MANAGING ACCESS CONTROL SYSTEMS IN DISTRIBUTED ENVIRONMENTS WITH DYNAMIC ASSET PROTECTION

PHD THESIS
University of Murcia

Author
D. Daniel Orlando Díaz López

Advisors
Dr. Félix Gómez Mármol
NEC Laboratories Europe

Prof. Dr. Gregorio Martínez Pérez
University of Murcia

November 30th, 2015
I. MOTIVATION

Access control is a key element to guarantee protection of assets.

Information security risks are changing all the time, so safeguards to protect assets should adapt accordingly.

There are new business models based on shared assets in distributed environments.

Almost each one of us has a digital life (asset) exposed to privacy risks in a hostile environment.
I. MOTIVATION

OUR MAIN GOAL IS TO ACHIEVE AN EFFECTIVE MANAGEMENT OF ACCESS CONTROL SYSTEMS IN DISTRIBUTED SCENARIOS WHICH PROTECTS INFORMATION ASSETS
II. ROADMAP

G1. Identify limitations of access control systems in multiple security domains

G2. Propose a solution for policy management in distributed environments

G3. Design an access control process which considers security risks

G4. Propose a solution aimed to mitigate security risks which considers business objectives

G5. Identify security and privacy challenges in live digital systems

G6. Propose an architecture for live digital systems which handle shared assets and are exposed to changing risks
III. MANAGING XACML INFRASTRUCTURE

Isolated access control processes

We know that the **authorization aspect** (privileges) over corporative **assets** is a must in security of information.

XACML offers a way to achieve a central access control process and supports **asset governance**!

However in real world **each corporate area** initially implements its **own access rules** to control access to **corporative assets** in their business unit.
XACML defines **XML schemas** for access policies, access request, response; and an **architecture** composed of PAP, PDP, PEP and PIP.

1) Is this suitable for larger environments where there are multiple “owners” of an asset?
2) Is this suitable for supporting distributed access control architectures?
III. MANAGING XACML INFRASTRUCTURE

XACML limitations

If each security domain deploys an independent XACML architecture with its own access policies how would it be possible to get a coordinated management?

- A main office and its subsidiaries
- A service virtualization business model
- A service composition model (cloud)

We are talking about extension of XACML to distributed/collaborative environments where many security domains control shared assets:

If each security domain deploys an independent XACML architecture with its own access policies how would it be possible to get a coordinated management?
III. MANAGING XACML INFRASTRUCTURE

Distributed XACML access policies management architecture

Now it is possible to have a coordinated management between domains through Meta-policies.

Two security domains are closely related but are not coordinated to manage shared assets.

Now it is possible to have a coordinated management between domains through Meta-policies.
How do we manage Access control policies in another domain?

XACML Policy

\[
\text{Policy} = \langle \text{Target} \\
\quad \mid (\emptyset \mid \text{Rule}_1, \ldots, \text{Rule}_n) \\
\quad \mid \text{RuleCombiningAlgorithm} \\
\quad \mid (\emptyset \mid \text{Obligation}_1, \ldots, \text{Obligation}_n) \rangle
\]

\[
\text{Rule} = \langle \text{Target} \\
\quad \mid (\emptyset \mid \text{Condition}_1, \ldots, \text{Condition}_n) \\
\quad \mid \text{Effect} \rangle
\]

\[
\text{Target} = \langle (\emptyset \mid \text{Subject}_1, \ldots, \text{Subject}_n) \\
\quad \mid (\emptyset \mid \text{Resource}_1, \ldots, \text{Resource}_n) \\
\quad \mid (\emptyset \mid \text{Action}_1, \ldots, \text{Action}_n) \\
\quad \mid (\emptyset \mid \text{Environment}_1, \ldots, \text{Environment}_n) \rangle
\]

