I. J. Computer Network and Information Security, **2017, 2, 12-21**
Published Online February 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.02.02

Application of Attribute Based Access Control Model for Industrial Control Systems

Erkan Yalcinkaya
Department of Production Engineering, Royal Institute of Technology, Stockholm, Sweden
E-mail: erkany@kth.se

Antonio Maffei and Mauro Onori
Department of Production Engineering, Royal Institute of Technology, Stockholm, Sweden
E-mail: {maffei, onori}@kth.se

Abstract—The number of reported security vulnerabilities and incidents related to the industrial control systems (ICS) has increased recent years. As argued by several researchers, authorization issues and poor access control are key incident vectors. The majority of ICS are not designed security in mind and they usually lack strong and granular access control mechanisms. The attribute based access control (ABAC) model offers high authorization granularity, central administration of access policies with centrally consolidated and monitored logging properties. This research proposes to harness the ABAC model to address the present and future ICS access control challenges. The proposed solution is also implemented and rigorously tested to demonstrate the feasibility and viability of ABAC model for ICS.

Index Terms—Attribute based access control (ABAC), industrial control systems (ICS), fine grained authorization, central policy enforcement.

I. Introduction

Industrial control systems (ICS) are designed to automate and control a wide range of industrial processes such as manufacturing, water supply, power generation, transportation and so forth.

ICS can be in different forms for instance programmable logic controllers (PLC), supervisory control and data acquisition systems (SCADA) and distributed control systems (DCS). Many of these controlling units were initially designed for fairly specific tasks which were assumed to be performed in isolated environments like factory production lines. However, since the industry 4.0 revolution, ICS have become more versatile to perform diverse tasks. Moreover, due to the rapid increase in computational power, ICS has evolved into programmable interconnected computers rather than individual units.

The era of interconnection has brought ICS to the forefront of cyber security. Therefore, the reported number of incidents related to ICS has increased in the last five years. Fig. 1 shows the number of “ICS related vulnerability reports — tickets” reported between the year 2010 and 2013 [1][2].

According to the research published by the U.S. Department of Homeland Security [3], poor access control and misconfigured authorization schemas were the second and the third highest percentage of ICS vulnerabilities identified between 2009 and 2010.

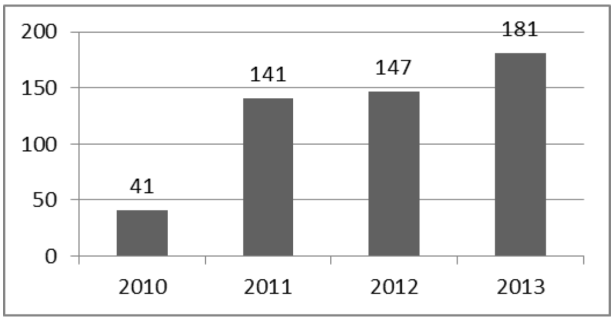


Fig.1. - ICS Related Vulnerability Reports - Tickets between the Year 2010 and 2013

Likewise, the report published by ICS-CERT [4] highlights the unauthorized access issues with interconnected ICS/SCADA devices. The same report also identifies “Abuse of access authority” and “Weak authentication” as the key incident vectors of the year 2014.

As GE Measurement & Control Solutions [5] and National American Reliability Council [6] state, authorization, authentication and access control vulnerabilities are the most common vulnerabilities identified in the ICS domain.

As stated above, many ICS related security risks are due to the insufficient, misconfigured or vulnerable access control mechanisms. Therefore, in order to address those weaknesses, this research proposes to harness the attribute based access control (ABAC) model for ICS.

II. Access Control Mechanism

In the context of information security, access control mechanisms ensure that subjects are allowed to perform only authorized operations on objects in question. In other words, access control mechanisms enforce confidentiality [7, p. 2], integrity [7, p. 3] and indirectly availability [7, p. 4] of a given protected object.

The access control paradigm describes the objects as resources (for instance hardware, sensor, robot, database table etc.) and subjects as entities initiating the access request. The same paradigm also describes [9] number of security services namely authentication (confirmation of subject's identity [7, p. 171]), authorization (granted set of permissions to perform certain type of actions) and auditing (accountability by monitoring subject's activities [7, p. 423]) to achieve the desired access protection.

III. Traditional Access Control Models

The most prominent traditional access control models are Mandatory Access Control (MAC) Model, Discretionary Access Control (DAC) Model and Role-Based Access Control (RBAC) Model. The following three subsections briefly elaborate these models.

A. MAC Model

The MAC (a.k.a. Rule based) model compares the subject's clearance with the object's classification level. The access decision is given by the operating system which is considered as a black box and cannot be influenced by the end users [6, p. 53]. Military IT systems often rely on MAC.

B. DAC Model

In contrast to the MAC, the DAC (a.k.a. Identity-based) model allows the object owners to set/control the access rules (via access control lists) [6, p. 53].

C. RBAC Model

The RBAC (a.k.a. nondiscretionary access control) model defines access groups which are set of privileges to perform a particular type of operation(s) [9]. The access groups are assigned to subjects and often determined by classification of job functions or responsibilities within the enterprise.

IV. Attribute Based Access Control Model

The traditional access control models described in the previous sections focus only on subject's identity. Thus, the possible combinations of access conditions are quite limited.

