Assured Resource Sharing in Ad-hoc Collaboration

DE-FG02-10ER25984
DOE PI Meeting, Sept 16-17 2014

Gail-Joon Ahn
Professor, Computer Science and Engineering
Arizona State University

Ira A. Fulton school of engineering
ARIZONA STATE UNIVERSITY

U.S. DEPARTMENT OF ENERGY

Assured Resource Sharing in Ad-Hoc Collaboration
PI: Gail-Joon Ahn

Project Goals

- Develop an innovative framework to enable users to access and selectively share resources in distributed environments
- Investigate secure sharing and assurance mechanisms for ad-hoc collaboration, focused on Grids, Clouds and Virtual Network Communities

Current Accomplishments

- Articulated sharing patterns and corresponding access control model and developed analysis module for policy anomalies that violate sharing requirements
- Published and disseminated research results through the leading security journals such as IEEE Transactions on Dependable and Secure Computing and Journal of Computer Security
- Established a software-defined infrastructure to articulate requirements relevant to delegation and access control modules

Impacts on DOE's Mission

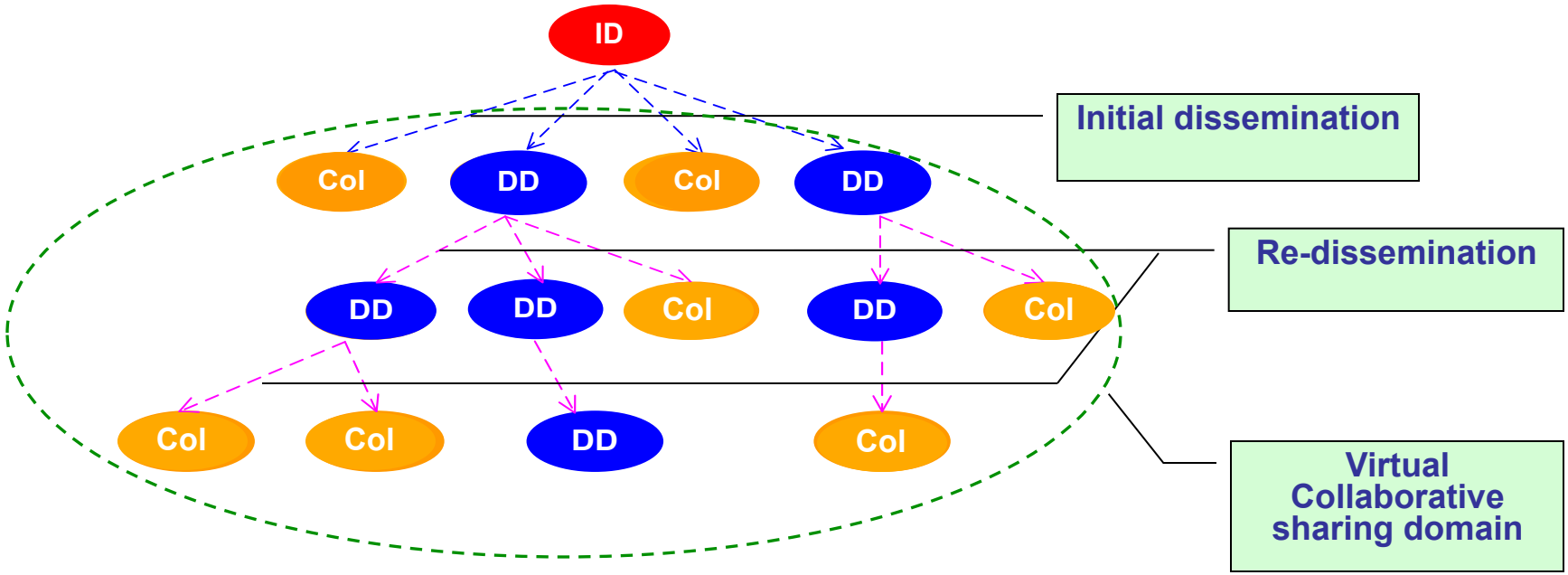
- Enabling research community with a security-aware, scalable framework to sharing resources in a secure and selective manner
- Producing deployment architectures and software modules for establishing trustworthy collaboration environments including access control and delegation management in such dynamic network environments

Problem statement

- Information sharing in ad-hoc collaboration is always *conditional,* and needs to be *highly controlled.*

- Approaches
  - Secure sharing in Grids and Cloud
    - Effective access control framework
  - Policy analysis for assurance

