HOT Admin

Human, Organization, and Technology Centred Improvement of IT Security Administration

Konstantin Beznosov, Sidney Fels, Lee Iverson

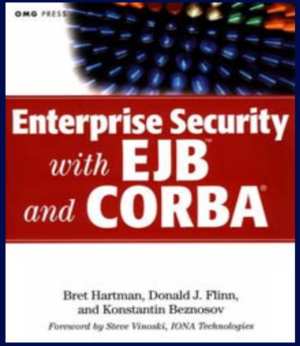
University of British Columbia

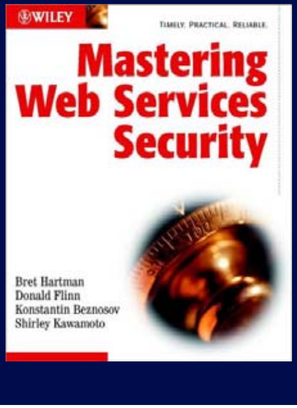
Brian Fisher

Simon Fraser University

Who’s Konstantin Beznosov

- Education
  - M.S. (1997) & Ph.D. (2000) in CS, Florida International University
  - B.S. in Physics (1993), Novosibirsk State University
- Experience
  - Assistant Prof., Electr. and Comp. Egn., UBC (2003-present)
  - Directs Laboratory for Education and Research in Secure Systems Engineering (LERSSE)
  - US industry (1997-2003): end-user, consulting, and software vendor organizations
- Contributed to
  - OMG
    - CORBA Security revisions
    - Resource Access Decision
    - Security Domain Membership Management
  - OASIS
    - eXtensible Access Control Markup Language v1.0


OMG PRESS
Enterprise Security with EJB and CORBA
Bret Hartman, Donald J. Flinn, and Konstantin Beznosov
Foreword by Steve Vinoski, IONA Technologies



Hypothetical Example

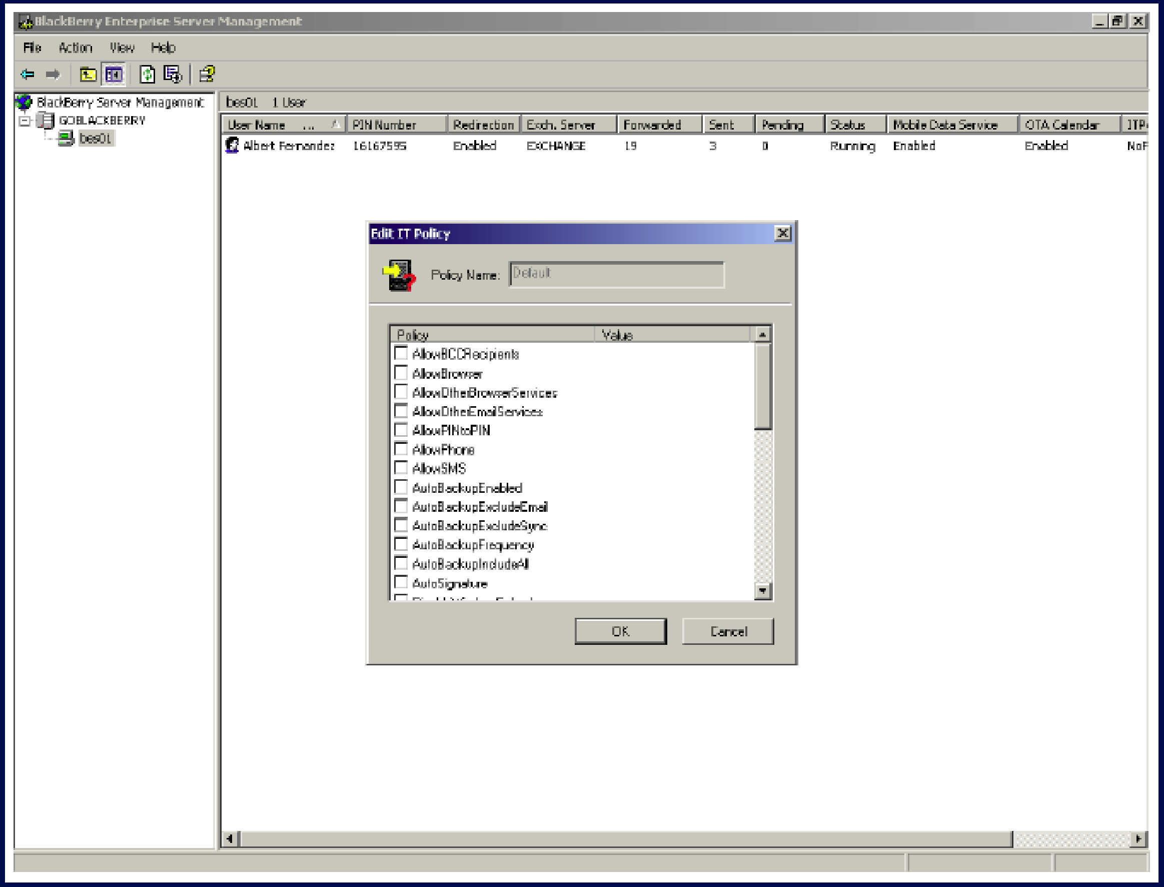
ABC Inc.
large company
with 5 divisions

Jehny Smith
senior security administrator
at ABC

Business policy:

All e-mail messages between senior management
must be end-to-end secure

Blackberry Enterprise Server Management


BlackBerry Enterprise Server Management
File
Action
View
Help
BlackBerry Server Management
GOBLACKBERRY
bes01
OK
Cancel

bes01 1 User

User Name	PIN Number	Redirection	Exch. Server	Forwarded	Sent	Pending	Status	Mobile Data Service	OTA Calendar	ITP
Albert Fernandez	16167595	Enabled	EXCHANGE	19	3	0	Running	Enabled	Enabled	NoF

Edit IT Policy

Policy Name: Default

Policy	Value
□ AllowBCCRecipients	
□ AllowBrowser	
□ AllowOtherBrowserServices	
□ AllowOtherEmailServices	
□ AllowPINtoPIN	
□ AllowPhone	
□ AllowSMS	
□ AutoBackupEnabled	
□ AutoBackupExcludeEmail	
□ AutoBackupExcludeSync	
□ AutoBackupFrequency	
□ AutoBackupIncludeAll	
□ AutoSignature	

Configuring BES to Enforce the Policy

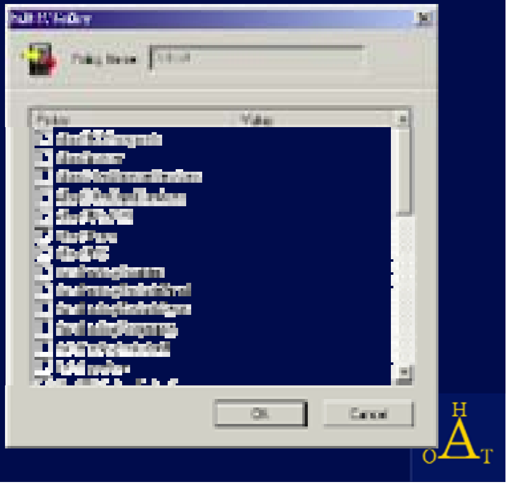
1. turn MIME (S/MIME) encryption on
2. enable S/MIME encryption for the user