The DAC model offers only basic level of security which can potentially be circumvented [10]. For instance, assume a subject who is granted read only access to a particular file. Even though the subject is prohibited any other operation then reading, he/she can copy the file content to another file which he/she might have full access to perform any operation [11].

The MAC model is pretty rigid and difficult to administrate [10]. Therefore it is impractical to utilize in contemporary transaction intense distributed IT systems.

The RBAC model well suits for small size systems, however, due to the cross referencing issue, the required number of roles for large enterprises may potentially exceed manageable levels [11].

These shortcomings of the traditional access control models are addressed by the attribute based access control (ABAC) model.

The ABAC model in a nutshell is based on five fundamental cornerstones (Fig. 2). These are subject-object attributes, environment conditions, centrally administrated access policy and desired operation.

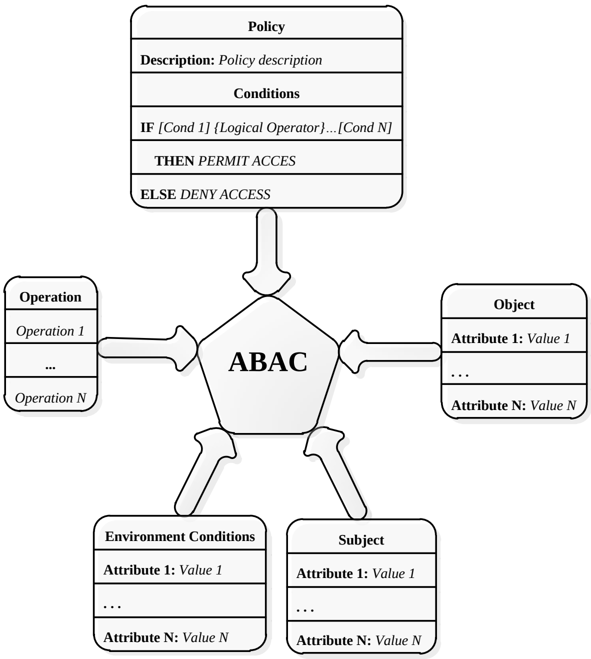


Fig.2. Five Cornerstones of ABAC: Policy, Subject, Object, Operation Type and Environment Conditions

As visualized in Fig. 2, the access request is permitted or denied if all the policy conditions are met. The access policy validates the combinations of subject, object, and environment attribute values as well as the operation type. Therefore, the number of possible variations of distinct access conditions (i.e. access granularity) is significantly larger than the traditional access control models.

The versatility of ABAC model boils into its simplicity and flexibility to support fine-grained authorizations enforced by centrally administered access control policies. Therefore, the access control is logically decoupled from the business logic. Thus, both introducing a new policy and updating an existing one can easily be performed from the central policy repository without affecting the integrated systems.

The ABAC model is also capable of interpreting different threat levels as environment or subject attributes [12]. If the risk score is above a certain threshold, the access request can automatically be denied. For example, assume an access policy which identifies the risk threshold score as 5. If a subject is authenticated with a single factor from the enterprise network, the risk assessment engine evaluates the risk score as 3, and the access request is granted. However, if the subject is authenticated with a single factor from a remote location, the risk score is evaluated as 7. Thus, the access request is denied. If the same subject is identified with a secondary means of authentication (multifactor authentication), then the risk score is lowered to 4 and the access request is granted.

In addition to all these advantages, the ABAC model is backwards compatible. In other words, it is also flexible and versatile enough to support proprietary systems designed to work with traditional access control models such as MAC, DAC and RBAC [9].

V. NIST Reference ABAC Architecture

There are number of recommended reference architectures addressing the ABAC model in an enterprise environment. However, this research focuses on the reference ABAC architectural framework described in the NIST Special Publication 800-162 [10]. Table 1 highlights the main components of the reference architecture.

Table 1. Architectural Components of NIST Reference ABAC Framework

Component	Description
Subject	An entity requesting access to a protected object entity
Protected Object	A protected resource entity being requested for access
Policy	A rule expressing the relationship between a subject and a protected object
Attribute	Set of properties bound to a particular subject or a protected object
Operation	A type of action that a subject attempts to perform on a protected object
Environment Conditions	A set of properties which are not bound to a subject or a protected object but related to the context such as current date, time, place or risk level
Policy Repository	An enterprise-wide central database of authorization policies
Attribute Repository	An enterprise-wide central database of protected object and subject attributes
Policy Decision Point (PDP)	A central access decision engine which permits or denies the access requests by evaluating the authorization policy along with the attributes of a subject, a protected object and environment conditions
Policy Enforcement Point (PEP)	An interceptor mediating all access requests towards a specific protected object. PEP queries PDP to validate if the subject in question is permitted or denied the access request
Policy Information Point (PIP)	A data service interface towards PDP to fetch environment conditions, subject and protected object attributes
Policy Administration Point (PAP)	An external tool to manage authorization policies

As shown in Fig. 3, a subject requests permission from PEP to perform an operation on a protected object. Upon this, PEP queries PDP for the access decision. PDP then finds the corresponding access policy which may require relevant subject, object and/or environment attribute values (via PIP) to evaluate the final access decision. The outcome of the evaluation is then passed to PEP which ultimately “Denies” or “Permits” the requested operation. Last but not least, audit logs chronologically record all activities among different components of the ABAC system.

