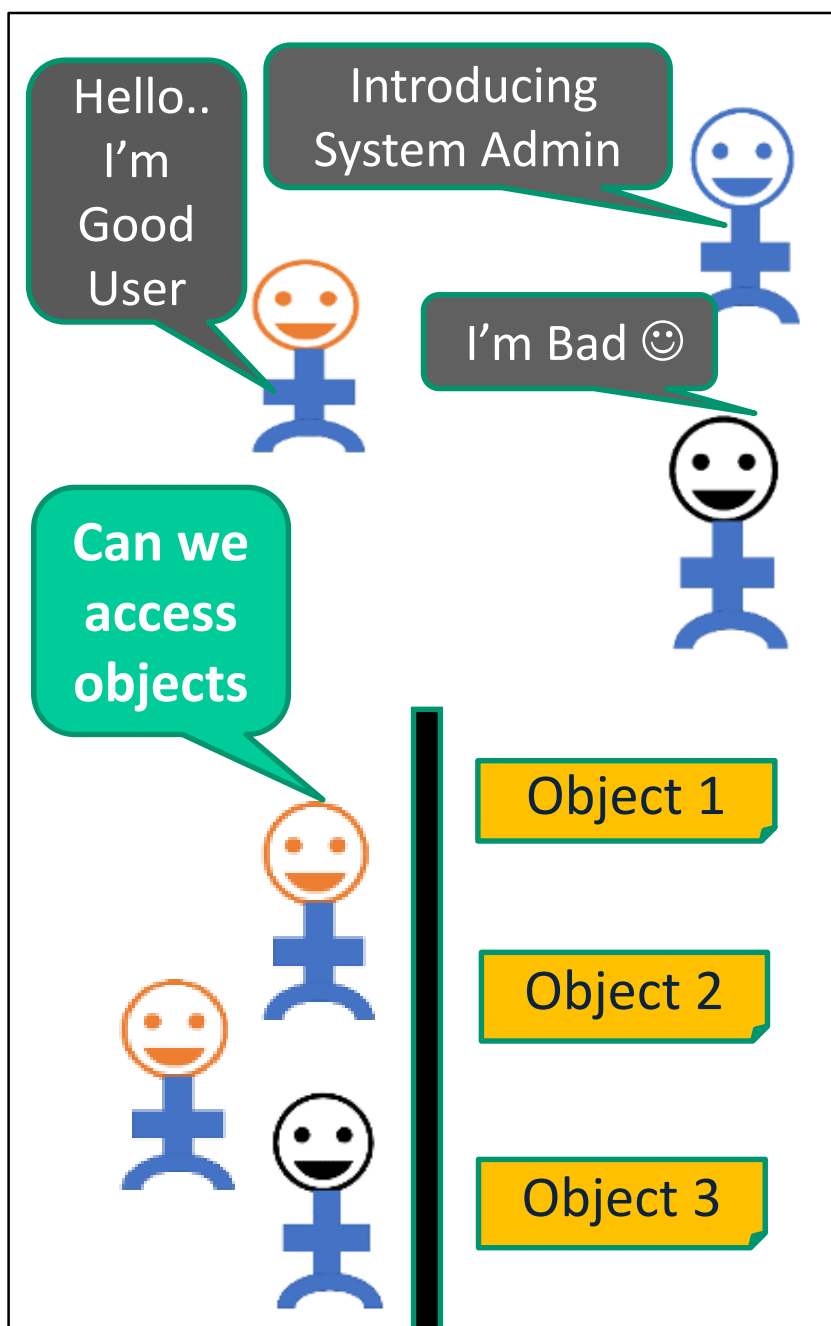


Shuvra Chakraborty, Ram Krishnan and Ravi Sandhu

The Institute for Cyber Security and Department of Computer Science, The University of Texas at San Antonio, San Antonio 78249, TX

### Meet the Scenario



Protect objects from unauthorized access

### Ask Questions!

- What is Authorization?
- Why Attribute-Based Access Control(ABAC)?
- Atomic Attributes
- Set Attributes
- Range
- Consistency

### Features

- ✓ **New direction !**
- ✓ **Always consistent**
- ✓ Atomic valued attribute
- ✓ Set valued attribute
- ✓ Assigned order of attribute values are really important
- ✓ Espresso constructs nearly optimal minimized form
- ✓ Manage ACCEPT, DENY and DON'T CARE
- ✓ Policy update is reasonably straightforward!

