Integrated Security Services for Dynamic Coalition Management

Himanshu Khurana

Electrical and Computer Engineering Department,
University of Maryland
College Park, Maryland 20742

DARPA DC PI Meeting
July 25, 2003
Honolulu, Hawaii
Integrated Security Services for Dynamic Coalition Management

**Project Title:** Integrated Security Services for Dynamic Coalition Management

**Project Start Date:** March 15, 2000

**Project Duration:** 36 months

**Options:** None

**Contract No:** F30602-00-2-0510

**Agent POC:** Brian T. Spink, AFRL/IFGB, Rome Research Site

**Personnel:**

Virgil D. Gligor (PI) ECE UMCP, gligor@eng.umd.edu
John S. Baras (Co-PI) ECE/CS/ISR UMCP, baras@isr.umd.edu

Research Associate: Himanshu Khurana

Faculty Research Assistant: Serban Gavrila

Graduate students: Vijay Bharadwaj, Rakesh Bobba, Emilian Dinu, Radostina Koleva, Anuja Sonalker, Gelareh Taban
Recent Work

• Coalition-Resource Management Tools: Architecture, Implementation for Supporting Coalition Dynamics (Demo Wednesday)
  – Supporting Coalition Dynamics requires Methods and Tools for
    • Wholesale, selective distribution and revocation of access permissions
    • Repeated negotiation of common access state
    • Review of the common access state
  – Performance measurements illustrate support for dynamic domain joins and leaves in minutes/hours (vs. weeks using current techniques)
Dynamic Coalitions

• Formed by autonomous domains to achieve a common objective by sharing resources
  – E.g., commercial research and development, health care, public emergency response teams, joint military task forces
  – Shared Resources – objects, applications, services

• Support Dynamic changes of membership
  – Member join / departure at any time after coalition creation/setup
  – Member join / departure must not require new coalition creation from scratch

• Support Dynamic Sharing of Coalition Resources
  – Achieved by distribution of access permissions for resources
  – Based on resource-sharing agreements, or common access states
Private Resource Sharing
Joint Administration of Access Policies

Joint Creation:
Coalition Attribute Authority (AA)

Domain 1
CA1
ID Cert.
Admin_D1

Domain 2
CA2
ID Cert.
Admin_D2

Domain 3
CA3
ID Cert.
Admin_D3

Threshold Attribute Certificate

Joint Access Request

Coalition Web Server
ACL write
Object O

ACL
Object O
Requirement: Wholesale, Selective Distribution and Revocation of Permissions

- **Wholesale**: distributed to (revoked from) *all users* of the joining (departing) domain
  - For both privately and jointly administered resources

- **Selective**: need to selectively target users of the departing/joining domain
  - Cannot exclude a member domain simply by modifying CA trust relations
    - Trust relations needed to share resources with that domain as part of other operations and applications
Requirement: Repeated Negotiation of Common Access States (CAS)

• Negotiation process is time-consuming and error-prone
  – Even when number of domains is small (3 – 7)
  – Number of objects is large; e.g., a joint task force may choose from tens of applications to be shared by hundreds of users
  – Number of negotiation rounds may be large

• Negotiation process is repetitive
  – Undertaken multiple times as domains join and leave the coalition
    • Domain may leave voluntarily or involuntarily (based on a majority decision)
Requirement: Review of the Common Access State

• **In general, review required to:**
  – View (very large) access matrix along desired lines; e.g., subject permissions for a specific application, application access to specific objects
  – Verify satisfaction of policies and constraints; e.g., SOD policies, obligation constraints

• **Common Access State Review required to:**
  – Specify access control policies of shared coalition resources
  – Verify satisfaction of constraints and policies in the presence of administrative actions
- Domain A allows local users to write to the Intelligence Database via role membership
- However, Domain A does not want foreign domain users to be able to write to the Database
To specify access policy for sharing Patient Database:

- Domain A reviews permissions of roles for Intelligence Database access
- Creates roles and permissions such that any write action must be approved by local domain user
- Creates a separation-of-duty (SOD) constraint to be verified against the negotiated common access state
CAS Review in the Presence of Administrative Actions

- Over time, an administrator (in error or oversight) might
  - Assign a foreign domain user to a role that inherits (from a role hierarchy) approve permissions for Intelligence Database

- Review is required to ensure satisfaction of defined SOD constraint
  - at (pre)defined intervals, or
  - at every administrative action (to prevent violation)

- Current CAS may not satisfy all constraints of the negotiated common access state as a result of administrative actions
  - Necessary to review constraint satisfaction prior to re-negotiating CAS to ensure that negotiation process begins in a secure state
Tools for Supporting Coalition Dynamics

We provide support for coalition setup and coalition dynamics over the internet.
Component Development

