Semantic Attribute-Based Access Control
An overview of the existing approaches

Hamed Arshad
Department of Informatics
University of Oslo

March 2018
Table of Contents

1. Introduction
2. Attribute-Based Access Control (ABAC)
3. Semantic-Based Access Control (SBAC)
4. Semantic Attribute-Based Access Control (SABAC)
1 Introduction

2 Attribute-Based Access Control (ABAC)

3 Semantic-Based Access Control (SBAC)

4 Semantic Attribute-Based Access Control (SABAC)
Introduction

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

Access control enforced by
**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

Access control enforced by
- Access Control Lists
- Capabilities
- ...
Attribute-Based Access Control (ABAC)

- ABAC a successor of RBAC
Attribute-Based Access Control (ABAC)

• ABAC a successor of RBAC
  • control based on the entities attributes
ABAC a successor of RBAC
- control based on the entities attributes
A set of attributes in ABAC
Attribute-Based Access Control (ABAC)

- ABAC a successor of RBAC
  - control based on the entities attributes
- A set of attributes in ABAC
  - the same as a role in RBAC
ABAC is a successor of RBAC. It is a control based on the entities attributes.

A set of attributes in ABAC is the same as a role in RBAC.

The XACML standard is a policy language, which is sufficiently fine-grained and declarative as well as an architecture for ABAC.
Attribute-Based Access Control (ABAC)

- ABAC a successor of RBAC
  - control based on the entities attributes
- A set of attributes in ABAC
  - the same as a role in RBAC
- The XACML standard
  - a policy language, which is sufficiently fine-grained and declarative
ABAC a successor of RBAC
- control based on the entities attributes

A set of attributes in ABAC
- the same as a role in RBAC

The XACML standard
- a policy language, which is sufficiently fine-grained and declarative
- as well as an architecture for ABAC
Attribute-Based Access Control (ABAC)

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.
Attribute-Based Access Control (ABAC)

The attribute values are stored in Policy Information Point (PIP).

1. Policy
2. Access request
3. Request
4. Request
5. Attribute queries
6. Attribute queries
7a. Subject attributes
7b. Object attributes
7c. Environment attributes
8. PIP
9. Attribute
10. Response
11. Response
12. Obligations

Access requestor -> PEP -> PDP -> PIP -> Subjects -> Environment
PEP -> Obligations service

Resources
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.
Attribute-Based Access Control (ABAC)

```xml
<?xml version="1.0" encoding="UTF-8"?>
      <Target/>
      <Rule Effect="Permit" RuleId="urn:oasis:names:tc:xacml:3.0:example:MyRule">
        <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 record</AttributeValue>
              </Match>
            </AllOf>
          </AnyOf>
        </Target>
      </Rule>
    </PolicySet>
```
Attribute-Based Access Control (ABAC)

```xml
<PolicySet PolicySetId = "PolicySetInstitute1" policy-combining-algorithm="permit- overrides">  
<Target>  
/**:Attribute-Category :Attribute ID :Attribute Value */
AnyOf :access-subject
  :access-subject :Role :Researcher
  :access-subject :Role :Doctor
AnyOf :resource
  :resource :Type :HealthData
  :resource :Type :AggregateHealthData
AnyOf :action
  :action :Action-id :Release
  :action :Action-id :Read
   :action :Action-id :Write
</Target>
<Policy PolicyId ="Policy1" rule-combining-algorithm="deny-overrides">
// Institute 1 Rules //</Policy>
<Target>
/** :Attribute-Category :Attribute ID :Attribute Value */
:access-subject :Role :Researcher
AnyOf :resource
  :resource :Type :HealthData
  :resource :Type :AggregateHealthData
:action :Action-id :Release
</Target>
<Rule RuleId = "I1R1" Effect="Permit">
<Condition>
Function: string-equal
/** :Attribute-Category :Attribute ID :Attribute Value */
:access-subject :HIPAA Comp :Yes
</Condition>
</Rule>
</PolicySet>
```
ABAC is supposed to be a proper solution in *open and distributed systems*.

Heterogeneous systems = mismatch between attributes

Example: An e-healthcare system may represent adult patients with an attribute "Adult". Patients may try to prove using "hasDriverLicense" or "age". Considering all the possible synonyms (semantically) of each attribute defining several policies or one general policy. A change in the policy a large number of manual work.

