ReBAC in ABAC

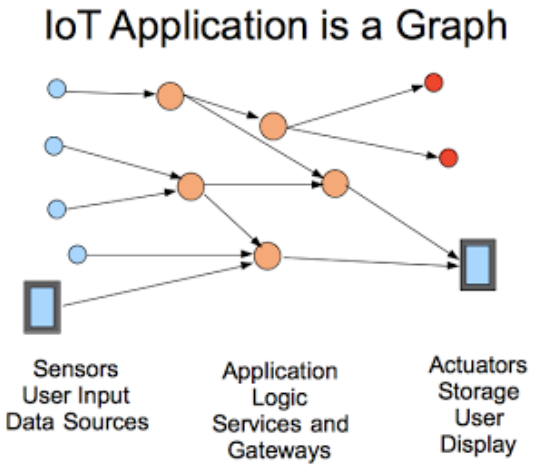
by

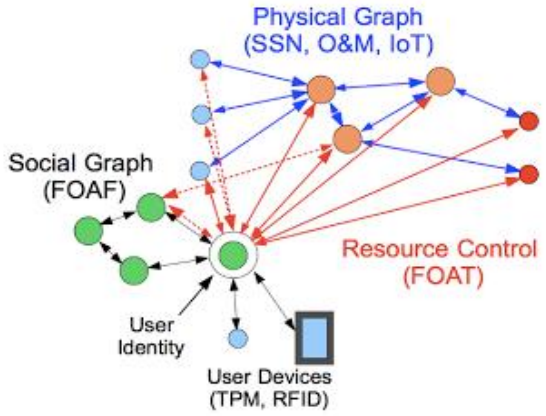
Tahmina Ahmed
Department of Computer Science
University of Texas at San Antonio
4/29/2016

Outline

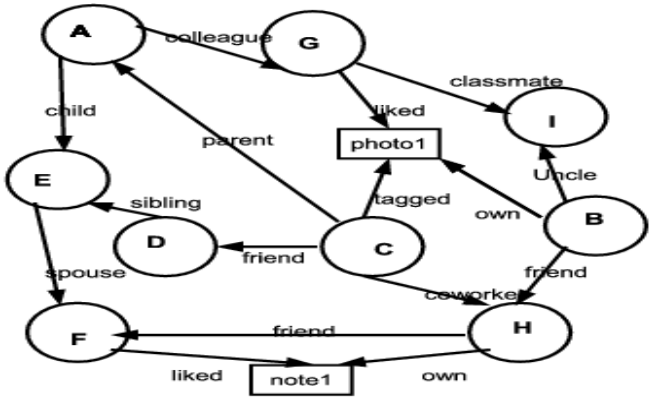
- Introduction and BackGround
- A Simple ReBAC Model
- Relationships in ABAC
  - Attribute Composition
  - Composite Attribute
- A Composite ABAC Model
- Comparison
  - Expressive Power
  - Complexity

