
# UNIVERSIDAD DE MURCIA

## FACULTAD DE INFORMÁTICA

Managing Access Control Systems in Distributed Environments with Dynamic Asset Protection

Gestión de Sistemas de Control de Acceso en Ambientes Distribuidos Orientada a la Protección Dinámica de Activos de Información

**D. Daniel Orlando Díaz López**

**2015**

The following Thesis is a compilation of the next published articles, being the PhD student the main author in all of them:

1. Daniel Díaz-López, Ginés Dólera-Tormo, Félix Gómez-Mármol, Gregorio Martínez-Pérez, "Managing XACML systems in distributed environments through Meta-Policies", Computers & Security, Volume 48, February 2015, Pages 92-115, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2014.10.004

2. Daniel Díaz-López, Ginés Dólera-Tormo, Félix Gómez-Mármol, Gregorio Martínez-Pérez, "Dynamic counter-measures for risk-based access control systems: An evolutive approach", Future Generation Computer Systems, Available online 12 November 2014, ISSN 0167-739X, http://dx.doi.org/10.1016/j.future.2014.10.012

3. Daniel Díaz-López, Ginés Dólera-Tormo, Félix Gómez-Mármol, Jose M. Alcaraz-Calero, Gregorio Martínez-Pérez, "Live digital, remember digital: State of the art and research challenges", Computers & Electrical Engineering, Volume 40, Issue 1, January 2014, Pages 109-120, ISSN 0045-7906, http://dx.doi.org/10.1016/j.compeleceng.2013.11.008

# Table of Contents

# Acknowledgements

During the development of this PhD thesis, a set of very good opportunities and circumstances have converged, that with no doubt deserve now and always a sincere and special acknowledgement.

First, I must thank my thesis advisors, Félix and Gregorio, because they have always accompanied me, even before starting this doctoral route when I was a master student in the University of Murcia, full of inquiries but also with a big excitement about getting satisfactory results in the research route. It has been, Félix and Gregorio, who have supported me from the beginning with words of wisdom, right advices, constructive comments, understanding attitudes and strict revisions. Thanks to Félix for his honest friendship and understanding, which have allowed me to express myself freely and receive the best of him. Thanks to Gregorio for his guidance and wisdom, which have given me always the clarity in the hard times. Thanks Félix and Gregorio for everything, you are an example of professionals and human beings.

The route in researching could not start without the support of the Fundación Carolina (FC) who, through its scholarship program for Latin America countries, allowed me to study the MSc on New Technologies in Computer Science in the University of Murcia, which later enabled me to be part of the PhD program in Computer Science. In these beginnings I was also with great people: Neto, Gabriela, Andy, Edgar, Esther, Amir, James, David, Lingshuang, Susana, Monika and Robert. For all this, I will always be grateful with the FC and with all these friends who were my family during my study time in Spain.

During these doctoral years, I have also known very valuable persons that with no doubt have contributed in different ways to the construction of this thesis's results. During my internship at NLE I must mention Mohammed, Surendran, Arnau, Antonio, Ginés, Ricardo, Joao, Nader, Stavros, Carlos, Leyre and Raihan, among many others, who were always very good friends and office mates. These people were a big support and helped me significantly to have a productive and nice study time in Germany.

In the last years, I had the chance to work in Colombia together with Gary, friend and former coach, to whom I thank as he allowed me to learn about the aspects of the consultancy and the project management, points that have contributed in some way to improve this PhD thesis.

Finally, I thank immensely my family (Orlando, María Eugenia, Stella, Juan Diego y Diana), who have always been with me, supporting my decisions, and giving me the affection and support required to go forward. I also remember and thank a lot the people who are with me in a spiritual way because they are not physically present, especially to my grandmother Delia who passed away before I came back home.

En el desarrollo de esta tesis doctoral han convergido un conjunto de muy buenas oportunidades y circunstancias, que sin duda merecen ahora y siempre un especial y sincero reconocimiento.

Primero debo agradecer a mis directores de tesis, Félix y Gregorio, porque han estado siempre conmigo incluso desde antes de comenzar este camino doctoral cuando aún me perfilaba como estudiante de máster en la Universidad de Murcia, lleno de inquietudes pero también con mucha ilusión en conseguir resultados satisfactorios en la ruta de la investigación. Han sido Félix y Gregorio quienes me han apoyado desde un principio con palabras sabias, consejos acertados, comentarios constructivos, actitudes comprensivas y revisiones exigentes. Muchas gracias a Félix por su amistad sincera y entendimiento que me han permitido siempre expresarme y recibir lo mejor de él. Muchas gracias a Gregorio por su dirección y sabiduría, que han dado siempre la claridad en los momentos de dificultad. Muchas gracias Félix y Gregorio por tanto, son ustedes un ejemplo de profesionales y de seres humanos.

El camino en la investigación no pudo haber comenzado sin el apoyo de la Fundación Carolina (FC), quien mediante su programa de becas para países iberoamericanos, me permitió realizar el Máster en Nuevas Tecnologías en Informática en la Universidad de Murcia, el cual posteriormente me permitió aspirar a ser parte del programa de Doctorado en Informática. En estos comienzos también estuve rodeado de grandes personas: Neto, Gabriela, Andy, Edgar, Esther, Amir, James, David, Lingshuang, Susana, Monika y Robert. Por ello tendré siempre gratitud hacia la FC y hacia todos aquellos amigos que fueron mi familia durante mi tiempo de estudio en España.

A lo largo de estos años de formación doctoral también he conocido a personas muy valiosas que sin duda han aportado en diferentes ámbitos a la construcción de los resultados de esta tesis. Durante mi estancia en NLE debo mencionar a Mohammed, Surendran, Arnau, Antonio, Ginés, Ricardo, Joao, Nader, Stavros, Carlos, Leyre and Raihan, entre muchos otros, que fueron siempre muy buenos amigos y compañeros. Fueron estas personas un gran apoyo y me ayudaron en gran medida a pasar un productivo y agradable tiempo de estudio en Alemania.

En los últimos años también tuve la oportunidad de trabajar en Colombia en conjunto con Gary, amigo y antiguo jefe, con quien hemos estado en diferentes iniciativas y a quien agradezco haberme permitido aprender de las cuestiones de la consultoría y la gerencia de proyectos, aspectos que han aportado en alguna forma a enriquecer esta tesis doctoral.

Finalmente, agradezco enormemente a mi familia (Orlando, María Eugenia, Stella, Juan Diego y Diana), que siempre han estado conmigo, apoyando mis decisiones y dándome siempre el afecto y soporte necesario para seguir adelante. También recuerdo y agradezco mucho a todos quienes están en espíritu conmigo porque físicamente ya no se encuentran, especialmente a mi abuela Delia quien partió antes de mi regreso a casa.

**Abstract**

# I Motivation and Goals

Access control can be defined as:

> "A process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy." [1]

The access control process mentioned in the previous definition is developed around the concept of "asset" [2] which is a component of an information system that, due to its value, it can be attacked producing an undesired consequence for the organization owing such asset. "Assets" include information, services, software, hardware, facilities and personnel, among others. "Resources" and "entities" are also assets. The asset valuation is the determination of the loss of value for the organization caused by an incident over the asset [3] and it can consider the following aspects in the valuation process: replacement cost for acquisition or installation, labor cost invested in recovering, loss of income, loss of capacity to operate, legal penalties, operative injuries, environmental damage and image and reputation affectations, among others. In this context, a well defined access control process is essential to guarantee authorized accesses which in turn allow assets security and business operability, known in the literature as balance between security and utility [4, 5].

Going a step forward and considering the application of an access control process in the field of online services (like order management, information query, payment, inventory management, data analysis, campaign management, and other services), it is possible to better emphasize the relevance of the access control, mainly because of the attention deserved by the "valuable commodity" that is behind most of these services, i.e. the information (which is an "asset" whose utilization is regulated by the access control process). Information is effectively a key element in organizations, since an accurate, safe and available information can make the difference in successful business operations and even define the business continuity.

In order to apply an access control process to regulate privileges over assets, some access control models exist nowadays [6], each one with different complexity and features, for example: access control list (ACL), role-based access control (RBAC), attribute-based access control (ABAC), policy-based access control (PBAC) and risk-adaptable access control (RAdAC). These access control models are in charge of processing access control requests and generate authorizations decisions. The benefits of each model make some of them more appropriate for some situations than others.

Generally, one or more models can be applied in one single security domain. A security domain is conformed by components (applications, modules, servers, resources, networks, persons, etc) complying and sharing the same security configuration (commonly expressed in the form of security policies) [7]. The concept of security domain can be applied in an organizational context where a company or a department can be seen as single domains, but also in a technical model, like in an architecture for cloud computing, where there are network, service and storage security domains [8].

Considering the interaction between organizations for business or technical reasons, like the establishment of association, consortium or partnership relations, and additionally the existence of shared assets, like the ones used in composition of services, it is prevailing to think over the interaction between different security domains to get joint authorization decisions. This context of multiple security domains using and sharing assets, and exchanging security assertions, sets up a distributed environment which brings two challenges in the context of access control policies management: 1) The need to propose mechanisms to allow the composition of access control policies from different organizations in order to achieve a right authorization decisions making, and 2) The need to take into account privacy, confidentiality and autonomy requirements into the authorization decisions making process.

Thus, one of our main goals in this PhD thesis is to tackle the access control policies management in a distributed environment considering the previous academic proposals, the practical requirements that organizations manifest nowadays and the forthcoming needs according to new technologies and business models.

On the other side, formal security reports based on real security incidents issued by different organizations, confirm the impact caused by different data breach events. One of the most respectable security reports is the Data Breach Investigation Report (DBIR) from Verizon [9], which has an annual periodicity and is built up with the reports of security incidents from 70 global organizations from 61 countries. These organizations belong to some of the following groups: CSIRTS (Computer Security Incident Response Teams), Cyber Centers, Forensic providers, Infosec product and service providers, ISACS (Information Sharing & Analysis Center), Law Enforcement Agencies and others. This annual report allows us to better understand the access control process from the perspective of the data breaches and gives us some insightful facts:

- Three different types of actors (or entities) can be considered as authors of data breaches: 1) Internal, 2) External and 3) Partners. Since 2007, data breaches provoked by external authors represent the highest percentage of occurrences compared with the other two actors, having variations from year to year (in 2007 data breaches provoked by external actors represented 39%, but in 2013 it reached up to 89% and in 2014 it got 84,69% of all the occurrences). This situation evidences the special attention that security managers have to put on enforcing the access to data that can be reached by external actors, not underestimating that internal users and partners still represent a non-negligible source of threats. Actually, due to the existence of a certain level of trust with internal and partner actors, data breaches provoked by these actors can have a higher impact than those provoked by external actors and even these data breaches can be more difficult to detect and hold back.

- The top three goals for a data breach are: 1) Financial, 2) Espionage and 3) Ideology/Fun. Espionage has specially increased in the last years raising from 6.8% in 2010 to 17,2% in 2013. However, financial reasons keep along all the time the highest percent value, being 89.1% in 2010 and 66.5% in 2013. The most recent DBIR report [9] does not include the percentages for the goals behind the data breaches, however it does indicate that in 2014

the financial reason was the main motivation for phishing, crimeware, web app attacks and insider misuse (mainly privilege abuse) incidents. These values suggest us that in order to identify the threats for an asset it is necessary to think over all the possible interests (any type) that the asset can appeal, and therefore the access control process should include all these factors as key elements to define an authorization decision.

- From the asset categories considered in DBIR (Server, User devices, Kiosk, Person, Media, Network), which are potential targets of an attack aiming to produce a data breach, it is the "server category" the one which generally gets the highest percentage of attacks, being 44,5% for 2013, followed by "user devices" category with 20.8% and "person" with 15.95% of the attacks. This is understandable since "servers" host most of the business data and therefore they constitute the most attractive target in an attack. However, user devices constitute an important percentage of the attacks due to the popularization of connected personal devices, like smartphones, laptops or tablets, that represent a path to access personal data and even a small window to access critical information systems. The most recent DBIR report [9] does not include the percentages of attacks for each asset category in 2014, however it indicates that 70% of the attacks included a secondary victim, which is a compromised "server" used in a DoS (Denial of Service) attack, host malware or phishing. A secondary victim is an asset that is compromised by an attacker as a way to achieve a different attack against another victim. This emphasize the fact that "server category" keeps the highest percentage of attacks in 2014. In any case, it is a fact that an efficient access control process should offer protection to data regardless of the device over which it is hosted.

- From all different kinds of incidents considered in the DBIR report, it is important to stand out "insider and privilege misuse", which corresponds to an unapproved or malicious use of organizational resources, which can be originated by any of the actors (entities): insiders, outsiders (by collusion) or partners. This incident can be caused by different threat actions, but according to the reports 88% in 2013 and 55% in 2014 of the initiators of this incident are the "privilege abuse actions", that is to say, using some granted privileges (due to an employee or partner relationship) to commit evil acts. This percentage suggests that even if a security policy has been initially defined in a right way, this has to be reviewed constantly to keep it aligned to the changes in the environment, referring specifically to changes in the trust relationships, suspicions of resource misuse, abnormal behaviors in the actors, etc.

As we can see, there are many challenges around the generation of authentication and authorization decisions nowadays reflected in security incidents, which in real situations are not easily addressed due to the quantity and complexity of the variables to take into account (e.g. kind of actors in the environment, possible data breach motivations, different asset categories, different threat actions, impact of the data breach, criticality of the asset, trust between partners, etc). This previous context engenders another goal within this PhD thesis that is to provide a dynamic asset protection which can be achieved with an improvement to the access control process, aiming to make it more effective facing security information threats, and more appropriated for a context exposed to different security risks.

Getting closer to the user's perspective, a big amount of data is captured daily through our personal interactions with ICT devices or applications in general, building up the idea that each one of us has a "digital life". This historical data could be stored, processed and subsequently accessed for different kind of purposes like: productive, healthy, legal or entertainment, just to mention some of them. However, in order to take the most of this personal data, different issues

around security and privacy must be solved before the overcrowding of this kind of "live digital" services. An access control process also takes relevance in this kind of systems as it should ensure that only authorized users/applications access certain types of personal data based on restrictions defined by the data owner.

Finally, all of the previous situations make the access control systems an important research topic, over which the research community is working on and which was specifically supported in the eighth edition of the framework program for research and technological development "Horizon 2020" from the European Union [10]. The access control topic has been considered inside the "secure societies" challenge, which is focused in the protection of citizens, society, economy, European assets, infrastructure and services [11].

Additionally, the Science and Technology Directorate from the Department of Homeland Security of USA, which is a department constituted in 2003 after the attacks of September 11, 2001, has also defined its own strategic directions in order to protect critical assets. Between these directions there are two specially related to the subject of this thesis: "Trusted Cyber Future: Protecting Privacy, Commerce, and Community" and "Enable the Decision Maker: Actionable Information at the Speed of Thought" [12]. The first of them embraces the idea of a self-detecting, self-protecting and self-healing infrastructure in order to guarantee a trusted cyber space. The second one aims to incorporate risk analysis and modelling systems to enable a decisions making process with the required information.

Also, the National Institute of Standards and Technology (NIST) from USA has also published the Framework for Improving Critical Infrastructure Cybersecurity [13], which emerged through the executive order 13636 in the policy of the United States of America to enhance the security and resilience of the national critical infrastructures. This framework has as purpose the definition of standards and best practices to help American organizations to handle security risks. Inside this framework, access control and risk management have a special place in the development of protection as a core function.

Previous statements define the access control as an important research topic over which public and private (including academy) sectors are working on in order to use it as a key element in the assets protection. Assets protection is a main component to achieve a proper risk management that enables the securing of the current and future cyber space.

Thus, the main goal in this PhD Thesis is to develop proposals for the management of access control systems using innovative elements and pursuing its applicability in real scenarios which are distinguished for having a noticeable authorization component. In the same way, the specific goals of this Thesis, which are closely related with the previously presented main goal, are defined below:

- Study existing designs of access control systems, identifying their main limitations when applied to multiple security domains with shared assets (i.e. distributed environments).
- Propose a solution for an effective policy management in distributed environments which allows security domains to maintain certain autonomy and confidentiality.
- Achieve an innovative access control process to assets which considers the security risks as part of the authorization context.
- Propose a solution aimed to mitigate security risks in assets in a reasonable time frame and considering the security objectives of an organization.
- Identify security and privacy challenges through the analysis of existing solutions in the area of live digital systems.

- Propose an architecture to support live digital systems with a prevailing data security and privacy approach and with the possibility to apply results obtained in previous objectives.

# II Methodology

This PhD Thesis has been elaborated as a result of different internships in R&D (Research and Development) and industrial sectors within the area of information security, mainly at NLE (NEC Laboratories Europe) in Germany, with a continuous guidance from the Department of Information and Communications Engineering (DIIC) of the University of Murcia in Spain. The outcomes produced along all these internships were depurated and revised in detail from a research and industrial perspective, driving to the consolidation of research papers published in JCR journals. Thus, the methodology described next corresponds to the set of processes and activities developed to reach a publications compilation thesis.

Research activities around this thesis started with a research internship at NLE, where a first contact with real authentication and authorization engines was facilitated, allowing us to identify and analyze all the complexity behind an access control process. As a result of this approach, different improvements were proposed and developed over the XACML engine hold at NLE, most of them related with the PDP (Policy Decision Point) module, in order to make the composition of authorization decisions, and with the PAP (Policy Administration Point) module, in order to manage efficiently all the set of security policies. These initial labors allowed us to tackle partially one of the specific goals of the thesis around studying existing designs of access control systems.

Working over these mentioned improvements to the XACML engine of NLE, some inquiries and ideas emerged on how to translate the functionalities of an authentication and authorization engine to a distributed and collaborative environment, like the one composed by different business units (different organizations or branches of the same organization) each one constituting an independent security domain. Consequently, an architecture to manage access control policies in distributed environments was proposed and developed (Chapter 1), which considered and resolved different aspects related to the communication between parties, the management of access control policies and the securing of the communications. With this proposal we could establish a model based on operations to manage policies (diffuse, update, delete, etc.) within a distributed context in a simple and integrated way, which can be extended or adapted to support new management operations. This proposal was widely revised and analyzed by different researchers, helping to improve and tune up different aspects of the proposal until reaching a consistent and robust solution.

After the development of the previous architecture oriented to an efficient management of access control systems, a new opportunity of research appeared focused on algorithms that could help in the process of finding the appropriate authorization decision to regulate the access to an asset, but also to contribute to mitigate an identified security risk. Thus, another research internship was developed at NLE in order to develop the idea of using authorization decisions influenced by a measured risk to achieve a dynamic asset protection. Searching about different ways to manage the security risk, we got involved in RAdAC (Risk-Adaptable Access Control) systems [14] and we discovered that in fact no existing proposals around the inclusion of the security risks in the process of determination of an authorization decision had considered evolutive algorithms.

A small access control system that regulates access to a few assets can consider the different risk level changes associated to them, and for each risk level change, it can generate manually a security control to protect the resource and in this way allow a secure access. However, in medium or large access control systems the big amount of resources and the potential risk level changes

associated to them make unfeasible to react manually to each situation in order to guarantee the access and mitigate correctly the risk through a set of applicable counter-measures. Additionally, this context of medium/large scale access control systems generally contains multiple resources, subjects, actions and environment variables, that must be considered in the process of building an authorization decision. We agreed that this previous dynamic and multi-variable context represented an adequate space to apply a solution based on evolutive algorithms that allows us to find the best set of counter-measures applicable for a specific authorization context in an acceptable time.

While the development of this idea about the application of evolutive algorithms to compute authorization decisions was progressing, an opportunity to be part of a project of design of an Information Security Management System (ISMS) under the standard ISO 27001 [15] arose. This project was developed within a stage at CINTEL (ICT Research and Development Center) which is a Technology Development Center of the industry of Information and Communication Technologies in Colombia. The ISMS design was done for a public sector company and had as scope the development of all the planning and doing phase according to the Deming cycle. The Deming cycle is a continuous improvement model related to different management systems which defines the following four steps: Planning, Doing, Checking and Acting. This project allowed us to understand the security of information as a process inside the organizations and see how such security has been addressed through different good practices and standards in order to fit a generic requirements that allow to establish, implement, maintain and improve an ISMS inside the context of an organization.

One of the requirements for an ISMS is to hold an information security risk assessment process which can be addressed by the principles described in the standard ISO/IEC 27005 [16]. The information security risk assessment process must define criteria to assess and manage security risks, establish a way to identify them and analyze them according to the impact and the probability of occurrence. Also, for the identified security risks the organization must establish a reasonable treatment according to security controls, which are also named counter-measures. All of these inputs from an applied security project, achieved through the internship at CINTEL, allowed us to improve considerably our initial idea about the application of evolutive algorithms to compute authorization decisions, but now considering the risk assessment process inside the organizations.

It was in this way that we defined a proposal for the adoption of dynamic counter-measures changing along time to face variations in the measured risk level for every resource, based on genetic algorithms (Chapter 2). This proposal was developed aiming to fulfill the requirements of an ISMS regarding assessment and treatment of security risks. The risk management is achieved through outputs from our model which considers the acceptable risk level defined for the assets, so the assets do not get exposed or overprotected. A risk management methodology addressed by the principles described in the standard ISO/IEC 27005 [16] can also be integrated into the proposed model.

After tackling situations of management of access control policies in distributed environments and access control systems with ability to respond dynamically with counter-measures against a detected threat, we decided to go forward a situation more in the user domain where access control systems could represent a key element to guarantee security and privacy. To this end, we explored the state of the art and challenges of live digital systems (i.e. systems with the ability of gathering, organizing, storing and visualizing data associated to the digital fingerprint that users have on all the IT devices with which they interact).

The live digital systems require the interaction and coordination of different components between endpoint devices, applications, service providers, processing services, identity and storage providers, among others, which set up a distributed environment. This distributed environment

can be composed of different security domains interacting, where the most prevailing shared asset is the user information. In this way, an access control model which allows to regulate the access to this asset in a distributed environment is clearly a need. Thus, we found in live digital systems a context where it could be possible to apply the results of our model detailed previously in Chapter 1. Additionally, it is predictable that due to the personal information that is processed in live digital systems, these systems will be exposed to different kind of security threats. Also, the big number of assets (all the data belonging to users) and the risk changes affecting them, bring the fact that live digital systems would be an interesting space to deploy a solution like the one proposed in Chapter 2, which contributes an access control system providing a dynamic asset protection.

The output of the research around live digital systems consisted of a complete revision of works that could have an approach to live digital systems and a study of the architecture of these systems in order to find existing functionalities and shortcomings. Then, we made an abstraction of the steps behind a live digital system and an identification of different challenges around the development of these steps. A special collection of challenges related to security and privacy, including access control aspects, was also determined. These findings of state of the art and challenges helped us to propose a Client/Server architecture which could incorporate the required modules and components to develop a live digital system able to deliver a secure and private service (Chapter 3).

## III Results

The first results of this PhD Thesis are detailed in the paper "Managing XACML systems in distributed environments through Meta-Policies" [17], which was published in the Elsevier Computers & Security journal. This paper makes an extension of the already-known functionalities of an access control system working for one security domain, toward a context composed of multiple security domains (and therefore multiple access control systems) which need to be coordinated in order to resolve appropriately all the authorization requests. This coordination implies the existence of a trust relationship between security domains, which enables them to interact and exchange security information. A context of multiple security domains can be easily found in real life if we consider the concept of shared assets, which suggests that all the related owners of an asset should agree with the use that the asset will have. This is applicable to the situation of virtualization services which are usually composed of multiple service providers, each one of them delivering a specific component of the whole service. Another common example of a context of multiple domains regulating an asset could be organizations with a main office and some branches or subsidiaries, which have to share resources amongst them, but each of them in fact constitutes an independent office and therefore can set their own security policies over their assets.

The work presented in [17] proposes an architecture to manage access control policies in distributed environments, which considers and resolves different aspects like: i) A proposal of communication strategy between security domains through the use of key elements on both sides of the communication (Master and Slave Policy Administration Points), ii) The utilization of a element called "Meta-Policy" to regulate the privileges over access control policies and enforce an acceptable use of them, whereby the access control policies become the managed resource themselves, iii) The provision of a security mechanism through the SAML protocol to protect the transmission of policies management messages between security domains.

This paper [17] offers a clear perspective about how different XACML access control systems can interact in a secure way, offering low overhead for situations where there is a high number of authorization requests that have to be resolved considering more than one contributor to the

decision. Additionally, in [17] the XACML architecture was reused with the aim of managing privileges over distributed policies (known as Meta-Policies inside the paper), allowing to save time and effort in implementation and deployment of a new access control architecture designed for this purpose. Finally, it is worth to mention that through the expressiveness of XACML it is possible to properly define privileges and guarantee the privacy and confidentiality of policies and attributes in each security domain.

After the previous development of an architecture to manage XACML systems in distributed environments, we put our attention on situations where the definition of an authorization decision must include the security risk over the asset as a key factor (as denoted later in [18]). This inclusion constitutes a big challenge to the access control process since the security risk is variable and therefore the authorization decisions coming from the access control process must also change to be aligned with the variations in the risk.

Thus, we developed a proposal of adoption of dynamic counter-measures changing along time to face variations in the risk level of every resource [18]. This model generates sets of customizable counter-measures taking into account factors (attributes) relevant for a kind of asset and for a specific risk level. With this proposal there are two main benefits, namely: i) Application of a risk management process to guarantee a dynamic asset protection and ii) Management of privileges over assets through an access control system. The counter-measures provide the protection to the asset in order to mitigate the security risk, and can be integrated in different parts of an access control policy: target, condition or obligation.

Furthermore, considering a set of threats and security controls, and the capacity of the proposed method to generate the best candidate solutions in acceptable times, the solution presented in [18] also allows to react to concurrent risk situations that represent variations of the risk level avoiding delays in responses aiming to protect dynamically assets without requiring manual intervention.

The elaboration and testing of this proposal was reported in the paper "Dynamic counter-measures for risk-based access control systems: An evolutive approach" [18], published in the Elsevier Future Generation Computer Systems journal. Behind the proposal there is a genetic algorithm to find the optimal set of counter-measures applicable for a very specific situation of security risk, probability of threat occurrence, impact of a successful attack and effectiveness of the security controls to protect the assets of an organization. An implementation of the proposal was conducted and tested using different values of security controls effectiveness and security risk level.

Finally, our last step in the research route was to analyze and explore from a security perspective an innovative and promising area related to the use of personal information. Additionally, we were interested in an area where we could take benefit of the experience developed through the previous outputs from this thesis. This area was the live digital systems, which will be considerably boosted by the Internet of Thing tendency. All the challenges identified from live digital systems, along with a Client/Server architecture were proposed and described in the paper "Live digital, remember digital: State of the art and research challenges" [19], published in the Elsevier Computers and Electrical Engineering journal.

In [19] a complete comparison of tools to manage personal information is conducted, and it is used as input to identify which features must be present in a live digital system in order to be a service which effectively allows to recover any digital event occurred in the past. These wished features are presented as common challenges for all the live digital systems and they refer to recalling, navigating, searching, sharing, organizing, filtering, auditing and visualizing events. Additionally, a set of challenges specifically related to security and privacy were identified and described in [19]. Considering the context of live digital systems, we believe that the proposals developed previously in this PhD Thesis ([18] and [17]), allow to face certain challenges described

in [19], specifically: selective-access, selective-gathering, transversal security and privacy and assurance of technological infrastructure, among others.

The selective-access challenge states that access to user data should be regulated in a fine-grained way according to the permissions defined by the data owner. The selective-access actually constitutes a challenge since in the context of live digital systems some elements in the server side (service providers, processing services, identity and storage providers) conform a distributed context where user data are accessed by many parties, standing out the need of an effective access control model which regulates the access. In order to support this selective-access challenge the access control model proposed in [18] can be used as baseline, as it would allow the data owner to manage certain access control policies in the infrastructure of the data stores referring to its own data. One example is the diffusion of access control policies toward the data stores reflecting the access and utilization permissions defined by the data owner.

On the other hand, the selective-gathering challenge refers to the ability to define what kind of data can be gathered by a specific application or device in a live digital system. Considering that each application or device used in the gathering of interactions can conform a security domain, it is possible to pose the fact that the data owner could manage some access control policies in the gathering-involved security domains, in order to manage what kind of data are gathered and processed. In this case, a proposal like the one indicated in [18] can be used as a starting point to allow an effective control over the gathering process. The utilization of a solution like the one mentioned in [18] to resolve access and gathering challenges brings also the benefit that the process of determining authorization decisions will consider the data owner policies as a key input.

The transversal security and privacy challenge focuses on providing security and privacy along all the activities involved in the gathering, storing, processing, indexing and visualizing processes of user information. And secondly, the assurance of technological infrastructure challenge aims to face possible security threats over services and physical infrastructure. Both these challenges can be addressed from a risk management perspective since security conditions of the processes involved in a live digital system and security conditions of services and technological infrastructure are exposed to changing risk conditions. Inside the processes involved in live digital systems many entities can participate, whose trust relation can be redefined constantly affecting the operation from a security perspective. Additionally, the services and the physical infrastructure are exposed to a big amount of external threats which are evolving and which require an internal adjustment of the live digital system settings in order to face them. Additionally, it is presumable that the value of the assets will be also variable depending on the kind of personal information. Therefore, the security controls used to protect the information should also be adjusted to all these changing situations.

In this way, a risk management perspective is useful in the context of a live digital system to face these two challenges, reacting with a set of counter-measures according to the value of criticality of the asset, the probability of occurrence of a threat and the current security controls. Considering the above, the proposal described in [17] offers effectively a risk-adaptable access control system which has the ability to react to changing contexts with a set of counter-measures to face risk variations. A proper set of counter-measures allows to mitigate an identified risk and guarantees that the live digital system operation is being conduced properly and the user information is treated accordingly. The information treatment should be aligned with the security requirements of the information owner, the current regulation (specifically related to privacy) and the business security objectives.

Turning back again to the results included in [19], an architecture supporting the functionalities formerly identified in that paper was also proposed. This architecture describes all the main elements in the server and client side needed to support a secure service. The components

in the client side cover two main functionalities, some components associated to the gathering, filtering and encryption of interactions, and others related to the searching, recovering and decryption of the stored information. On the other hand, the components in the server side cover functionalities associated to the reception, organization and storing of encrypted interactions, and also recovering and delivering query results.

Additionally, the proposed architecture in [19] has been thought to be able to support different kinds of services, endpoint technologies, storage mechanisms and interaction with other service or identity providers. As a practical case, a health care situation was presented to show the potential of this kind of solutions, provided that the access control mechanism guarantees the security and privacy of the data.

# IV Conclusions and Future works

Today more than ever "information" becomes a key element within our society, being essential in different areas like social, cultural, economic and politics. It is information and communication technologies (ICT) which mainly ease all the activities related to information, like creation, modification, distribution and sharing, among others.

In the path to build a real "information society" there are many obstacles to overcome, being security of information one of the most important ones. And as a key element of security of information we can highlight the "access control process", as it has the mission of managing the access and the privileges for the assets (including information). In fact, a well thought-out access control process can contribute significantly to the success of an "information society".

Bearing in mind that the access control process is a highly critical component, this PhD Thesis addresses the challenge of defining proposals for the management of access control systems pursuing its later applicability in real scenarios which incorporate authorization processes. In this way, this PhD Thesis addresses some of the most vital challenges around, like the extension of access control policies to more than one security domain (a distributed environment), the dynamic management of security risks through an access control engine which provides privileges management and suitable protection over the assets, and the proposition of an architecture able to support a system with high volumes of personal data to be protected by an advanced access control system.

Our proposal for managing XACML systems in distributed environments through Meta-Policies [17] offers a set of administration operations, which combined with a set of well defined Meta-Policies, allows to have a distributed environment with many access control engines performing communication and coordination between them. We believe this proposal can be used as a foundation to future implementations of distributed access control engines.

On the other side, the work done in this PhD Thesis with the proposal of dynamic countermeasures integrated in risk-adaptable access control systems [18] definitely provides an alternative to handle the security risks, since it considers the nature of the risk (i.e. its dynamism) and integrates this feature in the process of making authorization decisions. This proposal additionally integrates effectively an access control system in an ISMS (Information Security Management System), giving a practical application of the solution and definitively putting on the scene an opportunity to implement it as part of future security products or services.

The results achieved in this Thesis around live digital systems [19] give a practical perspective of all the challenges in the field of security and privacy in order to provide this kind of services. The work done in [17] and [18] allows to face some of these challenges as mentioned in Section III. The correct addressing of these challenges will enable a dependable and reliable service which we foresee will be highly demanded and requested in the coming years due to its multiple

possibilities of application. The architecture proposed in [19] for the live digital systems, plus the results obtained in [17] and [18], set the first step in the road to a nearby implementation.

Regarding future works, we believe there is a high potential of extension for our proposal to manage XACML systems in distributed environments through Meta-Policies [17]. Researching about the application of the proposal defined in [17] to manage the access to different types of information is definitely promising: every data owner or data responsible should be able to decide the treatment over his data. On the one side, this proposal could be applied in the composition of new services and implementations which use shared assets or require the participation of different implied actors to get an authorization decision.

Additionally, the model proposed in [17] could be used as the foundation in the application of personal data protection laws which regulate the rights of the data owner and the commitments of the companies in charge of the treatment. Authorization systems can be definitely improved to make them more accurate and effective since they can consider all applicable policies (from others domains) in an authorization decision process. Additionally, situations of high risk over a given infrastructure, like the ones included in cyber defense, bring also another interesting research opportunity to explore the use of access control policies in distributed environments. In this case, it would be interesting to explore the convenience of maintaining different authorization models over the assets. One model could be used in normal situations with more flexible policies, whereas another could be applied to high risk situations with more strict policies. In any case, the policy management operations would allow an effective control over the given remote infrastructure, like the one required in a cyber defense system for instance.

With regards to our proposal of dynamic counter-measures integrated in risk-adaptable access control systems [18], there are also opportunities for future works as there are different risk management methodologies (each one with variations in the estimation and management of the risk) and applying the methodology that fits in a better way the requirements of an organization is essential to make an effective risk mitigation. Each one of these methodologies could be integrated in a RAdAC system and used in order to provide a dynamic asset protection. The extension of our proposal to new types of threats, assets and counter-measures also constitutes an appealing line of research. Risk-based decisions are essential to operate an useful cyber defense system and, therefore, there is also a big opportunity around the integration or implementation of this proposal in an existing cyber defense decision process, like the OODA (Observe, Orient, Decide and Act) [20, 21] or CAESARS (Continuous Asset Evaluation, Situational Awareness, and Risk Scoring) [22].

The model proposed in [18] has a defensive purpose since it employs evolutive algorithms to find a set of counter-measures which are able to face a specific measured risk. In the same way, it would be certainly interesting to research about the use of similar bio-inspired techniques but for offensive purposes. This can be expressed in a model which can consider the probability of occurrence of a threat and the impact of a compromised asset, in order to find a set of attack vectors which can overpass the acceptable risk levels of an organization.

Finally, regarding live digital systems and our architecture proposed in [19], future works are wide enough to allow facing any of the identified challenges related to security, like purpose-based exposure, storage and processing of private data, encrypted data retrieval or forensic evidence, to mention some of them. Additionally, depending on the data, some of them can request a higher confidentiality and its access possibly would be restricted just to some third parties or applications. Therefore, there is an interesting topic around selective access which has to be attended in order to allow a big diversity of services and applications related to the registered data in these systems. Finally, an interesting future work based on the extension of this PhD Thesis can be considered through the integration of the results obtained in [17] and [18] around an implementation of the architecture proposed in [19].

