Architecture-Centered Composition of Adaptive and Dependable Enterprise Security Services

Yi Deng
Konstantin Beznosov
Center for Advanced Distributed Systems Engineering (CADSE)
School of Computer Science
Florida International University
{deng,beznosov}@cs.fiu.edu

Outline

- Overview of CADSE
- Architecture-Centered Composition of Application Authorization Service - Research Approach
- Preliminary Research Results
- The next steps

CADSE Goals

- To establish a streamlined program that integrates basic research, applied R&D, graduate education and training
  - Establish proper balance between basic research with applied R&D
  - Use real-world problems to guide basic research and to facilitate technology transfer
  - Use R&D to facilitate and complement basic education
  - Integrate research & education with industry collaboration

CADSE Overview

- Personnel: 3 professors, 4 postdocs and research associates, close to 20 graduate students
- Facility: 5 research labs total over 3500 sq. ft, over 50 workstations, servers and other equipment
- Funding: Over $3 million research funding from various Federal agencies and industry

Current Projects

- Distributed object technology
- Enterprise system development based on CORBA
- Software Security
- Software architecture and domain specific architecture
- Formal engineering methods, software verification and testing
- Distributed multimedia Information systems

Outline

- Overview of CADSE
- Architecture-Centered Composition of Application Authorization Service - Research Approach
- Preliminary Research Results
- The next steps

Composibility of Secure Enterprise Systems

- Support for integration
- Uniform administration of enterprise security policies
- Assurance to end-to-end properties
  - security policies, performance, availability, etc
- Support for continuous evolution
  - add or change system/components
  - change policies or business process, etc

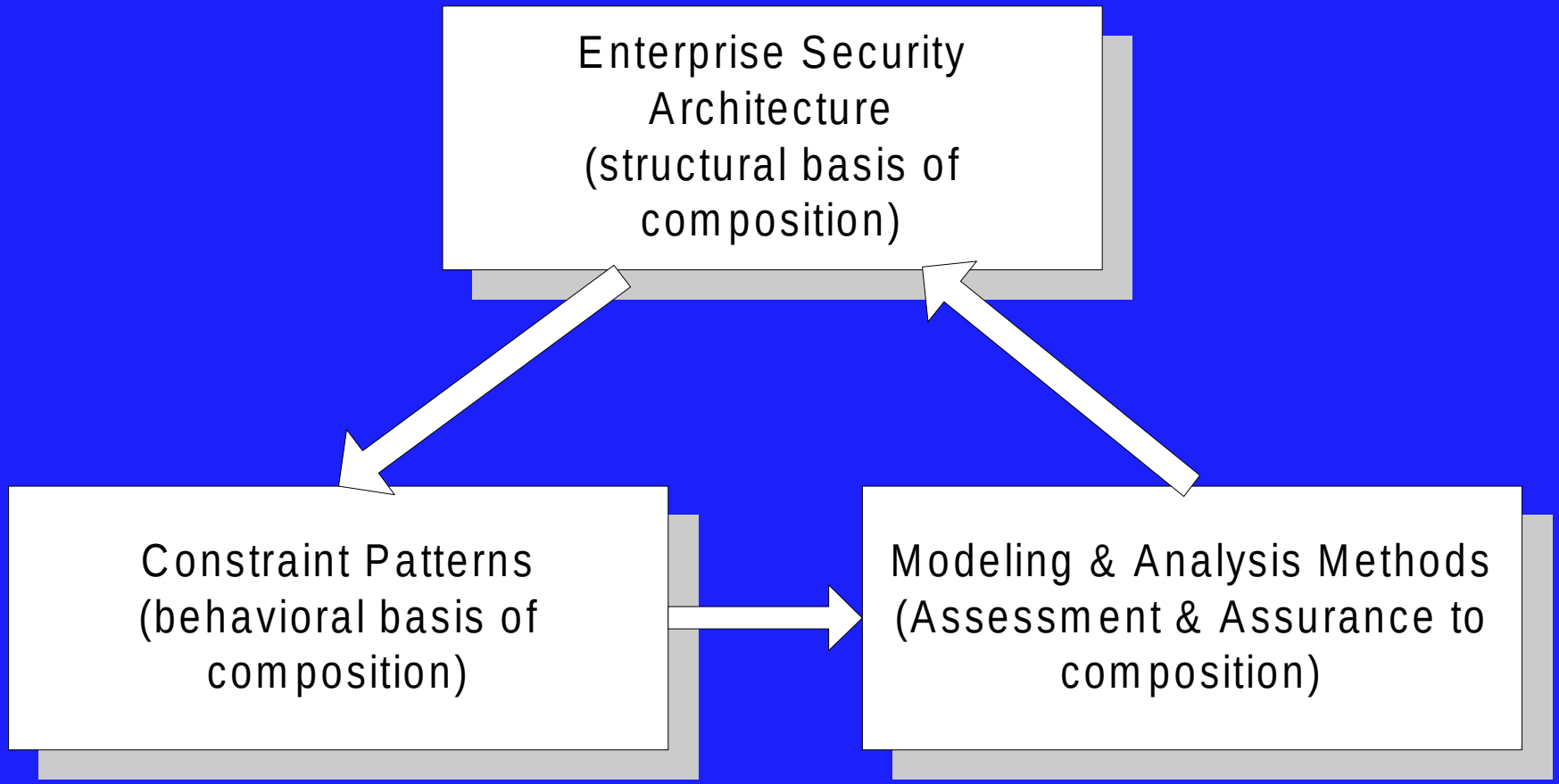
Problems in Application-Level Security

- Must handle fine grain, complex, dynamic policies
- Embedded in application systems today
  - multiple points of control
  - problems in administration
  - expensive life-cycle

What Solutions Available Today?