Using Relations For Controlling Access

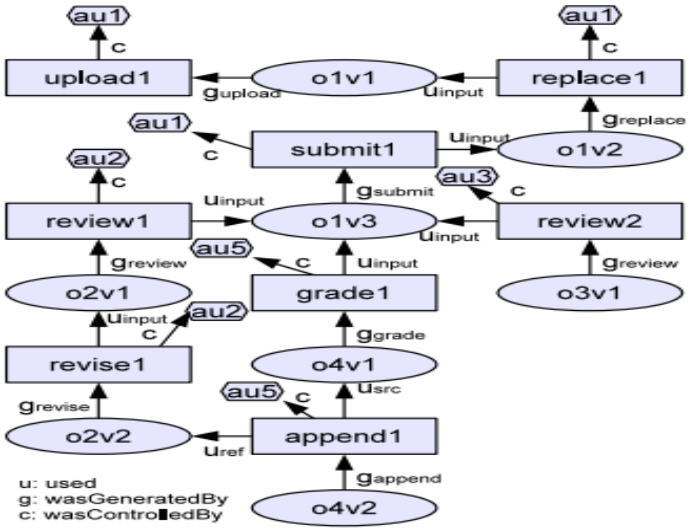




Access control for IOT

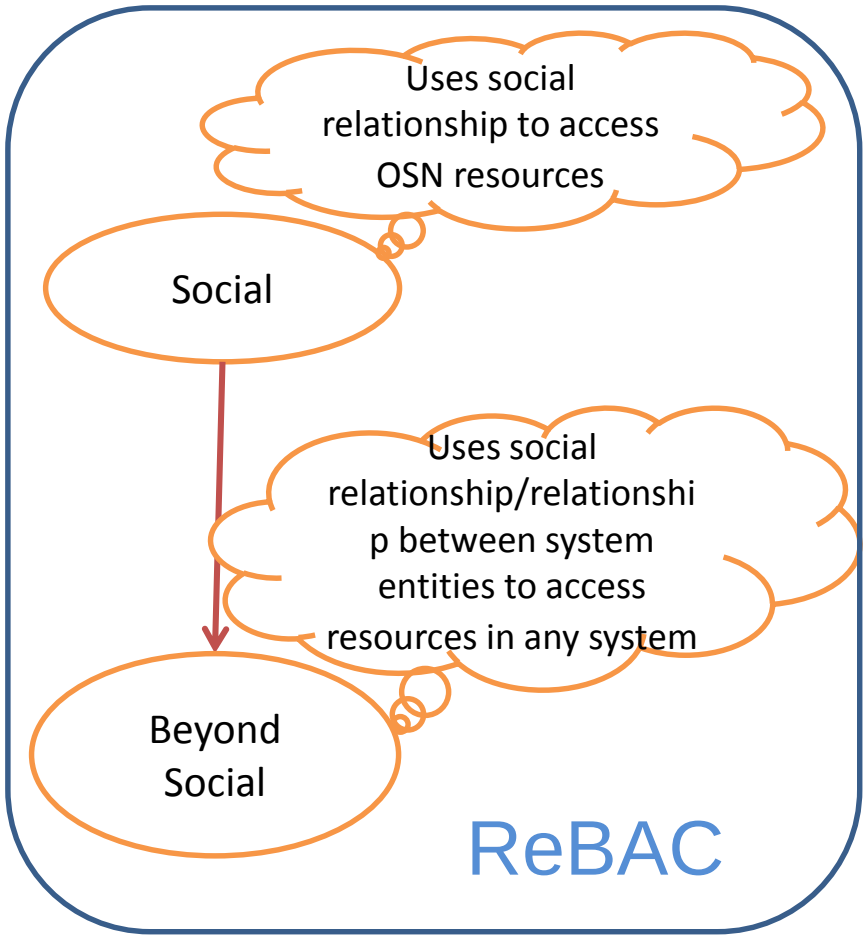


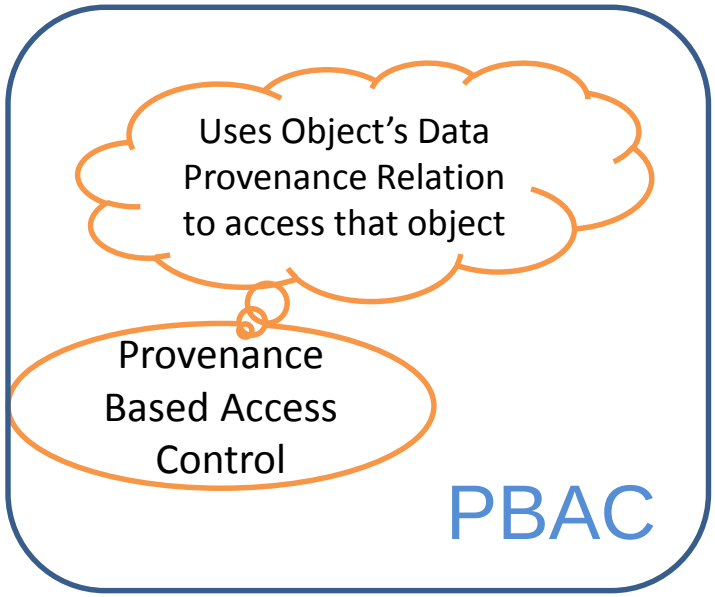
A sample social graph



A sample Provenance Graph (Park et al. 2012)

Existing Access Control Models those use some kind of Relations for authorization policy Expression

