Usable Access Control Enabled by Sensing Enterprise Architectures

Mikel Uriarte
Nextel S.A. Parque Científico y Tecnológico de Bizkaia, C/ Camino de Laida Edificio 207, Bloque B 1º planta 48170 Zamudio, SPAIN
muriarte@nextel.es

Oscar Lázaro
Innovalia Association, Rodríguez Arias, 6, Dto. 605, 48008 Bilbao, SPAIN
olazaro@innovalia.org

Alicia González
Innovalia Association, Rodríguez Arias, 6, Dto. 605, 48008 Bilbao, SPAIN
agonzalez@innovalia.org

Iván Prada
Innovalia Association, Rodríguez Arias, 6, Dto. 605, 48008 Bilbao, SPAIN
iprada@innovalia.org

Oscar López
Nextel S.A. Parque Científico y Tecnológico de Bizkaia, C/ Camino de Laida Edificio 207, Bloque B 1º planta 48170 Zamudio, SPAIN
olopez@nextel.es

Jordi Blasi
Nextel S.A. Parque Científico y Tecnológico de Bizkaia, C/ Camino de Laida Edificio 207, Bloque B 1º planta 48170 Zamudio, SPAIN
jblasi@nextel.es

Eneko Olivares
Polytechnic University of Valencia, Department of Communications, Superior Technical School of Telecommunication Engineering, Camino de Vera S / N; 46022 Valencia, SPAIN
enolgor@upv.es

Carlos E. Palau
Polytechnic University of Valencia, Department of Communications, Superior Technical School of Telecommunication Engineering, Camino de Vera S / N; 46022 Valencia, SPAIN
cpalau@dcom.upv.es

1. Introduction

We are watching an exponential increase on the amount and type of devices with Internet connectivity capabilities, from very common nowadays smartphones to other more specialized devices such as machine tools in industrial environments. This is leading to what is known as the Internet of Everything (IoE), which is an evolution of the concept of the internet of things (IoT), in which a huge number of devices (50 billion by 2020 according to Cisco) will interconnect people, things, processes, information, etc. All this connectivity is intrinsically linked with the generation of a huge amount of heterogeneous information, known as BIG DATA, This boost of information is turning companies of the future in "Sensing Enterprises", as an enterprise making use of the sensing possibilities provided by interconnected 'environments', anticipating future decisions by using multi-dimensional information captured through physical and virtual objects, and providing added value information to enhance its global context awareness (Santucci et al., 2012).

Today's businesses are beginning to evaluate and exploit using advanced analytical techniques that allow them to find patterns among consumers, define more effective business strategies, analyse market reactions, and improve their processes (cost reduction, increased production quality, streamline activities, improving information for decision making, enhance collaboration, etc.). This unavoidably immerses them in the competitive nature that comes with the

In: M. Zelm (eds.): Proceedings of the 6th Workshop on Enterprise Interoperability, Nîmes, France, 27-05-2015, published at http://ceur-ws.org

inference between Information Technology and Business Processes. Furthermore, to facilitate collaborative activities, adapt to new business scenarios and to increased user mobility, plus supporting systems migration to the cloud, in search for better availability, scalability and reduced total cost of the operation, business are imposed with the need of enabling information exchange between organizations.[1]

This operation scenario, of different connected components and "total availability", raises a number of disadvantages stemming mainly from the problems related to privacy, security and trust, and in most cases as a result of unauthorized access to corporate networks and systems access. Therefore, collaboration between companies requires security solutions and federated access control that grants trust between the parties.

Access control is one of the fundamental security services used for mitigating risks in networked environments. Therefore, it is imperative for companies to implement a robust and reliable system to ensure that their most valuable information assets are safe. Traditionally, increasing security in access control systems is directly tied to a reduction in the usability of user services. The ACIO project and its results provide mechanisms to improve usability in managing access control and interoperability. These mechanisms have been validated in different application domains, such as transport and port logistics, on stage at the Port of Valencia.

This article exposes the ACIO approach to enable fast decision making in multi-domain access control management using context-sensitive features, and the synchronization and exchange of data between the physical and logical world. The article is structured as follows: section 2 presents the state of the art related to access control mechanisms in organizations, after this, section 3 introduces the use case on which the solution has been validated and the proposed architecture in the ACIO project. Following this, article IV explains the performance evaluation carried out, and finally conclusions and future work are presented in section V.