- Middleware security architectures
  - CORBA, EJB, DCE, DCOM
- Resource Access Decision (RAD) specification
  (to be discussed later)
- Open issues
  - support for fine-grain, complex policies
  - dynamic changes and configuration
  - performance and availability concerns
  - end-to-end properties assurance

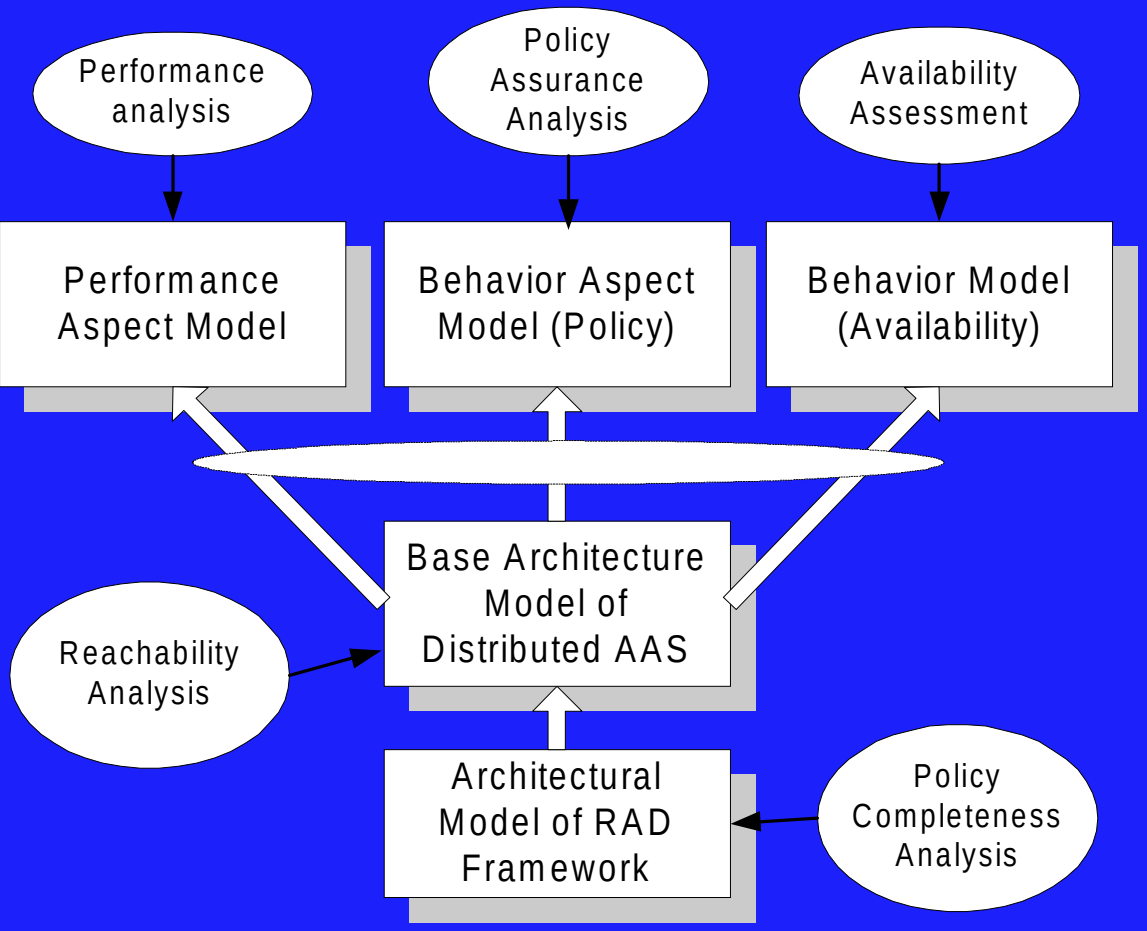
Framework of Our Approach



Distributed Security Architecture: Research Issues

- Focus on CORBA-based Application Authorization Service (AAS) Architecture
  - Configurability
    - support dynamic policy changes
    - support different distributed, e.g. Internet based e-commerce, environments
  - Adequate performance (distributed authorization and load balancing)
  - High availability (replication and fault tolerance)
  - Application composibility

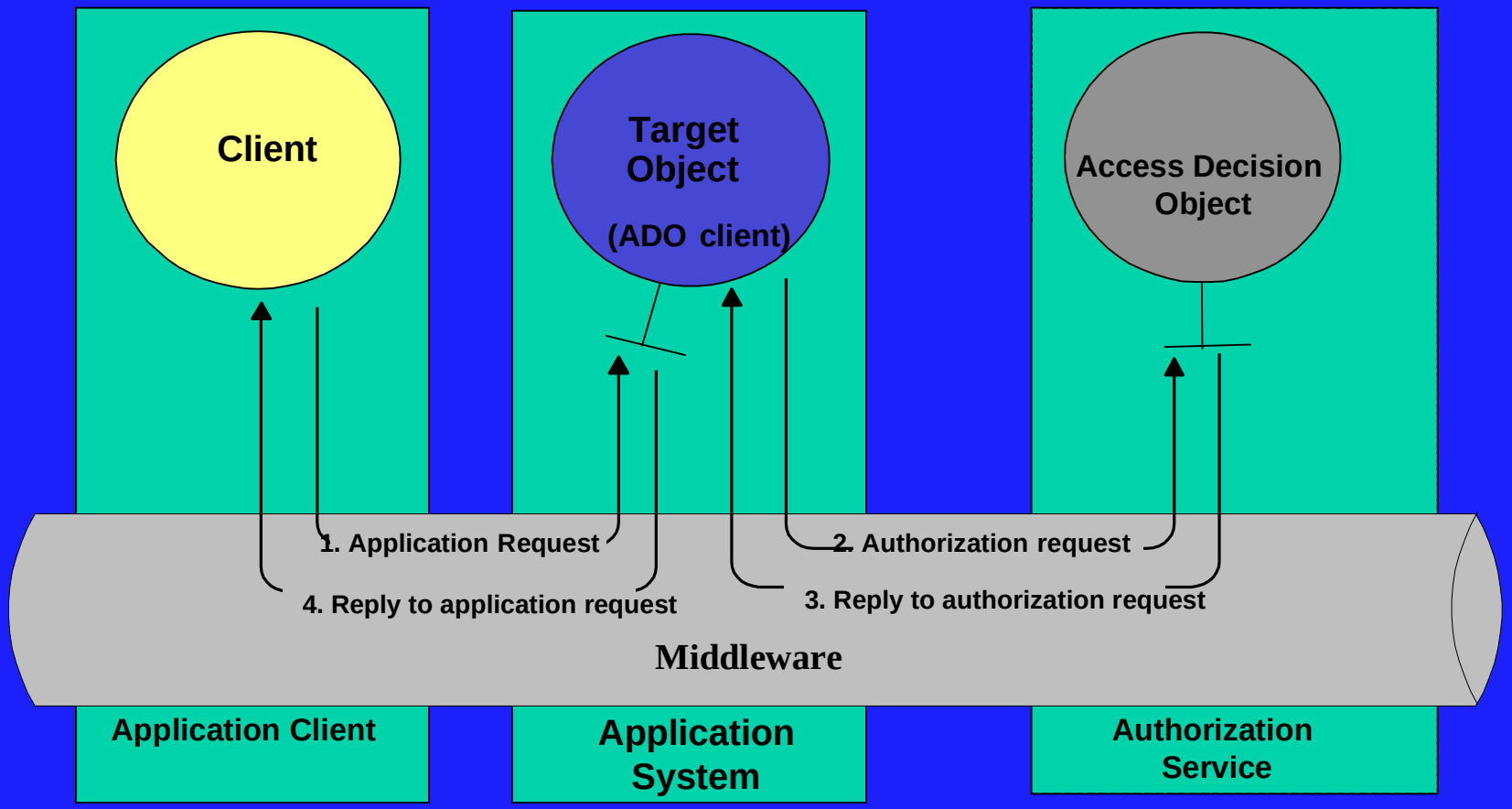
Aspect-Oriented Models of Security Service