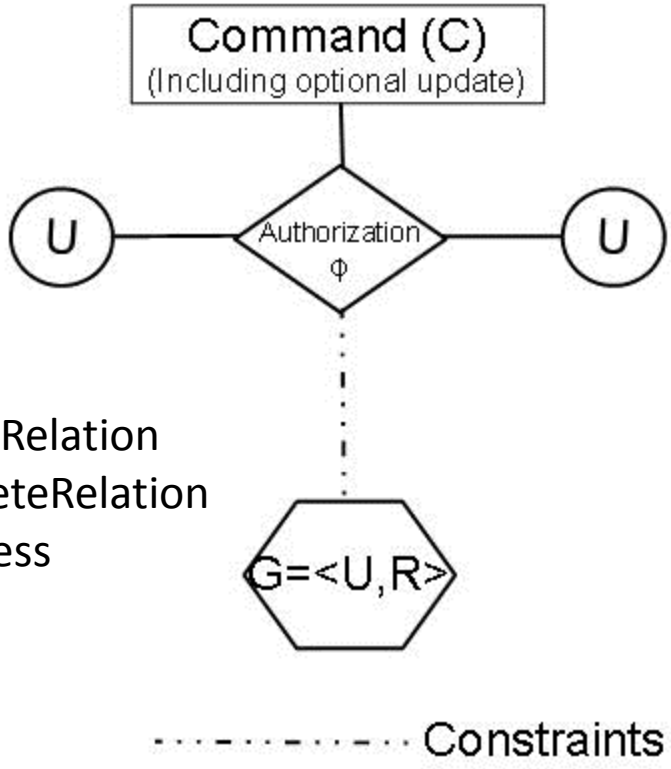




What Does ReBAC Mean?

- What does relationship based access control mean?
- What are the core characteristics of a ReBAC Model ?

A Simple ReBAC Model (SReBAC[p])