VI. ABAC Model for ICS

The majority of the industrial control systems (ICS) are not designed security in mind and they usually depend on perimeter-based security tools like firewalls to split the secure internal factory networks from unsecure internet ecosystems. However, as [13] elaborates; this is a false sense of security. First of all, firewalls designed to block or permit only specific protocols (port numbers) therefore they can merely offer a limited level of security. Moreover, cross referencing firewall rules may easily become over complicated. According to [13], 80% of the enterprise firewall installations are vulnerable due to misconfigured complex rules. The same research also indicates that the firewalls do not provide protection against insider threats originated by trusted partners, former or existing employees.

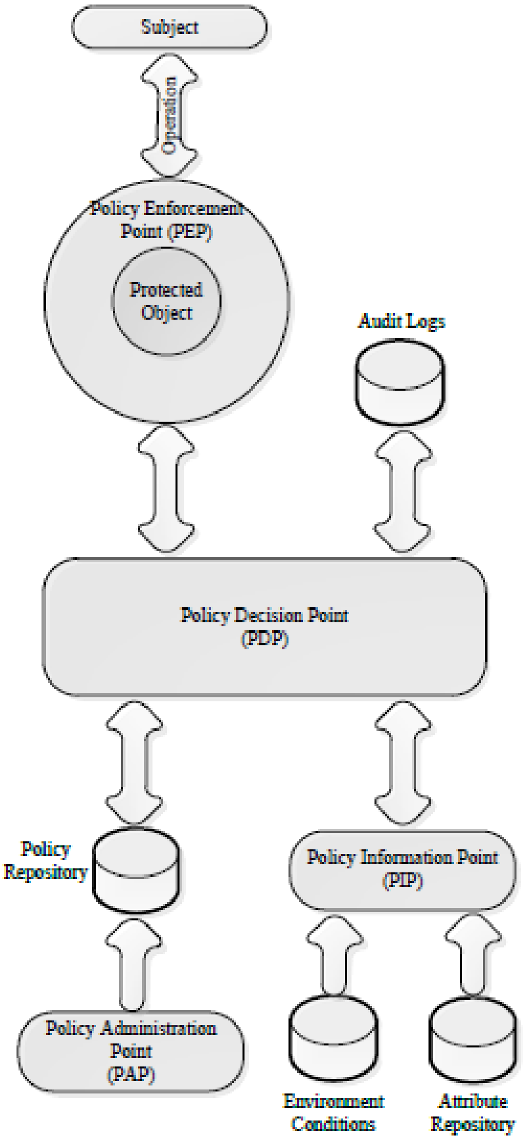

Subject
Operation
Policy Enforcement Point (PEP)
Protected Object
Audit Logs
Policy Decision Point (PDP)
Policy Repository
Policy Information Point (PIP)
Policy Administration Point (PAP)
Environment Conditions
Attribute Repository

Fig.3. ABAC Reference Architecture

One way of addressing the insider threats is employing enterprise wide strict access control mechanisms. Thus, some researchers proposed ICS to harness RBAC model [14][15]. Although it is a step forward, due to flexibility and scalability issues as well as difficulties to implement fine-grained authorization rules and complexity in role administration (especially considering the complex system to system, human to system, and human to human interactions) for cross-referencing roles, the RBAC model is not the optimal access control solution for ICS.

The audit trail, records of all activities of a particular object during a given time interval, is another vital ICS security feature highlighted by NIST [16]. A comprehensive audit trail ensures accountability and is considered as one of the most important assets for performing forensics investigations. Thus, enterprise-wide audit records have to be centrally administered and secured. However, log consolidation is not straight forward for ICS, as they are scattered around the factory floor or even geographically remote locations.

Compliance and adherence to international standards, laws and company policies are imperative. When it comes to the ICS domain, ISA99 [17] and NIST Publication 800-82 [16] are the two foremost standards both of which have a dedicated chapter for controlling unauthorized access. However, due to the versatility and ubiquity, it has always been extremely challenging to prove and enforce the compliance requirements for the ICS-based ecosystems.

The industry 4.0 revolution has empowered cyber physical systems to highly interact with each other to increase the production efficiency. The improved ICS computational power will eventually allow the cyber physical systems to become more autonomous. As Evolvable production systems (EPS) concept describes [18], the future production systems will eventually be equipped with extraordinary skills like self-organization, self-diagnose and self-healing capabilities.

One of the biggest design challenges of EPS is controlling and restricting the interaction between autonomous systems. Therefore, EPS requires a flexible and highly scalable access control model to reach the ultimate goal of autonomy.

As mentioned in the previous sections, the ABAC model offers fine-grained, highly scalable, interoperable and flexible authorization model that is suitable for different layers of any given enterprise infrastructure. Moreover, regulatory compliance and auditing are streamlined by centrally enforced, managed and monitored policies. Likewise, the central management consolidates the audit logs and reduces the complexity of log management. Therefore, forensics investigations are substantially simplified. Furthermore, the ABAC model is backward compatible with the traditional access control models. In other words, proprietary ICS depending on DAC, MAC or RBAC model can be transparently converted to employ the ABAC model.