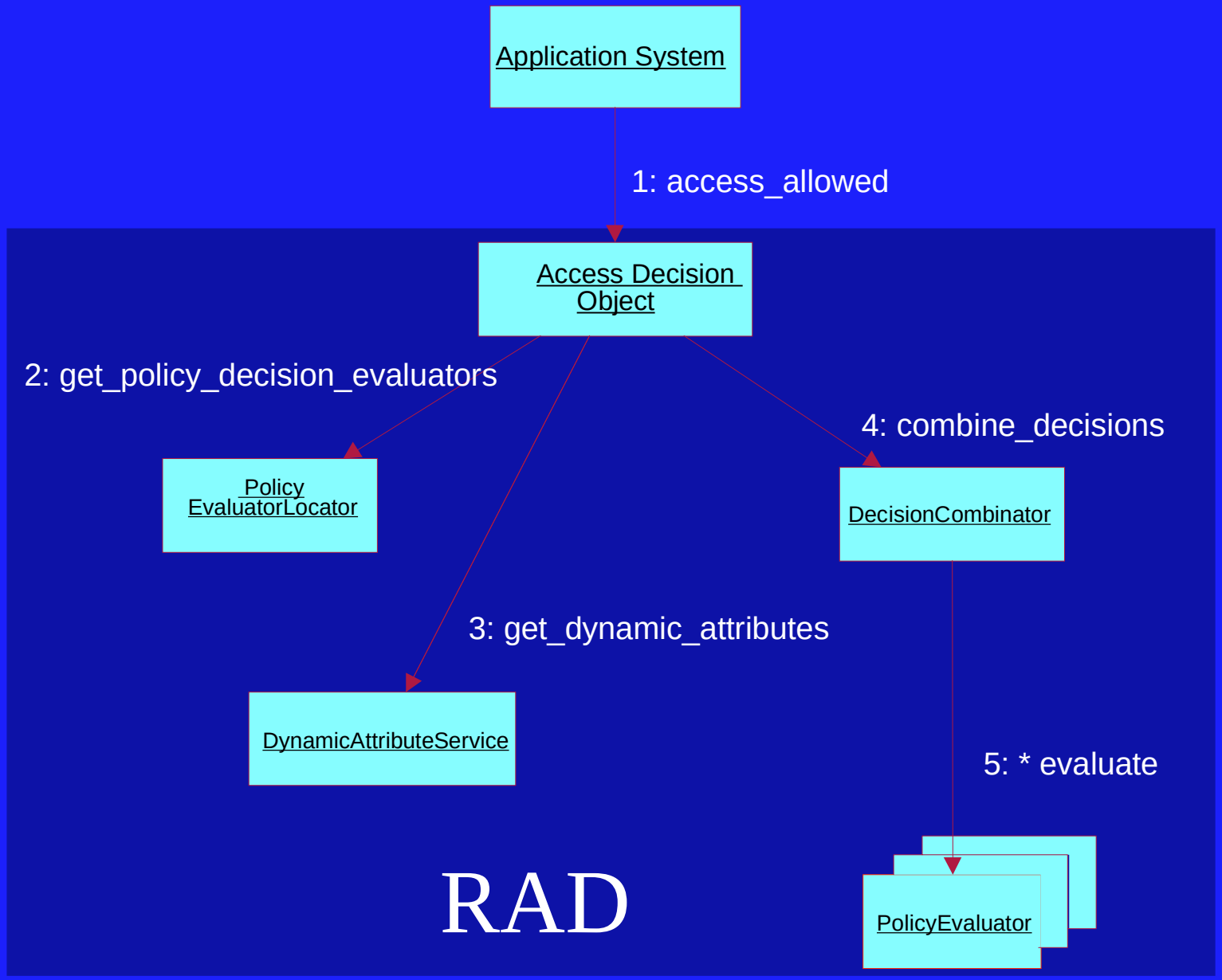
Outline

- Overview of CADSE
- Composition of Adaptive and Dependable Application Authorization Service - Research Approach
- Preliminary Research Results
  - Research in application authorization service
  - An example
  - Modeling and analysis of AAS
- The next steps