- set alpha-numeric rules:
  3. Cert. Status Cache Timeout
  4. Cert. Status Maximum Expiry Time
  5. FIPS Level
  6. S/MIME Allowed Content Ciphers
  7. Trusted Certificate Thumbprints
- Set to False
  8. Allow Other Email Services
- Set to True:
  9. Disable Email Normal Send
  10. Attachment Viewing
  11. S/MIME Force Digital Signature
  12. S/MIME Force Encrypted Email
  13. Disable Invalid Certificate Use
  14. Disable Revoked Certificate Use
  15. Disable Stale Status Use
  16. Disable Untrusted Certificate Use
  17. Disable Unverified Certificate Use
  18. Disable Unverified CRLs
  19. Disable Weak Certificate Use

Total 19 steps!

It’s Not All!

- Now do (most of) the same for other senior managers
- Now do the same on other four servers
- Hard
  - Which of 140 rules need to be set and how?
  - How to remember the right values?
  - How to make sure these are the right values?
  - How to make sure no error was made?



Obvious Limitations of the GUI

- Some interrelations can easily be confused
  - Five rules on public key
    - disable sending of messages encrypted with “Invalid,” or “Revoked,” or “Untrusted,” or “Unverified,” or “Weak” certificates
    - Can a certificate have more than one status, e.g., “Weak” and “Unverified”?
    - What is the result of applying more than one of these rules to the same certificate?
    - Which one overrides others, and in what circumstances?
- Difficult to determine the results of changes
  - with the “FIPS Level” = “2”
    - the values of 8 other rules (“Password Required,” etc.) are automatically forced to specific values.
- Miss-grouped commands may cause confusion
  - Maximum Security Timeout + Non-Grouped Device-Only

