Current Research and Open Problems in Attribute-Based Access Control

Daniel Servos
dservos5@uwo.ca

Western
UNIVERSITY · CANADA
Department of Computer Science

Topics Survey/Proposal

1. Talk Outline

1. Outline
2. Background
    - Traditional Models
    - Attribute-Based Access Control
3. Literature Review
    - Methodology & Taxonomy
    - Hybrid Models
    - Open Problems
4. Research Proposal
    - Goals
    - Approach
    - Work to Date
5. Conclusions

2. Background

1. Outline
2. Background
    - Traditional Models
    - Attribute-Based Access Control
3. Literature Review
    - Methodology & Taxonomy
    - Hybrid Models
    - Open Problems
4. Research Proposal
    - Goals
    - Approach
    - Work to Date
5. Conclusions

Traditional Models

- Discretionary Access Control
- Mandatory Access Control
- Role-Based Access Control

Traditional Models

- Discretionary Access Control
- Mandatory Access Control
- Role-Based Access Control

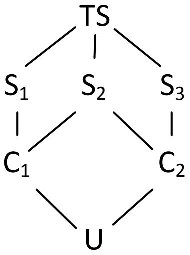
DAC

	O_1	O_2	..	O_n
S_1	$A[S_1, O_1]$	$A[S_1, O_2]$	..	$A[S_1, O_n]$
S_2	$A[S_2, O_1]$	$A[S_2, O_2]$	..	$A[S_2, O_n]$
..	..	..	..	..
S_n	$A[S_n, O_1]$	$A[S_n, O_2]$	..	$A[S_n, O_n]$

Traditional Models

- Discretionary Access Control
- Mandatory Access Control
- Role-Based Access Control

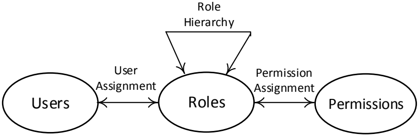
MAC



Traditional Models

- Discretionary Access Control
- Mandatory Access Control
- Role-Based Access Control

RBAC



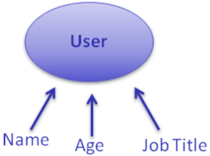
ABAC

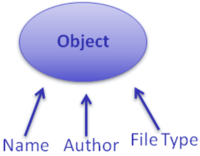
ABAC

User

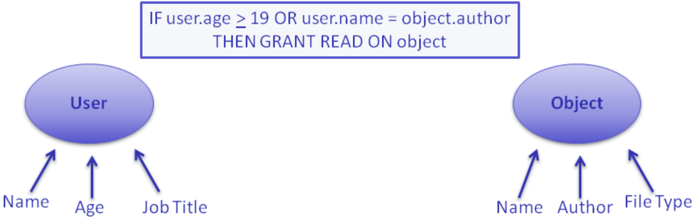
Object

ABAC



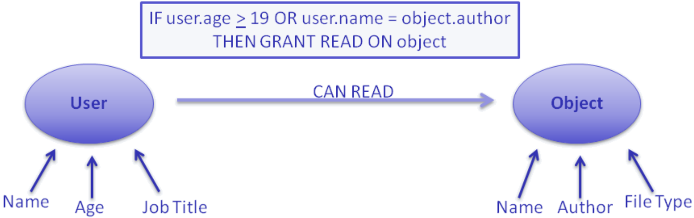


ABAC



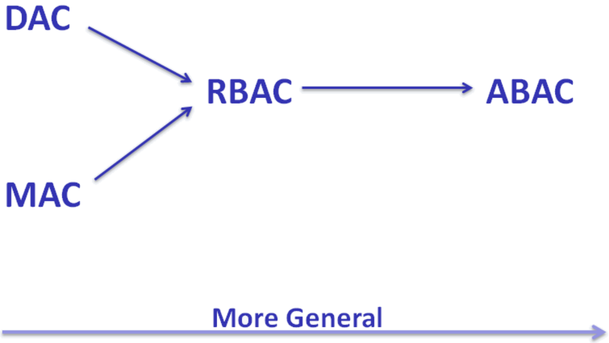
IF user.age ≥ 19 OR user.name = object.author
THEN GRANT READ ON object

ABAC

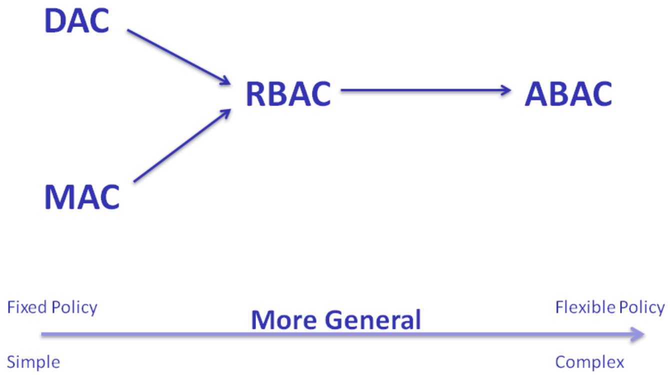


IF user.age ≥ 19 OR user.name = object.author
THEN GRANT READ ON object

ABAC



ABAC


DAC
MAC
RBAC
ABAC
Fixed Policy
Simple
More General
Flexible Policy
Complex

3. Literature Review

1. Outline
2. Background
   - Traditional Models
   - Attribute-Based Access Control
3. Literature Review
   - Methodology & Taxonomy
   - Hybrid Models
   - Open Problems
4. Research Proposal
   - Goals
   - Approach
   - Work to Date
5. Conclusions

Methodology

Inclusion Criteria:

- Refereed journal papers, conference papers and dissertations
- Found via using queries relating to ABAC on Google Scholar and DBLP

Exclusion Criteria:

- Non-refereed work
- Not in English
- Unavailable
- Date of publication
- Attribute-based encryption
- Near duplicates

Methodology

Inclusion Criteria:

- Refereed journal papers, conference papers and dissertations
- Found via using queries relating to ABAC on Google Scholar and DBLP

Exclusion Criteria:

- Non-refereed work
- Not in English
- Unavailable
- Date of publication
- Attribute-based encryption
- Near duplicates

Methodology

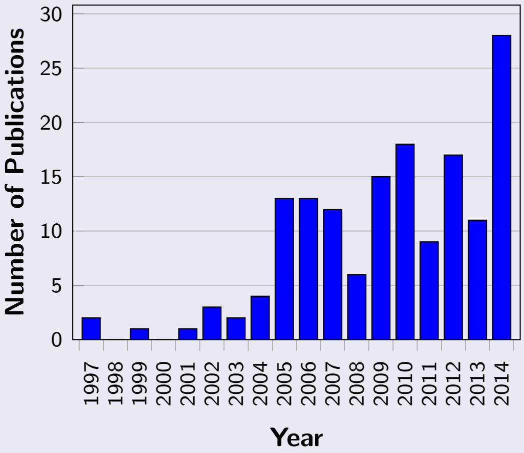
Inclusion Criteria:

- Refereed journal papers, conference papers and dissertations
- Found ar and DBLP

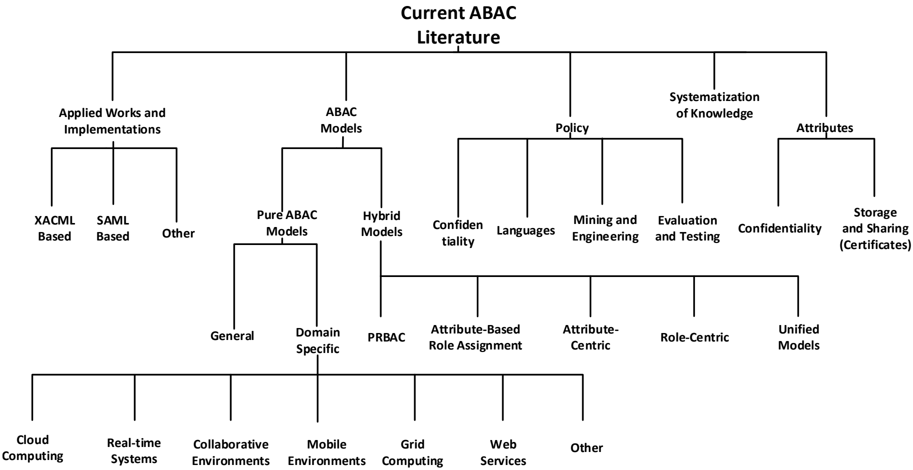
Exclusion C

- Non-re
- Not in
- Unavai
- Date o
- Attribu
- Near d

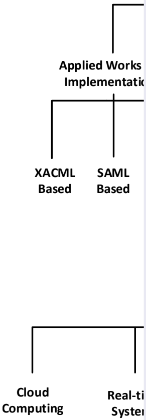
ABAC Publications per Year



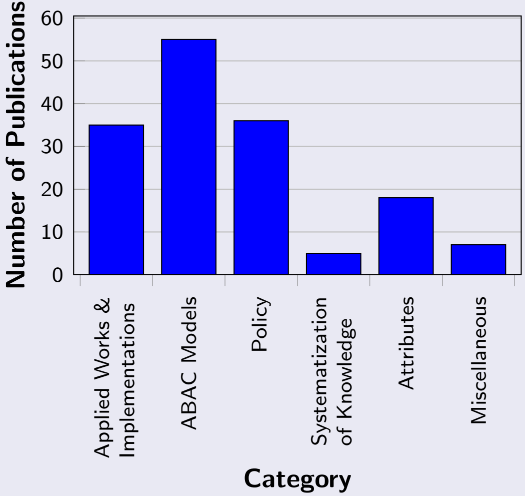
Taxonomy of Current Research

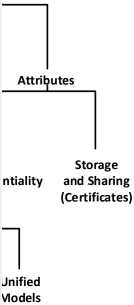


Taxonomy of Current Research

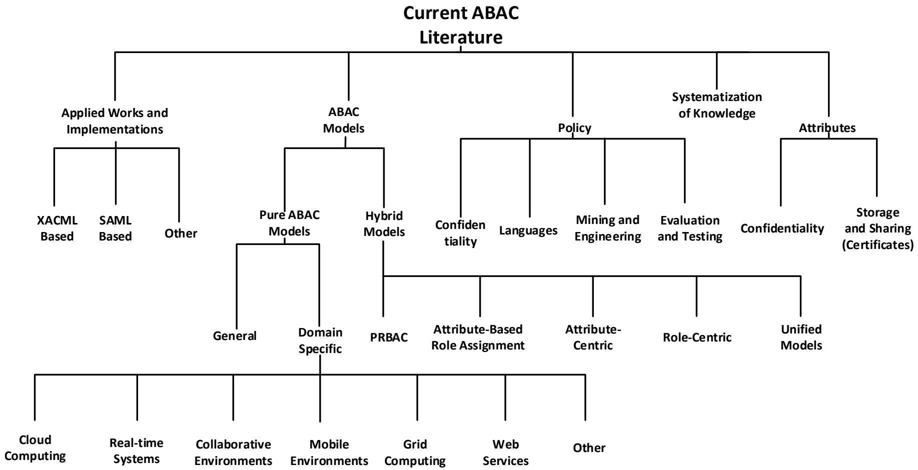


ABAC Publications per Category

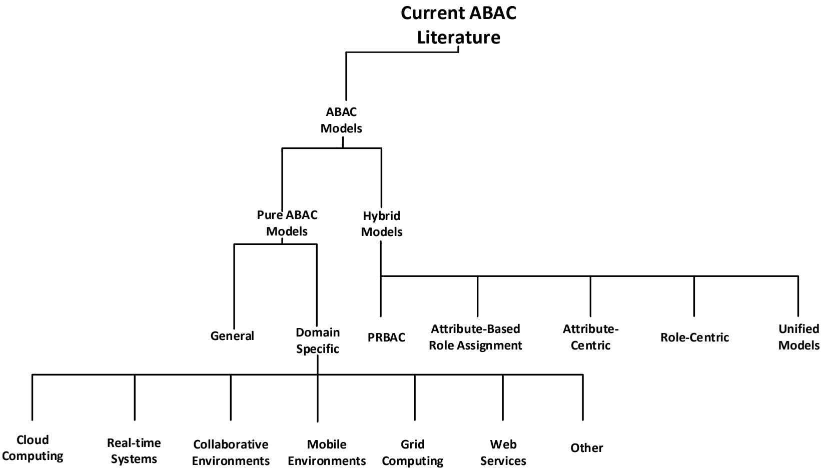




Taxonomy of Current Research

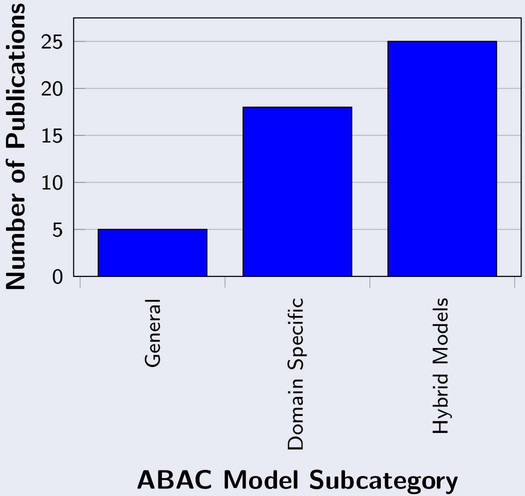


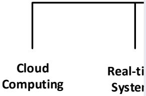
Taxonomy of Current Research



Taxonomy of Current Research

ABAC Model Publications per Subcategory





General Models

	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
A Logic-based Framework for ABAC	✗	✓	✗	✗	Attributes	✗	✗	✓	✗	✗
ABAC$_\alpha$	✓	✓	✗	✗	✗	✗	✗	✓	Limited	✓
ABAM	✓	✓	✗	✗	✗	✗	✗	✓	Very limited	✓
Supporting Secure Collaborations with ABAC	✓	✓	✓	✗	✗	✗	✗	Largely informal	✗	✓
HGABAC	✓	✓	✓	✓	Objects & groups	✗	✗	✓	✗	✓

