I·C·S
The Institute for Cyber Security

C·SPECC
Center for Security and Privacy Enhanced Cloud Computing

On the Feasibility of Attribute-Based Access Control Policy Mining

Shuvra Chakraborty[1], Ravi Sandhu[1] and Ram Krishnan[2]

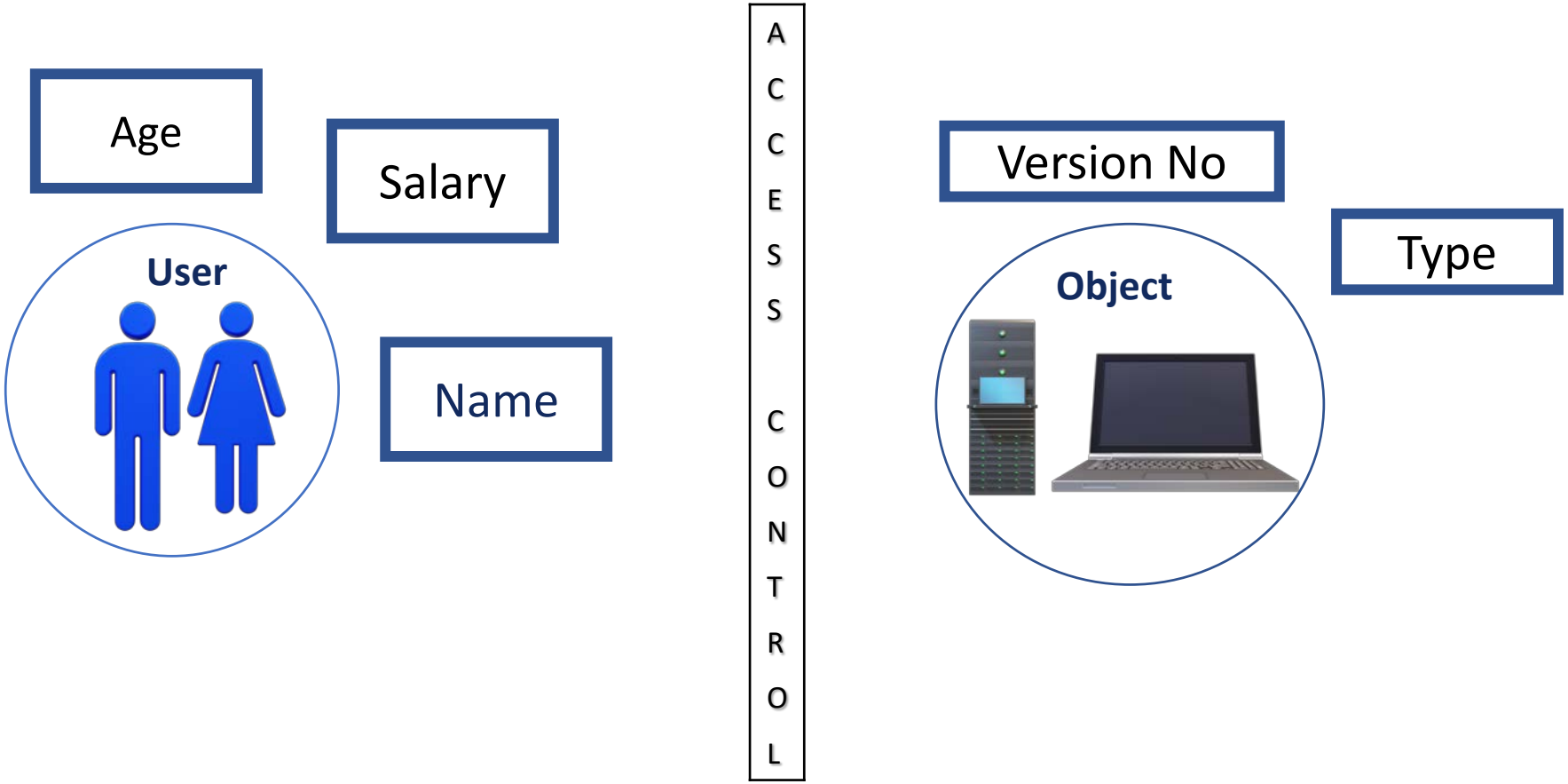
[1]Dept. of Computer Science, [2]Dept. of Electrical and Computer Engineering
[1,2]Institute for Cyber Security
University of Texas at San Antonio, TX 78249

20th IEEE International Conference on Information Reuse and Integration for Data Science (IRI '19)
Los Angeles, California, USA, July 30-August 1, 2019

World-Leading Research with Real-World Impact!