Another Example: Enterprise Authorization Servers

classical access control solution

subjects

S

Have access to objects

objects

O

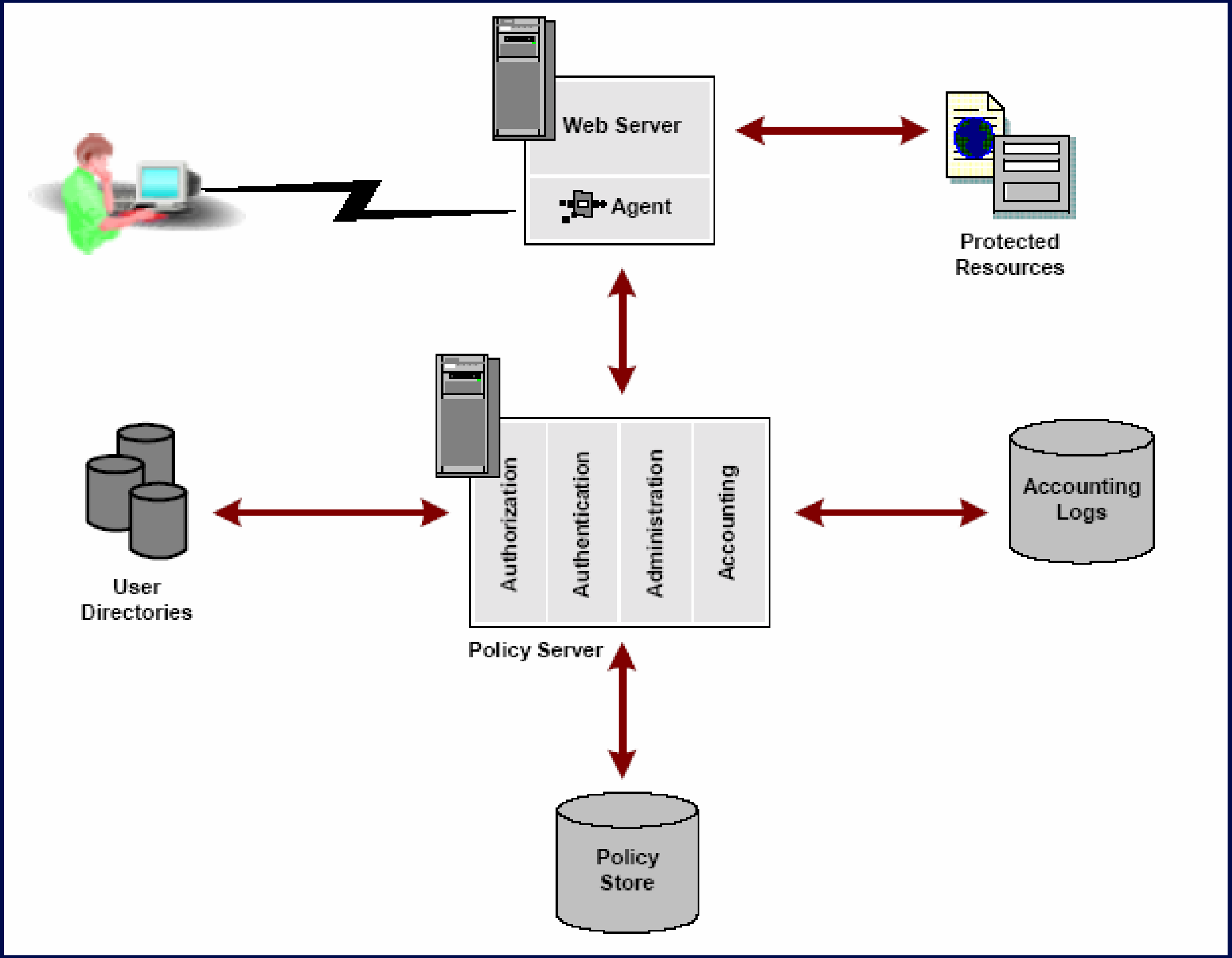
To be protected

Access Matrix

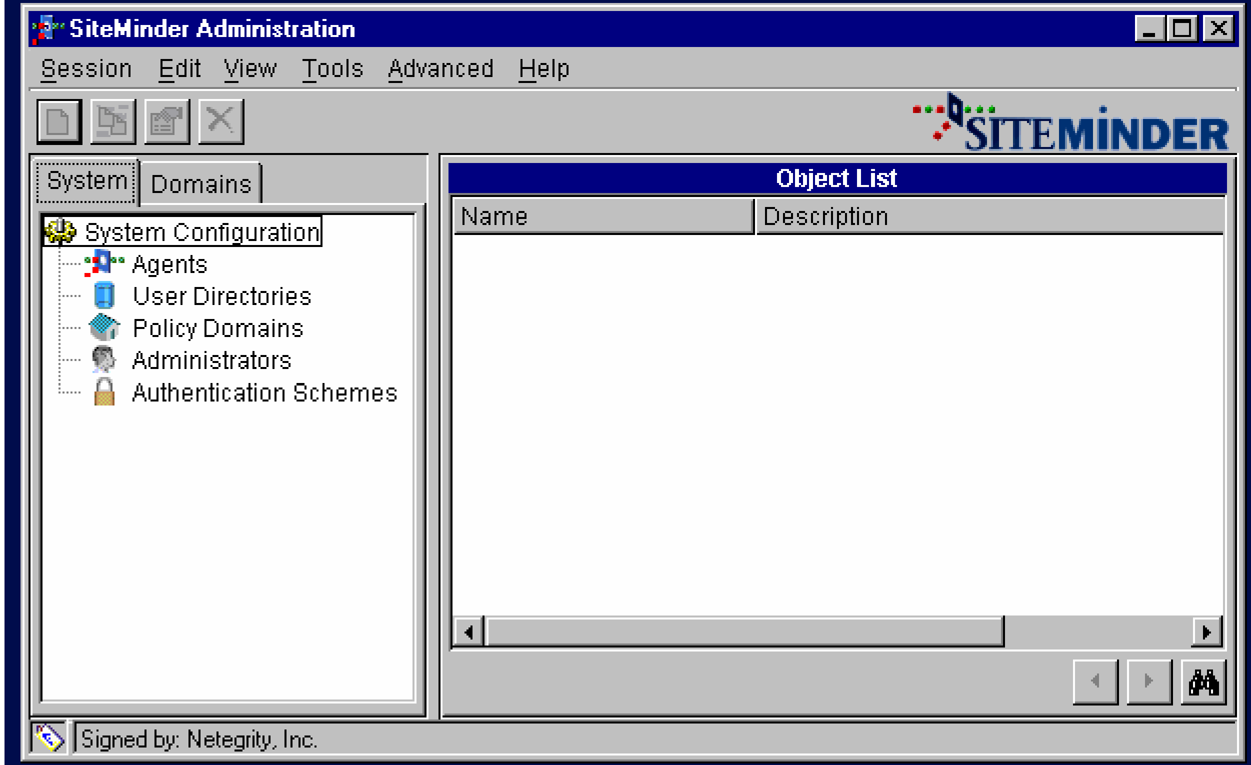
A

	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	

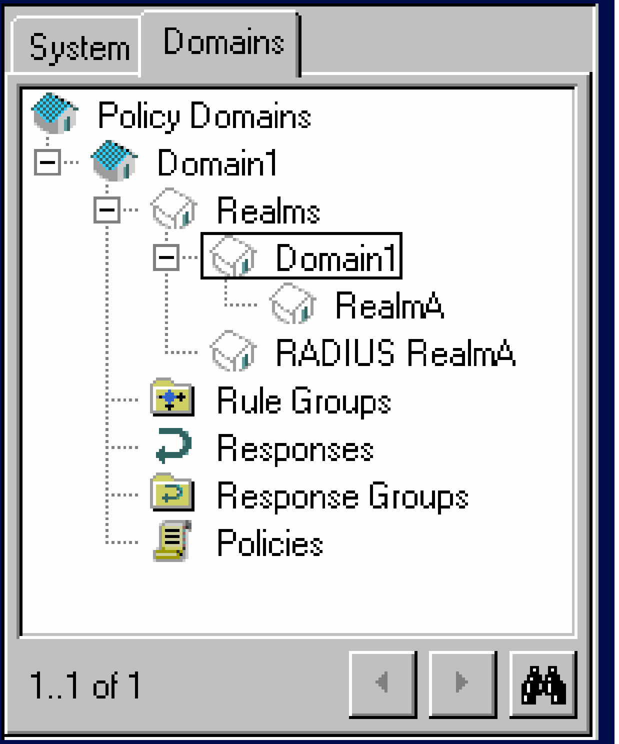
enterprise-scale security server



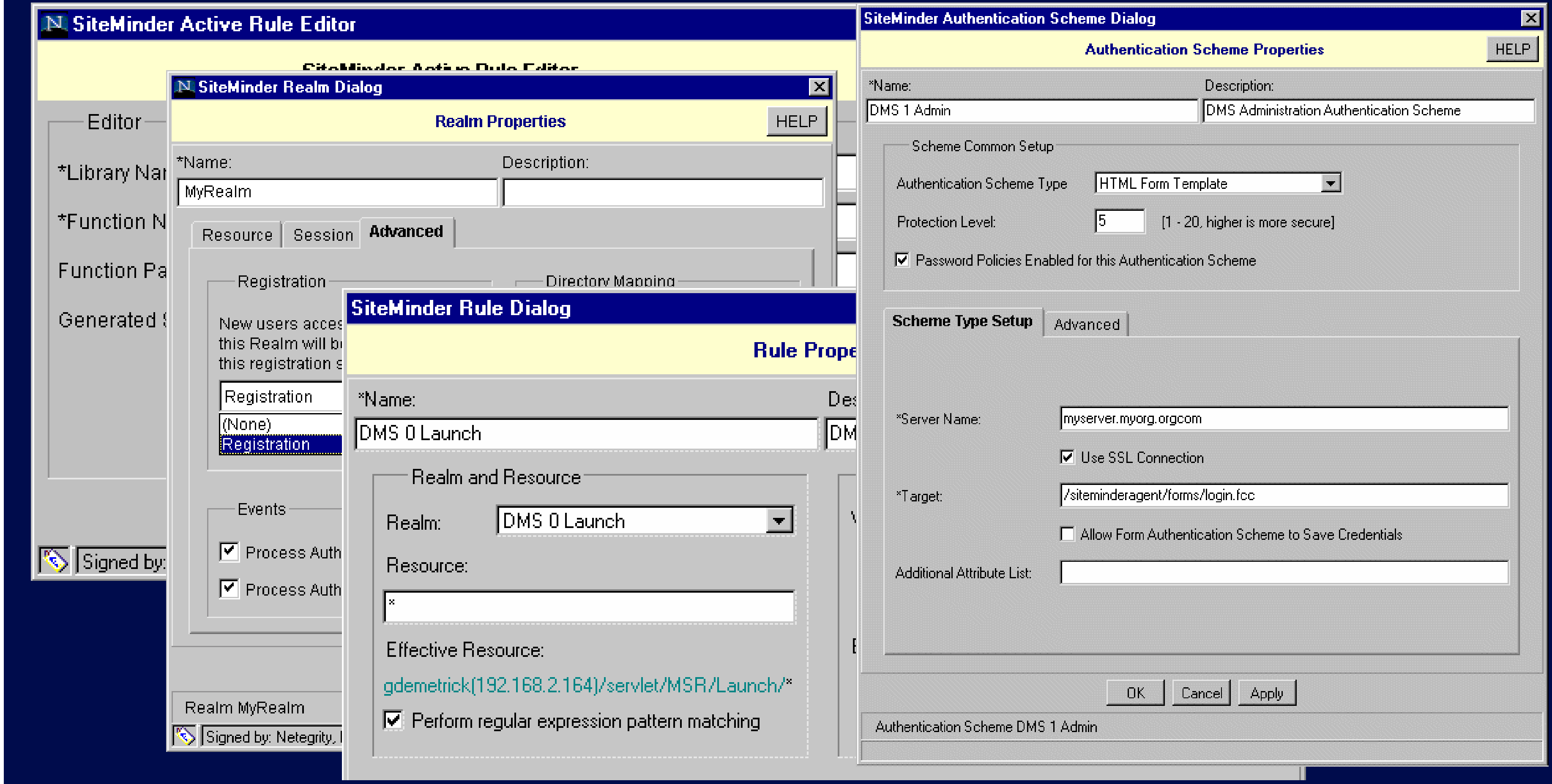
everything starts with simple tree-like structure