ABAC needs to be extended.
ABAC is supposed to be a proper solution in open and distributed systems.

*Heterogeneous* systems = *mismatch* between attributes.

Example:
An e-healthcare system may represent adult patients with an attribute "Adult". Patients may try to prove using "hasDriverLicense" or "age". Considering all the possible synonyms (semantically) of each attribute defining several policies or one general policy. A change in the policy requires a large number of manual work.
Attribute-Based Access Control (ABAC)

- ABAC is supposed to be a proper solution in open and distributed systems.
- *Heterogeneous* systems = *mismatch* between attributes.

**Example**

- An e-healthcare system may represent adult patients with an attribute "Adult".
Attribute-Based Access Control (ABAC)

- ABAC is supposed to be a proper solution in *open and distributed systems*
- *Heterogeneous* systems = *mismatch* between attributes

**Example**

- An e-healthcare system may represent adult patients with an attribute “Adult”
- Patients may try to prove using “hasDriverLicense” or “age”
Attribute-Based Access Control (ABAC)

- ABAC is supposed to be a proper solution in open and distributed systems
- **Heterogeneous** systems = mismatch between attributes

**Example**
- An e-healthcare system may represent adult patients with an attribute “Adult”
- Patients may try to prove using “hasDriverLicense” or “age”
- Considering all the possible synonyms (semantically) of each attribute
Attribute-Based Access Control (ABAC)

- ABAC is supposed to be a proper solution in *open and distributed systems*
- *Heterogeneous* systems = *mismatch* between attributes

**Example**

- An e-healthcare system may represent adult patients with an attribute "**Adult**"
- Patients may try to prove using "**hasDriverLicense**" or "**age**"
- Considering all the possible synonyms (semantically) of each attribute
  - defining several policies or one general policy
Attribute-Based Access Control (ABAC)

- ABAC is supposed to be a proper solution in *open and distributed systems*
- **Heterogeneous** systems = *mismatch* between attributes

**Example**

- An e-healthcare system may represent adult patients with an attribute "**Adult**"
- Patients may try to prove using "**hasDriverLicense**" or "**age**"
- Considering all the possible synonyms (semantically) of each attribute
  - defining several policies or one general policy
- A change in the policy
Attribute-Based Access Control (ABAC)

- ABAC is supposed to be a proper solution in **open and distributed systems**
- **Heterogeneous** systems = **mismatch** between attributes

**Example**

- An e-healthcare system may represent adult patients with an attribute **“Adult”**
- Patients may try to prove using **“hasDriverLicense”** or **“age”**
- Considering all the possible synonyms (semantically) of each attribute
  - defining several policies or one general policy
- A change in the policy
  - a large number of manual work
Attribute-Based Access Control (ABAC)

- ABAC is supposed to be a proper solution in open and distributed systems
- Heterogeneous systems = mismatch between attributes

**Example**

- An e-healthcare system may represent adult patients with an attribute “Adult”
- Patients may try to prove using “hasDriverLicense” or “age”
- Considering all the possible synonyms (semantically) of each attribute
  - defining several policies or one general policy
- A change in the policy
  - a large number of manual work

**ABAC needs to be extended**
Table of Contents

1. Introduction

2. Attribute-Based Access Control (ABAC)

3. Semantic-Based Access Control (SBAC)

4. Semantic Attribute-Based Access Control (SABAC)
Semantic-Based Access Control (SBAC)

The description of the ontology using classes, properties and instances
Idea: ABAC + semantic technologies

Formally define entities and their attributes and relationships using an ontology

Describing relations for specific conditions using rule markup languages
Idea: ABAC + semantic technologies

- making decisions semantically as well as considering the semantic relationships for inferring implicit policies from explicit ones
Semantic Attribute-Based Access Control (SABAC)

- Idea: ABAC + semantic technologies
  - making decisions semantically as well as considering the semantic relationships for inferring implicit policies from explicit ones
- Formally define entities and their attributes and relationships using an ontology
Idea: ABAC + semantic technologies
- making decisions semantically as well as considering the semantic relationships for inferring implicit policies from explicit ones
- Formally define entities and their attributes and relationships using an ontology
- Describing relations for specific conditions using rule markup languages
• Separation of *ontology* management from *access* management
Semantic Attribute-Based Access Control (SABAC)