UTSA Computer Science

Introduction



Attribute-Based Access Control (ABAC) limits user to object access by using properties of both user and objects, namely "attribute".

ABAC policy mining

Access Control System

Authorization (AUTH)
(John, obj1, write)
(Lina, obj2, write)

Equivalent ABAC system

Supporting Data

UAValue		
User (U)	**Position**	**Dept.**
John	Officer	CS
Lina	Student	CS
Ray	Officer	CS
Tom	Officer	CS

OAValue	
Object (O)	**Type**
Obj1	File
Obj2	Printer

RangeSet	
Position	{Officer, Student, Faculty}
Dept.	{CS, EE}
Type	{File, Printer, Scanner}

Does an equivalent ABAC system exist for the given access control system and supporting data?

Example 0: no ID

Access Control System

Authorization (AUTH)
(John, obj1, write)
(Lina, obj2, write)

Equivalent ABAC system

Supporting Data

UAValue		
User (U)	**Position**	**Dept.**
John	Officer	CS
Lina	Student	CS
Ray	Officer	CS
Tom	Officer	CS

OAValue	
Object (O)	**Type**
Obj1	File
Obj2	Printer

RangeSet	
Position	{Officer, Student, Faculty}
Dept.	{CS, EE}
Type	{File, Printer, Scanner}

No IDs → Not possible

no way to separate John from Ray and Tom

Example 0: with ID

I·C·S The Institute for Cyber Security

C·SPECC Center for Security and Privacy Enhanced Cloud Computing

Access Control System

Authorization (AUTH)
(John, obj1, write)
(Lina, obj2, write)

Equivalent ABAC system

Supporting Data

UAValue			
User (U)	**uID**	**Position**	**Dept.**
John	u1	Officer	CS
Lina	u2	Student	CS
Ray	u3	Officer	CS
Tom	u4	Officer	CS

OAValue		
Object (O)	**oID**	**Type**
Obj1	o1	File
Obj2	o2	Printer

RangeSet	
Position	{Officer, Student, Faculty}
Dept.	{CS, EE}
Type	{File, Printer, Scanner}

Entity IDs → Always possible

e.g., RuleSet = {<u1, o1, write>, <u4, o2, print>}

Example 1

Access Control System

Authorization (AUTH)
(John, obj1, write)
(Ray, obj1, write)
(Tom, obj1, write)
(Lina, obj2, write)

Equivalent ABAC system

Supporting Data

UAValue		
User (U)	**Position**	**Dept.**
John	Officer	CS
Lina	Student	CS
Ray	Officer	CS
Tom	Officer	CS