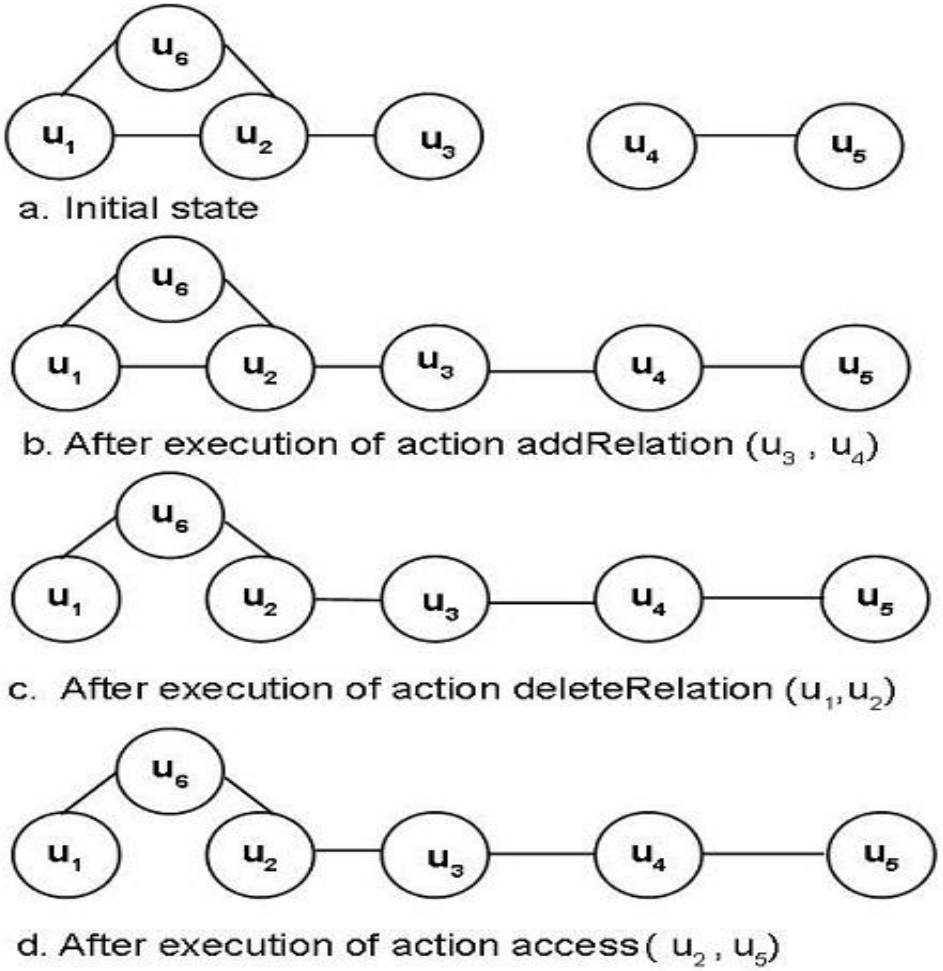
Commands

- addRelation
- deleteRelation
- access

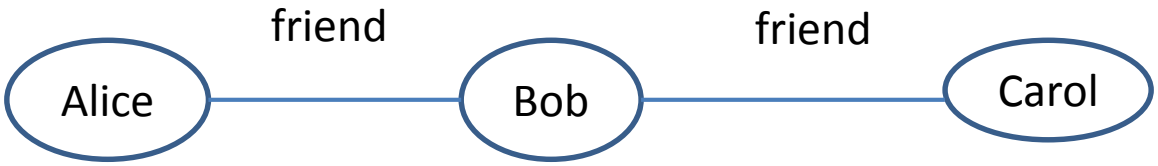
An Example Command Instantiation of SReBAC[3]

- addRelation^3(u_s:U, u_t :U)
  If $u_t \notin P^1(u_s)$then
  $R \cup = \{u_s, u_t\}$
- deleteRelation^3(u_s:U, u_t:U)
  If $u_t \in P^1(u_s) \wedge u_t \notin P^2(u_s)$ then
  $R \setminus = \{u_s, u_t\}$
- access^3(u_s:U, u_t:U)
  If $u_t \in P^3(u_s)$ then
  allow

An Example of a Simple ReBAC Command Execution



Expression of Relationship in ABAC



Attribute Composition

- Needs one attribute: friend
- Policy Expression uses Attribute composition

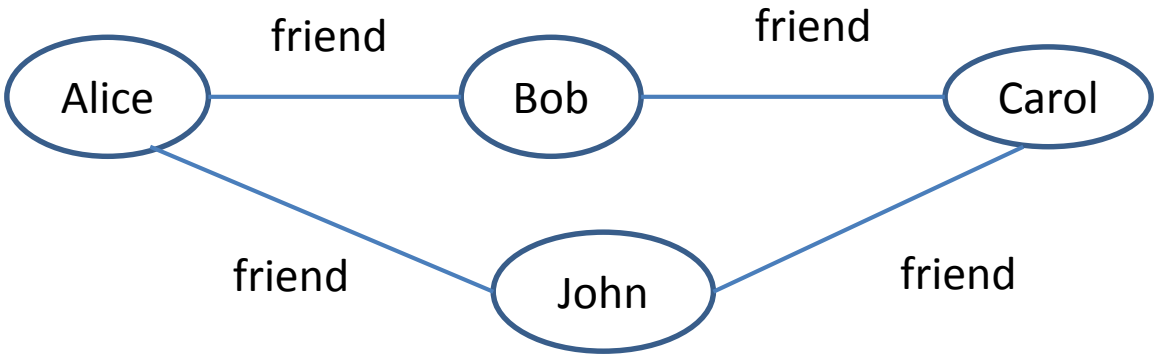
friend(Alice)={Bob}
friend(friend(Alice))={Carol}

Composite Attribute

- Needs two attribute
  1. friend
  2. friendoffriend
- Policy Expression uses direct attributes

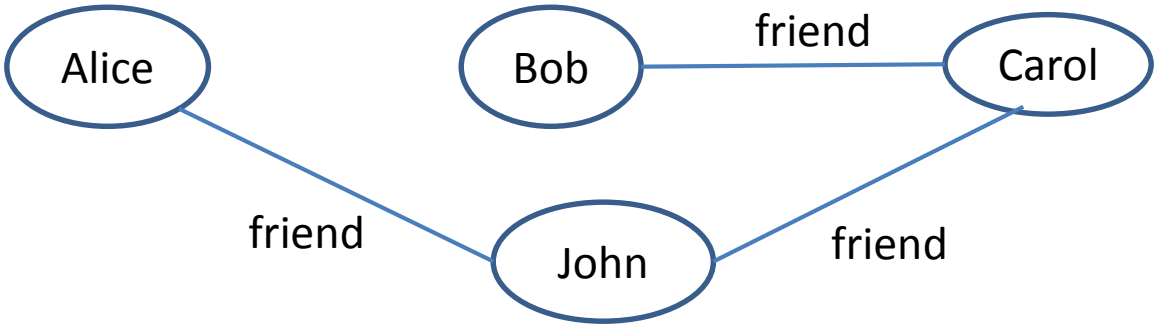
friend(Alice) ={Bob}
friendoffriend(Alice)={Carol}

