2016 IEEE First International Conference on Internet-of-Things Design and Implementation

Sensing enabled capabilities for access control management

IoT as an enabler for the advanced management of access control

Mikel Uriarte, Oscar López, Jordi Blasi
Nextel S.A
Zamudio, SPAIN
{muriarte, olopez, jblasi} @nextel.es

Oscar Lázaro, Alicia González, Iván Prada
Innovalia Association
Bilbao, SPAIN
{olazaro, agonzalez, iprada} @innovalia.org

Eneko Olivares, Carlos E. Palau, Benjamín Molina
Universitat Politecnica de Valencia
Valencia, SPAIN
{enolgor, cpalau, benmomo} @dcom.upv.es

Miguel A. Portugués, Alejandro García
Infoport Valencia S.A
Valencia, SPAIN
{maportugues, agserrano} @infoportvalencia.es

***Abstract*—Current knowledge and assets that support organizations competitiveness must be protected. This protection is highly dependent on a proper access control management. Unfortunately, traditional access control management approaches are rigid and isolated, constrained by proprietary requirements not easily interoperable. In this article, the ACIO framework is presented and described. It provides a flexible, open, fluid and collaborative middleware for building access control management systems, based on the Sensing Enabled Access Control (SEAC) concept. This framework establishes the principles allowing the development of an access control management system that copes with today organization's needs. The paper also provides a description of a real use case raised to validate the framework, as well as the laboratory results supporting its scalability.**

Keywords—Access Control, Security, Sensing, IoT, ACIO, SEAC

I. INTRODUCTION

The new economy, conditioned by the global competence under which organizations are, is strongly based on knowledge and asset management which must be protected from unauthorized access and preserved as key aspects for business continuity and success. Among other security aspects, one initial and relevant step involves access control management, granting access uniquely to right people and systems, both at physical and logical layers.

Access Control (AC) is one of the main strategies for network security prevention and protection. Its main task is to fully share system resources, manage user's access rights and ensure that network resources are not used from unauthorized access. Unfortunately, traditional AC solutions are commonly an obstacle or, at least, are not properly adapted to new technologies such as the enterprise cloud, cloud-based apps, social media, and high-powered mobile devices which offer more ways to access corporate data and therefore more security issues. In the so called Bring Your Own Device (BYOD) era, moving data across various devices and networks increases security risks to the corporate network and may expose sensitive corporate data to leaks and attacks. There are some approaches to reduce risks, such as blacklisting and Bring Your Own Application (BYOA), which separates corporate and personal data on mobile devices using Mobile Application Management (MAM). Even so, security experts still point out that the ability to manage and track corporate data has become more difficult with the adoption of both cloud and mobile storage services in the enterprise. For that reason, nowadays organizations need to go beyond traditional security practices and policies and look at new ways for setting policies, control access and preventing data loss at both the application (logical) and device (physical) levels.

The BYOA concept relates to a partially local concept involving a user and its related company whereas the general perspective is much more complicated as we all currently live in the Internet of Things (IoT), with a huge increase in the use of devices connected to the Internet (e.g. smartphones or smart objects). If multiple companies with different devices have to interact in the IoT, there is a clear problem regarding interoperability for access control information exchange between organisations, which leads to implementing federated access control systems. Different proposals have been addressed to cover such problem; in our design we propose a framework that merges many pieces of information treating some of them as sensor data that serves as input for the required policies. This is called Sensing Enriched Access Control (SEAC) and will be further described in the next sections. The proposed SEAC framework has been tested in the premises of a Critical Infrastructure (CI). CIs are logical/physical facilities that are essential assets in the economy and social well-being of a nation. The testbed described in this paper took place in the city of Valencia, and selected as CI the port, which is the sixth most important one in Europe in terms of container traffic.