Resumen

# I Motivación y Objetivos

El control de acceso se puede definir como:

> "Un proceso mediante el cual el uso de los recursos del sistema se regula de acuerdo a una política de seguridad y es permitido solamente a aquellos entes autorizados (usuarios, programas, procesos u otros sistemas) de acuerdo a dicha política." [1]

El proceso de control de acceso mencionado en la definición anterior se desarrolla alrededor del concepto de "activo de información" [2], el cual se corresponde con un componente de un sistema de información que debido a su valor puede ser atacado produciendo una consecuencia indeseada para la organización. Como "activos de información" se incluye información, servicios, software, hardware, instalaciones y personas, entre otros. Los"recursos del sistema" y los "entes autorizados" también son activos de información. La valoración de los activos es la determinación de la pérdida de valor para la organización causada por un incidente sobre el activo [3] y dicha valoración puede considerar los siguientes aspectos: costos de remplazo por adquisición o instalación, costos de recursos humanos invertidos en recuperación, pérdida de ingresos, pérdida de capacidad para operar, penalizaciones por no cumplir la legalidad, daño operativo, daño ambiental y afectaciones a la imagen y reputación, entre otros. En este contexto, un proceso de control de acceso bien definido es esencial para garantizar accesos autorizados, lo cual permite tener seguridad sobre los activos y operatividad del negocio, conocido en la literatura como balance entre seguridad y utilidad [4, 5].

Considerando la aplicación del proceso de control de acceso en el área de servicios o transacciones en línea (gestión de pedidos, consulta de información, pagos, gestión de inventarios, análisis de datos, gestión de campañas y otros servicios), es posible enfatizar la relevancia del control de acceso, principalmente por la atención que merece aquel "elemento valioso" que está detrás de estos servicios, que es la información (que como se mencionó anteriormente es por definición un "activo" cuya utilización se regula por el proceso de control de acceso). La información es efectivamente un elemento clave en organizaciones, dado que una información precisa, segura y disponible puede marcar la diferencia en unas operaciones de negocio exitosas e incluso llegar a definir la continuidad del negocio.

Con el fin de aplicar un proceso de control de acceso para regular privilegios sobre activos, existen hoy en día algunos modelos de control de acceso [6], cada uno con diferente complejidad y características, por ejemplo: listas de control de acceso (ACL), control de acceso basado en roles (RBAC), control de acceso basado en atributos (ABAC), control de acceso basado en políticas (PBAC) y control de acceso adaptable al riesgo (RAdAC). Estos modelos de control de acceso se

encargan de procesar solicitudes de control de acceso y generar decisiones de autorización. Los beneficios de cada modelo hacen de algunos de ellos los más apropiados para algunas situaciones por encima de otros.

Generalmente, uno o más modelos pueden ser aplicados en un único dominio de seguridad. Un dominio de seguridad está conformado por componentes (aplicaciones, módulos, servidores, recursos, redes, personas, etc.) que cumplen y comparten la misma configuración de seguridad (expresado comúnmente en forma de políticas de seguridad) [7]. El concepto de dominio de seguridad puede ser aplicado en un contexto organizacional donde una compañía o un departamento pueden ser vistos como dominios aislados, pero también en un modelo técnico, como en una arquitectura para computación en la nube, donde hay dominios de seguridad para diferentes niveles de la arquitectura: red, servicios, y almacenamiento [8].

Considerando la interacción entre organizaciones por razones técnicas o de negocio, tales como el establecimiento de relaciones de asociación, consorcio o sociedad empresarial, y adicionalmente la existencia de activos compartidos, como los usados en la composición de servicios, es imperante pensar sobre la interacción requerida entre diferentes dominios de seguridad para obtener decisiones de autorización conjuntas. Este contexto de múltiples dominios de seguridad usando y compartiendo activos e intercambiando elementos relacionados a la seguridad, constituye un ambiente distribuido el cual trae consigo dos principales desafíos para el contexto de gestión de políticas de control de acceso: 1) La necesidad de proponer mecanismos para permitir la composición de políticas de control de acceso de diferentes organizaciones, con el objeto de lograr un adecuado proceso de toma de decisiones de autorización, y 2) La necesidad de direccionar el proceso de toma de decisiones de autorización para tomar en cuenta requisitos de privacidad, confidencialidad y autonomía.

Así, uno de nuestros principales objetivos en esta tesis doctoral es abordar la gestión de políticas de control de acceso en ambientes distribuidos considerando las propuestas académicas previas, los requerimientos prácticos que las organizaciones manifiestan hoy en día, así como las necesidades venideras de acuerdo a nuevas tecnologías y modelos de negocio.

Por otro lado, informes de seguridad formales basados en incidentes de seguridad emitidos por diversas organizaciones confirman el impacto causado por diferentes eventos de compromiso de datos. Uno de los más respetables informes de seguridad es el informe DBIR (Data Breach Investigation Report) de Verizon [9], el cual tiene una periodicidad anual y se construye con los reportes de incidentes de seguridad de 70 organizaciones globales de 61 países. Estas organizaciones pertenecen a algunos de los siguientes grupos: CSIRTS (Equipos de respuesta a incidentes de seguridad de la información), Ciber centros, proveedores de servicios forenses, proveedores de productos y servicios de seguridad de la información, ISACS (Centros de análisis y gestión de información), agencias gubernamentales y otros. Estos informes nos permiten entender mejor el proceso de control de acceso desde una perspectiva del compromiso de los datos y nos arrojan algunos hechos interesantes:

- Se pueden considerar tres tipos diferentes de actores (o entes) como autores de eventos de compromiso de datos: 1) Internos, 2) Externos y 3) Asociados. Desde 2007, los compromisos de datos provocados por autores externos representan el porcentaje más alto de ocurrencias comparado con los otros dos actores, teniendo variaciones cada año (en 2007 los compromisos de datos provocados por actores externos representaron el 39%, pero en el 2013 éstos alcanzaron un 89% y en el 2014 consiguieron un 84,69% de todas las ocurrencias). Esta situación pone en evidencia la especial atención que los administradores de seguridad deben poner en el control del acceso a los datos que pueden ser accedidos por actores externos, sin subestimar que los usuarios internos y asociados aún representan una posible fuente de amenazas. Adicionalmente, debido a la existencia de un cierto nivel de

confianza con actores internos y asociados, los eventos de compromiso de datos provocados por estos actores pueden tener un impacto más alto que aquellos provocadas por actores externos e incluso estos eventos pueden ser más difíciles de detectar y contener.

- Las tres motivaciones principales de un evento de compromiso de datos son: 1) Financieras, 2) Espionaje y 3) Ideológicas/Diversión. Las motivaciones asociadas a espionaje han incrementado especialmente en los últimos años, elevándose desde un 6.8% en 2010 a un 17,2% en 2013. Sin embargo, las razones financieras mantienen a lo largo del tiempo el valor de porcentaje más alto, siendo 89.1% para el 2010 y 66.5% para el 2013. El reporte DBIR [9] más reciente no incluye un porcentaje para las motivaciones detrás de los eventos de compromiso de datos, sin embargo apunta en 2014 a las razones financieras como la principal motivación para incidentes de suplantación, crimen, ataque a aplicaciones web y "uso indebido de información" (principalmente abuso de privilegios). Estos valores nos sugieren que con el propósito de identificar las amenazas para un activo es necesario validar todos los posibles intereses (de cualquier tipo) que un activo puede atraer, y por lo tanto el proceso de control de acceso debería incluir todos esos factores como elementos clave para tomar una decisión de autorización.

- De las categorías de activos consideradas en el reporte DBIR (servidor, dispositivos de usuarios, quioscos, personas, medios de comunicación, red), que realmente representan objetivos potenciales de un ataque conducente a un compromiso de datos, es la categoría de "servidor" la cual generalmente obtiene el porcentaje más alto de ataques, alcanzando un 44,5% para el 2013, seguido por la categoría de "dispositivos de usuario" con un 20,8% y "personas" con un 15,95 % de los ataques. Esto es entendible dado que los activos de tipo "servidor" albergan la mayoría de los datos del negocio y por lo tanto constituyen el objetivo más atractivo en un ataque. Los "dispositivos de usuario" constituyen un porcentaje importante en los ataques debido a la popularización de los dispositivos personales conectados, como teléfonos inteligentes, computadores portátiles o tabletas, que representan una vía para acceder a los datos personales e incluso una pequeña ventana para acceder a sistemas de información críticos. El reporte DBIR mas reciente [9] no incluye los porcentajes de ataques para cada categoría de activo para el 2014, sin embargo indica que el 70% de estos ataques incluyeron una víctima secundaria, el cual actúa como "servidor" comprometido usado para ataques DoS (Denial of Service), distribución de malware o phishing. Una víctima secundaria es un activo que es comprometido por un atacante como una forma de desarrollar un ataque diferente contra otra víctima. Esto enfatiza el hecho de que los activos de la categoría "servidor" mantienen el porcentaje mas alto de ataques en el 2014. En cualquier caso, es un hecho que un proceso de control de acceso eficiente debería ofrecer protección a los datos independientemente del dispositivo sobre el cual éstos estén almacenados.

- De todos los diferentes tipos de incidentes considerados en el reporte DBIR, es importante resaltar el "uso indebido de privilegios e información", que corresponde a un uso malicioso y no aprobado de los recursos organizacionales, el cual puede ser originado por cualquiera de los actores (entes): internos, externos (por conspiración) o asociados empresariales. Este tipo de incidente puede ser causado por diferentes amenazas, pero de acuerdo a los informes 88% en el 2013 y 55% en el 2014 de los iniciadores de este tipo de incidente fueron "acciones de abuso de privilegios" que corresponde a usar algunos privilegios otorgados (debido a una relación laboral o de asociación) para cometer actos maliciosos. Este porcentaje sugiere que aun si una política de seguridad ha sido inicialmente definida en una forma correcta, ésta tiene que ser revisada constantemente para mantenerla alineada a los cambios

en el ambiente, refiriéndose específicamente a los cambios en las relaciones de confianza, sospechas sobre el mal uso de recursos, comportamientos anormales en los entes, etc.

Como podemos ver, hay muchos desafíos alrededor de la generación de decisiones de autenticación y autorización que se reflejan hoy en día en incidentes de seguridad, los cuales en situaciones reales no son fácilmente abordados debido a la cantidad y complejidad de las variables a tomar en cuenta (por ejemplo, las clases de actores en un entorno, las posibles motivaciones para un compromiso de datos, las diferentes categorías de activos y amenazas, el impacto de los eventos de compromiso de datos, la criticidad de los activos, la confianza entre asociados empresariales, etc.). Este contexto previo deriva otro objetivo dentro de esta tesis doctoral que no es otro sino proveer una protección dinámica de activos mediante una mejora al proceso de control de acceso, buscando hacerlo más efectivo en la confrontación de amenazas de seguridad de la información, y más apropiado para un contexto expuesto a diferentes riesgos de seguridad.

Acercándonos a la perspectiva de los usuarios, una gran cantidad de datos son capturados diariamente a través de nuestras interacciones personales con dispositivos TIC (Tecnologías de la Información y las Comunicaciones) o aplicaciones en general, construyendo la idea de que cada uno de nosotros tiene una "vida digital". Estos datos históricos podrían ser almacenados, procesados y accedidos con posterioridad para diferentes clases de propósitos como: fines productivos, de salud, legales o de entretenimiento, por mencionar tan sólo algunos de ellos. Sin embargo, para obtener una utilidad de los datos personales, diferentes asuntos alrededor de la seguridad y privacidad deben ser resueltos antes de la popularización de esta clase de servicios de "Live Digital". El proceso de control de acceso también toma relevancia en esta clase de sistemas debido a que éste debería asegurar solamente el acceso de aplicaciones/usuarios autorizados a ciertas clases de datos personales basado en las restricciones definidas por el propietario de los datos.

Finalmente, todas las situaciones previas hacen de los sistemas de control de acceso un tópico importante de investigación, sobre el cual la comunidad científica se encuentra trabajando y el cual fue específicamente apoyado en la octava edición del programa para la investigación y el desarrollo tecnológico "Horizon 2020" por parte de la Unión Europea [10]. El tópico de control de acceso ha sido considerado dentro del desafío "sociedades seguras", enfocado en la protección de ciudadanos, sociedad, economía, activos europeos, infraestructura y servicios [11].

Adicionalmente, la Dirección de Tecnología y Ciencia del Departamento de Seguridad Nacional de Estados Unidos (departamento constituido en 2003 después de los ataques del 11 de septiembre del 2001), ha definido sus propias direcciones estratégicas con el objeto de proteger activos críticos. Entre estas direcciones hay dos especialmente relacionadas al tema de esta tesis: "Ciber futuro confiable: La protección de la privacidad, el comercio y la comunidad" y "Habilitando el decisor: Información procesable a la velocidad del pensamiento" [12]. El primero de éstos aborda la idea de una infraestructura con la capacidad de hacer detección, autoprotección y autoremediación con el objeto de garantizar un ciberespacio confiable. El segundo busca incorporar el análisis de riesgos y sistemas de modelado para habilitar un proceso de toma de decisiones apoyado en información requerida.

Así mismo, el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos publicó el marco para mejorar la ciber seguridad en infraestructuras críticas [13], el cual emergió a través de la orden ejecutiva 13636 en la política de los Estados Unidos para mejorar la seguridad y resistencia de las infraestructuras críticas nacionales. Este programa tiene como propósito la definición de estándares y mejores prácticas para ayudar a organizaciones americanas a manejar riesgos de seguridad. Dentro de este programa, el control de acceso y la gestión de riesgos tienen un lugar especial en el desarrollo de la protección como una función clave.

Las apreciaciones anteriores definen el control de acceso como un importante tópico de investigación sobre el cual sectores públicos y privados (incluyendo la academia) están trabajando con el propósito de usarlo como un elemento clave en la protección de los activos. La protección de activos es un componente principal para lograr una adecuada gestión del riesgo que permita el aseguramiento del ciberespacio actual y futuro.

Así, el objetivo principal en esta tesis doctoral es desarrollar propuestas para la gestión de sistemas de control de acceso usando elementos innovadores y buscando su aplicabilidad en escenarios reales distinguidos por tener un notorio componente de autorización. De la misma forma, los objetivos especificos de esta tesis, los cuales se encuentran estrechamente relacionados con el objetivo principal previamente presentado, son definidos a continuación:

- Estudiar diseños de sistemas de control de acceso existentes, identificando sus principales limitaciones cuando son aplicados a situaciones de múltiples dominios de seguridad con activos compartidos (i.e. ambientes distribuidos).
- Proponer una solución para una efectiva gestión de políticas en ambientes distribuidos que permita a los dominios de seguridad mantener cierta autonomía y confidencialidad.
- Lograr una forma innovadora de proveer un proceso de control de acceso para activos de información que considere los riesgos de seguridad como parte del contexto de autorización.
- Proponer una solución orientada a mitigar riesgos de seguridad en activos de información en una ventana de tiempo razonable y considerando los objetivos de seguridad de la organización.
- Identificar desafíos de seguridad y privacidad a través del análisis de soluciones existentes en el área de sistemas Live Digital.
- Proponer una arquitectura para soportar sistemas Live Digital con una aproximación prevalente a la seguridad de los datos y la privacidad, y con la posibilidad de aplicar los resultados obtenidos de los objetivos previos.

# II Metodología

Esta tesis doctoral ha sido elaborada como resultado de diferentes estancias en sectores de I+D (Investigación y Desarrollo) e industria dentro del área de seguridad de la información, principalmente en NLE (NEC Laboratories Europe) en Alemania, con una continua orientación del Departamento de Ingeniería de la Información y las Comunicaciones (DIIC) de la Universidad de Murcia en España. Los resultados producidos a lo largo de todas las estancias fueron depurados y revisados en detalle desde una perspectiva de investigación y de industria, conduciendo a un consolidado de artículos de investigación publicados en revistas JCR. De esta forma, la metodología descrita a continuación corresponde al conjunto de procesos y actividades desarrolladas para alcanzar una tesis basada en compendio de publicaciones.

Las actividades de investigación alrededor de esta tesis se iniciaron con una estancia de investigación en NLE, donde se nos facilitó un primer contacto con motores de autenticación y autorización, permitiéndonos identificar y analizar toda la complejidad detrás de un proceso de control de acceso. Como resultado de esta aproximación, diferentes mejoras fueron propuestas y desarrolladas sobre el motor XACML alojado en NLE, la mayoría de ellas relacionadas con el módulo PDP (Policy Decision Point), con el objeto de hacer composición de decisiones de autorización, y con el módulo PAP (Policy Administration Point), con el objeto de administrar eficientemente todo el conjunto de políticas de seguridad. Estas labores iniciales nos permitieron

abordar parcialmente uno de los objetivos específicos de la tesis alrededor del estudio de diseños de sistemas de control de acceso existentes.

Trabajando sobre estas mejoras mencionadas al motor XACML de NLE, algunas inquietudes e ideas surgieron acerca de cómo trasladar las funcionalidades de un motor de autenticación y autorización a un ambiente distribuido y colaborativo, como el compuesto por diferentes unidades de negocio (diferentes organizaciones o sucursales de la misma organización) cada una conformando un dominio de seguridad independiente. Consecuentemente, una arquitectura para administrar políticas de control de acceso en ambientes distribuidos fue propuesta y desarrollada (Capítulo 1), la cual consideró y resolvió diferentes aspectos relacionados con la comunicación entre partes, la administración de políticas de control de acceso y la seguridad de las comunicaciones. Con esta propuesta pudimos establecer un modelo basado en operaciones para la administración de políticas (difundir, actualizar, borrar, etc.) dentro de un contexto distribuido de una forma simple e integrada, con la posibilidad de ser extendida o adaptada para soportar nuevas operaciones de administración. Esta propuesta fue ampliamente revisada y analizada por diferentes investigadores, ayudando a mejorar y ajustar diferentes aspectos de la propuesta hasta alcanzar una solución robusta y consistente.

Después del desarrollo de la arquitectura previa orientada a una gestión eficiente de sistemas de control de acceso, una nueva oportunidad de investigación surgió enfocada en algoritmos que pudieran ayudar a determinar la decisión de autorización apropiada para regular el acceso a un activo, pero también pudieran contribuir a mitigar un riesgo de seguridad identificado. Así, otra estancia de investigación fue desarrollada en NLE con el objeto de desarrollar la idea de utilizar decisiones de autorización influenciadas por riesgos medidos para lograr una protección de activos dinámica. Buscando sobre diferentes formas de administrar los riesgos de seguridad, descubrimos los sistemas RAdAC (Sistemas de control de acceso adaptable al riesgo) y concluimos que ninguna propuesta existente sobre la inclusión de riesgos de seguridad en la determinación de una decisión de autorización había considerado la incorporación de algoritmos evolutivos.

En un sistema de control de acceso de tamaño pequeño que regule el acceso a un conjunto delimitado de activos se pueden considerar los diferentes cambios en los niveles de riesgo asociados a los activos, y por cada cambio en el nivel de riesgo, el sistema puede generar manualmente un control de seguridad para proteger el activo y de esta forma permitir un acceso seguro. Sin embargo, en un sistema de control de acceso de tamaño medio o grande la ingente cantidad de activos y los cambios potenciales en el nivel de riesgo asociados a éstos hacen improbable reaccionar manualmente a cada situación para garantizar el acceso y al mismo tiempo mitigar correctamente el riesgo a través de un conjunto de contramedidas aplicables. Adicionalmente, este contexto de sistemas de control de acceso de tamaño medio o grande generalmente contiene múltiples recursos, sujetos, acciones y variables del entorno que deben ser considerados para construir una decisión de autorización. En este punto, estuvimos de acuerdo en que este contexto dinámico y multi-variable representaba un espacio adecuado para aplicar una solución basada en algoritmos evolutivos que nos permitiera encontrar el mejor conjunto de contramedidas aplicables para un contexto de autorización específico en un tiempo aceptable.

Mientras se progresaba en el desarrollo de esta idea acerca de la aplicación de algoritmos evolutivos para computar decisiones de autorización, surgió una oportunidad para ser parte de un proyecto de diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) bajo el estándar ISO27001 [15]. Este proyecto fue desarrollado dentro de una estancia en CINTEL (Centro de Desarrollo e Investigación en Tecnologías de la Información y las Comunicaciones), un Centro de Desarrollo Tecnológico de la industria de la tecnología de la información y las comunicaciones en Colombia. El diseño del SGSI fue realizado para una compañía del sector público en Colombia y tuvo como alcance el desarrollo de la fase 'planear' y 'hacer' de acuerdo

al ciclo Deming. El ciclo Deming es un modelo de mejora continuo relacionado con diferentes sistemas de gestión que define las siguientes cuatro etapas como parte del desarrollo del sistema: Planear, Hacer, Verificar y Actuar. Este proyecto nos permitió entender la seguridad de la información como un proceso dentro de las organizaciones y ver cómo éste ha sido dirigido hasta ahora a través de diferentes buenas prácticas y estándares con el propósito de cumplir un conjunto de requisitos genéricos que permitan establecer, implementar, mantener y mejorar un SGSI dentro del contexto de una organización.

Uno de los requerimientos de un SGSI es mantener un proceso de evaluación de riesgos de seguridad de la información que pueda ser dirigido por los principios descritos en el estándar ISO/IEC 27005 [16]. El proceso de evaluación de riesgos de seguridad de la información debe definir los criterios para evaluar y administrar riesgos de seguridad, establecer una forma de identificarlos y analizarlos de acuerdo al impacto y la probabilidad de ocurrencia. Adicionalmente, para los riesgos de seguridad identificados, la organización debe establecer un tratamiento razonable de acuerdo a ciertos controles de seguridad, también llamados contramedidas. Todos estos aportes de un proyecto de seguridad aplicado a través de la estancia en CINTEL nos permitieron mejorar considerablemente nuestra idea inicial acerca de la aplicación de algoritmos evolutivos para computar decisiones de autorización, incluyendo ahora el proceso de evaluación de riesgos dentro de las organizaciones.

Fue de esta forma que definimos una propuesta de modelo para la adopción de contramedidas dinámicas que cambian en el tiempo para enfrentar las variaciones en el nivel de riesgo medido para cada recurso, basándonos en algoritmos genéticos (Capítulo 2). Esta propuesta fue desarrollada con el objetivo de cumplir los requerimientos de un SGSI con respecto a la evaluación y el tratamiento de riesgos de seguridad. La gestión de riesgos se consigue a través de los resultados generados en nuestro modelo propuesto, el cual considera el nivel de riesgo aceptable definido para los activos de información de tal forma que los activos no queden expuestos pero tampoco sobreprotegidos. Una metodología de gestión de riesgos dirigida por los principios descritos en el estándar ISO/IEC 27005 [16] también puede ser integrada en nuestro modelo propuesto.

Después de abordar situaciones de gestión de políticas de control de acceso en ambientes distribuidos y sistemas de control de acceso con habilidad para responder dinámicamente con contramedidas contra una amenaza detectada, decidimos dirigirnos hacia una situación cercana al dominio del usuario en donde los sistemas de control de acceso podrían representar un elemento clave para garantizar la seguridad y privacidad. Para este fin, exploramos el estado del arte y los desafíos de los sistemas Live Digital (i.e. sistemas con la habilidad de recolectar, organizar, almacenar y visualizar datos asociados a la huella digital que un usuario deja sobre todos los dispositivos IT con los que interactúa).

Los sistemas Live Digital requieren la interacción y coordinación de diferentes componentes como dispositivos de usuario final, aplicaciones, proveedores de servicio, servicios de procesamiento y proveedores de identidad y almacenamiento, entre otros, los cuales en conjunto configuran un ambiente distribuido. Este ambiente distribuido puede estar compuesto de diferentes dominios de seguridad que interactúan, en donde el activo compartido más prevalente es la información del usuario. De esta forma, un modelo de control de acceso que permita regular el acceso a este activo en un ambiente distribuido es claramente una necesidad. Así, encontramos en los sistemas Live Digital un contexto donde puede ser posible aplicar los resultados de nuestro modelo detallado previamente en el Capítulo 1. Adicionalmente, es predecible que debido a la información personal que se procesa en sistemas Live Digital, estos sistemas estarán expuestos a diferentes clases de amenazas de seguridad. Adicionalmente, el gran número de activos (todos los datos de usuario) y los cambios en los valores del riesgo sobre éstos, traen consigo el hecho de que los sistemas Live Digital serían un espacio interesante para desplegar una solución como

la propuesta en el Capítulo 2, la cual aporte un sistema de control de acceso que provea una protección de activos dinámica.

El resultado de la investigación alrededor de los sistemas Live Digital consistió en una completa revisión de trabajos que pudieran tener una aproximación hacia sistemas Live Digital y un estudio de la arquitectura de estos sistemas con el fin de encontrar funcionalidades y limitaciones existentes. Posteriormente hicimos una abstracción de los pasos que soportan un sistema Live Digital y una identificación de los diferentes desafíos alrededor del desarrollo de estos pasos. Un conjunto especial de desafíos relacionados con seguridad y privacidad, incluyendo aspectos de control de acceso, también fueron determinados. Estos hallazgos del estado de arte y los desafíos identificados nos ayudaron a proponer una arquitectura cliente/servidor que pudiese incorporar los módulos y los componentes requeridos para desarrollar un sistema Live Digital capaz de entregar un servicio seguro y privado (Capítulo 3).

## III Resultados

Los primeros resultados de esta tesis doctoral están descritos en el artículo "Managing XACML systems in distributed environments through Meta-Policies" [17], publicado en la revista Computers & Security de Elsevier. Este artículo hace una extensión de las funcionalidades ya conocidas de un sistema de control de acceso funcional en un dominio de seguridad, hacia un contexto compuesto de múltiples dominios de seguridad (y por lo tanto múltiples sistemas de control de acceso) en el cual se requiere coordinación con el fin de resolver apropiadamente todas las solicitudes de autorización. Esta coordinación implica la existencia de una relación de confianza entre dominios de seguridad que los habilite para interactuar e intercambiar información de seguridad. Un contexto de múltiples dominios de seguridad puede encontrarse fácilmente en la vida real si consideramos el concepto de activos compartidos, el cual sugiere que todos los propietarios de un activo deberían estar de acuerdo con el uso que tendrá dicho activo. Esto es aplicable a la situación de servicios de virtualización que están compuestos usualmente por múltiples proveedores de servicio, cada uno de ellos entregando un componente específico de todo el servicio. Otro ejemplo común de un contexto de múltiples dominios regulando un activo de información podría estar en organizaciones con una oficina principal y algunas sucursales o subsidiarias, teniendo que compartir recursos entre éstas, considerando que cada una de ellas constituye de hecho una oficina independiente y por lo tanto puede configurar sus propias políticas de seguridad sobre sus activos.

El trabajo presentado en [17] propone una arquitectura para administrar políticas de control de acceso en ambientes distribuidos, considerando y resolviendo diferentes aspectos como: i) Una propuesta de estrategia de comunicación entre dominios de seguridad a través del uso de elementos claves en ambos lados de la comunicación (Master y Slave PAPs), ii) La utilización de un elemento llamado "Meta-Política" para regular los privilegios sobre políticas de control de acceso y forzar un uso aceptable de ellas, con lo que las políticas de control de acceso llegan a ser ellas mismas el recurso gestionado, iii) La provisión de un mecanismo de seguridad a través del protocolo SAML para proteger la transmisión de mensajes de administración de políticas entre dominios de seguridad.

Este artículo [17] ofrece una clara perspectiva acerca de cómo diferentes sistemas de control de acceso XACML pueden interactuar en una forma segura, ofreciendo baja sobrecarga en situaciones donde hay un alto número de solicitudes de autorización que tienen que ser resueltas considerando más de un colaborador a la decisión. Adicionalmente, en [17] la arquitectura XACML fue reutilizada con el objetivo de administrar privilegios sobre políticas distribuidas (conocidas como Meta-Políticas en el artículo), permitiendo ahorrar tiempo y esfuerzo en la implementación y despliegue de una nueva arquitectura de control de acceso diseñada para este

propósito. Finalmente, vale la pena mencionar que a través de la expresividad de XACML es posible definir adecuadamente privilegios y garantizar la privacidad y confidencialidad de políticas y atributos en cada dominio de seguridad.

Después del anterior desarrollo de una arquitectura para administrar sistemas XACML en ambientes distribuidos, pusimos nuestra atención en situaciones en donde la definición de una decisión de autorización debe incluir el riesgo de seguridad sobre el activo de información como un aspecto clave (como se indica posteriormente en [18]). Esta inclusión constituye un gran desafío para el proceso de control de acceso dado que el riesgo es variable y por lo tanto las decisiones de autorización provenientes del proceso de control de acceso también deberán cambiar para estar alineadas con las variaciones en el riesgo.

Así, desarrollamos una propuesta de adopción de contramedidas dinámicas cambiando a lo largo del tiempo para dar respuesta a las variaciones en el nivel de riesgo de cada recurso [18]. Este modelo genera conjuntos de contramedidas ajustadas tomando en cuenta factores (atributos) relevantes para la clase de activos y para el nivel de riesgo específico. Con esta propuesta hay dos beneficios principales: i) Aplicación de un proceso de gestión de riesgos para garantizar una protección dinámica de activos y ii) Gestión de privilegios sobre activos a través de un sistema de control de acceso. Las contramedidas proporcionan la protección al activo de información con el propósito de mitigar el riesgo de seguridad, y pueden ser integradas en diferentes partes de una política de control de acceso: objetivo (target), condición (condition) u obligación (obligation).

Además, considerando un conjunto de amenazas y controles de seguridad, y la capacidad del método propuesto para generar las mejores soluciones candidatas en tiempos aceptables, la solución presentada en [18] también permite reaccionar a situaciones de riesgo concurrente representadas en variaciones del nivel de riesgo, evitando retrasos en las respuestas necesarias para proteger dinámicamente los activos de información sin requerir intervención manual.

Esta propuesta fue desarrollada y testeada en el artículo "Dynamic counter-measures for risk-based access control systems: An evolutive approach" [18], publicado en la revista Future Generation Computer Systems de Elsevier. La propuesta se fundamenta en un algoritmo genético que permite encontrar el conjunto óptimo de contramedidas aplicables para una situación muy específica de riesgo, probabilidad de ocurrencia, impacto y efectividad de controles de seguridad. Se desarrolló una implementación de la propuesta y se usaron diferentes valores de efectividad y niveles de riesgo para ponerla a prueba.

Finalmente, nuestro último paso en la ruta de investigación fue analizar y explorar desde una perspectiva de seguridad un área innovadora y prometedora que estuviese relacionada con el uso de información personal. Adicionalmente, nos interesamos en un área sobre la cual pudiéramos aprovechar la experiencia adquirida a través de los resultados anteriores de esta tesis. Este área correspondió a los sistemas Live Digital, que en nuestra opinión serán impulsados de una forma considerable por la tendencia del Internet de la Cosas. Todos los desafíos en los sistemas Live Digital, al igual que una arquitectura cliente/servidor, fueron propuestos y descritos en el artículo "Live digital, remember digital: State of the art and research challenges" [19], publicado en la revista Computers and Electrical Engineering de Elsevier.

En [19] se incluye una comparación detallada de herramientas para administrar información personal, que utilizamos como un elemento de entrada para identificar las características que deben estar presentes en un sistema Live Digital con el fin de que éste sea un servicio que efectivamente permita recuperar cualquier evento digital ocurrido en el pasado. Estas características deseadas se presentan en forma de desafíos comunes para todos los sistemas Live Digital y corresponden a la recordación, navegación, búsqueda, uso compartido, organización, filtrado, auditoría y visualización de eventos. Adicionalmente, un conjunto de desafíos específicamente relacionados a seguridad y privacidad en sistemas Live Digital fueron identificados y descritos

en [19]. Considerando el contexto de sistemas Live Digital, creemos que las propuestas desarrolladas previamente en esta tesis doctoral a través de [18] y [17], permiten enfrentar ciertos desafíos descritos en [19], específicamente los siguientes: acceso selectivo, recolección selectiva, seguridad y privacidad transversal y aseguramiento de infraestructura tecnológica, entre otros.

El desafío de acceso selectivo plantea que el acceso a datos de usuario debería ser regulado en una forma fina de acuerdo a los permisos definidos por el propietario de los datos. En el contexto de los sistemas Live Digital algunos elementos en el lado del servidor (proveedores de servicio, servicios de procesamiento, proveedores de identidad y almacenamiento) reflejan un contexto distribuido en donde los datos de usuarios son accedidos por muchas partes, destacando la necesidad de un modelo de control de acceso efectivo que regule el acceso. Con el fin de abordar este desafío de acceso selectivo, el modelo de control de acceso propuesto en [18] puede ser utilizado como línea base, debido a que éste permitiría al propietario de los datos administrar ciertas políticas de control de acceso en los gestores de los datos con respecto a sus propios datos. Un ejemplo es la difusión de políticas de control de acceso hacia los gestores de los datos que reflejen los permisos de acceso y utilización definidos por el propietario de los datos.

Por otro lado, el desafío de una recolección selectiva se refiere a la habilidad para definir qué clase de datos pueden ser recolectados por una aplicación específica o dispositivo en un sistema Live Digital. Considerando que cada aplicación o dispositivo usado en la recolección de interacciones puede conformar un dominio de seguridad, es posible plantear el hecho de que el propietario de los datos podría administrar algunas políticas de control de acceso en los dominios de seguridad involucrados en la recolección, con el fin de administrar qué clase de datos son recolectados y procesados. En este caso, una propuesta como la indicada en [18] puede ser utilizada como un punto de partida para permitir un control efectivo sobre el proceso de recolección. La utilización de una solución como la mencionada en [18] para resolver los desafíos de acceso y recolección selectiva trae también el beneficio de que el proceso de determinar decisiones de autorización considerará a las políticas del propietario de los datos como un parámetro de entrada clave.

El desafío de seguridad y privacidad transversal se enfoca en proporcionar seguridad y privacidad a lo largo de todas las actividades involucradas en los procesos de recolección, almacenamiento, procesamiento, indexación y visualización de información de usuario. En segundo lugar, el desafío de aseguramiento de infraestructura tecnológica busca resolver posibles amenazas de seguridad sobre servicios e infraestructura física. Ambos desafíos pueden ser abordados desde una perspectiva de gestión de riesgo porque las condiciones de seguridad de los procesos involucrados en un sistema Live Digital y las condiciones de seguridad de los servicios e infraestructura tecnológica están expuestos a condiciones de riesgo variable. Dentro del proceso involucrado en sistemas Live Digital muchas entidades pueden participar, cuya relación de confianza puede ser redefinida constantemente afectando la operación desde una perspectiva de seguridad. Adicionalmente, los servicios y la infraestructura física están expuestos a una gran cantidad de amenazas externas las cuales están evolucionando y las cuales requieren un ajuste interno de las configuraciones de los sistemas Live Digital con el fin de hacerles frente. Adicionalmente, es presumible que el valor de los activos también será variable dependiendo de la clase de información personal. Por lo tanto, los controles de seguridad usados para proteger la información también deberían ser ajustados a todas estas situaciones cambiantes.

De esta forma, una perspectiva de gestión del riesgo es útil en el contexto de un sistema Live Digital porque permitiría enfrentar estos dos desafíos, debido a que ésta provee la habilidad para reaccionar con un conjunto de contramedidas de acuerdo al valor de criticidad del activo, la probabilidad de ocurrencia de una amenaza y los actuales controles de seguridad. Considerando lo anterior, la propuesta descrita en [17] ofrece efectivamente un sistema de control de acceso basado en riesgo el cual tiene la habilidad para reaccionar a contextos cambiantes por medio de

un conjunto de contramedidas que enfrentan las variaciones del riesgo. Un conjunto adecuado de contramedidas permite mitigar un riesgo identificado y garantiza que la operación del sistema Live Digital sea conducida adecuadamente y la información del usuario sea tratada como corresponde. El tratamiento de la información debería estar alineado con los requerimientos de seguridad del propietario de la información, la regulación vigente (específicamente aquella relacionada con privacidad) y los objetivos de seguridad de la organización.