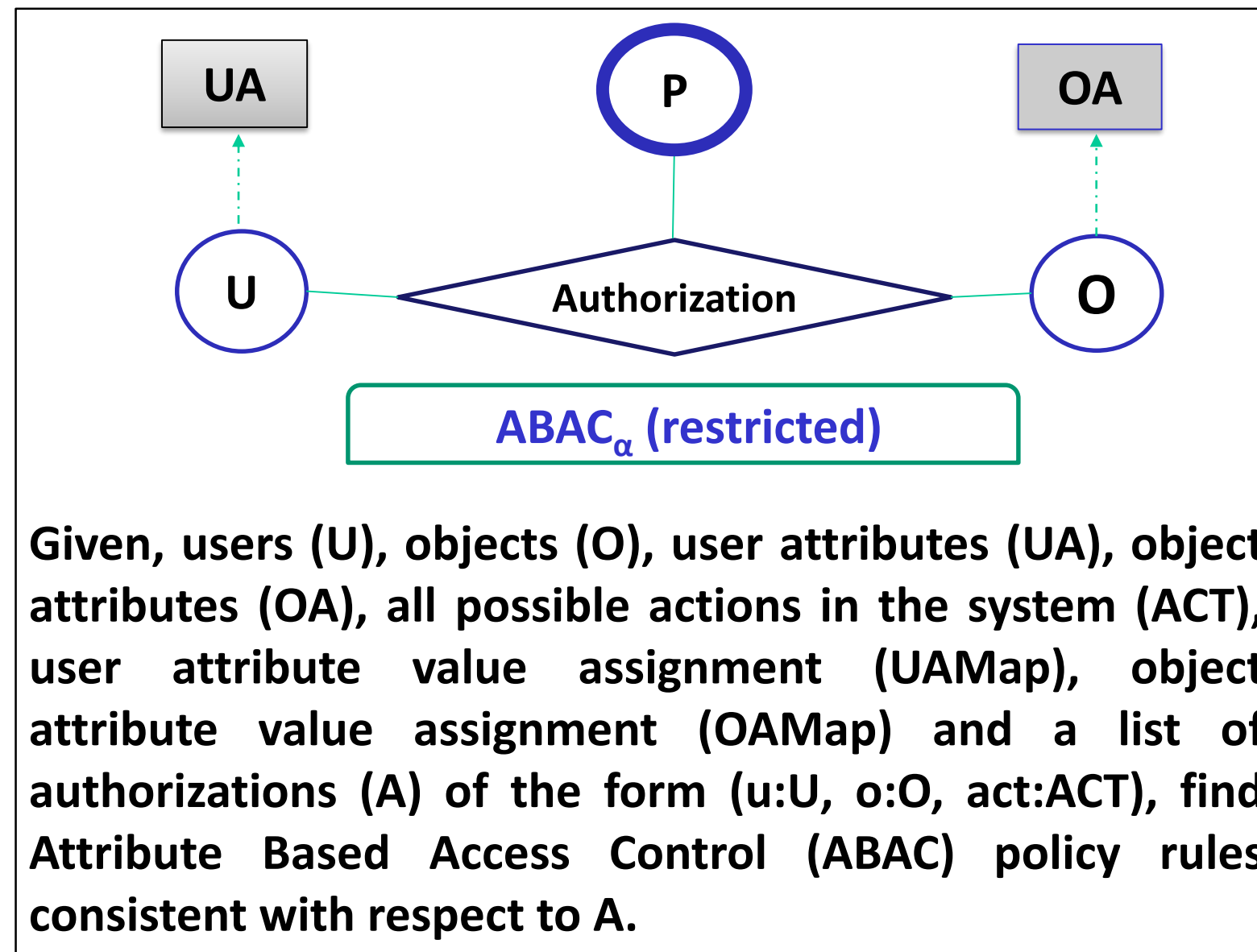
### Experiments

$F1(A,B,C,D,E) = ABCDE' | ABCD'E | AB'CDE'$   
 $F2(A,B,C,D,E) = ABCDE' | ABCD'E | AB'CDE'$

ESPRESSO LOGIC MINIMIZATION

$F1(A,B,C,D,E) = ACDE' | ABCD'E$   
 $F2(A,B,C,D,E) = ACDE' | ABCD'E$

### Problem Statement



### Check out use case!

User	Rank	Sec. Label	Object	Type	Authorization List
u1	Manager	{high, low}	r1	Database (DB)	(u1, r1, EDIT + PRINT) (u1, r2, EDIT + PRINT)
u2	Manager	{low}	r2	Document (DOC)	(u2, r1, EDIT + PRINT) DENY otherwise !!!

Rank = Manager	Sec. Label = high	Sec. Label = low	Type = DB	Type = DOC	EDIT	PRINT
1	1	1	1	0	1	1
1	1	1	0	1	1	1
1	0	1	1	0	1	1

A	B	C	D	E	F1 (A,B,C,D,E) = EDIT	F2 (A,B,C,D,E) = PRINT
1	1	1	1	0	1	1
1	1	1	0	1	1	1
1	0	1	1	0	1	1

Do you see the resemblance with truth table???

Total rules in policy = |ACT|

Finite domain only

“Hidden Assumption: Each user and object have distinct binary representation”

### Policy Refinement

Add (u2, r2, PRINT)  
(u2, r2, PRINT) → AB'CD'E

**Just OR and DONE!**

Revoke (u2, r1, PRINT)  
(u2, r1, PRINT) → AB'CDE'

Original eq. PRINT  
= ACDE' | ABCD'E  
= ACDE'. (B | B') | ABCD'E  
= ABCDE' | AB'CDE' | ABCD'E  
= ABCDE' | ABCD'E  
**EXPAND, CANCEL and DONE!**

### Future Works

- ✓ More experiments!
- ✓ Reduce total number of attributes