Framework of Resource Access Decision Facility



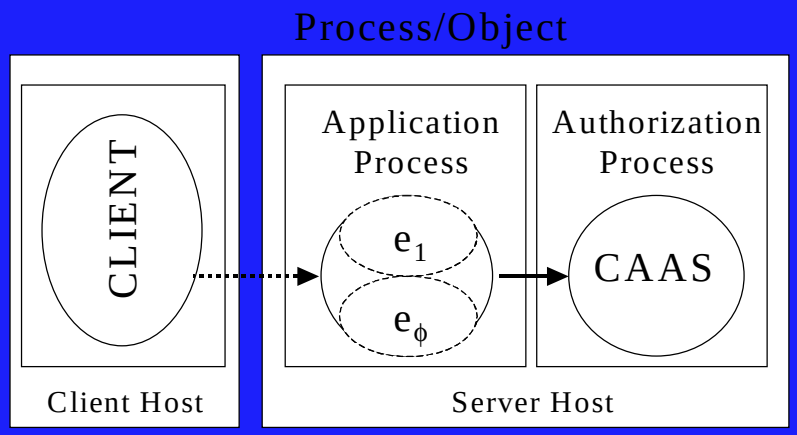
RAD Components

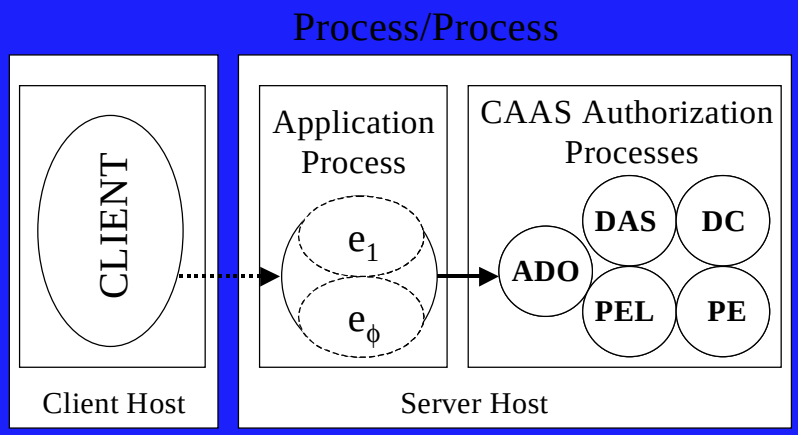


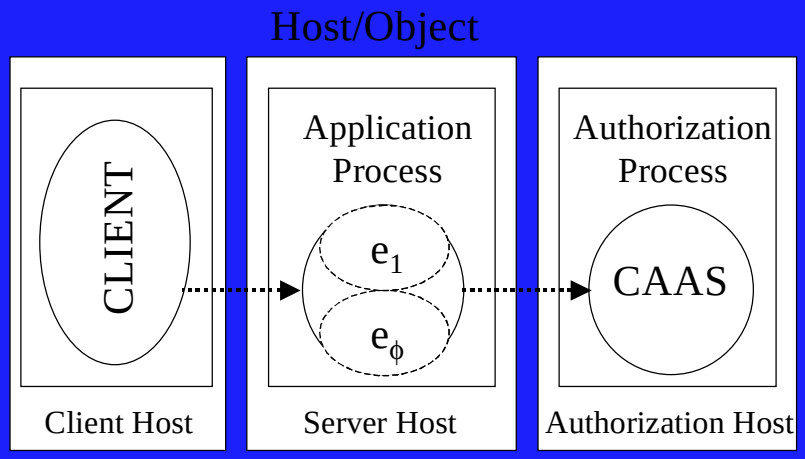
Current Results

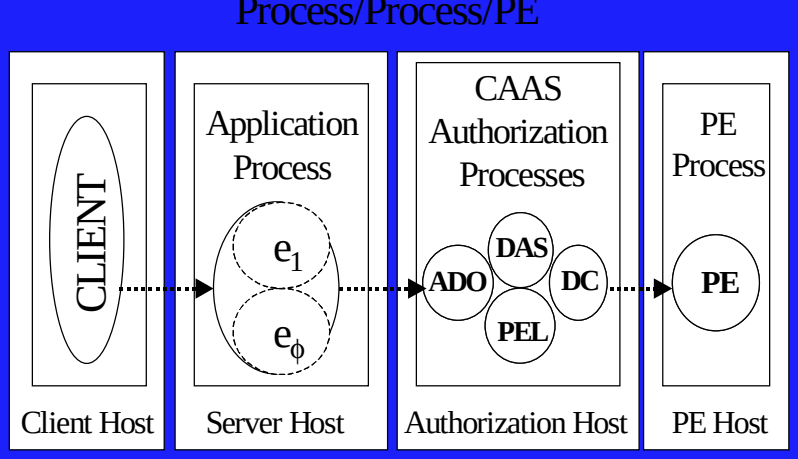
- Conceptual architecture of RAD
- A prototype CORBA-based Application Authorization Service (CAAS)
  - CORBA-based
  - highly configurable
  - portable (Java)
- Performance experiments
- Support for different types of policies
  - federations, multi-policy, RelBAC