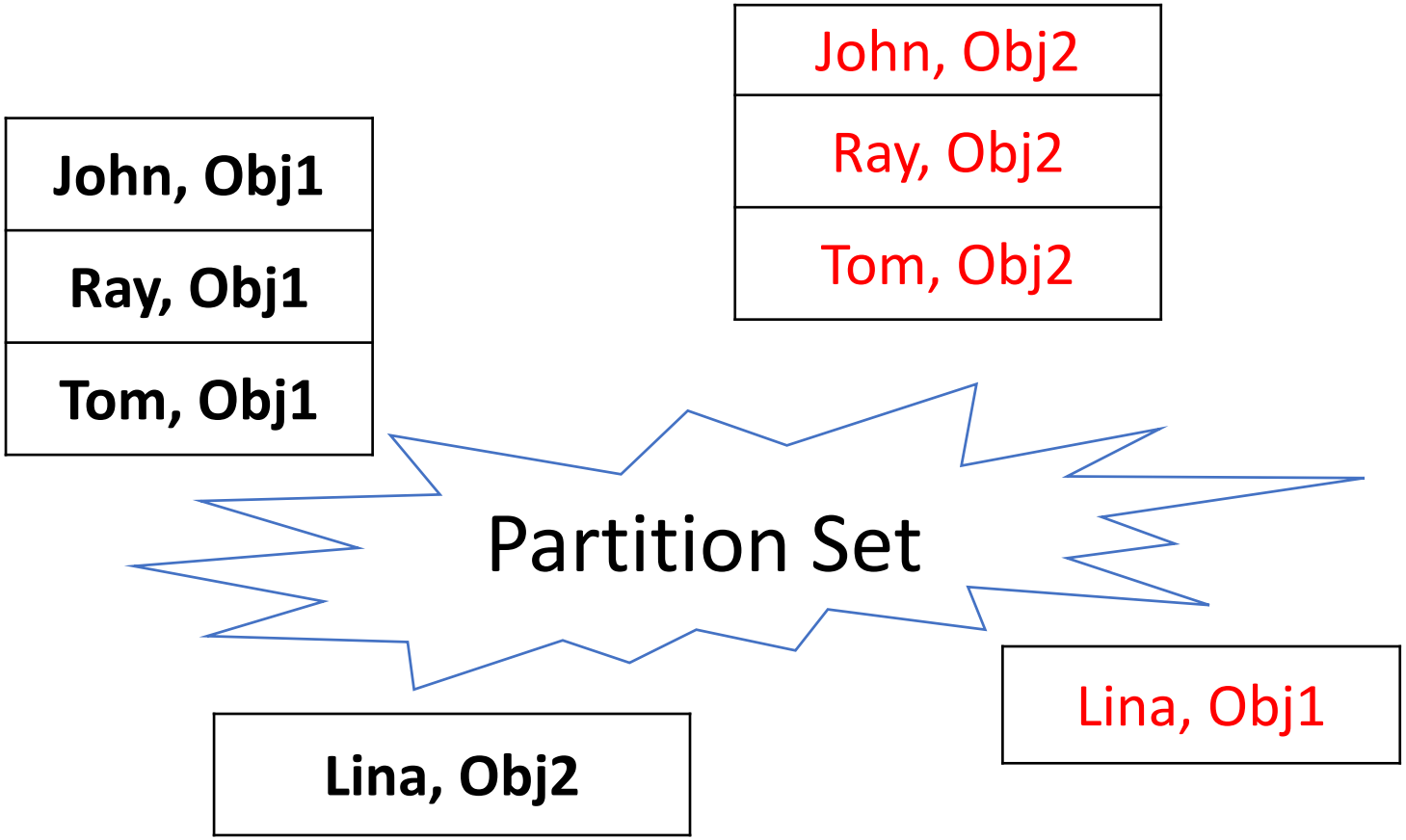
OAValue	
Object (O)	**Type**
Obj1	File
Obj2	Printer

RangeSet	
Position	{Officer, Student, Faculty}
Dept.	{CS, EE}
Type	{File, Printer, Scanner}

Determine the feasibility before rule generation!

