Attribute-Based Access Control

Hamed Arshad

Department of Informatics
University of Oslo
hamedar@ifi.uio.no

May 2019
Table of Contents

1. Introduction
2. The Limitations of the Role-Based Access Control (RBAC)
3. Attribute-Based Access Control (ABAC)
4. Example
Table of Contents

1 Introduction

2 The Limitations of the Role-Based Access Control (RBAC)

3 Attribute-Based Access Control (ABAC)

4 Example
Introduction

- **Access control**: restricting access for computer resources, especially in multi-user and data sharing settings
Access control: restricting access for computer resources, especially in multi-user and data sharing settings

Authentication vs Access control
Introduction

- **Access control**: restricting access for computer resources, especially in multi-user and data sharing settings

Authentication vs Access control
Access control: restricting access for computer resources, especially in multi-user and data sharing settings

Authentication vs Access control

Authentication: Who goes there?
- Restrictions on who (or what) can access the system
Introduction

- **Access control**: restricting access for computer resources, especially in multi-user and data sharing settings

  *Authentication vs Access control*

- **Authentication**: Who goes there?
  - Restrictions on who (or what) can access the system

- **Access control**: Are you allowed to do that?
  - Restrictions on actions of authenticated users
1 Introduction

2 The Limitations of the Role-Based Access Control (RBAC)

3 Attribute-Based Access Control (ABAC)

4 Example
The Limitations of the Role-Based Access Control

- ABAC: a successor of Role-Based access control (RBAC)

- ABAC: a successor of Role-Based access control (RBAC)
The Limitations of the Role-Based Access Control

- ABAC: a successor of Role-Based access control (RBAC)
- RBAC: coarse-grained, predefined, and static AC configurations
The Limitations of the Role-Based Access Control

- ABAC: a successor of Role-Based access control (RBAC)
- RBAC: coarse-grained, predefined, and static AC configurations
  - Does not consider the context
The Limitations of the Role-Based Access Control

- ABAC: a successor of Role-Based access control (RBAC)
- RBAC: coarse-grained, predefined, and static AC configurations
  - Does not consider the context
  - Does not capture the purpose of an access
The Limitations of the Role-Based Access Control

- ABAC: a successor of Role-Based access control (RBAC)
- RBAC: coarse-grained, predefined, and static AC configurations
  - Does not consider the context
  - Does not capture the purpose of an access
  - Role Explosion
The Limitations of the Role-Based Access Control

- ABAC: a successor of Role-Based access control (RBAC)
- RBAC: coarse-grained, predefined, and static AC configurations
  - Does not consider the context
  - Does not capture the purpose of an access
  - Role Explosion
  - Toxic Combinations
ABAC: a successor of Role-Based access control (RBAC)

RBAC: coarse-grained, predefined, and static AC configurations

- Does not consider the context
- Does not capture the purpose of an access
- Role Explosion
- Toxic Combinations
- Management Nightmares
The Limitations of the Role-Based Access Control

- ABAC: a successor of Role-Based access control (RBAC)
- RBAC: coarse-grained, predefined, and static AC configurations
  - Does not consider the context
  - Does not capture the purpose of an access
  - Role Explosion
  - Toxic Combinations
  - Management Nightmares
In most of mortgage application systems, there are two types of access: create [a mortgage] and approve.
Example

- In most of mortgage application systems, there are two types of access: create [a mortgage] and approve.
- First, a customer-facing employee should create a mortgage for a customer.
The Limitations of the Role-Based Access Control

Example

- In most of mortgage application systems, there are two types of access: create [a mortgage] and approve.
- First, a customer-facing employee should create a mortgage for a customer.
- Then, the mortgage application needs to be approved by a different employee.

Hamed Arshad (UiO)
ABAC
May 2019
Example

- In most of mortgage application systems, there are two types of access: create [a mortgage] and approve.
- First, a customer-facing employee should create a mortgage for a customer.
- Then, the mortgage application needs to be approved a different employee.
- They need to check that it is suitable and does not breach their policies. For instance, they cannot give a 3million NOK mortgage to a customer with the annual salary 20k NOK.
Example

- In most of mortgage application systems, there are two types of access: create [a mortgage] and approve.
- First, a customer-facing employee should create a mortgage for a customer.
- Then, the mortgage application needs to be approved a different employee.
- They need to check that it is suitable and does not breach their policies. For instance, they cannot give a 3million NOK mortgage to a customer with the annual salary 20k NOK.
- After approving the application, they can “release” the mortgage.
The Limitations of the Role-Based Access Control

Example

- In most of mortgage application systems, there are two types of access: create [a mortgage] and approve.
- First, a customer-facing employee should create a mortgage for a customer.
- Then, the mortgage application needs to be approved by a different employee.
- They need to check that it is suitable and does not breach their policies. For instance, they cannot give a 3 million NOK mortgage to a customer with the annual salary 20k NOK.
- After approving the application, they can “release” the mortgage.
- This process aims to prevent any frauds.
In most of mortgage application systems, there are two types of access: create [a mortgage] and approve.