XACML MetaPolicy

\[
\text{MetaPolicy} = \langle \text{Target} \\
\quad \mid (\emptyset \mid \text{Rule}_1, \ldots, \text{Rule}_n) \\
\quad \mid \text{RuleCombiningAlgorithm} \\
\quad \mid (\emptyset \mid \text{Obligation}_1, \ldots, \text{Obligation}_n) \rangle
\]

\[
\text{Rule} = \langle \text{Target} \\
\quad \mid (\emptyset \mid \text{Condition}_1, \ldots, \text{Condition}_n) \\
\quad \mid \text{Effect} \rangle
\]

\[
\text{Target} = \langle (\emptyset \mid \text{Subject}_1, \ldots, \text{Subject}_n) \\
\quad \mid (\emptyset \mid \text{Policy}_1, \ldots, \text{Policy}_n) \\
\quad \mid (\emptyset \mid \text{PolicySet}_1, \ldots, \text{PolicySet}_n) \\
\quad \mid (\emptyset \mid \text{Action}_1, \ldots, \text{Action}_n) \\
\quad \mid (\emptyset \mid \text{Environment}_1, \ldots, \text{Environment}_n) \rangle
\]

XACML architecture is reused and its fine-grained access control capacity is applied to policy management.
XACML does not define protocols or transport mechanisms, but it can be secured by SAML

Risks against confidentiality and integrity on policies are reduced

We propose a new group of 5 queries and 5 responses to support the new policy management operations
There at least two possible attacks:

i. Attempt to **tamper messages (integrity)** involved in a policy management operation during the communication processes

ii. Attempt to execute any ill-intentioned action to get access to **information assets** (i.e. policies and attributes) in one domain (confidentiality)

These attacks can be executed through some of the following threats:

<table>
<thead>
<tr>
<th>Threats</th>
<th>XML encryption over SAML</th>
<th>XML signature over SAML</th>
<th>SSL/TLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data modification</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Eavesdropping</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity spoofing</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Man-in-the-Middle</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denial-of-Service</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Forged Claims</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replay of Message parts</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

And these threats can be faced with the following **three valid security controls**:
**ROADMAP**

**DACPM: Distributed access control policies management**

- **G1** Identify **limitations** of access control systems in **multiple security domains**
- **G2** Propose a solution for **policy management in distributed environments**

**Shared assets**

- **G5** Identify **security and privacy challenges** in live digital systems
- **G6** Propose an **architecture** for live digital systems which handle **shared assets** and are exposed to **changing risks**

**Risk management**

- **G3** Design an access control process which considers **security risks**
- **G4** Propose a solution aimed to **mitigate security risks which considers business objectives**
IV. RISK-BASED ACCESS CONTROL SYSTEMS

Regular operation of access control systems

There is a general assumption in access control systems: **homogeneity** (requesters, endpoints, context, etc.) But in fact access conditions are constantly changing: user, environment, assets, vulnerabilities, threats, etc.

Reliability on IT User conduct Purpose

Lack of dynamism. Access control policies need to be adapted to cover each case.

Lack of efficiency. Hard to manage manually in medium/large organizations.

Thus, there are two limitations of a regular XACML architecture:

- **Lack of dynamism.** Access control policies need to be adapted to cover each case.
- **Lack of efficiency.** Hard to manage manually in medium/large organizations.
IV. RISK-BASED ACCESS CONTROL SYSTEMS

Considering risk to compute authorization

RADAC SYSTEMS (opposite to regular systems), incorporates a Risk Analysis as a key input for the authorization decision process:

\[ RL = \frac{P \times I}{E} \]

But, next facts can occur:

1. If P, I or E do not change, decision will not change: The access to the asset is denied

2. When \( RL \) is intolerable, the system admin must trigger counter-measures to protect the asset properly: Not the most effective option
We propose a method to chose the best set of counter-measures applicable in a system with variable risk levels.