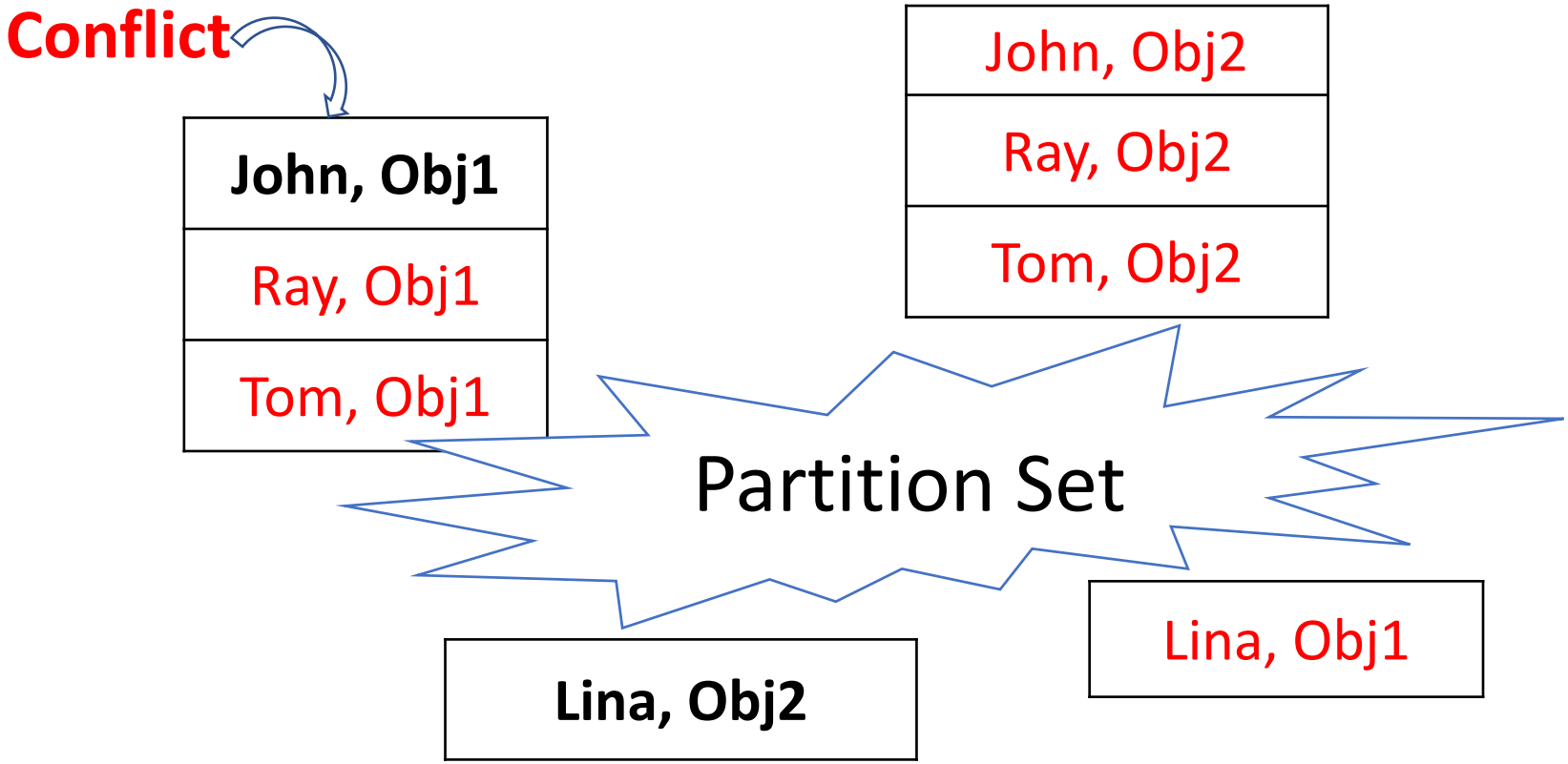
Our solution: Partition-based strategy

Partition set: example 1



Partition set is conflict-free w.r.t. write → Yes

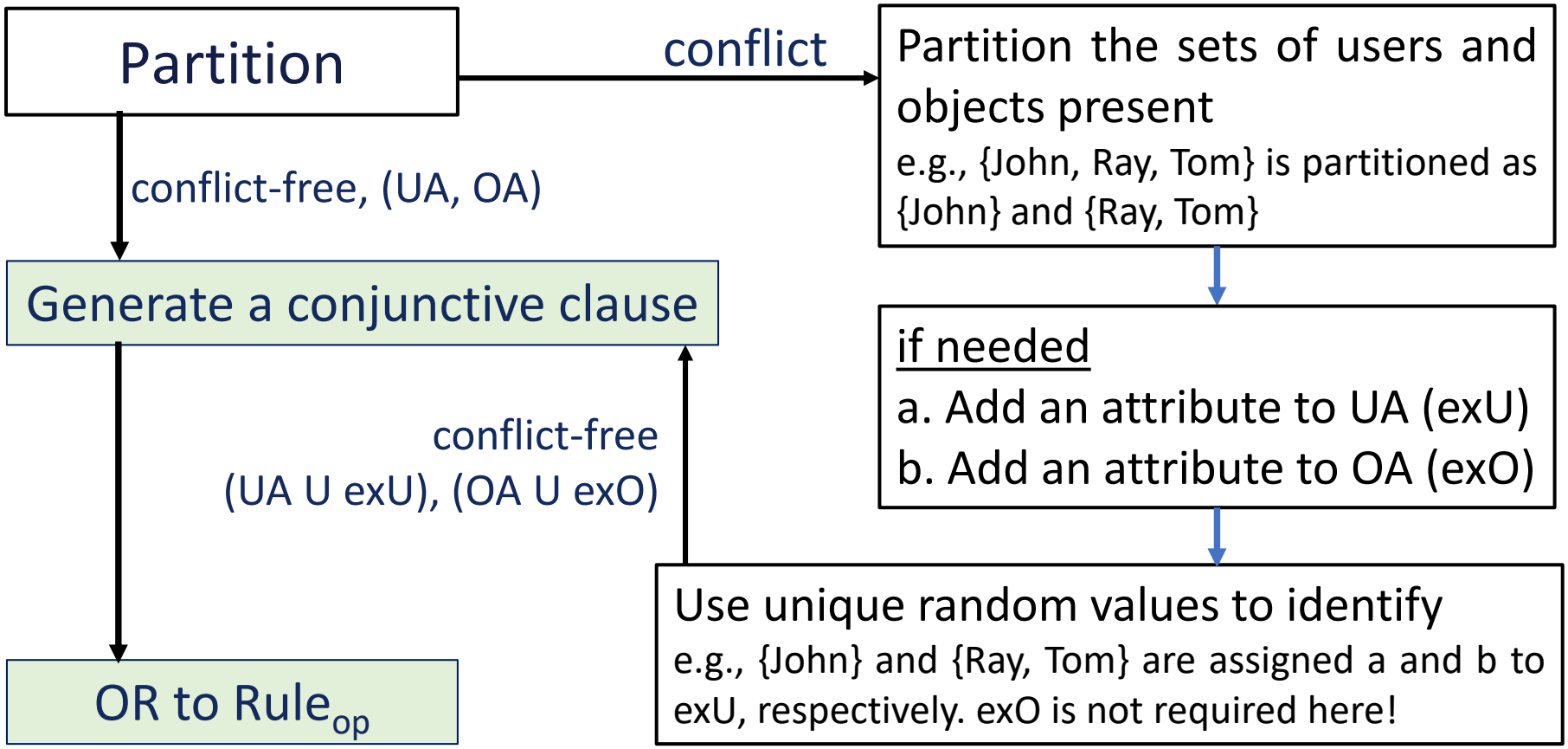
