Toward Usable Security Administration

Konstantin Beznosov

The University of British Columbia

Outline

- What’s the problem?
- Why is usability of sec. admin. important?
- What are we doing?

What’s the problem?

Classical Access Control Solution

Domains

D

Have access to objects

Access Matrix

A

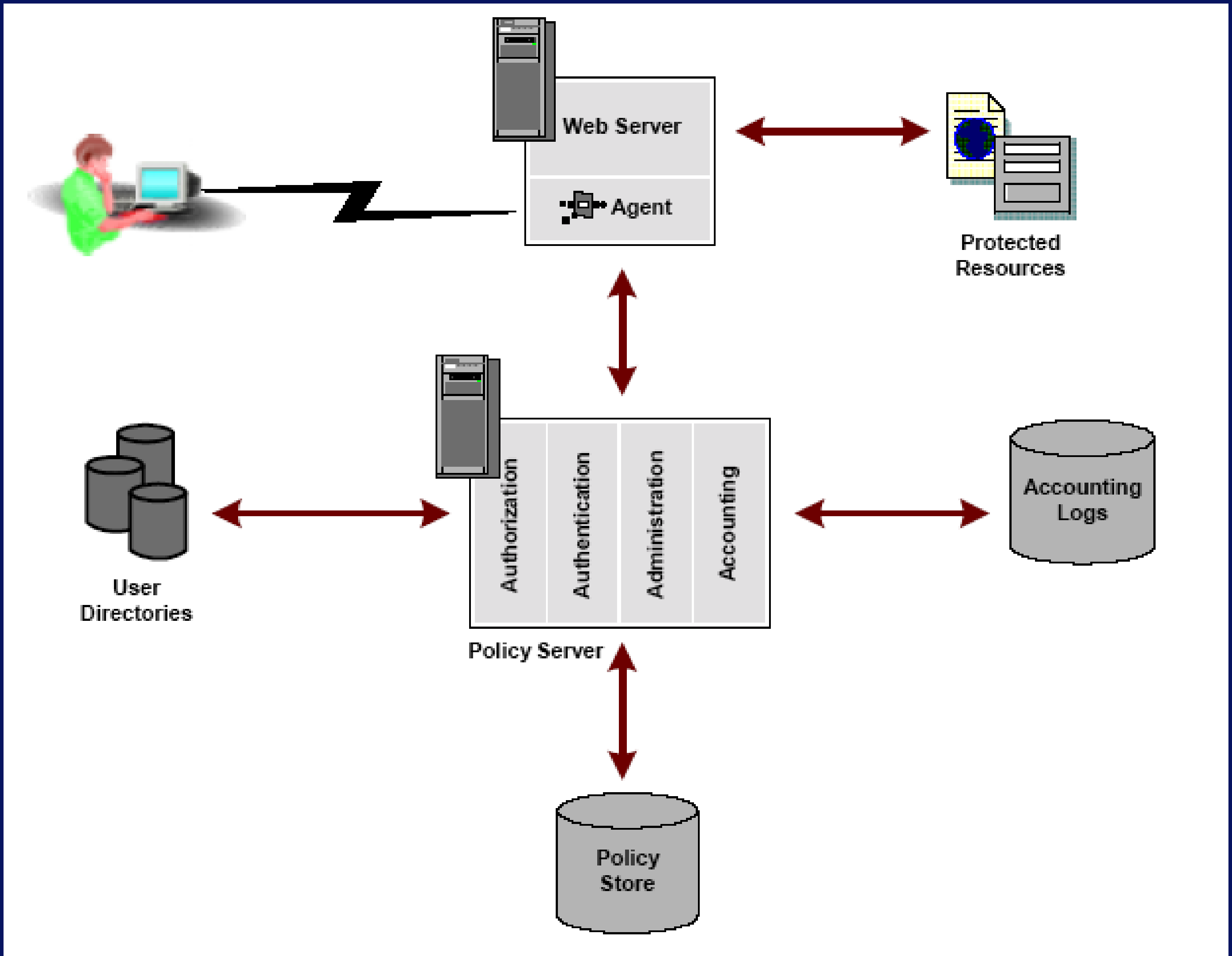
	Domain 1	Domain 2	Domain 3	File 1	File 2	Process 1
Domain 1	*owner control	*owner control	*call	*owner *read *write		
Domain 2			call	*read	write	wakeup
Domain 3			owner control	read	*owner	