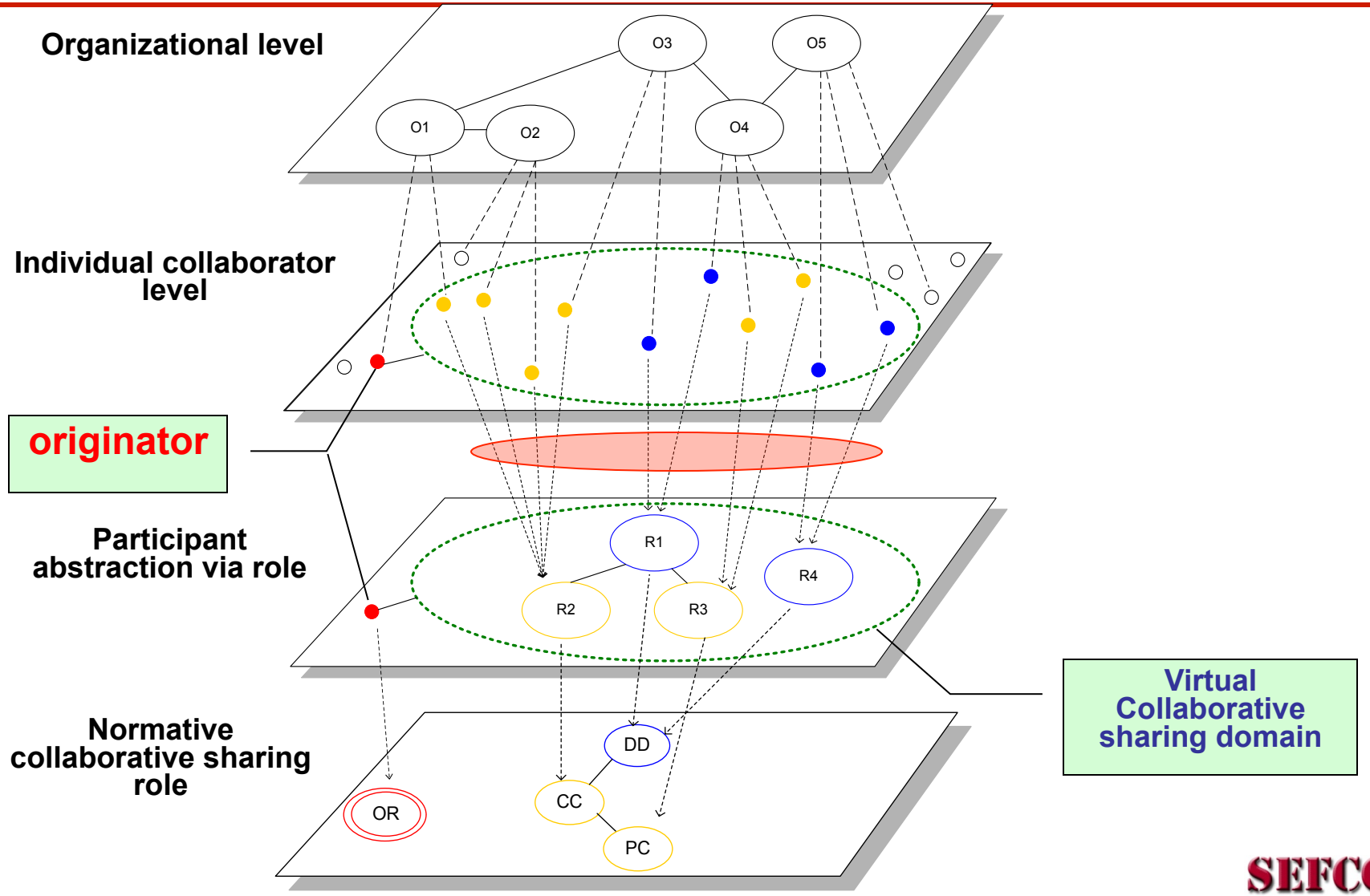
Secure Sharing: Access Control Requirements



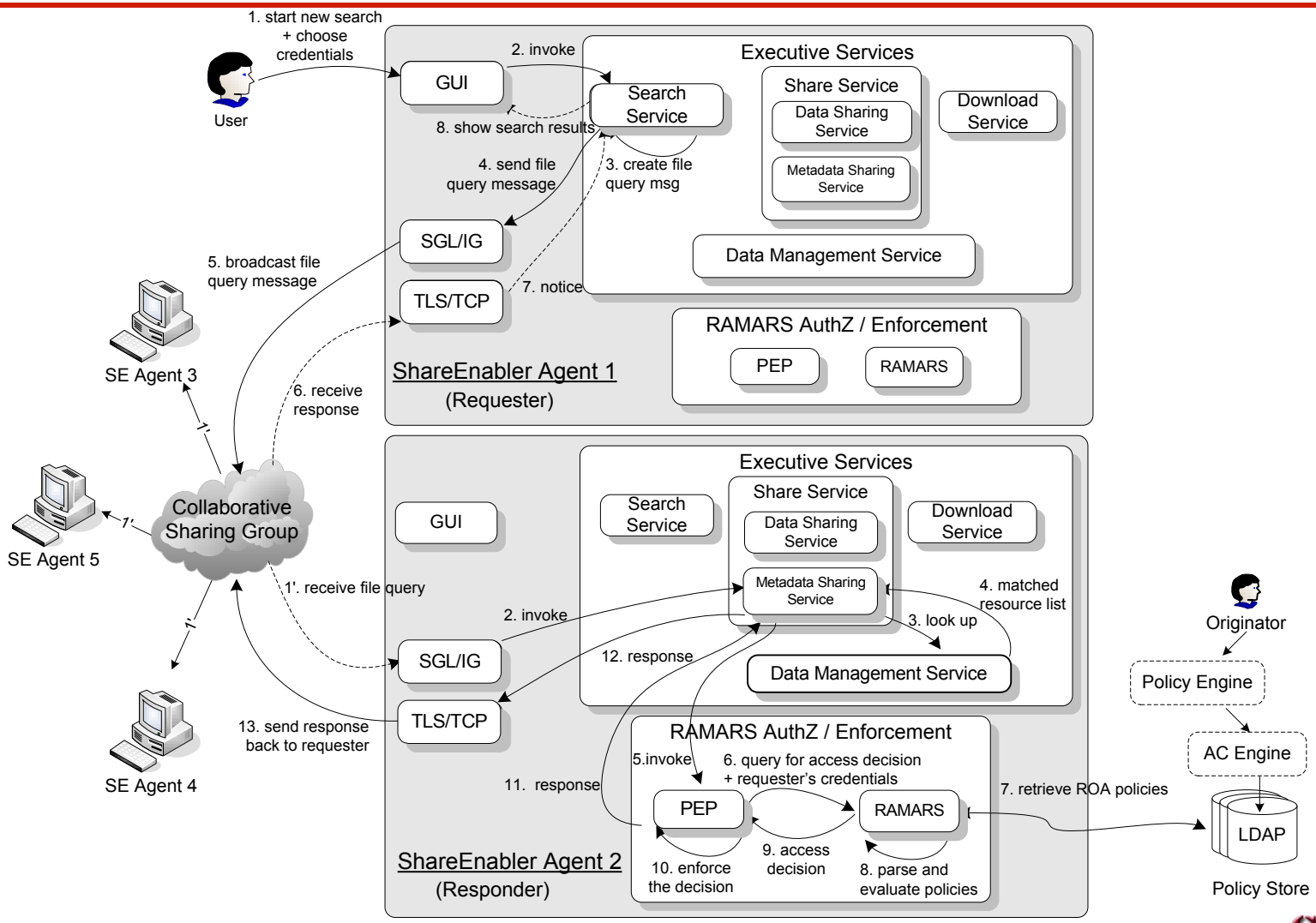
- Access management requirements:
  - The originator needs an effective way to define the virtual collaborative sharing domain and authorize the unknown collaborators inside the domain
  - Access control should guarantee the sharing occurs within the originator's collaborative sharing domain, and sharing behaviors must be well regulated