978-1-4673-9948-7/16 $31.00 © 2016 IEEE
DOI 10.1109/IoTDI.2015.20

The paper exposes the ACIO (Access Control in Organizations) access control management framework and is structured as follows. First, the concepts of Sensing Enriched Access Control (SEAC) and the role of IoT are introduced and explained. Later on, the ACIO access control management framework is presented. Its main functioning principles, components and characteristics are detailed. Then, a use case which showcases the concept is explained, including the previous deficiencies of the access control management and the proposed solution based in the ACIO framework, going through the advantages provided by the ACIO components and its value for the access control management. Finally, the paper ends with the conclusions reached as well as the future work.

II. THE ACIO FRAMEWORK

The ACIO framework is a compendium of principles, schemes and concepts that guide in the development of an open, flexible, scalable and highly secure and usable access control management system. In this chapter we will describe the Sensing Enriched Access Control concept, the ACIO framework principles and finally the proposed architecture.

A. Sensing Enriched Access Control (SEAC)

Access control principles are stated and immobile; there are three main options to identify an individual into a system: who he is, what he has or what he knows. Examples of these three methods are biometrics (who he is), identity cards (what he has) and secrets, such as user and passwords (what he knows). Current and future improvements in the management of the previous principles will deal therefore with how this information is provided, stored, acquired and processed.

The Internet of Things (IoT) is a concept that deals with the connectivity capabilities enabled in physical objects, making them able to communicate over networks, such as the Internet. Most research carried out, in which security and IoT are present as keywords, deal with security requirements of this type of communications [1] [2]. However, in our previous bibliographic research and to the best of our knowledge the use of networked things contributing to the AC granting process in order to enhance security has not been studied until the moment.

IoT enables the addition of multiple layers of information that can enhance access control decision making, such as presence sensors, biometric readers, productivity monitoring mechanisms, etc. The communication capabilities of such devices open the door to their inclusion as information into the equation of access granting, enabling the merge between two previously isolated management processes, physical and logical access control. This concept of including sensing information gathered through the sensor devices deployed in companies, organizations or CIs is what we have called SEAC (Sensing Enabled Access Control). The idea by itself is not new, as there are context brokers able to gather sensor information; the innovation lies in the applicability to AC.

Under the scope of the SEAC concept, a sensor does not only limit to (physical) devices devoted to measure physical or chemical magnitudes, but it includes any device which can provide useful information, such as user's mobile devices acting as logical devices. SEAC is supported in:

- Physical-Digital world data synchronisation and exchange.
- Multi-domain, context-sensitive seamless access control for fast decision making.

SEAC establishes that access control management has to be a flexible and smart procedure that coherently takes advantage of all potentially useful information sources to increase certainty in decision making, pondering the information sources with respect to their associated (configured) weight for identification and usability of the system. Under the SEAC concept, already deployed information sources have to be analysed and included into the decision making system and additional required identification mechanisms are selected giving priority to usability. The aim is to increase the number of information sources that will not degrade the system's usability instead of deploying highly secure mechanisms that affect severely fluency. The main aim is to keep the same security level but higher fluency and usability.

B. ACIO Framework principles

The ACIO principles are set by the SEAC concept. There are four main principles in the ACIO framework:

- The access control management should be smart; it should learn over time, anticipating risk situations and detect anomalous behaviours or patterns to act accordingly. Note that self-learning and proactive detections have always been key aspects in security management, especially in access control.
- Access Control management must maximize the incorporation of relevant information sources, multiplying the information sources to enrich decision making and the security level of the system, without degrading usability. This relates to a scalable and interoperable module able to integrate any potential information source (sensor in a general sense).
- The incorporation of new information sources must be coherent, weighting in each case its contribution to decision about access granting against complexity of its integration to the system and to the overall processing. Just adding new sources does not necessarily help the decision making process and adds extra complexity; therefore, the relevance of any aggregated source must be previously analysed and given a certain weight on each implied access control policy.
- Decisions for Access granting must be balanced between security and usability, proposing or executing additional actions of control, rather than access decisions which will degrade fluency. The capabilities of new technologies should be seized to complement the access control.