CAAS Configuration Examples









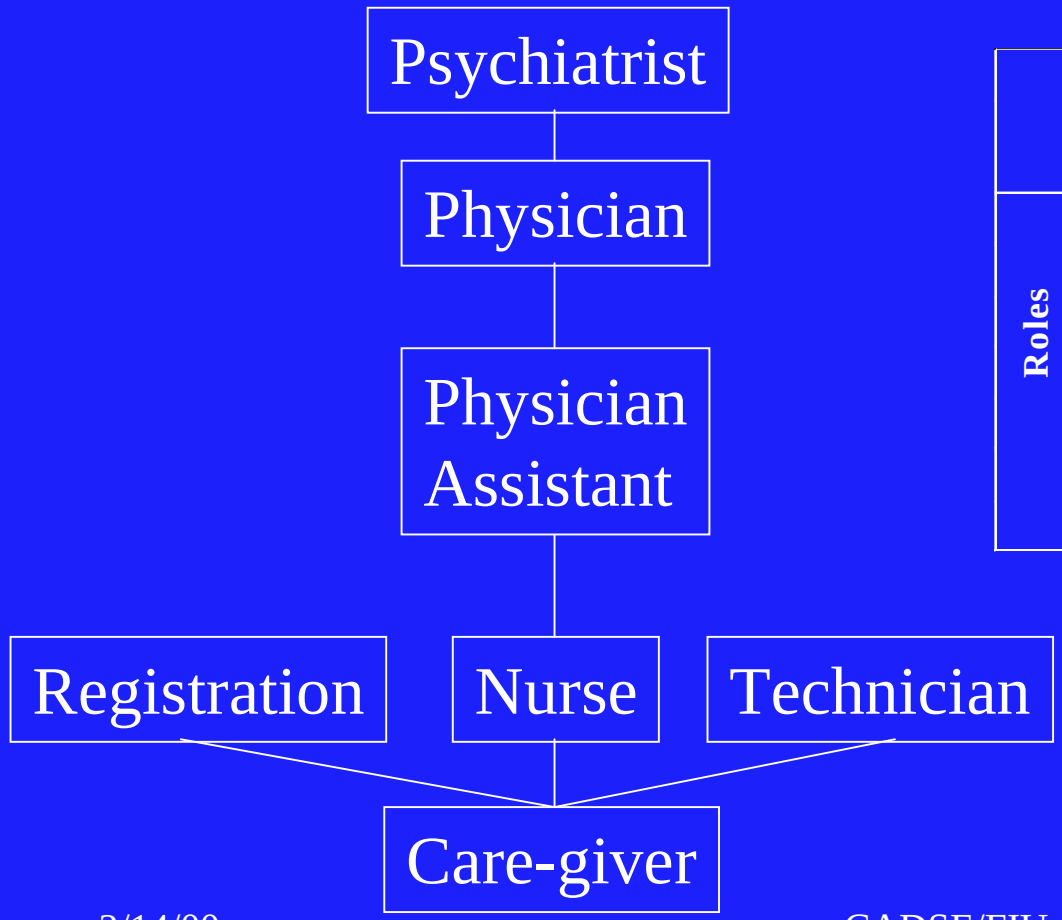
Example

An Example: Initial Policies

No.	Description
P-1	Any **caregiver** can read patient's name.
P-2	**Registration clerk** can modify patient name and demographic information.
P-3	**Nurse** can read patient's name and demographic information, modify current episode demographic information, can read current episode regular records and current episode regular test results.
P-4	**Technician** can modify current episode regular and sensitive test results.
P-5	**Assistant physician**, in addition to what a nurse can do, can also read all regular records of patients.
P-6	**Physician**, in addition to what assistant physician can do, also can modify current episode regular and sensitive records, and read regular and sensitive records and test results from previous episodes.
P-7	**Psychiatrist**, in addition to what a physician can do, also can modify mental information.

Modeling with RBAC

Role Hierarchy



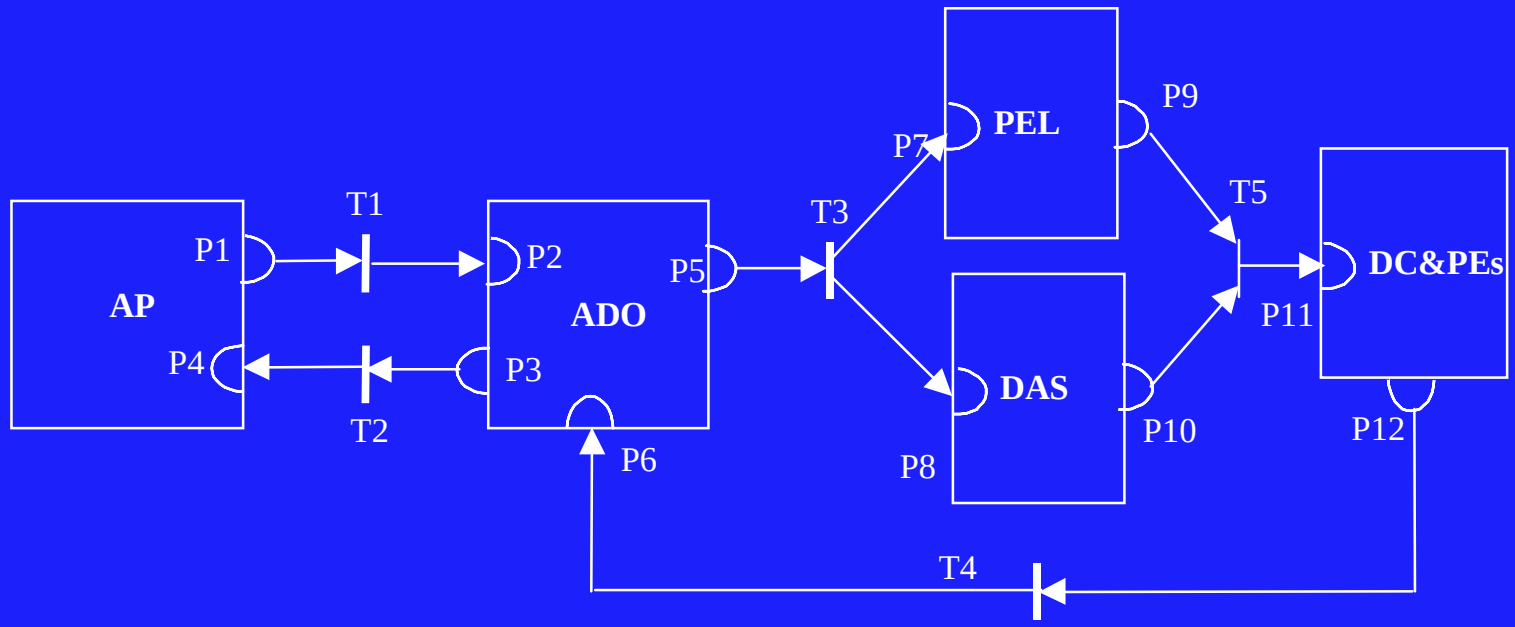
User to Role Assignment Relation (UA)