Regresando a los resultados incluidos en [19], también se propuso una arquitectura que soporta las funcionalidades anteriormente identificadas en dicho artículo para sistemas Live Digital. Esta arquitectura describe todos los elementos principales en el lado cliente y servidor necesarios para soportar un servicio seguro. Los componentes en el lado cliente cubren dos principales funcionalidades, algunos componentes asociados a la recolección, filtrado y cifrado de interacciones, y otros relacionados a la búsqueda, recuperación y descifrado de información almacenada. Por otro lado, los componentes en el lado del servidor cubren funcionalidades asociadas a la recepción, organización y almacenamiento de interacciones cifradas, y también la recuperación y entrega de resultados de las consultas.

Adicionalmente, la arquitectura propuesta en [19] ha sido pensada para ser capaz de soportar diferentes clases de servicios, tecnologías de usuarios final, mecanismos de almacenamiento e interacciones con otros proveedores de servicios o de identidad. Como un caso práctico, una situación de atención en salud fue presentada con el propósito de mostrar el potencial de esta clase de soluciones, siempre que el mecanismo de control de acceso garantice la seguridad y la privacidad de los datos.

# IV Conclusiones y Trabajos futuros

Hoy más que nunca la "información" llega a ser un elemento clave dentro de nuestra sociedad, siendo esencial en diferentes áreas como la social, cultural, económica y política. Son las tecnologías de la información y las comunicaciones (TIC) quienes principalmente facilitan todas las actividades relacionadas con la información, como la creación, modificación, distribución e intercambio, entre otras.

En el camino para construir una verdadera "sociedad de la información" hay muchos obstáculos que sobrepasar, siendo la seguridad de la información uno de los más importantes. Y como un elemento clave de la seguridad de la información podemos resaltar el "proceso de control de acceso", dado que éste tiene la misión de administrar el acceso y los privilegios para los activos (incluyendo la información). De hecho, un proceso de control de acceso adecuadamente diseñado puede contribuir significativamente al éxito de una "sociedad de la información".

Teniendo en mente que el proceso de control de acceso es un componente altamente crítico, esta tesis doctoral afronta el desafío de definir propuestas para la gestión de sistemas de control de acceso buscando su aplicabilidad final en escenarios reales que incorporen procesos de autorización. De esta forma, esta tesis doctoral considera algunos de los desafíos más vitales, como la extensión de políticas de control de acceso a más de un dominio de seguridad (un ambiente distribuido), la gestión dinámica de riesgos de seguridad a través de un motor de control de acceso que provea gestión de privilegios y protección adecuada sobre los activos, y la propuesta de una arquitectura capaz de soportar un sistema con altos volúmenes de datos personales para ser protegidos mediante un sistema de control de acceso avanzado.

Nuestra propuesta para administrar sistemas XACML en ambientes distribuidos a través de Meta-Políticas [17] ofrece un conjunto de operaciones de administración, que combinadas con un conjunto de Meta-Políticas bien definidas, permiten tener un ambiente distribuido con muchos motores de control de acceso realizando comunicación y coordinación entre ellos. Creemos que

esta propuesta puede ser usada como base para implementaciones futuras de motores de control de acceso.

Por otro lado, el trabajo hecho en esta tesis doctoral con la propuesta de contramedidas dinámicas integradas en sistemas de control de acceso adaptables al riesgo [18] definitivamente provee una alternativa para manejar los riesgos de seguridad, dado que ésta considera la naturaleza del riesgo (i.e. su dinamismo) e integra esta característica en el proceso de construcción de decisiones de autorización. Esta propuesta adicionalmente integra de manera efectiva un sistema de control de acceso en un SGSI (Sistema de Gestión de Seguridad de la Información), dando una aplicación práctica de la solución y definitivamente poniendo sobre la escena la oportunidad para implementarla como parte de futuros productos o servicios de seguridad.

Los resultados logrados en esta tesis alrededor de sistemas Live Digital [19] dan una perspectiva práctica de todos los desafíos en el campo de seguridad y privacidad que se deben abordar con el objeto de proveer esta clase de servicios. El trabajo hecho en [17] y [18] permite enfrentar algunos de estos desafíos como se mencionó en la Sección III. El correcto abordaje de estos desafíos permitirá un servicio seguro y confiable que prevemos será altamente demandado y solicitado en los próximos años debido a sus múltiples posibilidades de aplicación. La arquitectura propuesta en [19] para sistemas Live Digital, sumado a los resultados obtenidos en [17] y [18], representan el primer paso en el camino hacia una implementación cercana de este tipo de sistemas.

Con respecto a los trabajos futuros, creemos que hay un gran potencial de extensión para nuestra propuesta de administración de sistemas XACML en ambientes distribuidos a través de Meta-Políticas [17]. La investigación alrededor de la aplicación de la propuesta definida en [17] para administrar el acceso a diferentes tipos de información es definitivamente prometedora, ya que cada propietario o responsable de los datos debería ser capaz de decidir el tratamiento sobre sus datos. Por un lado, esta propuesta podría ser aplicada en la composición de nuevos servicios e implementaciones que usen activos compartidos o requieran la participación de diferentes actores implicados para lograr una decisión de autorización.

Adicionalmente, el modelo propuesto en [17] podría ser usado como base en la aplicación de leyes de protección de datos personales que regulen los derechos de los propietarios de los datos y los compromisos de las compañías a cargo del tratamiento de los datos. Los sistemas de autorización pueden ser definitivamente mejorados para hacerlos más precisos y efectivos dado que ellos pueden considerar todas las políticas aplicables (desde otros dominios) en un proceso de decisión de autorización. Adicionalmente, situaciones de alto riesgo sobre una infraestructura dada, como las incluidas en ciber defensa, suponen también otra oportunidad de investigación interesante para explorar el uso de políticas de control de acceso en ambientes distribuidos. En este caso, sería interesante explorar la conveniencia de mantener diferentes modelos de autorización sobre los activos. Un modelo podría ser utilizado en situaciones normales con políticas más flexibles, mientras que otro podría ser aplicado a situaciones de alto riesgo con políticas más estrictas. En cualquier caso las operaciones de gestión de políticas permitirían un control efectivo sobre la infraestructura remota, como aquella requerida en un sistema de ciber defensa.

Adicionalmente, alrededor de nuestra propuesta de contramedidas dinámicas integradas en sistemas de control de acceso adaptables al riesgo [18] también hay oportunidades para trabajos futuros dado que hay diferentes metodologías de gestión de riesgos (cada una con variaciones en la estimación y administración del riesgo) y aplicar la metodología que mejor se ajusta a los requerimientos de una organización es esencial para hacer una mitigación de riesgos efectiva. Cada una de estas metodologías podría ser integrada en un sistema RAdAC y usada para proveer una protección de activos dinámica. La extensión de nuestra propuesta a nuevos tipos de amenazas, activos y contramedidas también constituye una línea de investigación atractiva. Las decisiones basadas en riesgo son esenciales para operar un sistema de ciber defensa efectivo y, por lo tanto, hay una gran oportunidad alrededor de la integración o implementación de

esta propuesta en un proceso de toma de decisiones de ciber defensa existente, como OODA (Observar, Orientar, Decidir y Actuar) [20, 21] o CAESARS (Evaluación de activos continua, conciencia de la situación, y valoración del riesgo) [22].

El modelo propuesto en [18] tiene un propósito defensivo dado que éste emplea algoritmos evolutivos para encontrar un conjunto de contramedidas con capacidad de enfrentar un riesgo medido específico. De la misma forma, sería ciertamente interesante investigar acerca del uso de técnicas bio-inspiradas similares pero para propósitos ofensivos. Esto puede ser expresado en un modelo que pueda considerar la probabilidad de ocurrencia de una amenaza y el impacto de un activo comprometido, con el objeto de encontrar un conjunto de vectores de ataque que puedan sobrepasar los niveles de riesgo aceptables de una organización.

Finalmente, acerca de los sistemas Live Digital y nuestra arquitectura propuesta en [19], los trabajos futuros son suficientemente amplios para permitir enfrentar cualquiera de los desafíos identificados relacionados con seguridad, como exposición basada en propósito, almacenamiento y procesamiento de datos privados, recuperación de datos cifrados o evidencia forense, por mencionar algunos de ellos. Adicionalmente, dependiendo de los datos, algunos de ellos pueden requerir una confidencialidad más alta y su acceso posiblemente será restringido sólo a algunas terceras partes o aplicaciones. Por lo tanto, hay un tópico interesante alrededor del acceso selectivo que debe ser atendido para permitir la ejecución de una gran diversidad de servicios y aplicaciones que estén relacionadas con los datos registrados en estos sistemas. Finalmente, un trabajo futuro interesante basado en la extensión de esta tesis doctoral puede ser considerado a través de la integración de los resultados obtenidos en [17] y [18] en una implementación de la arquitectura propuesta en [19].

# Publications composing

# the PhD Thesis

# 1

# Managing XACML systems in distributed environments through Meta-Policies

| | |
|---|---|
| **Title**: | Managing XACML systems in distributed environments through Meta-Policies |
| **Authors**: | Daniel Díaz-López, Ginés Dólera-Tormo, Félix Gómez-Mármol, Gregorio Martínez-Pérez |
| **Type**: | Journal |
| **Journal**: | Computers & Security |
| **Impact factor (2014)**: | 1.031 |
| **Publisher**: | Elsevier |
| **Volume**: | 48 |
| **Number**: | 2 |
| **Pages**: | 92-115 |
| **Year**: | 2015 |
| **Month**: | February |
| **DOI**: | http://dx.doi.org/10.1016/j.cose.2014.10.004 |
| **State**: | Published |

Table 1: Managing XACML systems in distributed environments through Meta-Policies

COMPUTERS & SECURITY 48 (2015) 92–115

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

# Managing XACML systems in distributed environments through Meta-Policies

Daniel Díaz-López [a,*], Ginés Dólera-Tormo [a], Félix Gómez-Mármol [b], Gregorio Martínez-Pérez [a]

[a] Departamento de Ingeniería de la Información y las Comunicaciones, Universidad de Murcia, 30100, Murcia, Spain
[b] NEC Laboratories Europe, Kurfürsten Anlage 36, 69115, Heidelberg, Germany

ARTICLE INFO

*Article history:*
Received 12 September 2013
Received in revised form
13 August 2014
Accepted 14 October 2014
Available online 1 November 2014

*Keywords:*
XACML
Access control system
Distributed environments
SAML
Access control policy
Policy management

ABSTRACT

Policy-based authorization systems have been largely deployed nowadays to control different privileges over a big amount of resources within a security domain. With policies it is possible to reach a fine-grained level of expressiveness to state proper responses of a system against multiple access control requests. In this context, XACML has achieved a big popularity between both industry and academy as a standard for the definition of access control policies, as well as an architecture for the evaluation of authorization requests and for the issuing of authorization decisions. However, the applicability of XACML is still not clear in collaborative and distributed environments composed of several security domains sharing the access control over some specific resources. Such a circumstance manifests when many security domains can simultaneously define the behavior that a resource will have upon received authorization requests, like for instance an organization with many subsidiaries, a company with a service virtualization business model, etc. In this paper we propose a solution to reach an effective distributed policy management considering that a number of policies in one domain may be confidential. To this end, the default XACML architecture has been redefined in order to use i) Master and Slave PAPs to communicate security domains, ii) Meta-Policies to define privileges over access control policies (the policies become the managed resources) and iii) SAML extensions to protect the policy management messages which flow between security domains. The experiments and the defined scenarios in the paper prove the validity of the proposed solution.



## 1. Introduction

Enterprises and corporations are usually composed of different working areas or departments, namely: human resources, operations, business office, administrative office, etc. And traditionally, for each of these sections there are specific access control solutions which have been commonly developed on a generic way to suit different application scenarios and manage access privileges on the information assets they manage.

Additionally, in this context each working area implements access control rules that handle its own information and resources and are, somehow, enforcement points. Such

* *Corresponding author*. Tel.: +34 868 887 646.
E-mail addresses: danielorlando.diaz@um.es (D. Díaz-López), ginesdt@um.es (G. Dólera-Tormo), felix.gomez-marmol@neclab.eu (F. Gómez-Mármol), gregorio@um.es (G. Martínez-Pérez).
http://dx.doi.org/10.1016/j.cose.2014.10.004
0167-4048/

atomization hinders from having a global vision of high-level security policies of the company and many times impedes having a complete integrated security system.

Among the plentiful private solutions for resource management, a widely accepted standard has emerged, named XACML (eXtensible Access Control Markup Language) (Moses et al., 2005) and defined by the OASIS consortium, like an effort to define an XML-based common language for formulation of access control policies making possible to manage efficiently different resources, including those belonging to the information system of an organization. XACML has been used in many deployments, has constituted the base for other standards and there are many research groups working on it worldwide (XACML References and Products, Version 1.85, June 2011; Martin et al., 2006).

XACML defines a schema for access control policies, but it also defines the schema for an access request and the associated response. For the definition of access control policies, XACML has 3 levels of elements: PolicySet, Policy and Rules, whereby the allowed Actions are defined on a specific Resource (which may be a data, a service or a system component) by a particular Subject (access requester entity) within a determined environment in an organization. The access control policies are contained in an element called PAP (Policy Administration Point) within the XACML architecture.

The defined architecture for XACML has been mainly designed (and widely validated) for an environment having a set of centralized policies, which are usually managed by a single PAP. However, this standard can not be so easily applied in more distributed environments (Hu et al., 2006), specially when several authorization architectures and hence several access control policies (clustered in PAPs) are deployed.

A distributed environment is understood in this research in those situations where there are multiple independent security domains which share control over some common elements, like the one presented in an organization composed by multiple subsidiaries, which can manage its own resources (i.e. information, software, services) but having in mind the general policies of the organization. Another situation for a distributed environment, which is more common nowadays, is due to the appearance of service virtualization like a new business model, which poses the existence of multiple providers doing collaboration around a complex service ecosystem in order to compose better services to customers. These multiple providers will also define in a particular way the conditions over which they are willing to collaborate, therefore the deployment of the service depends on the liaison of the different providers. This can be observed, for instance, in a cloud computing context where many providers are involved around a single service: infrastructure provider (which provides the equipment like servers, storage and network to support the service), application provider (which provides software like email, file processors and test environment that deliver the service), data provider (which provides well structured datasets that can be used like an input for the service), etc. Each provider (representing a security domain) is required to compose the service and a coordination of terms of use have to be done between the providers to reach a successful and secure service composition. This coordination can be achieved employing different provider's access control policies referring to the terms of use of its resources.

Additionally, the architecture defined by the standard has a local approach, since it does not include interactions between different XACML architectures, like it would be supposed, for example, in the case of large corporative environments where a headquarter office expects to manage some parts of the access control policies of its subsidiaries, or in the case where a unique organization has different local XACML architectures for different purposes or roles but all of them need to be managed by a root server that sets general-purpose policies.

In order to tackle the aforementioned shortcomings, in this paper we aim to resolve the emerging question of how to manage the access control functionality of a remote resource (i.e. that one belonging to another security domain) in a safe and accurate way using the concept of Meta-Policies. The access control functionality of a resource means the definition of the general behavior that such resource will claim upon any authorization requests, and not just the turn on/off of a resource functionality once, as it usually happens in certain remote control systems (Yang, 2011). This general behavior in the context of our research is defined through XACML access control policies.

Finally, we also aim to provide a solution to the situation when the access control functionality of a resource is shared between different distributed security domains. That is to say, when many security domains can concurrently define the behavior that a resource will have against authorization requests, like for instance an organization with many subsidiaries, a company with a service virtualization business model, etc.

Therefore, the solution presented in this paper aims to enable a root PAP (later on defined as Master PAP) to effectively manage different policy sets belonging to operationally independent but closely linked XACML architectures. Furthermore, each XACML architecture should perform its own access control functions in order to ensure that only some authorized external/internal XACML domains and its corresponding administrators can manage certain policies over its specific local XACML elements (subjects, actions and resources) and to prevent a leakage of confidentiality.

The remaining of the article is organized as follows. We further describe the aforementioned limitations of XACML in Section 2 and present some related work in the field of management of access control policies and practical applications in Section 3. In Section 4, a novel architecture to manage policies in a distributed access control system is presented as one of the main contributions of this document. Specifically, we define the elements of the architecture and a set of operations to administer remote access control policies. Then, we introduce the concept of Meta-Policies, used to define the privileges of administrators when managing local and remote policies. Next, in Section 5 we extend this solution with an SAML-based transport mechanism which includes protocols and assertions, and at the same time encloses a security mechanism related with authenticity and validity of queries and responses. Additionally, we conduct some experiments

related with distributed policy management operations in Section 6. In order to validate the strengths of the architecture against possible attacks, an analysis related to security of communications and assurance of confidentiality in policies is done in Section 7. We finally conclude the article in Section 8 and present some future research lines derived from this work.

## 2. Problem statement

The architecture described in the XACML specification (Moses et al., 2005) is composed of 4 main elements, namely: i) PAP (Policy Administration Point) is the element where PolicySets, Policies and Rules are created and maintained, ii) PDP (Policy Decision Point), that reaches an authorization decision based on the results of the evaluation of policies, iii) PEP (Policy Enforcement Point), that receives the initial access control requests for a resource and applies the access control decision issued by the PDP, and iv) PIP (Policy Information Point) which in practice is a data repository for the managed elements by the access control system and can be useful for the PDP to make the authorization decision. A detailed description of the process of resolution of an access request or authorization decision can be found in Moses et al. (2005).

Nowadays, there are some XACML implementations, mainly focused on XACML 2.0, such as XACMLLight (Gryb, 2012) and SUNXACML (Sun's XACML Implementation, June 2006), which support all mandatory features (functions, components, data types) defined in the XACML specification. A comprehensive list of implementations of XACML can be also found in XACML References and Products, Version 1.85 (2011).

However, the specified XACML architecture is limited since it mainly works in a single security domain and it is not always suitable for distributed environments where several security domains need to interact to define the allowed usage of resources, such a situation might occur in the case where a security domain (customer) manages the access to a resource that is actually hold in another security domain (service provider), such as in cloud computing environments. Here, the service provider should grant, under certain circumstances, some ability to the customer to enable the resources management, but it should also take care that its own usage directives about the resources are respected. On the other hand, the customer should guarantee that in the management of the resources, it does not make a disclosure of internal directives that are not needed for the resources management or that can cause a management information leakage. To this end, a proper autonomy and confidentiality between security domains need to be addressed, allowing an interaction between domains in a distributed environment. XACML 3.0 has performed some work in this direction, defining the Administration and Delegation Profile (Parducci and Lockhart, 2010; Blasch et al., 2012), where an administrator can delegate the right to other administrator to manage a set of resources. Nevertheless, the exchange of policies between PAPs belonging to the same or different organizational units is not possible even if they are related or there is an explicit relationship.

To understand the challenges involved in a distributed environment, let us imagine a large corporation composed of a central office and multiple subsidiaries. We may consider that the central office and each of its subsidiaries are security domains which independently implement an XACML architecture with their own access policies (established in a PAP) to manage their own resources, as shown in Fig. 1. Since this is the same corporative context, the central office will need to have an appropriate management over the XACML access control policies of the subsidiaries, in order to establish, for instance, a set of common policies for all subsidiaries (depending for example on some mandatory corporate regulations) or to assign specific policies to each one (depending for example on the type of service that each subsidiary provides), but at the same time allowing that each subsidiary implements its own local policies. Similarly, in another case the central office could retrieve a copy of the policies that are being applied in a subsidiary in order to have an overview of the applicability of best practices in security regarding a specific authorization context, but without infringing the confidentiality of certain local policies which should not be disclosed out of the subsidiary. Thus, in this case there is a need to manage efficiently, from a central XACML architecture, a specific set of access control policies hosted in distributed XACML architectures, allowing the implantation and recovery of policies related to certain resources that have been defined between the involved domains as resources under a common management.

In an XACML architecture there is possibility for conflicts between policies i.e. when a set of policies are applicable to the same request (Target) but they proclaim different authorization decisions (Permit, Deny, No applicable, etc). XACML 2.0 and XACML 3.0 provide combining algorithms which are intended to resolve policy conflicts, and additionally in the research field there are some proposals that complement the XACML specification in order to detect and resolve conflicts using different techniques (Huonder, 2010; St-Martin, 2012). In a context of distributed policy management, it is reasonable to think about the existence of conflicts between policies from different security domains, which must be resolved initially by the combining algorithm installed in the XACML architecture which is processing the authorization decision request.

Yet, in order to reach a distributed policy management through different XACML architectures, there are a number of constraints that need to be considered:

- Some policies, or a portion of them, hosted in a security domain (which can be integrated by an XACML architecture) may be confidential in a specific context. Thus, only some policies, or parts of them, are allowed to flow towards other domains; so this poses the need to control the policies that go away from a security domain.
- A security domain may have certain autonomy to manage resources locally i.e. policies referring to a specific and local target (subject, resource, action) without the intervention of another security domain. Therefore, there should be a restriction about the implantation of policies coming from other domains that are focused on local resources.
- A security domain has to manage the version and location of policies that it has implanted in other security domains

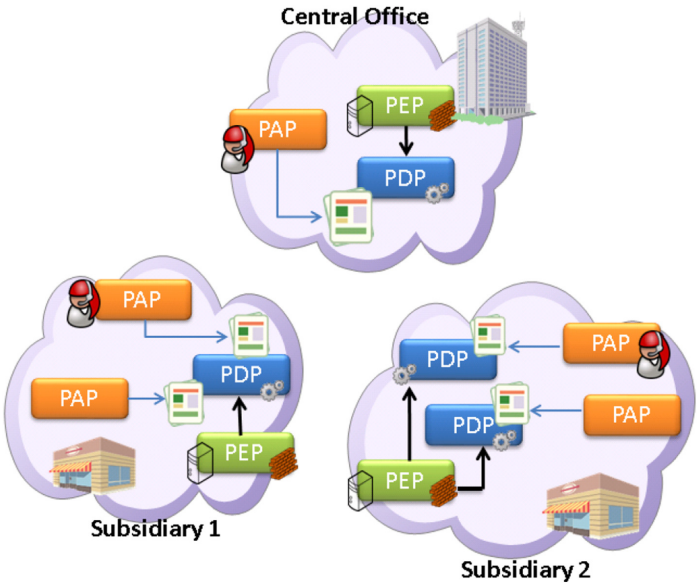


**Fig. 1 – Corporative scenario with independent XACML architectures.**

and attempt to keep them updated in order to guarantee the expected behavior in the authorization decisions.

## 3. Related work

Distributed systems, like grid computing environments (Foster, 2002), are commonly composed of different services and systems which need to be processed by an authorization system which controls how these can be used. XACML is proposed in Lorch et al. (2003) as the access control language to manage distributed resources in a grid computing environment and presents a solution which does a unified and centralized management of XACML policies by one Policy Manager which feeds policies to PDPs.

Additionally, some adaptations to XACML standard have been proposed in the academy in order to make it more versatile, for example Ardagna et al. (2009) presents some improvements to XACML standard such as the inclusion of metadata about digital certificates (credentials) as part of the access request information used for reasoning about an authorization decision, obtaining in this way a credential-based access control. Ardagna et al. (2009) also uses the concept of abstractions and recursions integrated with XACML, using XQuery language like the key component to query XML data. Finally, Ardagna et al.'s (2009) paper considers the use of dialogs between XACML components so that the PDP can request just the needed information to resolve an authorization request, avoiding privacy issues for exposure of credentials but also indeterminate states due a lack of information. These novelties are presented but exercises that prove its validity are not included.

The setting of policies in an environment with multiple systems requires the definition of some rules for an homogeneous application and management of the policies. In this sense, in Hosmer (1992) the concept of Meta-Policy is introduced to define those rules and also some kinds of Meta-Policies for different purposes are suggested: policy description, organization control, policy relationship, multipolicy coordination, etc. For example, organization controls Meta-Policies include the description of the policy renewal or modification process, whereas policy relationship Meta-Policies define the hierarchical or collegial relationships between policies. Therefore, Meta-Policies become a key element due to their function over the policies execution in a security domain. Additionally, in Khnhauser (1995) there is a description of the concept of Meta-Policy concerning its applicability in coordination functions in contexts with many security domains. Furthermore, a Conflict Matrix and Cooperation Matrix are proposed, which include functions to resolve conflicts and precedence issues between policies, respectively. Likewise, in Lupu and Sloman, 1997 the Meta-Policy concept is also addressed in the context of identification of application-specific conflicts between policies, which are expressed as logical predicates.

Rao et al. (2009) tackles the problem of integration of policies when two or more policies decide over a resource. Even if the combination algorithms proposed by the XACML standard are the basis for more common conflict cases, Rao et al. (2009)

use them as starting point and consider another more complex cases for which develop an algebra (FIA, Fine-grained Integration Algebra) in order to allow the definition of integrated policies which fit some specific integration requirements associated with request, effects and domains. The representation of policies is done thorough MTBDDs (Multi-Terminal Binary Decision Diagrams).

Moreover, an interesting XACML model focused on distributed environments is proposed in Demchenko et al. (2008) with the name OHRM (Obligations handling reference model). OHRM defines the dataflow for generic authorizations and obligations generated by a central authorization service (SCAS) and executed by remote PEPs. SCAS in charge of the access policy management of the resources of all domains. This model may be used in grid and networking applications, opening the possibility for issuing obligations which manage accounts, quotas, usable resources, logging and accounting. Another similar model is stated in Peters et al. (2007) which proposes extensions of COPS (Common Open Policy Service) protocol to transport XACML policies from a centralized PDP to remote PEPs. Proposal in Peters et al. (2007) is based on a SicAri platform which allows to support service-oriented applications in ubiquitous internet context. Peters et al. (2007) lacks of an implementation of the proposal and also establishes as future research line policy negotiation considering policies from different security domains.

Additionally, in Garzoglio et al. (2011) an XACML profile is proposed defining in a detailed way attributes for subject, resource, action, environment and obligations to promote interoperability between authorization decisions in grid environments. The idea of having a centralized authorization system is interesting as long as the authorization service can reply properly to all the multiple queries and is able to manage all the resource attributes belonging to the grid.

Basically, we noted that all these solutions mainly consider a centralized policy management, defining a unique element of the architecture as a policy generator, and neglecting the idea that in a multi-domain context each domain/subdomain may have certain autonomy and local policies. This means that even if one domain can generate and impose policies regarding a group of resources, there might be also other policy generators in other domains that should be considered.

Regarding the exchange of authorization decisions between domains, in DeCouteau et al. (2008) a profile of XACML is defined to support the exchange of authorizations statements between a consumer and service health care organizations, through the definition of common attributes used in the policies evaluation process. Here, it is assumed that each domain manages its own access control policies and just final decisions flow between them.

Finally, in Lischka et al. (2009) an architecture for evaluation of XACML access control policies in a distributed way is proposed. This architecture is applied in a context where an authorization decision in one local domain depends on the authorization decisions of other remote domains. It is based on the idea of referencing external policies and attributes inside a policy of a local domain, in such a way that when an authorization decision needs to be solved for that policy, an authorization request is launched towards the remote domains hosting the referred policies. In this way, the responses of the remote domains will compose a single authorization response in the local domain. This architecture is applicable in a distributed environment but, unfortunately, it is significantly inefficient since, for each single authorization request in a local domain, a remote authorization request towards different remote domains has to be done, which represents administrative traffic that can congest the network and introduce latency. A comparison of our proposal with Lischka et al. (2009) is done in Section 6.

## 4. Distributed access control policies management

### 4.1. *Definition of new entities in the XACML access control architecture*

In this paper we propose an architecture to support XACML access control policies management in a distributed way, based on the communication between the policy management entities of a regular XACML architecture, namely the PAPs, for a specific domain.

Even though in a distributed system all the PAPs could be at the same level, we have to differentiate the role that PAPs hold during the time that a management operation is developed. In this way, we differentiate the PAP which starts the management operations from the PAPs that receive and perform such operations. To this end, we introduce two new definitions within a distributed policy management architecture.

- Master PAP: It consists of a PAP element in an XACML architecture responsible of initiating policy management operations over policies intended to other PAPs that belong to XACML architectures from the same or a different organization. For example, a Master PAP located in a headquarter could distribute a set of policies to some PAPs located in subsidiaries in benefit of a company constraint that aims to have uniformity about a specific authorization context (e.g. access to the buildings on weekends) in all the enterprise branches. The management done by the Master PAP can be achieved performing a number of operations (as we will see later) over a Policy or a PolicySet, or even parts of them, such as ID, target, policy combining algorithm, etc.
- Slave PAP: It denotes a PAP in an XACML architecture which executes the policy management operations coming from one or many Master PAPs. It must be able to have local policies to manage privileges over local resources, but it also should allow the execution of certain policy management operations, started in one or many Master PAPs, aiming to be applied over certain local resources.

Both "Master PAP" and "Slave PAP" are not fixed properties of the different PAPs, but rather the operational mode (role) of a given PAP in a specific context and time. That is, a PAP can act as a Master PAP with a group of certain Slave PAPs for a specific service management, but at the same time act as Slave PAP for other PAPs.

Additionally, there should be an authorization system controlling the privileges (Wei et al., 2011) to perform some

kind of operations (defined in Section 4.2) on distributed policies established in a Master PAP and Slave PAP. In order to manage these privileges in a simple and efficient way we propose the use of an XACML architecture based on policies to control operations over distributed policies. These mentioned policies are called "Meta-Policies" to differentiate their purpose from a regular XACML policy. With this Meta-Policies architecture, defined in Section 4.3, it is possible to implement restrictions about confidentiality and privacy of policies and autonomy of XACML architectures.

### 4.2. *Operations related to distributed access control policies management*

The concern to achieve a distributed access control policies management involves all kind of operations related to the control of remote policies, in such a way that a system, represented by a Master PAP, can easily generate changes in the behavior of a remote system, represented by a Slave PAP. These operations (as shown in Table 1) could involve actions over XACML elements, i.e. PolicySet and Policy, but also over inner parts and attributes of them. One useful operation is "diffuse", which allows a Master PAP to send a specific Policy or PolicySet towards a specific target or group of targets, asking for the installation of such Policy in the Slave PAP(s). Likewise, it is necessary a "delete" operation to produce the removal of a specific Policy in a Slave PAP, for example in the case when the policy has no longer applicability or is wrong. Additionally, intermediate situations could be possible: in the case that a new version of an existent Policy attempts to be installed but also keeping the old version, an "update" operation would be required.

When a Master PAP manages remote policies, it would be necessary for it to know detailed information about a deployed Policies and PolicySets in a Slave PAP, e.g. version, target, effect, full body, etc, so a "policy attribute query" operation is needed too, allowing to recover this data from a unique Policy identifier (Policy id) and the name of the concerned attribute. But in case the Master PAP does not know the id of a specific Policy, it is also necessary to include an operation which allows recovering the list of Policy identifiers deployed in a Slave PAP.

In the case of a main system that needs to know which policies in a remote system are applicable for a specific subject or resource on account of some evaluation, validation or statistics purposes, or if the main system is interested in knowing which policies allow a specific subject to perform a specific action in a remote system, then it is imperative the inclusion of a "query" operation which recovers all these related policies and returns them towards the Master PAP.

If we consider the big scope of XACML policies that can be handled in a simple domain (which includes different combinations of many types of subjects, resources and actions), and if we then consider that another domain has the possibility to manage this group of policies (or part of them), as in our case, then the number of possible operations would be considerable and so would be its functionality. For our development we have considered a group of basic operations (Diffuse, Delete, Update, Policy Query, Attribute Policy Query), but keeping in mind that they are extensible according to more complex scenarios.

### 4.3. *Policy management with Meta-Policies*

In a standalone XACML architecture, the policies have to be controlled locally by some administrator, whilst, in the context of distributed policy management, the distributed policies are controlled, in some way, by a remote administrator. In both cases, it is necessary to define a mechanism to manage the administrator privileges (Wurster and Van Oorschot, 2010). In order to define such mechanism in the context of distributed policy management, we have to note that with the XACML specification, it is possible to define a PolicySet (1), which can include a group of Policies (2); and these last ones can include, in turn, a set of Rules (3). The applicability of a PolicySet, Policy or Rule is determined by the Target (4), which specifies a resource, where resource stands for: data, service or system component.

$$\begin{aligned} PolicySet = \langle & Target \\ & \| \quad (\varnothing \mid Policy_1, \ldots, Policy_n) \\ & \| \quad PolicyCombiningAlgorithm \\ & \| \quad (\varnothing \mid Obligation_1, \ldots, Obligation_n) \rangle \end{aligned} \tag{1}$$

**Table 1 – Main operations for distributed access control policy management.**

| Operation | Description |
|---|---|
| Diffuse Policy | Spread a new Policy/PolicySet to a list of Slave PAPs. A response from each Slave PAP is expected indicating the result of the remote installation. |
| Delete Policy | Delete a remote Policy/PolicySet in a list of Slave PAPs. A response from each Slave PAP is expected indicating the result of the remote deletion. |
| Update Policy | Update an existent Policy/PolicySet with a new version. It has to be possible to indicate the version to be replaced and the persistence of the old version. A response from each Slave PAP is expected indicating the result of the remote update. |
| Policy Query | Get a copy of an installed Policy/PolicySet in a Slave PAP. It has to be possible to indicate an id, target or context request as the search parameter. A response from each Slave PAP is expected containing the Policy/PolicySet if it was found. |
| Policy Attribute Query | Get attributes from one or more Policy/PolicySet installed in a Slave PAP. It has to be possible to indicate a specific id and attribute name. A response from each Slave PAP is expected containing the attribute if it was found. |

$$\begin{aligned} Policy = \langle Target \\ \| \quad (\varnothing \mid Rule_1, \ldots, Rule_n) \\ \| \quad RuleCombiningAlgorithm \\ \| \quad (\varnothing \mid Obligation_1, \ldots, Obligation_n)\rangle \end{aligned} \tag{2}$$

$$\begin{aligned} Rule = \langle Target \\ \| \quad (\varnothing \mid Condition_1, \ldots, Condition_n) \\ \| \quad Effect\rangle \end{aligned} \tag{3}$$

$$\begin{aligned} Target = \langle (\varnothing \mid Subject_1, \ldots, Subject_n) \\ \| \quad (\varnothing \mid Resource_1, \ldots, Resource_n) \\ \| \quad (\varnothing \mid Action_1, \ldots, Action_n) \\ \| \quad (\varnothing \mid Environment_1, \ldots, Environment_n)\rangle \end{aligned} \tag{4}$$

In the context of distributed policy management, a policy is actually a piece of data, specifically an XML file, so the XACML policies could be considered as a typical resource itself. Thus, we propose the use of an XACML architecture as the instrument to manage local and distributed XACML policies as resources within an organization. Moreover, we incorporate the concept of Meta-Policies (5) (previously named in Section 3), which are policies including rules (6) that describe the privileges related to the policies maintained at all the PAPs of an organization.

