A Secure EPC Discovery Service System in EPCGlobal Network

- Jie Shi, Darren Sim, Yingjiu Li, Robert Deng
Background

- Internet-of-Things (IOT) is the next big thing
- Vast amount of Data to be generated through IOT devices & users
- Urgent need for an effective search engine to make sense of this data
- System needs to process search efficiently, while remaining secure
Architecture of EPCglobal Network
Security of EPCDS

Motivation for Access Control

Sensitivity of Data

High Value of Data
Security of EPCDS

Requirements and Challenges

Different access control policies from different EPCISes

Users may not be known in advance

Visibility policy only in EPCDS
Visibility Policy

- Whole stream policy
- Up stream policy
- Down stream policy
Supply chain (R1 define policy for his event information about epc1)

Whole stream policy

Up stream policy

Down stream policy

Diagram:

- Node M1: Policy creator
- Node D1: Allow to access
- Node R1: Not allow

Timeline:

- 2011-01-20
- 2011-01-23
- 2011-02-05
- 2011-02-15
Attribute-based access control

- Subject attribute, object attribute, visibility attribute
- Authorization Language

AUL:=object condition \& subject condition \\
| object condition \& visibility condition \\
| object condition \& subject condition \& visibility condition
Example

- Security requirements of company R1:

  For the information about any product handled after 2011-01-01, it is allowed to be accessed by the users of these companies who also handle this product and are distributor companies.

- Policy:

  $\text{Time} > 2011-01-01 \land \text{Visibility} = \text{whole-stream} \land \text{Role} = \text{Distributor}$
SecDS system
Policy Management

- Manage access control policies
- Three steps taken in creation of ABAC policy

ABAC policy transformation enhances query performance at the cost of policy management
Example

(b) User-Companies

<table>
<thead>
<tr>
<th>UserID</th>
<th>Name</th>
<th>CompanyId</th>
</tr>
</thead>
<tbody>
<tr>
<td>U1001</td>
<td>Bob</td>
<td>C101</td>
</tr>
<tr>
<td>U1002</td>
<td>Andy</td>
<td>C102</td>
</tr>
<tr>
<td>U1003</td>
<td>John</td>
<td>C103</td>
</tr>
<tr>
<td>U1004</td>
<td>Peter</td>
<td>C104</td>
</tr>
<tr>
<td>U1005</td>
<td>Jack</td>
<td>C105</td>
</tr>
</tbody>
</table>

(c) Companies

<table>
<thead>
<tr>
<th>CompanyId</th>
<th>Name</th>
<th>Role</th>
<th>URI</th>
</tr>
</thead>
<tbody>
<tr>
<td>C101</td>
<td>M1</td>
<td>Manufacturer</td>
<td><a href="http://www.m1.com">http://www.m1.com</a></td>
</tr>
<tr>
<td>C102</td>
<td>D1</td>
<td>Distributor</td>
<td><a href="http://www.d1.com">http://www.d1.com</a></td>
</tr>
<tr>
<td>C103</td>
<td>D2</td>
<td>Distributor</td>
<td><a href="http://www.d2.com">http://www.d2.com</a></td>
</tr>
<tr>
<td>C104</td>
<td>R1</td>
<td>Retailer</td>
<td><a href="http://www.r1.com">http://www.r1.com</a></td>
</tr>
<tr>
<td>C105</td>
<td>R2</td>
<td>Retailer</td>
<td><a href="http://www.r2.com">http://www.r2.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Predicate</th>
<th>Creator</th>
<th>CompanyId</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>pol1</td>
<td>$\text{Time} &gt; 2011-01-01 \land (\text{Visibility} = \text{whole-stream} \land \text{Role} = \text{Distributor})$</td>
<td>C1001</td>
<td>C101</td>
</tr>
<tr>
<td>2</td>
<td>pol2</td>
<td>$\text{EPC LIKE urn:epc:id:sgtin:4049588:083310:* \land Name IN (M1, D1, R1)}$</td>
<td>C1002</td>
<td>C102</td>
</tr>
<tr>
<td>3</td>
<td>pol3</td>
<td>$\text{EPC NOT LIKE urn:epc:id:sgtin:4049588:083310:* \land Visibility = whole-stream}$</td>
<td>C1002</td>
<td>C102</td>
</tr>
<tr>
<td>4</td>
<td>pol4</td>
<td>$\text{Time} &gt; 2011-03-01 \land \text{Visibility = up-stream}$</td>
<td>C1004</td>
<td>C104</td>
</tr>
</tbody>
</table>

Table 2: ABAC Policy Table.