SEFCOM

Secure Sharing: sharing patterns

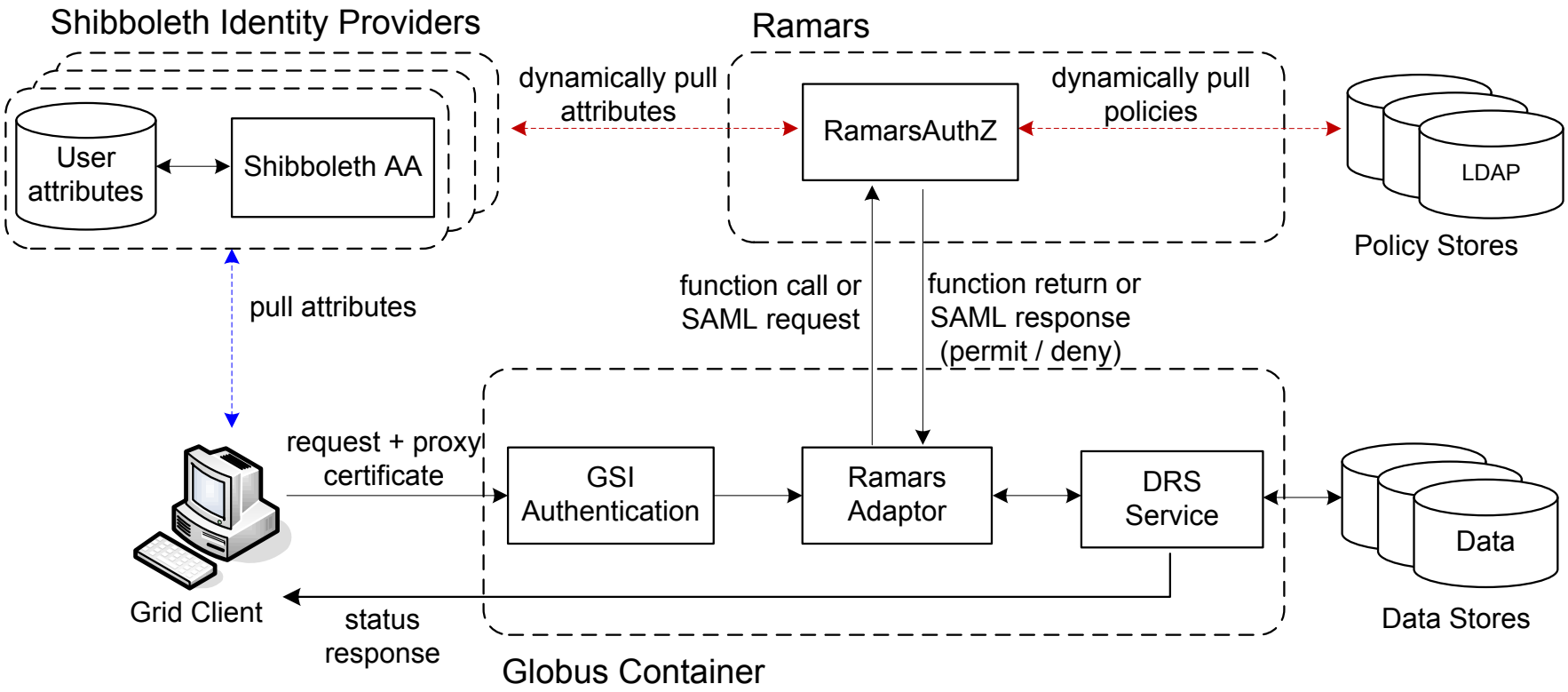


Secure Sharing with P2P – ShareEnabler



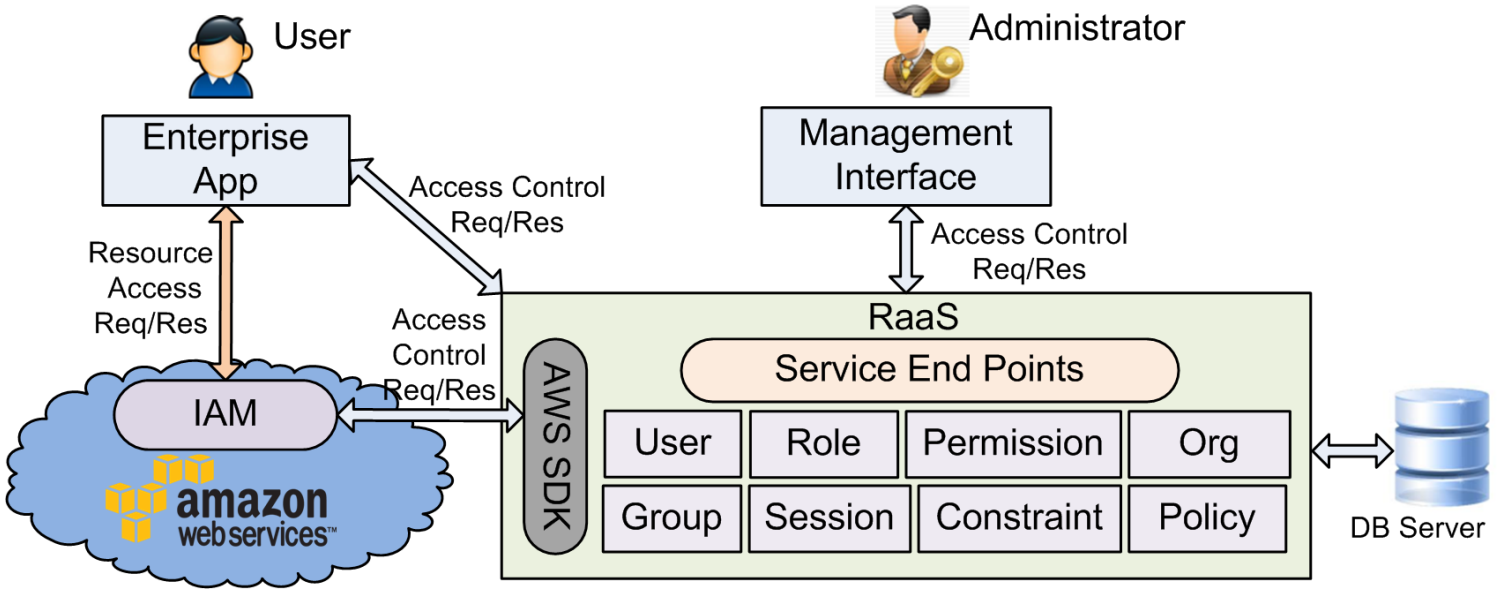
SEFCOM

Secure Sharing with Grids – RamarsAuthZ service



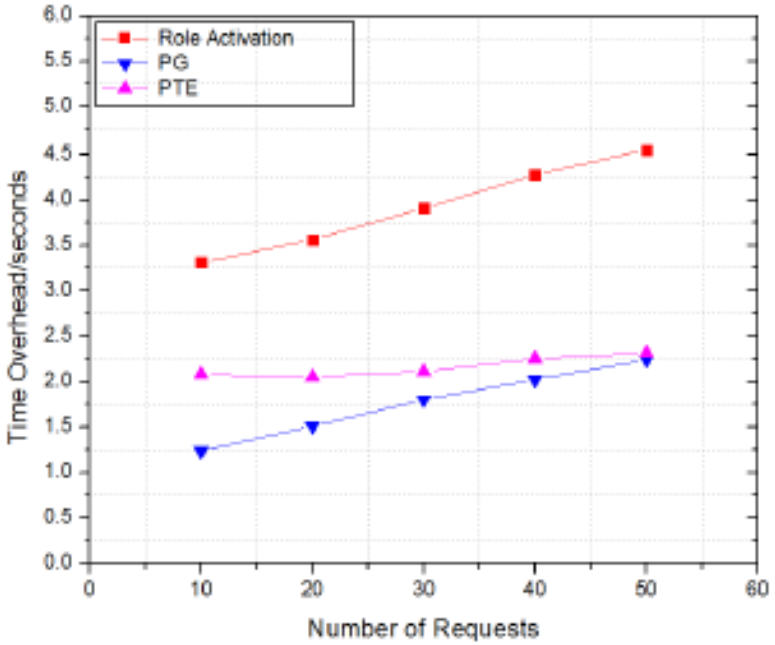
Secure Sharing with Cloud–ACaaS$_{RBAC}$