In this case, the resource field within the target (7) will be, in fact, a PolicySet or a Policy. Including these two elements, the solution provides the same level of granularity that it is provided by the XACML standard (Moses et al., 2005). The actions to control the resource will correspond to the set of possible actions (diffuse, delete, update, policy query, acquire attributes, etc.) applicable on a local or remote Policy or parts of it. Finally, the subject element will represent any human administrator or software entity that requires access to the policies, in order to manage them.

$$\begin{aligned} MetaPolicy = \langle Target \\ \| \quad (\varnothing \mid Rule_1, \ldots, Rule_n) \\ \| \quad RuleCombiningAlgorithm \\ \| \quad (\varnothing \mid Obligation_1, \ldots, Obligation_n)\rangle \end{aligned} \tag{5}$$

$$\begin{aligned} Rule = \langle Target \\ \| \quad (\varnothing \mid Condition_1, \ldots, Condition_n) \\ \| \quad Effect\rangle \end{aligned} \tag{6}$$

$$\begin{aligned} Target = \langle (\varnothing \mid Subject_1, \ldots, Subject_n) \\ \| \quad ((\varnothing \mid Policy_1, \ldots, Policy_n) \mid \\ \quad (\varnothing \mid PolicySet_1, \ldots, PolicySet_n)) \\ \| \quad (\varnothing \mid Action_1, \ldots, Action_n) \\ \| \quad (\varnothing \mid Environment_1, \ldots, Environment_n)\rangle \end{aligned} \tag{7}$$

In the context of distributed policy management, the Meta-Policies are used in the Master PAP to control any policy management operation over some Slave PAPs. And in the case of a Slave PAP, the Meta-Policies are used to control the actions that any Master PAP can execute over its policies. Thanks to the expressiveness of XACML, it is possible to have a fine-grained control over the management operations, because a Meta-Policy could consider subjects, actions, resources (i.e. policies) and authorization decision attributes, like factors for the evaluation. For example in the case of a Master PAP, it is possible to define a Meta-Policy specifying that only a group of policies (i.e. resource) are allowed to be diffused (i.e. action) to certain group of Slave PAPs and, once the diffusion is completed, send an informative message to the main responsible of the XACML architecture (i.e. obligation). On the other hand, in a Slave PAP it is possible to define a Meta-Policy which states that a Master PAP (i.e. subject) can only create policies (i.e. action) referring to a certain group of local assets (i.e. resource) or even a Meta-Policy which states that a Master PAP (i.e. subject) can only query information of policies (i.e. action) that applied for a single resource during a specific interval of time (i.e. environment) and with the consent of a local administrative authority (i.e. condition).

The XACML architecture implementing the Meta-Policies should be independent of the XACML architecture supporting the regular policies of the organization. In Fig. 2 a policy management scenario between a central office and a subsidiary is shown. Both locations have an XACML policies architecture (represented by the round dot type border) composed of PEP, PDP, PIP and PAP, and additionally a Meta-Policies architecture (represented by the dash type border) to manage the access over the XACML policies. The point of intersection between these two architectures (policies and Meta-Policies) is the Master and Slave PAP, which in this case are kept in the central office and in the subsidiary, respectively. Additionally the Master and Slave PAP have two roles, since they represent the "policies" for the XACML policies architecture and the "resource" for the Meta-Policies architecture.

Among the advantages of reusing the same XACML architecture is the saving of time and effort in its implementation and deployment, since it is not necessary to develop a new Policies language managing Policies, as the XACML concepts associated with resource administration are directly applicable to the administration of Policies. Additionally, XACML is flexible enough to allow the expressiveness of applicable actions on the Policies, the conditions on which they must be conducted and the obligations involved in an issued authorization decision.

## 5. Security extensions for distributed access control policies management

As already mentioned, XACML as such is a language for describing Policies, access control requests and responses to those requests. Moreover, it specifies architectural components to implement an XACML access control system. However, it does not define protocols or transport mechanisms among the interacting parties (PDP, PEP, PAP, Attribute Authority, context handler, etc). A standard commonly used to fill these gaps is SAML (Security Assertion Markup Language)

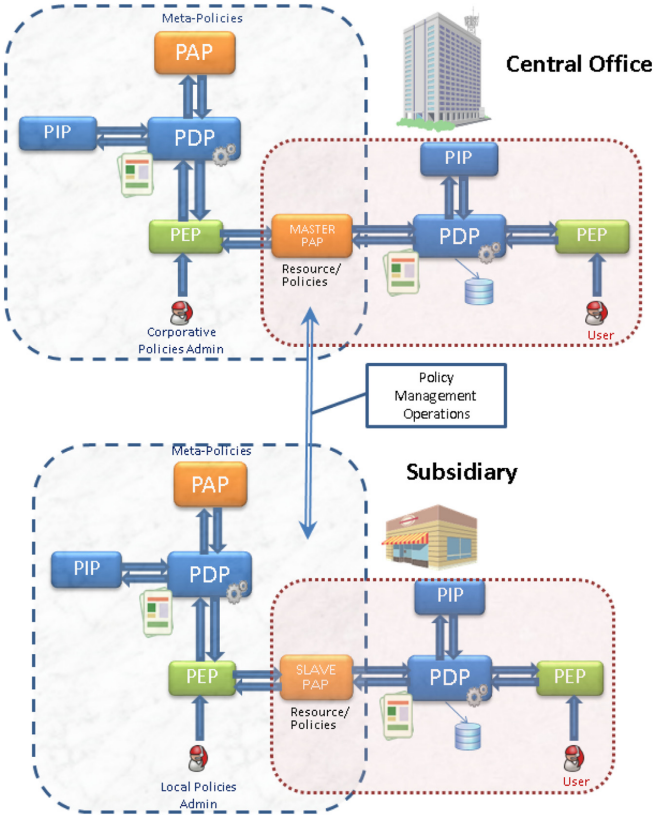


**Fig. 2 – Architecture for distributed access control policies management.**

(Hughes and Maler, 2006; Vacca, 2012), which defines assertions and protocol mechanisms (Cantor et al., 2005a, 2005b), and additionally includes information for the identification and validation of the assertions, such as identity assertion issuer, validity period and digital signature.

The SAML 2.0 profile of XACML v2.0 (Anderson and Lockhart, 2005; Garzoglio et al., 2009) defines 6 types of queries and statements, applicable to an XACML generic architecture. These types are:

- `AttributeQuery`: SAML request used by the PDP to query the PIP about subject or resource attributes which are used to make an authorization decision.
- `AttributeStatement`: A statement with one or more attributes, used in response to an `AttributeQuery`.
- `XACMLPolicyQuery`: SAML request used by a PDP to request policies to a PAP.
- `XACMLPolicyStatement`: A statement containing one or more policies, used in response to a `XACMLPolicyQuery`.
- `XACMLAuthorizationDecisionQuery`: SAML request containing an authorization decision request issued by a PEP to a PDP.
- `XACMLAuthorizationDecisionStatement`: A statement with an authorization response corresponding to a `XACMLAuthorizationDecisionQuery`.

With the above queries and statements provided by SAML, it is possible to protect, transport and request XACML schema instances used in an XACML architecture to resolve an authorization request. However, there is no mechanism to support the policy management operations defined previously in Section 4, in which the exchange of messages is developed between at least two security domains (i.e. XACML architectures) and with different needs of transportation according to the executed operation. For example in the case of a diffuse policy operation, a complete Policy or PolicySet needs to be transported in order to be installed in a Slave PAP, but in the case of an attribute policy query operation, both an identifier of the

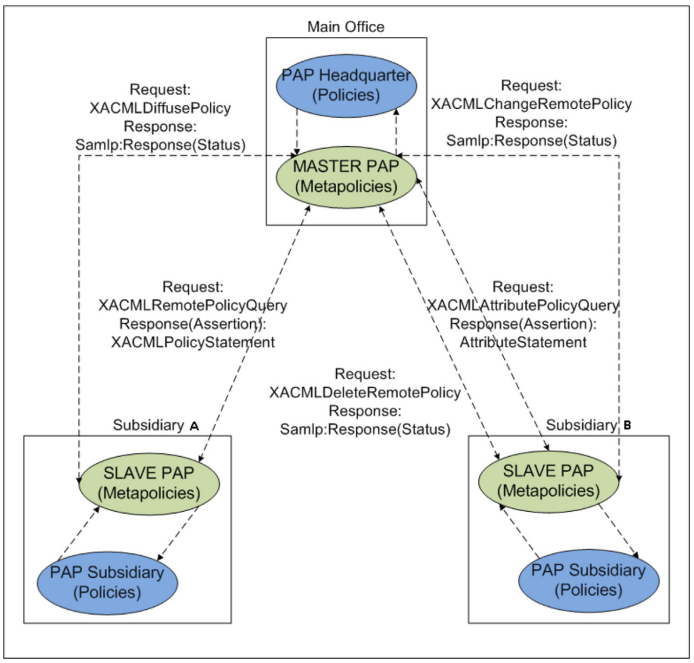


**Fig. 3 – XACML model with SAML queries and statements.**

policy and attribute required need to be included. Additionally, each operation has a response or an expected answer, which has to be returned to the Master PAP and corresponds effectively to the query done in the previous operation.

Therefore, for each policy management operation, it is needed to develop a specific SAML schema which includes the appropriate attributes and elements, allowing always flexibility in its structure to guarantee extensibility and applicability. Thus, we propose a new group of queries and responses in subsections 5.1 and 5.2, respectively. A graphical representation of the message flow (query/response) in a distributed policies management context is shown in Fig. 3, being this context also applicable for the corporative scenario indicated in Fig. 1.

Additionally, the context of policy management through PAPs also requires a complete authentication of the involved peers, due to the fact that it would be very risky to receive operation queries or responses from a fake Master or Slave PAP. This flaw is covered by SAML, since SAML schemas include information needed to identify and validate the contents of the assertions, such as the identity of the assertion issuer, the validity period of the assertion, and the digital signature of the assertion.

### 5.1. *Queries*

We define a new set of SAML queries focused on the possible operations (diffuse, delete, update, policy query, acquire attributes, etc.) on any local or distributed Policy belonging to a distributed access control system. In this way, we define the following queries which use the SAML complex type `RequestAbstractType` as a base. `RequestAbstractType` includes in its elements: <saml:Issuer>, which identifies the entity that generated the request message and <ds:Signature> which is an XML signature (Bartel et al., 2008; Rosen et al., 2012) that authenticates the requester and provides message integrity.

- `XACMLDiffusePolicy`: Used by the Master PAP to spread Policies or PolicySets towards a set of Slave PAPs. The difussion of Policies or PolicySets toward the Slave PAP will depend on the privileges to diffuse certain policies defined in the Meta-Policies of the XACML architecture in the Master PAP side. The schema for `XACMLDiffusePolicy` and `XACMLPolicyStatement` is indicated in SAML schema 1.

```
<xs:element name="XACMLDiffusePolicy"
            type="XACMLDiffusePolicyType"/>
 <xs:complexType name="XACMLDiffusePolicyType">
  <xs:complexContent>
   <xs:extension base="samlp:RequestAbstractType">
    <xs:choice minOccurs="0" maxOccurs="unbounded">
     <xs:element ref="xacml:PolicyStatement"/>
    </xs:choice>
   </xs:extension>
  </xs:complexContent>
 </xs:complexType>

<xs:element name="XACMLPolicyStatement"
            type="XACMLPolicyStatementType"/>
 <xs:complexType name="saml:XACMLPolicyStatementType"/>
  <xs:complexContent>
   <xs:extension base="samlp:StatementAbstractType">
    <xs:choice minOccurs="0" maxOccurs="unbounded">
     <xs:element ref="xacml:Policy"/>
     <xs:element ref="xacml:PolicySet"/>
    </xs:choice>
   </xs:extension>
  </xs:complexContent>
 <xs:complexType>
```

**SAML schema 1** — `XACMLDiffusePolicy` **and** `XACMLPolicyStatement`**.**

- `XACMLDeleteRemotePolicy`: Used by the Master PAP to generate an erasing operation over Policies or PolicySets of a Slave PAP. The deletion of Policies or PolicySets in the Slave PAP will depend on the privileges to delete certain policies defined in the Meta-Policies of the XACML architecture in the slave PAP side. The schema for `XACMLDeleteRemotePolicy` is indicated in SAML schema 2.

```
<xs:element name="XACMLDeleteRemotePolicy"
            type="XACMLDeleteRemotePolicyType"/>
 <xs:complexType name="XACMLDeleteRemotePolicyType">
  <xs:complexContent>
   <xs:extension base="samlp:RequestAbstractType">
    <xs:choice minOccurs="0" maxOccurs="unbounded">
     <xs:element ref="xacml:PolicySetIdReference"/>
     <xs:element ref="xacml:PolicyIdReference"/>
    </xs:choice>
   </xs:extension>
  </xs:complexContent>
 </xs:complexType>
```

**SAML schema 2** — `XACMLDeleteRemotePolicy`**.**

- `XACMLUpdateRemotePolicy`: Used by the Master PAP to generate a substitution in a Policy or PolicySet stored in a Slave PAP. It involves sending the new Policy and the particular version to be replaced and the persistence or not of the older version of such Policy in the Slave PAP. The change of the Policy or PolicySet in the Slave PAP will depend on the privileges to change certain policies defined in the Meta-Policies of the XACML architecture in the slave PAP side. The schema for `XACMLUpdateRemotePolicy` is indicated in SAML schema 3.

```
<xs:element name="XACMLUpdateRemotePolicy"
            type="XACMLUpdateRemotePolicyType"/>
 <xs:complexType name="XACMLUpdateRemotePolicyType">
  <xs:complexContent>
   <xs:extension base="samlp:RequestAbstractType">
    <xs:element ref="xacml:PolicyStatement"/>
    <xs:attribute name="DeletePrevious" type="boolean" use="optional" default="false"
        />
    <xs:attribute name="version" type="decimal" use="optional" default="0.0" />
   </xs:extension>
  </xs:complexContent>
 </xs:complexType>
```

**SAML schema 3** – `XACMLUpdateRemotePolicy`.

- `XACMLRemotePolicyQuery`: Used by the Master PAP to query a group of Policies or PolicySets, which are stored in a Slave PAP. The query can be addressed using a Policy identifier, a matching target or a Request Context. In any case the policies that are effectively returned from the Slave PAP to the Master PAP will depend on the privileges to query certain policies defined in the Meta-Policies of the XACML architecture in the Slave PAP side. The schema for `XACMLRemotePolicyQuery` is indicated in SAML schema 4.

```
<xs:element name="XACMLRemotePolicyQuery"
            type="XACMLRemotePolicyQueryType"/>
 <xs:complexType name="XACMLRemotePolicyQueryType">
  <xs:complexContent>
   <xs:extension base="samlp:RequestAbstractType">
    <xs:choice minOccurs="0" maxOccurs="unbounded">
     <xs:element ref="xacml-context:Request"/>
     <xs:element ref="xacml:Target"/>
     <xs:element ref="xacml:PolicySetIdReference"/>
     <xs:element ref="xacml:PolicyIdReference"/>
    </xs:choice>
   </xs:extension>
  </xs:complexContent>
 </xs:complexType>
```

**SAML schema 4** – `XACMLRemotePolicyQuery`.

- `XACMLAttributePolicyQuery`: Used to query for specific attributes of a remote Policy or PolicySet. Therefore, it contains the identifier of the Policy on which the query is performed and an attribute name to query. If the identifier of the Policy is not specified, but the attribute name is, it is assumed that the query is intended to obtain the indicated attribute of all the Policies in the Slave PAP for which the Master PAP has access. This enables the Master PAP to make queries such as: "get the ID of all the Policies", or "get the Target of a specific Policy". The schema for `XACMLAttributePolicyQuery` is indicated in SAML schema 5.

```
<xs:element name="XACMLAttributePolicyQuery"
            type="XACMLAttributePolicyQueryType"/>
 <xs:complexType name="XACMLAttributePolicyQueryType">
  <xs:complexContent>
   <xs:extension base="samlp:RequestAbstractType">
    <xs:choice minOccurs="0" maxOccurs="1">
     <xs:element ref="xacml:PolicySetIdReference"/>
     <xs:element ref="xacml:PolicyIdReference"/>
    </xs:choice>
    <xs:element ref="saml:Attribute"/>
   </xs:extension>
  </xs:complexContent>
 </xs:complexType>
```

**SAML schema 5** – `XACMLAttributePolicyQuery`.

### 5.2. *Responses*

SAML uses the `StatusResponseType` complex type as the basis for all responses to `RequestAbstractType` requests (the one used in the queries). This complex type contains several elements such as Issuer, Signature, Extensions and Status, and further defines a set of attributes used to associate the response to a specific query within an SAML context. The Status element is particularly important since it provides information on the status of resolution of the query. Within the Status element there is a `StatusCode` element (represented as an URN) with information related to the result of the request-response SAML communication process. However, although the specification defines some permissible `StatusCode`, there

is not an element related to the status of the policy management XACML process.

In order to integrate in a simple way a status element related to the resolution of an XACML access control request in the `StatusResponseType` message, we propose the use of the `StatusMessage` element (which is an optional element within the Status element that defines a string message that may be returned to the operator according to the specification) to indicate the status of an XACML request performed within the context of a distributed policies system.

The mandatory and simplest values that might be contained in the `StatusMessage` element can be: Committed and Failure, indicating the success or fail, respectively, of the asked operation in the Slave PAP. Yet, according to the implementation, different kind of values can be returned.

In the case of Failure, it could be possible to additionally indicate some kind of more specific information regarding what type of error occurred, namely: Request for a non-existent Policy element, Policy element being processed by another application, Policy parse errors, etc.

In order to match the defined queries in the previous subsection, we have to state the following considerations:

- The value of `StatusMessage` is necessary for the following types of XACML queries: `XACMLDiffusePolicy`, `XACMLDeleteRemotePolicy` and `XACMLUpdateRemotePolicy`, since the Master PAP needs to know whether the operations have been successfully completed or not. For instance, if the Master PAP sends a `XACMLDeleteRemotePolicy` to a Slave PAP in order to delete a policy already deployed, the Slave PAP would reply with a message like the one presented in SAML schema 6. In this message, the `InResponseTo` attribute specifies the identifier of the query so the Master PAP could relate which query this response corresponds to. It also specifies the issuer of this message, i.e. the Slave PAP identifier in this case. Finally, it indicates the success of the operation within the Status element including the `StatusCode` and the `StatusMessage` elements.

```
<samlp:Response ID="i-394850299771738593"
InResponseTo="5282749464276207842"
IssueInstant="2012-06-14T14:06:17.022Z" Version="2.0"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
 <saml:Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">SlavePAP</saml:Issuer>
 <samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  <samlp:StatusMessage Value="Committed"/>
 </samlp:Status>
</samlp:Response>
```

**SAML schema 6 – Successful SAML Response to a `XACMLDeleteRemotePolicy` operation.**

- For a query of type `XACMLRemotePolicyQuery`, the SAML element `XACMLPolicyStatement` is used as part of the response (as it is defined in the SAML 2.0 profile of XACML v2.0). SAML schema 7 shows an example of a response to a `XACMLRemotePolicyQuery`, hence including the requested policy. The requested policy is specified within the `PolicyStatement` element, which, in turn, is contained in an SAML assertion. The SAML assertion specifies additional details of the response, such as issue instant, the issuer of the assertion (the Slave PAP in this example), which could be used to establish a trust context.

```
<samlp:Response ID="i4723449756591206554"
InResponseTo="2282749444786209142"
IssueInstant="2012-06-14T14:06:16.934Z" Version="2.0"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
 <saml:Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">SlavePAP</saml:Issuer>
 <samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
 </samlp:Status>

 <saml:Assertion ID="-6261562949985739125" IssueInstant="2012-06-14T14:06:16.935Z"
     Version="2.0" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml:Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">SlavePAP
      </saml:Issuer>
  <saml:Subject>
   <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/>
  </saml:Subject>
  <xacml:PolicyStatement xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">
    --Here the Policy--
  </xacml:PolicyStatement>
 </saml:Assertion>
</samlp:Response>
```

**SAML schema 7 – Successful SAML Response to a `XACMLRemotePolicyQuery`.**

- For a query of type `XACMLAttributePolicyQuery`, the SAML element `AttributeStatement` is used as part of the response. In this case, this SAML element includes a `<saml:attribute>` with the name and value of the requested attribute. SAML schema 8 shows an example of a response to a `XACMLAttributePolicyQuery` where a Master PAP has asked an Slave PAP for the identifier of a given policy. Besides issuer information and timestamps to establish a security context, the Slave PAP includes the value of the requested attribute in the `AttributeValue` element.

```
<samlp:Response ID="i52930752670553351 56"
InResponseTo="7242749364272201812"
IssueInstant="2012-06-14T14:06:17.123Z" Version="2.0"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
 <saml:Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">SlavePAP</saml:Issuer>
 <samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
 </samlp:Status>

 <saml:Assertion ID="4388346244295603602" IssueInstant="2012-06-14T14:06:17.124Z"
     Version="2.0" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml:Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">SlavePAP
      </saml:Issuer>
  <saml:Subject>
   <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/>
  </saml:Subject>
  <saml:AttributeStatement>
   <saml:Attribute Name="POLICYID" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
       format:uri">
   <saml:AttributeValue>urn:oasis:names:tc:xacml:2.0:conformance-test:IIB007:policy</
       saml:AttributeValue>
   </saml:Attribute>
  </saml:AttributeStatement>
 </saml:Assertion>
</samlp:Response>
```

**SAML schema 8 – Successful SAML Response to a `XACMLAttributePolicyQuery`.**

## 6. Experiments and analysis

NEC Laboratories Europe (NLE) has been researching in last years on topics related with authorization systems, making focus on XACML as the standard that defines the procedures for the evaluation of authorization requests. Additionally, NLE has created its own XACML engine which has a local Java API for the execution of the basic operations over local XACML access policies (Lischka et al., 2009). This last implementation has been tested to fit all the mandatory functions according to the standard (Kuketayev, 2005) and over this implementation we have done some measurements.

In order to apply the proposed architecture in this paper to a real environment, we define a distributed scenario where a central office and many subsidiaries share the management of certain technological assets (i.e. information, hardware, software, etc). In this scenario the central office and each one of the subsidiaries make up an independent security domain with an XACML engine for managing the authorization decision. With such a setting, we could face two potential different situations, amongst others:

1. A set of assets are property of each subsidiary, but due its nature they must be managed in a joint way with the central office, specifically the followings assets: payroll information, database of intellectual property and customers database. To achieve the dual management, the subsidiaries must add (through a Meta-Policy) privileges for the central office to allow diffuse, change and query policies related with those previously defined assets. In this way the central office will be able to diffuse an access control policy to all the subsidiaries containing for

example the requirements that must be fulfilled to deliver access to those resources anytime, e.g.: only users with a management role are allowed to read and modify payroll, intellectual property and customer information. Additionally, each subsidiary can assign internally between its employees the management role, and also create its own access control policies to define who inside the organization is allowed to read and change those assets. Depending on the combination algorithm installed in the subsidiary XACML engine, this will allow the access only if the requester fits the requirements from the central office and/or from the subsidiary. In this first situation of the defined scenario the subsidiary acts like a Slave PAP and the central office acts like a Master PAP.

2. Another situation can be shown when a central office holds a set of IT laboratory resources (e.g. virtual machines) which are made available for its subsidiaries for the purpose of testing, learning or development of new products. The central office must add (through a Meta-Policy) privileges for a specific set of subsidiaries to allow diffuse, change and query policies related with those laboratory resources. In this way the subsidiaries are allowed to diffuse access control policies to the central office which define who in their offices is allowed to access to the resource and under what conditions. Additionally the central office can dispose internally their own access control policies to specify requirements about the kind of allowed secure connection protocol, trusted origin IP network, suitable access profile, etc. Depending on the combination algorithm installed in the central office XACML engine, this will allow the access only if the requester fits the requirements from the central office and/or from the subsidiary. In this second situation, the central office acts like a Slave PAP and the subsidiary like a Master PAP.

The two previously described situations have a real applicability, however the experiments included in this section will be based on the second one, mainly because this one concentrates more transactions over a single security domain (that one located in the central office) coming from all the subsidiaries performing distributed policy management operations addressed to the central office. This allows us to validate the behavior of the proposed solution against a complex scenario with multiple security domains. On the other hand, in the first use case the central office is the only one that starts management operations toward the security domains contained in the subsidiaries, but it is still a good scenario where our proposal may be applied.

Additionally, in order to guarantee an appropriate access control management in this second situation, the following requirements must be considered: 1) It is necessary to control the policies that go away from the central office (specifically when policy query operations are requested from the subsidiaries) because certain policies hosted in that security domain may have a confidential level, 2) There should be restrictions for the implantation of policies coming from the subsidiaries because in some cases the local security domain (i.e. the one in the central office) can have autonomy to manage certain resources locally. To overcome these constraints, a set of Meta-Policies in the central office are defined to control over which policies (using the policy ID) the management operations (Diffuse, Update, etc) are allowed. Below we can observe an example of an XACML Meta-Policy 9 used by the central office to allow an admin of a subsidiary located in Japan diffusing policies related to the virtual machine 6678 installed in the laboratory.

On the other hand, next we can see an example of an access control policy 10 diffused from the subsidiary in Japan to the central office in order to grant a user (J. Hibbert) access to the virtual machine 6678 using the proposed `XACMLDiffusePolicy` SAML schema. As can be seen in the access control policy 10, XML Encryption and XML Signature were not considered in the policy definition for these experiments.

Following experiments were conducted over the XACML engine developed in NLE (Lischka et al., 2009) which includes the management operations proposed in this paper. Even if the XACML engine used in these experiments is not public, XACML-Light (Gryb, 2012) is a public XACML implementation over which it is possible to obtain similar results, this mainly because both implementations fit all mandatory functions defined in the standard (Kuketayev, 2005).

The first experiment developed in this paper aims to compare the consumed time to execute different distributed policy management operations (named in Table 1) with regards to the number of policies or policy references over which they are applied. In this case the subsidiaries start the management operations which are addressed to access control policies related to the virtual machines kept at the central office. In these experiments we have disposed that the number of access control policies varies from 1 to 100 policies, which are considered as applicable values in this situation. An example of the structure of the diffuse policy operation that was used in these experiments can be seen in `XACMLDiffusePolicy` SAML schema 11. `XACMLDiffusePolicy` SAML schema 11 corresponds to the case when 100 policies are diffused simultaneously from the subsidiary to the central office (for sake of simplicity just the first policy has been transcribed).

An example of the structure of the policy query operation that was used in these experiments can be seen in `XACMLRemotePolicyQuery` SAML schema 12. `XACMLRemotePolicyQuery` SAML schema 12 correspond to the case when a set of 100 access control policies are queried by the subsidiary to the central office using in this situation 100 `PolicyIdReference`.

An example of the structure of the update policy operation that was used in these experiments can be seen in `XACMLUpdateRemotePolicy` SAML schema 13. `XACMLUpdateRemotePolicy` SAML schema 13 correspond to the case when a set of 100 access control policies are updated by the subsidiary to the central office (for sake of simplicity just the first policy has been transcribed).

```
<?xml version="1.0" encoding="UTF-8"?>
<PolicySet xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-
    overrides"
PolicySetId="urn:oasis:names:tc:xacml:2.0:policyset1"
xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
access_control-xacml-2.0-policy-schema-os.xsd">
 <Description />
 <Target />
 <Policy PolicyId="urn:oasis:names:tc:xacml:2.0:policy1"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
      applicable">
  <Description>Meta-Policy to allow a Subsidiary to Diffuse Policies related to Virtual
      Machine No 6788 installed in the laboratory</Description>
  <Target>
    <Subjects>
     <Subject>
       <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
             JapanSubsidiaryAdmin</AttributeValue>
         <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0
             :subject:subject-id" DataType="http://www.w3.org/2001/XMLSchema#string"/>
       </SubjectMatch>
     </Subject>
   </Subjects>
   <Resources>
     <Resource>
       <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
             urn:oasis:names:tc:xacml:2.0:VirtualMachine6788:Policy1</AttributeValue>
         <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0
             :resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#string" />
       </ResourceMatch>
     </Resource>
   </Resources>
   <Actions>
     <Action>
       <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Diffuse</
             AttributeValue>
         <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action
             -id" DataType="http://www.w3.org/2001/XMLSchema#string"/>
       </ActionMatch>
     </Action>
   </Actions>
  </Target>
  <Rule Effect="Permit" RuleId="urn:oasis:names:tc:xacml:2.0:rule1">
    <Description />
  </Rule>
  </Policy>
</PolicySet>
```

**XACML Meta-Policy 9 – Meta-Policy to manage privileges over a dual management resource (virtual machine).**

```
<?xml version="1.0" encoding="UTF-8"?> <soap:Envelope
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.
    xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.
    xsd">
 <soap:Header> <wsa:Action>http://gryb.info/schemas/xacml/wsdl/diffusePolicy</wsa:Action><
     wsa:MessageID>uuid:431ad367-35e7-4e5c-b12b-09f62e291597</wsa:MessageID><wsa:To>soap://
     wmcs/</wsa:To><wsse:Security><wsu:Timestamp wsu:Id="Timestamp-26ed4e81-7727-484f-b651-
     ac6475cd3e3d"><wsu:Created>2008-02-10T06:09:26Z</wsu:Created><wsu:Expires>2008-02-10
     T06:14:26Z</wsu:Expires></wsu:Timestamp></wsse:Security> </soap:Header>
<soap:Body>
 <samlp:XACMLDiffusePolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="
     urn:oasis:names:tc:SAML:2.0:assertion" ID="aaf23196-1788-2113-474a-fe114412ab72"
     Version="2.0" IssueInstant="2008-02-10T06:09:26">
  <saml:Issuer>https://sp.example.com/SAML2</saml:Issuer>
   <xacml:PolicyStatement xmlns:xacml ="urn:oasis:names:tc:xacml:2.0:policy:schema:os">
    <PolicySet xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os" xmlns:xsi="http://www.
        w3.org/2001/XMLSchema-instance" PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0
        :policy-combining-algorithm:deny-overrides" PolicySetId="urn:oasis:names:tc:xacml:2
        .0:policyset800" xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
        access_control-xacml-2.0-policy-schema-os.xsd">
     <Description />
     <Target />
     <Policy PolicyId="urn:oasis:names:tc:xacml:2.0:policy800" RuleCombiningAlgId="
         urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
     <Description />
     <Target>
      <Subjects>
       <Subject>
        <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">J. Hibbert</
             AttributeValue>
         <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0
             :subject:subject-id" DataType="http://www.w3.org/2001/XMLSchema#string" />
        </SubjectMatch>
       </Subject>
      </Subjects>
      <Resources>
       <Resource>
        <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
             VirtualMachine6788</AttributeValue>
         <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0
             :resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#string" />
        </ResourceMatch>
       </Resource>
      </Resources>
      <Actions />
     </Target>
     <Rule Effect="Permit" RuleId="urn:oasis:names:tc:xacml:2.0:rule800">
      <Description />
     </Rule>
     </Policy>
    </PolicySet>
   </xacml:PolicyStatement>
 </samlp:XACMLDiffusePolicy>
</soap:Body>
</soap:Envelope>
```

**Access control policy 10 – Virtual machine Policy in a `XACMLDiffusePolicy` SAML schema.**

```
<?xml version="1.0" encoding="UTF-8"?> <soap:Envelope
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.
    xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.
    xsd">
<soap:Header> <wsa:Action>http://gryb.info/schemas/xacml/wsdl/diffusePolicy</wsa:Action><
    wsa:MessageID>uuid:431ad367-35e7-4e5c-b12b-09f62e291597</wsa:MessageID><wsa:To>soap://
    wmcs/</wsa:To><wsse:Security><wsu:Timestamp wsu:Id="Timestamp-26ed4e81-7727-484f-b651-
    ac6475cd3e3d"><wsu:Created>2013-02-10T06:09:26Z</wsu:Created><wsu:Expires>2015-02-10
    T06:14:26Z</wsu:Expires></wsu:Timestamp></wsse:Security>
</soap:Header>
<soap:Body>
 <samlp:XACMLDiffusePolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="
     urn:oasis:names:tc:SAML:2.0:assertion" ID="aaf23196-1788-2113-474a-fe114412ab72"
     Version="2.0" IssueInstant="2013-02-10T06:09:26">
  <saml:Issuer>https://sp.example.com/SAML2</saml:Issuer>
   <xacml:PolicyStatement xmlns:xacml ="urn:oasis:names:tc:xacml:2.0:policy:schema:os">
    <PolicySet xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os" xmlns:xsi="http://www.
        w3.org/2001/XMLSchema-instance" PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0
        :policy-combining-algorithm:only-one-applicable" PolicySetId="
        urn:oasis:names:tc:xacml:2.0:policyset1" xsi:schemaLocation="
        urn:oasis:names:tc:xacml:2.0:policy:schema:os access_control-xacml-2.0-policy-
        schema-os.xsd">
     <Description />
     <Target />
     <Policy PolicyId="urn:oasis:names:tc:xacml:2.0:policy1" RuleCombiningAlgId="
         urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable">
     <Description />
     <Target>
      <Subjects>
       <Subject>
        <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">A. Simpsons</
             AttributeValue>
         <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0
             :subject:subject-id" DataType="http://www.w3.org/2001/XMLSchema#string" />
        </SubjectMatch>
       </Subject>
      </Subjects>
     <Actions />
     </Target>
      <Rule RuleId="urn:oasis:names:tc:xacml:2.0:conformance-test:IID026:rule1" Effect="
          Permit">
       <Description>A subject whose name is A. Simpsons may perform any action on any
           resource.</Description>
        <Target>
         <Subjects>
          <Subject>
           <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">A. Simpsons<
                /AttributeValue>
            <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0
                :subject:subject-id" DataType="http://www.w3.org/2001/XMLSchema#string"/>
           </SubjectMatch>
          </Subject>
         </Subjects>
        </Target>
      </Rule>
     </Policy>
     <Policy PolicyId="urn:oasis:names:tc:xacml:2.0:policy2" RuleCombiningAlgId="
         urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable">
        ...
     </Policy>
     ...
     ...
     <Policy PolicyId="urn:oasis:names:tc:xacml:2.0:policy100" RuleCombiningAlgId="
         urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable">
         ...
     </Policy>
    </PolicySet>
   </xacml:PolicyStatement>
 </samlp:XACMLDiffusePolicy>
</soap:Body> </soap:Envelope>
```

**Diffuse Policy Operation 11 – Diffuse policy operation in a `XACMLDiffusePolicy` SAML schema.**

```
<?xml version="1.0" encoding="UTF-8"?> <soap:Envelope
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.
    xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.
    xsd">
<soap:Header>
<wsa:Action>http://gryb.info/schemas/xacml/wsdl/PolicyQuery</wsa:Action><wsa:MessageID>
    uuid:431ad367-35e7-4e5c-b12b-09f62e291597</wsa:MessageID><wsa:To>soap://wmcs/</wsa:To><
    wsse:Security><wsu:Timestamp
wsu:Id="Timestamp-26ed4e81-7727-484f-b651-ac6475cd3e3d"><wsu:Created>2013-02-10T06:09:26Z</
    wsu:Created><wsu:Expires>2015-02-10T06:14:26Z</wsu:Expires></wsu:Timestamp></
    wsse:Security>
</soap:Header> <soap:Body>
 <samlp:XACMLRemotePolicyQuery xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="aaf23196-1788-2113-474a-
     fe114412ab72" Version="2.0" IssueInstant="2013-02-10T06:09:26">
  <saml:Issuer>https://sp.example.com/SAML2</saml:Issuer>
   <xacml:PolicyIdReference>
    urn:oasis:names:tc:xacml:2.0:policy1
   </xacml:PolicyIdReference>
   <xacml:PolicyIdReference>
    urn:oasis:names:tc:xacml:2.0:policy2
   </xacml:PolicyIdReference>
    ...
    ...
   <xacml:PolicyIdReference>
    urn:oasis:names:tc:xacml:2.0:policy100
   </xacml:PolicyIdReference>
 </samlp:XACMLRemotePolicyQuery>
</soap:Body> </soap:Envelope>
```

**Policy query Operation 12 – Policy query operation in a `XACMLRemotePolicyQuery` SAML schema.**

```
<?xml version="1.0" encoding="UTF-8"?> <soap:Envelope
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
<soap:Header>
<wsa:Action>http://gryb.info/schemas/xacml/wsdl/diffusePolicy</wsa:Action><wsa:MessageID>uuid:431ad367-35e7-4e5c-b12b-09f62e291597</wsa:MessageID><wsa:To>soap://wmcs/</wsa:To><wsse:Security><wsu:Timestamp
wsu:Id="Timestamp-26ed4e81-7727-484f-b651-ac6475cd3e3d"><wsu:Created>2013-02-10T06:09:26Z</wsu:Created><wsu:Expires>2015-02-10T06:14:26Z</wsu:Expires></wsu:Timestamp></wsse:Security>
</soap:Header> <soap:Body>
 <samlp:XACMLUpdateRemotePolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="aaf23196-1788-2113-474a-fe114412ab72" Version="2.0" IssueInstant="2013-02-10T06:09:26">
  <saml:Issuer>https://sp.example.com/SAML2</saml:Issuer>
   <xacml:PolicyStatement xmlns:xacml ="urn:oasis:names:tc:xacml:2.0:policy:schema:os">
    <PolicySet xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:only-one-applicable" PolicySetId="
        urn:oasis:names:tc:xacml:2.0:policyset1" xsi:schemaLocation="
        urn:oasis:names:tc:xacml:2.0:policy:schema:os access_control-xacml-2.0-policy-schema-os.xsd">
     <Description />
     <Target />
     <Policy PolicyId="urn:oasis:names:tc:xacml:2.0:policy1" RuleCombiningAlgId="
         urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable">
     <Description />
     <Target>
      <Subjects>
       <Subject>
        <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">B. Roosevelt</AttributeValue>
         <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" DataType="http://www.w3.org/2001/XMLSchema#string" />
        </SubjectMatch>
       </Subject>
      </Subjects>
     <Actions />
     </Target>
      <Rule RuleId="urn:oasis:names:tc:xacml:2.0:conformance-test:IID026:rule1" Effect="Permit">
       <Description>A subject whose name is B. Roosevelt may perform any action on any resource.</Description>
        <Target>
         <Subjects>
          <Subject>
           <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">B. Roosevelt</AttributeValue>
            <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" DataType="http://www.w3.org/2001/XMLSchema#string"/>
           </SubjectMatch>
          </Subject>
         </Subjects>
        </Target>
       </Rule>
      </Policy>
      <Policy PolicyId="urn:oasis:names:tc:xacml:2.0:policy2" RuleCombiningAlgId="
          urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable">
         ...
      </Policy>
      ...
      ...
      <Policy PolicyId="urn:oasis:names:tc:xacml:2.0:policy100" RuleCombiningAlgId="
          urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable">
         ...
      </Policy>
     </PolicySet>
    </xacml:PolicyStatement>
  </samlp:XACMLUpdateRemotePolicy>
</soap:Body> </soap:Envelope>
```

**Update Policy Operation 13 – Update policy operation in a `XACMLUpdateRemotePolicy` SAML schema.**

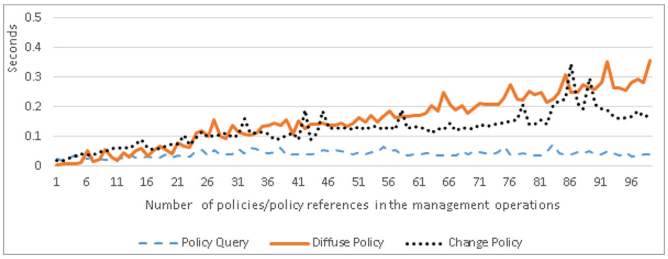


**Fig. 4 – Measured time for different distributed policies management operations.**

The measured times for the different distributed policies management operations varying the number of <Policy/> or <PolicyIdReference/> from 1 to 100 are shown in Fig. 4.