Partition set: example 0



Authorization (AUTH)
(John, obj1, write)
(Lina, obj2, write)

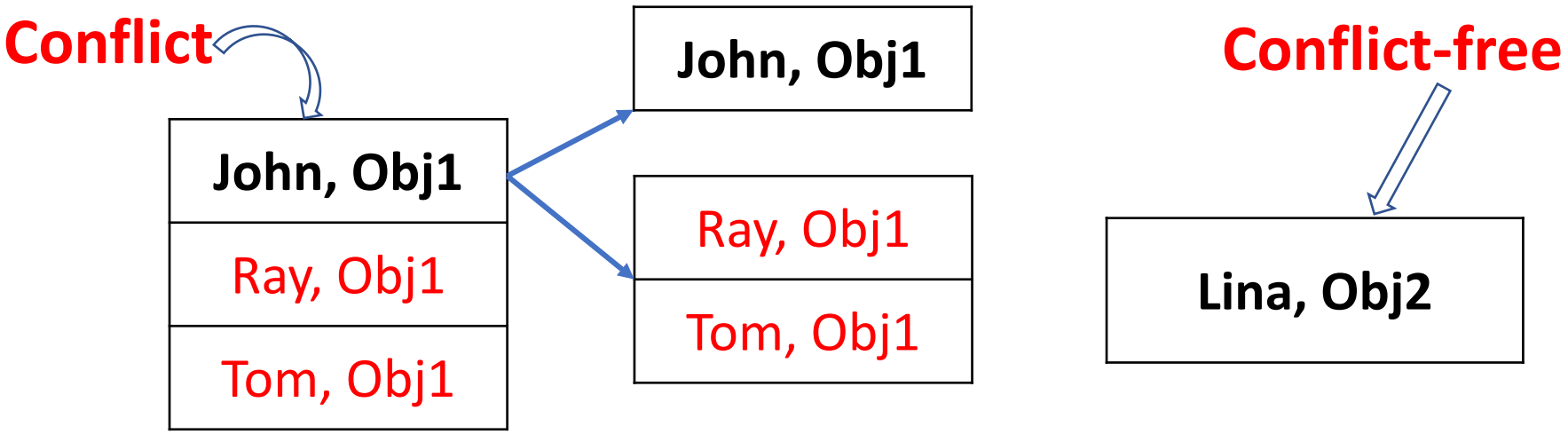
Ray and Tom has no authorization compared to example 1