- ACaaS$_{RBAC}$ introduces RBAC as a service (RaaS), which is an RBAC module can be hosted by AWS or any third party service provider

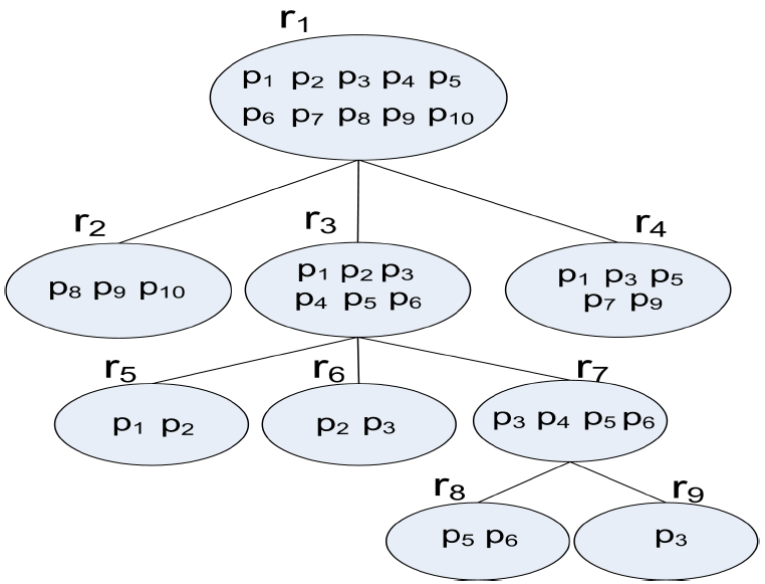


Secure Sharing with Cloud–ACaaS$_{RBAC}$

- In order to measure scalability of ACaaS$_{RBAC}$, measure average performance overhead while increasing the numbers of simultaneous role activation and deactivation requests from users