First, a customer-facing employee should create a mortgage for a customer.

Then, the mortgage application needs to be approved by a different employee.

They need to check that it is suitable and does not breach their policies. For instance, they cannot give a 3million NOK mortgage to a customer with the annual salary 20k NOK.

After approving the application, they can “release” the mortgage.

This process aims to prevent any frauds.

However, a problem may occur when someone has two roles allowing her to create and approve.
1. Introduction

2. The Limitations of the Role-Based Access Control (RBAC)

3. Attribute-Based Access Control (ABAC)

4. Example
ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach

- ABAC: a different approach
Attribute-Based Access Control (ABAC)

- ABAC: a different approach
  - making decisions without previous knowledge

Receiving a request, it makes a decision based on the attributes of the requester and object, environment conditions, and a set of policies.

Creating and managing policies without direct reference to potentially numerous users and objects.

Users do not need to be registered in the system in advance.
ABAC: a different approach

- making decisions without previous knowledge
  - knowledge of the object by the subject
  - or knowledge of the subject by the object-owner

Provides dynamic and context-aware access control

Creating and managing policies without direct reference to potentially numerous users and objects

Users do not need to be registered in the system in advance
Attribute-Based Access Control (ABAC)

- ABAC: a different approach
  - making decisions without previous knowledge
    - knowledge of the object by the subject
    - or knowledge of the subject by the object-owner
  - Provides dynamic and context-aware access control
Attribute-Based Access Control (ABAC)

- ABAC: a different approach
  - making decisions without previous knowledge
    - knowledge of the object by the subject
    - or knowledge of the subject by the object-owner

- Provides dynamic and context-aware access control

- Assigning the capabilities (operation/object pairs) to the subjects (roles/groups) before the request
ABAC: a different approach
- making decisions without previous knowledge
  - knowledge of the object by the subject
  - or knowledge of the subject by the object-owner

Provides dynamic and context-aware access control

Assigning the capabilities (operation/object-pairs) to the subjects (roles/groups) before the request

Receiving a request, it makes a decision
Attribute-Based Access Control (ABAC)

- ABAC: a different approach
  - making decisions without previous knowledge
    - knowledge of the object by the subject
    - or knowledge of the subject by the object-owner
- Provides dynamic and context-aware access control
- Assigning the capabilities (operation/object pairs) to the subjects (roles/groups) before the request
- Receiving a request, it makes a decision
  - based on the attributes of the requester and object, environment conditions, and a set of policies
Attribute-Based Access Control (ABAC)

- ABAC: a different approach
  - making decisions without previous knowledge
    - knowledge of the object by the subject
    - or knowledge of the subject by the object-owner
- Provides dynamic and context-aware access control
- Assigning the capabilities (operation/object pairs) to the subjects (roles/groups) before the request
- Receiving a request, it makes a decision
  - based on the attributes of the requester and object, environment conditions, and a set of policies
- Creating and managing policies without direct reference to potentially numerous users and objects
Attribute-Based Access Control (ABAC)

- ABAC: a different approach
  - making decisions without previous knowledge
  - knowledge of the object by the subject
  - or knowledge of the subject by the object-owner

- Provides dynamic and context-aware access control

- Assigning the capabilities (operation/object pairs) to the subjects (roles/groups) before the request

- Receiving a request, it makes a decision
  - based on the attributes of the requester and object, environment conditions, and a set of policies

- Creating and managing policies without direct reference to potentially numerous users and objects

- Users do not need to be registered in the system in advance
Attribute-Based Access Control (ABAC)
Attribute-Based Access Control (ABAC)

- Extensible access control markup language (XACML)
Attribute-Based Access Control (ABAC)

- Extensible access control markup language (XACML)
- An AC framework consistent with ABAC
Extensible access control markup language (XACML)

An AC framework consistent with ABAC

A policy language, which is sufficiently fine-grained and declarative
  employs elements such as rules, policies, rule- and policy-combining algorithms, attributes (subject, object, action and environment conditions), and obligations
Extensible access control markup language (XACML)

An AC framework consistent with ABAC

A policy language, which is sufficiently fine-grained and declarative
- employs elements such as rules, policies, rule- and policy-combining algorithms, attributes (subject, object, action and environment conditions), and obligations

An architecture for ABAC
- includes PDP, PEP, PAP, and PIP
The access request is submitted to the Policy Enforcement Point (PEP). The PEP needs to determine the access control decision and enforce it.
The request may be submitted by the user in its native format that differs from the XACML canonical form. The context handler is responsible for translating these requests into the canonical form and also converting the response back to the user’s native format.
XACML reference architecture

The attribute values are stored in Policy Information Point (PIP).
The policies are created and stored by the Policy Administration Point (PAP).
The request, converted by the context handler, is forwarded to the Policy Decision Point (PDP). The PDP looks at the request and retrieves the applicable policies, evaluates the policies, and returns the decision to the PEP.
XACML policy structure

PolicySet

Target
PolicySet applies if ...