2. State of the Art

Access control is defined as the protection of the resources of a system against unauthorized access and the process by which the use of resources of the system is regulated according to a security policy and only allowed by entities authorized (users, programs, processes, or other systems) in accordance with that policy[2]. There are two types of access control are the physical and logical.

Physical access control encompassed those security measures that are implemented in the physical world designed to prevent unauthorized access to facilities, equipment and resources, and in this sense, protecting staff and resources. In dependence of the required levels of security, this measures can be: (i) anti-vandalism measures; (ii) dissuasive measures or (iii) Measures for intrusion detection and electronic surveillance. The control systems of physical access do not necessarily work in an isolated manner, and there are complete solutions that enable a centralized management of access control. This type of solutions allow to manage the security levels of the different access points in real time, generate reports, conduct audits, etc. and incorporate a full range of capabilities that include: (i) Identity Management; (ii) Management of security policy; (iii) Remote Device Management.

However, physical access control presents a major shortcoming, as there is a lack of interoperability between different available access control systems, creating problems of integration and scaling. This lack of interoperability is caused by the unavailability of efficient standards for the effective and regulated communication between devices from different manufacturers, since these operate under own proprietary communication protocols. This complexity also affects negatively the processes of improving the management of access control, since this heterogeneity adds complexity to the activities of monitoring and auditing.

On the other side, logical access control is defined as the interposition of security mechanisms to prevent access of unauthorized users to data resources at virtual level, and also the selective restriction of privileges that authorized users have on the system's assets. Logical Access control is nowadays evolving rapidly due to the rise of cloud services, collaboration between organizations and high usability requirements of users, and there are various standards that have been defined and maintained to cover different aspects of logical access control in cloud

[1] CISCO IBSG, 2013
[2] RFC 4949: http://tools.ietf.org/html/rfc4949

environments: (i) OpenID; (ii) OAUTH 2.0; (iii) The markup Security Assertion (SAML) and (iv) The extensible markup language access control (XAMCL).

There are a multitude of models for managing logical access control which differ mainly in the way in which the system manages user's privileges: (i) Mandatory Access Control (Mandatory Access Control - MAC); (ii) discretionary access control (Discretionary access control - DAC); (iii) Access control based on roles (Role Based Access Control - RBAC); (iv) Access control based on attributes (Attribute-Based Access Control - ABAC); (v) Semantic-aware attribute-based access control model - SABAC); (vi) Access control based on context and semantics (Semantic Context-Based Access Control model - SCBAC); (vii) Access control based on experience (Experience Based Access Management - EBAM); and (viii) Based Access Control capabilities (Capacity-Based Access Control - CapBAC).

The main deficiency that logical access control models available today present, is related in addressing access control as a dichotomy between security and usability, reducing one of these aspects when reinforces the other and vice versa, making them unsuitable for environments requiring high levels of both at the same time.

3. Proposed Solution

3.1 Use Case Description

The selected use case in order to validate the results of the ACIO proposed architecture for Access Control is the dependencies of the Port of Valencia. The port has highly complex control requirements both at physical and logical access control level. This complexity in port Access Control management is a result of the interaction of a great variety of actors and heterogeneous elements (e.g. Containers, machinery, trucks of different operators, etc.), the high dependency of the port's competiveness in the fluidity of the ongoing operations, and the obligation to comply with different rules and national and international legislation. In the port premises there are five container terminals. Most of them support more than 4000 truck movements and 10,000 containers per day. The port management system is based on a PCS (Port Community System) in the cloud, which manages the exchange of information among the large number of actors from the port (port authority, customs, transport companies, companies providing services etc.), accessing their facilities and interact in a federated way between them.

