Integrated Security Services for Dynamic Coalition Management

Himanshu Khurana and Vijay Bharadwaj

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

DARPA DC PI Meeting
July 9, 2002
Newport, Rhode Island
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
Faculty Research Assistant: Serban Gavrilă, Himanshu Khurana
Graduate students: Vijay Bharadwaj, Radostina Koleva, Emilian Dinu, Rakesh Bobba
Recent Work

• Coalition-Resource Management Tools: Architecture, Implementation
  – Joint Administration of Access Policies (Demo Today)

• Negotiation of Coalition Resources
  – A State Transition Model of the Negotiation Process

• Software Agents for Decentralized Negotiation of Coalition Resources: Design, Analysis
Integration Goal: Develop Coalition Resource Management (CRM) Tools
Example: CRM Components for Two Domains

* Policy specification/negotiation language and visual tools are included
Previous Demos

* Policy specification/negotiation language and visual tools are included
Stage III Demo

* Policy specification/negotiation language and visual tools are included
Joint Administration of Access Policies for Coalition Resources

A Coalition Example

- Pharmaceutical Company
- Genetics Firm (Discovers Gene Sequence)
- Private Hospital

Coalition Web Server

Must remain with coalition

Research Data for Gene Sequence

Policy

Joint Administration

Joint Ownership
1 Joint Coalition authority
   - Supports coalition access to jointly owned resources in the presence of coalition dynamics
   - Can be implemented in a self-contained or distributed manner

2 Coalition-closed administration of shared access policies
   - Outsourcing policy administration requires trust in outside domain
   - Outside domain would become single point of trust failure

3 Consensus for administration of access policies
   - No single domain should be able to unilaterally define and modify access policies of a jointly owned resource without consent of all other resource owner-domains
Stage III Demo: Architecture
(Satisfying Requirements I & II)

Joint Attribute Authority
Access_CA

RBAC tool

Coalition Resource Server
Web Server

App O

Jointly Owned

Domain 1
ID CA
ID Cert.
User 1

Domain 2
User 2

ID CA
ID Cert.

Attribute Cert.

Access Request (Attr. Cert)

Commit

Accept/Negotiate
Propose State

Joint Administration
Stage III Demo: Architecture (Satisfying Requirement III)

Domain 1 (Sign)  Domain 2 (Game)  Domain 3 (Crypt)

Coalition Authority (Trust)

Coalition App O

1 Import

Create Virtual Directory

2 RCC

Gen. Certs.

3 Create Certs.

4 Request Attribute Cert.

5 Request Attribute Cert.

6 Resource Access Request

Web Server

Shared Public_key K

Access CA

Request Attribute Cert.

Signature Server

Private Key K_{2^{-1}}

Signature Server

Private Key K_{3^{-1}}

User D1

ID Cert.

Domain 1 (Sign)

Domain 2 (Game)

Domain 3 (Crypt)
Stage III: Implementation

- **Operating System**: Windows 2000 Server

- **Access Control Policy**: RBAC Tool (Role Control Center-RCC)
  - *Developed by VDG Inc with partial NIST support*

- **Certificate Authority**: Windows 2000 Server Stand-Alone CA & Shared Access CA (Malkin, Wu, and Boneh)

- **Application Server**: Windows IIS Web Server
  - Access to website using certificates (X.509 v3) over SSL
Negotiating Access to Coalition Resources

Domain 1
- London – Washington DC
- Paris - Washington DC
- Vienna – Washington DC

Domain 2
- Singapore – London
- New Delhi – London
- Tokyo – London

Internet

Local Access Constraint:
- no user can perform both “pricing” and “reservation” operation on any route app

Global Negotiation Constraint: Share resources based on least privilege principle

Negotiate

Common Access State
- is agreed on by all domains
- satisfies neg. constraints
- satisfies each domain’s access constraints
Need for Negotiation Tools: Supporting Coalition Dynamics

• Domain join
  – Re-negotiate common access state to satisfy new objectives
    • Shared accesses to new and existing coalition resources

• Voluntary domain departure
  – Cannot withdraw jointly administered resources
  – Re-negotiate common access state for two reasons
    • Continued joint administration of jointly owned resources
    • Withdrawal of resources essential to coalition mission

• Involuntary domain departure
  – Re-negotiate common access state to exclude departing domain
  – May allow withdrawal of all resources contributed to coalition
A State Transition Model of the Negotiation Process

- **Application of model transitions results in common access state that**
  - Satisfies coalition objectives
  - Satisfies negotiation constraints
    - Resource based constraints: e.g., least privilege, cost-based
    - Permission based constraints: e.g., SOD, obligation
    - Extended RCL 2000 (Ahn & Sandhu) into NL for constraint spec.
  - Satisfies each domain’s access constraints

