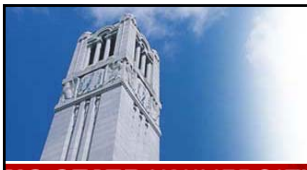


NC STATE UNIVERSITY Computer Science

# Logical Key Hierarchy Protocol

March 31, 2003

Yiquan Hu



## Overview

- Internet Draft, expired on Aug. 30, 1999
- Presents an implementation of Logical Key Hierarchy (LKH) Compromise Recovery (CR)
- Supplement of RFC2627: *Key Management for Multicast: Issues and Architectures*

## Outline

- Background
  - Security for Multicast
- Compromise Recovery
  - Definitions, CR Policy, Requirements
- LKH CR Protocol Specification
  - Group Establishment, CR Policy and Enforcement
- Recommendations
- Summary



## Background - Security for Multicast

- Multicasting allows a group of participants to communicate efficiently between themselves using public networks.
- Security has been a key area holding back widespread adoption of multicast.
- Challenge: providing effective method of controlling access to the group.
- Primary method: encryption of group information and selective distribution of the keys

## Security for Multicast (Cont'd)

- Mechanisms used to secure the data while it is in transit between the multicast group members.
- Management of the security groups.
  1. Creation and distribution of keys.
  2. Enforcement of access control policies.
  3. Operational control (e.g., compromise recovery, rekey, identy infrastructure issues).



## Outline

- Background
  - Security for Multicast
- Compromise Recovery
  - Definitions, CR Policy, Requirements
- LKH CR Protocol Specification
  - Group Establishment, CR Policy and Enforcement
- Recommendations
- Summary

## Compromise Recovery - Definitions

- A group is a gathering of communicating members with a single key.
- If the group key is compromised, the secure communication must be restored through a recovery action.
- A compromise occurs when a member of the group can no longer be trusted (e.g. group member loses their key or a group member's key is stolen).
- When this happens, the group needs to change the compromised keys, without giving the new keys to the compromised member.



## Compromise Recovery Policy

- Restoration of Secure Network Operations
  - quickly and efficiently
- Restrict Compromise Recovery Actions to Authorized Individuals
  - Only authorized individuals should be allowed to identify that a compromise has occurred, assess the risk, and implement the necessary CR action.
- Secure Compromise Recovery Life-Cycle
  - Generation of CR materials, establishment of the CR group, execution of recovery from and event, and termination of CR for a group.
- System Stability After a Compromise
  - The outcome of any compromise event and the resulting CR action must leave the group capable of recovering from another compromise.

# Compromise Recovery - Requirements

- Generation of LKH Arrays
  - Must be protected from unauthorized access.
- Generation of Support Materials
  - The LKH CR process will be supported by certificates.
  - The mechanisms and processes within the certificate registration process must be verifiable and protected from unauthorized access and disclosure.
- Secure Compromise Recovery
  - Identifying all group members
  - Identifying all CR agents
  - Verifying the authority for all sensitive acts
  - Verifying the integrity of all data exchanges
  - Protecting all information that could be used to attack the CR system
  - Verifying the assurance level of all CR computer components



# LKH CR Requirements (Cont'd)

- Normal Operation Requirements
  - Minimal Exposure of LKH Arrays
  - Authentication of Identities
  - Verification of Authorization
  - Computer Security Trust Requirements
  - Cryptographic Structure of Groups
  - CR Message Requirements
  - Compromise Event Discovery and Reporting

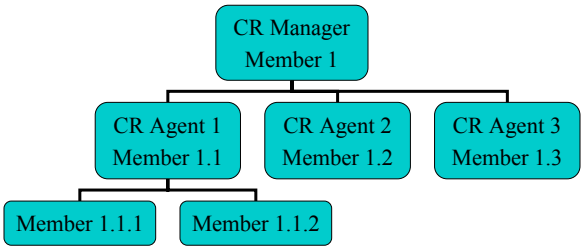
## Outline

- Background
  - Security for Multicast
- Compromise Recovery
  - Definitions, CR Policy, Requirements
- LKH CR Protocol Specification
  - Group Establishment, CR Policy and Enforcement
- Recommendations
- Summary



## Group Establishment

- A large group can be serviced by several independent CR Agents each controlling a subset of the CR domain.



## Generation of LKH Array

- Method 1: CR Manager generates a very deep array capable of encompassing all the potential members of the group
- Method 2: CR Manager generates a smaller array capable of recovering all CR Agents. Each agent generates LKH array for his branch members.
  - Greater scalability for large groups
  - CR Manager and CR Agents must be identified to the group members prior to group establishment.



## Distribution of LKH Array to Group Members

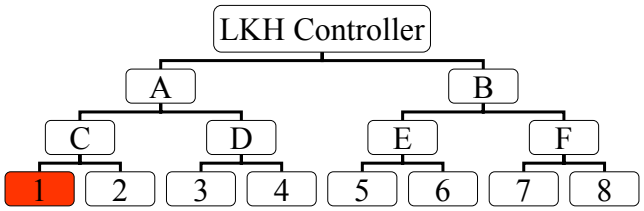
- The generator of the LKH array could distribute pieces of the array to authorized distribution points within the group for subsequent distribution.
- Establishment of SA (ISAKMP like)
  - Verification of all identities
  - Validation of public certificates (if used)
  - Creation of a pairwise traffic confidentiality key
  - Transfer of identity and certificate information to multicast security management protocol

## Recovery Protocol

- CR Manage sends CR message to all members of its domain using the multicast address of the group.
- Each member verifies that the CR message is authentic and that the signature on that message comes from a party that is authorized to send a CR message.
- Each CR message contains a Date/Time stamp
  - CR messages are processed according to timestamp order.



## CR Message Example




- Letters – virtual nodes
- Numerals – member nodes
- Member 1 is compromised

## Example (Cont'd)

- Recovery Message:
  CompHdr{[Sec HdrB(MGK')B],
  [SecHdrD(MGK',A')D],
  [Sec Hdr2(MGK',C',A')2]
  }Siglkhc
- Notation:
  - CompHdr{} = CR message header
  - [SecHdr*(MGK').] = Data packet containing a security header that allows the decryption of the data package encrypted in key * (in this case, the data packet contains MGK: Multicast Group Key Prime)
  - {}SigXo = Public key signature of data contained within {}, public key to verify is Xo.



## Single Message to Exclude Compromised Member

- The CR Manager has been notified of the compromised status of member 1.
- The CR Agent in the compromise path generates a message using keys stored in its database that will exclude the compromised member from receiving the new group key:

CompHdr{[SecHdrB(MGK0)B];
[SecHdrD(MGK0;A0)D];
[SecHdr1:1:2(MGK0; C0; A0)1:1:2]
}SigX1:1

- All nodes in the subgroup receive the message and each authorized member decrypts the new traffic key.

## New Group Key

- The CR Manager sends a combination message to the delegated CR Agent (Member 1.1).
  - Notifies the compromise of its sub-nodes
  - Passes the new secure group key
- The CR Agent updates its group key, then begins CR actions for his domain



## Summary

This document presents a Logical Key Hierarchy (LKH) Compromise Recovery (CR) implementation for the key management protocol suggested in RFC2627

- Defines the CR method
- Identifies the requirements
- Defines the operational protocol
- Recommends an implementation

# Questions?