Is this enough to keep the end user as an attribute value for Composite Attribute?



friend(Alice) = {Bob, John}
friendoffriend(Alice) = {Carol}

Is this enough to keep the end user as an attribute value for Composite Attribute?

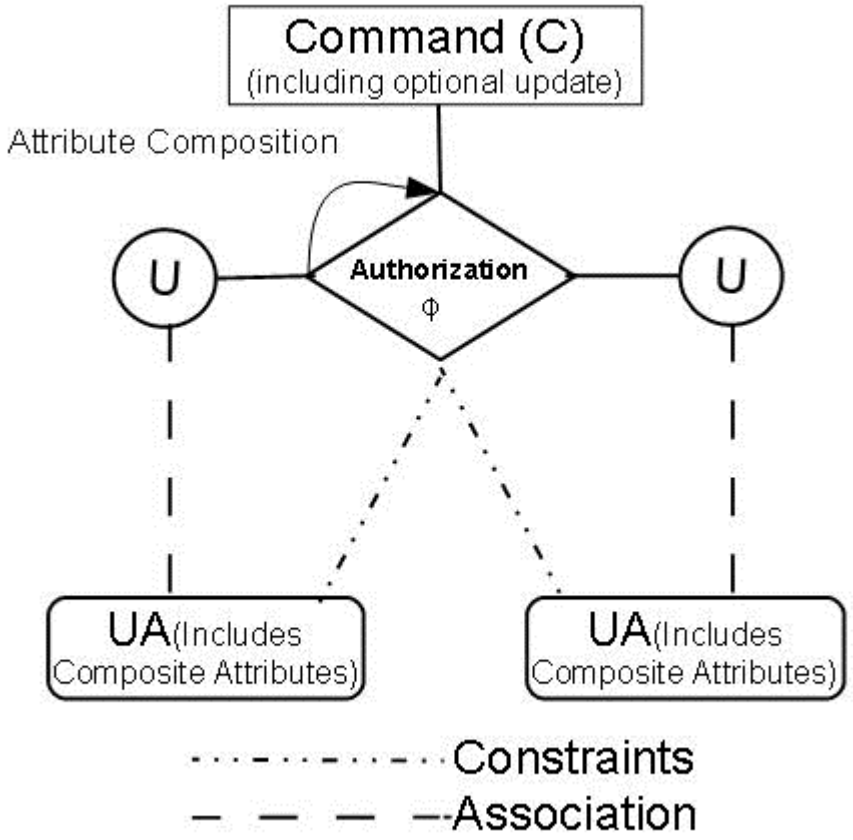


After execution of deleteRelation("Alice", "Bob")

friend(Alice) = {John}
friendoffriend(Alice) = ?

So we need to keep the relationship path information as a value of a composite attribute.
friendoffriend(Alice) = {Bob.Carol, John.Carol}----- Before Deletion
friendoffriend(Alice) = {John.Carol} ------ After Deletion

A Composite ABAC Model : $ABAC_C$ [n,m]



Comparison: Expressive Power Vs. Complexity

SReBAC [p] : Can Express Authorization Policy upto level p

$ABAC_C$ [n,m]: Can do n level attribute composition in authorization policy and has m -1 composite attributes.

