CERIAS

the center for education and research in information assurance and security

# *Specification and Enforcement of Flexible Security Policy for Active Cooperation*

Yuqing Sun[† ‡], Bin Gong[‡], Xiangxu Meng[‡], Zongkai Lin[*],and Elisa Bertino[†]

*† Purdue University, US ‡Shandong University, China *Chinese Academy of Sciences, China*

## Problem

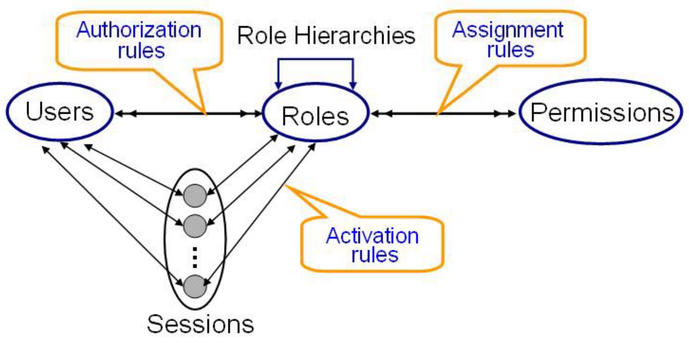
Interoperation and services sharing are becoming new paradigms for enterprise collaboration, which brings a meaningful requirement of flexible specification and enforcement of security policies in information systems:

- *Flexible specification*: specifying policy against multi elements with different criteria, like evaluating partners' qualification by different weights on attributes, consideration of history transaction data with different impacts etc.
- *Flexible enforcement*: allowing environmental factors to influence how and when security policy is enforced. Dynamically monitoring the state changes of an underlying system and take into account the changes into policy enforcement.
- *Flexible adjustment*: allowing smooth update of security policy without huge hop of legacy system operation

Although traditional access control models and their extensions can be content-aware or dynamically enforced based on predefined rules, they are still less expressive for above active security policies, especially without considering the transaction data and much more attributes with different impact factors.

## Specification of Security Policies

### Restriction Rules




- Authorization rules, Assignment rules and Activation rules
- *SR.Rtype*::*rule_name* = A → B, where *SR* is a remained identifier , *Rtype* is a rule type, and *rule_name* is the rule name, A is the prerequisite condition and B is the yielded target.

### Complex Condition with factors

A=(*E,α,ß, threshold* )

Semantics:

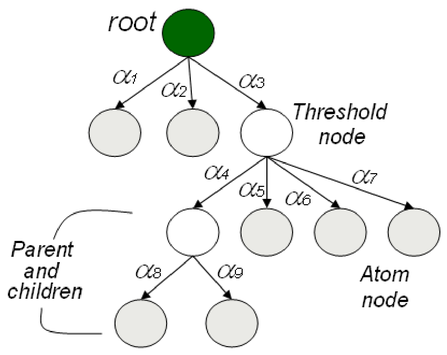
$$\begin{pmatrix} E_{11}, E_{12},\ldots, E_{1m} \\ E_{21}, E_{22},\ldots, E_{2m} \\ \ldots\ldots \\ E_{k1}, E_{k2},\ldots, E_{km} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \ldots \\ \alpha_m \end{pmatrix} \quad (ß_1, ß_2, \ldots, ß_k) \geq threshold$$

## Enforcement of Security Policies

### Condition Determination

- Condition tree expression
- Using key nodes to accelerate condition computing
- Calculation of condition tree

$$\sum_{i=1}^{m} \alpha_i * \mathrm{E_i} \geq threshold_j$$

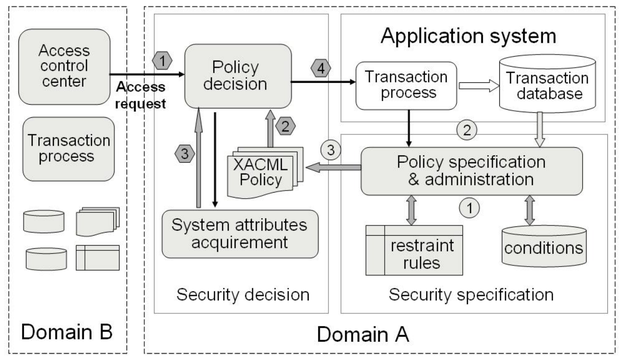



Condition Tree

### Consistency Verification

- Conflict detection
- Redundancy check

### Implementation




***Publications*** *:*

1. Yuqing SUN, Bin GONG, Xiangxu MENG, and Zongkai LIN, *"Active Authorization Management for Multi-domain Cooperation, "* 11th International Conference on Computer Supported Cooperative Work in Design, Australia, 2007

2. Y. Sun, B. Gong, X. Meng, Z. Lin, and E. Bertino. *" Specification and Enforcement of Flexible Security Policy for Active Cooperation*", Submitted.

**Acknowledgement :**

We are thankful to the 863 Program of China 2006AA01A113 and the US NSF grant 0712846 for supporting this project.

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center