Negotiating Access Control Policies Using Collaborative Games
V. Bharadwaj/J. Baras

Introduction
- Dynamic coalitions are formed when a number of security domains agree to share resources to achieve a common goal.
- The operations of the coalition may also create new resources, which will be shared among the members.
- The coalition members need to agree on a common access control policy for all shared resources.
- The policy must be decided through negotiation, usually during coalition formation.
- We use game theory to study the dynamics of this negotiation.

Game Theory
- Tools for mathematical modeling of conflict behavior between rational intelligent agents.
- Offers two kinds of approaches:
  - Solution concepts - what is likely to happen in a given situation?
  - Mechanism design - how to set up rules so that a certain thing happens?
- We focus on cooperative game theory - individuals are allowed to collude and form alliances.

Solution Concepts
- Nucleolus:
  - “Fair” outcome - minimizes dissatisfaction of most dissatisfied participant.
- Shapley Value
  - Measure of “bargaining power” - measures the average contribution (hence importance) of individuals to an alliance.

Example 1: Bandwidth Sharing
- Three domains D1, D2, D3 sharing bandwidth between X and Y.
- Nucleolus:
  - All domains share equally; each gets 1.17 Mbps
  - Shapley Value:
    - D1: 1.42 Mbps, D2: 1.17 Mbps, D3: 0.92 Mbps

Example 2: Intelligence Sharing
- Three agencies A1, A2, A3 sharing intelligence sources. Compromise renders a source useless.
- Nucleolus:
  - A1 shares 2, A2 shares 4, A3 shares 10
- Shapley Value:
  - In this case, the minimum number of uncompromised sources an agency must receive to make participation worthwhile.

Negotiating Access Control
- An access control policy consists of
  - A policy model, and a policy model interpretation
    - Access Authorization, Access Attribute and Access Management properties
  - An access control state for the system satisfying the policy model
    - Assignment of access privileges to various principals.
- In practice, the state is often implemented through certificate authorities that issue attribute certificates to principals based on identity certificates in their own domains.
- We focus on negotiating the access control state.
- Currently working within the framework of Role Based Access Control.
- Initial implementation uses a centralized negotiation server to collect proposals from members and commit final state.

Future Work
- Develop a state transition model of access control negotiation and the associated optimization problem.
- Apply game theoretic methods to above optimization problem.
- Develop parsimonious negotiation protocols, i.e., protocols which do not require negotiators to unnecessarily divulge private information.
- Integration of above protocol with a Role Based Access Control (RBAC) system.