- Separation of *ontology* management from *access* management
- Two parts:
  - An ontology management system
Semantic Attribute-Based Access Control (SABAC)

- Separation of *ontology* management from *access* management
- Two parts:
  - An ontology management system
    - provides the extended user and resource attributes
Semantic Attribute-Based Access Control (SABAC)

- Separation of **ontology** management from **access** management
- Two parts:
  - An ontology management system
    - provides the extended user and resource attributes
  - An access control system
Semantic Attribute-Based Access Control (SABAC)

- Separation of **ontology** management from **access** management
- Two parts:
  - An ontology management system
    - provides the extended user and resource attributes
  - An access control system
    - uses the extended attributes for access evaluation
What has been done till now?
What has been done till now?

Publications per year

<table>
<thead>
<tr>
<th>Year</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>2</td>
</tr>
<tr>
<td>2005</td>
<td>2</td>
</tr>
<tr>
<td>2006</td>
<td>5</td>
</tr>
<tr>
<td>2007</td>
<td>5</td>
</tr>
<tr>
<td>2008</td>
<td>1</td>
</tr>
<tr>
<td>2009</td>
<td>3</td>
</tr>
<tr>
<td>2010</td>
<td>14</td>
</tr>
<tr>
<td>2011</td>
<td>10</td>
</tr>
<tr>
<td>2012</td>
<td>10</td>
</tr>
<tr>
<td>2013</td>
<td>7</td>
</tr>
<tr>
<td>2014</td>
<td>4</td>
</tr>
<tr>
<td>2015</td>
<td>7</td>
</tr>
<tr>
<td>2016</td>
<td>10</td>
</tr>
<tr>
<td>2017</td>
<td>4</td>
</tr>
</tbody>
</table>
What has been done till now?

- Journal paper: 21
- Conference paper: 59
- Book chapter: 5
What has been done till now?

<table>
<thead>
<tr>
<th>Title</th>
<th>Year</th>
<th>Journal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-level authorisation model and framework for distributed</td>
<td>2010</td>
<td>IET Information Security</td>
</tr>
<tr>
<td>semantic-aware environments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Utilizing Semantic Knowledge for Access Control in Pervasive and</td>
<td>2010</td>
<td>Mobile Networks and Applications</td>
</tr>
<tr>
<td>Ubiquitous Systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ontology based policy interoperability in geo-spatial domain</td>
<td>2011</td>
<td>Computer Standards &amp; Interfaces</td>
</tr>
<tr>
<td>Privilege Management Infrastructure for Virtual Organizations in</td>
<td>2011</td>
<td>IEEE Transactions on Information Technology in</td>
</tr>
<tr>
<td>Healthcare Grids</td>
<td></td>
<td>Biomedicine</td>
</tr>
<tr>
<td>A semantic approach for fine-grain access control of e-health</td>
<td>2012</td>
<td>Logic Journal of IGPL</td>
</tr>
<tr>
<td>documents</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Building and evaluating an ontology-based tool for reasoning about</td>
<td>2013</td>
<td>AMIA Annu Symp Proc</td>
</tr>
<tr>
<td>consent permission</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extensible access control markup language integrated with Semantic</td>
<td>2013</td>
<td>Information Sciences</td>
</tr>
<tr>
<td>Web technologies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A SEMANTIC SECURITY FRAMEWORK FOR SYSTEMS OF SYSTEMS</td>
<td>2013</td>
<td>International Journal of Cooperative Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Systems</td>
</tr>
<tr>
<td>Empowering citizens with access control mechanisms to their personal</td>
<td>2013</td>
<td>International Journal of Medical Informatics</td>
</tr>
<tr>
<td>health resources</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control for Web Services</td>
<td></td>
<td>(IRECOS)</td>
</tr>
<tr>
<td>Sophisticated Access Control via SMT and Logical Frameworks</td>
<td>2014</td>
<td>ACM Transactions on Information and System Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(TISSEC)</td>
</tr>
<tr>
<td>Fine-grained filtering to provide access control for data</td>
<td>2015</td>
<td>Concurrency and Computation: Practice &amp; Experience</td>
</tr>
<tr>
<td>providing services within collaborative environments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A Combination of Semantic and Attribute-based Access Control Model</td>
<td>2015</td>
<td>The ISC International Journal of Information Security</td>
</tr>
<tr>
<td>for Virtual Organizations</td>
<td></td>
<td>(ISeCure)</td>
</tr>
<tr>
<td>A HIGH PERFORMANCE UCON AND SEMANTIC-BASED AUTHORIZATION FRAMEWORK</td>
<td>2016</td>
<td>Journal of Information &amp; Communication Technology</td>
</tr>
<tr>
<td>FOR GRID COMPUTING</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Control as a Service for Information Protection in</td>
<td>2016</td>
<td>Journal of Internet Computing and Services</td>
</tr>
<tr>
<td>Semantic Web based Smart Environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Semantically Enriched Data Access Policies in eHealth</td>
<td>2016</td>
<td>Journal of Medical Systems</td>
</tr>
<tr>
<td>for Cloud Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Semantic Based Authorization Framework For Multi-Domain</td>
<td>2017</td>
<td>Procedia Computer Science</td>
</tr>
<tr>
<td>Collaborative Cloud Environments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Semantic privacy-preserving framework for electronic health record</td>
<td>2017</td>
<td>Telematics and Informatics</td>
</tr>
<tr>
<td>linkage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proactive user-centric secure data scheme using attribute-based</td>
<td>2018</td>
<td>Future Generation Computer Systems</td>
</tr>
<tr>
<td>semantic access controls for mobile clouds in</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Semantic Attribute-Based Access Control (SABAC)