(a) Activation Time



SEFCOM

Problem statement (revisited)

- Information sharing in ad-hoc collaboration is always *conditional,* and needs to be *highly controlled.*

- Approaches
  - Secure sharing in Grids and Cloud
    - Effective access control framework
  - Policy analysis for assurance

Policy analysis for assurance

- Motivation
  - Access Control Policies
    - Handle complex system properties by separating policies from system implementation
    - Enable dynamic adaptability of system behaviors by changing policy configurations without reprogramming the systems
- Challenge
  - Ensuring the correctness of these policies is critical, and yet difficult
    - Demands strong support of automated **reasoning** techniques
    - Demands systematic mechanism for policy **anomaly management**

Anomaly Management for Access Control Policy

- Policy conflict
  - Conflicts in a policy may lead to
    - Safety problem (e.g. allowing unauthorized access)
    - Availability problem (e.g. denying legitimate access)
- Policy redundancy
  - Redundancies in a policy may adversely affect the performance of policy evaluation
    - Response time of an access request largely depends on the number of rules to be parsed

Anomaly Management for Access Control Policy -- Conflict Detection

- Conflict detection approach
  - Policy-based segmentation technique
    - Partition the entire authorization space of a policy into disjoint segments
  - Identification of conflicting segments
    - Each conflicting segment indicates a conflict

Algorithm 1: Identify disjoint conflicting Authorization Spaces of Policy P

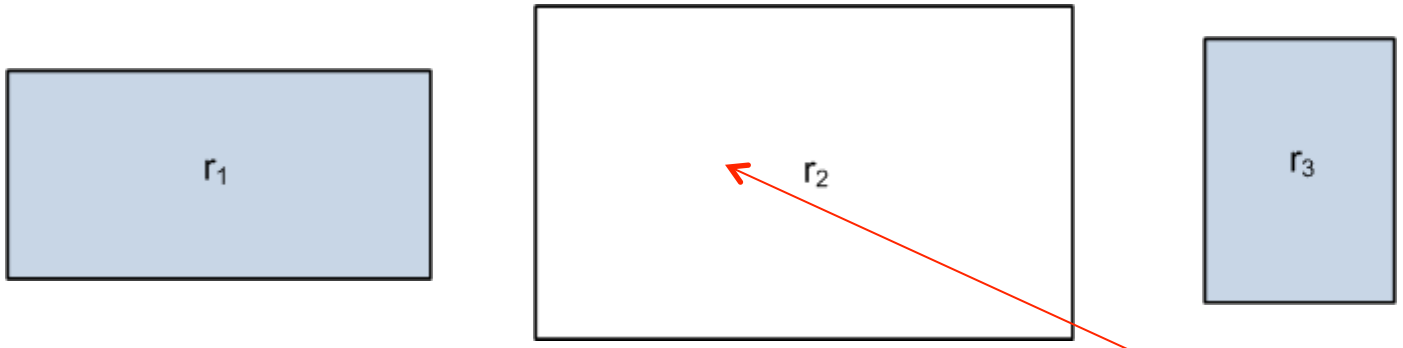
Input: A policy P with a set of rules.
Output: A set of disjoint conflicting authorization spaces CS for P.

```
1  /* Partition the entire authorization space of P into disjoint spaces*/
2  S.New();
3  S ⟵ Partition_P(P);
4  /* Identify the conflicting segments */
5  CS.New();
6  foreach s ∈ S do
7      R' ⟵ GetRule(s);
8      if ∃r_i ∈ R', r_j ∈ R', r_i ≠ r_j and Effect(r_i) ≠ Effect(r_j)
       then
9          CS.Append(s);

10 Partition_P(P)
11 R ⟵ GetRule(P);
12 foreach r ∈ R do
13     s_r ⟵ AuthorizationSpace(r);
14     S ⟵ Partition(S, s);

15 Partition(S, s_r)
16 foreach s ∈ S do
17     /* s_r is a subset of s*/
18     if s_r ⊂ s then
19         S.Append(s \ s_r);
20         s ⟵ s_r;
21         Break;
22     /* s_r is a superset of s*/
23     else if s_r ⊃ s then
24         s_r ⟵ s_r \ s;
25     /* s_r partially matches s*/
26     else if s_r ∩ s ≠ ∅ then
27         S.Append(s \ s_r);
28         s ⟵ s_r ∩ s;
29         s_r ⟵ s_r \ s;
30 S.Append(s_r);
31 return S;
```

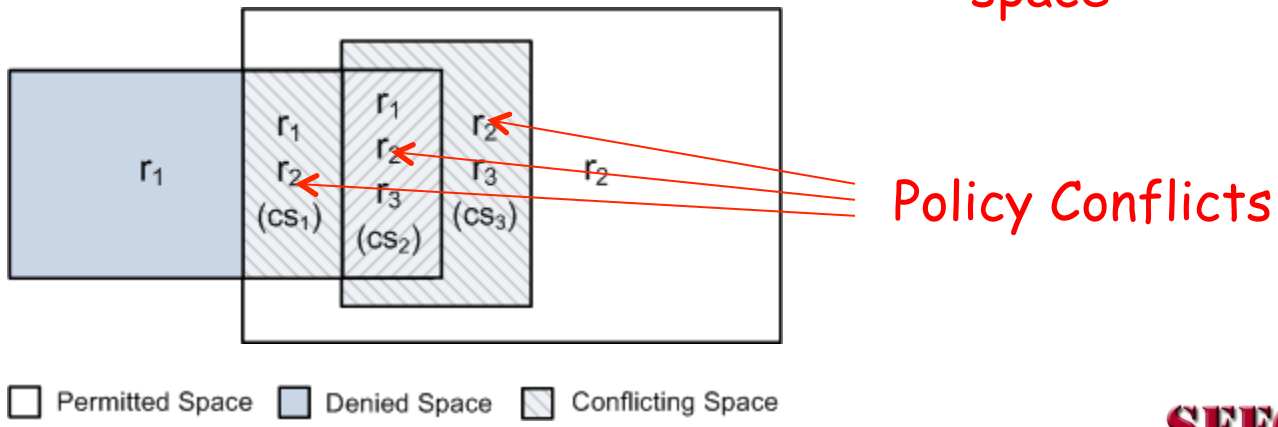
SEFCOM

Anomaly Management for Access Control Policy -- Conflict Detection (cont'd)