The usability of the Access control management in the use case presents multiple points capable of improving and some relevant problems. In this sense, Figure 1. Use Case Access Control Chain and related deficienciesshows the current Access Control chain of the use case and each step related deficiencies that have been identified:

Figure 1: Use Case Access Control Chain and related deficiencies

With the aim of improving these aspects regarding usability without degrading the security of the AC management, the following features are proposed which can be seen in Figure 2. Proposed Use Case AC management improvements:

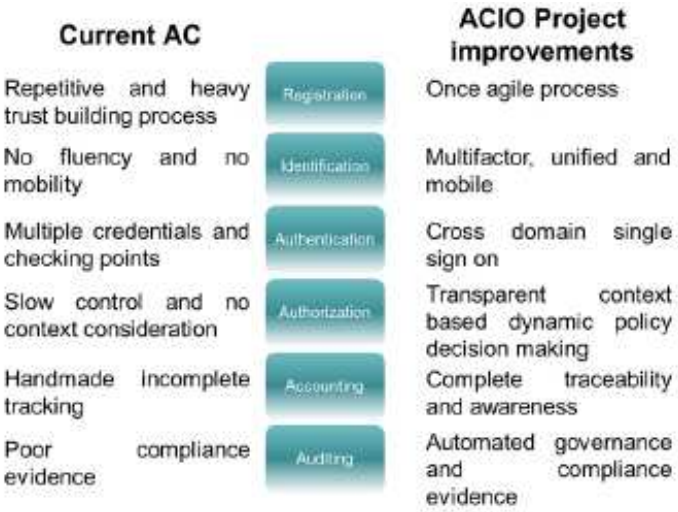

Figure 2. Proposed Use Case AC management improvements

Therefore, the consequent AC management of the Use case will evolve from a static, inefficient and low security AC approach, to a secure and user centred AC management, which will provide high usability and enhanced security in compliance with the seaports requirements.

3.2 ACIO architecture

The application of IoE management to digital business processes has resulted in the proposal of new management architectures for services under the umbrella of "Sensing Enterprise". This SOA 2.0 architecture, encompassing Service Oriented and Event-driven (SOA-EDA) architectures rely on advanced middleware to interconnect seamlessly and efficiently information (data and events) of logical and physical worlds (real, virtual and digital information):

- **Real World**: Information devices that handle the physical components (sensors, actuators)
- **Digital World**: Digital services, analysis, modelling, metadata or multimedia information.
- **Virtual World**: models of virtual and augmented reality.

Thus, “Sensing Enterprise” architectures allow anticipating future decisions by using multidimensional information captured through physical objects and synchronized digital-virtual services in a transparent way to users.

ACIO proposes the application of this type of advanced service management architectures and events as a mechanism for improving the usability and performance of access control mechanisms in highly complex and sensorized environments. The main advantage for the AC mechanisms that is provide by the logical and physical services interconnection, is that the information generated will be used to improve decision making for Access Control in real-time, in a transparent way to the user.

For this to be possible, access control models of the different worlds must evolve and integrate into the middleware which facilitate the sensing enterprises world’s interoperability. ACIO promotes the development of models and Access Control solutions based in the Sensing Enterprise architectures, that can facilitate the exchange of security information between the three worlds (real, digital and virtual), and led to a new model for access Control: The "Sensing access control" which adds value to the access control over the architecture of the Sensing Enterprise, as presented in Figure 3. ***Reference architecture model for "Sensing Access Control"***

According to the cluster of digital innovation process and the OSMOSE European project[3], the reference architecture for the Sensing Enterprise consists of the following elements:

- **Inter-world router**: It handles the exchange of data and events between physical-digital-virtual services such as the interoperability mechanism.
- **Intra-world Bus**: It handles the events and data exchange between the systems components (digital-analysis services, sensors-actuators, simulators, virtual-augmented displays).
- **Context manager**: Element in charge of the analysis of policy related to message, events and data delivery, and the planning of their transmission.
- **Service Manager**: Element responsible for the publication and services subscription to the event and data reception.