General Models

	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
A Logic-based Framework for ABAC	✗	✓	✗	✗	Attributes	✗	✗	✓	✗	✗
ABAC$_\alpha$	✓	✓	✗	✗	✗	✗	✗	✓	Limited	✓
ABAM	✓	✓	✗	✗	✗	✗	✗	✓	Very limited	✓
Supporting Secure Collaborations with ABAC	✓	✓	✓	✗	✗	✗	✗	Largely informal	✗	✓
HGABAC	✓	✓	✓	✓	Objects & groups	✗	✗	✓	✗	✓

General Models

	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
A Logic-based Framework for ABAC	✗	✓	✗	✗	Attributes	✗	✗	✓	✗	✗
AB										
AB										
Sup Sec orat AB										
HG										

A Logic-based Framework for Attribute-based Access Control

L. Wang et al., 2004

- One of the first "pure" and "general" ABAC models
- Focused on the representation, consistency and performance of attribute-based policies
- Introduces hierarchical attributes
- Missing object attributes
- Only formalizes policies and their evaluation

General Models

	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
A Logic-based Framework for ABAC	✗	✓	✗	✗	Attributes	✗	✗	✓	✗	✗
ABAC$_\alpha$	✓	✓	✗	✗	✗	✗	✗	✓	Limited	✓
ABAM	✓	✓	✗	✗	✗	✗	✗	✓	Very limited	✓
Supporting Secure Collaborations with ABAC	✓	✓	✓	✗	✗	✗	✗	Largely informal	✗	✓
HGABAC	✓	✓	✓	✓	Objects & groups	✗	✗	✓	✗	✓

General Models

	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
A Logic-based Framework for AB	✗	✓	✗	✗	Attributes	✗	✗	✓	✗	✗
AB										
AB										
Sup Sec orat AB										
HG										

A unified attribute-based access control model covering DAC, MAC and RBAC

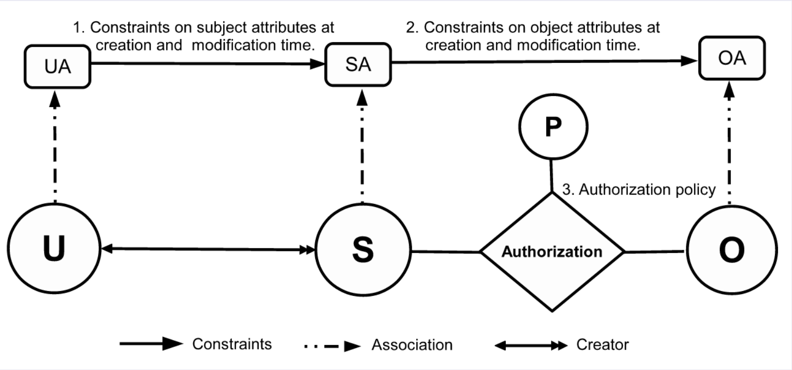
X. Jin et al., 2012

- Just sufficiently expressive to capture DAC, MAC and RBAC
- Formalizations of the basic ABAC elements
- Partial policy and constraint language (CPL)
- Lacks necessary components for real world
- CPL is limited.

General Models

	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
A Logic-based Framework for AB	✗	✓	✗	✗	Attributes	✗	✗	✓	✗	✗
AB										
AB										
Sup Sec orat AB										
HG										

A unified attribute-based access control model covering DAC, MAC and RBAC



1. Constraints on subject attributes at creation and modification time.
2. Constraints on object attributes at creation and modification time.
UA
SA
OA
P
3. Authorization policy
U
S
Authorization
O
Constraints
Association
Creator

General Models

	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
A Logic-based Framework for ABAC	✗	✓	✗	✗	Attributes	✗	✗	✓	✗	✗
AB										
AB										
Sup Sec orat AB										
HG										

A unified attribute-based access control model covering DAC, MAC and RBAC

X. Jin et al., 2012

- Just sufficiently expressive to capture DAC, MAC and RBAC
- Formalizations of the basic ABAC elements
- Partial policy and constraint language (CPL)
- Lacks necessary components for real world
- CPL is limited.

Domain Specific Models

	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
Cloud Computing										
CA-ABAC	✓	✓	✓	✗	✗	✗	✗	✗	✗	Mostly describes policy use
Real-time Systems										
T-ABAC	?	?	?	✗	✗	✗	✗	Real-time attr. and packets	✗	Only models real-time attr.and packets
Collaborative Environments										
ABAC for Collaboration Environments	✓	✓	✗	✗	✗	✗	✗	✓	✗	Lacks details
MPABAC	✓	✓	✓	✗	✗	✗	✗	✓	✗	Lacks details

Domain Specific Models

	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
Mobile Environments										
CABAC	✓	✓	✓	✗	✗	✗	✗	✗	✗	?
An Access Control Model for Mobile Physical Objects	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓
Grid computing										
ABMAC	✓	✓	✓	Shown in example but not model	✗	✗	✗	✓	✗	✓
Grid_ABAC	✓	✓	✓	✗	✗	✗	✗	✗	✗	Minimal model

Domain Specific Models

	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
Web Services										
ABAC for Web Services	✓	✓	✓	✗	✗	✗	✗	Simplistic	✗	✓
WS-ABAC	✓	✓	✓	✗	✗	✗	✗	Simplistic	✗	✓
ABAC-based cross-domain access control in SOA	✓	✓	✓	✗	✗	✗	✗	Simplistic	✗	More implementation then model
Study on Action and ABAC Model for Web Services	✓	✓	✓	✗	✗	✗	✗	✓	✗	✓
SABAC	✗	✓	✗	✗	✗	✗	✗	✗	✗	Architecture combining existing works
ABAC Security Model in Service-Oriented Computing	✓	✓	✓	✗	✗	✗	✗	✗	✗	Architecture combining existing works