In conclusion, considering the features of the ABAC model along with the existing and the future ICS access control challenges, this research propose to utilize the ABAC model for ICS.

VII. ABAC Model for ICS use Case

This section describes a use case to exemplify the proposed concept. The use case embodies authorization of an operator (human actor) to perform certain operations with the help of a PLC controlled robotic arm. Fig. 4 depicts the high-level relationship between the operator and the PLC-controlled robotic arm in the context of ABAC model.

For further clarification, it is worth materializing the use case with a real life scenario. Table 2 lists the attributes of sample subject-object couple along with environment conditions. Likewise, Table 3 defines a sample access policy.

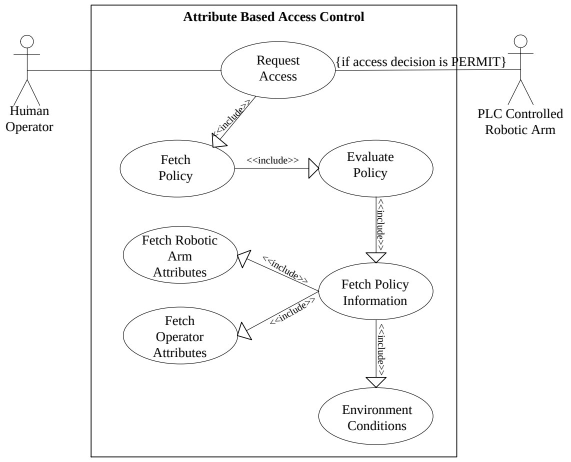


Fig.4. Use Case - A Human Operator and a PLC-Controlled Robotic Arm

Table 2. A Subject, Object and Environment Attribute Examples

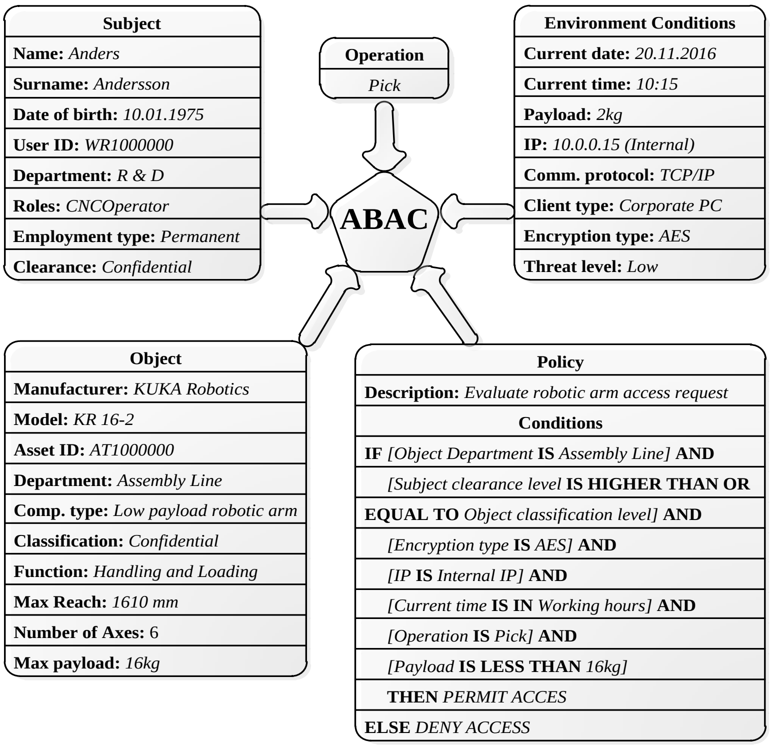
Subject	
Name	Anders
Surname	Andersson
Date of birth	10.01.1975
User ID	WR1000000
Department	R & D
Roles	CNCOperator
Emp. type	Permanent
Clearance	Confidential

Environment Conditions	
Current date	10.10.2015
Current time	10:15
Payload	2kg
IP	10.0.0.15
Comm. protocol	TCP/IP
Client type	Corporate PC
Encryption Type	AES
Threat level	Low

Object	
Manufacturer	KUKA Robotics
Model	KR 16-2
Asset ID	AT1000000
Department	Assembly Line
Comp. type	Low payload robotic arm
Classification	Confidential
Function	Handling and Loading
Max Reach	1610 mm
Number of Axes	6
Max payload	16kg

Table 3. A Policy Example

Policy	
Description	Evaluate robotic arm access request
Conditions	**IF** [Object Department **IS** Assembly Line] **AND** [Subject clearance level **IS HIGHER THAN OR EQUAL TO** Object classification level] **AND** [Encryption type **IS** AES] **AND** [IP **IS** Internal IP] **AND** [Current time **IS IN** Working hours] **AND** [Operation **IS** Pick] **AND** [Payload **IS LESS THAN** 16kg] **THEN** PERMIT ACCES **ELSE** DENY ACCESS



Subject
Name: *Anders*
Surname: *Andersson*
Date of birth: *10.01.1975*
User ID: *WR1000000*
Department: *R & D*
Roles: *CNCOperator*
Employment type: *Permanent*
Clearance: *Confidential*