		Users						
		a	b	c	d	e	f	g
Roles	Psychiatrist	✓						
	Physician		✓					
	Physician Assistant			✓				
	Nurse				✓			
	Registration Clerk					✓		
	Technician				✓		✓	
	Care-giver							✓

Permission Assignment (PA) Relation

Roles		Resources											
		PN	DD	CDD	CRR	CSR	CRT	CST	PRR	PSR	PRT	PST	AMD
	Psychiatrist												RW
	Physician				W	RW		R		R		R	
	Physician Assistant								R		R		
	Nurse		R	RW	R		R						
	Registration Clerk	W	RW										
	Technician						RW	RW					
	Care-giver	R											

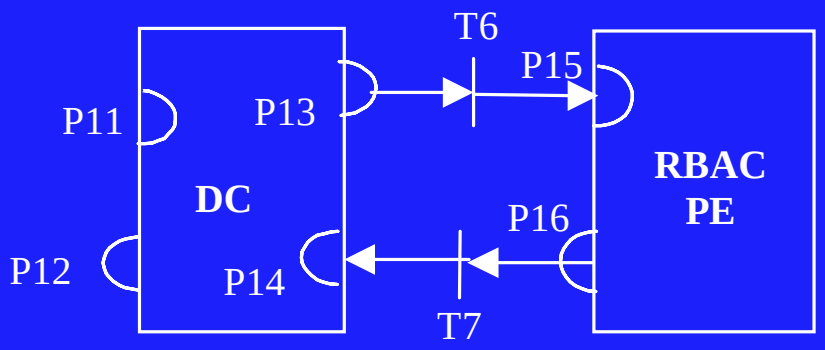
Base Architecture Model



Sample constraints (reachability):

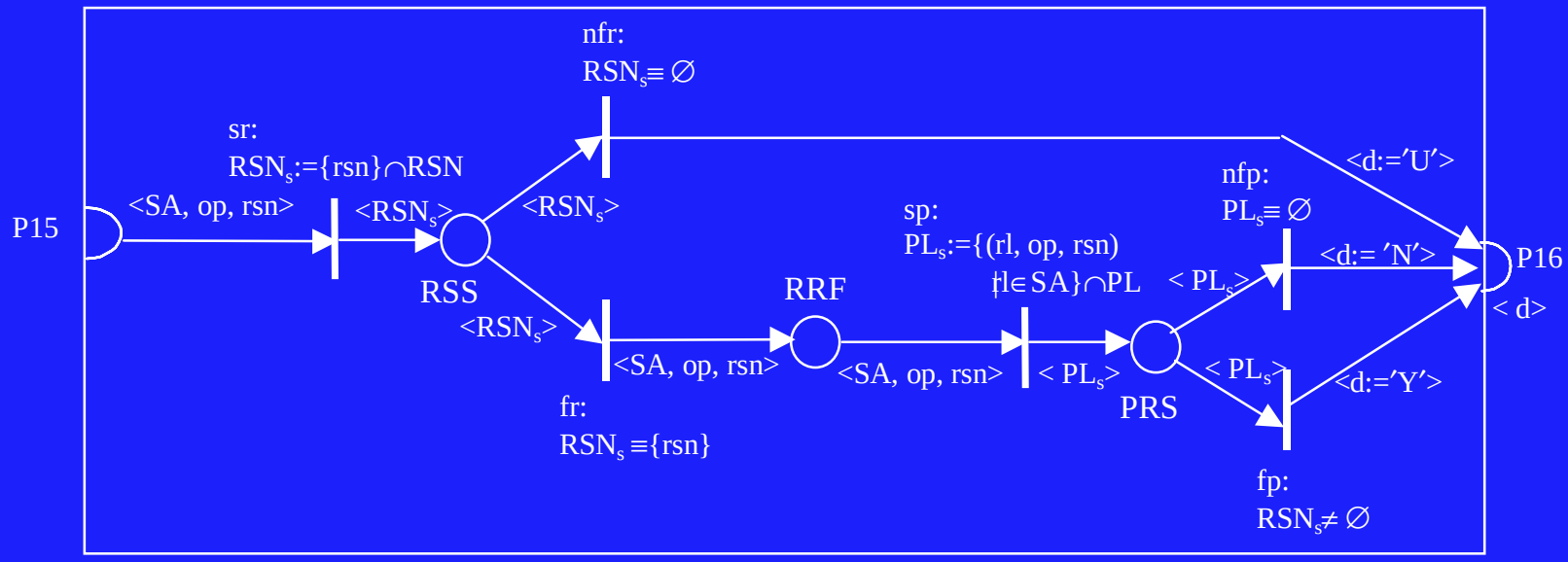
P2 $\rightarrow$ *AF* P5, P7 $\rightarrow$ *AF* P9, P8 $\rightarrow$ *AF* P10, P11 $\rightarrow$ *AF* P9, P6 $\rightarrow$ *AF* P3

Composition of DC&PEs based on RBAC Policies



P13 Attributes
P14 Decisions from PE
P15 Attributes received by RBAC PE
P16 Decision made by RBAC PE
T6 DC invokes RBAC PE
T7 RBAC PE passes decision to DC