What has been done till now?

<table>
<thead>
<tr>
<th>Title</th>
<th>Year</th>
<th>Conference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extending Policy Languages to the Semantic Web</td>
<td>2004</td>
<td>Web Engineering - 4th International Conference, ICWE 2004</td>
</tr>
<tr>
<td>Supporting Attribute-based Access Control with Ontologies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure Web Services Using Semantic Web Technology</td>
<td>2007</td>
<td></td>
</tr>
<tr>
<td>New paradigms for access control in open environments</td>
<td>2008</td>
<td></td>
</tr>
<tr>
<td>Description Logic and Semantic Web Technology</td>
<td>2009</td>
<td></td>
</tr>
<tr>
<td>Access Control in E-Learning Using Attributes and Ontology</td>
<td>2010</td>
<td></td>
</tr>
<tr>
<td>Provenance Explorer – Customized Provenance Views Using Semantic Inference</td>
<td>2011</td>
<td></td>
</tr>
<tr>
<td>Supporting Attribute-based Access Control in Authentication and Authorization with Ontologies</td>
<td>2012</td>
<td></td>
</tr>
<tr>
<td>Enforcing Privacy by Means of an Ontology Driven XACML Framework</td>
<td>2013</td>
<td></td>
</tr>
<tr>
<td>Building a Distributed Semantic-aware Security Architecture</td>
<td>2014</td>
<td></td>
</tr>
<tr>
<td>A Role-and-Attribute-Based Access Control System Using Semantic Web Technologies</td>
<td>2015</td>
<td></td>
</tr>
<tr>
<td>Semantic-Based Access Control for Grid Data Resources</td>
<td>2016</td>
<td></td>
</tr>
<tr>
<td>Semantic Description Logic and Subject Attribute-Based Grid Authorization Model</td>
<td>2017</td>
<td></td>
</tr>
<tr>
<td>A Semantic-Aware Attribute-Based Access Control Model for Web Services</td>
<td>2018</td>
<td></td>
</tr>
<tr>
<td>Supporting RBAC with XACLML-DLW</td>
<td>2019</td>
<td></td>
</tr>
<tr>
<td>Attribute Mapping for Cross-Domain Access Control</td>
<td>2020</td>
<td></td>
</tr>
<tr>
<td>Enabling Privacy-preserving Credential-based Access Control with XACLML and SAML</td>
<td>2021</td>
<td></td>
</tr>
<tr>
<td>Dynamic context-aware information access in virtual organizations</td>
<td>2022</td>
<td></td>
</tr>
<tr>
<td>Fine-grained access control in Virtual Organizations</td>
<td>2023</td>
<td></td>
</tr>
<tr>
<td>Secure views using semantic access control</td>
<td>2024</td>
<td></td>
</tr>
<tr>
<td>A New Trust Degree-based Access Control Method for Semantic Web Services</td>
<td>2025</td>
<td></td>
</tr>
<tr>
<td>A Semantic-and-Attribute-Based Framework for Web Services Access Control</td>
<td>2026</td>
<td></td>
</tr>
<tr>
<td>Semantic Security Architecture for Web Services: The Access-Gov Solution</td>
<td>2027</td>
<td></td>
</tr>
<tr>
<td>Extending XACLML Profile for RBAC with Sematic Concepts</td>
<td>2028</td>
<td></td>
</tr>
<tr>
<td>Concept Alignment in Attribute Based Access Control</td>
<td>2029</td>
<td></td>
</tr>
<tr>
<td>Towards Semantic Matching of Attributes in Multi-Domain Access Control</td>
<td>2030</td>
<td></td>
</tr>
<tr>
<td>Ontology-based Access Control Interoperability</td>
<td>2031</td>
<td></td>
</tr>
<tr>
<td>An Access-aware Security Attribute-based Access Control Model for Mobile Web Services</td>
<td>2032</td>
<td></td>
</tr>
<tr>
<td>APHR: An Authorised Personal Health Record for Enabling Pervasive Healthcare</td>
<td>2033</td>
<td></td>
</tr>
<tr>
<td>Ontology-based Interoperation for Securely Shared Services: Security Concept Matching for Authorization Policy Interoperability</td>