[3] http://www.osmose-project.eu/

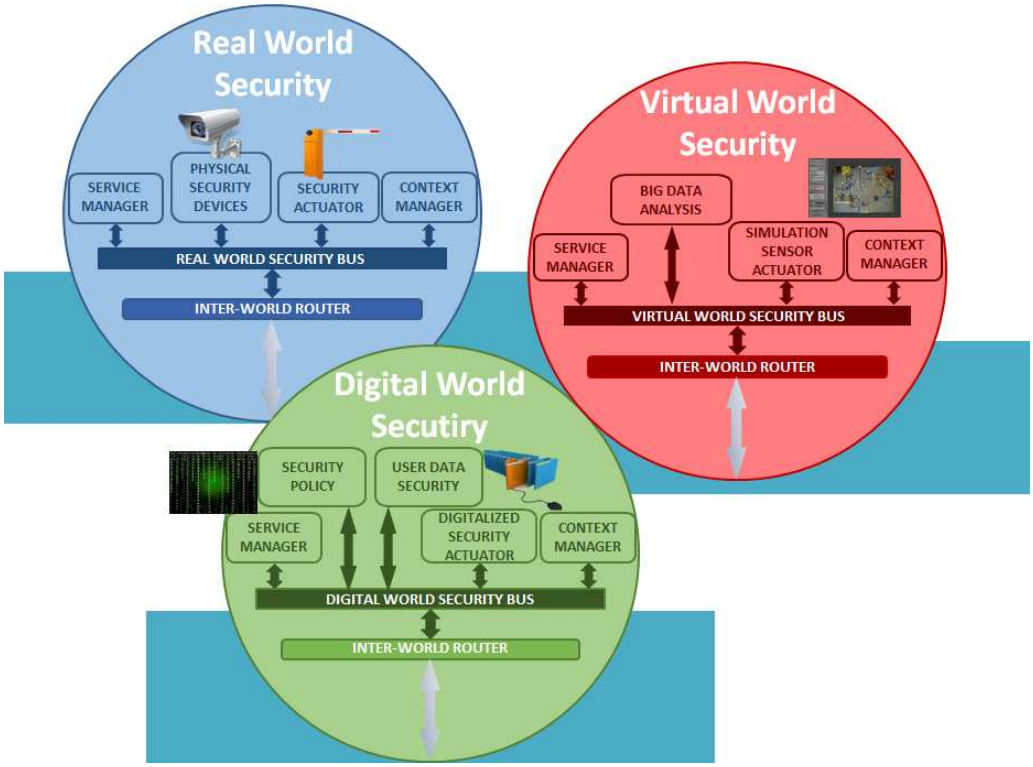

Figure 3: Reference architecture model for "Sensing Access Control"

To enable the materialization of the model for “Sensing Access Control”, it is necessary to define solutions for the multi-domain collection of relevant information (interoperability) in real time, its intelligent processing for AC decision making, and an intelligent actuator system which can respond to the instructions of the system efficiently. ACIO, as shown in Fig.2, has proposed an instantiation of the reference architecture for Sensing Enterprise, a solution that improves the usability of access control without compromising security, by using context information, and synchronization and data exchange between physical and logical world to enable rapid decision-making in the management of multi-domain access control.

In the proposed architecture, the central element (Authorization System), is responsible for the communication bus implementation and also implements access control decision-making in real time through the collection of information from the different worlds (physical and logical). The sources of information from the Sensing Enterprise architecture that the ACIO solution interoperates on are:

- **Identification System (physical)**: Composed by improved physical in-motion identification mechanisms, vehicle identification devices, and container and plate number reading mechanisms (physical perimeter access control).
- **Contextual Information System (logical)**: this system is responsible for the collection, processing and storing of all the contextual information generated, and of ensuring the interoperability and sharing of all information available in order to avoid duplicates or inaccuracies.
- **Terminal’s logical access control system (logical)**: Single-Sign-On authentication of user through a Identity Provider / Service Provider (IdP / SP) model under SAML, and multi-factor authentication based on XACML architecture for distributed environments.
- **Multi-domain security policy Configuration (logical)**: management of security policies and inter-domain SLAs based on context.

- **Data analysis**: Provides multi-source logs standardization and categorization through the use of Big Data analysis techniques, threat detection algorithms, pattern matching and statistical correlation.
- **Geolocation System (logical)**: Advanced positioning for people and good tracking between different domains and port subsections.
- **Actuator System (physical)**: intelligent access control mechanisms with IP connectivity to apply the security actions defined by the authentication server.