The consumed time for a management operation increases with the number of policies or policy references over which it is operated. In the case of a diffuse policy operation, this is because the SAML message transmitted from the subsidiary to the central office carries all the access control policies that are being diffused, and additionally those policies must be processed one by one in the central office to validate its correctness and proceed to store them. For the change policy operation, the SAML message contains new versions of access control policies which will replace directly existent policy with the corresponding policy ID in the central office. In all cases, the measured time is under 400 ms.

Additionally, different measurements have been done to compare the quantity of transmitted data (bytes) produced by a single distributed policies management operation that is requested from the subsidiary and executed in the central office. These values for different operations are compared with the quantity of transmitted data (bytes) produced by a remote authorization request according to the solution proposed in Lischka et al. (2009) and named "deductive policies strategy". In the context of these experiments, a "deductive policies strategy" implies that the central office sends a request to a subsidiary to resolve each authorization request.

The results of these measures are shown in Fig. 5. In both cases, the measured transmitted data corresponds to administrative traffic (overhead) that goes into the network, potentially generating possible congestion in the network. A first analysis of Fig. 5 indicates that the data transmitted by a single distributed policies management operation is, in general, bigger than the data transmitted by a remote authorization request in the "deductive policies strategy". This because the distributed policy management operations (Policy query, Diffuse policy, Change Policy) contain a significant block of data corresponding to the access control policy being transmitted from or to the central office (as can be seen in access control policy 10). In the case of a delete policy operation, an access control policy is not transmitted, but the reference to a policy ID that will be deleted, turning this operation like the less data consuming. Finally, in a remote authorization request for the "deductive policies strategy" a message with the authorization request which contain the target and the features of the request is transmitted toward the subsidiaries and these ones reply with an authorization decision (Deny, Permit).

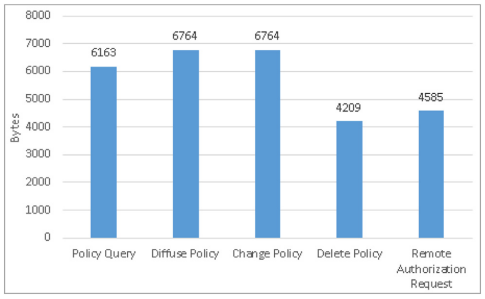


**Fig. 5 – Comparison of transmitted data for single distributed policy management operations (bytes).**

The results in Fig. 5 are related with a policy management operation and a remote authorization request which occur one time, but in a real environment these transactions can occur many times along the time, therefore the total value of transmitted data with these operations will depend on the frequency of the distributed policies management operations and the remote authorization requests in a time span. These values have been calculated seizing the payloads that are transmitted when a policy management operation is developed. In the case of a policy query operation all the transmitted data corresponds to a `XACMLRemotePolicyQuery` SAML schema which contains a `PolicyIdReference` and an SAML response which contains a `PolicyStatement`. In the case of diffuse and update policy operations all the transmitted data corresponds to a `XACMLDiffusePolicy` and `XACMLUpdateRemotePolicy` SAML schema, respectively, which contain in both cases a `PolicyStatement`. The response for these both cases (diffuse and update) corresponds to an SAML response which contains a `StatusMessage` element. In the case of a delete operation all the transmitted data corresponds to a `XACMLDeleteRemotePolicy` SAML schema which contains a `PolicyIdReference` and an SAML response which contains a `StatusMessage` element. Finally, for a remote authorization request in the context of a deductive policies strategy all the transmitted data corresponds to a `XACMLAuthorizationDecisionQuery` SAML schema which is responded with a `XACMLAuthorizationDecisionStatement` SAML schema containing an authorization response.

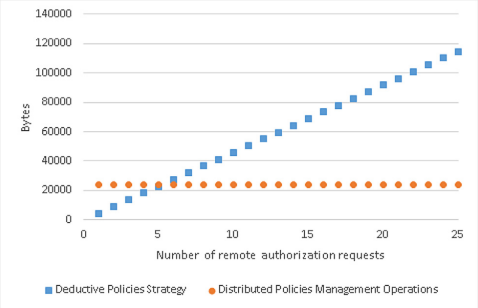


**Fig. 6 – Comparison of transmitted data to resolve multiple remote authorization request.**

Fig. 6 aims to compare the quantity of data (bytes) that is transmitted using the "deductive policies strategy" (Lischka et al., 2009) when multiple remote authorization requests addressed to a subsidiary have to be resolved in order to find an authorization decision in the central office. Values presented in Fig. 6 are calculated considering the traffic values found for each distributed policy management operation in Fig. 5. As the number of remote authorization requests using the "deductive policies strategy" increases, the transmitted data will also increase proportionally, as shown in Fig. 6. This value is compared with the quantity of data that is transmitted as a result of a set of distributed policies management operations (proposed in this paper) which are started in a subsidiary and executed in the central office. Thus, counting the overall amount of data that would be transmitted by the following management operations over a single policy: diffuse policy, delete policy, update policy and policy query, which are represented in Fig. 5 being equivalent to 23,900 bytes and it is shown in Fig. 6.

As shown in Fig. 6 as well, the transmitted data to resolve a single remote authorization request using a deductive policy strategy is 4585 bytes and this value tends to increase in realtime systems where hundreds or thousands of remote authorization requests must be resolved. On the other hand, the data (bytes) transmitted as result of a set of distributed policies management operations depends on the number of management operations generated by the administrator of the distributed access control system and is not dependent on the number of authorization requests. Finally, in a real access control systems the number of authorization requests would surpass probably the number of management operations in some factor, doing the proposed architecture in this paper more appropriate because of the less produced overhead.

## 7. Security threats analysis

So as to guarantee that a distributed policy management system works properly, it is also necessary to conduct a threat analysis which validates the strengths of our proposal against possible attacks. Considering the architecture for distributed access control policies management proposed in Section 4 and the extension related to an SAML-based transport mechanism described in Section 5, we have identified two possible attacks: i) attempt to tamper messages involved in a policy management operation during the communication processes, and ii) attempt to execute any ill-intentioned action to affect confidential information assets (i.e. policies and attributes) in one domain.

With the aim of reviewing these aspects, we have done an analysis related to security and robustness in the communications between components of the system (Subsection 7.1). Additionally we have added an analysis about the protection of disclosure of attributes and policies between domains in Subsection 7.2.

### 7.1. *Security in communications*

The threats in communications in a distributed policy management system are related to actions that affect the confidentiality and integrity of the exchanged messages between XACML domains, specifically between PAPs. Between the most common threats that we could find in this context are: eavesdropping, data modification, identity spoofing, password-based attacks, Denial-of-Service and Man-in-the-Middle (Goyal et al., 2010).

An eventual eavesdropping or sniffer attack could cause a disclosure of content of the messages, for example the kind of management operations being executed and their corresponding answers. On the other hand identity spoofing, password-based attacks and Man-in the-Middle would permit cheating the system regarding the identity of one of the peers in the communication. It clearly opens the possibility of inducing wrong operations which could affect the confidentiality and integrity of the data (i.e. policies).

As stated in Section 5, we propose the use of request-response SAML messages to secure the communication processes related to distributed policy management between different XACML domains since it includes mechanisms for the identification and validation of assertions, namely, XML Encryption (Imamura et al., 2002; Lakshminarayanan, 2008) and XML Signature (Bartel et al., 2008; Rosen et al., 2012).

With XML Encryption it is possible to hide an `<Assertion>` element (used to transport policies), an `<Issuer>` (used to define the issuer of an assertion or protocol message) or an `<Attribute>` (used to transport XACML policy attributes) using any of the algorithms defined in the XML Encryption standard. For these three cases, the encrypted data must be located in the same position that the plain text information, inside the SAML message structure; and it is optional to include wrapped decryption keys besides the recipient to whom the key is addressed.

On the other hand, XML Signature is applicable to guarantee the identification of the peers involved in the exchange of request/response messages and assertions. The SAML specification defines the element `<ds:Signature>`, that is used in the `RequestAbstractType` and `StatusResponseType` complex types, which are the base to compose the queries and responses defined in the Sections 5.1 and 5.2, respectively. According to the SAML specification, the SAML requester and responder (Master and Slave PAP in our scenario) must verify that the signature received is valid according to the XML Signature specification (i.e. that the message has not been modified). A valid signature allows to

**Table 2 – Communication threats in a distributed policy management system.**

| | | Technologies | | |
|---|---|---|---|---|
| | | XML encryption over SAML | XML signature over SAML | SSL/TLS |
| Threats | Data modification | | X | X |
| | Eavesdropping | Partially | | X |
| | Identity spoofing | | X | X |
| | Man-in-the-Middle | Partially | | X |
| | Denial-of-Service | | Partially | Partially |
| | Forged Claims | | X | X |
| | Replay of Message parts | | X | X |

determine the identity of the issuer and process the request. In this way, XML Signature provides integrity of the message and identification of the communications peers.

Optionally, as SAML messages are transported using SOAP messages, it is possible to apply SSL/TTL mechanisms to protect SOAP and at the same time guarantee confidentiality for the SAML messages. In Cantor et al. (2005a, 2005b) it is also stated that SAML is able to work together with SSL 3.0 (Dong and Chen, 2012) or TLS 1.0 (Krief, 2013), in that case, each peer of the communication must use X.509 v3 certificates (Ganguly and Lahiri, 2012) to determine the identity of the SAML relying peer.

In Table 2 we can observe a comparison of the applicability of XML Encryption and XML Signature over SAML messages, in addition to SSL/TTL solutions to tackle threats in the communication between PAPs. XML Encryption can "partially" resolve the problems of eavesdropping and Man-in-the-Middle since it considers the encryption of some elements (`<Assertion>`, `<Issuer>` and `<Attribute>`) of the request/response messages, but unfortunately it does not protect the reminder of the elements. Meanwhile, XML Signature effectively prevents the data modification, identity spoofing, forged claims and replay of message parts. XML signature has the ability to identify the peers in a communication, and this can be considered as a partial protection measure to face a denial of service by filtering all peers not recognized like valid. On the other hand, due to the ability to identify and encrypt the communication between peers, SSL/TLS is clearly applicable to resolve all the threats identified in Table 2 (excepting Denial of Service, for which SSL/TLS represents a partial protection measure for its peer identification function). Therefore, depending on the required security level for a distributed policy management system, it is possible to consider the application of a mix of XML Encryption/XML Signature technologies or an SSL/TLS cryptographic system with certificates in each endpoint of the communication.

### 7.2. *Privacy and confidentiality of policies*

The confidentiality and autonomy between domains must be ensured in such a way that it is only possible to access and execute authorized actions over allowed data. In the context of a distributed policy management system, the data to protect consist of all the policies and attributes that represent the behavior of a security domain and give details about its operation. The solution must provide mechanisms in order to guarantee that only the authorized subjects are able to obtain and administrate such policies and attributes.

As we have previously proposed in Section 4, the Meta-Policies are the element in charge of controlling all the privileges over policies and therefore over them lays the responsibility of any authorization decision related to policy management. Thus, it is fundamental to properly build Meta-Policies that represent clearly the requirements of confidentiality and autonomy of a security domain.

The applicability of a Meta-Policy is determined by the matching of its target, which is composed of statements about subject, action, resource and environment. Through matching processes and attribute evaluation functions of the subject (i.e. a Master PAP), the action (i.e. a management operation), the resource (i.e. a Policy/PolicySet) and the environment (i.e. attributes from the context) it is possible to define detailed conditions of use of a Meta-Policy. As an XACML Policy/PolicySet is written in XML, it can be included seamlessly in a decision request and hence, it is also possible to use the content of the Policy/PolicySet as part of the attribute evaluation needed to take an authorization decision. For attribute evaluation, XACML provides a big set of equality, arithmetic, string conversion, numeric conversion, logical, numeric comparison, bag, date and time functions which are extremely useful to define in a fine-grained fashion the conditions in which a policy effect is enforced. For example, it is possible to state in a Meta-Policy belonging to a Slave PAP, that a specific Master PAP can only "read" policies (i.e. a Policy Query operation) related to a specific kind of resources.

Additionally, it is possible to use the profile for role-based access control (RBAC) (Anderson, 2004; Ferraiolo et al., 2003) to create Meta-Policies. With this profile it is possible to define Discretional Access Control (DAC) (Das et al., 2012), which allows to control the actions that an administrator can do over the resources he/she has been authorized to manage; in our case the allowed actions that an administrator can make over a policy.

With RBAC, it is also possible to state Mandatory Access Control (MAC) (Hu et al., 2006), through which a central authority enforces protection decisions over subjects (i.e. administrators) who are authorized to control an object (Policy/PolicySet). The MAC restrictions overlay the decision originated by an administrator and so it is possible to define generic Meta-Policies which avoid security flaws provoked by the administrators when they control policies or to restrict the control over specific policies or its attributes. An example could be a Meta-Policy that specifies that any management operation can be done (independent of the requester) only during a specific range of time. Finally with the RBAC profile it is also possible to implement Separation of Duty (SoD) (Hu

et al., 2006) and role assignment functionalities to restrict the tasks which can be executed by a policy administrator.

Therefore, the expressiveness of XACML and its profiles are key to define Meta-Policies that restrict privileges properly and guarantee the privacy and confidentiality of policies and attributes in an XACML domain.

## 8. Conclusions and future work

In the paper at hand we have developed an architectural model to manage policies within a distributed context in a simple and integrated way, which can be extended or adapted to support new management functions. Seamlessly reusing the XACML architecture with the aim of managing privileges over distributed policies (i.e. through Meta-Policies) saves time and effort in implementation and deployment of a new access control architecture for this purpose. Furthermore, through the expressiveness of XACML and its profiles (applied in Meta-Policies) it is possible to define privileges properly and guarantee the privacy and confidentiality of policies and attributes in each security domain.

The conducted experiments show the advantages of using a distributed policy management with regards to a deductive policies strategy. The advantages are specially notable for situations where the number of authorization requests is bigger that the number of management operations.

The management of distributed policies (and its attributes and parts) also allows the development of new operations over policies, like the dynamic creation (by composition/decomposition) of new policies in a Master PAP or in a Slave PAP. We are researching at present over these new operations and expect to integrate them to the existent policy management framework.

Finally, SAML complements XACML within the context of a distributed policies system, providing protocols and transport mechanisms (assertions validity, digital signature, identity issuer, etc), to guarantee a secure communication scheme. Moreover, with a set of well known technologies (XACML/SAML/SOAP/HTTPS) it is possible to achieve a distributed XACML policies management over multiple security domains.

As future work we are researching over the integration of the defined operations into existent policy management frameworks. Part of our research plans includes an analysis of conflicts related to contradictory policies caused by inconsistencies between policies enforced by an external entity and policies enforced by a local administrator. This analysis of conflicts will consider different alternatives to integrate policies considering the applicability of such integration in a distributed environment.

## REFERENCES


Anderson A, Lockhart H. SAML 2.0 profile of XACML v2.0. OASIS Standard; February 2005. http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-saml-profile-spec-os.pdf.

Anderson A. XACML profile for role based access control (RBAC), OASIS Access Control TC committee draft 1. 2004. p. 1–13.

Ardagna CA, di Vimercati SDC, Pedrini E, Paraboschi S, Samarati P, Verdicchio M. Extending XACML for open web-based scenarios, W3C workshop on access control application scenarios, Luxembourg. 2009.

Bartel M, Boyer J, Fox B, LaMacchia B, Simon E. XML-signature syntax and processing. W3C recommendation. 2nd ed. June 2008. http://www.w3.org/TR/xmldsig-core/.

Blasch E, Bossé É, Lambert D. High-level information fusion: management and systems design, Artech House intelligence and information operations series, ARTECH HOUSE Incorporated. 2012.

Cantor S, Kemp J, Philpott R, Maler E. Assertions and protocols for the OASIS security assertion markup language (SAML) V2.0. OASIS Standard; March 2005a.

Cantor S, Hirsch F, Kemp J, Philpott R, Maler E, Cahill C, et al. Bindings for the OASIS security assertion markup language (SAML) V2. 0. OASIS Standard; March 2005b.

Das S, Kant K, Zhang N. Handbook on securing cyber-physical critical infrastructure. Morgan Kaufmann; 2012.

DeCouteau D, Davis M, Staggs D. Cross-enterprise security and privacy authorization (XSPA) profile of security assertion markup language (SAML) for healthcare, OASIS Committee Draft. November 2008. https://www.oasis-open.org/committees/download.php/29921/xspa-saml-profile-cd-01.doc.

Demchenko Y, Koeroo O, de Laat C, Sagehaug H. Extending XACML authorisation model to support policy obligations handling in distributed application. In: Proceedings of the 6th international workshop on middleware for grid computing, no. 5 in MGC '08. New York, NY, USA: ACM; 2008. http://dx.doi.org/10.1145/1462704.1462709.

Dong L, Chen K. Cryptographic protocol: security analysis based on trusted freshness. Springer; 2012.

Ferraiolo D, Kuhn D, Chandramouli R. Role-based access controls, Artech House computer security series. Artech House; 2003.

Foster I. What is the grid? A three point checklist. J Grid Today 2002;1(6):4.

Ganguly D, Lahiri S. Network and application security: fundamentals and practices. Science Publishers – CRC Press; 2012.

Garzoglio G, Ananthakrishnan R, Koeroo O. An XACML attribute and obligation profile for authorization interoperability in grids, CS document 2952–v3. Grids Fermilab; August 2011.

Garzoglio G, Alderman I, Altunay M, Ananthakrishnan R, Bester J, Chadwick K, et al. Definition and implementation of a SAML-XACML profile for authorization interoperability across grid middleware in OSG and EGEE. J Grid Comput 2009;7(3):297–307.

Goyal P, Batra S, Singh A. A literature review of security attack in mobile ad-hoc networks. Int J Comput Appl 2010;9(12):24–8.

Gryb O. XACMLight reference. Official Project Web Site. July 2012., http://xacmllight.sourceforge.net/.

Hosmer HH. Metapolicies I. SIGSAC Rev 1992;10(2–3):18–43. http://dx.doi.org/10.1145/147092.147097. http://doi.acm.org/10.1145/147092.147097.

Hu V, Ferraiolo D, Kuhn D. Assessment of access control systems, NIST interagency report 7316. National Institute of Standards and Technology; September 2006.

Hughes J, Maler E. Security assertion markup language SAML v2.0 technical overview, OASIS Working Draft. October 2006.

Huonder F. Conflict detection and resolution of XACML policies (Master's thesis). University of Applied Sciences Rapperswil; July 2010.

Imamura T, Dillaway B, Simon E, Eastlake D, Reagle J. XML encryption syntax and processing, W3C recommendation. December 2002. http://www.w3.org/TR/xmlenc-core/.

Khnhauser WE. On paradigms for security policies in multipolicy environments. In: Proceedings of the 11th international

information security conference (IFIP/SEC '95). Cape Town, South Africa: Chapman and Hall; 1995.
Krief F. Communicating embedded systems: networks applications. ISTE – Wiley; 2013.
Kuketayev A. XACML version 2.0 conformance tests, version 0.5, Non-normative tests – OASIS Consortium. October 2005. https://www.oasis-open.org/committees/download.php/14877/ConformanceTests.html.
Lakshminarayanan S. Oracle web services manager, from technologies to solutions. Packt Publishing, Limited; 2008.
Lischka M, Endo Y, Sánchez Cuenca M. Deductive policies with XACML. In: Proceedings of the 2009 ACM workshop on secure web services. Chicago, Illinois, USA: ACM; 2009. p. 37–44.
Lorch M, Kafura D, Shah S. An XACML-based policy management and authorization service for globus resources. In: Proceedings of the 4th international workshop on grid computing. Phoenix, AZ, USA: IEEE Computer Society; 2003. p. 208–13.
Lupu E, Sloman M. Conflict analysis for management policies. In: Integrated Network Management V, IFIP The International Federation for Information Processing. Springer US; 1997. p. 430–43.
Martin E, Xie T, Yu T. Defining and measuring policy coverage in testing access control policies. In: Proc. 8th international conference on information and communications security – ICICS, vol. 4307. Springer; 2006. p. 139–58.
Moses T, Anderson A, Nadalin A, Parducci B, Engovatov D, Flinn D, et al. eXtensible Access Control Markup Language (XACML) version 2.0, OASIS Standard. February 2005. http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf.
Parducci B, Lockhart H. XACML v3.0 administration and delegation profile version 1.0, OASIS Committee Specification. August 2010. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-administration-v1-spec-cs-01-en.pdf.
Peters J, Rieke R, Rochaeli T, Steinemann B, Wolf R. A holistic approach to security policies policy distribution with XACML over COPS. Electron Notes Theor Comput Sci 2007;168(0):143–57. http://dx.doi.org/10.1016/j.entcs.2006.08.025. proceedings of the Second International Workshop on Views on Designing Complex Architectures (VODCA 2006), https://www.sciencedirect.com/science/article/pii/S1571066107000333.
Rao P, Lin D, Bertino E, Li N, Lobo J. An algebra for fine-grained integration of xacml policies. In: Proceedings of the 14th ACM symposium on access control models and technologies, SACMAT '09. New York, NY, USA: ACM; 2009. p. 63–72. http://dx.doi.org/10.1145/1542207.1542218. http://doi.acm.org/10.1145/1542207.1542218.
Rosen M, Lublinsky B, Smith K, Balcer M. Applied SOA: service-oriented architecture and design strategies. Wiley; 2012.
St-Martin M. A verified algorithm for detecting conflicts in XACML access control rules (Master's thesis). University of Ottawa; 2012.
Official Project Web Site Sun's XACML implementation. Sun Microsystems, Inc; June 2006., http://sunxacml.sourceforge.net/.
Vacca J. Computer and information security handbook, no. 2. Elsevier Science; 2012.
Wei Q, Crampton J, Beznosov K, Ripeanu M. Authorization recycling in hierarchical RBAC systems. ACM Trans Inf Syst Secur TISSEC 2011;14(1).
Wurster G, Van Oorschot P. A control point for reducing root abuse of file-system privileges. In: Proceedings of the 17th ACM conference on computer and communications security. Chicago, Illinois, USA: ACM; 2010. p. 224–36.
XACML references and products, version 1.85, OASIS consortium, list. June 2011. https://www.oasis-open.org/committees/download.php/42588/xacmlRefs-V1-85.html.
Yang S. Internet-based control systems: design and applications, advances in industrial control. Springer; 2011.

**Daniel Díaz López** is a PhD student in computer engineering from the University of Murcia. His research interests include systems for management and federation of identity, security in cloud computing, privacy and anonymity. At the time of writing this paper he was a student research assistant in the security group at NEC Laboratories Europe, Heidelberg, Germany. He received an MSc in computer engineering from the University of Murcia. Contact him at danielorlando.diaz@um.es

**Ginés Dólera Tormo** is a researcher in the Department of Information and Communications Engineering of the University of Murcia. His research interests include authorization, authentication and identity management, user-centric technologies and trust management. He received an MSc and PhD in computer engineering from the University of Murcia, Spain. Contact him at ginesdt@um.es

**Felix Gómez Mármol** is a senior research scientist in the security group at NEC Laboratories Europe, Heidelberg, Germany. His research interests include authorization, authentication and trust management in distributed and heterogeneous systems, security management in mobile devices and design and implementation of security solutions for mobile and heterogeneous environments. He received an MSc and PhD in computer engineering from the University of Murcia. Contact him at felix.gomez-marmol@neclab.eu

**Gregorio Martínez Pérez** is an associate professor in the Department of Information and Communications Engineering of the University of Murcia. His research interests include security, privacy and management of IP-based communication networks. He received an MSc and PhD in computer engineering from the University of Murcia. Contact him at gregorio@um.es

# 2

# Dynamic counter-measures for risk-based access control systems: An evolutive approach

| | |
|---|---|
| **Title**: | Dynamic counter-measures for risk-based access control systems: An evolutive approach |
| **Authors**: | Daniel Díaz-López, Ginés Dólera-Tormo, Félix Gómez-Mármol, Gregorio Martínez-Pérez |
| **Type**: | Journal |
| **Journal**: | Future Generation Computer Systems |
| **Impact factor (2014)**: | 2.786 |
| **Publisher**: | Elsevier |
| **Volume**: | - |
| **Number**: | - |
| **Pages**: | - |
| **Year**: | 2014 |
| **Month**: | November |
| **DOI**: | http://dx.doi.org/10.1016/j.future.2014.10.012 |
| **State**: | In Press |

Table 2: Dynamic counter-measures for risk-based access control systems: An evolutive approach

ARTICLE IN PRESS

Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮–▮▮

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

# Dynamic counter-measures for risk-based access control systems: An evolutive approach

Daniel Díaz-López [a,*], Ginés Dólera-Tormo [a], Félix Gómez-Mármol [b], Gregorio Martínez-Pérez [a]

[a] Departamento de Ingeniería de la Información y las Comunicaciones, Universidad de Murcia, 30.100, Murcia, Spain
[b] NEC Laboratories Europe, Kurfürsten Anlage 36, 69115, Heidelberg, Germany

## HIGHLIGHTS

- Finding of best sets of counter-measures to protect resources.
- Dynamic countermeasures to face variations in the Risk Level (*RL*).
- Access depending on the fulfillment of a set of specific security controls.
- Method based on genetic algorithms with applicability in a real scenario.
- Resource protection according to the risk level (not under or overestimated).

## ARTICLE INFO

*Article history:*
Received 20 November 2013
Received in revised form
29 August 2014
Accepted 9 October 2014
Available online xxxx

*Keywords:*
ISO 27001
ISMS
Risk management
Access control systems
Genetic algorithms
Counter-measures

## ABSTRACT

Risk-based access control systems are a new element in access control categories, incorporating risk analysis as part of the inputs to consider when taking an authorization decision. A risk analysis over a resource leads generally to temporal allocation of the resource in a risk level (e.g. high, medium, low). Ideally, for each risk level and kind of resource, the access control system should take an authorization decision (expressed like a permit or deny) and the system administrator should also trigger specific counter-measures to protect resources according to their risk level. In a small access control system with few resources it is possible for an administrator to follow the risk level changes and react promptly with counter-measures; but in medium/large access control systems it is almost unfeasible to react in a customized way to thousands of risk level emergencies asking for attention. In this paper we propose the adoption of dynamic counter-measures (which can be integrated within access control policies) changing along time to face variations in the risk level of every resource, bringing two main benefits, namely: (i) a suitable resource protection according to the risk level (not under or over estimated) and (ii) an access control system granting/denying access depending on the fulfillment of a set of security controls applicable in an authorization access request. To define the most appropriate set of counter-measures applicable for a specific situation we define a method based on genetic algorithms, which allows to find a solution in a reasonable time frame satisfying different required conditions. Finally, the conducted experiments show the applicability of our proposal in a real scenario.



## 1. Introduction

Access control systems are used in a wide variety of scenarios to manage privileges over resources, being the following the most conventional access control models: ACL (Access Control List) [1,2], RBAC (Role-Based Access Control) [3,4], ABAC (Attribute-Based Access Control) [5,6] and PBAC (Policy-Based Access Control) [7,8]. Risk-based access control systems [9,10] are the last evolution in access control systems as they incorporate a risk level analysis as main input for the authorization decision process. In typical risk-based access control systems, the risk level calculation is usually focused on the protection of assets, being an asset anything that has a value for the organization, i.e. information, equipment, software, services, etc.

* Corresponding author. Tel.: +34 868 887 646.
*E-mail addresses:* danielorlando.diaz@um.es (D. Díaz-López), ginesdt@um.es (G. Dólera-Tormo), felix.gomez-marmol@neclab.eu (F. Gómez-Mármol), gregorio@um.es (G. Martínez-Pérez).

http://dx.doi.org/10.1016/j.future.2014.10.012
0167-739X/

Please cite this article in press as: D. Díaz-López, et al., Dynamic counter-measures for risk-based access control systems: An evolutive approach, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.10.012

Asset protection is achieved through counter-measures, security controls or safeguards that are deployed by an organization in order to avoid that intentional or no-intentional actions affect its information assets. In this paper, a counter-measure *cm* will consist of a specific security control category *scc*, plus an associated effectiveness of such security control category $E(scc)$, as we will see later.

The risk level value, which can be estimated for an asset or a group of assets, must be under a well defined maximum threshold (acceptable risk) which is defined by the organization and represents the maximum risk level that such organization is willing to accept [11] (either for each particular asset, or overall for the whole organization).

The risk level can be measured using different risk analysis methodologies, which are a core element in Information Security Management Systems (ISMS), like the ones defined by ISO 27001 and ISO 17799 [12,13]. As shown in Eq. (1), the risk analysis methodologies commonly include the following elements to compute the risk level of a particular asset $\mathcal{A}$, given a specific threat $\mathcal{T}$, $RL(\mathcal{A}, \mathcal{T})$: (i) a factor related to the relevance of the asset $\mathcal{A}$ for the organization (impact $I(\mathcal{A})$), (ii) a factor associated to the probability that a specific threat $\mathcal{T}$ can be truly materialized over the asset $\mathcal{A}$ (probability of occurrence $P(\mathcal{T}, \mathcal{A})$) and (iii) a factor regarding the effectiveness of the security controls implemented in the organization to protect such asset $\mathcal{A}$, $E(\mathcal{A})$.

$$RL(\mathcal{A}, \mathcal{T}) = \frac{P(\mathcal{T}, \mathcal{A}) \cdot I(\mathcal{A})}{E(\mathcal{A})}. \quad (1)$$

As we can observe, whenever the probability of occurrence of a given threat $\mathcal{T}$ over a specific asset $\mathcal{A}$, $P(\mathcal{T}, \mathcal{A})$, and the impact of such asset $\mathcal{A}$, $I(\mathcal{A})$, are not negligible, there will always exist an associated risk level $RL(\mathcal{A}, \mathcal{T})$ (from now on, for simplicity, also noted just as *RL*), even if this is quite small due to a high security control effectiveness $E(\mathcal{A})$. According to the standard ISO/IEC 27001 [14], in the risk level evaluation and treatment process every organization evaluates the risk level of its assets and implements security controls to reduce that risk level (by decreasing the probability of occurrence of a threat $\mathcal{T}$, $P(\mathcal{T}, \mathcal{A})$, and/or increasing the effectiveness of the security controls over each of its assets $\mathcal{A}$, $E(\mathcal{A})$). However, after the corresponding risk level treatment, there is always a residual risk level which is remaining.

Additionally, according to the widely applied standard ISO/IEC 27005 [11], every organization should define the risk acceptance criteria, which determines how much an organization is willing to accept risks. A level of risk acceptance ($\widehat{RL}(\mathcal{A}, \mathcal{T})$ or, for simplicity, just $\widehat{RL}$) can be defined for all the assets or for specific groups of assets, and considers organization policies, objectives and interests of the different stakeholders. The levels of risk acceptance are determined and approved by the managers of the organization and require regular revision. As the context changes, the risks do and therefore it is necessary to adjust the levels of risk acceptance. In a continual improvement cycle for an Information Security Management Systems (ISMS), it is normal to observe a gradual decrement in the levels of risk acceptance (acceptable risk values).

### 1.1. Motivation and contribution

The model previously introduced for risk-based access control systems is in some way static, since it does not take into account the fact that the impact of an asset $\mathcal{A}$, $I(\mathcal{A})$, the probability of occurrence of a particular threat $\mathcal{T}$ over such given asset $\mathcal{A}$, $P(\mathcal{T}, \mathcal{A})$, and the security control effectiveness for that specific asset $\mathcal{A}$, $E(\mathcal{A})$, can change dynamically in short periods of time so that the risk level $RL(\mathcal{A}, \mathcal{T})$ can become remarkably variable. Besides, these systems use a set of static access control policies to process authorization requests over the assets $\mathcal{A}$ of an organization; but due to the dynamism of the aforementioned variables, it is reasonable to think that a static access control policy does not apply to every situation, since the response of the system (authorization decision) has to change and adapt to the current risk level of asset $\mathcal{A}$, $RL(\mathcal{A}, \mathcal{T})$, when a user is trying to access or manipulate it.

Current risk-based access control systems will use the risk level computed for each asset $\mathcal{A}$ within an organization, $RL(\mathcal{A}, \mathcal{T})$, to make their authorization decisions and, in the case of a high risk level, every authorization request toward such asset $\mathcal{A}$ has a high probability of being denied. Unless the risk level $RL(\mathcal{A}, \mathcal{T})$ decreases (actually, the probability of occurrence $P(\mathcal{T}, \mathcal{A})$ or impact $I(\mathcal{A})$), the authorization decision will not change, since the security controls are static and so their effectiveness $E(\mathcal{A})$ is not adapting to the changing conditions.