- Overlapping authorization space for a policy
  - With two dimensional geometric representation



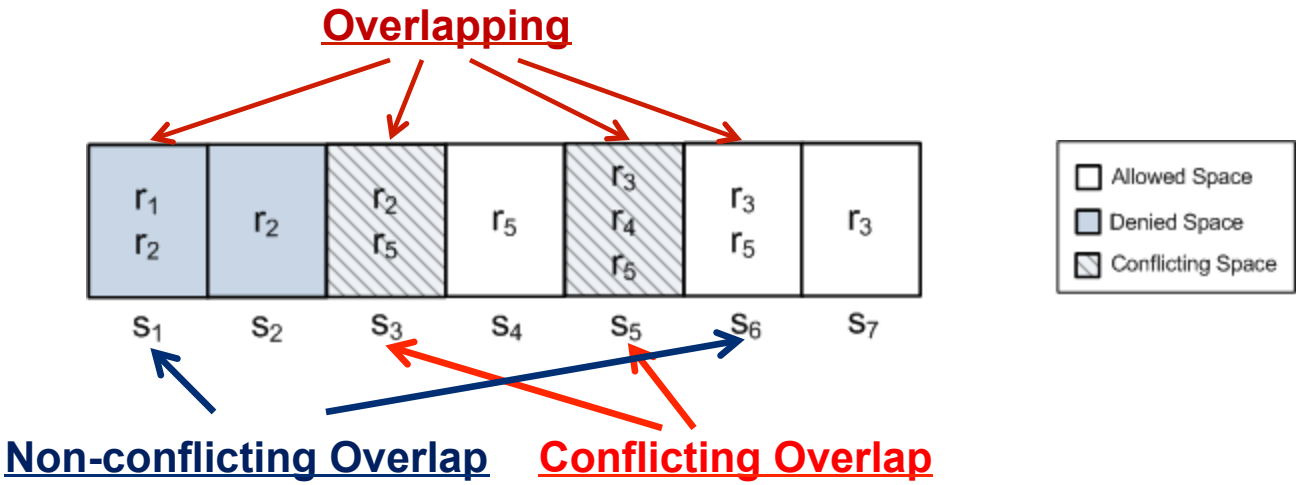
- Space segmentation



SEFCOM

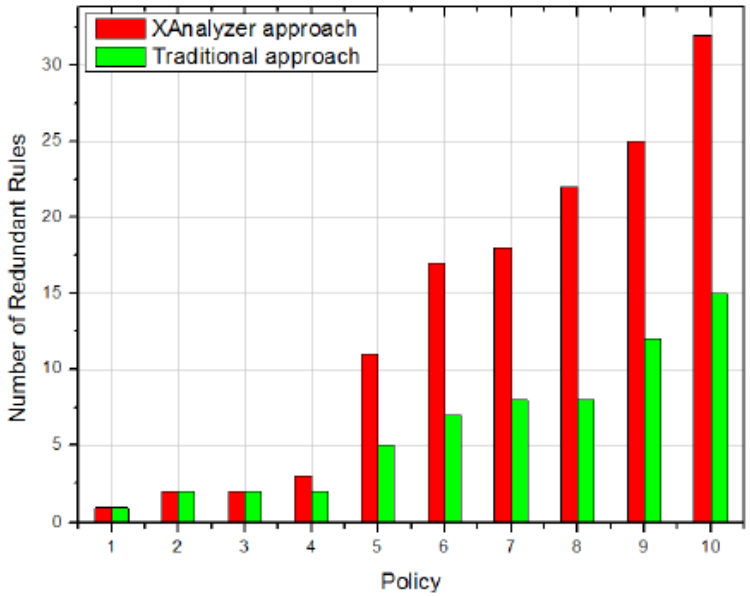
Anomaly Management for Access Control Policy -- Redundancy Removal

- Segment classification
  - Non-overlapping segment (s_2, s_4, s_7)
  - Overlapping segment
    - Conflicting overlapping segment (s_3, s_5)
      - Indicate a conflict
    - Non-conflicting overlapping segment (s_1, s_6)
      - Indicate a potential redundancy

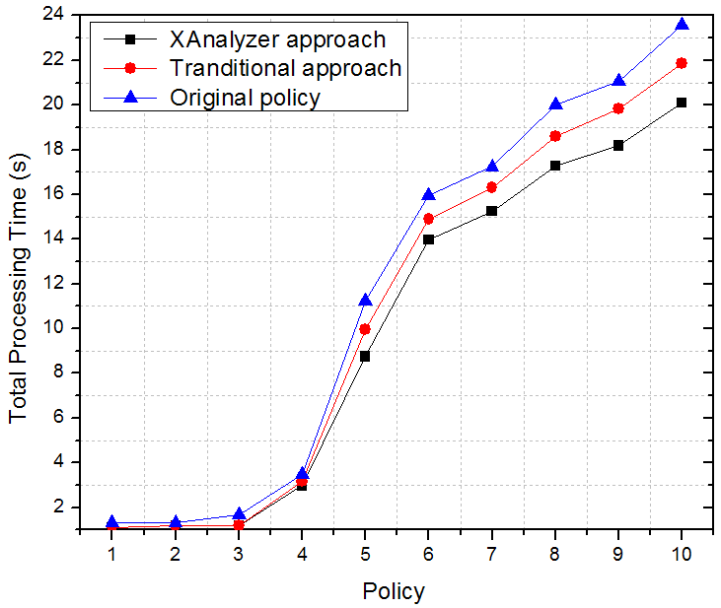


Evaluation (cont'd)