**Algorithm**  Optimization Algorithm

```plaintext
repeat
  i. Best individuals selection
  ii. Crossover
  iii. Mutation
  iv. New generation
until StopCondition
```
IV. RISK-BASED ACCESS CONTROL SYSTEMS

Best solutions found varying measured risk levels and acceptable risk levels

Conditions detected:

1. Failed connection from *two different locations*
2. Dictionary attacks have been registered
3. One new encryption vulnerability discovered
4. The file server contains confidential information

Non-negligible “*Unauthorized Access threat*” with RL = 10

Now, $RL \leq \bar{RL}$

After 69 generations, a Best set of counter-measures is found with a Fitness = 0.9:

i. Authentication mechanism (E = Low)
ii. Encryption techniques (E = Low)
iii. Attestation techniques (E = Medium)
iv. Isolation means (E = Medium)
v. Input validation strategies (E = Low)
vi. Change management strategies (E = Medium)
vii. Monitoring Strategy (E = Low)
viii. Software execution schema (E = Medium)
ix. Session Time Assignment (E = Medium)
x. Resource Exposure (E = High)
xii. Alert Mechanism (E = Medium)
xii. User Advertising Strategy (E = Low)
IV. RISK-BASED ACCESS CONTROL SYSTEMS

Best solutions found varying measured risk levels and acceptable risk levels

As the MEASURED risk level **increases**, having a **CONSTANT** acceptable risk, the counter-measures must be **more effective**
IV. RISK-BASED ACCESS CONTROL SYSTEMS

Best solutions found varying measured risk levels and acceptable risk levels

As the ACCEPTABLE risk level increases, having a CONSTANT measured risk, the counter-measures effectiveness decrease.
Propose an architecture for live digital systems which handle shared assets and are exposed to changing risks

Identify security and privacy challenges in live digital systems

Design an access control process which considers security risks

Propose a solution for policy management in distributed environments

Identify limitations of access control systems in multiple security domains

Propose a solution aimed to mitigate security risks which considers business objectives

DACPM: Distributed access control policies management

G1

G2

G3

G4

G5

G6

RbACS: Risk-based access control system

Shared assets

Risk management

User domain

DACPM

RbACS
“Your online life, permanent as a tattoo”
Juan Enriquez, TED Talks speaker

The greater our digital experience, the greater the amount of information we generate is distributed and stored along different computer systems.
### Desktop Search Tools

<table>
<thead>
<tr>
<th></th>
<th>Copernic</th>
<th>Locate32</th>
<th>Google</th>
<th>Yahoo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search within files</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Work across network shares</td>
<td>Untill Copernic 3.0</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Sources of personal information</td>
<td>File system</td>
<td>File system</td>
<td>File system, web, Google services (mail, IM)</td>
<td>File system, Yahoo services (mail, IM)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indexation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Structure</td>
<td>Structure</td>
<td>Structure</td>
<td>Structure</td>
<td>Structure</td>
</tr>
<tr>
<td>Process and store information preserving privacy</td>
<td>Include multiple service providers as part of the result</td>
<td>Develop new operations: sharing, auditing, etc.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Running</td>
<td>Continuously</td>
<td>Manual starting</td>
<td>Continuously</td>
<td>Continuously</td>
</tr>
<tr>
<td>Scope</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### MyLifeBits Project

|                   |          |          |        |       |
| Search within files |          |          | Yes    | Yes   |
| Work across network shares |          | Yes     | Yes    | No    |
| Sources of personal information |          |          |        |       |
| Indexation          |          |          |        |       |
| Storage             |          |          |        |       |
| Structure           | Structure | Structure | Structure | Structure |
| Association         | Association – linking of events using a DAG (Directed Acyclic Graph) based model. |
| Running             |          |          |        |       |
| Scope               |          |          |        |       |
| Project Status      |          |          |        |       |
We have now defined the different involved steps, but these bring many challenges ...
Security and Privacy Challenges

- RbACS: Risk-based access control system
- DACPM: Distributed Access control policies management

It is in different ways a context with **shared assets** and **variable risks**

- **RbACS**
  - Assurance of technological infrastructure
- **Forensic evidence**
- **Transparency**
- **Transversal security and privacy**
- **Encrypted data retrieval**
- **Private data processing**
- **Private storage of data**
- **Selective gathering**
- **Purpose-based exposure**
- **DACPM**
  - Selective access