Denying access is a way of protecting assets in a risky situation, but it is rather not the most effective one for its blocking consequences on the service delivery. On the other hand, defining static security controls with an excessively high effectiveness $E(\mathcal{A})$ in order to keep the risk level low, becomes self-defeating since this can produce an overestimated protection for an asset $\mathcal{A}$ which does not really need it, or at least, not all the time. Furthermore, when a risk level variation occurs, the system administrator should trigger specific counter-measures to protect every asset $\mathcal{A}$ according to the current risk level $RL(\mathcal{A}, \mathcal{T})$. Yet, if the risk level rapidly varies in short periods of time for many assets (e.g. in medium large infrastructures) it is a cumbersome task for a system administrator to manually handle each risk level variation in a proper and timely fashion.

Thus, the main contribution of this paper lies in the definition, implementation and evaluation of a method inspired on evolutive algorithms to assist risk-based access control systems by dynamically finding a catalog of the best set of counter-measures describing how to adapt the access control policies related to a specific asset $\mathcal{A}$, in order to effectively and efficiently protect such asset according to its current risk level $RL(\mathcal{A}, \mathcal{T})$.

In particular, these optimal counter-measures are devoted to adapt the effectiveness $E(\mathcal{A})$ of the applied security controls and, in turn, the measured risk level for such specific asset $\mathcal{A}$, $RL(\mathcal{A}, \mathcal{T})$, to meet the pre-defined acceptable risk level $\widehat{RL}(\mathcal{A}, \mathcal{T})$.

The following main features and benefits can be named:

- In contrast to traditional risk-based access control systems, where the access control policies remain static regardless the variation in the risk level of the assets belonging to an organization, with this method inspired on evolutive algorithms the access control policies are dynamically re-shaped, adapting this way the effectiveness of the security controls over a specific asset $\mathcal{A}$, $E(\mathcal{A})$, and consequently modifying its current risk level $RL(\mathcal{A}, \mathcal{T})$.
- Such mechanism is able to promptly and accurately react to sudden and numerous variations of the risk level of several assets within an organization in an autonomous and automatic way, releasing human system administrators from the overwhelming task of manually adapting the security controls of each asset to protect them in such a dynamic environment.
- Instead of adopting the simplistic, but at the same time drastic and counter-productive remedy of denying access to an asset $\mathcal{A}$ when its current risk level $RL(\mathcal{A}, \mathcal{T})$ exceeds the acceptable risk $\widehat{RL}(\mathcal{A}, \mathcal{T})$, this method is able to find the optimal set of counter-measures specific for the current risk level of such asset $\mathcal{A}$, $RL(\mathcal{A}, \mathcal{T})$, not under or over estimating its protection, achieving the right balance between risk control and service denial.

Please cite this article in press as: D. Díaz-López, et al., Dynamic counter-measures for risk-based access control systems: An evolutive approach, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.10.012

- With this method it is possible to develop an access control system which allows access depending on the fulfillment of a set of security controls appropriated to handle the measured risk $RL$ and turn it to permissible values $\widehat{RL}$. In this way the protection of the asset is not based on the denegation of the access, but in the hardening of the security controls that enable the security of the access to the resource.
- The proposed method incorporates different levels of effectiveness (low, medium, high) for different categories of security controls (encryption techniques, backup strategies, authentication mechanisms, etc.) within the counter-measures. The system administrator determines the actual meaning of each of these effectiveness levels based on different well-known technologies or standards, depending on own technical considerations. For instance, within the category of encryption techniques, a symmetric encryption with a key length of 112 bits can be associated with a high effectiveness for the security control encryption against an eavesdropping threat. On the other hand, the same encryption but with a 88 bits key may be associated with a medium effectiveness against the same threat. This fact gives enough flexibility and openness in the selection of different technologies to actually implement security controls applicable within a counter-measure.

The remainder of the paper is organized as follows: In Section 2 we describe the concept of risk-adaptable access control, while in Section 3 we present our solution to dynamically generate counter-measures using evolutive algorithms in the context of risk-based access control systems. An instantiation of the previous proposal is shown in Section 4 and experiments for a specific authorization scenario are reported and analyzed in Section 5. Finally, Section 6 surveys some of the most relevant related works and Section 7 outlines the conclusions and new ideas for future work.

## 2. Toward risk based access control systems

The objective of access control systems is to handle privileges over assets, which are typically digital information, in a way that the assets' responsible can manage to whom and how the assets are disclosed. Nowadays, these systems have special importance with the growing information access necessity by the population and the high digital content production by a number of different sources [15].

Some typical access control systems are based upon the idea that operational benefits for sharing information are bigger than the risk involved in the sharing procedure, underestimating the threats that could affect data. In this context, it is typical that access control systems dangerously assume an homogeneous environment where everybody who requires access to the information is trusted and is located in safe environments. Moreover, it is assumed that the endpoints (e.g. laptops, tablets, etc.) used by the requesters fit minimum security requirements. In this typical scenario, MAC (Mandatory Access Control) policies [16] are initially evaluated and only if these succeed, then DAC (Discretionary Access Control) policies [17] are evaluated to conclude a final authorization decision.

### 2.1. Risk-adaptable access control systems

A new paradigm in access control environments named Risk-Adaptable Access Control (RAdAC) [18,19] is based upon the concept that an authorization decision has to be the result of evaluating access risk levels ($RL$), access operational needs ($OP$) and access control policies, as shown in Fig. 1.

As observed, in a RAdAC system, regardless of the chosen implementation framework, there is a RAdAC engine which makes the resolution of authorization decisions using inputs from the following modules: (i) risk level module, (ii) operational need module and (iii) access control policies module. The RAdAC engine implements a logic which compares the calculated risk levels $RL$ coming from the risk level module with the permissible risk levels $\widehat{RL}$ defined by the access control policy which apply for that specific authorization context.

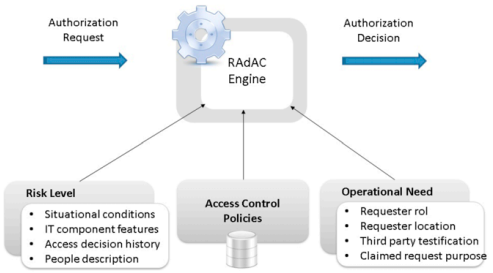


**Fig. 1.** RAdAC process model.

On the one hand, the risk level $RL$ (similarly the acceptable risk level $\widehat{RL}$) refers to the evaluation of security conditions over which the authorization request is done and it is calculated upon different factors like: IT components features (asset ownership, security compliance), objects features (sensitivity, object ownership), situational conditions (hostility, emergency), people description (trust, skills) and past situations (antecedents, heuristics). For each of these $n$ factors there are associated risk levels $RL_i$ which together compose a unique risk level $RL$, as described in Eq. (2). The risk level depends on the methodology used for quantifying individual risk and some application-based proposals can be found in [20,21].

$$\begin{aligned} RL &= f_1(RL_1, RL_2, \ldots, RL_n) \\ \widehat{RL} &= f_2(\widehat{RL}_1, \widehat{RL}_2, \ldots, \widehat{RL}_n). \end{aligned} \tag{2}$$

On the other hand, the operational need $OP$ (named "purpose" in some literature) refers to the process of evaluating the requester necessity for executing an action over a specific resource. This evaluation can be performed in every authorization decision evaluation or just when the access control policy requires it. This evaluation process is particularly critic in situations where the calculated risk levels do not fall within suitable ranges, but the circumstances merit the access (i.e. life danger situations, national security alerts, etc.). The operational need $OP$ must be delimited and quantifiable, and it depends on many factors (like the user role, localization, etc.) and may include a third party testification which justifies a claimed operational need. As shown in Eq. (3), the overall operational need $OP$ also depends on the operational need $OP_i$ associated to each of the mentioned $m$ factors.

$$\begin{aligned} OP &= g_1(OP_1, OP_2, \ldots, OP_m) \\ \widehat{OP} &= g_2(\widehat{OP}_1, \widehat{OP}_2, \ldots, \widehat{OP}_m). \end{aligned} \tag{3}$$

The operational need and the risk levels must be consistent and precise since a mistake in the calculation could trigger a disclosure or denegation for sensitive information. Additionally, these processes must be developed in real time and with a low latency to guarantee that the RAdAC model can be deployed in real conditions.

Finally, the access control policies are the elements that include all the specified values over which an operational need $\widehat{OP}$ and a risk level $\widehat{RL}$ can be considered as valid to grant a succeeded authorization access; and additionally may assign different weights to different components of a risk level (e.g. personal risk, IT risk, environmental risk) in order to calculate a unique risk value.

Please cite this article in press as: D. Díaz-López, et al., Dynamic counter-measures for risk-based access control systems: An evolutive approach, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.10.012

Depending on the result of the comparison between $RL$ and $\widehat{RL}$ made by the RAdAC engine, two situations are plausible:

1. If the calculated risk levels are in the permissible margins (i.e., $RL \leq \widehat{RL}$), the engine will proceed to check if the access control policy requires an operational need validation in order to grant access.
   (a) If the access control policy does not require operational need validation, the access is granted.
   (b) Otherwise, the engine will compare the calculated operational need $OP$ coming from the operational need module with the permissible operational need value $\widehat{OP}$ defined by the access control policy which applies for that specific authorization context.
      i. If the calculated operational need values are in the permissible margins (i.e., $OP \leq \widehat{OP}$), the engine will grant the access.
      ii. Otherwise access will be denied.
2. In case the calculated risk levels are out of the permissible margins (i.e., $RL > \widehat{RL}$), the engine will check if the access control policy allows an exceptional situation where specific operational need values prevail over risk level even if the latter does not fit in permissible margins.
   (a) If an exceptional situation is not considered in the access control policy, the access will be denied.
   (b) If the access control policy allows the exceptional situation, the engine will compare the calculated operational need values $OP$ with the permissible operational need values $\widehat{OP}$ defined by the access control policy which apply for that specific authorization context.
      i. If the calculated operational need values are in the permissible margins (i.e., $OP \leq \widehat{OP}$), the engine will grant the access.
      ii. Otherwise access will be denied.

In any case, the RAdAC model considers the inclusion of the authorization result in a log in order to support future decision resolutions, as for adjusting values used in comparison processes (permissible risk levels $\widehat{RL}$, permissible operational need values $\widehat{OP}$) defined in the access control policies.

## 3. Dynamic counter-measures management approach

Recent publications [22–24] have proposed the inclusion of threat analysis which considers some conditions like the trust and risk level over which a resource is accessed in order to influence an authorization decision. A threat analysis over a resource leads generally to temporal allocation of the resource in a risk level (high, normal, low or so). For each risk level and kind of resource, an administrator has to trigger specific counter-measures to protect the resource. In an undersized access control system an administrator could have a well perspective of resources and attributes that allows him to follow the changes in risk level and react promptly with a set of counter-measures. However in medium/large access control systems some issues arise related to the number of resources that need to be protected, the significant number of users and the amount of systems that need to be configured for access control. The complexity of the access control system grows up due to the many access control policies associated with resources that make almost impossible to react in a proper way to a bunch of risk level emergencies asking for attention.

One of the first issues is related to the fact that in access control systems the number of risk level emergency situations is depending clearly on the way to estimate the risk, but it is also proportional to the number of managed resources. This suggests that for an active and sizable system, it is likely to have hundreds of risk level emergencies converging in one single moment, becoming unfeasible for a system administrator to settle appropriate counter-measures for each emergency, bearing in mind the attributes related to each kind of resource.

Further, a counter-measure proposed by an administrator is not always the best solution, since there are many possibilities to protect a resource using different kinds of attributes and security validations. Additionally, if the organization holding the access control system adopts a standard for information security management, like ISO/IEC 27001, the security actions launched by the administrator have to be aligned with specific objectives for information security controls.

Generally, a risk level is temporal and it changes according to the variability of access conditions and the responsiveness of the method to develop the threat analysis. This leads into an oscillation of the risk level values along the time, being necessary to define a set of counter-measures for each of these values. Defining counter-measures as a function of the risk level is also a strenuous commitment for an administrator, but also necessary to allow different protection levels in accordance with the circumstances and no just counter-measures of generic application.

Moreover, it is likely to consider the junction of single counter-measures as a more effective resource protection mechanism than if each counter-measure stands apart. Doing junction requires the consideration of many crossing possibilities and many of them would be hardly considered by an administrator.

Given the above considerations, this section proposes a method that includes different smart mechanisms and techniques to choose the best set of counter-measures applicable in a system where a number of resources might dynamically have associated certain risk levels. These sets of found counter-measures guarantee the security controls that are necessary to turn the risk from a measured level $RL$ to an acceptable level $\widehat{RL}$. Additionally, it enables the access control system to manage the access depending on the fulfillment of certain security conditions expressed in the counter-measures that are integrated in the access control policies.

### 3.1. Evolutive algorithms and genetic algorithms

Evolutive computation [25] uses natural evolution models based on individuals representing an adaptation solution to a context, and simulate them through computing, using probabilistic optimization techniques. Within evolutive computation techniques there is a subgroup called genetic algorithms [26], which are defined as optimization, search and learning algorithms inspired by natural evolution and genetic evolution. Genetic algorithms are generally composed of the following procedures: (i) initialization of a population, (ii) selection of individuals from such population, (iii) recombination of individuals, (iv) mutation of individuals and (v) evaluation of generated individuals until a stop condition is satisfied. Two main models are possible inside genetic algorithms, namely: generational and stationary model. Generational model refers to the creation in each iteration of a new generation of individuals which replaces completely the previous generation, whereas stationary model refers to the choice of two parents in each iteration to generate one or more new individuals who replace part (not all) of the previous population.

In order to find the best set of counter-measures applicable for a specific authorization context, in this paper we adopt some concepts around genetic algorithms. Specifically, the evolutive method to find the best individual involving the aforementioned different steps (initialization, selection, recombination, mutation and evaluation) will be applied to find the best set of counter-measures. As we will see later, in our case an individual represents a combination of a number of single counter-measure defining the security actions to appropriately protect a certain asset according to the detected risk condition.

Please cite this article in press as: D. Díaz-López, et al., Dynamic counter-measures for risk-based access control systems: An evolutive approach, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.10.012

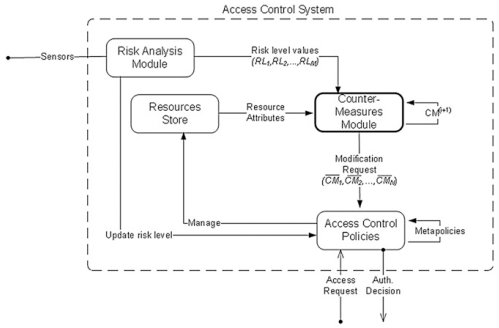


**Fig. 2.** Counter-measures module within the context of an access control system.

### 3.2. Integration in risk-based access control systems

Counter-measures can be represented in an access control policy through security predicates which are included in one or many sections of a policy, for example in XACML (eXtensible Access Control Markup Language) [27,28], which is one of the most popular languages for policies definition, these parts are: Target, Condition and Obligation. The security predicates define wished characteristics of the parties (subject, resource, action, environment) through attribute statements, conditions and disjunctive/conjunctive sequences (grouping of predicates). The existence of security predicates in access control policies defines the authorization context information which will be verified and evaluated in order to grant or deny a permit. Thus, more strict security predicates in an access control policy represent more strict counter-measures.

A regular access control architecture can be seen in Fig. 2. This architecture comprises an "Access control policies" module, which is responsible of handling the established access control policies, receiving access control requests and issuing and enforcing access control decisions. Another module depicted in Fig. 2 is the "Resources store", containing the attributes of the assets to be managed (for example criticality, ownership, location, etc.) and it is accessed by the "Access control policies" module when some asset information is required to resolve an authorization decision.

Additionally, in order to conform a risk-based access control system, a module called "Risk analysis module" is also included in this architecture. This module essentially uses sensors which review regularly the context and measure variables required to calculate the risk (e.g. threat score, user conduct, threat likelihood, actual security controls, etc.). A practical example of a solution used in some enterprises to estimate risk is McAfee Risk Advisor [29,30], which estimates a risk score for each asset and each threat identified in the McAfee Threat Intelligence Services (MTIS) database. In this proprietary solution the risk level ($RL_{McAfee}$) goes from 0 to 100 and it is computed as shown in Eq. (4) (which, essentially, is similar to Eq. (1)):

$$RL_{McAfee} = \frac{T \cdot V \cdot A_c}{C} \tag{4}$$

where

- $T$: Threat score from the MTIS database. Possible values: from 0 to 10, being 10 a very serious threat.
- $V$: Vulnerability status. Possible values: 0 (not vulnerable), 0.5 (insufficient data), 1 (vulnerable).
- $A_c$: Asset criticality. Possible values: 2 (low), 4, 6 (high), 8, 10 (most critical).
- $C$: Countermeasure status. Possible values: 1 (not protected), 10 (protected).

Finally, in order to get an access control policy which can be suitable for a specific risk level ($RL$), a set of dynamically-generated counter-measures (which can be integrated in the policy) are defined to face variations in the risk level. To define the most appropriate set of counter-measures applicable for a specific situation we propose a method inspired on optimization algorithms (specifically, genetic algorithms [31,32]). Such method would be integrated in a "counter-measures module" modifying the access control policies according to the risk levels, as shown in Fig. 2.

An example of a counter-measures set can be illustrated when the "risk analysis module" detects an "unauthorized access threat" over an information asset (e.g., a file) and the "access control module" has to apply an access control policy including a proper set of counter-measures which in turn have been previously defined by the "counter-measures module". Some examples of possible counter-measures against an "unauthorized access threat" could be: (1) encryption techniques, (2) alert mechanisms, (3) user advertising strategies and (4) authentication mechanisms. Each of these counter-measures constitute a security control which can be applied in different degrees (high, medium or low effectiveness) according to the detected risk level:

- Encryption techniques [33,34] allow us to secure the communication channel between endpoints even in an unknown and possible hostile environment, being the "encryption key size" and the "algorithm" (e.g., AES-128, AES-192, AES-256) important parameters to set up the encryption hardiness and therefore define the effectiveness against the detected threat.
- Alert mechanisms allow to inform certain stakeholders who are related to the threatened information asset. For example, if the threat is considered to have low danger it would be pertinent to inform the direct asset custodian, while in case the threat is considered to be moderately perilous, it would be pertinent to inform the asset custodian and responsible, and in case the threat is considered highly harmful, it would be necessary to inform the asset custodian, responsible and owner.
- User advertising strategies [35,36] are useful to avoid unintentional unauthorized accesses by warning the asset user about a restricted access. For example, a pop-up message indicating that the asset has a certain level of confidentiality can be displayed when a regular user attempts to access a restricted file. In case an intentional unauthorized access is detected (multiple attempts), a pop-up message indicating legal implications related with those irregular attempts can also help to persuade the attacker to cease this kind of activities.
- Authentication mechanisms [37,38] can be used as a counter-measure by defining different authentication requirements for different situations when an unauthorized threat is detected. For example, when the risk is high, three different authentication factors (a physical token, a password and a fingerprint) can be required; when the risk is medium, two different authentication factors (a physical token and a password) can be required, and when the risk is low two instances of one authentication factor (a password and a secret question) can be required.

The counter-measures are integrated within the access control policies, so when the authorization context is detected with a specific risk value and threat, some access conditions can be applied in order to guarantee a secure access to a specific resource.

### 3.3. Proposal steps

#### 3.3.1. Initialize acceptable risk levels

An acceptable risk level $\widehat{RL}$ is allocated for each managed asset $\mathcal{A}$ in an access control system. This asset (or resource) attribute (acceptable risk level) gives details about the security requirements for a resource according to a protection and classification policy

Please cite this article in press as: D. Díaz-López, et al., Dynamic counter-measures for risk-based access control systems: An evolutive approach, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.10.012

for resources implemented by the organization who owns the resource. In multi-level security systems (MLS) [39] the risk level allocated to a resource depends on its properties regarding: confidentiality, sensibility, availability, integrity or importance. In addition, a common risk level may indicate information related to the business impact, like financial and reputation damage for the organization if an unauthorized disclosure of the resource is produced.

*3.3.2. Initialize measured risk levels*

As shown in Fig. 2, a set of $M$ risk level values associated with an asset $\mathcal{A}$, $\{RL_1, RL_2, \ldots, RL_M\}$, are received from an active risk analysis module. The number and kind of risk levels depends on the implementation of the risk analysis module.

*3.3.3. Find optimal counter-measures*

The goal of our proposed method consists of finding the optimal set of counter-measures to apply for each one of the given $M$ risk levels $\{RL_1, RL_2, \ldots, RL_M\}$ in order to adapt such measured risk and lead it to the given acceptable risk level $\widehat{RL}$, in order to achieve an effective and efficient protection of asset $\mathcal{A}$.

1. Initialize population of set of counter-measures
   Initialize $N$ individuals $I_i = \overline{CM}_i$ to set up an initial population $P$, where each $\overline{CM}_i$ is a set of $r_i$ single counter-measures $cm_j^i$. And each atomic counter-measure $cm_j^i$, in turn, is a set of $x_j^i$ security predicates suitable for tuning an access control policy (see Eq. (5)).

$$P = \{I_1, I_2, \ldots, I_N\} = \{\overline{CM}_1, \overline{CM}_2, \ldots, \overline{CM}_N\};$$

$$\overline{CM}_i = \{cm_1^i,\ cm_2^i, \ldots,\ cm_{r_i}^i\}$$

$$cm_j^i = \{Predicate_1, \ldots, Predicate_{x_j^i}\}. \quad (5)$$

   In order to increase the possibility of finding an optimal individual for each risk condition through an evolutive process, it is necessary the existence of at least one possible solution $\overline{CM}_i$ for each risk level $RL_k$, and therefore the following condition is defined: $N \geq M$.

   The inclusion of security predicates in an access control policy entails the alteration of some of its parts and these parts change depending on the policy definition language. In the case of XACML, which is the most popular language to define access control policies, a policy is composed of three main parts: target, condition and obligation. Thus in XACML an atomic counter-measure $cm_j^i$ would include predicates related to Target and/or Condition and/or Obligation (see Eq. (6)).

$$cm_j^i = \{Predicate_{Target},\ Predicate_{Condition},\ Predicate_{Obligation}\}. \quad (6)$$

2. Execution of the optimization algorithm:

**Algorithm 1** Optimization Algorithm

**repeat**
  i. Best individuals selection
  ii. Crossover
  iii. Mutation
  iv. New generation
**until** *StopCondition*

Algorithm 1 shows the main steps of the optimization process, where

$$StopCondition = GenerationsNumberReached \vee ComputationTimeReached \vee NoImprovementInSecurity.$$

*NoImprovementInSecurity* stop condition states the moment when the difference in the value returned from an evaluation function associated to the set of best individuals between successive loops is smaller than a representative threshold.

(a) Best individuals selection:
Apply an evaluation function $F(\overline{CM}_i, RL_k) = \phi_k^i$ to each individual $\overline{CM}_i$ in the population $P$ to determine its affinity with every risk level $RL_k$ (as shown in Algorithm 2). An example of evaluation function will be described in Section 4.3.3 where a fitness function is defined, considering different counter-measures related variables.

**Algorithm 2** Individuals fitness computation

**for** $i \leftarrow 1$ **to** $N$ **do**
  **for** $k \leftarrow 1$ **to** $M$ **do**
    Calculate $F(\overline{CM}_i, RL_k) = \phi_k^i$
  **end for**
**end for**

The result of applying $F(\overline{CM}_i, RL_k)$ for each one of the $M$ risk levels $RL_k$ can be represented as a matrix of $M$ columns and $N$ rows.

$$A = \begin{pmatrix} \phi_1^1 & \phi_2^1 & \cdots & \phi_M^1 \\ \phi_1^2 & \phi_2^2 & \cdots & \phi_M^2 \\ \vdots & \vdots & \ddots & \vdots \\ \phi_1^N & \phi_2^N & \cdots & \phi_M^N \end{pmatrix}.$$

In this way, each column $k$ of the matrix $A$ contains the evaluation of the whole population $P$ for a specific risk level $RL_k$.

Then, next step consists of selecting a maximum of $M$ different individuals $\overline{CM}_i$ with the highest value $\phi_k^i$ for each column in the matrix $A$ and putting them in the set *BCM* (Best counter-measures) as described in Algorithm 3.

$$BCM = \{\overline{CM}_{RL_1}, \overline{CM}_{RL_2}, \ldots, \overline{CM}_{RL_M}\}.$$

This $M$ individuals represent the best set of counter-measures applicable for each risk level $RL_k$ at the moment. Hence, the individuals included in *BCM* pass to the new generation.

In order to generate the remainder $N - M$ individuals necessary to complete a new population of size $N$, reproduction operations are developed according to steps ii and iii of Algorithm 1. The individuals over which these reproduction operations are applied, are selected from the previous population $P$ and are represented in the new set *RCMP* (Reproductive counter-measures population). The selection can be done through any regular method, including common selection methods (e.g. roulette wheel selection, stochastic universal sampling, etc.) [40,41], considering some attributes of the individuals (size, content, age, etc.), using a random process, or even a mix of these.

(b) Crossover:
Execute a crossover operation (union, intersection, etc.) between two individuals $(I_a, I_b)$ from *RCMP*. The resulting individual $I_c$ has to pass a validity function which verifies the nonexistence of contradictions or inconsistencies due to the crossover operations. It is necessary to execute a crossover operation as many times as needed until reaching $N - M$ valid individuals (see Algorithm 4). The new individuals are placed in the set *RCMP'*, which is the entrance to the next step.

The selection of two individuals from *RCMP* may be done in different ways according to some attributes of the individuals (e.g. size, content), through conventional selection

Please cite this article in press as: D. Díaz-López, et al., Dynamic counter-measures for risk-based access control systems: An evolutive approach, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.10.012

**Algorithm 3** Best individuals selection

**for** $k \leftarrow 1$ **to** $M$ **do**
  $\phi_k^i \leftarrow max\left\{\phi_k^1, \ldots, \phi_k^N\right\}$
  $\overline{CM}_{RL_k} \leftarrow \overline{CM}_i$
  Add $\overline{CM}_{RL_k}$ to $BCM$
**end for**

**for** $l \leftarrow 1$ **to** $(N - M)$ **do**
  $I_l \leftarrow SelecteOneIndividual(P)$
  Add $I_l$ to $RCMP$
**end for**

**return** $\{BCM, RCMP\}$

**Algorithm 4** Crossover operation

**repeat**
  $(I_a, I_b) \leftarrow SelectTwoIndividuals(RCMP)$

$$I_c = \begin{cases} I_a \cap I_b \text{ with probability } p_1 \\ I_a \cup I_b \text{ with probability } p_2 \\ I_a \setminus I_b \text{ with probability } p_3 \\ operation_l \text{ with probability } p_l \end{cases}$$

  **if** $(ValidityFunction(I_c) = \text{TRUE})$ **then**
    Add $I_c$ to $RCMP'$
    $d \leftarrow d + 1$
  **end if**
**until** $d = N - M$

methods or using a random process. Equally, the decision of applying one of the crossover operations (union, intersection, difference, etc.) may be a deterministic or random process.

(c) Mutation:
Execute a mutation operation (add, delete, modify, discompose, etc.) over each individual in the set $RCMP'$. Mutation operation has an effect directly on the atomic counter-measures $cm_j^i$ integrated within the individual $\overline{CM}_i$ (see Algorithm 5). In the case of an "add operation", a $cm_j$ is selected from a group of external counter-measures $EC$ and incorporated to the individual $\overline{CM}_i$.

**Algorithm 5** Mutation operation

**for** $i \leftarrow 1$ **to** $|RCMP'|$ **do**

$$\overline{CM}_i = \begin{cases} \overline{CM}_i \cup cm_{new} \text{ where } cm_{new} \in EC \\ \qquad \text{with probability } p_1 \\ \overline{CM}_i \setminus cm_j^i \text{ where } j \in \{1, \ldots, r_i\} \text{ randomly} \\ \qquad \text{with probability } p_2 \\ \text{modify } cm_j^i \in \overline{CM}_i \text{ to obtain } \widetilde{cm}_j^i \\ \qquad \text{with probability } p_3 \\ \text{split } cm_j^i \in \overline{CM}_i \text{ into } cm_{j_1}^i \text{ and } cm_{j_2}^i \\ \qquad \text{with probability } p_4 \\ \qquad \vdots \\ operation_l \text{ with probability } p_l \end{cases}$$

**end for**

(d) New generation:
The new generation is composed by the individuals $\overline{CM}_i$ stored in $BCM$, plus the individuals stored in $RCMP'$, as shown in Eq. (7).

$$P \leftarrow BCM \cup RCMP'. \tag{7}$$

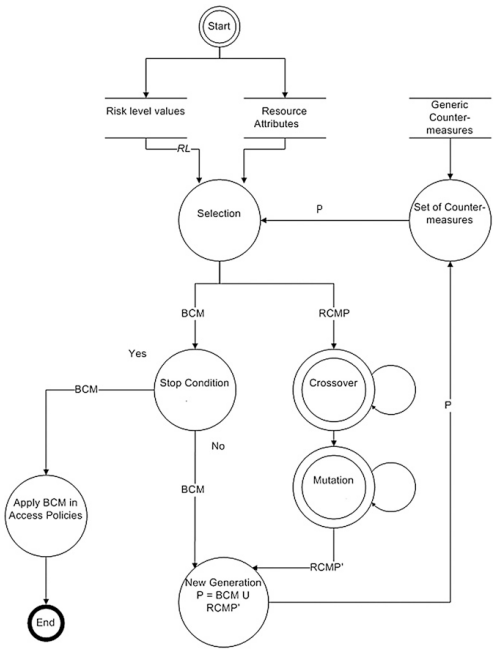


**Fig. 3.** Data flow diagram for the proposed model.

3. Apply counter-measures:
At the end of the optimization process, $BCM$ contains the best individuals $\overline{CM}_{RL_k}$ (sets of individual counter-measures) applicable for each risk level $RL_k$. Therefore, it is necessary to select those access control policies protecting the affected asset $\mathcal{A}$ through a $SelectPolicies(\mathcal{A})$ function. Subsequently, we must integrate the optimal counter-measures found for each risk level over those selected policies, as described in Algorithm 6.

**Algorithm 6** Apply counter measures operation

$Policies_{\mathcal{A}} \leftarrow SelectPolicies(\mathcal{A})$
**for** $k \leftarrow 1$ **to** $M$ **do**
  $ModifyPolicies(Policies_{\mathcal{A}}, \overline{CM}_{RL_k})$
**end for**

Any modification over an access control policy has to be done generally through administrative policies. An administrative policy defines operations that a given entity can execute over a certain policy. In order to integrate a number of counter-measures in a particular policy, at least one administrative policy has to be defined within the access control system, stating that a given module can modify the parts of such policy over which the counter-measures are applied.

A data flow diagram representing the execution of the previous steps is shown in Fig. 3.

## 4. Proposal instantiation

In this section we develop one possible instantiation of the method proposed in Section 3.3, defining and analyzing different aspects of the evolutive algorithm in place.

Please cite this article in press as: D. Díaz-López, et al., Dynamic counter-measures for risk-based access control systems: An evolutive approach, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.10.012

**Table 1**
Security control categories.

| | Security control category | Applicable asset type | Covered threats |
|---|---|---|---|
| $scc_1$ | Authentication mechanisms | Software, Information | Unauthorized access, Privileges escalation |
| $scc_2$ | Encryption techniques | Software, Information | Eavesdropping, Unauthorized access |
| $scc_3$ | Attestation techniques | Information | Unauthorized access, Information loss |
| $scc_4$ | Repudiation mechanisms | Information | Manipulation of info, Information loss |
| $scc_5$ | Isolation means | Software | System failure, Malicious code |
| $scc_6$ | Input validation strategies | Software | Malicious code, Denegation of service |
| $scc_7$ | Settings change management strategies | Software | Malicious code, Privileges escalation |
| $scc_8$ | Versions management strategies | Information | Manipulation of information, Malicious code |
| $scc_9$ | Monitoring strategies | Software | Privileges escalation, System failure, Unauthorized access, Malicious code, Denegation of service |
| $scc_{10}$ | Software execution schemas | Software | System failure, Malicious code |
| $scc_{11}$ | Session time assignment | Software | Privileges escalation, Unauthorized access, Malicious code |
| $scc_{12}$ | Resource exposure | Information | Unauthorized access, Eavesdropping |
| $scc_{13}$ | Alert mechanisms | Software, Information | Unauthorized access, Eavesdropping, Manipulation of information, Information loss, Denegation of service, Malicious code, Privileges escalation, System failure |
| $scc_{14}$ | User advertising strategies | Software, Information | Manipulation of Information, Information loss, Unauthorized access |
| $scc_{15}$ | Routing mechanisms | Information | Eavesdropping, Denegation of service |
| $scc_{16}$ | Backup strategies | Information | Manipulation of information, Information loss, Denegation of service |

In order to evaluate the previously proposed method in a real scenario, we have defined a situation in a regular enterprise holding many information assets whose access is handled using access control systems. This scenario is composed by a risk analysis module, a resource store, a counter-measures module and an access control policies engine, as represented in Fig. 2.

### 4.1. Risk analysis module

The risk analysis module monitors context conditions to identify a threat $\mathcal{T}_j$ over an asset $\mathcal{A}_i$ and calculate an asset-associated risk value ($RL(\mathcal{A}_i, \mathcal{T}_j)$, or just $RL$). We assume this module to be implemented using a risk estimation methodology which gives us (in real time) a measured risk level value and an ID of the threat which provoked this risk for a specific asset.

Such risk estimation methodology used to assess the measured risk level value commonly considers variations in the vulnerabilities exploitation probability, the estimated asset impact and factors like: IT components features, objects features, situational conditions, user profile and past situations (heuristic). We define the measured risk level value as $RL(\mathcal{A}_i, \mathcal{T}_j) \in [1, 10]$, where 1 is the lowest risk value and 10 the highest risk value that can be measured.

In turn, we have identified 8 types of generic threats [42] that can occur over the assets of the aforementioned enterprise, namely: (i) denegation of service, (ii) unauthorized access, (iii) eavesdropping, (iv) manipulation of records, (v) information loss, (vi) privileges escalation, (vii) system failure and (viii) malicious code. Each of these threats has internally an earmarked ID from 1 to 8 ($\{\mathcal{T}_1, \ldots, \mathcal{T}_8\}$), used to recognize the source of risk.

### 4.2. Assets store

The assets store (or resources store) contains attributes about the assets $\mathcal{A}_i$ which are used by the counter-measures module to define an appropriated solution for a specific kind of asset. In our scenario, the assets store provides the following asset attributes: (i) kind of asset (which we define as either information asset or software asset), (ii) acceptable computational load ($ACL$) for a found solution and (iii) acceptable risk level ($\widehat{RL}(\mathcal{A}_i, \mathcal{T}_j)$, or just $\widehat{RL}$).

Regarding $ACL$, it defines how much computational load the access control system is willing to dedicate to protect an asset $\mathcal{A}$. Each set of counter-measures $\overline{CM}_i$ that can be found as a solution to protect an asset $\mathcal{A}$ will require a computational load for its execution and, depending on the asset characteristics (e.g., importance, impact), the applicability of a set of counter-measures which require a high computational load could be acceptable or not. Therefore, we have defined the acceptable computational load as taking the following values $ACL \in \{Low, Medium, High\}$.

As for the acceptable risk level $\widehat{RL}(\mathcal{A}_i, \mathcal{T}_j)$, this value depends on the asset impact $I(\mathcal{A}_i)$ within the organization owning such protected asset, and represents how much the organization is willing to jeopardize a given asset $\mathcal{A}_i$. Critical assets are expected to have a low acceptable risk level since even the exploitation of an insignificant vulnerability could disrupt the normal asset state. We define the acceptable risk level as $\widehat{RL}(\mathcal{A}_i, \mathcal{T}_j) \in [1, 10]$, where 1 referred to a critical asset requiring the maximum possible protection level and 10 referred to a non-critical asset for which the minimum protection level is accepted.