Infeasibility correction



Exact Solution can be achieved many ways

Example 0: Rule Generation



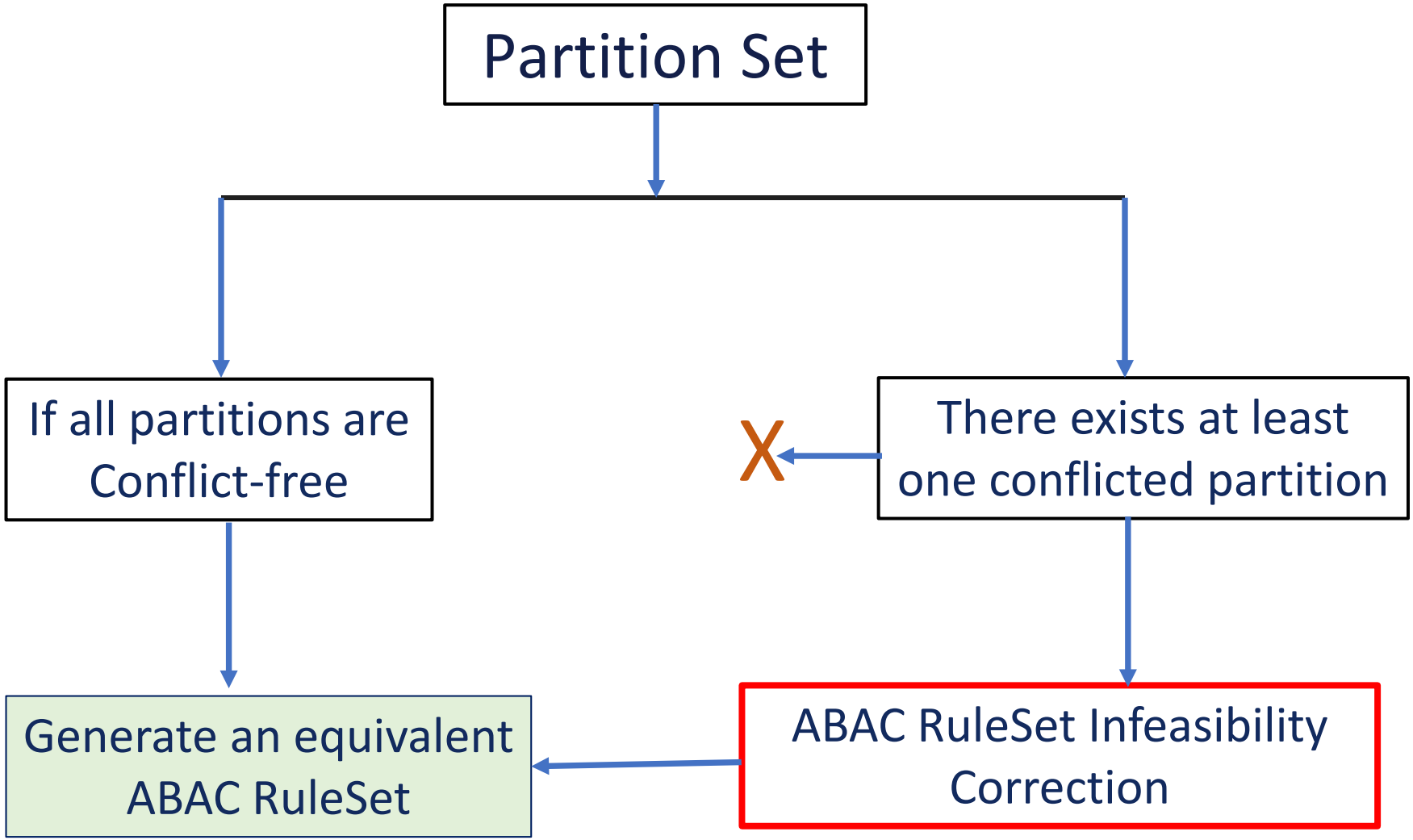
$Rule_{write}$ ≡ (Position = officer AND Dept = CS AND exU = a AND Type = File) OR (Position = student AND Dept=CS AND Type = Printer)