Objects

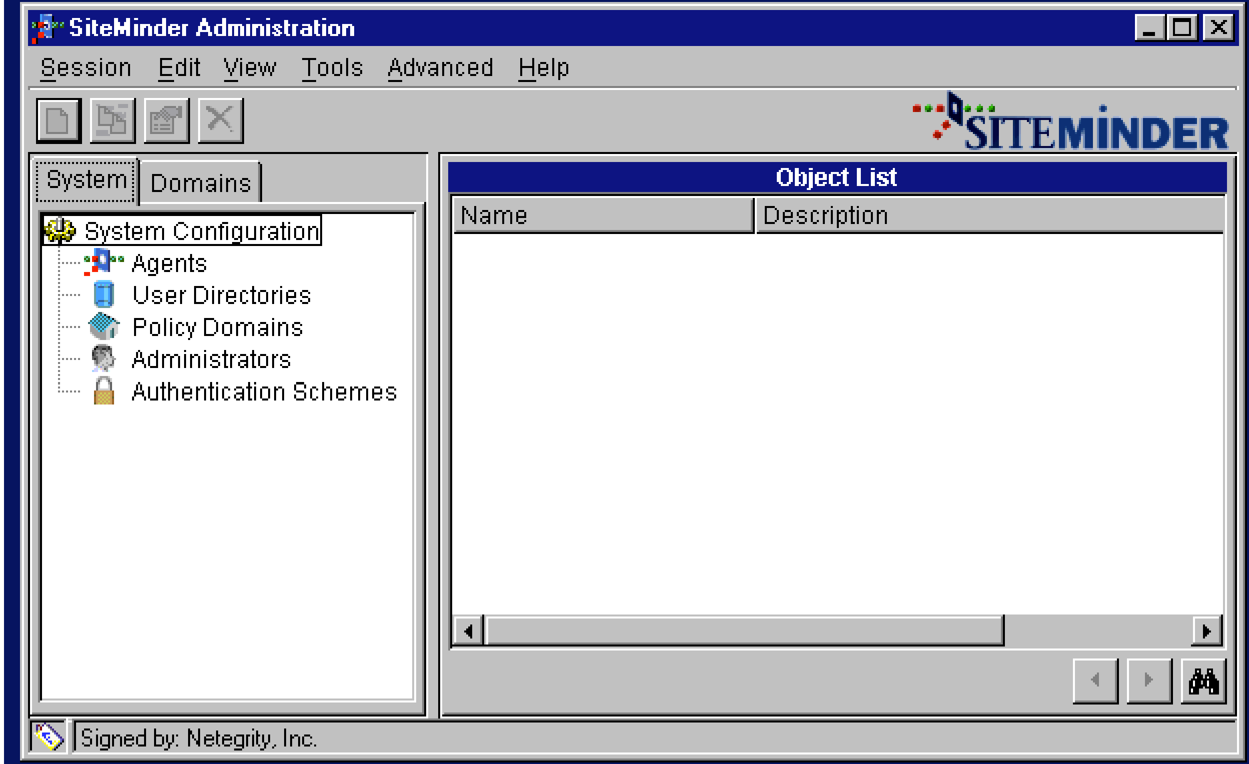
X

To be protected

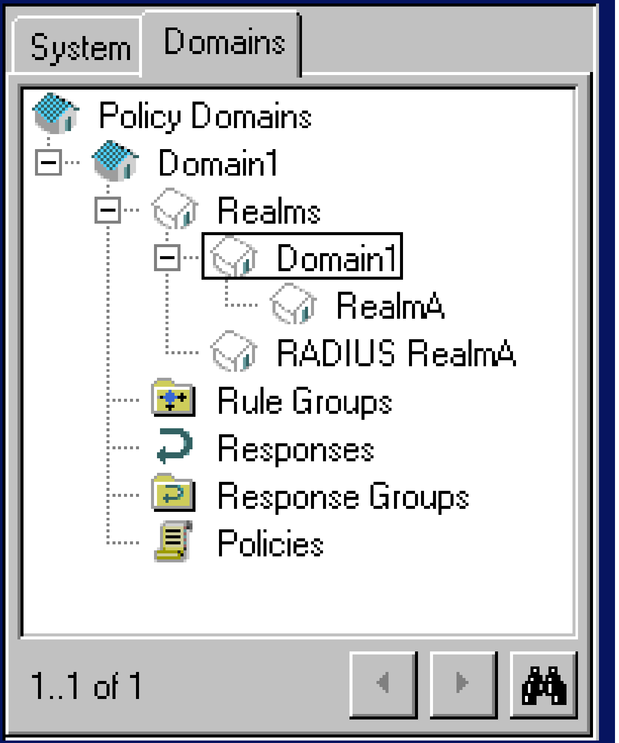