### 4.3. Counter-measures module

The counter-measures module contains an instantiation of the method proposed in Section 3, which aims to find the best set of counter-measures which can gauge the measured risk level value $RL$ to the acceptable risk level value $\widehat{RL}$ defined for an asset. In order to define the functionality of this module we have made some design decisions over the flow diagram shown in Fig. 3, as described next.

#### 4.3.1. Generic counter-measures sets

The initial population for the algorithm is a set of $N$ candidate solutions $P = \{\overline{CM}_1, \ldots, \overline{CM}_N\}$ built in a random way using as a basis the following 16 security controls categories ($\{scc_1, \ldots, scc_{16}\}$), which embrace actions used for platform assurance labors, namely: authentication mechanisms, encryption techniques, attestation techniques, repudiation mechanisms, isolation means, input validation strategies, settings change management strategies, versions management strategies, monitoring strategies, software execution schemas, session time assignment, resource exposure, alert mechanisms, user advertising strategies, routing mechanisms and backup strategies.

Each security controls category defines actions in benefit of the confidentiality, integrity and/or availability of the assets to be protected within the organization (see Table 1). Each solution

Please cite this article in press as: D. Díaz-López, et al., Dynamic counter-measures for risk-based access control systems: An evolutive approach, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.10.012

$\overline{CM}_i = \{cm_1^i, \ldots, cm_{r_i}^i\}$, where $r_i \in \{1, \ldots, r^{\max}\}$ and each $cm_j^i$ defines one out of the 16 security controls categories $scc_l^j$, $l \in \{1, \ldots, 16\}$. In the algorithm, the number $r_i$ of counter-measures $cm_j^i$ in a candidate solution $\overline{CM}_i$ are defined randomly considering the maximum permissible value $r^{\max}$. Additionally, each security controls category $scc_l^j$ comes with an effectiveness value $E(scc_l^j)$ representing how much effective should the application of the security control be to protect a certain asset $\mathcal{A}$ against a given threat $\mathcal{T}$. In the algorithm, this effectiveness of a category is set randomly and can take any of following values $E(scc_l^j) \in \{Low,\ Medium,\ High\}$. Eq. (8) shows, in a nutshell, these definitions (which are actually an instantiation of Eq. (5)).

$$\begin{aligned} &P = \{\overline{CM}_1, \overline{CM}_2, \ldots, \overline{CM}_N\};\\ &\overline{CM}_i = \{cm_1^i,\ cm_2^i, \ldots,\ cm_{r_i}^i\} \quad r_i \in \{1, \ldots, r^{\max}\}\\ &cm_j^i = \langle scc_l^j, E(scc_l^j)\rangle\\ &\quad E(scc_l^j) \in \{Low,\ Medium,\ High\}\ l \in \{1, \ldots, 16\}. \end{aligned} \tag{8}$$

#### 4.3.2. Selection method

Individual selection corresponds to the step of Algorithm 1 choosing those individuals over which reproduction operations will be applied. That is to say, more specifically, the *SelectOneIndividual*($P$) function in Algorithm 3. To this end, the following probabilistic selection methods are available [40,41]: roulette wheel selection, stochastic universal sampling, rank selection, sigma scaling and truncation selection. In particular for this instantiation, we decided to use the roulette wheel selection method, as this one fits well within our requirements.

#### 4.3.3. Fitness function

We have defined a fitness function assessing different aspects in a candidate solution $\overline{CM}_i$ in order to obtain an accurate fitness value for such candidate, $F(\overline{CM}_i, RL_k) = \phi_k^i$. There are many alternatives to implement a fitness function depending on the features (performance, robustness, accuracy, etc.) expected in a valid solution. These features can depend on the kind of assets, attributes of the assets, business objectives, some specific variables coming from the risk analysis module, etc.

For this proposal instantiation, the following features will be considered in the assessment of a candidate solution $\overline{CM}_i$: (i) type of asset correspondence ($TAC(\overline{CM}_i, \mathcal{A})$, or just $TAC_i^{\mathcal{A}} \in [0, 1]$), (ii) acceptable computational load suitability ($CLS(\overline{CM}_i)$, or just $CLS_i \in [0, 1]$), (iii) type of threat correspondence ($TTC(\overline{CM}_i, \mathcal{T})$, or just $TTC_i^{\mathcal{T}} \in [0, 1]$) and (iv) acceptable risk suitability ($ARS(\overline{CM}_i, RL_k)$, or just $ARS_i^k \in [0, 1]$). Each one of these aspects has an associated weight $w \in [0, 1]$ in the general candidate fitness Eq. (9).

$$\begin{aligned} F(\overline{CM}_i, RL_k) = {} & w_{TAC} * TAC_i^{\mathcal{A}} + w_{CLS} * CLS_i\\ & + w_{TTC} * TTC_i^{\mathcal{T}} + w_{ARS} * ARS_i^k \end{aligned} \tag{9}$$

where $w_{TAC} + w_{CLS} + w_{TTC} + w_{ARS} = 1$.

Amongst the benefits of this fitness function and the selected criteria it is worth to mention the following ones:

- All weights for each element included within Eq. (9) can be adjusted according to the context giving enough flexibility and adaptability to determine the most important factors at any time.
- Since the evaluation process considers the type of asset $TAC_i^{\mathcal{A}}$, it is guaranteed that the best candidate solution $\overline{CM}_{Best}$ will provide sets of security controls with real applicability over the threatened asset $\mathcal{A}$ (see Table 1).
- The effort to deploy a security control is an important factor to decide how to protect an asset $\mathcal{A}$. This aspect is considered through the element $CLS_i$, allowing to evaluate solutions $\overline{CM}_i$ according to how much effort (in terms of computational load) the organization is willing to spend protecting such specific asset $\mathcal{A}$.
- Through $TTC_i^{\mathcal{T}}$ it is possible to evaluate candidate solutions $\overline{CM}_i$ according to the correspondence of their security controls with the kind of identified threat $\mathcal{T}$ (see Table 1) and in this way face directly the threat.
- One of the objectives of this fitness function is to evaluate candidates according to its effectiveness, granting a bigger score $ARS_i^k$ when there is more proximity with the required effectiveness to adapt the measured risk level $RL_k$ to the acceptable risk level $\widehat{RL}$. This allows to protect the asset properly without under or over estimating the risk.

Next, each element of the fitness function defined in Eq. (9) is explained in detail:

*Type of asset correspondence ($TAC(\overline{CM}_i, \mathcal{A})$)*: One of the evaluated features is that the type of security control categories $scc_l^j$ which are present in a candidate solution $\overline{CM}_i$, are adequate for the type of asset being protected (information, software). From the 16 security controls categories previously defined, 6 are exclusively applicable for information assets, 6 are exclusively applicable for software assets and 4 are applicable for both types, so there is a maximum of 10 security controls categories applicable for each type of asset.

Let us define $\tau(\overline{CM}_i, \mathcal{A}) \in \{0, \ldots, 10\}$ as the number of different security controls categories contained in $\overline{CM}_i$ that are applicable to the type of asset $\mathcal{A}$, and $\eta(\overline{CM}_i, \mathcal{A}) \in \{0, \ldots, 6\}$ as the number of different security controls categories in $\overline{CM}_i$ that are not applicable to the type of asset $\mathcal{A}$. Then, $TAC(\overline{CM}_i, \mathcal{A}) \in [0, 1]$ is computed as shown in Eq. (10).

$$TAC(\overline{CM}_i, \mathcal{A}) = \frac{\tau}{10 + \eta}. \tag{10}$$

*Acceptable computational load suitability ($CLS(\overline{CM}_i)$)*: Another evaluated feature over a candidate solution $\overline{CM}_i$ is the computational load ($CL(\overline{CM}_i)$, or just $CL_i \in [0, 1]$) that the application of its counter-measures $cm_j^i$ will produce in the available infrastructure. The computational load of a good candidate solution should match with the acceptable computational load ($ACL^{\mathcal{A}} \in \{Low,\ Medium,\ High\}$) defined by means of an asset attribute in the assets store.

The evaluation process of the computational load for a candidate solution $\overline{CM}_i$ is based on the assumption that a security controls category $scc_l^j$ with a high effectiveness value ($E(scc_l^j) = High$) entails a greater computational load than one with $E(scc_l^j) = Medium$ or $E(scc_l^j) = Low$. Let us define $\xi_H \in [0, 1]$ (similarly, $\xi_M$ and $\xi_L$) as the percentage of different security control categories $scc_l^j$ within $\overline{CM}_i$ having $E(scc_l^j) = High$. Eq. (11) shows the way the candidate computational load ($CL_i$) is computed.

$$CL(\overline{CM}_i) = w_H * \xi_H + w_M * \xi_M + w_L * \xi_L \tag{11}$$

where $w_H, w_M, w_L \in [0, 1]$ represent the weight given to those security controls categories with *High*, *Medium* and *Low* effectiveness, respectively. Moreover, these weights fulfill that $w_H > w_M > w_L$ and $w_H + w_M + w_L = 1$.

Please cite this article in press as: D. Díaz-López, et al., Dynamic counter-measures for risk-based access control systems: An evolutive approach, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.10.012

Finally, the acceptable computational load suitability ($CLS(\overline{CM}_i)$) is obtained as indicated in Eq. (12).

$$CLS(\overline{CM}_i) = \begin{cases} 1 & \text{if } \left(ACL^{\mathcal{A}} = Low \wedge CL_i \in [0, 1/3)\right) \vee \\ & \left(ACL^{\mathcal{A}} = Medium \wedge CL_i \in [1/3, 2/3]\right) \vee \\ & \left(ACL^{\mathcal{A}} = High \wedge CL_i \in (2/3, 1]\right) \vee \\ 0 & \text{otherwise.} \end{cases} \quad (12)$$

*Type of threat correspondence ($TTC(\overline{CM}_i, \mathcal{T})$)*: The security controls categories $scc_l^j$ existing in a candidate solution $\overline{CM}_i$ have to be applicable to the type of threat $\mathcal{T}$ identified by the risk analysis module. In this way, from the 16 categories of security controls, there are categories applicable for some or many of the 8 considered threats ($\{\mathcal{T}_1, \ldots, \mathcal{T}_8\}$). A candidate solution $\overline{CM}_i$ including many security controls categories $scc_l^j$ applicable for the specific threat $\mathcal{T}$ which provoked the risk, is expected to get a high fitness value. Let us define $\mu(\overline{CM}_i, \mathcal{T}) \in \{4, \ldots, 9\}$ as the number of different security controls categories contained in $\overline{CM}_i$ that are applicable to threat $\mathcal{T}$ (see Table 1), and $\mu(\mathcal{T}) \in \{4, \ldots, 9\}$ as the total number of security control categories (amongst the 16 considered ones) that are applicable to threat $\mathcal{T}$. Thus, Eq. (13) expresses how $TTC_i^{\mathcal{T}} \in [0, 1]$ is calculated.

$$TTC(\overline{CM}_i, \mathcal{T}) = \frac{\mu(\overline{CM}_i, \mathcal{T})}{\mu(\mathcal{T})}. \quad (13)$$

*Acceptable risk suitability ($ARS(\overline{CM}_i, RL_k)$)*: The algorithm uses the measured risk level value $RL(\mathcal{A}, \mathcal{T})$, the effectiveness of the current security controls protecting asset $\mathcal{A}$, $E(\mathcal{A})$, coming from the risk analysis module and the effectiveness of the candidate solution $\overline{CM}_i$, $E(\overline{CM}_i)$, to estimate the risk level $\widetilde{RL}(\mathcal{A}, \mathcal{T})$ that would be generated by the candidate solution according to Eq. (14).

$$\widetilde{RL}(\mathcal{A}, \mathcal{T}) = \frac{RL(\mathcal{A}, \mathcal{T}) \cdot E(\mathcal{A})}{E(\overline{CM}_i)}. \quad (14)$$

The effectiveness of each candidate solution $\overline{CM}_i$, $E(\overline{CM}_i)$, is calculated from the effectiveness of its security controls categories as a weighted average, as shown in Eq. (15).

$$E(\overline{CM}_i) = w_{E_H} * \rho_{E_H} + w_{E_M} * \rho_{E_M} + w_{E_L} * \rho_{E_L} \quad (15)$$

where $w_{E_H}, w_{E_M}, w_{E_L} \in [0, 1]$ represent the weight given to those security controls categories with *High*, *Medium* and *Low* effectiveness, respectively. Moreover, these weights fulfill that $w_{E_H} > w_{E_M} > w_{E_L}$ and $w_{E_H} + w_{E_M} + w_{E_L} = 1$. In turn, $\rho_{E_H}$, $\rho_{E_M}$, $\rho_{E_L} \in [0, 1]$ represent the percentage of security control categories within candidate solution $\overline{CM}_i$ with *High*, *Medium* and *Low* effectiveness, respectively.

The goal is to find the candidate solution $\overline{CM}_i$ whose effectiveness adapts the measured risk level to the acceptable risk level (i.e., $\widetilde{RL}(\mathcal{A}, \mathcal{T}) \rightarrow \widehat{RL}(\mathcal{A}, \mathcal{T})$). Hence, the acceptable risk suitability for candidate solution $\overline{CM}_i$, $ARS(\overline{CM}_i, RL_k) \in [0, 1]$, is computed as described in Eq. (16).

$$ARS(\overline{CM}_i, RL_k) = 1 - \left|\widehat{RL}(\mathcal{A}, \mathcal{T}) - \widetilde{RL}(\mathcal{A}, \mathcal{T})\right|. \quad (16)$$

#### 4.3.4. Crossover operation

The selection model we adopted in order to choose two individuals (parents) for the crossover operation is the sigma scaling [40,41]. Let $\overline{CM}_a = \{cm_1^a, \ldots, cm_{r_a}^a\}$ and $\overline{CM}_b = \{cm_1^b, \ldots, cm_{r_b}^b\}$ be those two individuals and let us assume, without loss of generality, that $r_a \geq r_b$.

**Table 2**
Mutation of effectiveness values $E(scc_l^j)$ of the security control category $scc_l^j$.

| Original value | Mutated value |
|---|---|
| High | Medium |
| Medium | Low |
| Low | High |

Then, two new individuals $\overline{CM}_{c_1}$ and $\overline{CM}_{c_2}$, respectively, will be generated as shown in Eq. (16).

$$\overline{CM}_{c_1} = \{cm_\iota^{c_1} \mid cm_\iota \in \overline{CM}_a \cap \overline{CM}_b\}$$
$$\overline{CM}_{c_2} = \{cm_1^{c_2}, \ldots, cm_{r_a}^{c_2}\}. \quad (17)$$

For both individuals $\overline{CM}_{c_1}$ and $\overline{CM}_{c_2}$, the effectiveness of the security controls categories contained within those counter-measures belonging to the intersection of the two parents, i.e. $cm_\iota \in \overline{CM}_a \cap \overline{CM}_b$, is randomly selected from the effectiveness that such security controls categories have in the parents $\overline{CM}_a$ and $\overline{CM}_b$, $E(cm_\iota) = E(scc_l^\iota) \overset{random}{\in} \{E(scc_l^a), E(scc_l^b)\}$.

In the particular case of individual $\overline{CM}_{c_2}$, for those counter-measures not belonging to such intersection, $cm_{\iota'} \notin \overline{CM}_a \cap \overline{CM}_b$, their effectiveness is directly replicated from the one expressed in individual $\overline{CM}_a$, $E(cm_{\iota'}) = E(cm_{\iota'}^a)$.

#### 4.3.5. Mutation operation

In this operation one counter-measure $cm_j^i$ of a solution candidate $\overline{CM}_i$ is randomly selected, and a mutation operation over the effectiveness of its security controls category $scc_l^j$, $E(scc_l^j)$, is performed to generate a new individual as shown in Table 2.

## 5. Experiments and results

A set of experiments have been conducted to evaluate the ability of the proposed solution to protect an information asset using a set of counter-measures designed to adapt a risk level measured over an asset $RL(\mathcal{A}, \mathcal{T})$, to the acceptable risk level $\widehat{RL}(\mathcal{A}, \mathcal{T})$ defined for such information asset. This adaptation capability allows a RAdAC system to handle responses according to the current risk level measured over an information asset, and so protect it without over or under shielding the asset.

In order to develop the experiments, a framework for evolutionary computation[1] has been used to develop a RAdAC system that incorporates the logic described in Section 4. The experiments are based on a random set of initial counter-measures considering the 16 security controls categories shown in Table 1. The effectiveness values for each security control of each category can be *High*, *Medium* or *Low*. This initial set of counter-measures makes up the initial population that is put under the processes of evolution of the algorithm (Section 3.3.3).

Table 3 shows the variables of the algorithm that are susceptible to change, depending on the operation of the risk analysis module, the configuration of attributes in the resource store and the tuning of parameters for the counter-measures module. The last column (Experimental values) shows common values that we have used in this set of experiments (determined after a number of preliminary tests), offering a good approximation to the average behavior of the algorithm. The best candidate solution for a specific use case is shown in Section 5.1 where a real situation is described and our proposal determines a set of countermeasures with an

[1] http://watchmaker.uncommons.org/.

Please cite this article in press as: D. Díaz-López, et al., Dynamic counter-measures for risk-based access control systems: An evolutive approach, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.10.012

**Table 3**
Description, range of values and experimental values for each parameter used in the experiments.

| Parameter | Description | Range of values | Experimental values |
|---|---|---|---|
| $E(\mathcal{A})$ | Current effectiveness | [0.2, 5] | $E(\mathcal{A}) = 2$ |
| $N$ | Population size | $\mathbb{N}$ | $N = 200$ |
| $r^{max}$ | Maximum number of counter-measures $cm_j^i$ per counter-measures set $\overline{CM}_i$ | $\mathbb{N}$ | $r^{max} = 1$ |
| $RL$ | Measured risk level value | [1, 10] | $RL = \{1, \ldots, 10\}$ |
| $\mathcal{T}$ | Threat | {Denegation of service, Unauthorized access, Eavesdropping, Manipulation of records, Information loss, Privileges escalation, System failure and malicious code} | $\mathcal{T}$ = Unauthorized access |
| $\mathcal{A}$ | Asset | {Information, Software} | $\mathcal{A}$ = File repository (Software) |
| $CL$ | Computational load | {Low, Normal, High} | $CL$ =Normal |
| $\widehat{RL}$ | Acceptable risk | [1, 10] | $RL = \{1, \ldots, 10\}$ |
| | Selection method | {Roulette wheel selection, Stochastic universal sampling, Rank selection, Sigma scaling, Truncation selection} | Roulette wheel selection |
| $w_{TAC}$, $w_{CLS}$, $w_{TTC}$, $w_{ARS}$ | Fitness function weights | [0, 1] | $w_{TAC} = 0.1$, $w_{CLS} = 0.1$, $w_{TTC} = 0.1$, $w_{ARS} = 0.7$ |
| $w_H$, $w_M$, $w_L$ | Weights of effectiveness for candidate effectiveness calculation $E_{CM_i}$ | [0, 1] | $w_H = 0.5$, $w_M = 0.3$, $w_L = 0.2$ |
| | Stop condition (stagnation after a number of generations) | $\mathbb{N}$ | 500 |

effectiveness aligned to the acceptable risk. On the other hand, Section 5.2 includes the results in terms of effectiveness $E_{CM_{Best}}$ and fitness $F(\overline{CM}_{Best}, RL_k)$ for the best solutions found when varying the measured risk level.

### 5.1. Use case experiment

A common use case of the previous experiments can imply the existence of a software resource (e.g. file repository) belonging to a corporative network, where there is also an access control system (like the one described in Fig. 2) monitoring the network environment and managing counter-measures to protect such resource. After a scanning period, the risk analysis module finds out that there is an attempt to connect to the file server with the same user credentials from two different distant locations, which is not so reasonable. Moreover, a number of dictionary attacks have been registered over the authentication module of the file server and one new vulnerability has been discovered over the encryption engine which would affect the strength of the encryption algorithm defined for the communication between the file server and the clients. Finally, it is known that the file server contains some confidential information that should be treated carefully. Considering these suspicious facts, the risk analysis module defines that there is a non-negligible possibility of "unauthorized access threat" with a measured risk of $RL = 10$ to the file server.

The risk analysis module delivers all this information to the counter-measures module (measured risk value, threat), who checks the resource store about the attributes of the affected file repository and determines that, for this resource, a "normal" computational load is accepted, while the acceptable risk value raises up to $\widehat{RL} = 5$. Then, the counter-measures module processes the inputs, generates a generic set of counter-measures and after an evolutive process finds the best set of counter-measures applicable to reduce the measured risk value to the acceptable value. In case the proposed solution was absent in the organization, the access control system would immediately deny access since the measured risk $RL$ is bigger than the acceptable risk $\widehat{RL}$, and an alert would warn the network administrator about this situation, who should ideally review the conditions that provoked the risk (source of threat, impact, probability of occurrence, etc.) and decide after a time of revision and analysis a set of specific counter-measures to protect the resource.

Using our proposal with an initial population $P$ of $N = 200$ individuals (i.e. sets of counter-measures), after 69 generations in a reasonable time with a fitness of 0.9, the following best set of counter-measures were found: Authentication mechanism ($E = Low$), Encryption techniques ($E = Low$), Attestation techniques ($E = Medium$), Isolation means ($E = Medium$), Input validation strategies ($E = Low$), Change management strategies ($E = Medium$), Monitoring Strategy ($E = Low$), Software execution schema ($E = Medium$), Session Time Assignment ($E = Medium$), Resource Exposure ($E = High$), Alert Mechanism ($E = Medium$), User Advertising Strategy ($E = Low$).

After finding this set of counter-measures, the access control system will recover the access control policies applicable for the resource (i.e. file repository) and will integrate the twelve found counter-measures over them. By doing so, any forthcoming authorization request addressed to the file server can be limited to the fulfillment of a number of security controls with a specific effectiveness value. For example, the access control system will now require the authentication mechanism and encryption technique in use to have a high effectiveness value. The correlation between an effectiveness value and a specific mechanism or technique can be defined by the system administrator. With the fulfillment of the security controls, the protection of the resource according to the acceptable risk values is guaranteed.

### 5.2. Dynamic measured risk level

In order to test the capability of the algorithm to produce solutions (set of counter-measures) with a suitable effectiveness, the measured risk level $RL(\mathcal{A}, \mathcal{T}) \in [1, 10]$ varies while keeping a fixed acceptable risk level $\widehat{RL}(\mathcal{A}, \mathcal{T})$ and then the proposed algorithm is executed in order to find the best candidate solution with best fitness value (see Eq. (9)).

In Fig. 4, the effectiveness $E_{CM_{Best}} \in [0.2, 5]$ of the different best solutions (represented by a single bar) is shown in the primary $y$-axis (left axis) for each variation of acceptable and measured risk level, this latter shown in the $x$-axis. Additionally, the fitness value $F(\overline{CM}_{Best}, RL_k) \in [0, 1]$ of the different best solutions (represented by a single line with markers) is also indicated in the secondary $y$-axis (right axis). With these experiments it is possible to see the variations in the effectiveness for each best solution based on the measured and acceptable risk levels.

Please cite this article in press as: D. Díaz-López, et al., Dynamic counter-measures for risk-based access control systems: An evolutive approach, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.10.012

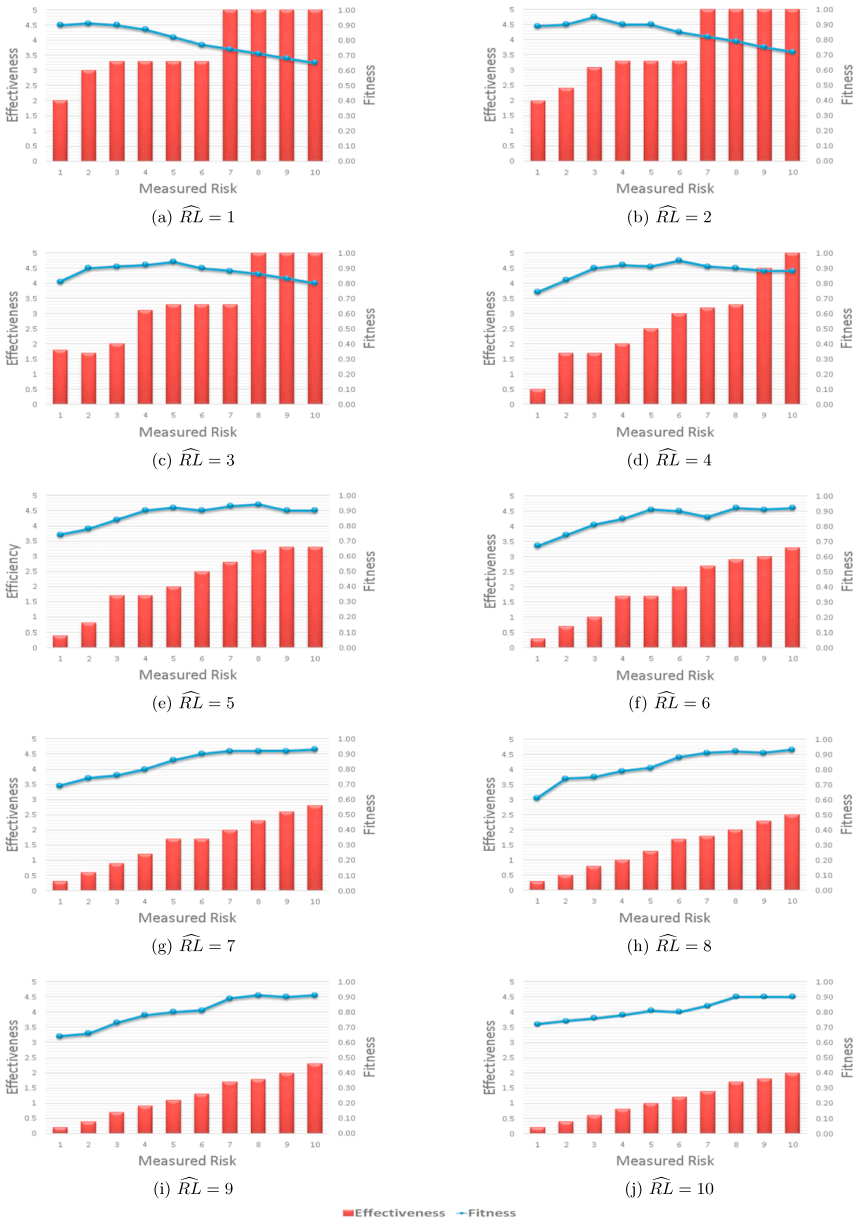


**Fig. 4.** Effectiveness $E_{CM_{Best}}$ and fitness $F(\overline{CM}_{Best}, RL_k)$ for the best solutions found varying measured risk levels $RL$ and acceptable risk levels $\widehat{RL}$.

As it can be observed in Fig. 4, for a situation of fixed acceptable risk level, when the measured risk level $RL(\mathcal{A}, \mathcal{T})$ increases, the value of efficiency of the candidate solution also increases. This phenomenon mainly occurs since, according to Eqs. (1) and (14), in order to reduce a bigger risk level value, a set of counter-measures with a higher effectiveness is needed. On the other hand, for a situation when the acceptable risk level $\widehat{RL}(\mathcal{A}, \mathcal{T})$ increases, the changes in the effectiveness can also be observed in Fig. 4. In this case, when the acceptable risk value increases, i.e., the asset owner is more tolerant with the associated risk for the asset, the effectiveness of the candidate solution decreases for the situation with the same measured risk level. Such behavior takes place

Please cite this article in press as: D. Díaz-López, et al., Dynamic counter-measures for risk-based access control systems: An evolutive approach, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.10.012

mainly due to the fact that less effectiveness is needed to fit the measured risk level within the acceptable risk level.

The behavior observed in these experiments allows the RAdAC system to deliver an accurate solution to protect the asset within an IT system by reducing or increasing the effectiveness of the security controls according to how much the asset owner has decided to expose the asset (acceptable risk level) and according to the risk level that is being measured in that moment. For each variation of both, the measured and the acceptable risk level, our algorithm founds solutions with different fitness values, being better for higher measured risk levels.

## 6. Related work

An approach to risk-based access control system is presented in [20], where privacy considerations for a health information system are taken into account in order to allow or deny the access to an e-health record. The risk of privacy violation is quantified using the concept of Shannon entropy considering the uncertainty associated to different accesses to different kind of information, with different purposes. When the risk exceeds frequently a tolerance threshold, which is computed using a statistical method, it is considered that can occur an over-accessing of patient's information.

Another interesting approach defining a RAdAC is presented in [19], where an attribute-based access control model called UCON (Usage Control Model) is used to simulate a RAdAC system. It proposes the addition of 3 elements to UCON in order to support RAdAC, namely: subject definition, access history and risk evaluation. Likewise, it proposes the extension of RAdAC systems with the following UCON principles: decision continuity and mutability of attributes.

Cloud environments offer a special case of research around security and privacy, and they are one of the fields of application of RAdAc systems, mainly because of the risk for information that need to be managed in order to guarantee customer trust and resilient service. [43,44] specifically make a survey about risk perspectives for cloud environments and describe some challenges that need to be addressed. Also, in [45] an analysis about the applicability of different access control models for a cloud environment is presented, considering factors like the possibility of making decisions aiming to collaborate in an ad hoc manner and adapt access control decisions to support elasticity. From this analysis, a trust-based access control model for the cloud is proposed, which includes users, roles, actions, objects and permissions. An analysis about risks in cloud environments is also presented in [46] which considers business level objectives (BLOs) of the organizations to make decisions about treatment of identified risks.

Furthermore, in [47] a method to combine multiple authentication factors in an online banking system is proposed. That method called QSBAF (Quantified riSk and Benefit adaptive Authentication Factors) considers quantified risk and benefit of access, which are measured according to historical data. Additionally, two methods to combine factors are presented, one using fuzzy logic and another using risk mitigation approach.

In [48], a self-adaptive authorization framework (SAAF) for RBAC/ABAC models is proposed, monitoring user behavior and proposing solutions to endorse or restrict authorization policies based on such behavior. The SAAF framework is composed by the following modules: monitor, analyzer, modeler, planner and effector, which represent a feedback loop. Subject behavior is analyzed similarly as an intrusion detection system does and historic behavior can be stored in a usage statistics and policy model. Many candidate solutions can be proposed to face a possible bad user behavior, however each one is evaluated to identify its implementation costs and the cost of doing nothing. Later, authors of [49] propose a system based on SAAF to manage access control autonomically using a feedback loop to identify and respond to insider threats. This paper is not focus on how to detect threats but on the use of models, model transformation and model verification to guarantee that adaptations are valid.

One method to do risk management based on dynamic trust and risk is shown in [10]. The trust value depends on the trustee behavior and trustor propensity, meanwhile the risk value depends on the threat likelihood and the disclosure impact, and both of them are calculated using a point-based system. If the estimated value of trust is bigger than the risk one, the access to the requested resource should be granted.

Additionally, a risk-based access control system is proposed in [50]. That paper introduces the concept of quantified risk-adaptive access control, which defines multiple authorization decisions according to the quantified risk. The quantified risk depends on the probability of damage and the value of damage. The risk value depends on the value of information (depending on the specific organization) and the probability of unauthorized disclosure, for which it considers two cases: disclosure by temptation and by inadvertence.

Finally, in [51] authors proposed a protocol called OoT (Obligation of Trust) to dynamically exchange obligations related to privacy between two peers. That method uses two elements: NOB (Notification of Obligations), which states privacy requirements, and SAO (Acceptance of Obligations), which states committed obligations. However, this method does not consider dynamic changes in NOB or SAO elements, as a function of the transaction conditions. The reason for such behavior is that a risk analysis about disclosure of PII (Personal Information) is done at the beginning, bearing in mind SLA (Service Level Agreements) or BLA (Business Level Agreements) and it keeps static during all the time.

Upon analysis of some of the most relevant works found in the literature within this field and topic, our proposal in the paper at hand integrates many aspects considered previously, like the evaluation of multiple variables to make decisions and the inclusions of levels of hardiness for some controls (e.g. multiple authentication factors). Yet, our proposal also incorporates new aspects like the evolutive computation approach brought by genetic algorithms offering a new perspective about the resolution of this kind of problems and bringing benefits in terms of applicability to many technologies, adaptation to different authorization situations and responsiveness according to business needs.

## 7. Conclusions and future work

The proposed method in the paper at hand, allow us to, based on genetic algorithms, effectively generate sets of customizable counter-measures taking into account factors (attributes) relevant for a kind of asset and for a specific risk level, in a context where the assets access needs to be controlled. Additionally, the proposed steps defined in the method to select the best individuals are flexible enough to include different instantiations and implementations. For example, it is possible to include different variables in the evaluation of a set of counter-measures for the fitness function, new crossover and mutation operations and different selection methods.

Furthermore, considering a set of threats and security controls, and the capacity of the proposed method to generate best candidate solutions in acceptable times, this method also allows to react to concurrent risk situations that represent variations of the risk level avoiding delays in responses aiming to protect assets and avoiding manual intervention. That is to say, when a resource is labeled in a risk level the system can apply the proposed set of counter-measures to protect the resource automatically. Additionally, the system administrator may also add new sets

Please cite this article in press as: D. Díaz-López, et al., Dynamic counter-measures for risk-based access control systems: An evolutive approach, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.10.012

of generic counter-measures which will be used by the genetic algorithm to update access policies, making this proposed method scalable. The possibility of resolving a multi-variable problem in an acceptable time makes the genetic algorithms to become a valid and effective approximation for a risk changing environment.

In terms of asset protection, the instantiation of the proposed method illustrated in Section 4 and specifically the fitness function depicted in Section 4.3.3 guarantees that the set of counter-measures that were found through the execution of the algorithm will protect the asset fairly without denying access. This feature is the key to achieve a risk management like the one defined in the ISO/IEC 27005 [11] standard, aiming to guarantee that a set of specially configured security controls are applied during the manipulation of an asset in order to avoid the probability that an unacceptable risk get materialized. Additionally, a proper risk management together with the application of a set of counter-measures brings not just advantages in terms of protection of resources, but also in the management of privileges done by an access control system.

According to experiments illustrated in Section 5 the proposed method has the ability to adapt the effectiveness of security controls to face variations in the measured risk level. This feature allows adaptation to dynamic and variable environments and brings proper protection to assets.

Regarding future research directions, there are actually several possibilities to extend the work presented in this paper. One alternative could include the implementation of different instantiations of the proposal making evaluation of additional variables coming from the risk analysis module and increasing the data to select the best candidate solution, even if additional variables also introduce complexity in the functions used along the evolutive process.

Furthermore, it would be useful to consider managing different risk scales for each threat according to its impact, which would allow a higher granularity for some specific threats that can be more critical for the objective business and that must be considered more precisely. A validation of the results obtained from the application of the found counter-measures which can be used by the counter-measures module to determine future decisions as a feedback from the authorization context can also provide a useful contribution to improve the accuracy of the proposed model.

## Acknowledgment

This work has been partially supported by the Funding Program for Research Groups of Excellence granted by the Séneca Foundation with code 04552/GERM/06.

