Qualitative Intention-Aware Attribute-Based Access Control Policy Refinement

Shohei Mitani¹, Jonghoon Kwon², Nakul Ghate¹, Taniya Singh¹, Hirofumi Ueda¹, Adrian Perrig²

¹NEC Corporation, Japan
²ETH Zürich, Switzerland
Background

Attribute-based Access Control (ABAC) policy generation.

✓ Rule mining vs. Machine learning (ML).

ACLs
Access logs

Rule mining

Machine learning


ACLs

Rule 1:
User’s position $\in \{\text{"Nurse", "Doctor"}\}$,
User’s department $== \text{Resource department}$, ....

ACLs

( “a0001p54”, “example.com/customer”, “Read”), “Allow”

ACLs

Decision engine

Attribute vector

“Deny”

[22] Zhongyuan Xu and Scott D Stoller. 2014.

Problem Definition

Pre-designed policies are assumed.

✓ Poor decisions arise outside the policy designers’ scopes (i.e., not envisioned).

Decision scopes

- Sales task
- Data breach prevention
- Production task 1
- Production task 2

ABAC policies
ACLs
Access logs
Machine Learning
Usage

Machine Learning

ABAC decision engine
Problem Definition

Pre-designed policies are assumed.

✓ Poor decisions arise outside the policy designers’ scopes (i.e., not envisioned).

Decision scopes

- Sales task
- Data breach prevention
- Production task 1
- Production task 2

ABAC policies
ACLs
Access logs
Usage

Machine Learning
ABAC decision engine

- Development tasks?
- Marketing tasks?
Problem Definition

Pre-designed policies are assumed.

✓ Poor decisions arise outside the policy designers’ scopes (i.e., not envisioned).

A sensitive source code is available to all users regardless of their job position.

- Development tasks?
- Marketing tasks?
Problem Definition

Pre-designed policies are assumed.
✓ Poor decisions arise outside the policy designers’ scopes (i.e., not envisioned).

Decision scopes

- Sales task
- Data breach prevention
- Production task 1
- Production task 2

- ABAC policies
- ACLs
- RBAC policies

- Access logs
- Usage

Machine Learning

- ABAC decision engine
- Maintenance access?
- Unnecessary disclosure?
Motivation

Better balances of security and usability,
✓ By refining access control policies (or access logs.)

Permissive

Restrictive

Non-sense

Beneficial

“All Allow”

Team’s resource is accessible from office.

“All Deny”

Access to public info. is allowed.

The “best” policy.

Random

Team’s source code is accessible with MFA from home.

Fine-grained access control
Motivation

Policy designers underlying intentions are assumed.

✓ Explicitly reflect the **intentions from various aspects** to policy refinement.

Permissive

- Non-sense
  - "All Allow"
  - "All Deny"
  - Random
  - Fine-grained access control

Restrictive

- Beneficial
- Confidentiality
- Access to public info. is allowed.
- Team’s source code is accessible with MFA from home.
- Team’s resource is accessible from home.

The "best" policy.
Goal

A decision engine is created by refining access control policies.
✓ Intentions lead to enhancing security without compromising usability.

Access Control Policies

Workers can access from office only.

Developers can access from anywhere.

Underlying intentions

Prefer to deny:
Sensitive data access from insecure system.

Prefer to allow:
Completion of development tasks.

Our Decision Engine

Developer’s access to source code from home with passwd.

Developer’s access to source code from home with MFA.
Goal

A decision engine is created by refining access control policies.

- Intentions lead to enhancing security without compromising usability.

Access Control Policies

- Workers can access from office only.
- Developers can access from anywhere.

Underlying intentions

- **Prefer to deny:** Sensitive data access from insecure system.
- **Prefer to allow:** Completion of development tasks.

Our Decision Engine

- **Deny**
  - Developer’s access to source code from home with passwd.
- **Allow**
  - Developer’s access to source code from home with MFA.

Business need > Security risk

✔ Business need > Security risk

✓ Intentions lead to enhancing security without compromising usability.
Methodology

A knowledge-informed ML which learns decision examples that follow initial policies.

✓ The feature vector is created by extra knowledge “Qualitative Intention.”
Methodology

A “Qualitative Intentions” is a preference to grant access from an aspect.

Access that is preferable to grant in all aspect is, overall, more valuable to grant.

✓ Access that is preferable to grant in all aspect is, overall, more valuable to grant.


1) Resources of the user: 1.0,
2) Project resources: 0.5,
3) Departmental resources: 0.0, ...

\[ (Ownership, Position, \ldots) = (0.5, -0.333, \ldots) \]

\[ v = 0.95 \]

Grant!
Methodology

In the paper, we present a two-stages computational model. The two stages correspond to the transformation and the value estimation model, respectively.
Methodology

Three applications to create ABAC decision engines from...
✓ (a) ACL/logs, (b) ABAC policy, (c) plus Q&A with policy managers.
Methodology

Three applications to create ABAC decision engines from...
✓ (a) ACL/access logs, (b) ABAC policy, (c) plus Q&A.
Evaluation Method

We have evaluated the **AUC** using access log dataset for the application for access logs. We used synthetic ABAC policies to evaluate other applications.

<table>
<thead>
<tr>
<th>Data set / Rule set</th>
<th>Compared algorithms</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training samples in access logs</td>
<td>Rule extractions</td>
<td><strong>AUC</strong> with the test samples</td>
</tr>
<tr>
<td>Partial rules of an ABAC policy</td>
<td>Machine learnings</td>
<td></td>
</tr>
<tr>
<td>(a)</td>
<td>Our models</td>
<td><strong>AUC</strong> with the ABAC policy</td>
</tr>
<tr>
<td>(b)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(c)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Evaluation Results

Two applications: Logs to decision engine and ABAC policy to decision engine.

➢ Our methods (especially DNN-based one) outperformed existing methods.
Evaluation Results

Application of ABAC policies to a decision engine with additional examples.

➢ Our methods performed the best with the least examples.

(c) ABAC policies to ABAC decision engine with additional decision examples (simulated Q&A).
Conclusion

◆ Proposal
A framework to refine access control policies (ACL policy, access logs, and ABAC policies) to an improved ABAC decision engine.

◆ Challenge
Appropriate decisions in business tasks and situations not envisioned.

◆ Solution
“Qualitative Intentions” to guide better access decisions defined as a minimal knowledge.

◆ Evaluation
The best performance in real access logs and synthetic sample policies.
Qualitative intentions for University sample policy

1. \{User.ID == Resource.StudentID\} > \{User.ID != Resource.StudentID\}
2. \{User.course.taken ∈ Resource.course\} > \{User.course.taken ∈ Resource.course\}
3. \{User.course.taught ∈ Resource.course\} > \{User.course.taught ∈ Resource.course\}
4. \{User.department == Resource.department\} > \{User.department != Resource.department\}
5. \{User.ischair == True\} > \{User.ischair == False\}