Operation
Pick

Environment Conditions
Current date: *20.11.2016*
Current time: *10:15*
Payload: *2kg*
IP: *10.0.0.15 (Internal)*
Comm. protocol: *TCP/IP*
Client type: *Corporate PC*
Encryption type: *AES*
Threat level: *Low*

Object
Manufacturer: *KUKA Robotics*
Model: *KR 16-2*
Asset ID: *AT1000000*
Department: *Assembly Line*
Comp. type: *Low payload robotic arm*
Classification: *Confidential*
Function: *Handling and Loading*
Max Reach: *1610 mm*
Number of Axes: 6
Max payload: *16kg*

Policy
Description: *Evaluate robotic arm access request*
Conditions
IF *[Object Department* **IS** *Assembly Line]* **AND**
[Subject clearance level **IS HIGHER THAN OR**
EQUAL TO *Object classification level]* **AND**
[Encryption type **IS** *AES]* **AND**
[IP **IS** *Internal IP]* **AND**
[Current time **IS IN** *Working hours]* **AND**
[Operation **IS** *Pick]* **AND**
[Payload **IS LESS THAN** *16kg]*
THEN *PERMIT ACCES*
ELSE *DENY ACCESS*

Fig.5. ABAC Model for ICS Example with Policy Conditions, Subject, Object, Operation and Environment Attributes

According to the use case; Anders, who is an operator, wishes to perform “Pick” operation with the help of PLC-controlled robotic arm. As shown in Fig. 3, the policy enforcement point (PEP) logically protects the robotic arm from unauthorized access. After receiving the access request, PEP queries the policy decision point (PDP) with the requested operation, “Pick”. Then PDP populates the five cornerstones of ABAC (Fig. 5). In other words, the access policy (Table 3) is fetched from the policy repository; the object, subject and environment attributes (Table 2) are fetched from the attribute repository via the policy information point (PIP). Subsequently, PDP evaluates the access policy and replies the access decision to the policy enforcement point (PEP) which then permits or denies the access request. Meanwhile, the central audit logging process in PDP updates the audit trail with relevant logging events.

In the scenario above, Anders belongs to the research and development department and his clearance level is higher than the classification of the robotic arm. Besides, he is located inside the enterprise network (internal IP) and the communication channel is secured with AES encryption. He requests to perform “Pick” operation for 2kg payload during the working hours. Given all these facts, PDP decides to “Permit” the access request and PEP allows Anders to carry out the operation.

The sequence diagram shown in Fig. 6 illustrates the relationship among all components mentioned in the scenario above.

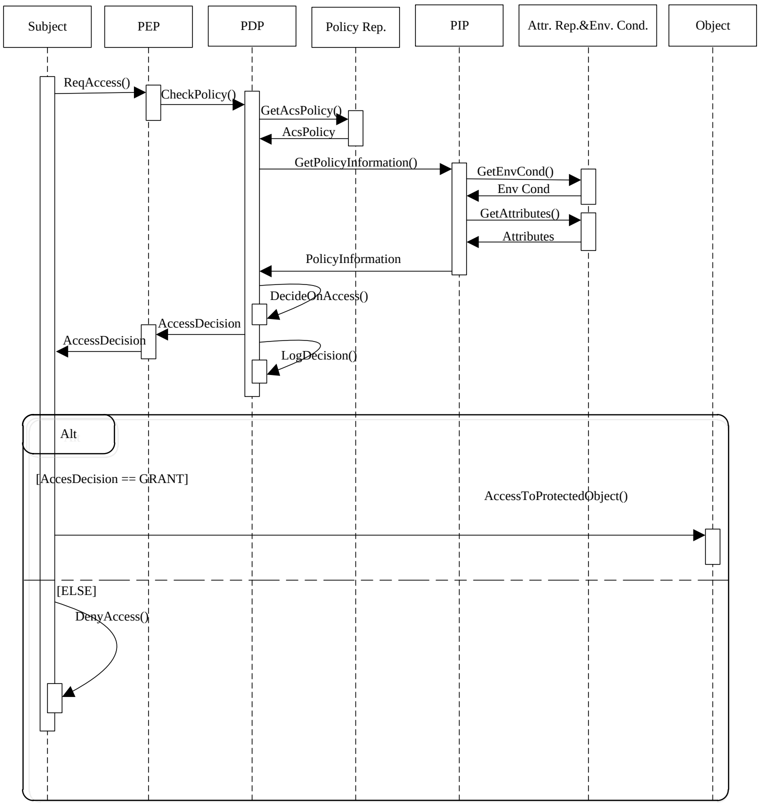


Fig.6. Sequence Diagram in the Context of Human Operator and PLC-Controlled Robotic Arm Authorization

VIII. Implementation

This section of the research elaborates the implementation details of the proposed scenario. The proof of concept setup is based on an open source framework, WSO2 Identity Server [19] and an open source relational database, MySQL [20]. Functional and load testing are performed with the help of another open source tool, Soap UI [21].

In the context of the ABAC reference architecture (Fig. 3), WSO2 Identity Server represents the policy decision point (PDP) and the policy repository, MySQL database functions (see Fig. 7 for Database Entity Relationship diagram) as the attribute repository for subject, object and environment conditions (see Appendix D for the definitions of the request and policy attributes). The custom developed (in Java) policy information point (PIP) fetches the relevant attribute values from the attribute repository. For the sake of simplicity, Soap UI assumed to represent the policy enforcement point (PEP). The prepared test cases simulate access requests (Soap format) towards PDP. Last but not least, the access rule (see Appendix B for the test policy) is implemented in eXtensible Access Control Markup Language (XACML).