The previous principles promote the development of a flexible and smart access control management system that copes with the current requirements of organizations.

C. *ACIO proposed architecture*

The proposed ACIO architecture searches for a throughput improvement of 2 or 3 times in respect to traditional systems, without major infrastructure investments, providing full traceability of people and assets while preserving and evolving the already implemented legacy systems in case they exist.

The systems developed under the ACIO framework, with a user centred access control management, provide:

- Automated data acquisition.
- Accelerated (multi-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.

Figure 1 shows the generic architecture for an ACIO framework Access Control management system. The main component is the Authorization System (AS), which is responsible for the access control decision-making in real time through the collection of information from the different worlds (physical and logical), as well as for the communication bus implementation among the involved entities and modules. The AS gathers and afterwards processes relevant information from multiple sources in order to provide access granting decisions, generate alerts and trigger concrete control (proactive and reactive) actions. The architecture encompasses the following information sources (see Fig. 1):

- *Identification System*: Composed by physical identification mechanisms, such as biometric sensors, vehicle identification devices, container and plate number reading mechanisms, etc.
- *Contextual Information System*: it is responsible for the collection, processing and storing of all contextual information generated, and of ensuring the interoperability and sharing of all information available in order to avoid duplicates or inaccuracies.
- *Logical access control system*: it involves all logical identification systems that provide digital means of identification: credentials, tokens, digital certificates, etc. are included under this category.
- *Multi-domain security policy Configuration*: this system processes the security policy for all interconnected domains, providing information about how the policy must be applied in each case.
- *Data analysis*: This information source includes all systems capable of the following features: threat detection, pattern matching and statistical correlation. The required data to be processed may come from other modules (e.g. Contextual Information System).
- *Geolocation System (logical)*: it involves systems that provide information about positioning that enable people or objects tracking between different domains and locations.

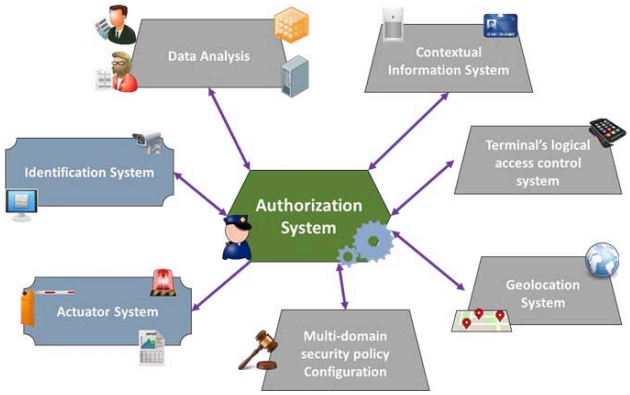

Fig. 1. ACIO framework proposed architecture

Finally, the architecture envisages the existence of a smart actuator system that applies the resulting access granting decisions made by the authorization system.

III. ACIO USE CASE

A specific solution defined under the framework to be implemented in a real world scenario has been used to demonstrate the framework's performance and benefits.

This use case refers to the dependencies of the Port of Valencia. Valencia seaport is an ideal scenario as CI and it encompasses highly complex control requirements both at physical and logical access control level. The port use case provides interaction among a great variety of actors and heterogeneous elements (e.g. containers, machinery, trucks of different operators, etc.). Additionally, there is a high dependency of the port's competitiveness regarding fluidity of the ongoing operations, and the obligation to comply with different rules and national and international legislation all of which set the success indicators for the results. The port premises allocate five container terminals (see Fig. 2) with more than 4000 truck movements and 10000 containers per day. The port operations are management through a PCS (Port Community System) in the cloud, which enables and conducts information exchange among all port actors (port authority, customs, transport companies, etc.), and interacts in a federated way with their systems.