Where would it be possible to apply **access control policies management**?
Where would it be possible to apply **variable risk mitigation**?
V. LIVE DIGITAL REMEMBER DIGITAL
Privacy and security challenges

Live Digital Server Side A

Resource Server

Id Provider

Live Digital Client Side

Secure Communication

GuI

Outlook

Live Digital Server Side B

DACPM: Distributed Access control policies management
RbACS: Risk-based access control system
V. LIVE DIGITAL REMEMBER DIGITAL
High-level architectural components and data capturing process

Client

Server

End user
V. LIVE DIGITAL REMEMBER DIGITAL
Data recovery process
GOALS

**Identify limitations of access control systems in multiple security domains**

**Propose a solution for policy management in distributed environments**

**Design an access control process which considers security risks**

**Propose a solution aimed to mitigate security risks which considers business objectives**

**Identify security and privacy challenges in live digital systems**

**Propose an architecture for live digital systems which handle shared assets and are exposed to changing risks**

**DACPM**: Distributed access control policies management

**RbACS**: Risk-based access control system

**LDS**: Live digital systems
OUR MAIN GOAL IS TO ACHIEVE AN EFFECTIVE MANAGEMENT OF ACCESS CONTROL SYSTEMS IN DISTRIBUTED SCENARIOS WHICH PROTECTS INFORMATION ASSETS
A well thought-out access control process contributes significantly to the success of an information society.

Our proposal for managing XACML systems in distributed environments through Meta-Policies allows to manage shared assets in a secure way.

Considering the security risk in an authorization context helps to perform operations based on business objectives and to get a practical application.

The dynamic countermeasures integrated in risk-adaptable access control systems provide a way to protect assets without denying access.

The live digital systems bring different challenges in the field of security and privacy in order to make these services effectively usable.

The architecture proposed for live digital systems, plus the results obtained previously in this PhD Thesis set the first step in the road to a nearby implementation.
VII. FUTURE WORKS

- **Management of XACML systems in distributed environments:**
  - New operations, kind of policies, others resources
  - New services around shared assets
  - Legal compliance, cyber defense, etc.

- **Risk-adaptable Access control systems:**
  - New risk methodologies, threats, assets and counter-measures
  - Integration with a cyber defense decision process (OODA, CAESARS)
  - Extension to offensive purposes (Ethical hacking)

- **Live digital systems:**
  - Purpose-based exposure, storage and processing of private data, encrypted data retrieval, forensic evidence, selective access, etc.

- **Integration of the live digital architecture with shared asset and risk-adaptable access proposals**
VIII. CONTRIBUTIONS
Journals with Impact Factor (JCR)


http://dx.doi.org/10.1016/j.cose.2014.10.004


http://dx.doi.org/10.1016/j.future.2014.10.012


http://dx.doi.org/10.1016/j.compeleceng.2013.11.008
Develop the Planning and Doing Phases of ISMS for SIC
Implement the ISMS under E-government Strategy MINTIC
Design the Business Continuity Plan for SIC
Develop the Planning and Doing Phases of ISMS for UPRA
Develop the Doing Phase of ISMS for SSF
Design the IT Strategic Plan for SSF

VIII. CONTRIBUTIONS
Internships and projects

2 Internships at NEC Laboratories Europe

UMU

“Managing XACML systems in distributed environments through Meta-Policies”
“Dynamic countermeasures for risk-based access control systems: An evolutive approach”
“Live digital, remember digital: State of the art and research Challenges”

6 Projects at CINTEL - Centro de Investigación y Desarrollo en TICs

Improve PAP, PDP implementations
Design a distributed policy administration environment
Develop advanced methods for distributing policies
Improve performance of policy evaluation decision
Design solution to find countermeasures
Integration of IDaaS into NEC’s IdM solution