

Access Control for XML Data



Vaibhav Gowadia

Dept. of Computer Science and Engineering
University of South Carolina, Columbia



Motivation

Current XML access control models do not provide:

- ◆ Flexible Security Granularity
- ◆ Flexible Conflict Resolution

Example

```
<document>
  <patient>
    <name>Bob </name>
    <phone>777-1234</phone>
    <age>50</age>
    <race>Caucasian</race>
    <diagnosis>cancer</diagnosis>
  </patient>
  ...
</document>
```



Example contd.

- ◆ Alice needs read privilege for <name> and <Phone> to contact patients for collecting feedback.
- ◆ Alice needs read privileges on <age>, <race> and <diagnosis> for preparing technical reports.
 - Do we need to trust Alice to look at entire patient record ?



Associated Elements

- ◆ A group of elements and/or attributes occurring together in user view.
- ◆ Examples:
 - Name and salary
 - Name and prescription1 and prescription2
 - Name and job1 and job2
- ◆ Note: Knowledge of individual elements and attributes to user is not significant.



Conflict Resolution

Current Solutions:

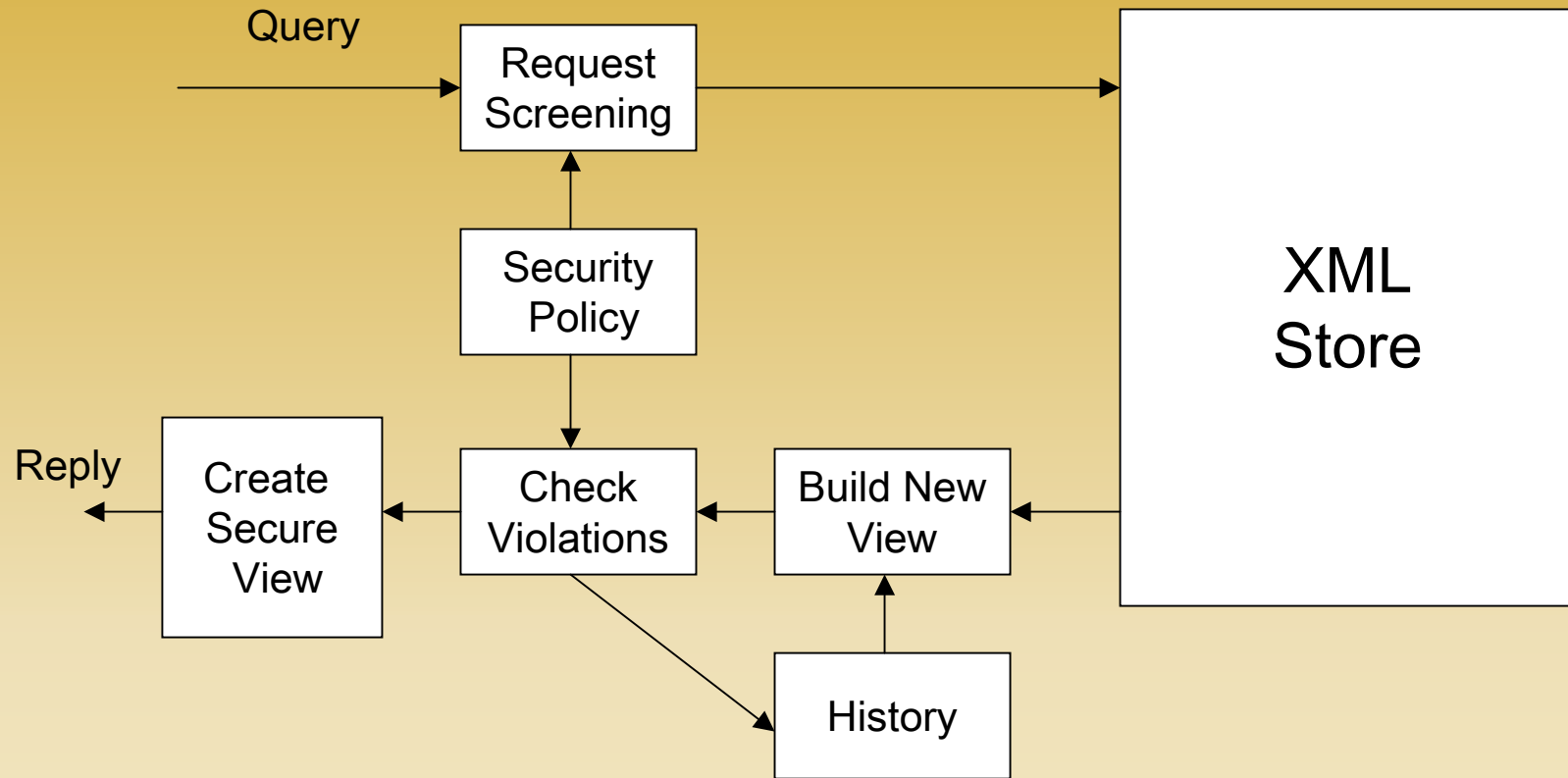
- Denials take precedence
- Most specific authorization takes precedence



Our Solution: RXACL

- ◆ RDF based eXtensible Access Control Solution
- ◆ Security Policy is defined in RDF
- ◆ Policy Components:
 - Objects
 - Rules
 - User's access right description
 - Conflict resolution

Enforcing RXACL



Conclusions

RXACL will provide:

- ✓ More granular access control
- ✓ Easy conflict resolution
- ✓ Policy Validation

