CSC 774 Advanced Network Security

Topic 5.3 Group Key Distribution

Acknowledgment: Slides on LKH were originally provided by Dr. Wensheng Zhang at Iowa State.

Outline

• Overview of group key distribution
• A naïve solution
• Iolus: A Framework for Scalable Secure Multicasting
• Logical key hierarchy (LKH)
Group Key Distribution

- Group session keys are determined by the group manager
  - Usually used for large groups.

A Naïve Solution

- Use a separate secure unicast connection from the group manager to EACH group member.
- Requirement
  - Each client shares a unique key with the controller.
- Poor scalability:
  - n-1 secure unicast connections
  - n secret keys
Problems Specific to Group Communication

• “1 affects n” problem
  – The actions of one member affects the entire group

  Group key manager

    Old members

    New member joins

Problems Specific to Group Communication (Cont’d)

• “1 does not equal n” problem
  – Cannot deal with the group as a whole
  – Must consider the conflicting demands of members on an individual basis

  Group key manager

    Group members

Example: Cannot use the old group key to distribute the new group key.

Member leaves
Iolus

- Divide a large group into smaller groups
- Introduce entities that manage and connect the subgroups
  - Group security controllers (GSC)
    - Control the entire group
  - Group security intermediaries (GSI)
    - Control the subgroups on behalf of GSC
  - GSC and GSI are both referred to as group security agent (GSA)
  - With GSC as the root, GSAs form a hierarchy of subgroups
    - A lower-level GSA is a member of the group headed by the higher-level GSA

Iolus (Cont’d)
Iolus (Cont’d)

• **Joins**
  – GSA generates $K_{GSA-MBR}$
  – Store this key along with other information
  – Send $K_{GSA-MBR}$ to the new member in a secure channel
  – Generate a new group key $K’_G$
  – Send $\{K’_G\}K_G$ to the group
  – Send $K’_G$ to the new member in a secure channel

• **Leaves**
  – Generate a new group key $K’_G$
  – Send $K’_G$ to each member MBR individually in the secure channel encrypted with $K_{GSA-MBR}$
Iolus (Cont’d)

- Data transmission
  - Data retransmitted within each subgroup

Iolus (Cont’d)

- Iolus for group key management
  - Replace the data with the group key in data transmission
Key Tree Approaches

- Two types of keys
  - SEKs (Session Encryption Key)
  - KEKs (Key Encryption Key)
- A Group Controller constructs a tree based hierarchy of KEKs

Logical Key Hierarchy (LKH)

- Keys are organized in a (logical) hierarchical tree
  - Group key is located at the root
  - Key encryption keys are the non-root, non-leave nodes
  - Members are located at the leaves
- Updates the group key and the key encryption key by means of the encryption of key-nodes
- Rekey with only $O(\log N)$ messages
LKH (Cont’d)

• Initialization

\[ K_0 \]
\[ \xrightarrow{\text{GKCs}} \]
\[ N \text{ secure channels} \]

\[ K_{11} \]
\[ K_{12} \]
\[ K_{22} \]
\[ K_{23} \]
\[ K_{24} \]

\[ M_1 \]
\[ M_2 \]
\[ M_3 \]
\[ M_4 \]
\[ M_5 \]
\[ M_6 \]
\[ M_7 \]
\[ M_8 \]

LKH (Cont’d)

• Member leave

\[ \ln(N) \]
\[ \ln(d) \]

Rekeying Messages

\[ K_0 \rightarrow K_0' \]
\[ K_{34}[K_{11}'] \]
\[ K_{35}[K_{12}'] \]
\[ K_{21}[K_0'] \]
\[ K_{22}[K_{11}'] \]
\[ K_{23}[K_{22}'] \]
\[ K_{24}[K_0'] \]

\[ K_{11} \rightarrow K_{11}' \]

\[ K_{21} \]
\[ K_{22} \]
\[ K_{23} \]
\[ K_{24} \]

\[ M_1 \]
\[ M_2 \]
\[ M_3 \]
\[ M_4 \]
\[ M_5 \]
\[ M_6 \]
\[ M_7 \]
\[ M_8 \]
LKH (Cont’d)

• Member join

\[ \frac{\ln(N)}{\ln(d)} \] Rekeying messages

GKCs

\[ K_0 \rightarrow K_0' \]

\[ K_1 \rightarrow K_1' \]

\[ K_2 \rightarrow K_2' \]

\[ K_3 \rightarrow K_3' \]

\[ K_4 \rightarrow K_4' \]

\[ K_5 \rightarrow K_5' \]

\[ K_6 \rightarrow K_6' \]

\[ K_7 \rightarrow K_7' \]

\[ K_8 \rightarrow K_8' \]

\[ \{ K_1' \}, \{ K_2' \}, \{ K_3' \}, \{ K_4' \}, \{ K_5' \}, \{ K_6' \}, \{ K_7' \}, \{ K_8' \} \]

\( \text{(Cont)} \)

\( \text{Member join} \)