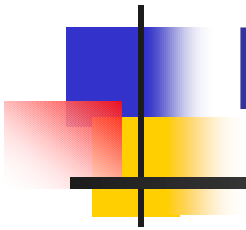


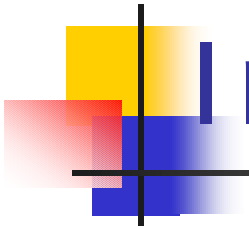
Rekey protocol

David McGrew/Cisco

mcgrew@cisco.com

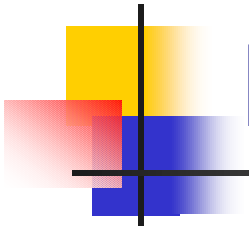
Lakshminath Dondeti/Nortel

ldondeti@nortelnetworks.com



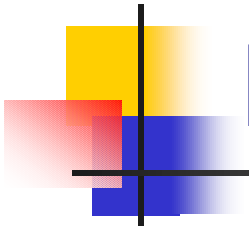
Introduction to rekey protocol

- Part of the GKM architecture
- Updates Rekey and Data Security SAs
- Used for fast rekeying of large and dynamic groups via key tree algms
- Our work independent of GSAKMP and GDOI
- KDC → member messages



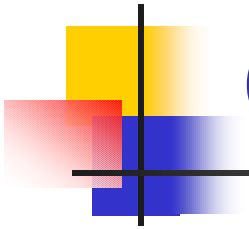
Rekey protocol issues

- Rekey message format(s)
- Key tree node numbering
- Optional secure back channel
- Subgroup communication to descendants of a sub-tree
- Others??



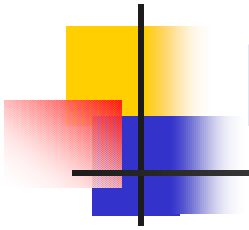
Rekey messages

- From the KDC to the members
- Sent via multicast or multi-unicast
- Reliable transport
  - External reliable channel
  - ALC/FEC
  - Repetition of messages
- May use key trees for efficiency
  - LKH/OFT/OFC and variations thereof



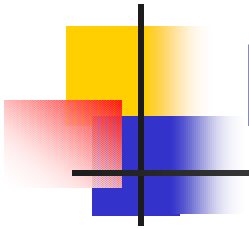
One or multiple messages?

- Group based rekeying
  - Send all rekeyed keys in one message
- Key based rekeying
  - Send each rekeyed key separately
- Tradeoffs
  - Not all members need all keys
  - KDC needs to sign multiple messages



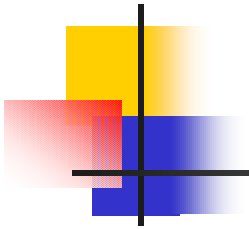
Key tree node numbering

- Natural number encoding
  - Numbering proceeds top to bottom and left to right
    - Root's ID is 1
- Binary string encoding
  - Parent's ID suffixed with 0 and 1 is given to left and right children



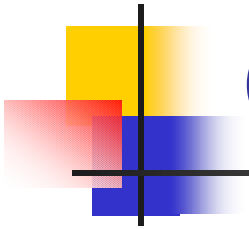
Rekey messages: our goals

- Rekey message should be able to handle
  - Group and key-based rekeying
  - Payloads for reliable transport
  - Transport of key tree related payloads
    - Key node ID changes
  - Different node numbering algorithms



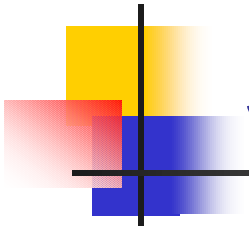
Member status messages

- Unicast from member to KDC
- Analogous to RTCP receiver reports
- KDC does not need to process or change state
- KDC processes as many as it can



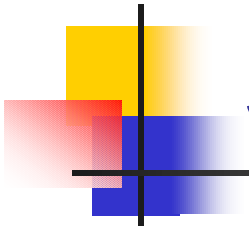
Optional back channel

- Usage
  - Member status messages (for FEC/ALC)
  - Leave/Renew notifications
    - DeRegistration protocol
- Optional !
  - When using external reliable transport
    - How do we secure retransmissions?
  - DeRegistration via an upper layer protocol
- How to secure the back channel
  - Do we keep SA1 (Reg. SA) around?
  - Other solutions?



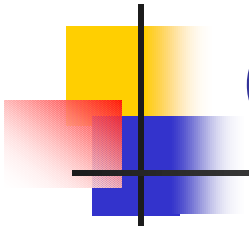
Subgroup communication

- Consider descendants of an internal node in the key tree
  - They all share a key
  - Could be considered as a subgroup for secure communication
- Issues
  - SA maintenance
  - Others?



Summary and Conclusion

- Rekey protocol is part of GKMArch
- Current model is to send a single message
  - using repetition for reliability
  - over external reliable channel
- We propose a rekey protocol that/with
  - supports group and key-based rekeying
  - provides increased support for reliable transport of rekey messages
  - support for key tree management



Open issues

- Should we have an optional back channel?
  - What should it be used for?
- Should we allow subgroup communication?
- Rekey message encoding and compatibility with GSAKMP and GDOI