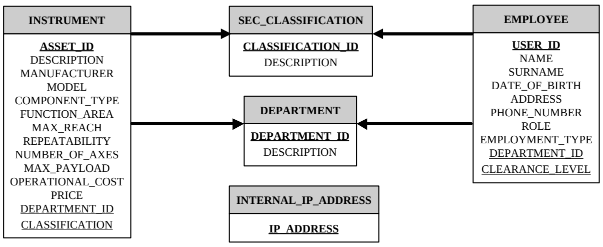


Fig. 7 – Database Entity Relationship Diagram

IX. Testing

The testing strategy comprises functional and load testing suites. As mentioned in the previous section, Soap UI is utilized for automating the testing procedure. The proof of concept setup is installed and configured on a Windows based office laptop with a quad-core desktop processor and 4GB of RAM.

The functional test suite has been formulated to cover positive and negative test cases. In other words, the correctness of deny and permit cases have been validated under various scenarios (see Appendix A for a sample Soap request resulting permit).

The load test suite has been formulated to measure the end to end average response time. The test suit blends a variety of successful and unsuccessful cases to simulate the real life scenario. Fig. 8 illustrates the average response time versus the total throughput (number of processed requests) for increasing number of concurrent requesting threads (from 1 to 100).

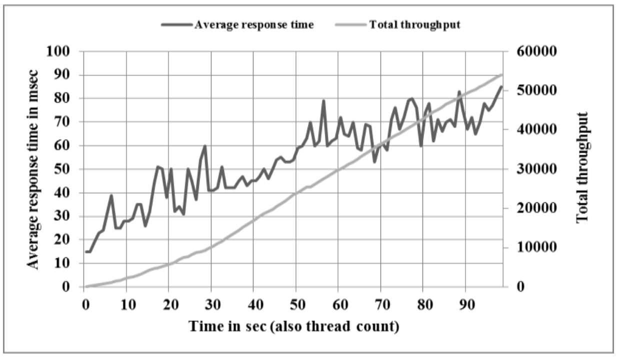


Fig.8. Average Response Time Compared Versus Total Throughput for Increasing Number of Concurrent Requesting Threads (From 1 to 100)

X. Discussions

The information security is fundamentally based on confidentiality, integrity and availability components. This research proposes to improve the confidentiality component for ICS by harnessing the ABAC model. However, the other two components are equally significant and improving one should not too much negatively affect the other two. In our case, introducing ABAC model for ICS apparently increases the computational burden which eventually affects the whole system's availability.

Although the latency requirement may vary for different types of ICS, it should be under a certain threshold to make sure that the criticality and responsiveness of the overall system are not compromised. According to Alcatel [23], the latency for real-time control and monitoring systems should be below 20 milliseconds whereas according to U.S. Department of Homeland Security [22], UTC and Avista [23], latency should not exceed 200 milliseconds.

In relation to our implementation; the end to end latency of the test setup reaches up to 85 milliseconds with roughly 500 request/sec throughput for 100 concurrent requesting threads (see Fig. 8). Given the low computational power of the test setup, the latency (availability) could still be considered at an acceptable level for many ICS.

Many of the ICS play a key role in automating and controlling core industrial processes, thus they are classified as business or even safety critical. Given their importance, system robustness and resilience are two fundamental design factors influencing the ICS based systems.

The proposed solution relies on a central decision point, PDP. Therefore PDP becomes a single point of failure and it has to be robust enough to tolerate the possible system faults. In other words, the access control manager has to be highly available and should employ redundancy.

The high availability and the low latency requirements can be met by distributing the system load among multiple instances of mirrored PDPs. Therefore, if one of the nodes is overloaded or down, the traffic could be diverted (failover) through the other instances.

XI. Conclusions

The majority of ICS lack even basic security services like authentication and authorization as ICS are believed to be operating in isolated network segments inside a factory or production line and having perimeter-based security tools such as firewalls is good enough to keep ICS secure. However, an increasing number of ICS related security incidences contradicts the common belief.

The industrial production systems are foreseen to evolve into having self-organization, self-diagnose and self-healing capabilities in the near future. These new capabilities also create new challenges such as access control and management.

Being identified as one of the key ICS incident vectors, poor access control has been proposed to be addressed by some researchers with traditional access control models like RBAC. However, due to the complexity of role administration, scalability issues and difficulties to implement fine-grained authorization rules, RBAC model does not fully fit the ICS access control challenges.

ABAC is an emerging access control model offering fine-grained authorization with central access policy management and consolidated logging functionalities.

This research proposes to harness the ABAC model for ICS to address the present and future ICS access control challenges. The proposed solution is implemented and successfully tested for numerous scenarios. The test results proved the viability of the proposed solution with a satisfactory performance that might even be improved with distributed system architecture.