Domain Specific Models

	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
Web Services										
ABAC for Web Services	✓	✓	✓	✗	✗	✗	✗	Simplistic	✗	✓
WS-ABAC	✓	✓	✓	✗	✗	✗	✗	Simplistic	✗	✓
ABAC-based cross-domain access control in SOA	✓	✓	✓	✗	✗	✗	✗	Simplistic	✗	More implementation then model
Study on Action and ABAC Model for Web Services	✓	✓	✓	✗	✗	✗	✗	✓	✗	✓
SABAC	✗	✓	✗	✗	✗	✗	✗	✗	✗	Architecture combining existing works
ABAC Security Model in Service-Oriented Computing	✓	✓	✓	✗	✗	✗	✗	✗	✗	Architecture combining existing works

Domain Specific Models

	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
Web Services										
ABAC for Web Services	✓	✓	✓	✗	✗	✗	✗	Simplistic	✗	✓
WS-										
ABA cross acce in S(										n-
Stud tion Mod Serv										
SABAC	✗	✓	✗	✗	✗	✗	✗	✗	✗	ture combining existing works
ABAC Security Model in Service-Oriented Computing	✓	✓	✓	✗	✗	✗	✗	✗	✗	Architecture combining existing works

Attributed based access control (ABAC) for web services

E. Yuan and J. Tong, 2005

- Basis for a number of other models
- Describe ABAC in terms authorization architecture and policy engineering
- Limited model

Domain Specific Models

	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
Web Services										
ABAC for Web Services	✓	✓	✓	✗	✗	✗	✗	Simplistic	✗	✓
WS-ABAC	✓	✓	✓	✗	✗	✗	✗	Simplistic	✗	✓
ABAC based cross acce in S										More en-
Stud tion Mod Serv										
SAB										ture ng g
ABAC Security Model in Service-Oriented Computing	✓	✓	✓	✗	✗	✗	✗	✗	✗	Architecture combining existing works

Attributed based access control (ABAC) for web services

$$ATTR(s) \subseteq SA_1 \times SA_2 \times .. \times SA_k$$
$$ATTR(r) \subseteq RA_1 \times RA_2 \times .. \times RA_k$$
$$ATTR(e) \subseteq EA_1 \times EA_2 \times .. \times EA_k$$

Rule: $can\_access(s, r, e) \leftarrow f(ATTR(s), ATTR(r), ATTR(e))$

Hybrid Models

Combination Strategies (D. Kuhn et al., 2010)

	U	R	A	Model	Permission Mapping
0	0	0	0	undefined	—
1	0	0	1	ABAC-basic	A_1 , ... , A_n → perm
2	0	1	0	undefined	—
3	0	1	1	ABAC-RBAC hybrid	R,A_1, ... , A_n → perm
4	1	0	0	ACL	U → perm
5	1	0	1	ABAC-ID	U,A_1, ... , A_n → perm
6	1	1	0	RBAC-basic	U → R → perm
7	1	1	1	RBAC-A, dynamic roles	U,A_1, ... , A_n → R → perm
8	1	1	1	RBAC-A, attribute-centric	U,R,A_1, ... , A_n → perm
9	1	1	1	RBAC-A, role-centric	U → R → A_1, ... , A_n → perm

Hybrid Models

Combination Strategies (D. Kuhn et al., 2010)

	U	R	A	Model	Permission Mapping
0	0	0	0	undefined	—
1	0	0	1	ABAC-basic	A_1 , ... , A_n → perm
2	0	1	0	undefined	—
3	0	1	1	ABAC-RBAC hybrid	R,A_1, ... , A_n → perm
4	1	0	0	ACL	U → perm
5	1	0	1	ABAC-ID	U,A_1, ... , A_n → perm
6	1	1	0	RBAC-basic	U → R → perm
7	1	1	1	RBAC-A, dynamic roles	U,A_1, ... , A_n → R → perm
8	1	1	1	RBAC-A, attribute-centric	U,R,A_1, ... , A_n → perm
9	1	1	1	RBAC-A, role-centric	U → R → A_1, ... , A_n → perm

Hybrid Models

Combination Strategies (D. Kuhn et al., 2010)

	U	R	A	Model	Permission Mapping
0	0	0	0	undefined	—
1	0	0	1	ABAC-basic	A_1 , ... , $A_n \rightarrow$ perm
2	0	1	0	undefined	—
3	0	1	1	ABAC-RBAC hybrid	R,A_1, ... , $A_n \rightarrow$ perm
4	1	0	0	ACL	$U \rightarrow$ perm
5	1	0	1	ABAC-ID	U,A_1, ... , $A_n \rightarrow$ perm
6	1	1	0	RBAC-basic	$U \rightarrow$ R $\rightarrow$ perm
7	1	1	1	RBAC-A, dynamic roles	U,A_1, ... , $A_n \rightarrow$ R $\rightarrow$ perm
8	1	1	1	RBAC-A, attribute-centric	U,R,A_1, ... , $A_n \rightarrow$ perm
9	1	1	1	RBAC-A, role-centric	$U \rightarrow R \rightarrow A_1$, ... , $A_n \rightarrow$ perm

Hybrid Models

Combination Strategies (D. Kuhn et al., 2010)

	U	**R**	**A**	**Model**	**Permission Mapping**
0	0	0	0	undefined	—
1	0	0	1	ABAC-basic	A_1 , ... , $A_n \rightarrow$ perm
2	0	1	0	undefined	—
3	0	1	1	ABAC-RBAC hybrid	R,A_1, ... , $A_n \rightarrow$ perm
4	1	0	0	ACL	$U \rightarrow$ perm
5	1	0	1	ABAC-ID	U,A_1, ... , $A_n \rightarrow$ perm
6	1	1	0	RBAC-basic	$U \rightarrow$ R $\rightarrow$ perm
7	1	1	1	RBAC-A, dynamic roles	U,A_1, ... , $A_n \rightarrow$ R $\rightarrow$ perm
8	1	1	1	RBAC-A, attribute-centric	U,R,A_1, ... , $A_n \rightarrow$ perm
9	1	1	1	RBAC-A, role-centric	$U \rightarrow R \rightarrow A_1$, ... , $A_n \rightarrow$ perm

Hybrid Models

- Dynamic Roles
- Attribute-Centric
- Role-Centric

Hybrid Models

- Dynamic Roles
- Attribute-Centric
- Role-Centric
- Parameterized Role-Based Access Control

Hybrid Models

- Dynamic Roles
- Attribute-Centric
- Role-Centric
- Parameterized Role-Based Access Control
- Unified Models of Access Control