Signed by: Netegrity, Inc.



then continues with simple forms to fill out …



SiteMinder Active Rule Editor

Editor

*Library Nar

*Function N

Function Pa

Generated S

Signed by:

SiteMinder Realm Dialog

Realm Properties

*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

*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

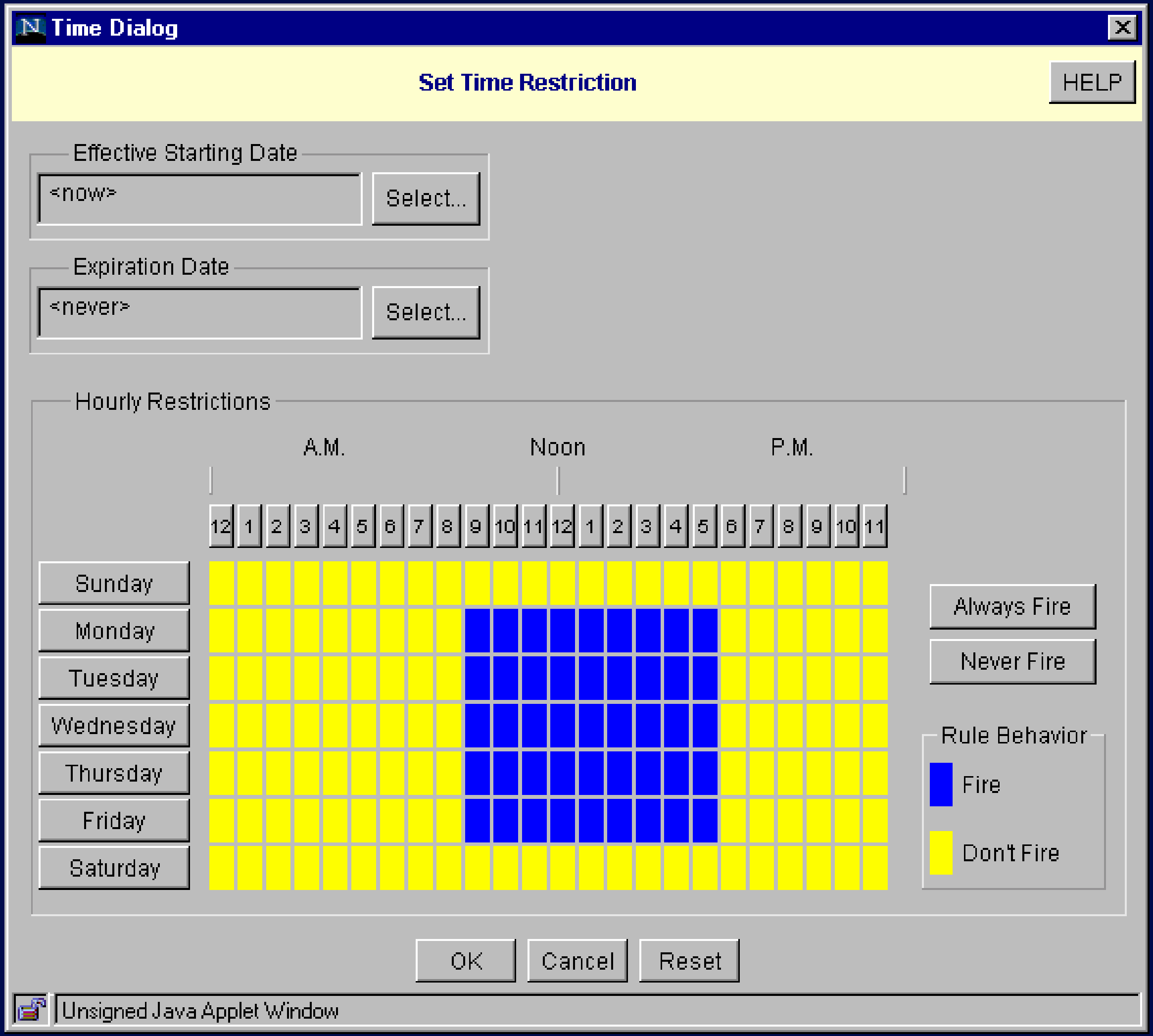
*Target: /siteminderagent/forms/login.fcc

☐ Allow Form Authentication Scheme to Save Credentials

Additional Attribute List:

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

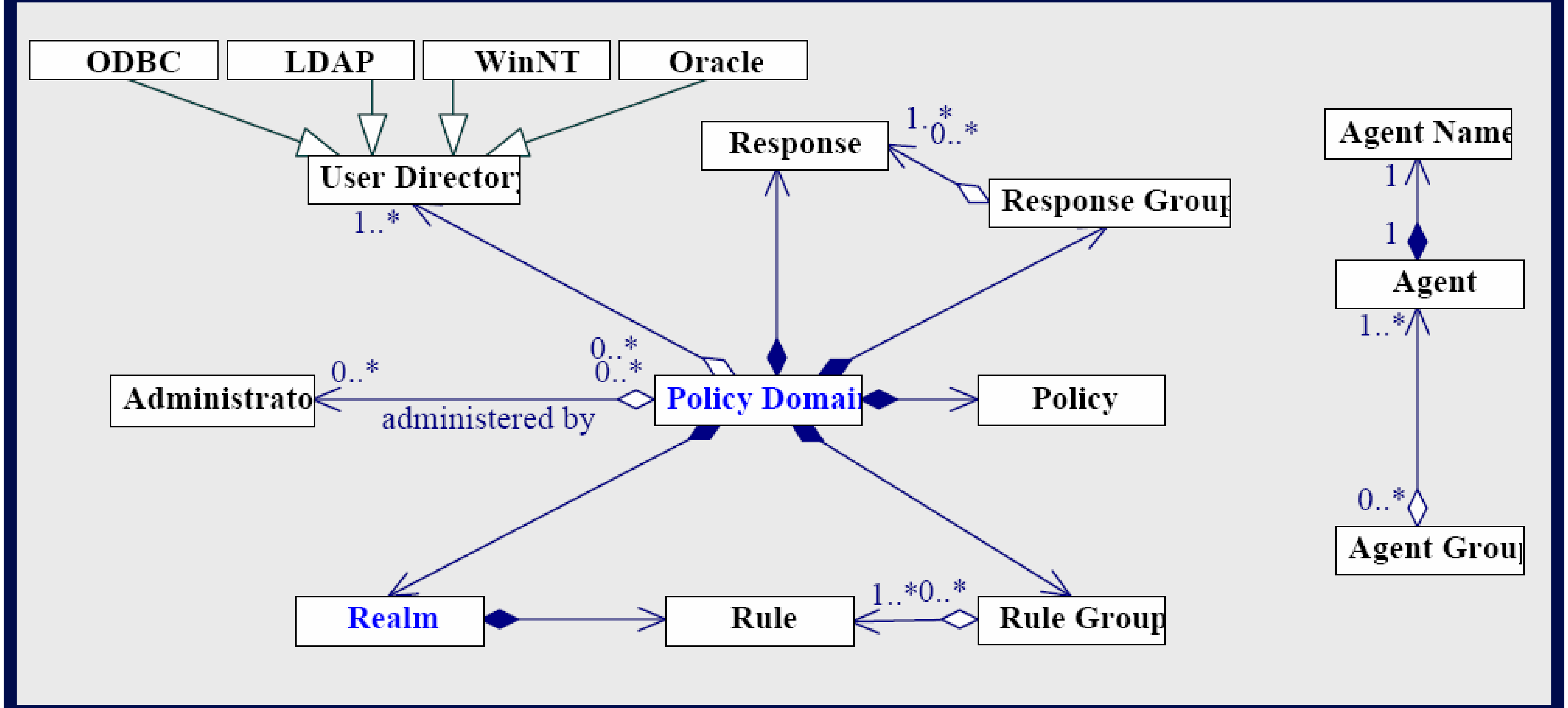
🟦 Fire

🟨 Don't Fire

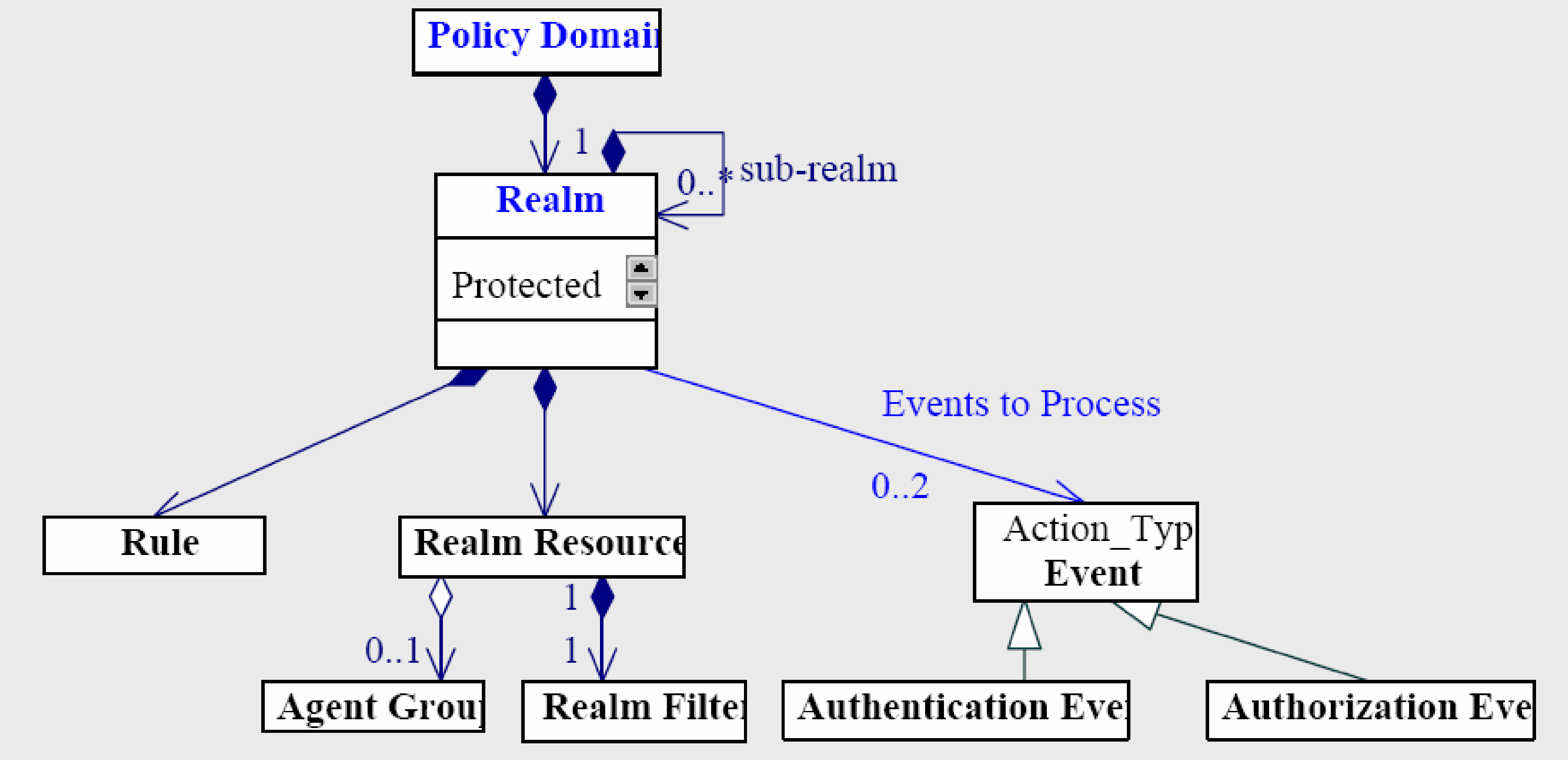
OK Cancel Reset

Unsigned Java Applet Window

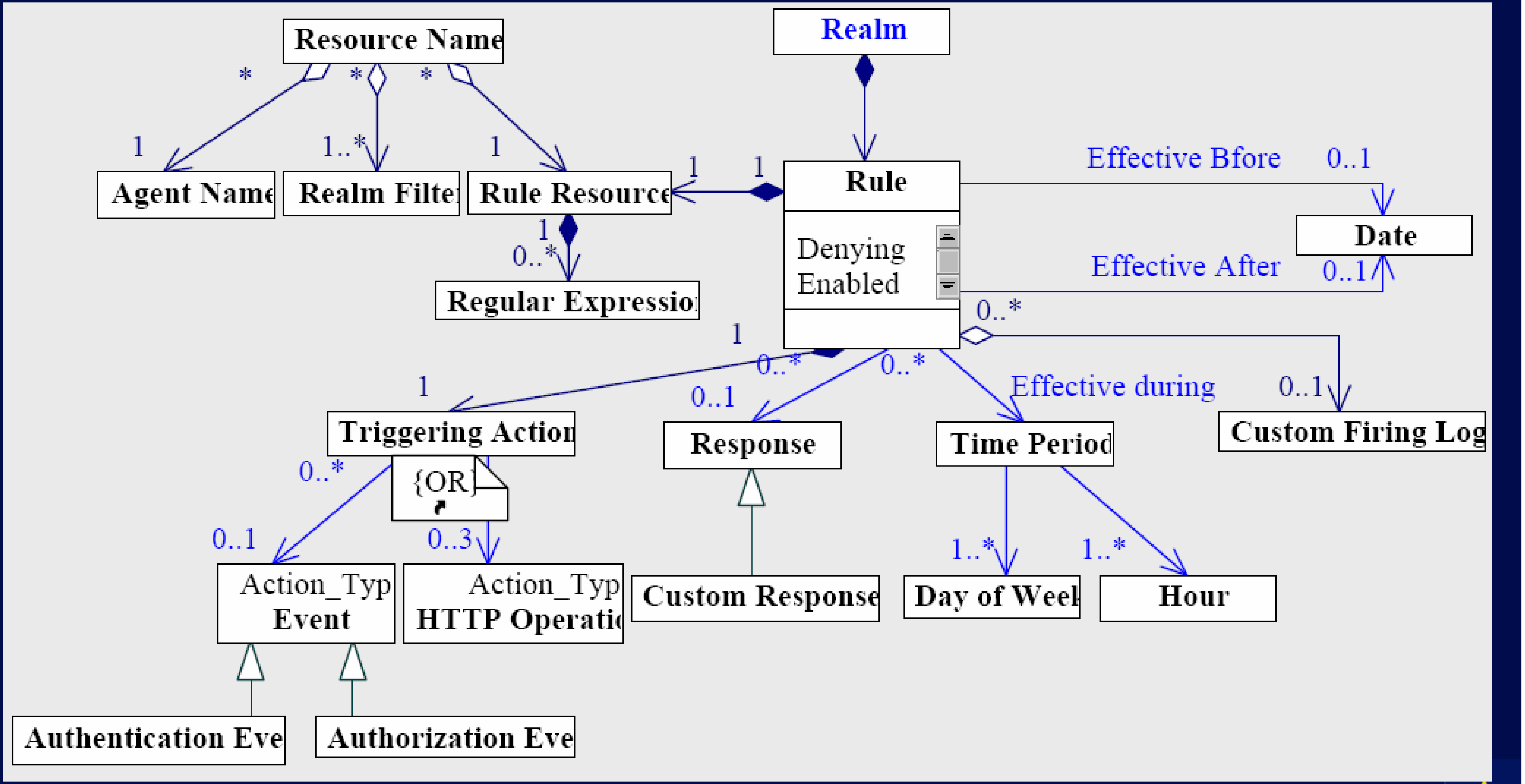
but the mental model is complex



… and even more …

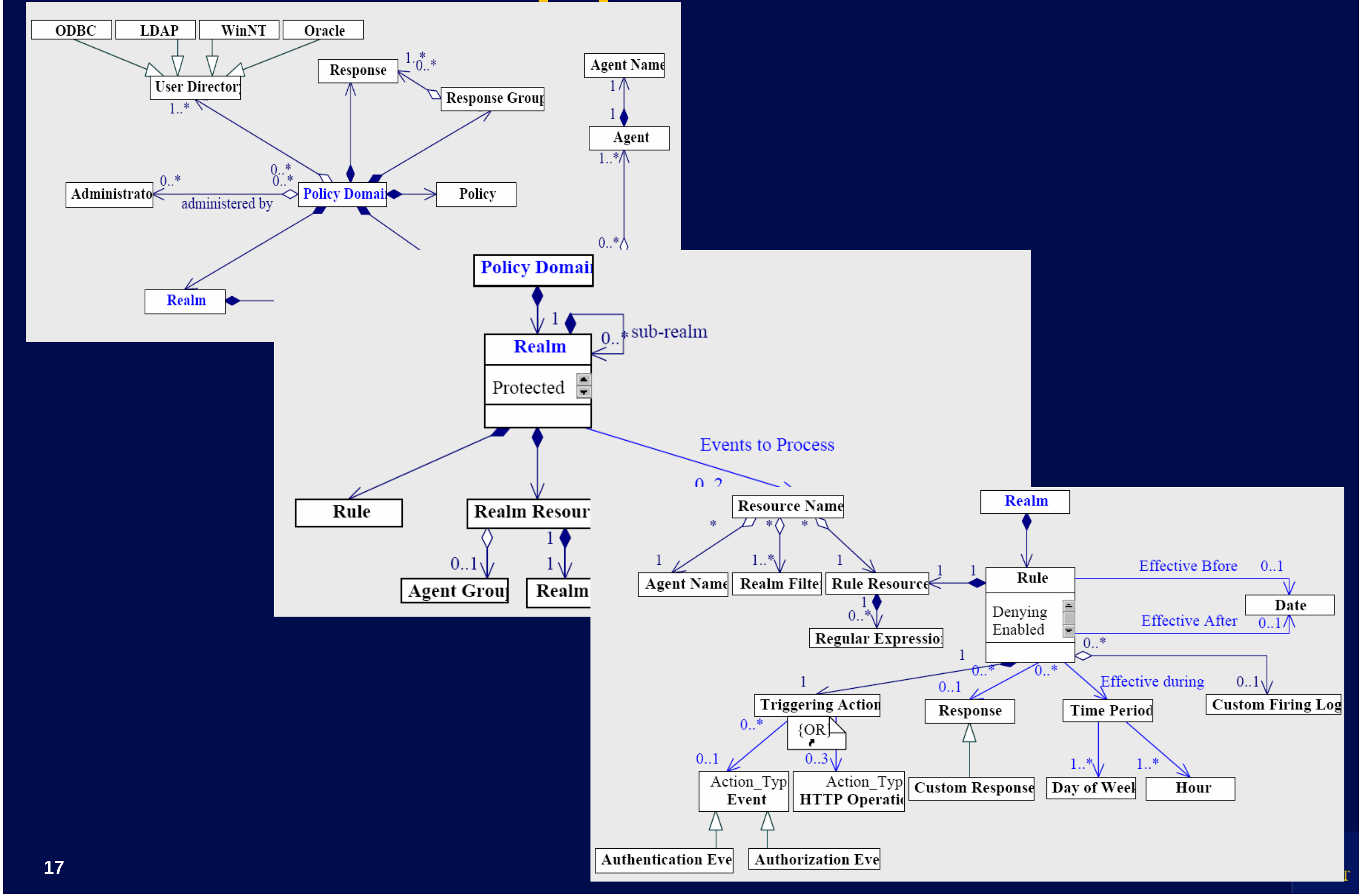


… complex



Resource Name
Realm
*
*
*
1
1..*
1
Agent Name
Realm Filte
Rule Resource
1
1
Rule
Effective Bfore
0..1
Date
Denying
Enabled
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 Operatic
Custom Response
Day of Weel
Hour
Authentication Eve
Authorization Eve

hard to map policies to models



so what?