Fig. 2. Valencia Port overview

To set the use case, the first step was to analyse the existing access control to detect deficiencies, strengths and potential improvement points, as well as gathering the port authorities' needs and the facts and figures regarding operations. As result of these evaluations, a number of deficiencies were detected and a solution based on the ACIO framework was analysed and proposed to tackle the previous weaknesses and are listed in Table 1. As can be seen, the use case will enable the evolution from the currently static and inefficient AC management of the port, with consequently low security, to a user centred AC management providing a high security level and high usability which complies with seaports requirements.

TABLE 1. ACIO FRAMEWORK BASED AC MANAGEMENT IMPROVEMENTS

ACIO framework approach in the Valencia Port AC management System		
AC process	***Current AC management system***	***ACIO improvements***
Registration	Repetitive and heavy	Agile process only done once
Identification	Identification of all users is currently not being done as it would affect fluency and does not support mobility	Multifactor, unified and mobile
Authentication	Interacting with the PCS requires multiple checkpoints with their consequent credentials	Cross-domain single-sign-on
Authorization	Current authorization process is slow and does not consider any additional information sources (context)	Transparent decision making and dynamic policy based in context
Accounting	Manual and incomplete	Complete and automated traceability and awareness
Auditing	Poor compliance evidence	Automated governance and compliance evidence

The proof of concept for the ACIO framework has been carried out in two phases. The first phase has been done under laboratory conditions and has been focused on assuring correct component functioning and integration, as well as improvements in scalability issues through extrapolation of results registered by processing power requirements.

For the demonstrations, carried out in the second phase, a test environment depicted in the Figure 3 has been used where the Valencia's specific AC management solution encompasses the following main components: a gateway (GW), a distributed message system based on apache Kafka (CK), and a stream processor based on Apache Samza (CS). The CS 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.

In order to prove the scalability of the solution, incoming data was generated directly from the GW, which emulated the exchange of a vast number of messages allowing the scalability evaluation of the ACIO solution. Therefore, the GW transmits input data to CK, which is deployed through multiple instances. Upon reception of requests the CK orders (classifies) the messages on a specific queue (topic), which will be used by the CS. The CS will, according to its policy subscription configuration, extract the message of a topic and perform cascade style processing through different jobs written in java. After that, the outputs of this processing are made available to the information provider that will also provide them to the access control process executed by the authorization server.

The current measured operations of the Valencia Port, in sensing terminals, state a flow of about 8,000 messages per second (m/s). Validation carried out deploying the cluster in general purpose systems, allowed the processing of 21,456 m/s, four times the current activity, using only 35% performance capacity. Taking into account the transparent elasticity enabled by cloud platforms, the ACIO solution has not only been validated in its deployment in Valencia's port, but in scenarios of similar growth and evolution. Worth mentioning in this sense is that the port of Valencia is the second most important one (after Algeciras Bay) in the Mediterranean see in terms of container traffic.

The final demonstration of the viability of the solutions developed under the ACIO framework is currently ongoing, and encompasses the deployment of a sample ACIO solution in several checkpoints and locations of the port premises to evaluate the systems performance and behaviour under real conditions. The use case will be deployed in 4 locations: (1) North access gate to the port, (2) Container terminal, (3) Cruise terminal and (4) Infoport (IPV) building (one ACIO project partner which is a main IT solution provider to port actors). These locations are showed in Figure 3.

Regarding the logical access control, the demo will show the integration of the solution with Sintraport [3], an IPV application for inland transport management interoperating with the current PCS in the Port of Valencia:

- Companies using Sintraport can send to the PCS all the information related to the vehicle, the cargo, the driver, the load/unload points and even the expected time schedules.
- All this data is sent to the authorization server to manage the policies.
- Companies introducing information for Sintraport will be marked as "secure" if they keep ACIO security policies, as an added value.

Unfortunately, the interaction of the ACIO solution components with the existing systems is unfeasible due to legislation constrains.

ACIO solution will be deployed therefore as an isolated system. Currently, accessing the port requires showing the Valencia port authorization card, a card allocated by the Port Authority of Valencia to the port employees.