Parameterized Role-Based Access Control

	Extends	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
A Design for Parametrized Roles	Role Graph Model	✓	✓	✗	✗	Roles	From extended model	✗	✓	From extended model	✓
Role Templates	RBAC	✓	✗	Time	✗	✗	✗	✗	✓	✗	Only vaguely defined
PFRBAC	FRBAC	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓
Reconciling RBM & RBAC	RBAC & RBM	✓	✗	Time	✗	Role	✗	✗	✗	✗	Lacks details
ORBAC	RBAC	✗	✓	✗	✗	✗	✗	✗	✓	✗	✓

Parameterized Role-Based Access Control

	Extends	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
A Design for Parametrized Roles	Role Graph Model	✓	✓	✗	✗	Roles	From extended model	✗	✓	From extended model	✓
Role Templates	RBAC	✓	✗	Time	✗	✗	✗	✗	✓	✗	Only vaguely defined
PFRBAC	FRBAC	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓
Reconciling RBM & RBAC	RBAC & RBM	✓	✗	Time	✗	Role	✗	✗	✗	✗	Lacks details
ORBAC	RBAC	✗	✓	✗	✗	✗	✗	✗	✓	✗	✓

Parameterized Role-Based Access Control

Role Templates for Content-Based Access Control

Luigi Giuri and Pietro Iglio, 1997

- Extends RBAC
- Permissions are extended with logical expressions (privilege restriction)
- Examples:
  1. *(delete, PatientRecord, PatientRecord.State = 'discharged')*
  2. *(delete, PatientRecord, today() in [Mon..Fri])*
- Role are extended with templates to compose parameterized privileges

		plete del
A De Param Roles		✓
Role T		ly uely ned
PFRB		✓
Recon RBM &		cks ails
ORBAC	✗ ✓ ✗ ✗ ✗ ✗ ✗ ✓ ✗	✓

Parameterized Role-Based Access Control

Role Templates for Content-Based Access Control

The example role template:

$$
\begin{aligned}
&R{<}prj,\ sal{>} = role(\\
&\qquad (select,\ Employee,\ Employee.project = prj), \\
&\qquad (update,\ Employee,\ Employee.project = prj \ \hat{}\ Employee.salary < sal))
\end{aligned}
$$

would produce the following template instance given the values prj = "PRJ1" and sal = 1000:

$$
\begin{aligned}
&R,{<}\text{“PRJ1”},\ 1000{>} = role(\\
&\qquad (select,\ Employee,\ Employee.project = \text{“PRJ1”}), \\
&\qquad (update,\ Employee,\ Employee.project = \text{“PRJ1”} \ \hat{}\ Employee.salary < 1000))
\end{aligned}
$$

ORBAC	RBAC	✗	✓	✗	✗	✗	✗	✗	✓	✗	✓

Attribute-Based Role Assignment

	Extends	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
RB-RBAC	RBAC	✗	✓	✗	✗	Roles	✗	✗	✓	✗	✓
Access Control Management in a Distributed Environment	GTRBAC	✗	✓	Time	✗	Roles	From extended model	✗	✓	✗	✓
A Role and ABAC System Using Semantic Web Technologies	RBAC	✗	✓	✗	✗	✗	✓	✗	Only RBAC modelling	✗	✗
GARBAC	RBAC	✓	✓	✗	✗	Roles	✗	✗	✓	✗	✓
ARBAC	RBAC	✓	✓	✗	✗	Roles	✓	✗	✓	✗	Limited details
Semantics-based Access Control Approach for Web Service	RBAC	✗	✓	✗	✗	Roles	✓	✗	✓	✗	✓

Attribute-Based Role Assignment

	Extends	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
RB-RBAC	RBAC	✗	✓	✗	✗	Roles	✗	✗	✓	✗	✓
Access Control Management in a Distributed Environment	GTRBAC	✗	✓	Time	✗	Roles	From extended model	✗	✓	✗	✓
A Role and ABAC System Using Semantic Web Technologies	RBAC	✗	✓	✗	✗	✗	✓	✗	Only RBAC modelling	✗	✗
GARBAC	RBAC	✓	✓	✗	✗	Roles	✗	✗	✓	✗	✓
ARBAC	RBAC	✓	✓	✗	✗	Roles	✓	✗	✓	✗	Limited details
Semantics-based Access Control Approach for Web Service	RBAC	✗	✓	✗	✗	Roles	✓	✗	✓	✗	✓

Attribute-Based Role Assignment

	Extends	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
RB-RBAC	RBAC	✗	✓	✗	✗	Roles	✗	✗	✓	✗	✓
Access Manag in a Di Enviror											✓
A Rol ABAC tem U Seman Techno											✗
GARBAC	RBAC	✓	✓	✗	✗	Roles	✗	✗	✓	✗	✓
ARBAC	RBAC	✓	✓	✗	✗	Roles	✓	✗	✓	✗	Limited details
Semantics-based Access Control Approach for Web Service	RBAC	✗	✓	✗	✗	Roles	✓	✗	✓	✗	✓

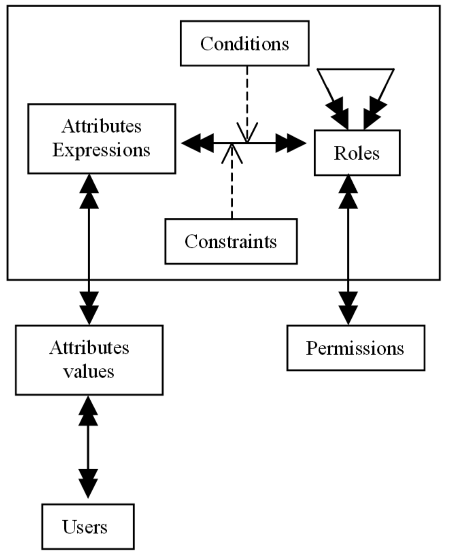
A model for attribute-based user-role assignment

M. Al-Kahtani and R. Sandhu, 2002

- Automates role assignment using user attributes
- Model demonstrated through real life use cases
- Lacks object attributes

Attribute-Base

A model for attribute-based user-role assignment



	Extends	Ob At	Formal Model	Admin Model	Complete Model
RB-RBAC	RBAC	✗	✓	✗	✓
Access Control Management in a Distributed Environment	GTRBAC	✗	✓	✗	✓
A Role and ABAC System Using Semantic Web Technologies	RBAC	✗	Only RBAC odelling	✗	✗
GARBAC	RBAC	✓	✓	✗	✓
ARBAC	RBAC	✓	✓	✗	Limited details
Semantics-based Access Control Approach for Web Service	RBAC	✗	✓	✗	✓