Enterprise-scale security server



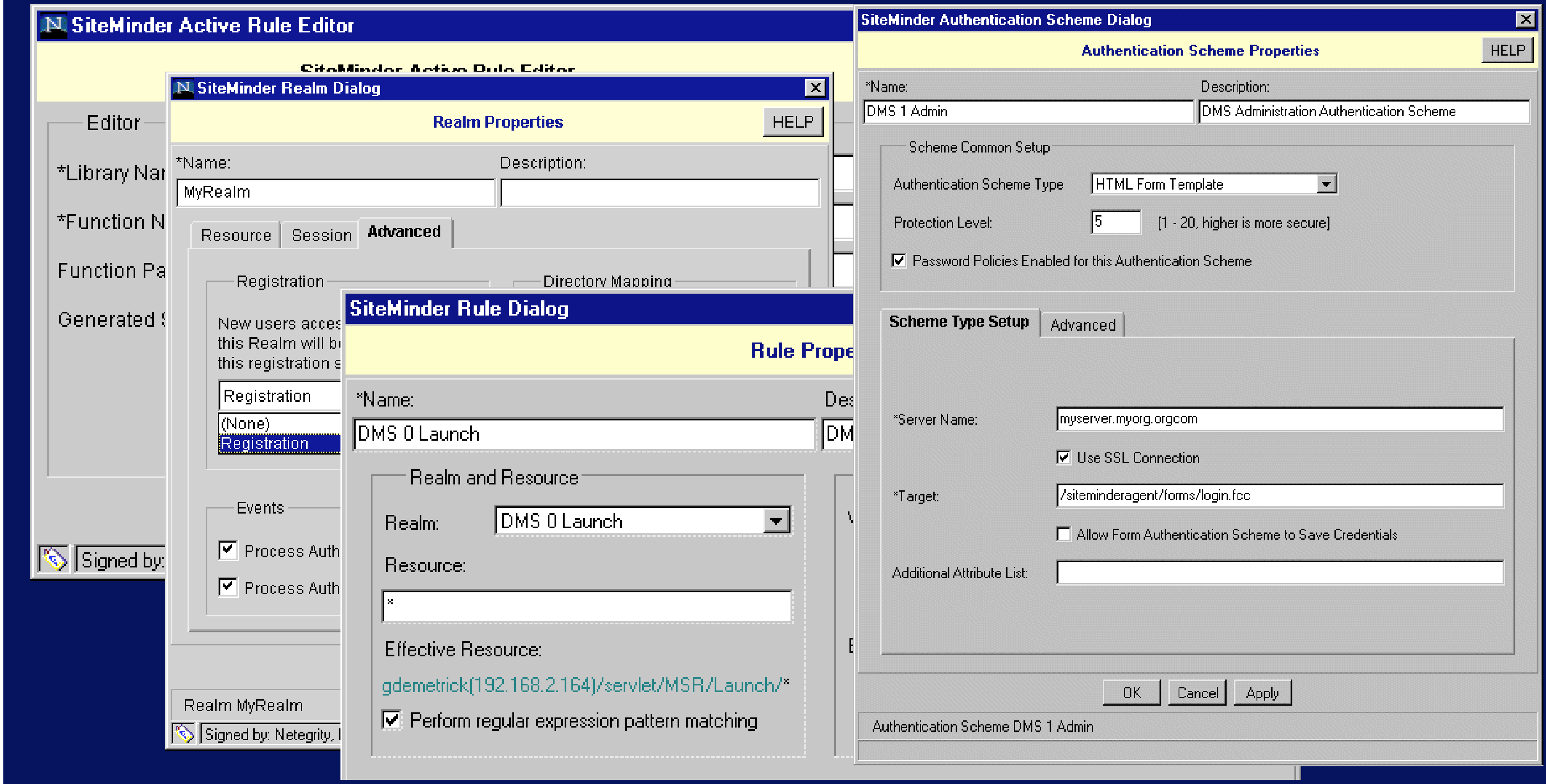
Everything starts with simple directory tree like structure