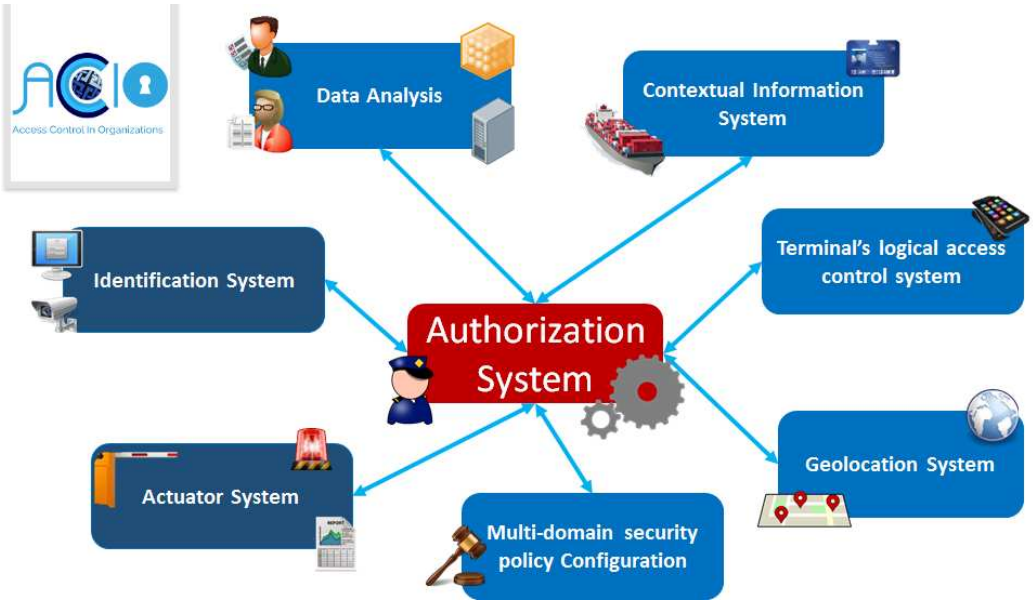

Figure 4: ACIO proposed Access Control Architecture

The proposed architecture is able to provide the following added features to the Access Control management:
- Automate data acquisition (use case: people, goods, vehicles, services).
- Accelerated (muti-domain) cross system and cross platform data exchange.
- Fast & easy (multi-factor) access control policy delegation with traceability.
- Big data context-related segmentation for fast analysis.
- Seamless Physical-digital world cloud-based data exchange management.
- Digital evidence management and auditing.

4. Tests and demonstrators

For the validation of results for the ACIO architecture, a test environment shown in the following figure (figure 3) has been used.

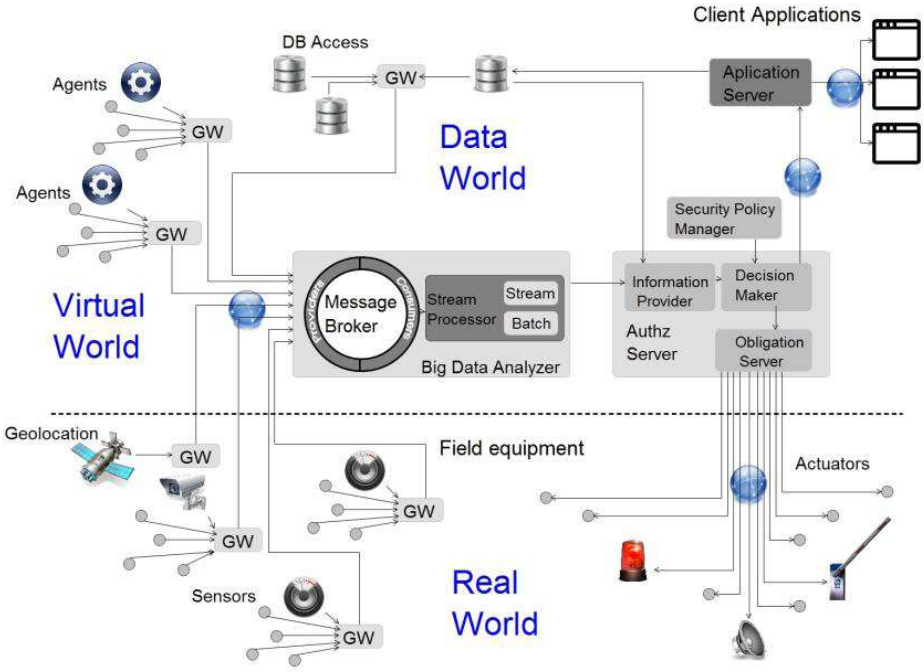

Figure 5: Implementation of the ACIO architecture

In order to validate the ACIO solution in its application to the port of Valencia, the following components are implemented: a gateway (GW), a Kafka (CK) cluster, and a Samza (CS) cluster, which provides data to an information provider, allowing the authorization server to use this information in the process of physical and logical access control in an integrated way.