ABAC system

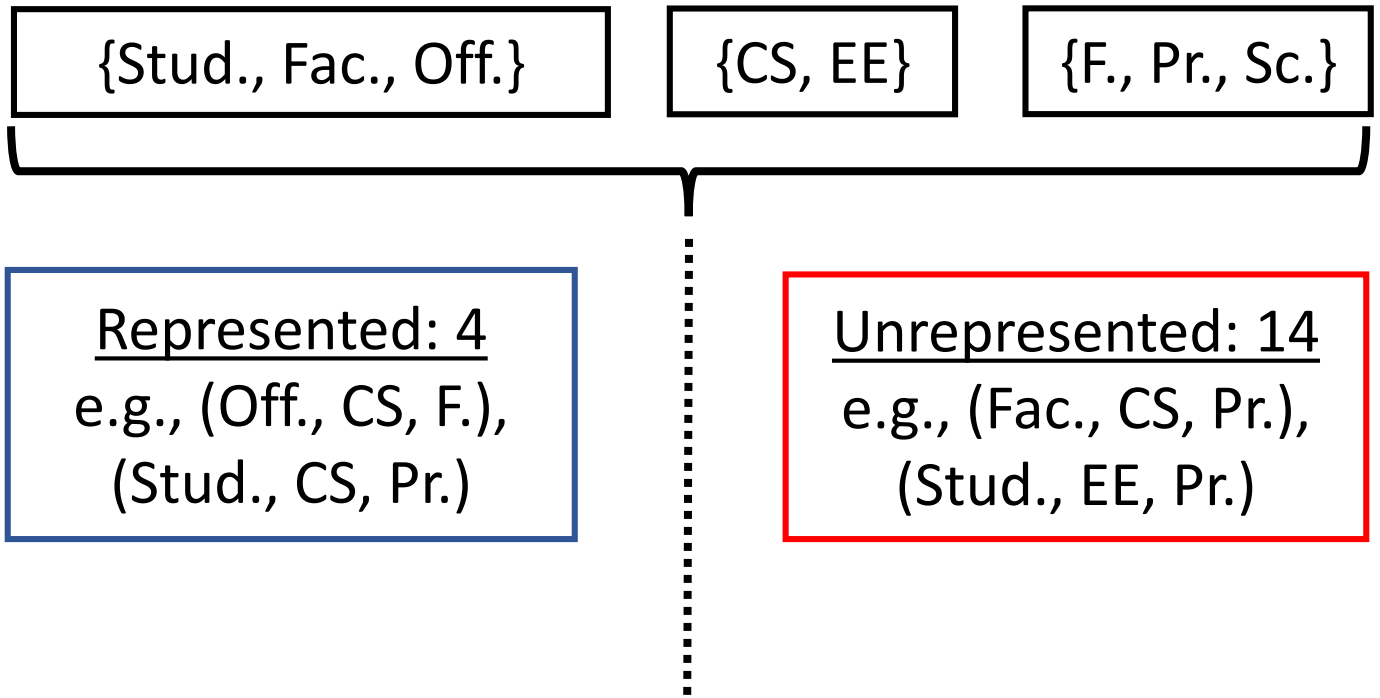
<U, O, OP, UA, OA, RangeSet, UAValue, OAValue,{$Rule_{write}$}, $checkAccess_{ABAC}$>

Equivalent ABAC system generation is always possible!

At a glance


Partition Set
If all partitions are Conflict-free
X
There exists at least one conflicted partition
Generate an equivalent ABAC RuleSet
ABAC RuleSet Infeasibility Correction

Unrepresented partition



Outcome of peculiarity in attribute value assignment

Contributions

- **Formalized notion of feasibility on ABAC policy mining: first time**
- **Exact solution is always possible**
- **Unrepresented partition problem**

- **<u>Challenges</u>**
- Can you replace random values?
- More compact set of rule generation
- Exact solution:
  - Reduce number of split partitions
  - Change number of attributes required
  - Changing existing attribute set, possible?
- Approximate Solution
  - Change authorization
  - Change existing attribute value assignment


Questions