  - Registration Protocol initializes the Rekey SA
  - Data SA is initialized by the Rekey Protocol

Group Security Association (GSA)

Contents of the Rekey SA

- Policy
- Group Identity
- Key encryption keys
- Authentication Key
- Replay Protection
- Security Parameter Index (SPI)

Group Security Association (GSA)

Contents of the Data SA

- Group Identity
- Source Identity
- Traffic Protection Keys
- Sequence Numbers
- Security Parameter Index (SPI)
- Data SA Policy

Security Considerations

Security Considerations

- authenticated key exchange techniques limit the effects of man-in-the-middle and connection-hijacking attacks
- sequence numbers and low-computation message authentication techniques can be effective against replay and reflection attacks
- cookies can reduce the effects of denial of service attacks

Security Considerations

- sharing of secrets among a group of members can cause problems
- the Registration protocol should be so good as the base protocol on which it is developed
- the Rekey protocol is new and has unkown risks associated with

Thanks for your attention

Questions?