Signed by: Netegrity, Inc.



Then continues with simple forms to fill out …



SiteMinder Active Rule Editor

SiteMinder Active Rule Editor

Editor

*Library Nar

*Function N

Function Pa

Generated S

Signed by:

SiteMinder Realm Dialog

Realm Properties HELP

*Name: MyRealm

Description:

Resource | Session | Advanced

Registration

New users acces this Realm will b this registration s

Registration

(None)

Registration

Directory Mapping

Events

☑ Process Auth

☑ Process Auth

Realm MyRealm

Signed by: Netegrity, I

SiteMinder Rule Dialog

Rule Prope

*Name: DMS 0 Launch

Des DM

Realm and Resource

Realm: DMS 0 Launch

Resource: *

Effective Resource: gdemetrick(192.168.2.164)/servlet/MSR/Launch/*

☑ Perform regular expression pattern matching

SiteMinder Authentication Scheme Dialog

Authentication Scheme Properties HELP

*Name: DMS 1 Admin

Description: DMS Administration Authentication Scheme

Scheme Common Setup

Authentication Scheme Type: HTML Form Template

Protection Level: 5 [1 - 20, higher is more secure]

☑ Password Policies Enabled for this Authentication Scheme

Scheme Type Setup | Advanced

*Server Name: myserver.myorg.orgcom

☑ Use SSL Connection

*Target: /siteminderagent/forms/login.fcc

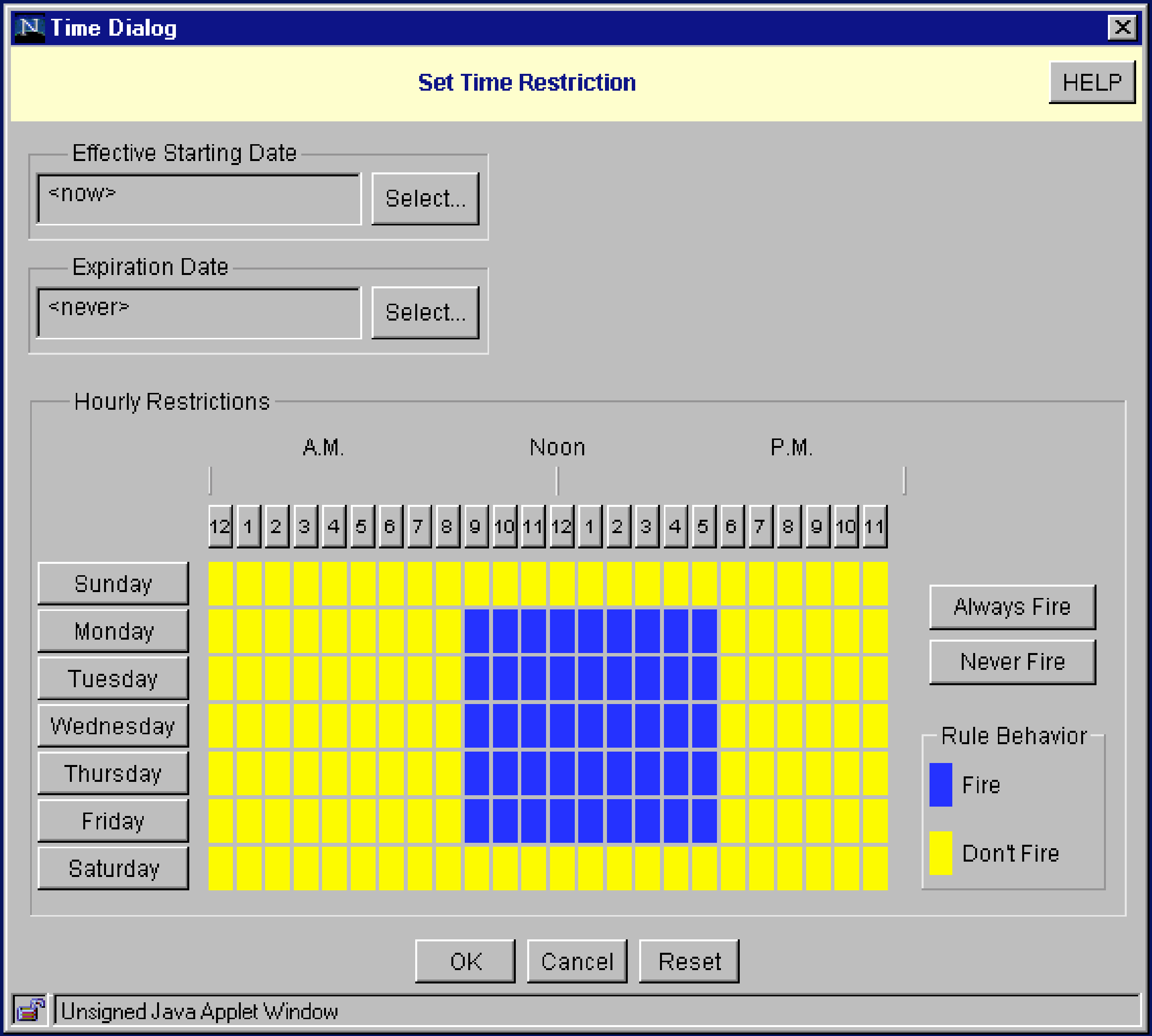
□ Allow Form Authentication Scheme to Save Credentials

Additional Attribute List:

OK Cancel Apply

Authentication Scheme DMS 1 Admin

… or select



Time Dialog

Set Time Restriction

HELP

Effective Starting Date

<now>

Select...

Expiration Date

<never>

Select...

Hourly Restrictions

A.M. Noon P.M.

	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
Sunday	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Monday	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟨	🟨	🟨	🟨	🟨	🟨
Tuesday	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟨	🟨	🟨	🟨	🟨	🟨
Wednesday	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟨	🟨	🟨	🟨	🟨	🟨
Thursday	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟨	🟨	🟨	🟨	🟨	🟨
Friday	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟨	🟨	🟨	🟨	🟨	🟨
Saturday	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨

Always Fire

Never Fire

Rule Behavior

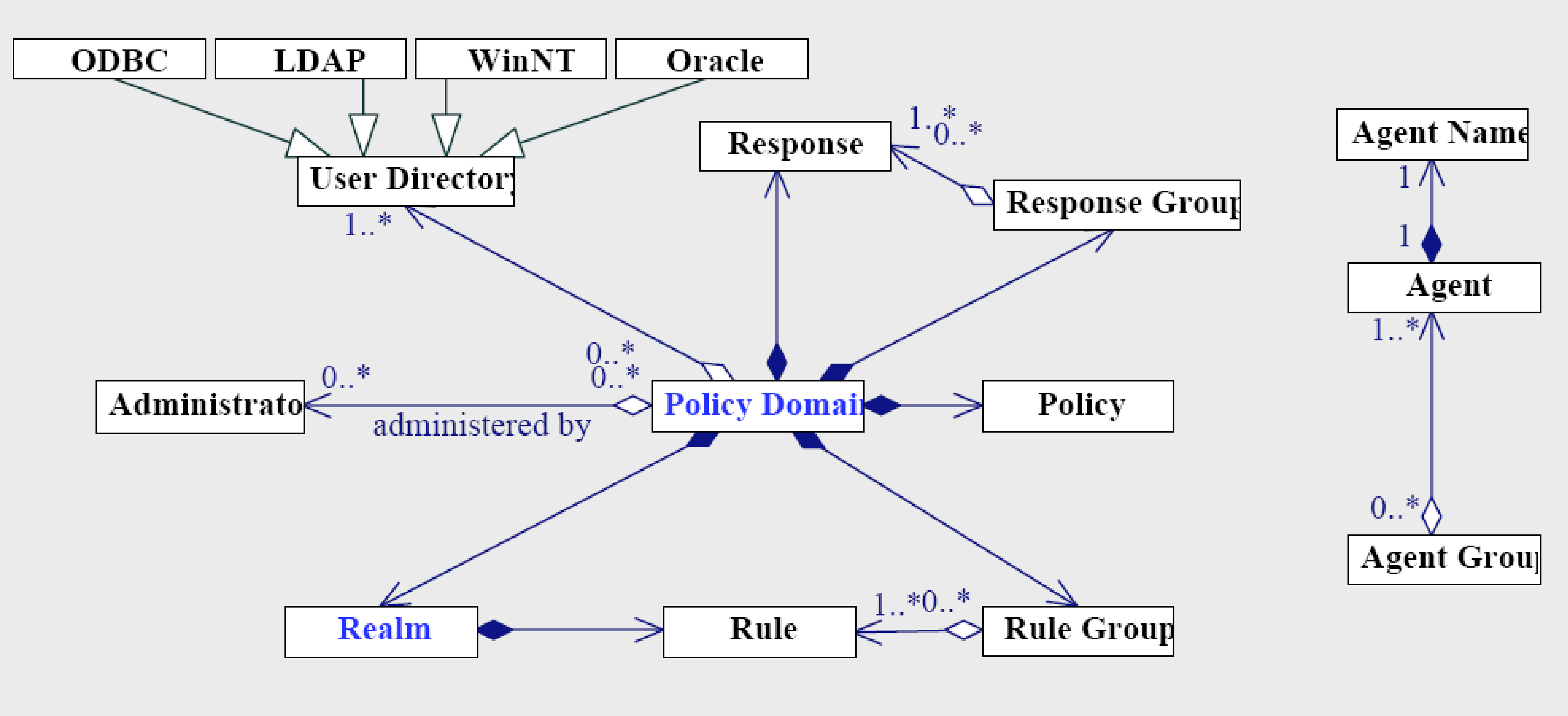
🟦 Fire

🟨 Don't Fire

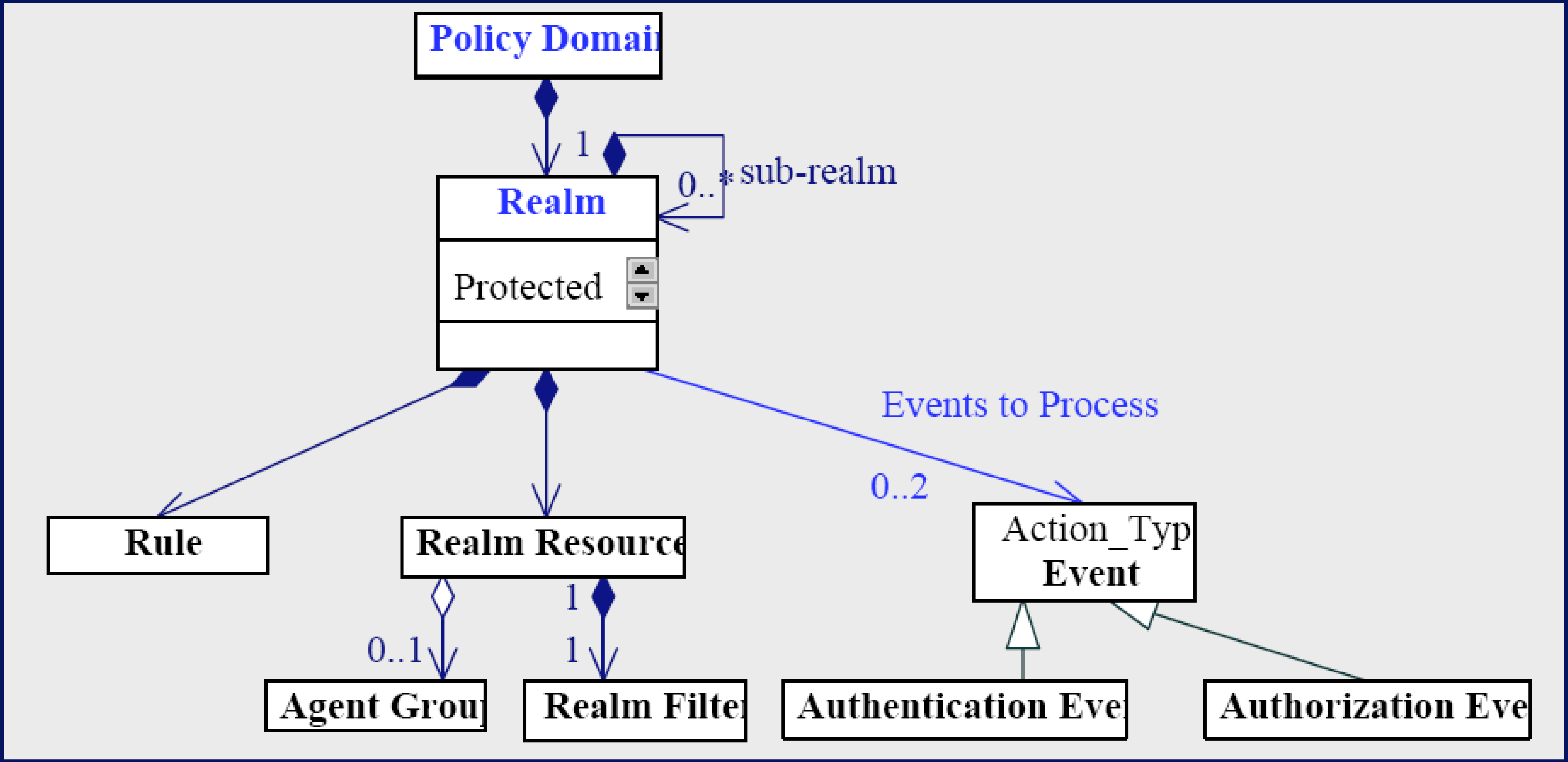
OK Cancel Reset

Unsigned Java Applet Window

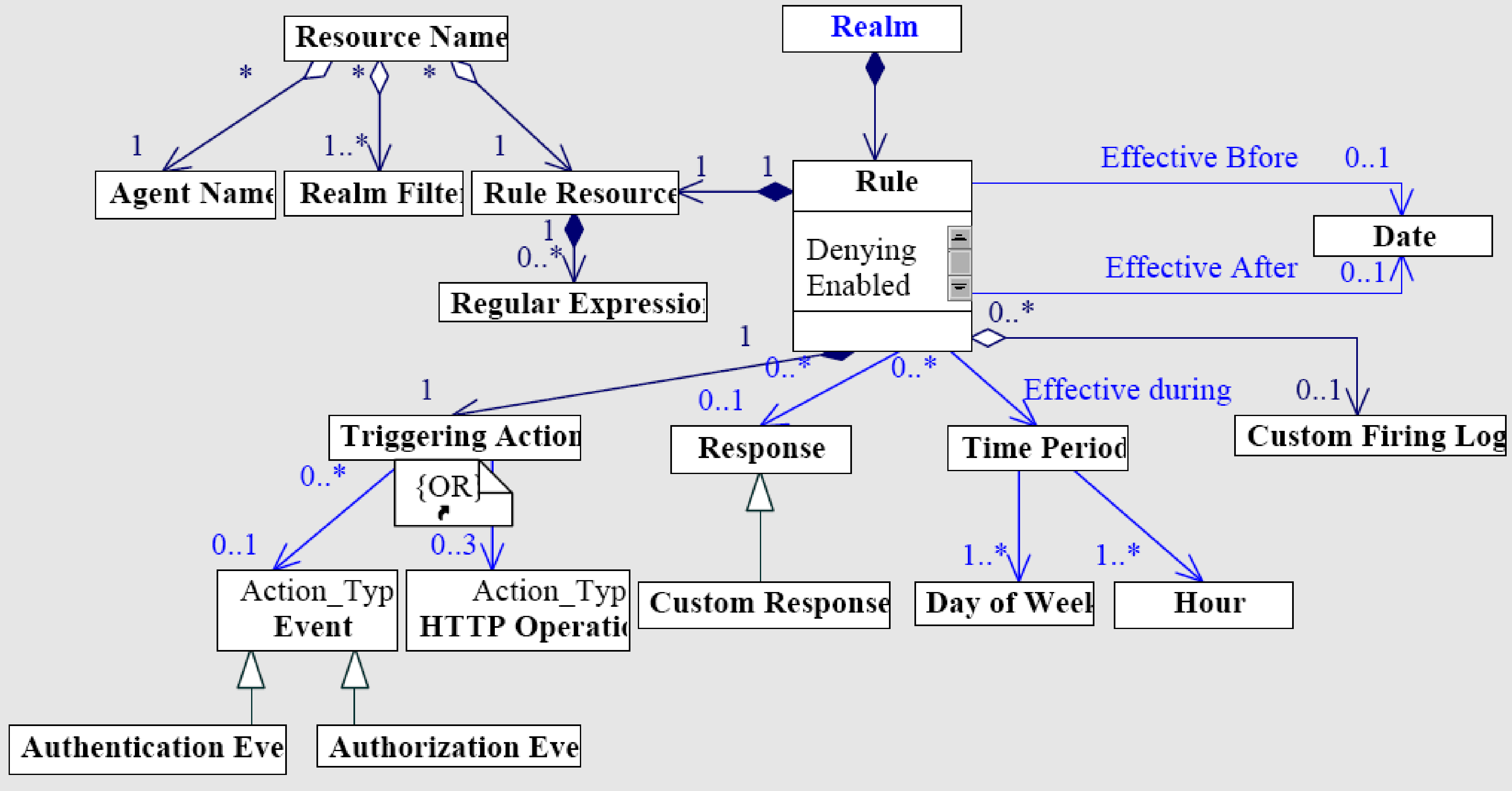
but the mental model is complex



… and even more …



… complex


Resource Name
Realm
*
*
*
1
1..*
1
Agent Name
Realm Filte
Rule Resource
1
1
Rule
Denying
Enabled
Effective Bfore
0..1
Date
Effective After
0..1
1
0..*
Regular Expressio
0..*
1
0..*
0..*
1
0..1
Effective during
0..1
Triggering Action
Response
Time Period
Custom Firing Log
0..*
{OR}
0..1
0..3
1..*
1..*
Action_Typ
Event
Action_Typ
HTTP Operati
Custom Response
Day of Weel
Hour
Authentication Eve
Authorization Eve

so what?

- **Steep learning** curve
- **Hard to fit** real world into the model
- Easy to make **costly mistakes**
  - “friendly” DoS
  - inadvertent hard to catch vulnerabilities
- **Hard to test**
  - **Expensive** to test required scenarios
  - **No** “what if” **scenarios** to test before changing
  - Hard to perform **complete testing**
- Motivates users and admins to **circumvent security**

the take on the problem

- improving **visualization** of the information
  - existing cognitive models of security administration
- improving **feedback** to security administrators
  - "what if" **scenarios**
  - safe staging **playgrounds**
  - **testing** system state
- better **cognitive** models
- **mappings** between different mental models/abstractions
  - **application**-specific model oriented on business processes
  - **mechanism**-specific technical model

the team

(in alphabetical order)

- Dr. Konstantin Beznosov, security, SE
- Dr. Sidney Fels, HCI
- Dr. Brian Fisher, HCI
- Dr. Lee Iverson, HCI, SE

Summary

- Security administration tools are too complex → **unusable**
- Unusable sec. admin. is **expensive** and **error prone.**
- We’ll improve **visualization**, mental **models**, and **feedback**.