- Evaluation of redundancy removal approach
  - Traditional approach: only identify redundancy relations between two rules



Redundancy elimination rate



Performance improvement

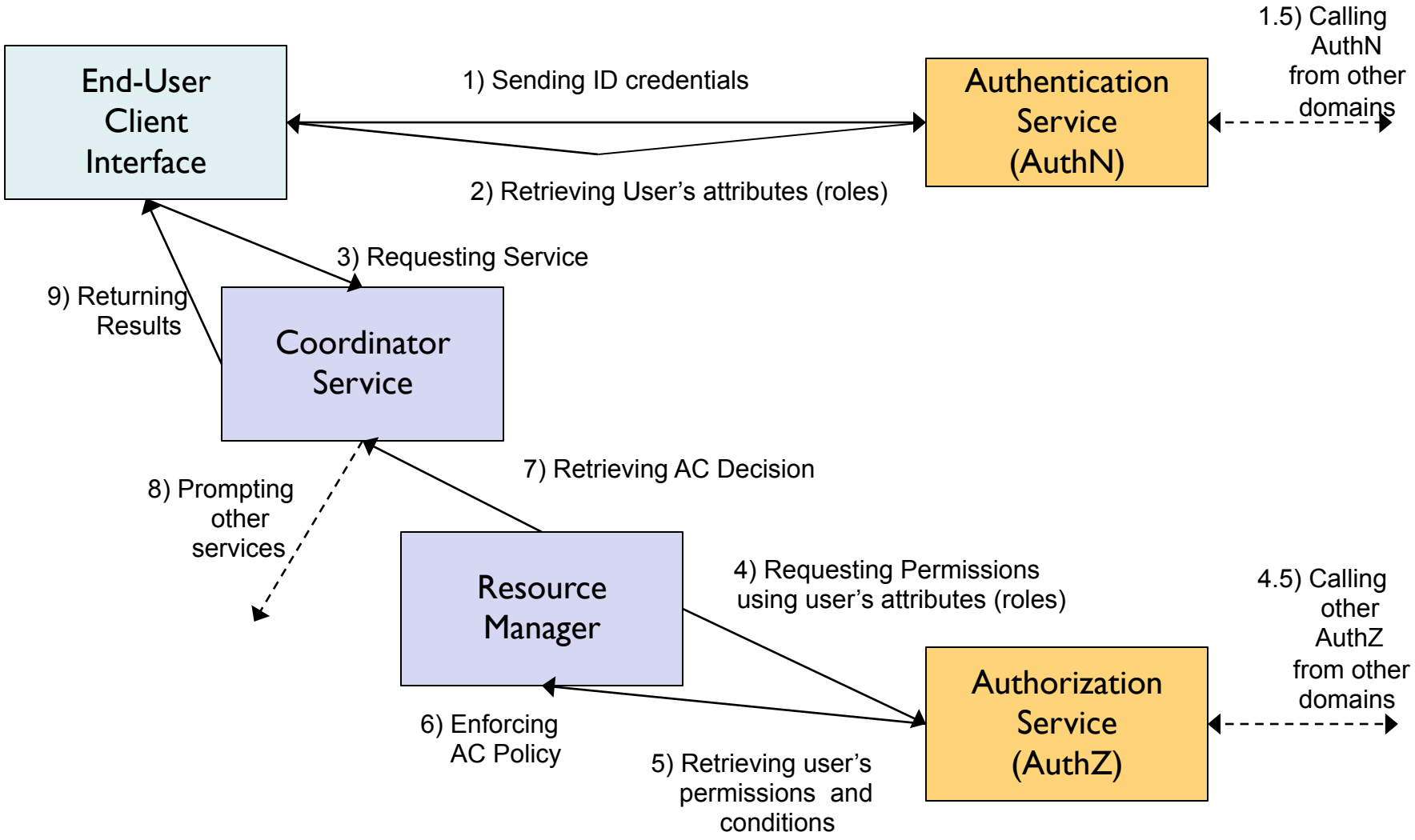
SEFCOM

Summary: Next Step

- Information sharing in ad-hoc collaboration is always *conditional,* and needs to be *highly controlled.*