- ✓ Manage addition, change and removal of attributes
- ✓ “Minimize number of rules”, possible or not?
- ✓ Any better approaches for logic minimization?

### References

- Jin X., Krishnan R. and Sandhu R. **A unified attribute-based access control model covering DAC, MAC and RBAC.** In Proceedings 26th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSec), pp. 41-55, 2012.
- Talukdar T., Batra G., Vaidya J., Atluri V. and Sural S. **Efficient Bottom-Up Mining of Attribute Based Access Control Policies.** In IEEE 3rd International Conference on Collaboration and Internet Computing (CIC), pp.339-348, 2017.
- Elhoussini F. A., Rabie A. R. and Ali. A. R. **Espresso for rule mining.** 5th international conference on Ambient systems, Network and Technologies (ANT), pp. 596-603, 2014.
- Calo S., Verma D. and Chakraborty S. **Self-Generation of Access Control Policies.** In Proceedings of 23rd ACM on Symposium on Access Control Models and Technologies (SACMAT), pp. 39-47, 2018.
- Center for Electronic Systems Design: Webpage: <https://ptolemy.berkeley.edu/projects/embedded/pubs/downloads/espresso/> (Access date: Sep 24, 2018).
- Xu Z., and Stoller S. D. **Mining attribute-based access control policies.** The IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 5, pp. 533-545, 2015.