Behavior Model of Policy Evaluator



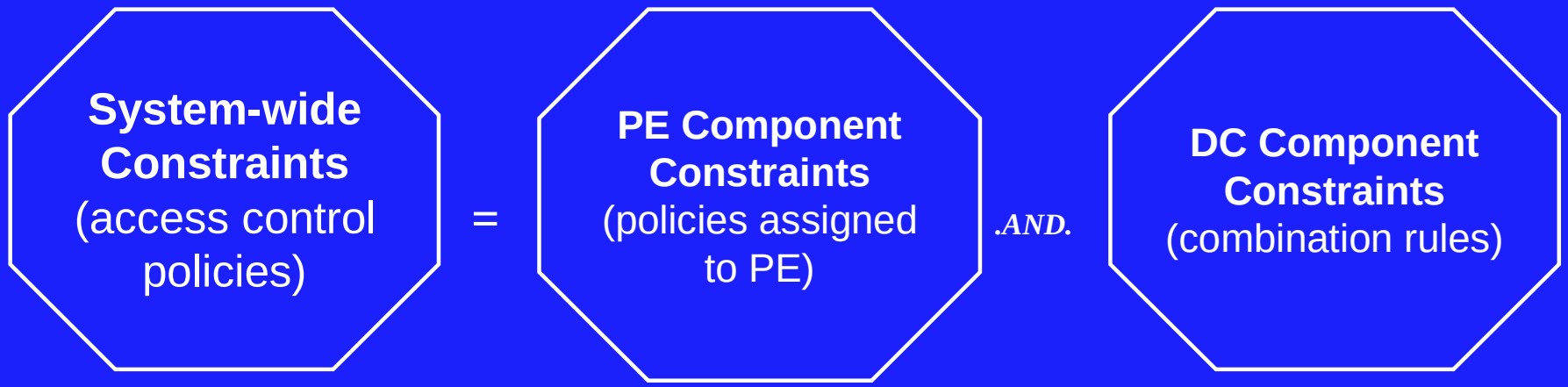
Constraints:

$[\forall(SA, op, rsn, d)\ \Box P15.(SA, op, rsn) \wedge (\ res \notin RES) \rightarrow \ \blacklozenge\ P16.d \wedge(\ d = \text{'U'})]$

$\wedge[\forall(SA, op, rsn, d)\ \Box\ P15.(SA, op, rsn) \wedge(res \in RES) \wedge (\exists\ rl \in SA, (rl, op,\ rsn) \in PA)$
$\rightarrow \blacklozenge\ P3.d \wedge(\ d = \text{'Y'})]$

$\wedge[\forall(SA, op, rsn, d)\ \Box\ P15.(SA, op, rsn) \wedge(res \in RES) \wedge (\forall\ rl \in SA, (rl, op, rsn) \notin PA)$
$\rightarrow \blacklozenge\ P3.d \wedge(\ d = \text{'N'})]$

System-wide Constraint Decomposition



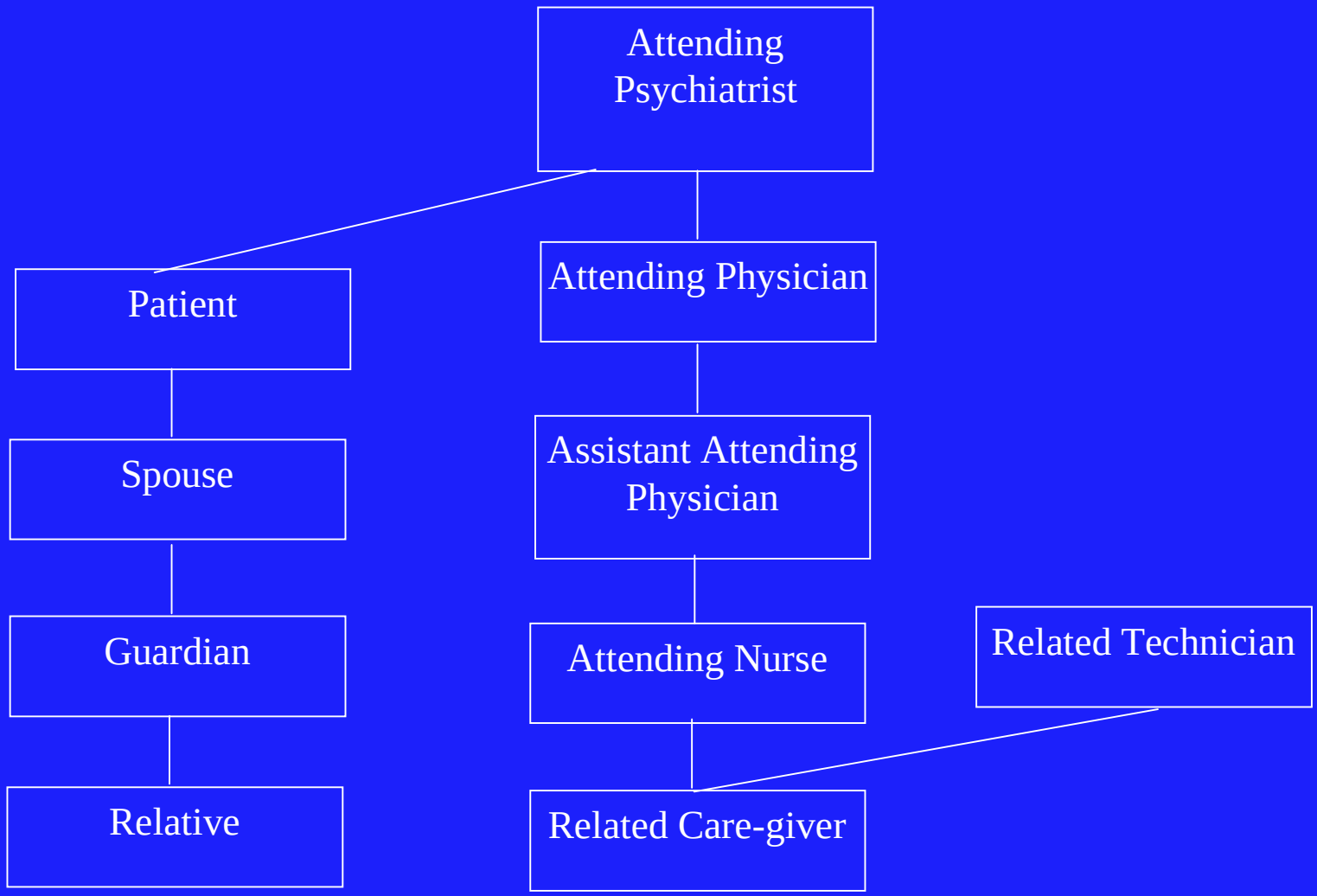
Compositional Analysis of Behavior Model

- Component analysis
  - each component analyzed individually against component constraints
- Composition analysis
  - composition constraints defined on multiple components verified based on composition of component analysis
- Analysis driven by satisfaction of architectural constraints.