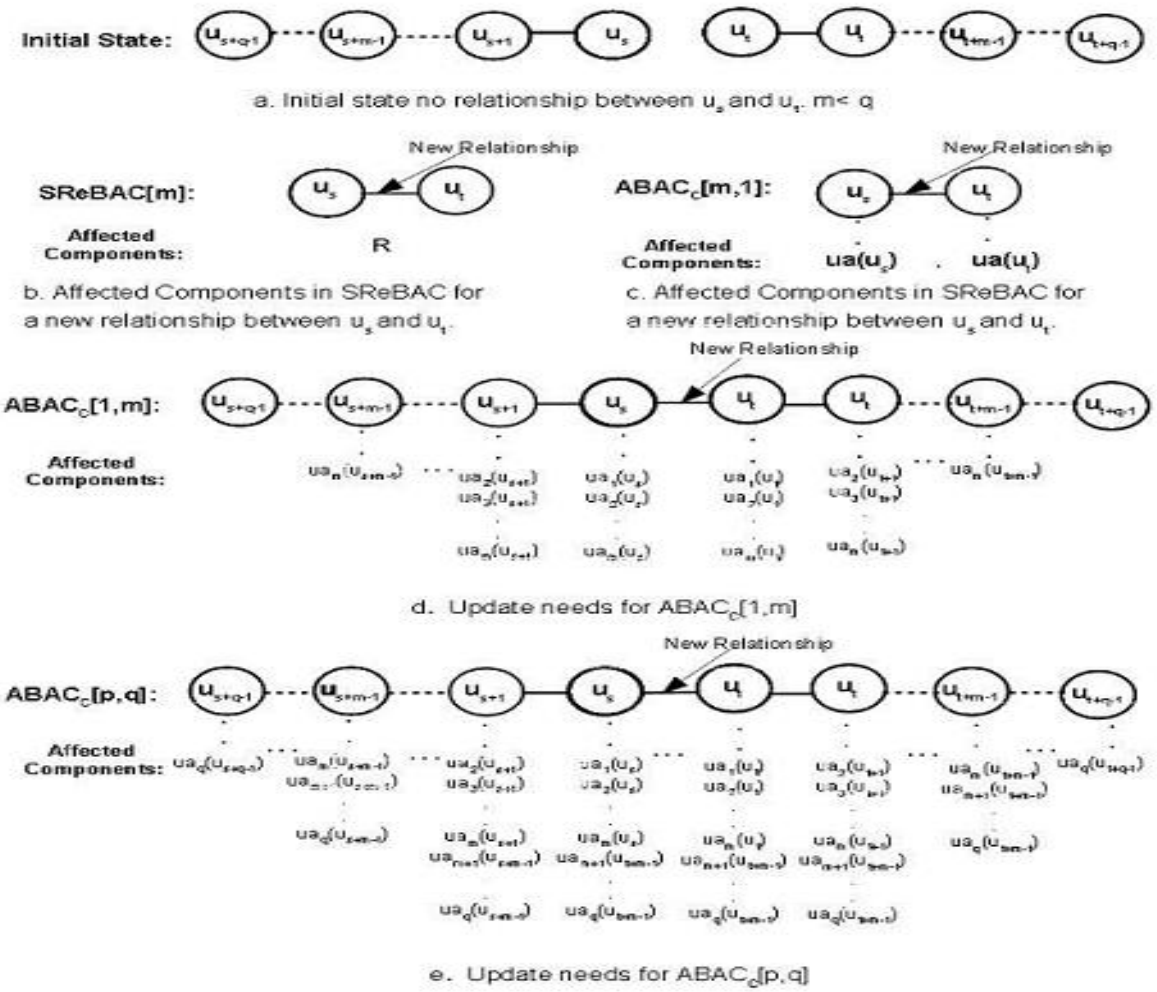
So $ABAC_C$ [n,m] can express Authorization Policy upto level n X m

Expressive Power Comparison:

So if p = n X m

SReBAC [p] has same expressive power as $ABAC_C$ [n,m]

Comparison: Expressive Power Vs. Complexity



Comparison: Expressive Power Vs. Complexity

Complexity Comparison

Performance Parameter	SReBAC[n]	$ABAC_C$[n,1]	$ABAC_C$[1,m]	$ABAC_C$ [p,q]
Space Complexity for Maintaining Relationship	$O(\|U\|+\|U\|^2)$	$O(\|U\|^2)$	$O(\|U\|^2 \times q)$	$O(\|U\|^2 \times q)$
Time Complexity for Computing Authorization Decision Rule	$O(\|U\|^n)$	$O(\|U\|^n)$	O(1)	$O(\|U\|^p)$
Number of update operations need for actions which change relationship	1	2	$\|U\| \times m \times (m+1)$	$\|U\| \times q \times (q+1)$
Cost for update (Worst Case)	O(1)	O(1)	O(m)	O(m)

Questions/Comments