For the outcome of this validation study, the incoming data is generated directly from the GW, and emulates the receipt and delivery of very large numbers of messages, which could be a base problem for the scalability of the ACIO solution. The GW sends all input data to CK, which is deployed in multiple instances. Once received the requests, the CK puts messages on a queue, which we call topic and will be used by the CS. The CS will then extract the message of a topic based on its policy subscription, performing the processing in cascade through different jobs written in java. The outputs of processing the data stream in the CK are made available to the information provider; that will provide them for the access control process, executed by the authorization server.

The continuous and massive reception of messages from the GW triggers different jobs processing activities, that culminate in the activity and context information required when making access control decisions. The following table (table 1), shows the reception and processing of messages:

Table 1: Reception and processing of messages in the ACIO solution validation deployment

CS transfromation jobs				
	Jobs	Executing instances	Entrance messages (m) per minute	Outgoing messages
Entry	SensorGet	3	429.123	entry x 3

Process	SensorGroup	3	1.287.369	3/min/partion
Ratio	SensorMean	1	9	3/10 min
Tolerance	SensorLimit	1	0,3	3/10 min

Table 2 shows the performance of the proposed system:

Table 2: CPU components performance in the message processing validation implementation

Component	CPU	Available RAM memory
Kafka1 Cluster	35 %	6,46 %
Samza1 Cluster	7 %	3,04 %

Recent measurements on a sensing terminal of the Valencia port environment state a flow of about 8,000 messages / second (m / s).

Through the validation it is found that taking a 35% performance of the deployed cluster in general purpose systems enables the processing of 21,456 m per second, allowing the proposed deployment to process four times the current activity. Therefore, and taking into account the transparent scalability shown by the system, the ACIO solution can be applied in scenarios of growth and evolution under a port like Valencia, which is currently among the ten busiest in Europe in number of containers, and is destined to be one of the top three in terms of movement of people and goods.

4. Conclusions

The ACIO validation tests show that the solution enables integrated and holistic access control in an environment like the Port of Valencia, improving the user experience through the recording of activity and the use of transparent correlation, and all this for the sake of safety, effectiveness and efficiency for port's processes. Moreover, the modularity and scalability of the ACIO solution allows the incorporation, in the required volume and accuracy, of the sensor and actuator systems into the access control management to ensure fluidity.

Acknowledgements

ACIO: Access Control In Organisations, to been co-funded by the Ministry of Industry through the Strategic Action for Digital Economy and Society (AEESD - TSI-100201-2013-50) in 2013 after receiving a CELTIC Plus (C2013 / 1) label by the Eureka cluster and has relied on the work done in the OSMOSE project (GA: 610905) funded by the European Commission through FP7-ICT

References

[1] Ravi S. Sandhu and Pierangela Samarati,: "Access Control: Principle and Practice", IEEE Communications Magazine, vol. 32, no. 9, September 1994, pp. 40-48.

[2] Jason Crampton and Charles Morisset: "Towards a Generic Formal Framework for Access Control", CoRR vol. abs/1204.2342 2012.

[3] Debin Liu,Ninghui Li,XiaoFeng Wang,L. Jean Camp: "Security Risk Management Using Incentives", in Proceeding IEEE Security and Privacy, November 2011, pp.20-28.

[4] Domenico Rotondi, Cristoforo Seccia, Salvatore Piccione: "Access Control and IoT: Capability Based Authorization Access Control System", November 2011.

[5] G. D. Skinner, “Cyber Security Management of Access Controls in Digital Ecosystems and Distributed Environments”, 6th International Conference on Information Technology and Applications (ICITA 2009), November 2009.