<table>
<thead>
<tr>
<th>UserID</th>
<th>BACPolicy</th>
<th>ObjectPredicate</th>
<th>Visibility</th>
<th>Creator</th>
<th>CompanyId</th>
</tr>
</thead>
<tbody>
<tr>
<td>1002</td>
<td>pol1</td>
<td>$\text{TIME &gt; 2011-01-01}$</td>
<td>whole-stream</td>
<td>U1001</td>
<td>C101</td>
</tr>
<tr>
<td>1003</td>
<td>pol1</td>
<td>$\text{TIME &gt; 2011-01-01}$</td>
<td>whole-stream</td>
<td>U1001</td>
<td>C101</td>
</tr>
<tr>
<td>1001</td>
<td>pol2</td>
<td>$\text{EPC LIKE urn:epc:id:sgtin:4049588:083310:*}$</td>
<td>NULL</td>
<td>U1002</td>
<td>C102</td>
</tr>
<tr>
<td>1002</td>
<td>pol2</td>
<td>$\text{EPC LIKE urn:epc:id:sgtin:4049588:083310:*}$</td>
<td>NULL</td>
<td>U1002</td>
<td>C102</td>
</tr>
<tr>
<td>1004</td>
<td>pol2</td>
<td>$\text{EPC LIKE urn:epc:id:sgtin:4049588:083310:*}$</td>
<td>NULL</td>
<td>U1002</td>
<td>C102</td>
</tr>
<tr>
<td>0</td>
<td>pol3</td>
<td>$\text{EPC NOT LIKE urn:epc:id:sgtin:4049588:083310:*}$</td>
<td>whole-stream</td>
<td>U1002</td>
<td>C102</td>
</tr>
<tr>
<td>0</td>
<td>pol4</td>
<td>$\text{TIME &gt; 2011-03-01}$</td>
<td>up-stream</td>
<td>U1004</td>
<td>C104</td>
</tr>
</tbody>
</table>

Table 3: FGAC policy table.
Policy Service

- FGAC Policy Searching Service (FPSS)

- FGAC Policy Combining Service (FPCS)
Transformation of Visibility Policy

- **Whole-stream policy:**
  \[ \text{exist (select 1 from } T1 \text{ where } T1\.companyId = c_1 \text{ and } T\.EPC = T1\.EPC) } \]

- **Up-stream policy:**
  \[ \text{exist (select 1 from } T1 \text{ where } T1\.companyId = c_1 \text{ and } T\.EPC = T1\.EPC \text{ and } T1\.Time < T\.Time) } \]

- **Down-stream policy:**
  \[ \text{exist (select 1 from } T1 \text{ where } T1\.companyId = c_1 \text{ and } T\.EPC = T1\.EPC \text{ and } T1\.Time > T\.Time) } \]
**Definition 7.1 (Policy Composition).** Given policies $p_i = (u, pr_i, c_i), i \in [1 \ldots n]$ for user $u$ defined by companies $c_i, i \in [1 \ldots n]$, the combined predicate $pr = (pr_1 \land o.owner = c_1) \lor \ldots \lor (pr_n \land o.owner = c_n)$. 

Own Predicate
The basic idea of query modification is that before being processed, user queries are transparently modified to ensure that users can access only what they are authorized to access.

Using the predicate combined in Policy Service to construct a temporary view and replace the table in users queries by this temporary view.
Experiments

Figure 6: The performance of varying maximum number of supply chains. The other parameters: the number of EPCISes: 300; the max number of EPCISes in a supply chain: 30; the percentage of access control policies: 50%.

Figure 7: The performance of varying Max number of EPCISes in a supply chain. The other parameters: the number of supply chains: 10000; the number of EPCISes: 300; the percentage of access control policies: 50%.
Experiments

- The average query response time is about 260ms in a setting of 50,000 supply chains, 300 EPCISes, on average 20 EPCISes being involved in each supply chain and on average 10 policies being evaluated for each query.
Conclusion

- We analyzed and summarized the requirements of access control for EPCDS;

- We extended ABAC to satisfy these requirements, especially for visibility policy;

- We mainly use two approaches to enhance the performance of users queries
  - Transform ABAC to FGAC
  - Query modification

- We implemented prototype of SecDS and conducted rigorous experiment. The results validate SecDS is practical.
Do You Have Any Questions?