CERIAS

the center for education and research in information assurance and security

Efficient and Flexible Attribute Policy Based Key Management

Mohamed Nabeel, Elisa Bertino
Department of Computer Science, Purdue University

Scalable, efficient and flexible key management is essential for many secure systems/services

Location based services

Cloud/outsourced storage services

Content dissemination

Multimedia streaming

Control access to content/service → Encryption → Group key management

A large group of users

Service/access provided to subsets of users

Users may collude

Common characteristics

New users join

Existing users leave

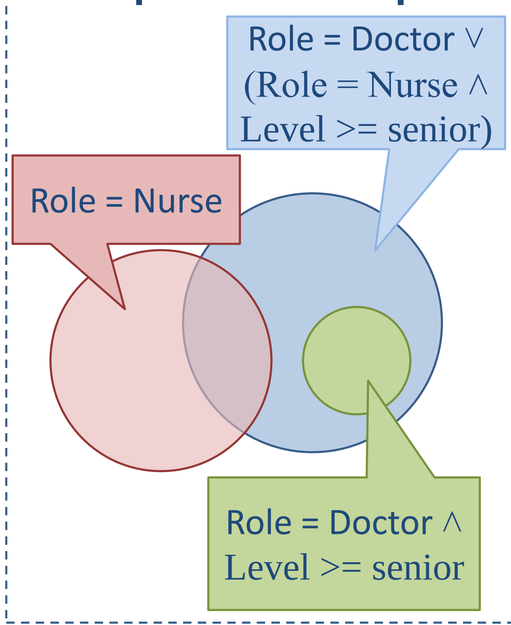
Dynamic nature of groups

User attributes change over time

Requirements

1. Forward/backward secrecy
2. Collusion resistance
3. Transparent join/leave (Stateless - Efficiency)
4. Flexible group policies (attribute based)
5. Single encryption

Group membership



Our key techniques

Any **broadcast GKM** scheme → *Subset-Cover* techniques → *Sub-linear* BGKM

Provide users **secrets** for each **attribute condition** → Construct a BGKM per attribute condition → Construct an **access tree** based on the policy using BGKMs as leaves

Threshold membership policies (Key derivation)

$q_1(0) = q_i(x)$

Each user is assigned a *unique* polynomial of degree *d - 1*

Attr Cond$_1$ (s$_1$) → BGKM$_1$
Attr Cond$_2$ (s$_2$) → BGKM$_2$
Attr Cond$_3$ (s$_3$) → BGKM$_3$
. . .
Attr Cond$_m$ (s$_m$) → BGKM$_m$

Polynomial interpolation with *d* intermediate keys

OR → *1*-out-of-*2*
AND → *2*-out-of-*2*
General → *d*-out-of-*m*

Bottom-up

Any monotonic membership policy (Keygen)

$q_1(x)$ n_1

Threshold = t_x
# children = n_x
$q(x)$ = degree $t_x - 1$ polynomial

$q_2(x)$ n_2 → $q_2(0) = q_1(2)$
$q_3(x)$ n_3 → $q_3(0) = q_1(3)$
$q_4(x)$ n_4 → $q_4(0) = q_1(4)$
. . .
$q_m(x)$ n_m → $q_m(0) = q_1(m)$

Continue until leaf nodes are reached

Internal nodes → Threshold gates
Leaves → BGKM instances

Top-down

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center