- steep learning curve
- hard to fit real world into the model
- easy to make costly mistakes
  - “friendly” DoS
  - inadvertent hard to catch config. 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

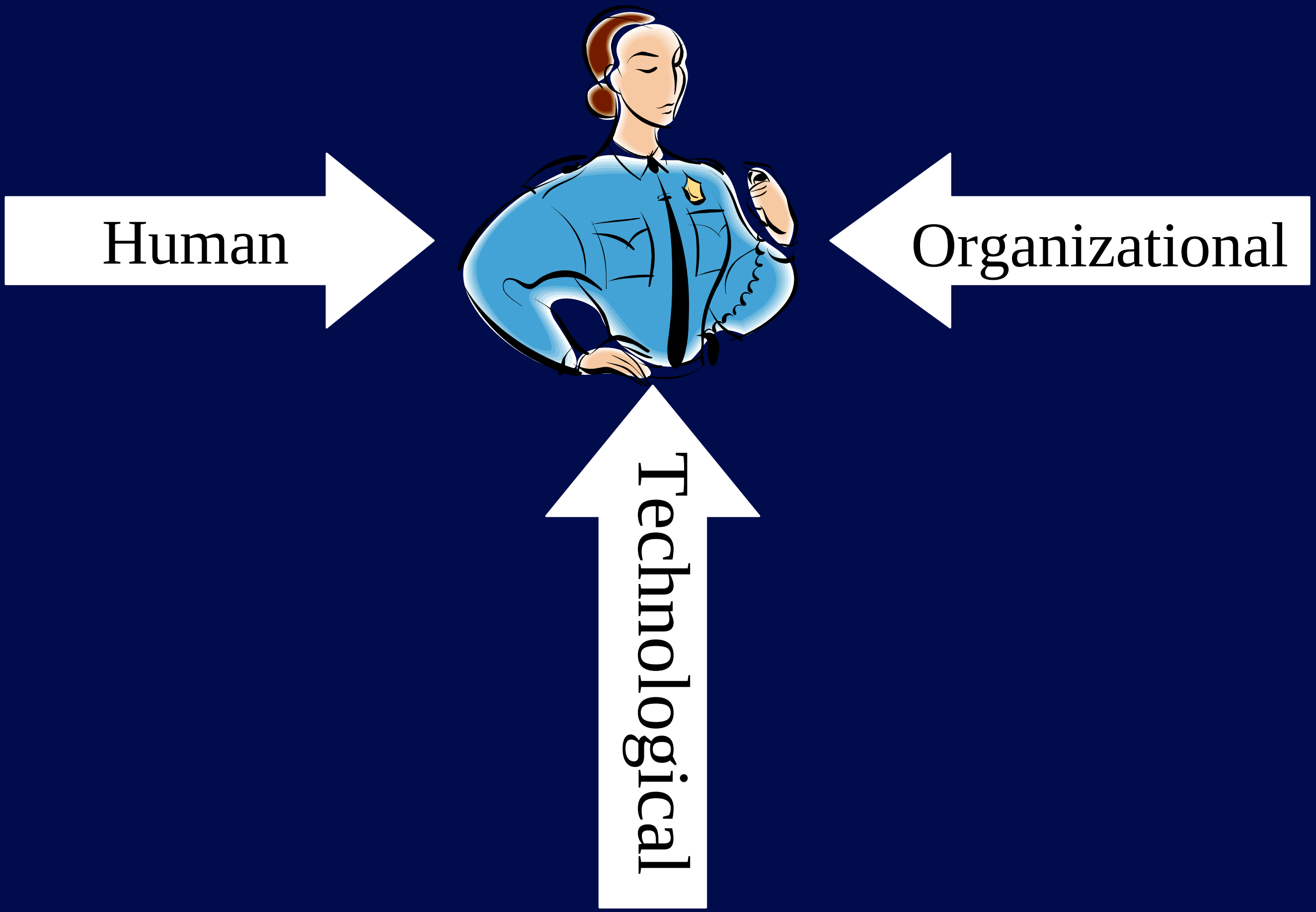
- revenues in security administration software:
  - $1B in 2003
  - $1.6B by 2007

Schroder, N. *Security Software Market Forecast, 2003-2007*, Gartner Group, 2003.

Who is Security Administrator?

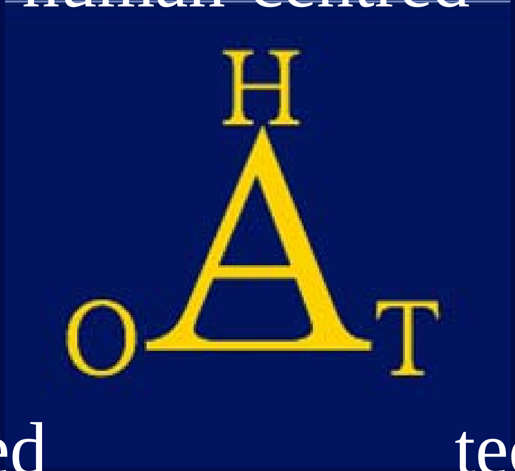
- Security administrators
  1. configure, maintain, test and install the technology used to enforce an organization’s security policy
  2. respond to and recover from malicious actions and attacks
  3. administer others’ systems or infrastructures
- end users, power users, administrators

administrators in the epicentres



approach

human-centred



organization-centred

technology-centred

HOT Admin project overview

- purpose
  1. evaluation methodology for sec. admin. effectiveness
  2. guidelines and techniques to design sec. admin. tools
- problem addressed
  - conflict of human, organizational, and technological forces
- approach
  - resolve the conflict through harmonizing the forces
- work plan (3 years)
  1. pilot studies to fine-tune the methodologies
  2. field research
  3. development of models
  4. design of techniques and methodologies
  5. validation and evaluation of the project’s key results.
- team
  - Beznosov (security), Fels (interfaces),
    Iverson (collaborations), Fisher (interaction)

purpose

1. methodology for evaluating the effectiveness of the existing IT security administrative tools

2. guidelines and techniques to systematically design effective technological solutions to aid security administrators

3. train graduate students

human-centred

better means for

1. visualizing the state of the security mechanisms
2. providing feedback to security admins
   - “what if” scenarios
   - safe staging playgrounds
   - tests of properties of the security state
3. support for cognitive models of system security

organization-centred

- patterns of communication between different parts of the organization and admins
- offload certain tasks from the admins

technology-centred

accommodate security technology to human and organizational needs

possible examples

- self-administration
- domain-specific access control models and languages
- flexible and reconfigurable policy engines