- **Operating System**: Windows 2000 Server
- **Access Control Policy**: RBAC Tool (Role Control Center-RCC) - Java
  - *Initially developed by VDG Inc with partial NIST support*
- **Certificate Authority**:
  - Windows 2000 Server Stand-Alone Identity CA
  - Domain Access CA - Java
  - Shared Access CA (**Yalta – NC State, MCNC**) – Java
  - Shared Access CA (**ITTC – Stanford**) - C
- **Group Communication**
  - Key Management Tool – Java
  - Server: Windows IIS Web Server – ASP
  - Multicast Communication Toolkit: **SPREAD (JHU)**
- **Application Server**: Windows IIS Web Server
  - Access to website using certificates (X.509 v3) over SSL
Experimental Setup

- **Coalition comprises three to five domains each with**
  - Ten applications that it shares with the coalition (private resources)
  - Ten roles that have permissions for the shared applications
  - Fifty users that get assigned to foreign domain and jointly administered roles for access to shared applications

- **Coalition sets up a joint coalition authority with**
  - Ten jointly administered applications
  - Ten roles with permissions for these applications

- **Events measured**
  - Time for Coalition set up (coalitions of 3, 4 and 5 domains)
  - Time for domain joining a coalition of 3 domains
  - Time for domain leaving a coalition of 4 domains
  - Measurements taken on 1 to 1.8 Ghz machines connected by a 100 Mbps LAN
## Coalition Setup

<table>
<thead>
<tr>
<th>Number of Domains</th>
<th>Shared-Key Generation (1024 bits)*</th>
<th>Importing CAS</th>
<th>Distributing Certificates for Jointly owned resources</th>
<th>Distributing Certificates for private resources</th>
<th>Total Time **</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ITTC ++</td>
<td>YALTA</td>
<td>ITTC</td>
<td>YALTA</td>
<td></td>
</tr>
<tr>
<td>3 Domains</td>
<td>1.4 min</td>
<td>41 min</td>
<td>11 min</td>
<td>5 min (500 Certs)</td>
<td>25 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3 * 2.5 min (3 * 500 Certs)</td>
<td>65 min</td>
</tr>
<tr>
<td>4 Domains</td>
<td>3 min</td>
<td>46 min</td>
<td>16 min</td>
<td>6 min (500 Certs)</td>
<td>35 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4 * 2.5 min (4 * 500 Certs)</td>
<td>78 min</td>
</tr>
<tr>
<td>5 Domains</td>
<td>5.5 min</td>
<td>68 min</td>
<td>19 min</td>
<td>9 min (500 Certs)</td>
<td>44 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4 * 2.5 min (4 * 500 Certs)</td>
<td>106 min</td>
</tr>
</tbody>
</table>

* Includes Computation and Communication times

** Negotiation Time not included.

++ Includes algorithm optimizations (Multi-threaded C Code)
## Domain Join and Leave Events

### Domain Joining a Coalition of 3 Domains

<table>
<thead>
<tr>
<th>Domain Joining a Coalition of 3 Domains</th>
<th>Shared-Key Generation (1024 bits)</th>
<th>Exporting CAS</th>
<th>Importing CAS</th>
<th>Certificate Distribution for Joint Resources</th>
<th>Certificate Distribution for Private Resources</th>
<th>Total Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITTC</td>
<td>Yalta</td>
<td>10 sec</td>
<td>16 min.</td>
<td>6 min (500 Certs)</td>
<td>4 * 1 min. (4 * 125 Certs)</td>
<td>30 min</td>
</tr>
<tr>
<td>3 min</td>
<td>46 min</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>72 min</td>
</tr>
</tbody>
</table>

### Domain Departing a Coalition of 4 Domains

<table>
<thead>
<tr>
<th>Domain Departing a Coalition of 4 Domains</th>
<th>Shared-Key Generation (1024 Bits)</th>
<th>Exporting CAS</th>
<th>Importing CAS</th>
<th>Certificate Revocation for Private Resources</th>
<th>Certificate Distribution for Joint Resources</th>
<th>Total Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voluntarily</td>
<td>N/A</td>
<td>10 sec</td>
<td>11 min.</td>
<td>3 * 1 min. (3 * 125 Certs)</td>
<td>N/A</td>
<td>14 min</td>
</tr>
<tr>
<td>Involuntarily</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITTC: Yalta:</td>
<td>1.4 min</td>
<td>10 sec</td>
<td>11 min.</td>
<td>3 * 1 min. (3 * 125 Certs)</td>
<td>5 min</td>
<td>21 min</td>
</tr>
<tr>
<td></td>
<td>41 min</td>
<td>10 sec</td>
<td>11 min.</td>
<td>3 * 1 min. (3 * 125 Certs)</td>
<td>5 min</td>
<td>61 min</td>
</tr>
</tbody>
</table>

+ RCC can verify satisfaction of SOD policies such as static SOD and permission-based SOD

July 25, 2003
Ongoing and Future Work

- Complete development of tools for negotiating access to coalition resources
  - Measurements for time taken to satisfy negotiation constraints
- Integration of ITTC key generation software with our infrastructure