Attribute-Centric & Role-Centric

	Extends	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
Attribute-Centric											
A Framework Integrating Attribute-based Policies into RBAC	RBAC & ABAC	✓	✓	✓	✗	✗	✗	✗	✓ (other than policy)	✗	✓
Role-Centric											
RABAC	NIST RBAC & ABAC$_\alpha$	✓	✓	✗	✗	Roles from NIST RBAC	From NIST RBAC	✗	✓	From NIST RBAC	✓

Attribute-Centric & Role-Centric

	Extends	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
Attribute-Centric											
A Framework Integrating Attribute-based Policies into RBAC	RBAC & ABAC	✓	✓	✓	✗	✗	✗	✗	✓ (other than policy)	✗	✓
Role-Centric											
RABAC	NIST RBAC & ABAC$_\alpha$	✓	✓	✗	✗	Roles from NIST RBAC	From NIST RBAC	✗	✓	From NIST RBAC	✓

Attribute-Centric & Role-Centric

	Extends	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
Attribute-Centric											
A Framework Integrating Attribute-based Policies into RBAC	RBAC & ABAC	✓	✓	✓	✗	✗	✗	✗	✓ (other than policy)	✗	✓
Role-Centric											
RABAC	NIST RBAC & ABAC$_\alpha$	✓	✓	✗	✗	Roles from NIST RBAC	From NIST RBAC	✗	✓	From NIST RBAC	✓

Attribute-Centric & Role-Centric

RABAC: Role-centric attribute-based access control

X. Jin et. al., 2012

- Based on NIST RBAC model
- First attempt at a formal role-centric model
- Reduces permission set available to a subject based on value of attributes
- Permission filtering policies reduce the maximum permission set
- Advantage over PRBAC unclear

e

Attr

A
Inte
Attr
base
into

Role-

RABAC	NIST RBAC & ABAC$_\alpha$	✓	✓	✗	✗	Roles from NIST RBAC	From NIST RBAC	✗	✓	From NIST RBAC	✓

Unified Models of Access Control

	Extends	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
A United Access Control Model for Systems in Collaborative Commerce	RBAC, TBAC, & ABAC	✓	✓	✗	✗	Roles	✓	✗	✓	✗	✓
BABAC	ABAC & BBAC	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓
UURAC$_A$	UURAC & ABAC	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓

Unified Models of Access Control

	Extends	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
A United Access Control Model for Systems in Collaborative Commerce	RBAC, TBAC, & ABAC	✓	✓	✗	✗	Roles	✓	✗	✓	✗	✓
BABAC	ABAC & BBAC	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓
UURAC$_A$	UURAC & ABAC	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓

Unified Models of Access Control

	Extends	Object Attr.	User Attr.	Env. Attr.	Conn. Attr.	Hierarchical	SoD	Delegation	Formal Model	Admin Model	Complete Model
A United Access Control Model for Systems in Collaborative Commerce	RBAC, TBAC, & ABAC	✓	✓	✗	✗	Roles	✓	✗	✓	✗	✓
BABAC	ABAC & BBAC	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓
UURAC$_A$	UURAC & ABAC	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓

Open Problems

- Foundational Models
- Emulating and Representing Traditional Models
- Hierarchical ABAC
- Auditability
- Separation of Duties
- Delegation
- Scalability

Open Problems

- Foundational Models
- Emulating and Representing Traditional Models
- Hierarchical ABAC
- Auditability
- Separation of Duties
- Delegation
- Scalability

Open Problems

- Foundational Models
- Emulating and Representing Traditional Models
- Hierarchical ABAC
- Auditability
- Separation of Duties
- Delegation
- Scalability

Open Problems

- Foundational Models
- Emulating and Representing Traditional Models
- Hierarchical ABAC
- Auditability
- Separation of Duties
- Delegation
- Scalability

Open Problems

- Foundational Models
- Emulating and Representing Traditional Models
- Hierarchical ABAC
- Auditability
- Separation of Duties
- Delegation
- Scalability

Open Problems

- Foundational Models
- Emulating and Representing Traditional Models
- Hierarchical ABAC
- Auditability
- Separation of Duties
- Delegation
- Scalability

Open Problems

- Foundational Models
- Emulating and Representing Traditional Models
- Hierarchical ABAC
- Auditability
- Separation of Duties
- Delegation
- Scalability

4. Research Proposal

1. Outline
2. Background
   - Traditional Models
   - Attribute-Based Access Control
3. Literature Review
   - Methodology & Taxonomy
   - Hybrid Models
   - Open Problems
4. Research Proposal
   - Goals
   - Approach
   - Work to Date
5. Conclusions

Goals

- Hierarchical ABAC
- Representing the Traditional Models
- Delegation Model
- Separation of Duties
- Administration Model

First Steps:

- Formal Model (HGABAC)
- Attribute-Based Policy Language
- Reference Implementation

Approach

Evaluation Methods:

- Use Cases
- Implementation
- Complexity
- Formal Methods

Approach

Evaluation Methods:

- Use Cases
- Implementation
- Complexity
- Formal Methods

Approach

Evaluation Methods:

- Use Cases
- Implementation
- Complexity
- Formal Methods

Approach

Evaluation Methods:

- Use Cases
- Implementation
- Complexity
- Formal Methods

Approach

Evaluation Methods:

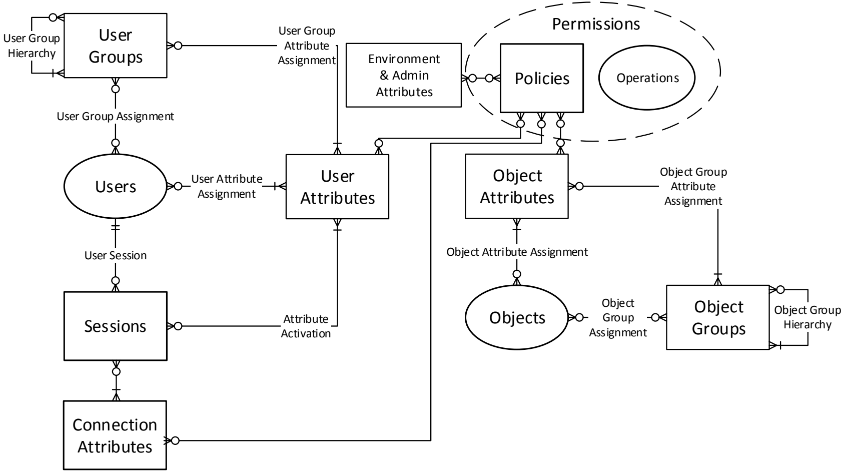
- Use Cases
- Implementation
- Complexity
- Formal Methods