APPENDIX A

```
<?xml version="1.0"?>
<Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
CombinedDecision="false" ReturnPolicyIdList="false">
  <Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject">
    <Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
IncludeInResult="true">
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">WR100000
0</AttributeValue>
    </Attribute>
  </Attributes>
  <Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:resource">
    <Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
IncludeInResult="true">
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">AT100000<
/AttributeValue>
    </Attribute>
    <Attribute AttributeId="http://kth.se/ics/departmentid"
IncludeInResult="true">
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">100</Attrib
uteValue>
    </Attribute>
    <Attribute AttributeId="http://kth.se/ics/payload"
IncludeInResult="true">
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">16</Attrib
uteValue>
    </Attribute>
  </Attributes>
  <Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:action">
    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-
id" IncludeInResult="true">
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">pick</Attri
buteValue>
    </Attribute>
  </Attributes>
  <Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment">
    <Attribute AttributeId="http://kth.se/ics/commencryptiontype"
IncludeInResult="true">
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">aes</Attrib
uteValue>
    </Attribute>
    <Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-
id" IncludeInResult="true">
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">10.0.0.15</
AttributeValue>
    </Attribute>
    <Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time"
IncludeInResult="true">
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#time">12:00:00</A
ttributeValue>
    </Attribute>
  </Attributes>
</Request>
```

APPENDIX B

```
<?xml version="1.0"?>
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
xmlns:xacml="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="ICS-Policy"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-
algorithm:first-applicable" Version="1.0">
  <Target/>
  <Rule RuleId="rule1" Effect="Permit">
    <Target>
      <AnyOf>
        <AllOf>
          <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-
equal-ignore-case">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">pick</Attri
buteValue>
            <AttributeDesignator MustBePresent="false"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
          <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-
equal-ignore-case">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">aes</Attrib
uteValue>
            <AttributeDesignator MustBePresent="false"
Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
AttributeId="http://kth.se/ics/commencryptiontype"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
          <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-
equal-ignore-case">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">100</Attrib
uteValue>
            <AttributeDesignator MustBePresent="false"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
AttributeId="http://kth.se/ics/departmentid"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </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:integer-greater-
than-or-equal">
          <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag-size">
            <AttributeDesignator MustBePresent="false"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject" AttributeId="http://kth.se/ics/ipaddress"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Apply>
          <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">1</Attribu
teValue>
        </Apply>
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
          <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">
                <AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time"
Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
```

```
DataType="http://www.w3.org/2001/XMLSchema#time"
MustBePresent="true"/>
        </Apply>
        <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#time">08:00:00</A
ttributeValue>
      </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">
          <AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time"
Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
DataType="http://www.w3.org/2001/XMLSchema#time"
MustBePresent="true"/>
        </Apply>
        <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#time">18:00:00</A
ttributeValue>
      </Apply>
    </Apply>
    <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
      <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-greater-
than-or-equal">
        <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-one-and-
only">
          <AttributeDesignator
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject" AttributeId="http://kth.se/ics/maxpayload"
DataType="http://www.w3.org/2001/XMLSchema#integer"
MustBePresent="false"/>
        </Apply>
        <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-one-and-
only">
          <AttributeDesignator
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
AttributeId="http://kth.se/ics/payload"
DataType="http://www.w3.org/2001/XMLSchema#integer"
MustBePresent="false"/>
        </Apply>
      </Apply>
      <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-greater-
than-or-equal">
        <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag-size">
          <AttributeDesignator MustBePresent="false"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject" AttributeId="http://kth.se/ics/clearancecheck"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Apply>
        <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">1</Attribu
teValue>
      </Apply>
    </Apply>
   </Apply>
  </Apply>
 </Condition>
</Rule>
<Rule RuleId="rule2" Effect="Deny"/>
</Policy>
```

APPENDIX C

1. SELECT IP_ADDRESS FROM INTERNAL_IP_ADDRESS WHERE IP_ADDRESS = '<http://kth.se/ics/ipaddress>' ;
2. SELECT MAX_PAYLOAD FROM INSTRUMENT WHERE ASSET_ID ='<urn:oasis:names:tc:xacml:1.0:resource:resource-id>' ;
3. SELECT ROLE FROM EMPLOYEE WHERE USER_ID ='<urn:oasis:names:tc:xacml:1.0:subject:subject-id>'AND EXISTS (SELECT * FROM INSTRUMENT WHERE EMPLOYEE.CLEARANCE_LEVEL >= INSTRUMENT.CLASSIFICATION AND ASSET_ID ='<urn:oasis:names:tc:xacml:1.0:resource:resource-id>') ;

APPENDIX D

Defined	Attribute	Description
Request	http://kth.se/ics/ commencryptiontype	Encryption type of the communication channel
Request	http://kth.se/ics/ departmentid	Object's department
Policy	http://kth.se/ics/ ipaddress	The result of SQL defined in Appendix C-1 deciding if the subject is internally located
Policy	http://kth.se/ics/ maxpayload	The maximum payload that the robotic arm can handle. The value is fetched from the attribute repository via PIP with the SQL defined in Appendix C-2
Policy	http://kth.se/ics/ clearancecheck	The result of SQL defined in Appendix C-3 which decides if the subject's clearance level is higher than or equal to the object's classification level
Request	http://kth.se/ics/payload	Actual payload
Request	urn:oasis:names:tc:xacml:1.0: subject:subject-id	User ID of the subject
Request	urn:oasis:names:tc:xacml:1.0: resource:resource-id	Asset ID of the object
Request	urn:oasis:names:tc:xacml:1.0: action:action-id	Attempted operation
Request	urn:oasis:names:tc:xacml:1.0: environment:environment-id	Actual IP address of the subject
Request	urn:oasis:names:tc:xacml:1.0: environment:current-time	Actual time of the request

REFERENCES

[1] ICS-CERT, “ICS-CERT Year in Review 2012.” 2012.