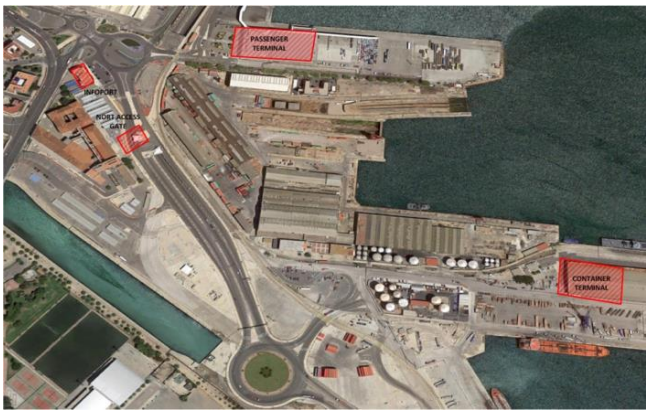

Fig. 3. Locations of the ACIO solution deployment in the Use Case

The main parameters that will be used to evaluate the performance of the ACIO solution will be:

- *Delay*: comparison of time needed by users to surpass checkpoints.
- *Identification*: Number of users identified

The ACIO components selected to be deployed will be:

1) **Sensors deployed**
- In-motion identification enabled by portable smart cameras.
- LPR (License Plate Recognition) camera to identify car plates.
- RFID reader to detect RFID tags that will be allocated in the vehicle to identify both the container and the car plate.
- Smartphone with GPS activated and tracking mobile application installed.
- QR readers for capability based AC deployment.
- Presence detectors.

2) **Network devices and power enablers**
- 4G wireless router and an Ethernet switch for the internet access.
- Power supply element.

3) **Actuators**
- Traffic lights and virtual barriers (microwave, photocells, etc.).

Table shows the expected results for the ACIO solution to be deployed against the current AC system.

A. Use case defined roles

The use cases are based in four main roles acting with the AC system, which will encompass the majority of the cases the port AC system will face:

1) **Visitor***:* This role represents a person who doesn't visit the port frequently. It includes three possible sub-roles:

- *First time visitor*: A person who enters in the port for the first time.
- *External company*: An employee of an external company who needs access to the port area to visit a port company.
- *Passenger*: A person who is going to go on a cruise and has to access the port to go to the cruise terminal.

2) **Habitual visitor***:* This role represents a person who has to access the port area frequently. For example the personnel of the maintenance service: a person in charge of carrying out maintenance tasks within port area.

3) **Employee***:* This role represents a person who, due to his/her job, has to access the port area every day.

4) **Security authority***:* A person who is part of a port security authority.

5) **Port employee***:* A person who works in a company located within the port area.

6) **Truck carrier***:* This role represents a truck driver who must access to the port to load or unload cargo in the terminal.
- Container: The cargo is a container.
- General cargo.

All roles, except employee role, have to register their visit before accessing the port. Depending on the destination, users will be registered in a different Identity Provider.

B. Use case decision making

The ACIO solution will make different decisions related to AC depending on the information received by the different system deployed in each of the locations, the location type, the security policies, etc. For the demonstrator, however, the most relevant parameters to be taken into account for AC decisions are the gathered pieces of information from the deployed AC mechanisms and the location of the access control decision point.

For the scope the use case, and due to the impossibility of taking control of the current actuators deployed in the port, the decisions made by the system will be presented through several visual interfaces. The possible decisions to be taken by the system will be limited for the sake of demonstration fluidity. The outputs of the authentication server regarding the AC decisions will therefore be limited to 4 possible states depending on the information received:

1) **Access granted***:* This means that the person requesting access to the port is known and authorized or unknown but trusted. The system will keep a record of unknown people that will enable identification if a security event is detected.