<td>2034</td>
<td></td>
</tr>
<tr>
<td>Ontology-based Interoperability for Securely Shared Services</td>
<td>2035</td>
<td></td>
</tr>
<tr>
<td>Ontology-based Matching of Security Attributes for Personal Data Access in e-Health</td>
<td>2036</td>
<td></td>
</tr>
<tr>
<td>Realisation Distributed Access Control Based on Ontology and Attribute with OWL</td>
<td>2037</td>
<td></td>
</tr>
<tr>
<td>Fact semantic Attribute Role-based Access Control (ARRAC) in a collaborative environment</td>
<td>2038</td>
<td></td>
</tr>
<tr>
<td>Semantic access control for cloud computing based on e-Healthcare</td>
<td>2039</td>
<td></td>
</tr>
<tr>
<td>XSTMella: A generalized extension of XACLML for context-aware spatio-temporal RBAC model with OWL</td>
<td>2040</td>
<td></td>
</tr>
<tr>
<td>Fine-Grained Data Provisioning Web Services with XACLML</td>
<td>2041</td>
<td></td>
</tr>
<tr>
<td>Ontological Approach for the Management of Informed Consent Permissions</td>
<td>2042</td>
<td></td>
</tr>
<tr>
<td>F-SAML: Reibly identifying Attributes and Their Identity Providers in a Federation</td>
<td>2043</td>
<td></td>
</tr>
<tr>
<td>An Attributes-Based Access Control Architecture with a Large-Scale Device Collaboration Systems Using XACLML</td>
<td>2044</td>
<td></td>
</tr>
<tr>
<td>Towards Semantic-Enhanced Attribute-Based Access Control for Cloud Services</td>
<td>2045</td>
<td></td>
</tr>
<tr>
<td>Web Service Semantic Access Control</td>
<td>2046</td>
<td></td>
</tr>
<tr>
<td>A Semantic Policy Framework for Context-aware Access Control</td>
<td>2047</td>
<td></td>
</tr>
<tr>
<td>A virtual PHR authorization system</td>
<td>2048</td>
<td></td>
</tr>
<tr>
<td>Standardized access control mechanisms for protecting ISO 13608-based electronic health record systems</td>
<td>2049</td>
<td></td>
</tr>
<tr>
<td>Attribute-based Fine Grained Access Control for Triple Stories</td>
<td>2050</td>
<td></td>
</tr>
<tr>
<td>An OWL-based XACLML Policy Framework</td>
<td>2051</td>
<td></td>
</tr>
<tr>
<td>Extensible privacy framework for objects based ubiquitous services</td>
<td>2052</td>
<td></td>
</tr>
<tr>
<td>Semantic Generation of Clouds Privacy Policies</td>
<td>2053</td>
<td></td>
</tr>
<tr>
<td>Ontology-Based Delegation of Access Control to the XACLML Delegation Profile</td>
<td>2054</td>
<td></td>
</tr>
<tr>
<td>Expandable policy framework for web of objects based ubiquitous services</td>
<td>2055</td>
<td></td>
</tr>
<tr>
<td>Semantic Generation of Clouds Privacy Policies</td>
<td>2056</td>
<td></td>
</tr>
<tr>
<td>An Access Control over Semantics-enabled Smart Grids to enable energy-efficiency and lifetime optimization</td>
<td>2057</td>
<td></td>
</tr>
<tr>
<td>An Ontology Ruling Privacy Oriented Access Control</td>
<td>2058</td>
<td></td>
</tr>
<tr>
<td>Representing Attribute-based Access Control Policies in OWL</td>
<td>2059</td>
<td></td>
</tr>
<tr>
<td>Context-Sensitive Policy Based Security in Internet of Things</td>
<td>2060</td>
<td></td>
</tr>
<tr>
<td>Semantic-Based Privacy Protection of Electronic Health Records for Collaborative Research</td>
<td>2061</td>
<td></td>
</tr>
<tr>
<td>Graphical interface for Ontology-driven Access Control</td>
<td>2062</td>
<td></td>
</tr>
<tr>
<td>Hamed Arshad (UiO) SABAC March 2018</td>
<td>18 / 25</td>
<td></td>
</tr>
</tbody>
</table>
What has been done till now?