[2] ICS-CERT, “ICS-CERT Year in Review 2013.” 2013.

[3] U.S. Department of Homeland Security, “Common Cybersecurity Vulnerabilities in ICS.” May-2011.

[4] ICS-CERT, “ICS-CERT Monitor between September 2014-February 2015.” 2015.

[5] GE Measurement & Control Solutions, “Top 10 Cyber Vulnerabilities for Control Systems.” 2012.

[6] National American Reliability Council, “Top 10 Vulnerabilities of Control Systems and their Mitigations.pdf.” Dec-2006.

[7] M. Bishop, Introduction to computer security. Boston: Addison-Wesley, 2005.

[8] L. Janczewski and A. M. Colarik, Eds., Cyber warfare and cyber terrorism. Hershey: Information Science Reference, 2008.

[9] R. S. Sandhu and P. Samarati, “Access control: principle and practice,” Commun. Mag. IEEE, vol. 32, no. 9, pp. 40–48, 1994.

[10] S. Oh and S. Park, “Task–role-based access control model,” Inf. Syst., vol. 28, no. 6, pp. 533–562, 2003.
[11] R. Sandhu, “Access control: The neglected frontier,” in Information Security and Privacy, 1996, pp. 219–227.
[12] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, “Guide to Attribute Based Access Control (ABAC) Definition and Considerations,” National Institute of Standards and Technology, NIST SP 800-162, Jan. 2014.
[13] L. Pietre-Cambacedes, M. Tritschler, and G. N. Ericsson, “Cybersecurity Myths on Power Control Systems: 21 Misconceptions and False Beliefs,” IEEE Trans. Power Deliv., vol. 26, no. 1, pp. 161–172, Jan. 2011.
[14] A. Valenzano, “Industrial Cybersecurity: Improving Security Through Access Control Policy Models,” IEEE Ind. Electron. Mag., vol. 8, no. 2, pp. 6–17, Jun. 2014.
[15] M. Cheminod, L. Durante, L. Seno, and A. Valenzano, “On the description of access control policies in networked industrial systems” in Factory Communication Systems (WFCS), 2014 10th IEEE Workshop on, 2014, pp. 1–10.
[16] K. Stouffer, J. Falco, and K. Scarfone, “NIST, Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security.” Jun-2011.
[17] “ISA99, Industrial Automation and Control Systems Security - ISA.” [Online]. Available: https://www.isa.org/isa99/. [Accessed: 04-Apr-2015].
[18] M. Onori and J. Barata, “Evolvable Production Systems: new applications in mechatronic equipment”, Transactions on Industrial Electronics, IEEE Journal, IES Society, 2010.
[19] WSO2 Identity Server 5.0.0. www.wso2.org: WSO2, 2015.
[20] MySQL Community Server 5.6.24. www.mysql.com: MySQL, 2015.
[21] SoapUI 5.2. www.soapui.com: SmartBear, 2015.
[22] U.S. Department of Homeland Security, “Control Systems Communications Encryption Primer” Dec-2009.
[23] U.S. Department of Energy "Communications Requirements of Smart Grid Technologies" Oct-2010.

Authors’ Profiles

Erkan Yalcinkaya is an independent industrial Ph.D. candidate at Department of Production Engineering, Royal Institute of Technology, Stockholm, Sweden. Erkan is an experienced IT security specialist focused on access control technologies. His main research focus is security aspects of industrial manufacturing systems and production lines.

Antonio Maffei received the B.E. and the M.E. degree in industrial engineering from the University of Pisa, Tuscany, Italy. Antonio received a Ph.D. degree in production engineering from KTH, Royal Institute of Technology in Stockholm, Sweden, in 2012.

After a postdoc within the Swedish strategic XPRES initiative, he started a tenure track with an assistant professorship on “Production System focus area business models” at KTH. Dr. Maffei is currently Head of the research group named Technologies for Adaptable Production. His current research interests include business models for advanced automation technology, assembly technology and engineering education. Dr. Maffei is a Research Affiliate of The International Academy for Production Engineering; active in a number of national and international networks.

Professor Mauro Onori is the current Head of Department of Production Engineering at the Royal Institute of Technology, School of Industrial Eng. & Management. Prof. Onori has published over 150 articles, has been European Project Leader since 2006 with participation since 1999, including projects E-Race, EUPASS, AssemblyNet, IDEAS, openMOS, etc. Prof. Onori has also been guest lecturer at both École Polytechnique Fédérale de Lausanne and the New University of Lisbon. Onori has also received several awards including the Japan Robot Association Award.

How to cite this paper: Erkan Yalcinkaya, Antonio Maffei, Mauro Onori,"Application of Attribute Based Access Control Model for Industrial Control Systems", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.2, pp.12-21, 2017.DOI: 10.5815/ijcnis.2017.02.02