Work to Date: HGABAC

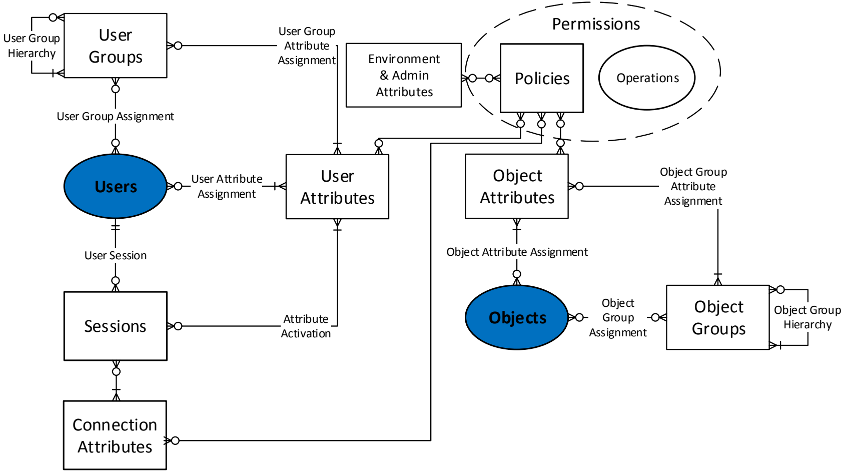
Current Progress:

- HGABAC Model
- Adds hierarchical constructs to ABAC
- Simplifies administration
- Emulation of traditional models
- Formal model on which future research can be built
- Presented at FPS'2014, forthcoming publication