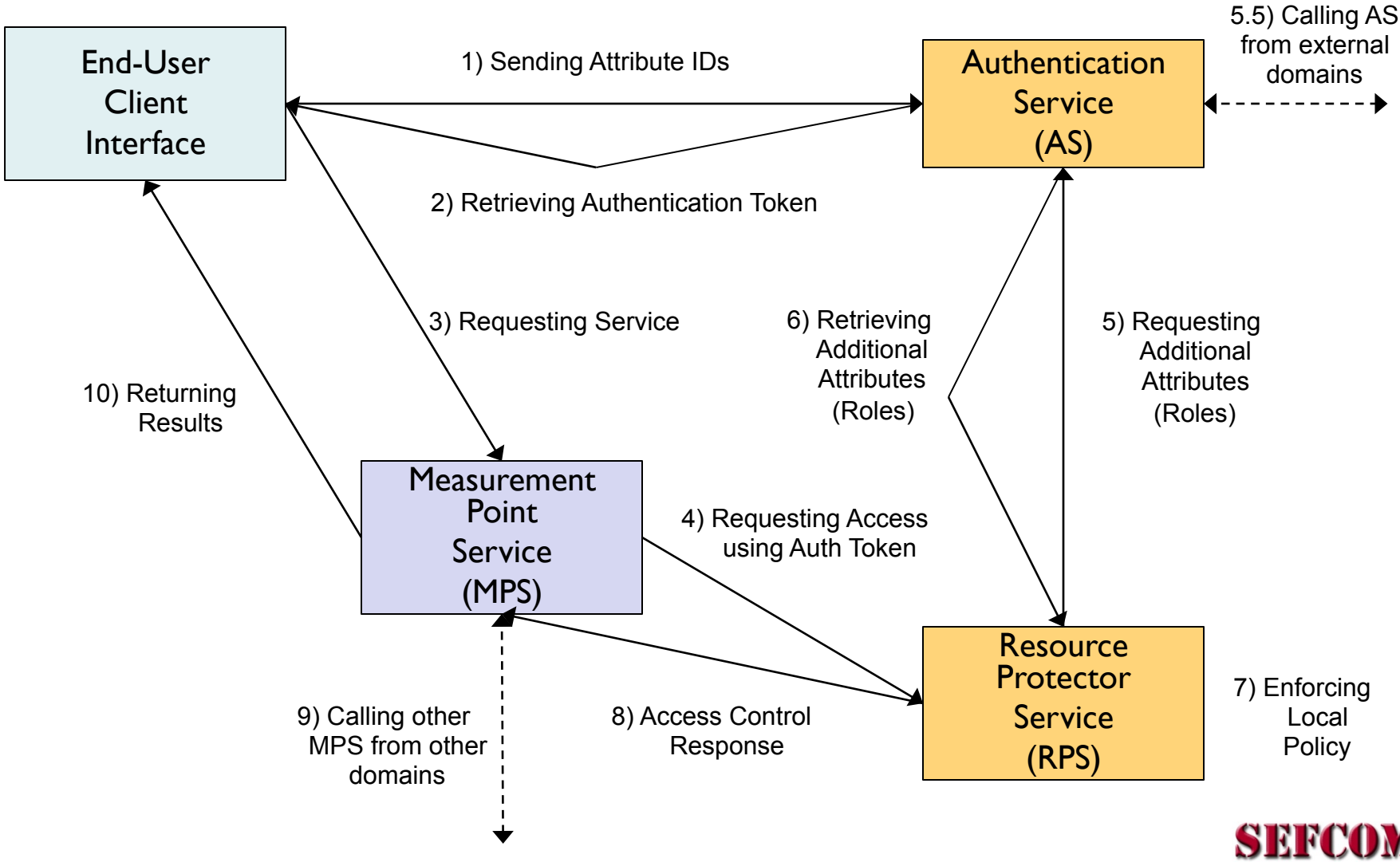
- Approaches
  - Secure sharing in Grids and Cloud
    - Effective access control framework
  - Policy analysis for assurance
    - Policy composition and schema integration
  - *Attribute-based multi-party control*

Exploring Attributes: OSCARS



SEFCOM

Exploring Attributes: perfSONAR



SEFCOM

What question does your research motivate you to now ask?

- Can we discover access patterns, provision access privileges, and generate access intelligence ?
- How can we cope with the resources handled by multiple parties ?
  - Multi-party access control
  - Multi-party policy evaluation
- Is the federation of access control services required?

Selected results

[1] Hongxin Hu*, **Gail-J. Ahn** and Ketan Kulkarni*, "Discovery and Resolution of Anomalies in Web Access Control Policies, " ***IEEE Transactions on Dependable and Secure Computing***. 2013

[2] **Gail-J. Ahn**, Jing Jin* and Mohamed Shehab, "Policy-driven Role-based Access Management for Ad-hoc Collaboration," ***Journal of Computer Security***, 2012

[3] Hongxin Hu*****, **Gail-J. Ahn** and Ketan Kulkarni*****,"Detecting and Resolving Firewall Policy Anomalies," ***IEEE Transactions on Dependable and Secure Computing***, 2012.

[4] Yan Zhu, **Gail-J. Ahn**, Hongxin Hu*****, Stephen S. Yau and Ho G. An, "Dynamic Audit Services for Outsourced Storages in Clouds," ***IEEE Transactions on Services Computing***, 2012.

[5] Hongxin Hu, **Gail-J. Ahn** and Ketan Kulkarni, "Anomaly Discovery and Resolution in Web Access Control Policies", In Proceedings of 16th ***ACM Symposium on Access Control Models And Technologies (SACMAT)***, Innsbruck, Austria, June 15-17, 2011.

[6] Hongxin Hu*, **Gail-J. Ahn** and Ketan Kulkarni*, "Ontology-based Policy Anomaly Management for Autonomic Computing", *In Proceedings of 7th* ***International Conference on Collaborative Computing (CollaborateCom)***, Orlando, Florida, USA, October 15-18, 2011.

[7] Hongxin Hu, **Gail-J. Ahn** and Ketan Kulkarni, "FAME: A Firewall Anomaly Management Environment", In Proceedings of ***ACM Workshop on Assurable & Usable Security Configuration*** in conjunction with 17th ACM CCS, Chicago, IL, USA, 2010.

[8] **Gail-J. Ahn**, Hongxin Hu*, Joohyung Lee and Yunsong Meng, "Representing and Reasoning about Web Access Control Policies", In Proceedings of 34rd Annual ***IEEE International Computer Software and Applications Conference (COMPSAC)***, Seoul, South Korea, July 19-23, 2010.

*** indicates students**

SEFCOM