work plan

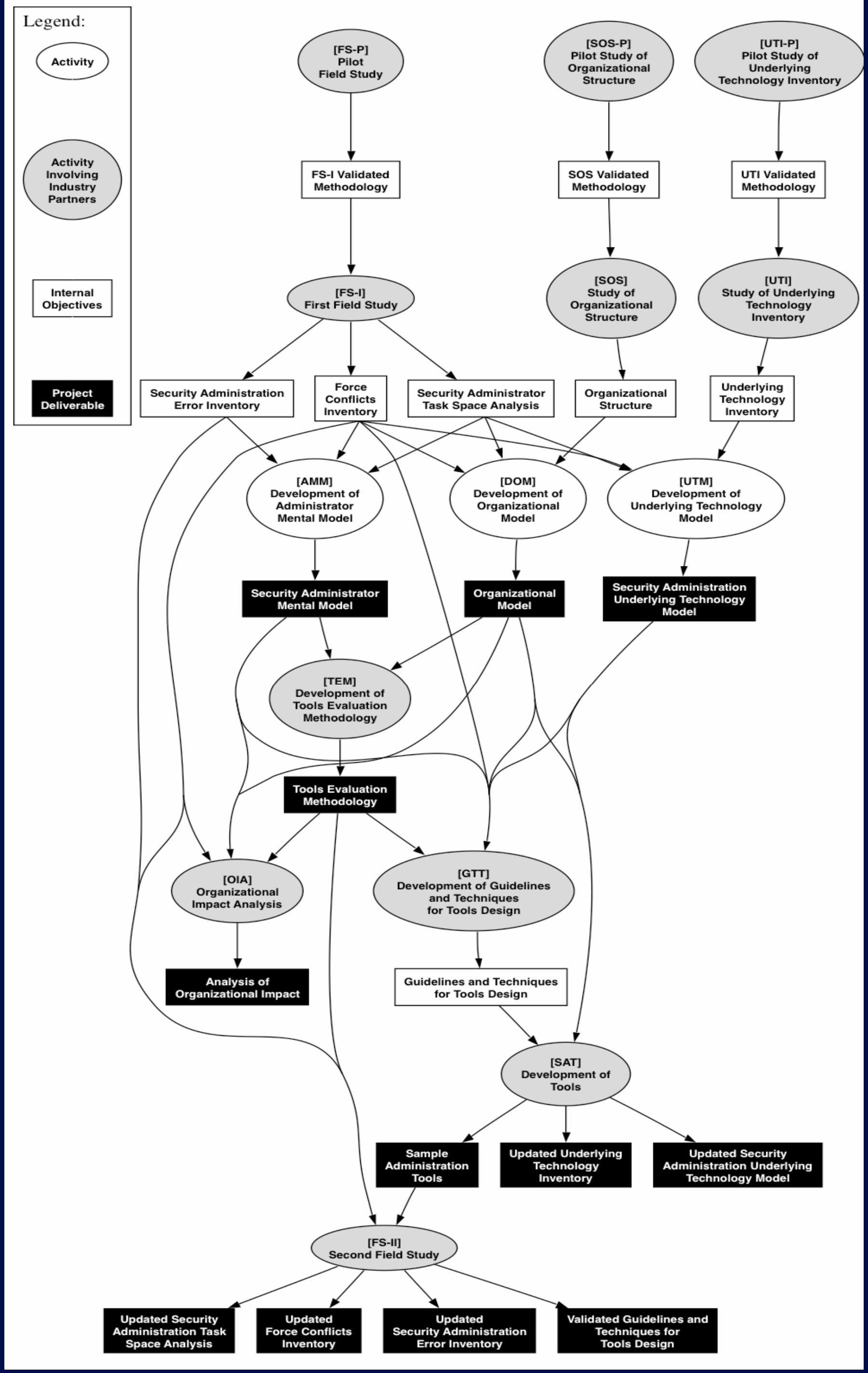
In 3 years

1. pilot studies to fine-tune study plans
2. inventories and an initial analysis through field studies with industry
3. development of models
   - human, organizational, technological
4. design of techniques and methodologies
5. validation and evaluation of the project’s key results
   - sample admin tools

First year

Second year

Third year



Legend:

Activity

Activity Involving Industry Partners

Internal Objectives

Project Deliverable

[FS-P] Pilot Field Study

[SOS-P] Pilot Study of Organizational Structure

[UTI-P] Pilot Study of Underlying Technology Inventory

FS-I Validated Methodology

SOS Validated Methodology

UTI Validated Methodology

[FS-I] First Field Study

[SOS] Study of Organizational Structure

[UTI] Study of Underlying Technology Inventory

Security Administration Error Inventory

Force Conflicts Inventory

Security Administrator Task Space Analysis

Organizational Structure

Underlying Technology Inventory

[AMM] Development of Administrator Mental Model

[DOM] Development of Organizational Model

[UTM] Development of Underlying Technology Model

Security Administrator Mental Model

Organizational Model

Security Administration Underlying Technology Model

[TEM] Development of Tools Evaluation Methodology

Tools Evaluation Methodology

[OIA] Organizational Impact Analysis

[GTT] Development of Guidelines and Techniques for Tools Design

Analysis of Organizational Impact

Guidelines and Techniques for Tools Design

[SAT] Development of Tools

Sample Administration Tools

Updated Underlying Technology Inventory

Updated Security Administration Underlying Technology Model

[FS-II] Second Field Study

Updated Security Administration Task Space Analysis

Updated Force Conflicts Inventory

Updated Security Administration Error Inventory

Validated Guidelines and Techniques for Tools Design

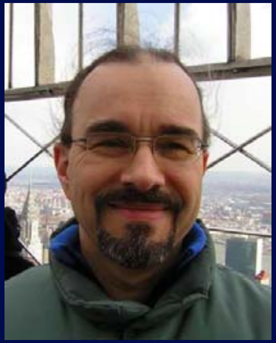
team

Dr. Konstantin Beznosov

- Principal investigator (PI)
- Assist. Prof., ECE, UBC
- security; 5 years of industry

Dr. Sidney Fels

- Assoc. Prof., ECE, UBC
- new interfaces design



Dr. Brian Fisher

- Assoc. Prof. of Inter. Arts and Techn., SFU
- Adjunct Prof. in MIS and CS, UBC
- cognitive science-based interaction design

Dr. Lee Iverson

- Assist. Prof., ECE, UBC
- Inform. visualiz., inform. systems
- collaboration infrastructures

Current Status

- Got funding
  - Natural Sciences and Engineering Research Council (NSERC) - $459K
- Got support
  - SAP
  - Entrust
- Getting students
- Getting participants
- Designing studies

project summary

- purpose: develop
  1. tool evaluation methodology
  2. tool design guidelines and techniques
- problem
  - conflict of human, organizational, and technological forces
- approach: resolve the conflict through harmonizing the forces
- work plan (3 years)
  1. pilot studies
  2. field research
  3. models
  4. techniques and methodologies
  5. validation and evaluation
- team
  - Beznosov (security), Fels (interfaces),
    Iverson (collaborations), Fisher (interaction)
  - + 5 graduate students

We Want You

participate

provide feedback

For HOT Admin!

hot-admin-info@ece.ubc.ca

if your organization participates

we’ll provide:

1. analysis of the organizational environment
2. inventory of the technologies
3. inventory of the conflicts of forces
4. common types of errors

- contact project members

if you want to provide feedback

- workshops with industry partners
- review results

- contact project members

Questions please

http://lersse.ece.ubc.ca/
tiki-index.php?page=Project_HOT-Admin