| Title                                                      | Year | Book                                                                            |
|------------------------------------------------------------|------|                                                                                 |
| Semantic Similarity-Based Web Services Access Control      | 2011 | Autonomous Systems: Developments and Trends                                      |
The existing approaches can be categorized as:

- Hybrid models: ABAC + SBAC
- New policy languages
- Extending the XACML architecture
The existing approaches can be categorized as:

- **Hybrid models: ABAC + SBAC**
The existing approaches can be categorized as:

- **Hybrid models: ABAC + SBAC**

- **New policy languages**
Semantic Attribute-Based Access Control (SABAC)

The existing approaches can be categorized as:

- **Hybrid models: ABAC + SBAC**

- **New policy languages**

- **Extending the XACML architecture**
  - Priebe et al. “Supporting attribute-based access control with ontologies”. In ARES 2006. IEEE.
Hybrid models: ABAC + SBAC
- **Hybrid models**: ABAC + SBAC
  - A two-stage process:
**Hybrid models: ABAC + SBAC**

- A two-stage process:
  - First stage: ABAC for access control inside organizations
Hybrid models: ABAC + SBAC

- A two-stage process:
- First stage: ABAC for access control inside organizations
  - XACML policies

- Second stage: a global SBAC server
  - OWL ontology for entities and SWRL rules for access policies
**Hybrid models: ABAC + SBAC**

- A two-stage process:
- First stage: ABAC for access control inside organizations
  - XACML policies
- Second stage: a global SBAC server
Hybrid models: ABAC + SBAC

- A two-stage process:
  - First stage: ABAC for access control inside organizations
    - XACML policies
  - Second stage: a global SBAC server
    - OWL ontology for entities and SWRL rules for access policies
**Hybrid models: ABAC + SBAC**

- A two-stage process:
  - First stage: ABAC for access control inside organizations
    - XACML policies
  - Second stage: a global SBAC server
    - OWL ontology for entities and SWRL rules for access policies
    - The ontology has two basic concepts (Subject and Object) and two basic relations (Permission and Prohibition)
**Hybrid models: ABAC + SBAC**

- A two-stage process:
  - First stage: ABAC for access control inside organizations
    - XACML policies
  - Second stage: a global SBAC server
    - OWL ontology for entities and SWRL rules for access policies
    - The ontology has two basic concepts (Subject and Object) and two basic relations (Permission and Prohibition)
Semantic Attribute-Based Access Control (SABAC)

Policy Enforcement Point (PEP)

Policy Decision Point (PDP)

ABAC Policy Rules (XACML)

Policy Decision Point (PDP)

Policy Inference Engine

Knowledge Base

Ontology (OWL)

SBAC Policy Rules (SWRL)
New policy languages
New policy languages

$MA(DL)^2$ logic for policy specification and inference
New policy languages

- MA(DL)$^2$ logic for policy specification and inference
Semantic Attribute-Based Access Control (SABAC)

- Extending the XACML architecture
Extending the XACML architecture

Adding a component to the architecture
Semantic Attribute-Based Access Control (SABAC)

- **Extending the XACML architecture**
  - Adding a component to the architecture

![Diagram of the SABAC architecture](chart.png)
Thank you!