Policy

PolicySet
XACML policy structure

**PolicySet**
- **Target**
  - PolicySet applies if ...
- **PolicySet**

**Policy**
- **Target**
  - Policy applies if ...
- **Rule**
XACML policy structure

**PolicySet**
- **Target**
  - PolicySet applies if...

**Policy**
- **Target**
  - Policy applies if...

**Rule**
- **Target**
  - Rule applies if...
- **Conditions**
  - Rule is satisfied if...
- **Effect**
  - If satisfied, permit/deny
Table of Contents

1 Introduction

2 The Limitations of the Role-Based Access Control (RBAC)

3 Attribute-Based Access Control (ABAC)

4 Example
Any user with an e-mail address in the “ifi.uio.no” namespace is allowed to perform any action on any resource within working hours (9-17). Otherwise, if the requester is a researcher or a doctor and if the request is read or the resource is medical records, then the access permission should be granted.
Any user with an e-mail address in the "ifi.uio.no" namespace is allowed to perform any action on any resource within working hours (9-17). Otherwise, if the requester is a researcher or a doctor and if the request is read or the resource is medical records, then the access permission should be granted.

( email= xxx@ifi.uio.no ∧ (09:00:00 ≤ current-time ≤ 17:00:00 ))
Any user with an e-mail address in the “ifi.uio.no” namespace is allowed to perform any action on any resource within working hours (9-17). Otherwise, if the requester is a researcher or a doctor and if the request is read or the resource is medical records, then the access permission should be granted.

- \((\text{email} = \text{xxx@ifi.uio.no} \land (09:00:00 \leq \text{current-time} \leq 17:00:00))\)
- \(((\text{subject-position} = \text{Doctor} \lor \text{subject-position} = \text{Researcher}) \land (\text{resource-name} = \text{medical records} \lor \text{action-type}=\text{read})))\)
Any user with an e-mail address in the “ifi.uio.no” namespace is allowed to perform any action on any resource within working hours (9-17). Otherwise, if the requester is a researcher or a doctor and if the request is read or the resource is medical records, then the access permission should be granted.

\[
( \text{email} = \text{xxx@ifi.uio.no} \land (09:00:00 \leq \text{current-time} \leq 17:00:00 ))
\]

\[
(( \text{subject-position} = \text{Doctor} \lor \text{subject-position} = \text{Researcher}) \land
(\text{resource-name} = \text{medical records} \lor \text{action-type}=\text{read} ))
\]

**Policy:**

\[
((( \text{subject-position} = \text{Doctor} \lor \text{subject-position} = \text{Researcher}) \land
(\text{resource-name} = \text{medical records} \lor \text{action-type}=\text{read} )) \lor (\text{email} = \text{xxx@ifi.uio.no} \land (09:00:00 \leq \text{current-time} \leq 17:00:00 )))
\]
<Rule RuleId="Email-Rule" Effect="Permit">
  - <Target>
    - <AnyOf>
      - <AllOf>
        - <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:rfc822Name-match">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">if. uio.no</AttributeValue>
            <AttributeDesignator MustBePresent="false" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" DataType="urn:oasis:names:tc:xacml:1.0:datatype:rfc822Name"/>
        </Match>
    </AllOf>
  </AnyOf>
</Target>
  - <Condition>
    - <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
      - <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than-or-equal">
        - <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-one-and-only">
        </Apply>
      </Apply>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">09:00:00</AttributeValue>
    </Apply>
    - <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-less-than-or-equal">
      - <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-one-and-only">
      </Apply>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">17:00:00</AttributeValue>
    </Apply>
  </Condition>
</Rule>
<Rule RuleId="urn:oasis:names:tc:xacml:3.0:example:MyRule" Effect="Permit">
  <Target>
    <AnyOf>
      <AllOf>
        <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">medical records</AttributeValue>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
  <Condition>
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-one-member-of">
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Doctor</AttributeValue>
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Researcher</AttributeValue>
      </Apply>
    </Apply>
    <AttributeDesignator MustBePresent="false" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:subject" AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" DataType="http://www.w3.org/2001/XMLSchema#string"/>
  </Condition>
</Rule>
Thank you!