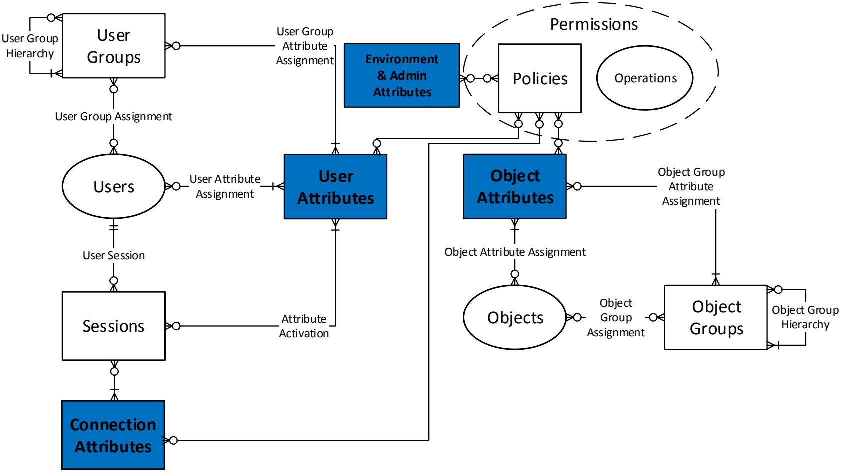
HGABAC: Model



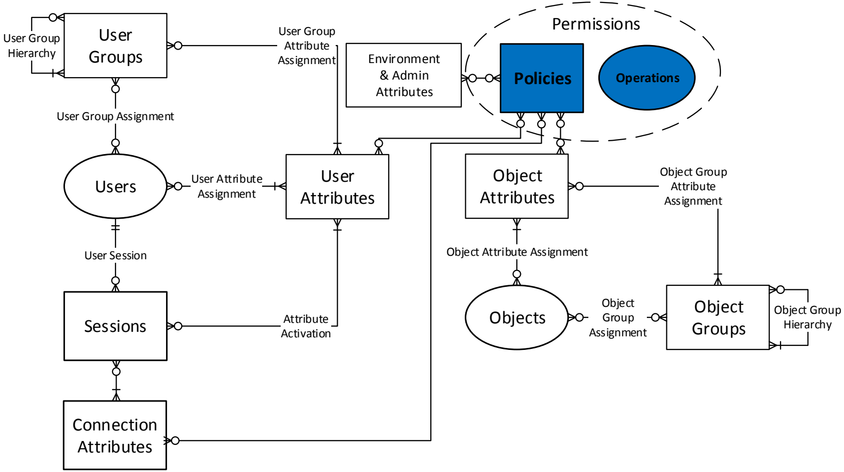
HGABAC: Model



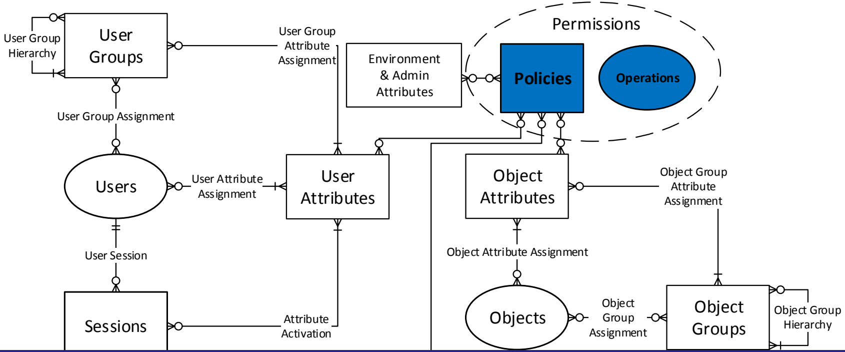
HGABAC: Model



HGABAC: Model



HGABAC: Model

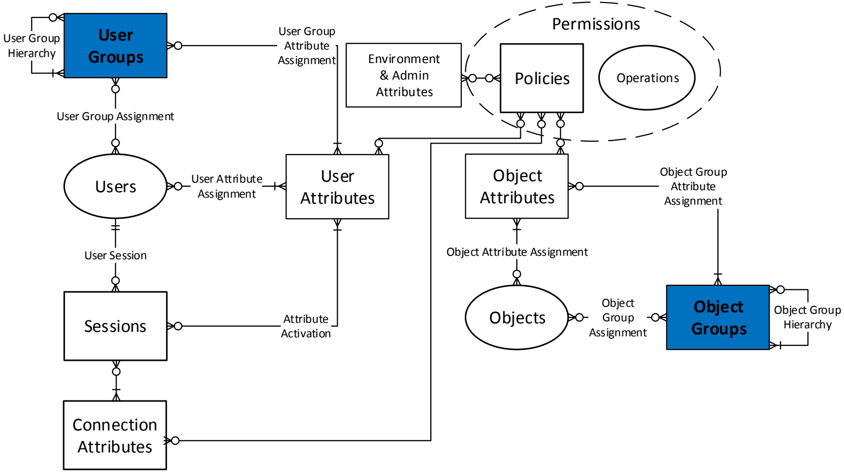


Permissions

user.id = *object.patient OR user.role* = *"doctor"* → **read**

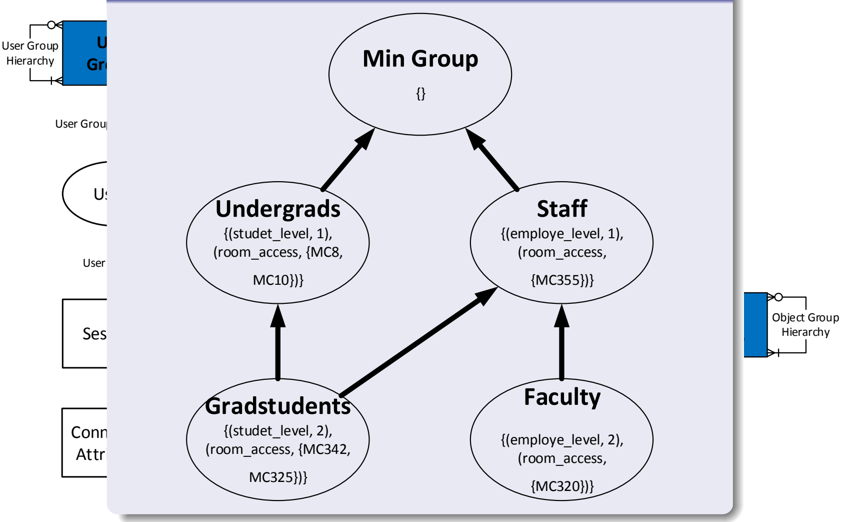
user.role = *"doctor"* → **write**

HGABAC: Model



HGABAC: Model

Group Graph


User Group Hierarchy
U
Gr
User Grou
U
User
Ses
Conn
Attr
Object Group Hierarchy
Min Group
{}
Undergrads
{(studet_level, 1), (room_access, {MC8, MC10})}
Staff
{(employe_level, 1), (room_access, {MC355})}
Gradstudents
{(studet_level, 2), (room_access, {MC342, MC325})}
Faculty
{(employe_level, 2), (room_access, {MC320})}

MAC Style Configuration

- For MAC with liberal *-property, each user is assigned only to a single read group and a single write group. Each read group is assigned a single attribute named "read" with a value equal to its clearance level and each write group is assigned a single attribute named "write" with a value equal to its clearance level.
- Policy is simply: *(object.level IN user.read)*→ **read**
  (object.level IN user.write) → **write**
- Users are limited to only activating attributes inherited from groups of a single security level in any given session.

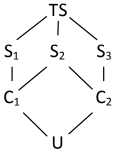
Emulating Traditional Models

MAC Style Configuration

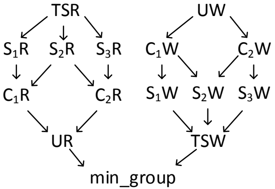
- For MAC with liberal *-property, each user is assigned only to a single read group and a single write group. Each read group is assigned a single attribute named "read" with a value equal to its clearance level and each write group is assigned a single attribute named "write" with a value equal to its clearance level.
- Policy is simply: *(object.level IN user.read)*→ **read**
  (object.level IN user.write) → **write**
- Users are limited to only activating attributes inherited from groups of a single security level in any given session.

Emulating Traditional Models
MAC Example

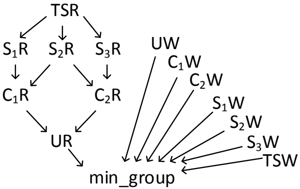
Security Lattice



Liberal-* Group Graph



Strict-* Group Graph



Liberal *-property Attributes:

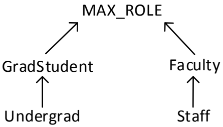
g	**direct(g)**	**effective(g)**
min_group	∅	∅
UR	"UR"	"UR"
C_1R	"C1R"	"UR", "C1R"
C_2R	"C2R"	"UR", "C2R"
S_1R	"S1R"	"UR", "C1R", "S1R"
S_2R	"S2R"	"UR", "C1R", "C2R", "S2R"
S_3R	"S3R"	"UR", "C2R", "S3R"
TSR	"TSR"	"UR", "C1R", "C2R", "S1R", "S2R", "S3R", "TSR"
TSW	"TSW"	"TSW"
S_1W	"S1W"	"TSW", "S1W"
S_2W	"S2W"	"TSW", "S2W"
S_3W	"S2W"	"TSW", "S3W"
C_1W	"C1W"	"TSW", "S1W", "S2W", "C1W"
C_2W	"C2W"	"TSW", "S2W", "S3W", "C2W"
UW	"UW"	"TSW", "S1W", "S2W", "S3W", "C1W", "C2W", "UW"

RBAC Style Configuration

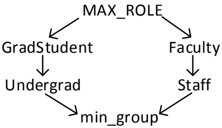
- Each group is assigned a single attribute named “perms” that contains the set of permissions that group grants.
- Objects are tagged with an attribute for each access mode that contains the set of permissions that grant that access mode on the object.
- Policy is simply: *(user.perms IN object.read)* → **read**
  (user.perms IN object.write) → **write**
- Emulating the separation of duty style constraints possible in NIST RBAC is left to future work.

Emulating Traditional Models
RBAC Example

Role Hierarchy



Group Graph



Role	Direct Permissions
Undergrad	P_1
Staff	P_2
GradStudent	P_3, P_4
Faculty	P_5, P_6
MAX_ROLE	$\emptyset$

g	direct(g)	effective(g)
min_group	$\emptyset$	$\emptyset$
Undergrad	P_1	P_1
Staff	P_2	P_2
GradStudent	P_3, P_4	P_1, P_3, P_4
Faculty	P_5, P_6	P_2, P_5, P_6
MAX_ROLE	$\emptyset$	P_1, P_2, P_3, P_4, P_5, P_6

5. Conclusions

1. Outline
2. Background
   - Traditional Models
   - Attribute-Based Access Control
3. Literature Review
   - Methodology & Taxonomy
   - Hybrid Models
   - Open Problems
4. Research Proposal
   - Goals
   - Approach
   - Work to Date
5. Conclusions

Conclusions

Literature Review:

- Taxonomy of ABAC research
- Comprehensive summaries of current work
- Identification of open problems
- Starting points for new research efforts

Proposal:

- Address yet to be resolved open problems
- Devised approach to tackle problems and evaluate solutions
- Summary of my work to date (HGABAC)

Conclusions

Literature Review:

- Taxonomy of ABAC research
- Comprehensive summaries of current work
- Identification of open problems
- Starting points for new research efforts

Proposal:

- Address yet to be resolved open problems
- Devised approach to tackle problems and evaluate solutions
- Summary of my work to date (HGABAC)