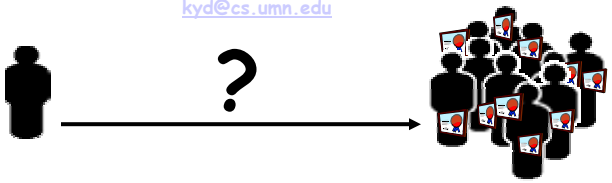
Admission Control in Peer Groups

Gene Tsudik, School of ICS, UC Irvine
gts@ics.uci.edu
Yongdae Kim, CS Dept., U. of Minnesota
kyd@cs.umn.edu



Challenge: HOW TO ADMIT NEW MEMBERS SECURELY?

Peer Groups:

- Any-to-any
- No hierarchy
- No centralized authority
- Common in MANETs
- Many Internet applications (e.g., content sharing)
- Security mechanisms difficult
- Prior work mostly in key mgmt and secure comm.
- Not really useful without admission control
- Also need revocation mechanisms (but admission must be solved first)

Group Membership Issues

- **Naming: Does name ➔ ownership? Location?**
- **Presence:**
  - **on-line: e.g., replicated servers, MANETs**
  - **off-line: e.g., Gnutella, MANETs**
- **Membership:**
  - **Static: reflected where?**
  - **Enumerated**
  - **Dynamic: admission rules/policies?**
- **Longevity:**
  - **Long-term**
  - **Transient**

What does a prospective member know?

- Group name, at least…
- Group location?
- Group membership?
- Group charter/policy?
- Group member(s)' name(s)/address(es)?
- LDAP? DNS? What about transient groups?

Group Charter



- **Admission policy must be available to prospective members**
- **1st step: embed in a group charter**
- **Who signs group charter?**
  - **Owner/Founder? ← how to confirm ownership?**
  - **Charter members? ← "peer"?**
  - **Current members? ← who are they?**
    - **Or fraction thereof?**
  - **CA? ← natural choice**

Contents of Group Charter:

- Group name
- GAUTH
- Admission Policy Type (APT)
- APT-dependent data
- Issuer Name
- Signature

Group Authority

- Group charter must be available to prospective members
- Where does it come from?
- Who vouches for membership?
  - Owner/Founder?
  - "Charter" members?
  - Current members or fraction thereof?
  - CA?
  - Group Authority (GAUTH)? ← natural choice
    - Must be specified in group charter
    - GAUTH's placement (e.g., in/out of group)
    - Composition of GAUTH (e.g., one or multiple entities)

Sample Admission Policy Types

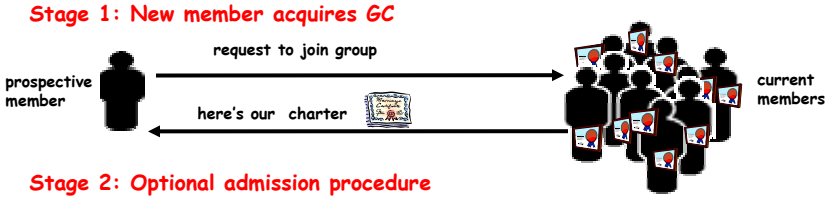
- APT_ACL: easiest, no GMCs, no GAUTH
- APT_GAUTH: discretion of GAUTH
- APT_GROUP: collective
  - STATIC: fixed "t" or explicit subset
  - DYNAMIC: fractional
- Any combination of the above… (no policy too weird)

Three Stages of Admission

Stage 0: GC creation (off-line)



Stage 1: New member acquires GC



Stage 2: Optional admission procedure

→ We focus on this ←

Stage 3: GAUTH issues a GMC



Relevant crypto techniques (usable in Stage 2)

Plain Signatures

- Inefficient: O(n) size, O(n) work
- Can be gathered asynchronously
- Can be used to prove membership
- No membership awareness
- Accountability easy
- Limited anonymity
- Linkable

Accountable sub-Group Multi-Signatures

- Due to Ohta, et al. (CCS'01)
- Based on aggregated Schnorr signatures
- Efficient (but still linear in size)
- Synchronous (on-line protocol)
- Membership awareness
- Can be used to prove membership
- Accountability easy
- Limited anonymity
- Linkable

Threshold Signatures

- Desmedt/Frankel (1989) and others
- Usually, fixed t
- Function sharing to avoid reconstr-n
- Inefficient
- Synchronous (on-line protocol)
- Membership awareness (partial, t)
- No Accountability
- Limited anonymity
- Linkable?
- Need trusted dealer to set up

Dynamic Threshold Signatures

- Frankel, et al. (FOCS'97)
- Supports shrinking t
- Very inefficient
- Synchronous (on-line protocol)
- Membership awareness (partial)
- No Accountability
- Limited anonymity
- Linkable?
- Still need trusted dealer

Relevant crypto techniques (contd.)

Better Dynamic Threshold Signatures

- Kong, et al. (ICNP'01)
- Supports growing t
- Efficiency unclear
- Synchronous (on-line protocol)
- Membership awareness (partial)
- No Accountability
- Limited anonymity
- Linkable?
- Still need trusted dealer to set up

Group Signatures

- Chaum & Van Heijst (1991) and others
- Inefficient (relative to plain sigs.)
- Asynchronous
- No membership awareness
- Can be used to prove membership
- Ltd. accountability (off-line, by Group Mgr)
- Anonymity
- Not linkable (except by Group Mgr)

Summary of Key Features

Signature Type	Prove membership	On-line presence	Membership awareness	Accountability	Anonymity	Unlinkability
Plain	YES	NO	NO	YES	YES	NO
ASM-s	YES	YES	YES	YES	YES	NO
Threshold fixed	NO	YES	NO	NO	YES	YES
Threshold dynamic	NO	YES	YES	NO	YES	YES
Group	YES	NO	NO	NO*	YES	YES*

Goals

- Investigate/assemble/implement mechanisms for peer group admission control
- Define formats for group charter and group membership certificates
- Design a "generic" group authority
- Develop a toolkit suitable for many APT-s and experiment!

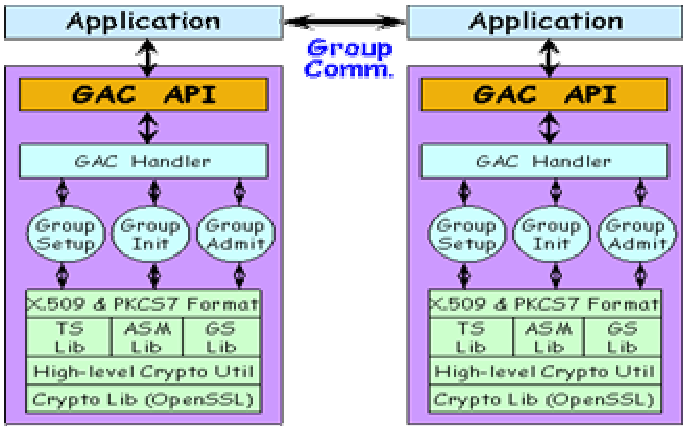
Anticipated "headaches":

- Negative "voting" in stage 2
- Dynamic revocation of membership (procedures, policy)

Related Work:

- Policymaker (AT&T Research) – general policy framework
- Trustbuilder (UIUC) – allows admission policy expression
- Antigone (UMich) – stages 1&2 of large mcast (not peer!) groups

Preliminary "architecture"



GAC = **G**roup **A**dmission **C**ontrol

For more info (including a paper) see:
http://sconce.ics.uci.edu/gac