TABLE 2. ACIO EXPECTED IMPROVEMENTS RESPECT TO THE CURRENT USE CASE AC MANAGEMENT SYSTEM

		Users			Organizations
		Identification time (AVG)		*AuthN&AuthZ adaptive transparent*	*Tracking and auditing*
LOCATION	**USER TYPE**	**No ACIO**	**with ACIO**		
Main Gate	Transporters	30-40"	8-10"	Yes	Yes
	Usual workers	8-10"	3-10"	Yes	Yes
	Outsources and visitors	30-40"	8-10"	Yes	Yes
	Passengers	30-40"	15-40"	Yes	Yes
Terminal	Transporters	25"	8-10"	Yes	Yes
Buildings	Usual workers	5"	3-5"	Yes	Yes
	Outsources and visitors	40-50"	5"	Yes	Yes
Passengers transport	Passengers	NA	NA	Yes	Yes

2) **Manual identification required***:* The system detects suspicious behaviour, untrusted user or other anomalies, and request the Port authority to manually identify the person.

3) ***Grant access but track activity (GEO-RBAC)***: Abnormal events using GEO-RBAC [4] tracking are detected.

4) ***Grant access and send alarm****:* The system will record access requests that present an anomaly but do not seem suspicious (e.g. authorized and expected user in an authorized but not expected vehicle).

5) **Deny Access***:* Finally, blacklisted people will not be permitted to access the port.

IV. CONCLUSION

The validation tests at laboratory level have demonstrated that a solution based in the ACIO framework enables an integrated and holistic access control management in highly demanding environments, assuring the system feasibility even when using general purpose equipment.

Furthermore, the ACIO approach permits the optimization of access control efforts and usability, by proposing the incorporation of additional information sources that contribute to perform consistent decision making for access granting in highly sensor available environments.

The solution deployed will demonstrate that an approach based in the ACIO framework is capable to cope with the current requirements of the most demanding business processes. The authorization server will gather information of the deployed information sources (sensors) and will react to different situations according to the defined actuation protocols (policies). The system is supported by a geo-tracking system, enabled by a mobile application that will serve to add further control capabilities, avoiding fluency operations interruptions or long delays when anomalous situations occur.

However, there is still further research regarding the access control management mechanism. Although the Physical-Digital world data synchronisation & exchange and Multi-domain, context-sensitive seamless access control for fast decision making features that the ACIO framework is capable of providing significant improvements with regard to the existing management systems for access control in organizations, the evolving nature of the IoT concept along with it challenges (security, privacy) and the sensing capabilities that are being incorporated to the "sensing enterprise" requires a deeper analysis and test cases, tracking current advances in the so called industrial IoT [5] where there are various interoperability approaches, as well as associations (Industrial Internet Consortium, Open Interconnect Consortium, IPSO Alliance).

ACKNOWLEDGMENT

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] E. Borgia, "The Internet of Things vision: Key features, applications and open issues", Elsevier Computer Communications, Volume 54, pp.1-31, 1 December 2014,

[2] K. T. Nguyena, M. Laurentb, N. Oualha, "Survey on secure communication protocols for the Internet of Things", Elsevier Ad Hoc Networks, Volume 32, pp.17-31, September 2015

[3] Sintraport, http://www.infoport.es/tag/sintraport/

[4] E. Bertino, B. Catania, M.L. Damiani, and P. Perlasca, "GEO-RBAC: a spatially aware RBAC", Proc. ACM symposium on Access control models and technologies, pp.29-37, New York, USA, 2005

[5] J. Eliasson, J. Delsing, et al., "Towards industrial Internet of Things: An efficient and interoperable communication framework," Proc. IEEE International Conference on Industrial Technology (ICIT), pp.2198-2204, 17-19 March 2015

[6] B. Molina, C.E. Palau, G. Fortino, A. Guerrieri, C. Savaglio, "Empowering smart cities through interoperable Sensor Network Enablers", Proc. IEEE Int. Conf. on Systems, Man and Cibernetics, pp.7-12, San Diego, USA, 5-8 October 2014

[7] G. Fortino, A. Guerrieri, W. Russo, "Agent-oriented smart objects development", Proc. IEEE Int. Conf. Computer Supporter Cooperative Work in Design, pp907-912, Wuhan, China, 23-25 May 2012