- **Show that model supports security formulations**
  - Start in secure state & apply secure transition ⇒ end in secure state
  - Move from secure state to secure state ⇒ there exist secure transitions between these two states
Automated Negotiation of Common Access State

• Goal: Design decentralized negotiation mechanisms and software agents
  – (At least partially) automate the negotiation process
  – Provide tools to assist human operators in negotiating an access control state for the coalition
  – Tools should reconcile domain constraints, identify conflicts and avoid revealing domain private information
Negotiation Process

- Coalition mission is the goal for which the coalition was formed. Domain objectives reflect the preferences of the domains.
- C0 may be empty, or it may contain constraints negotiated at a higher level.
- Problem: Find a state that satisfies M, C0, C1, C2, C3 while attaining O1, O2, O3 “as much as possible”.
Automated Negotiation of Access Control

State

• Problem features:
  – Usually, final coalition state cannot be uniquely determined from coalition mission and domain constraints
    • Underconstrained problem: There may be many states that satisfy all the domain constraints. We need to pick the “best” one, guided by the domain objectives.
    • Overconstrained problem: It may not be possible to completely satisfy all domain constraints. We need to identify this so a human operator can relax one or more constraints if desired.
  – Domain constraints may contain sensitive information.
  – Domain constraints may be influenced by the domain’s membership in other coalitions.
  – Domain constraints may contain clauses that are only evaluated at run time; e.g. “subject to approval of Program Manager”.
The coalition mission and the domain constraints are hard constraints that must be met.

The domain objectives are preferences, or “soft constraints”.

Soft constraints may be based on partial orders; e.g. “high integrity AND high confidentiality”.

Mathematical tools for representing such problems: c-semirings (partial orders), ordered monoids.
**Negotiation Agent**

- Constraint compiler converts mission and constraints to a constraint set in our mathematical framework.
- Current proposal is evaluated against these constraints.
- Proposal is accepted or improved. Conflicts, if any, are flagged.
- **Response can be:**
  - Agreement
  - Counter-proposal
  - A constraint that is being violated
Negotiation Models

- **Model 1: Client-server negotiation**
  - One domain proposes states, the other either accepts or responds with a constraint that is violated.
  - Similar (and complementary) to Automated Trust Negotiation ( Seamons et al.)
Negotiation Models

- **Model 2: Peer-to-peer negotiation**
  - One domain proposes a state, the others either accept or respond with their own proposals.
  - Reveals less about domain constraints, but can be less efficient.
Example: Airline Coalition

**Coalition mission:**
Create an airline network covering Europe, Asia and North America

**Domain 1**
- London – Washington DC
- Paris - Washington DC
- Vienna – Washington DC

**Domain Constraints:**
- Separation of duty between pricing and reservation functions
- No external access to frequent-flyer database

**Domain Objectives:**
- Wants to get more local flights in Europe
- Does not want more transatlantic capacity

**Domain 2**
- Singapore – London
- New Delhi – London
- Tokyo – London

**Domain Constraints:**
- Blocks of seats on European routes reserved for European partner airline
- No external access to frequent-flyer database

**Domain Objectives:**
- Needs transatlantic flights
- Wants to share its Europe-Asia routes

July 9, 2002
Properties of Negotiation Outcomes

- This negotiation can be studied using game theory.
- If all soft constraints are known to all domains,
  - If domains have equal power, the result is the nucleolus
    • Unique outcome that lexicographically minimizes the excess vector
  - If domains have unequal power, the outcome is the Shapley value
    • Outcome which rewards each domain in proportion to its contribution to the coalition mission
- If soft constraints are private, a stable outcome is reached in the 2-domain case if each domain follows a strategy of concessions with offer-dependent breakdown probabilities.
- The negotiated solution is stable if no domain has an incentive to try and change it
  - Pareto optimality: No domain can improve its position without leaving another domain worse off
  - Core: Any domain that tries to change the state will be worse off as a result
  - Currently working on proving stability for our negotiation models
Ongoing and Future Work

- Develop tools for negotiating access to coalition resources
  - include language for expressing wide variety of negotiation constraints
- Develop efficient solutions for supporting joint administration on domain departures and joins
  - current method requires generation of new shared-key and large scale revocation and re-distribution of privileges
- Establish expressiveness and complexity of constraint representation
- Efficient algorithms to transform policies and objectives to constraint framework
- Analysis of negotiation when domains have only partial knowledge of each other’s constraints
- Integrate negotiation tools with stand-alone and shared certificate authorities, group communication server, and access policy server
Research Publications

1. Multicast Key Management

J.S. Baras and H. Zhao “Design of Hierarchical Key Management Schemes for Group Communications in Mobile Wireless Networks” *submitted for publication*

2. Enforcing Dependencies among PKI certificates


3. Negotiations of Access Control Policies

4. Joint Administration of Access Control Policies for Coalition Resources

July 9, 2002