New Policies

No.	Description
P2-1	Any **care-giver** can read patient's name.
P2-2	**Registration clerk** can modify patient name and demographic information.
P2-3	**Nurse** can read patient's name and demographic information.
P2-4	**Attending nurse,** in addition to the rights of any other nurse, can modify current episode demographic information, can read current episode regular records and current episode regular test results.
P2-5	**Technician** can read patient's name and modify current episode regular test results.
P2-6	**Related technician**, in addition to the rights of any other technician, can modify current episode sensitive test results.
P2-7	**Attending assistant physician**, in addition to what a nurse can do, can also read all (i.e. from the current and previous episodes) regular records and all regular test results, as well as to modify current episode regular records.
P2-8	**Attending physician**, in addition to the rights of attending assistant physician, can modify current episode sensitive regular records and can read all regular and sensitive records from previous episodes.
P2-9	**Attending psychiatrist**, in addition to what an attending physician can do, also can modify mental information.
P2-10	**Patient relative** can read patient's current episode demographic and patient's name.
P2-11	**Patient guardian** can read previous episode regular data.
P2-12	**Patient spouse** can read previous episode sensitive data.
P2-13	**Patient representative** can read previous episode regular data provided that patient gives a consent.

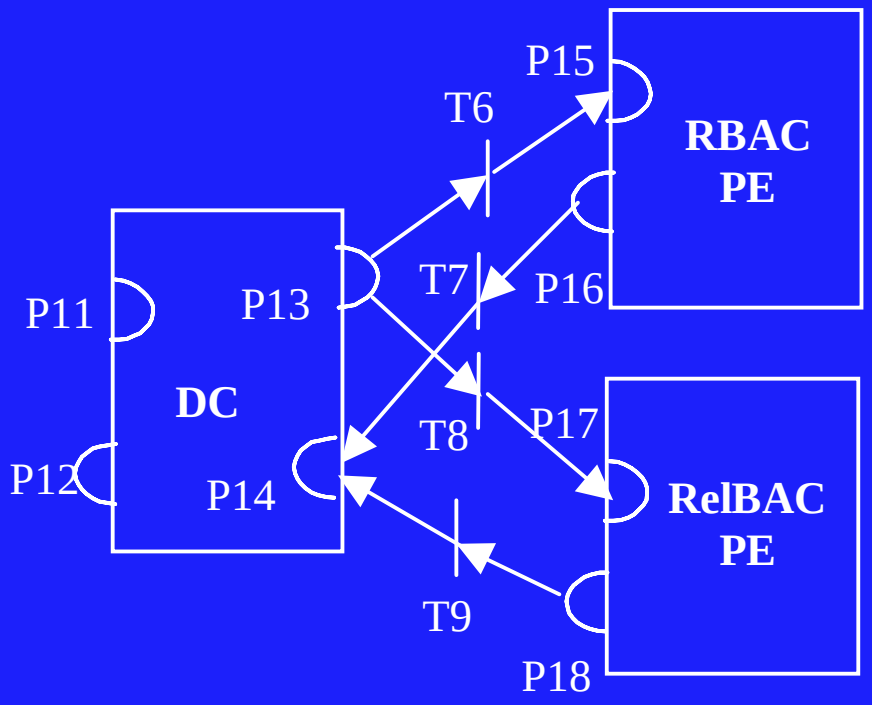
Relationship Hierarchy



Relationship to Permission Assignment Relation

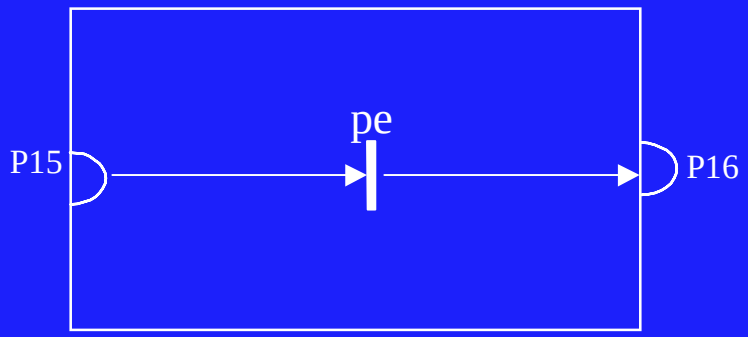
Relationships		Resources											
		PN	DD	CDD	CRR	CSR	CRT	CST	PRR	PSR	PRT	PST	AMD
	Attending Psychiatrist												RW
	Attending Physician					RW		R		R		R	
	Attending Physician Assistant				RW		R		R		R		
	Attending Nurse			RW	R		R						
	Related Technician							RW					
	Related Care-giver	R											
	Patient												
	Spouse									R		R	
	Guardian								R		R		
	Relative	R	R										

DC&PEs Model for Relationship-based Policies



P13 Attributes
P14 Decisions from PE's
P15 Attributes received by RBAC PE
P16 Decision made by RBAC PE
P17 Attributes received by RelAC PE
P18 Decision made by RelBAC PE
T6 DC invokes RBAC PE
T7 RBAC PE passes decision to DC
T8 DC invokes RelBAC PE
T9 RelBAC PE passes decision to DC

Performance Model of Policy Evaluator



(Transition *pe* is associated with stochastic firing times.)

Constraint:

$[\forall(x, y)\ \Box P15.x \rightarrow\ \blacklozenge\ P16.y \wedge (Expectation(\ y - x) \leq 10)]$

The Next Steps

- Distributed AAS architecture
  - prototype of distributed and CORBA-based AAS
- Case study
  - real life policies in healthcare (HIPAA)
  - sample application(s)
  - workload and scenario simulation
  - collaborators: NIST, Las Alamos National Lab
- Aspect-oriented modeling framework for security services
  - collaborator: University of Illinois at Chicago