## References

[1] J. Qian, S. Hinrichs, K. Nahrstedt, Acla: A framework for access control list (acl) analysis and optimization, in: R. Steinmetz, J. Dittman, M. Steinebach (Eds.), Communications and Multimedia Security Issues of the New Century, in: IFIP The International Federation for Information Processing, vol. 64, Springer US, 2001, pp. 197–211.
[2] A. Liu, E. Torng, C. Meiners, Compressing network access control lists, IEEE Trans. Parallel Distrib. Syst. 22 (12) (2011) 1969–1977.
[3] S.D. Stoller, P. Yang, M.I. Gofman, C. Ramakrishnan, Symbolic reachability analysis for parameterized administrative role-based access control, in: Access Control Methods and Technologies, Comput. Security 30 (23) (2011) 148–164. (special issue).
[4] Y. Jung, J.B. Joshi, Cribac: Community-centric role interaction based access control model, Comput. Security 31 (4) (2012) 497–523.
[5] Q. Zhang, Y. Mu, M. Zhang, Attribute-based authentication for multi-agent systems with dynamic groups, in: Computer Communications on Information and Future Communication Security, Computer Commun. 34 (3) (2011) 436–446. (special issue).
[6] B. Cha, J. Seo, J. Kim, Design of attribute-based access control in cloud computing environment, in: K.J. Kim, S.J. Ahn (Eds.), Proceedings of the International Conference on IT Convergence and Security 2011, in: Lecture Notes in Electrical Engineering, vol. 120, Springer Netherlands, Suwon, Korea, 2012, pp. 41–50.
[7] P. Kodeswaran, S.B. Kodeswaran, A. Joshi, T. Finin, Enforcing security in semantics driven policy based networks, Computer Standards and Interfaces, Special Issue: Secure Semantic Web 33 (1) (2011) 2–12.
[8] D. Huang, W.-T. Tsai, Y.-h. Tseng, Policy management for secure data access control in vehicular networks, J. Netw. Syst. Manage. 19 (2011) 448–471.
[9] Q. Ni, E. Bertino, J. Lobo, Risk-based access control systems built on fuzzy inferences, in: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ACM, 2010, pp. 250–260.
[10] R.A. Shaikh, K. Adi, L. Logrippo, Dynamic risk-based decision methods for access control systems, Computers & Security 31 (4) (2012) 447–464.
[11] ISO/IEC 27005 Information technology - Security techiques - Information security risk management, International Standard, edition 2 (June 2008).
[12] J. Hintzbergen, K. Hintzbergen, A. Smulders, Foundations of Information Security: Based on ISO27001 and ISO27002, Best practice, Bernan Assoc, 2010.
[13] A. Calder, S. Watkins, IT Governance: An International Guide to Data Security and ISO27001/ISO27002, ITPro collection, Kogan Page, 2012.
[14] ISO/IEC 27001 Information technology - Security techiques - Information security management systems - Requirements, International Standard, edition 2 (October 2013).
[15] D.D. López, G.D. Tormo, F.G. Mármol, J.M.A. Calero, G.M. Pérez, Live digital, remember digital: State of the art and research challenges, Comput. Electr. Eng. 40 (1) (2014) 109–120. 40th-year commemorative issue.
[16] T. Sakuraba, K. Sakurai, Proposal of the hierarchical file server groups for implementing mandatory access control, in: Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS, Palermo, Italy, pp. 639–644.
[17] J. Zhang, J. Yao, K. Huang, Research on access control policy for confidential information system, Appl. Mech. Material. 263 (2012) 3064–3067.
[18] R.W. McGraw, Risk-adaptable access control (radac), in: Privilege (Access) Management Workshop, NIST-National Institute of Standards and Technology-Information Technology Laboratory, NIST, 2009, gaithersburg, Maryland, USA.
[19] S. Kandala, R. Sandhu, V. Bhamidipati, An attribute based framework for risk-adaptive access control models, in: Sixth International Conference on Availability, Reliability and Security, ARES, 2011, pp. 236–241, Vienna, Austria.
[20] Q. Wang, H. Jin, Quantified risk-adaptive access control for patient privacy protection in health information systems, in: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS '11, ACM, 2011, pp. 406–410.
[21] M.E. Orwat, A decision framework for enhancing mobile ad hoc network stability and security, (Ph.d. thesis), Naval Postgraduate School Monterey CA, 2008, June.
[22] R.A. Shaikh, K. Adi, L. Logrippo, Dynamic risk-based decision methods for access control systems, Comput. Security 31 (4) (2012) 447–464.
[23] M. Sharma, Y. Bai, S. Chung, L. Dai, Using risk in access control for cloud-assisted ehealth, in: 14th IEEE International Conference on High Performance Computing and Communication & 9th International Conference on Embedded Software and Systems, HPCC-ICESS, IEEE, Liverpool, United Kingdom, 2012, pp. 1047–1052.
[24] L. Chen, J. Crampton, M. Kollingbaum, T. Norman, Obligations in risk-aware access control, in: 10th Annual International Conference on Privacy, Security and Trust (PST), IEEE, Paris, France, 2012, pp. 145–152.
[25] K. De Jong, Evolutionary computation: A unified approach, in: Proceedings of the 14th Annual Conference Companion on Genetic and Evolutionary Computation, GECCO '12, ACM, 2012, pp. 737–750.
[26] P. Guo, X. Wang, Y. Han, The enhanced genetic algorithms for the optimization design, in: Biomedical Engineering and Informatics, BMEI, 2010 3rd International Conference on, vol. 7, 2010, pp. 2990–2994.
[27] Extensible access control markup language (XACML) version 3.0, OASIS Standard (January 2013).
[28] S. Pina Ros, M. Lischka, F. Gómez Mármol, Graph-based xacml evaluation, in: Proceedings of the 17th ACM Symposium on Access Control Models and Technologies, SACMAT '12, ACM, New York, NY, USA, 2012, pp. 83–92.
[29] K.M. Kavanagh, M. Nicolett, J. Pescatore, Marketscope for vulnerability assessment, Gartner RAS Core Research Note G 156038.
[30] Product Guide, McAfee Risk Advisor 2.7 Software, https://kb.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/23000/PD23685/en_US/MRA_2.7.0_Product_Guide_en-us.pdf, Accessed: April 2014 (2012).
[31] E. Alba, B. Dorronsoro, Cellular Genetic Algorithms, in: Operations Research/Computer Science Interfaces Series; ORCS 42, vol. 42, Springer, London, Limited, 2008.
[32] A. Moraglio, S. Silva, K. Krawiec, P. Machado, C. Cotta (Eds.), 15th European Conference on Genetic Programming, EuroGP, in: Lecture Notes in Computer Science, vol. 7244, Springer, Malaga, Spain, 2012.
[33] M. Agrawal, P. Mishra, A comparative survey on symmetric key encryption techniques, Int. J. Comput. Sci. Eng. 4 (5) (2012) 877–882.
[34] S.U. Rehman, M. Bilal, B. Ahmad, K.M. Yahya, A. Ullah, O.U. Rehman, Comparison based analysis of different cryptographic and encryption techniques using message authentication code (mac) in wireless sensor networks (wsn), Int. J. Comput. Sci. Issues (IJCSI) 9 (1) (2012) 96–101.
[35] K. Floyd, J.P. Whelan, A.W. Meyers, Use of warning messages to modify gambling beliefs and behavior in a laboratory investigation, Psychol. Addictive Behaviors 20 (1) (2006) 69–74.

Please cite this article in press as: D. Díaz-López, et al., Dynamic counter-measures for risk-based access control systems: An evolutive approach, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.10.012

[36] F.-F. Cheng, C.-S. Wu, Debiasing the framing effect: The effect of warning and involvement, Decis. Support Syst. 49 (3) (2010) 328–334.
[37] S. Ismail, M. Ngadi, New security authentication mechanisms in grid computing web environment, in: International Conference on Research and Innovation in Information Systems, ICRIIS, Kuala Lumpur, Malaysia, 2011, pp. 1–4.
[38] R. Hasan, R. Khan, Interaction provenance model for unified authentication factors in service oriented computing, in: Proceedings of the 4th ACM Conference on Data and Application Security and Privacy, CODASPY '14, ACM, New York, NY, USA, 2014, pp. 127–130.
[39] D. Thorleuchter, D.V. den Poel, Improved multilevel security with latent semantic indexing, Expert Syst. Appl. 39 (18) (2012) 13462–13471.
[40] K. Tang, T. Chan, R. Yin, K. Man, Multiobjective Optimization Methodology: A Jumping Gene Approach, in: Industrial Electronic Series, CRC Press INC, 2012.
[41] A. Hopgood, Intelligent Systems for Engineers and Scientists, third ed., CRC Press, ISBN: 9781466516175, 2012.
[42] ISO/IEC 27033-3 Information technology - Security techniques - Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues, ISO Standard (December 2010).
[43] A.N. Khan, M.M. Kiah, S.U. Khan, S.A. Madani, Towards secure mobile cloud computing: A survey, Future Gener. Comput. Syst. 29 (5) (2013) 1278–1299. special section: Hybrid Cloud Computing. http://www.sciencedirect.com/science/article/pii/S0167739X12001598.
[44] J. Arshad, P. Townend, J. Xu, A novel intrusion severity analysis approach for clouds, Future Gener. Comput. Syst. 29 (1) (2013) 416–428. including Special section: AIRCC-NetCoM 2009 and Special section: Clouds and Service-Oriented Architectures. http://www.sciencedirect.com/science/article/pii/S0167739X11001488.
[45] I. Ray, I. Ray, Trust-based access control for secure cloud computing, in: K.J. Han, B.-Y. Choi, S. Song (Eds.), High Performance Cloud Auditing and Applications, Springer, New York, 2014, pp. 189–213.
[46] J.O. Fito, J. Guitart, Business-driven management of infrastructure-level risks in cloud providers, Future Gener. Comput. Syst. 32 (0) (2014) 41–53. special Section: The Management of Cloud Systems. http://www.sciencedirect.com/science/article/pii/S0167739X12001045.
[47] W. Han, C. Sun, C. Shen, C. Lei, S. Shen, Dynamic combination of authentication factors based on quantified risk and benefit, Security Commun. Netw. 7 (2) (2014) 385–396.
[48] C. Bailey, D. Chadwick, R. de Lemos, Self-adaptive authorization framework for policy based rbac/abac models, in: IEEE 9th International Conference on Dependable, Autonomic and Secure Computing, DASC, Sydney, Australia, 2011, pp. 37–44.
[49] C. Bailey, L. Montrieux, R. de Lemos, Y. Yu, M. Wermelinger, Run-time generation, transformation, and verification of access control models for self-protection, in: SEAMS'14: 9th International Symposium on Software Engineering for Adaptive and Self-Managing Systems, ACM, ACM, Hyderabad, India, 2014.
[50] P. Cheng, P. Rohatgi, C. Keser, P. Karger, G. Wagner, A. Reninger, Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control, in: IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2007, pp. 222–230.
[51] U.M. Mbanaso, G. Cooper, D. Chadwick, A. Anderson, Obligations of trust for privacy and confidentiality in distributed transactions, Internet Res. 19 (2) (2009) 153–173.

**Daniel Díaz López** is a Ph.D. student in computer engineering from the University of Murcia. His research interests include systems for management and federation of identity, security in cloud computing, privacy and anonymity. At the time of writing this paper he was a student research assistant in the security group at NEC Laboratories Europe, Heidelberg, Germany. He received an M.Sc. in computer engineering from the University of Murcia.

**Ginés Dólera Tormo** is a researcher in the Department of Information and Communications Engineering of the University of Murcia. His research interests include authorization, authentication and identity management, user-centric technologies and trust management. He received an M.Sc. and Ph.D. in computer engineering from the University of Murcia, Spain.

**Félix Gómez Mármol** is a senior research scientist in the security group at NEC Laboratories Europe, Heidelberg, Germany. His research interests include authorization, authentication and trust management in distributed and heterogeneous systems, security management in mobile devices and design and implementation of security solutions for mobile and heterogeneous environments. He received an M.Sc. and Ph.D. in computer engineering from the University of Murcia.

**Gregorio Martínez Pérez** is an associate professor in the Department of Information and Communications Engineering of the University of Murcia. His research interests include security, privacy and management of IP-based communication networks. He received an M.Sc. and Ph.D. in computer engineering from the University of Murcia.

Please cite this article in press as: D. Díaz-López, et al., Dynamic counter-measures for risk-based access control systems: An evolutive approach, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.10.012

# 3

# Live digital, remember digital: State of the art and research challenges

| | |
|---|---|
| **Title**: | Live digital, remember digital: State of the art and research challenges |
| **Authors**: | Daniel Díaz-López, Ginés Dólera-Tormo, Félix Gómez-Mármol, Jose M. Alcaraz-Calero, Gregorio Martínez-Pérez |
| **Type**: | Journal |
| **Journal**: | Computers & Electrical Engineering |
| **Impact factor (2014)**: | 0.817 |
| **Publisher**: | Elsevier |
| **Volume**: | 40 |
| **Number**: | 1 |
| **Pages**: | 109-120 |
| **Year**: | 2014 |
| **Month**: | January |
| **DOI**: | http://dx.doi.org/10.1016/j.compeleceng.2013.11.008 |
| **State**: | Published |

Table 3: Live digital, remember digital: State of the art and research challenges

Computers and Electrical Engineering 40 (2014) 109–120

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

# Live digital, remember digital: State of the art and research challenges ☆

Daniel Díaz López [a], Ginés Dólera Tormo [b], Félix Gómez Mármol [b], Jose M. Alcaraz Calero [c], Gregorio Martínez Pérez [a,*]

[a] Departamento de Ingeniería de la Información y las Comunicaciones, Universidad de Murcia, 30100 Murcia, Spain
[b] NEC Laboratories Europe, Kurfürsten Anlage 36, 69115 Heidelberg, Germany
[c] University of the West of Scotland, School of Computing, Paisley PA1 2BE, Glasgow, United Kingdom

ARTICLE INFO

*Article history:*
Available online 11 December 2013

ABSTRACT

The so called trend "live digital, remember digital" is acquiring higher relevance within the international research community, due to its several appealing challenges in a multitude of different fields within the Information and Communication Technologies. Today, many people live daily connected to the Internet through their mobile phones, laptops, tablets, etc. and the need to audit or log every single digital interaction emerges in many environments. By seamlessly recording those digital interactions and storing them in a privacy-preserving fashion, a number of benefits are brought to end users, like the provision of user-tailored services, amongst many others. In this paper we will particularly focus on the study of the security and privacy challenges within this field, as well as on the analysis of the currently existing solutions addressing these issues and we will propose an architecture for the so called live digital systems.



## 1. Introduction

Our interaction with computational systems has changed our lives. Nowadays, this interaction is defining a new concept in the human–computer interactive (HCI) experience [1]. This experience is influenced by the user interfaces which increasingly try to be more responsive and proactive, but also simple and effective. These systems are being developed as a result of an understanding of our needs and social behavior. This trend helps to define the concept of digital life in which almost everybody is, to some extent, involved nowadays. Simple questions can help us to note how digital our lives are: How many different websites do we visit per day? How many different applications do we use? How many electronic documents do we handle? How many e-mails do we send and receive? How many phone calls do we make? What information do we provide to whom?

This fact is even bigger considering the advent of the Internet of Things (IoT) [2]. We have a bunch of technologies (IMS [3], RFID [4], NFC [5], UWB [6,7] , ZigBee [8], PLC [9], etc.), data warehouses (decision support systems, knowledge based system, context management frameworks, business information systems, etc.) and services (online collaboration, online office, platforms, outsource processes, etc.) converging all around a future internet architecture [10,11]. This architecture allows interoperability, cloud computing access, mobility support, identity management, smart routing and discovery of services, amongst other features. This new trend takes the HCI experience to another level where the computing is more ubiquitous

☆ Reviews processed and approved for publication by Editor-in-Chief Dr. Manu Malek.

* Corresponding author. Tel.: +34 868 887646; fax: +34 868 884151.
*E-mail addresses:* danielorlando.diaz@um.es (D. Díaz López), gines.dolera@neclab.eu (G. Dólera Tormo), felix.gomez-marmol@neclab.eu (F. Gómez Mármol), JoseMaria.AlcarazCalero@uws.ac.uk (J.M. Alcaraz Calero), gregorio@um.es (G. Martínez Pérez).

0045-7906/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.compeleceng.2013.11.008

and pervasive. In the IoT, it is possible to imagine new interactions in our digital life, for instance through sensors able to capture data, transfer events and connect to the network with high degree of autonomy and interoperability.

The greater our digital experience is, the greater the amount of information we generate is distributed and stored along different computer systems. All these data make the end users to become the big source of his own digital information. Furthermore, when the information is related to the users' lifes, it entails new challenges that need to be addressed to open a myriad of new chances and markets in the data industry. A first overview about digital records and digital memory can give us some ideas of opportunities: increase the productivity at work by reducing the time to find required data, provide a way to proof what we did and consequently what we did not, assist elderly people to exercise their memory, maintain a complete and accurate medical record to improve early disease detection and treatment, easily share any of the digital information with relatives and friends, obtain user-tailored services by sharing (part of) our life logs with service providers, etc.

But to achieve this data industry, the most challenging aspect to be covered in this novel market is most likely the security and privacy required due to the nature of the information managed. Challenges ranging from the design of novel privacy and security technologies to enable smart and selective sharing of confidential information, novel data-centric encryption methods to new federated identification schemes, and novel access control systems, along another multitude of novel security and privacy principles. This paper identifies the set of problem statements and challenges associated to the ambitious project of gathering, storing, processing, indexing and visualizing this emerging concept of live digital/remember digital.

In order to better introduce these challenges to the reader, we have laid out this paper as follows. In Section 2, we introduce the scarce related works in the field to better emphasize the opportunity of this kind of solutions. We identify the different steps involved in the design of live digital/remember digital solutions in Section 3. The challenges associated to this kind of applications are identified in Section 4. Then, we describe our proposed architecture for live digital/remember digital solutions in Section 5. A real use case is introduced in Section 6. Finally, Section 7 concludes with some remarks and future research directions.

## 2. Related works

There is a clear lack of current approaches to address live digital/remember digital solutions. However, this section enumerates and analyzes the more representative projects or initiatives related to the management of personal information, in order to select a set of common characteristics.

### 2.1. MyLifeBits

MyLifeBits [12] is a research project from Microsoft intended to capture everything that is seen and heard (i.e. conversations, meetings, etc.) by a user. It includes sensors reading, health monitors and computer activity as additional features. This project allows organizing, searching, annotating and utilizing contents. It integrates a full-text search and allows the user to rate and make text and audio annotations (voice and text annotation tool) over each item. In terms of the project, it is estimated that it is necessary 1 Gb per month to store all the gathered information from a user, without taking the video into account. The database holds and links the information using metadata.

The scope of the project includes gathering what it is happening inside the desktop through different capture tools, such as an outlook interface, an IM (instant messaging) capture, a browser tool, a screen saver and an activity log, and also what happens outside the desktop as source of information, through capture tools, such as images capture devices (SenseCam [13]), radio capture, TV capture and telephone capture tools.

MyLifeBits offers an integrated view of the user information along the time through a GUI called MyLifeBits shell, which shows information as a list, thumbnails, and timeline. The items can be automatically linked using the time or the geographic proximity as parameter, or also explicitly linked. They are stored using a DAG (Directed Acyclic Graph) [14], instead of the traditional hierarchical way.

Even though MyLifeBits presents noticeable advantages, it presents some shortcomings regarding the collection and organization of the data. Its database does not have a structured permission list over the information, and it is assumed that all the information belonged to one user without possibilities to share part of the information with somebody else. Even if there are different capturing tools, the process of gathering and delivering are done by the same system. In other words, there is not option to choose another application. The capturing tools are designed to record everything, even if the information has a classification of confidential, restricted, internal use or public; equally, there is no control over information leak, and all the capture tools feed directly the database.

### 2.2. Yahoo, Google and Copernic Desktop Search

Many companies had the initiative to create a product to organize all user information inside the desktop, allowing the user to search over it anytime in a fast way [15,16]. Mentioning the most relevant, Yahoo [17], Google [18] and Copernic [19] developed a Desktop Search application, which allows resolving queries about emails, contacts, documents, music, pictures, HTML documents and compressed files using parameters like name, type, date/time, size or path.

The search involved in the query resolution process is done through an information indexing process which includes internal and external storage devices, like USB/Firewire devices. The indexation can additionally be set by file type, email client and contacts. Once an item is found after performing the search process, the application gives the option of accessing such item through a viewer or a player integrated into the application. Additionally it is possible to make some operations over the found files, such as open, delete or rename. These applications support searching within the files and in the case of Copernic (Up to version 3.0) and Google, it is also possible to search across network shares.

### 2.3. Locate32

A personal initiative to craft a Desktop Search Tool for files in a directory structure is Locate32 [20]. This tool has been popular for a decade and despite it does not allow to search inside files, it can be set to search in local repositories and network shares. It is based on one or multiple databases which index all the file information of specific drives and directories, and these databases are updated manually or based on a scheduled routine. Locate32 also allows many operations over the found items, which include the presets operations defined by Windows Explorer and some operations owned by the application. Locate32 holds a freeware license with an open source code.

### 2.4. E-Model

E-Model [21] is a research initiative focused on a new way of storing and searching personal information based on RDAG (Relational Direct Acyclic Graph). This model proposes the use of three types of objects: e-node, c-data and timestamp. E-node is used to represent an event, c-data is used to represent the name (e.g.: Location) and the value (e.g.: 25.799891, −80.223816) of a unique variable associated to the event, and timestamp is used to register the time (e.g.: Sun Dec 02 2012 09:14:00 GMT-0500 Eastern Standard Time) when the event was created. The main advantage of using a RDAG is that a graph allows object inheritance, abstraction and multiple relations between objects, which are features not available using a relational model.

The E-Model prototype was tested in a case study which includes the capture of information from different sensors: camera auto-triggered by sensors (ViconRevue), wearable camera (GoPro), smartphone (iPhone) and GPS (Garmin), along 109 days of Life Logging [22]. The GUI is composed of a Graph Explorer which allows the user to search a specific event (setting the number of nodes to search and the search depth) and see all the connected events. The GUI also offers a Spatio-Temporal event viewer which relates and shows different types of information (GPS tracks and pictures). Additionally, it allows the integration of structured (e.g.: email) and unstructured data (e.g.: pictures) to show the relations of these throughout time.

### 2.5. Comparison

As shown in Table 1, the analyzed Desktop Search Tools make an intensive search of any kind of files from the PC local disk, and additionally, in the case of Google and Yahoo, from the mail and IM services delivered for each service provider. On the other hand, MyLifeBits project is composed of a set of capture tools connected to a central MyLifeBits database, and amongst these tools one is focused on getting information of data from the NTFS files system, another one makes MSN IM capturing and another makes email capturing for Outlook and legacy email client. We can say that in some way the MyLifeBits project scope is wider than Desktop Search Tools because by means of an email client, it is possible to capture any email information independent of the email service provider, as is the case of Google and Yahoo. Even if MyLifeBits project has a wider scope, we can observe that it does not have possibilities to include information from shared networks in its database as it happens with Copernic, Locate32 and Google Desktop Search Tools.

Additionally, a main difference between these solutions resides in the way the data processing is done, evolving from a relational model where the user data are indexed and stored in a database, towards a graph-based model where the element unit is the "event" and it is related to other events according to data-features relations (e.g. location, name, timestamp, etc). This gap in the processing way is evident since the Desktop Search Tools do not make a linking process between gathered items, so every item is presented in an individual way without showing relations of any kind, whereas MyLifeBits and E-Model do make a process of association and linking of information based on time or geographic proximity which grants the user the possibility to see a special and useful presentation about related information. The linking between information is mainly supported by relations in a graph, which depends on the captured information.

## 3. Main steps in live digital

Once we have analyzed the main approaches in the literature with regards to live digital/remember digital solutions, this section presents some common steps extracted from them, as depicted in Fig. 1. Each one of these steps faces a number of important research challenges, as we will see in Section 4.

**Table 1**
Comparison between personal information management tools.

| | Desktop Search Tools | | | | MyLifeBits project | E-Model |
|---|---|---|---|---|---|---|
| | Copernic | Locate32 | Google | Yahoo | | |
| Search within files | Yes | No | Yes | Yes | Yes | Yes |
| Work across network shares | Until Copernic 3.0 | Yes | Yes | No | No | No |
| Sources of personal information | File system | File system | File system, web history | File system | File system Capture tools: Telephone, TV, IM Radio, Outlook, browser, GPS, Auto-triggered camera (SenseCam) | File System Capture; tools: Auto-triggered camera (ViconRevue), wearable camera (GoPro), iPhone, Garmin GPS |
| | | | Google services (mail, IM) | Yahoo services (mail, IM) | | |
| Processes over information and storage | Indexation (Customizable) and storage in a relational structure | Indexation and (Customizable) storage in one and storage in or many a relational structures | Indexation and storage in a relational structure | Indexation (Customizable) and storage in a relational structure | Association-linking of events using a DAG (Directed Acyclic Graph) based model | Association-Linking of events using RDAG Directed Acyclic Graph) based model |
| Processes over results | Sort and group | Sort and group | Sort and group | Save searches, preview | Sort and group | Sort and group |
| | | | | | Text and voice annotations, downloads<br>Relation of events according to time and location | Relation of events accord ing to time and location |
| Running | Continuously | Manual starting | Continuously | Continuously | Continuously | Manual starting |
| Scope | Search and list | Search and list | Search and list | Search and list | Collection, storing, holding, linking, searching and listing | Collection, storing, holding, linking, searching and listing |
| Project status | Up<br>Version 3.5 | Up<br>Version 3.1 | Discontinued (September 2011) | Discontinued<br>New commercial version is XI | Current | Current |

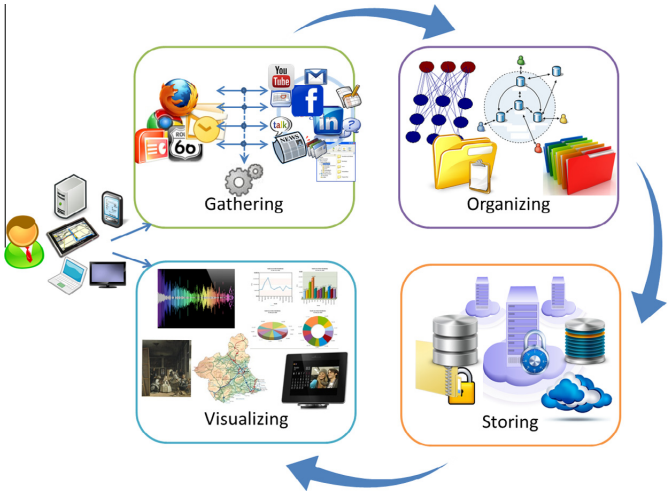


**Fig. 1.** Main steps in live digital: (i) gathering, (ii) organizing, (iii) storing and (iv) visualizing.

### *3.1. Gathering*

As a first step, any live digital solution needs to collect details of the user interactions (or events, in this context) with the digital world. While the user is interacting with different services, both local applications and external services, such as browsing the Internet, reading e-mails or using desktop or mobile applications, an application in the background should be gathering, isolating and analyzing information regarding such interactions. The information to be collected comprises: the kind of interaction, the date, the name and additional meta-information, among others. The idea is to relate each event with others and to allow smart searches. To facilitate and enrich the user experience, this information must be gathered seamlessly and automatically, although the user could guide the process. For example, she could mark certain accesses as important or avoid gathering irrelevant events. Furthermore, the application could learn the users' preferences automatically and adapt its behavior to them.

### *3.2. Organizing*

The live digital/remember digital application has to process and index the collected information from different interactions, so it could establish the relationships that the different interactions have with each other and also with a specific topic, set of keywords, or date. Additionally, since the information should be encrypted in order to preserve the user's (data owner's) privacy, some advanced cryptographic techniques have to be designed allowing establishing those relations even without revealing the content of the private information.

### *3.3. Storing*

Once the information of the user's interactions has been collected, it needs to be securely stored to be accessible in the future, even from multiple different devices. For example, users may access from their mobile phone to events that occurred in their personal computer and vice-versa. Furthermore, since this kind of tools are aimed to allow the user getting information of past interactions, the solution would be very limited if the user should store locally such information. Hence, this information may be securely stored in an external server, allowing users accessing it from any of their devices. Furthermore, the information could be stored in a distributed way so it does not belong to one unique server but to a complete "clouds constellation". The information to be stored is private and hence the application has to encrypt such information before uploading it to the server, ensuring this information could not be read either by the server or by any other party, except for the actual owner of such data.

### *3.4. Browsing and visualizing*

Finally, users want to recover details of a set of interactions which happened in the past. They may not remember all the details of their interactions, especially if these happened long time ago. Therefore, the live digital/remember digital

application has to present a user-friendly interface in such a way that they could request information about their past interactions. This application could also give some advices or hints on how to perform a more accurate query.

## 4. Challenges

Once the main steps that any live digital solution should address have been presented, this section remarks the common features to take into account, which in turn may be considered as the common challenges identified for this scenario.

- *Recall "WWW"*: Users should have the possibility to recall whatever (W) interaction they have performed online, wherever (W) and whenever (W) they feel like getting it back. This turns the users' information into a high availability asset which clearly needs to be accessed from an always-connected device.
- *Navigate*: Exploring our own information, allowing grouping of data and executing operations over the returned items should be one of the most requested features. An efficient navigation should provide the users with an easy and intuitive way to browse their well-structured information; hence a big effort in presentation duties to make it flexible and clear has to be done.
- *Search*: Executing user queries with high precision in terms of results that are truly relevant should be a mandatory feature. It is necessary to provide a friendly interface that receives inputs but also be proactive to ease the delivery of what the user is expecting. Additionally, it is important to say that the searching process will be easier if the information is better classified, for example in the case of multi-owner information it can be relevant to allow that each owner designs and shares tags over the data (e.g. photos, videos), which helps to define the type of information and improves the searching/finding process. In [23] authors show an analysis about the use of a tag-based classification in a social bookmarking systems combined with personal interests in order to improve the searching process.
- *Share*: Users should be able to share some of their own information with selected recipients by means of links to friends or relatives' digital lives. This has to be a natural concept because most of the time users make activities where they share space and time with other users and the information is being built for all the participants, so it requires a serious addressing of multi-owner information.
  One initiative developed in this field of access to private data consists of statistical disclosure control techniques, being the most popular the micro-aggregation technique [24,25] which offers simplicity and quality for small data sets, though there are even some proposals suitable for big data [26].
- *Organize*: The user should be able to group/ungroup sets of information according to some common characteristic or details of the data, as when the information shares time or location features. This action can be automatically performed if it is highly supported by the gathered metadata, but it can also be achieved by the users' own initiative and their wish to structure their own information around a personal event (for instance, create a photo album).
- *Filtering*: Taking into account the variety of information sources to collect users' interactions, the amount of data to be managed will be impracticable if it is not properly filtered before it becomes part of the system. The server would require a considerable amount of computational and storage resources and the users would find the system useless if they are overwhelmed even with the most insignificant pieces of information.
- *Audit*: The digital live may have a legal connotation if the user utilizes it to show the execution of specific activities. The confidence in these systems has to be guaranteed to turn them into a real evidence of activities.
- *Visualize*: Presumably, this type of solutions is associated to big data, which in turn requires novel visualization techniques enabling the users to get useful knowledge from the information gathered along their life. In this way, novel visualization techniques on which massive data aggregation is the big deal may be carefully addressed.
- *Access*: The users should be able to have access to any data related to them in order to allow for backing up, modifying or deleting such information. Novel distributed and scalable tracking systems may have to be designed in order to enable a globally tracking of replicated information which is semantically similar.
- *Recovery*: The system may be designed based on disaster recovery as principle. It requires dealing with redundancy, high availability and dependability. Thus, novel redundancy methods may need to be proposed in order to cover big data security and privacy maintenance as a clear requirement.
- *Relations with third-parties*: The users' data gathered and stored in these systems might be in the form of a URI (Universal Resource Identifier) for a resource and not the resource itself, so it will be necessary a cross-site interaction between the architecture client-side, an Identity provider and a resource server, which has to be, as far as possible, transparent for the user but also pursue the disclosure of the minimum user data required for identity authentication [27,28]. A couple of examples of solutions to avoid the disclosure of user data in cross-site interactions are presented in [29,30], respectively.

Even when the previous challenges are related to the essential use cases of live digital/remember digital solutions, probably privacy and security challenges are the most impacting ones due to the personal nature of the data managed therein. Thus, the following security and privacy challenges have been identified as essential for this kind of scenarios.

- *Selective access*: Any person, application or device must have access exclusively to the information granted by the user and only the user may take decisions over such access permissions. This feature imposes the design of novel encryption-aware authorization systems to control the selective access to the encrypted information.

- *Purpose-based exposure*: Any person may be able to determine not only which application, person or device can access to its own data but also for which purposes this access is granted. The gathering of partial information by a third-party with the exclusive purpose to provide personalized services may be a representative example. This feature implies the design of novel purpose-based systems to control the (partial) access to information.
- *Selective gathering*: Only the application that the user selects should make the gathering, process and storage of the information. The user should decide which part of his digital life should be recorded. It requires the design of novel techniques to ensure these policies are enforced correctly.
- *Private storage of data*: The storage should be done in a way that the system cannot use the data for its benefit, i.e. some kind of encryption should be implemented to guarantee that the user data are safe even if they are stored in a remote untrusted server. One example of secure storage for private information (financial data) using additive homomorphic cryptosystems is presented in [31]. Additionally, an analysis about insider threats has to be done in order to mitigate the possibility that a user of the system might access to unauthorized data. In the case of relational data model, there are some methods to identify threats and estimate certain Threats Predictions Value (TPV) which can be used to warn the system to protect the data [32].
- *Private data processing*: Only applications that the user selects should be able to make recovery and analysis of specific information [33]. Notice that applications to collect/process/store data may not be necessarily the same to recover/analyze/deliver data. In fact, IoT is fostering a new architecture in which it is possible to define different capturing systems for different kind of information produced by the same sensors, and likewise it is possible to define a variety of delivering applications for different purposes.
- *Encrypted data retrieval*: Users must be able to search over their data, even if this is encrypted and the query is also encrypted. It requires the design of novel search techniques, probably based on fully homomorphism encryption [34] or other mechanisms for achieving this searching and indexing of encrypted data without any unveiling of private information [35].
- *Transversal security and privacy*: The intrinsic personal connotations of the digital live requires a critical addressing of all the security and privacy aspects associated to the gathering, storing, processing, indexing and visualizing of the information. It requires novel techniques for encryption-based accesses, filtered-based information exchanges and other novel solutions. Moreover, both security and privacy may need to be addressed transversally along all the layers of the physical hardware and software involved. It covers from novel low level encryption-aware distributed file systems to new high level languages for defining self-encrypted queries to be executed over encrypted data. This aspect is quite relevant due to the popularization of ubiquitous elements (e.g. mobile phones, sensors, etc.) which store user data and are prone to be re-sold, re-furbished or exchanged before a process of private data elimination. An example of this phenomenon is shown in [36].
- *Transparency*: The system gets raw information from heterogeneous sources transparently to the user. It requires the design of novel techniques to seamlessly intercept multi-model information to enable the gathering of the live digital of the user.
- *Forensic evidence*: The system implies the design of novel techniques for managing any forensic evidence on the access to the information to be usable on trials. Every single access to the information may be stored in some way in which this evidence is also encrypted to preserve the privacy derived of the analysis of such evidence.
- *Assurance of technological infrastructure*: The threats over services and physical infrastructure must be considered as well, both in the client and the server side. Due to the nature of the presented service, which has to be available for the user in most of the circumstances, the seriousness of the stored user information, and the high interrelationship between information assets in a IT infrastructure (which produces a group vulnerability), it is necessary the implantation of methodologies to evaluate the network and service risks [37–39].
- *Stateless and simple access*: Users interact with the system using different devices, such as personal computers, laptops, and mobile phones, being some of them constrained on resources. The system could not base its functionality on installing complex applications to interact with the server, for instance to recover events, but it should be designed to be as light as possible and also allowing portability between devices.
- *Efficient encryption key revocation*: The users would encrypt the data before sending it to the server in order to protect their privacy. Encryption is usually done with a key which is only known by each user. The users should own a mechanism to quickly revoke a key in case such key is not valid any more, for instance if it has been stolen or compromised. Furthermore, there should also be a mechanism to generate new keys without requiring re-encrypting all the data in the server.
- *Identity management and access control*: Systems directly imply the management of individual identifiers, their authentication, authorization, privileges and other identity-related features. An exhaustive identity management framework has to be deployed to decide how the different users can interact with the system [40].

## 5. Proposed architecture

This section describes the components of the architecture proposed to face the live digital solution and how they interact with each other to achieve the processes described in Section 3. As introduced above, the information of the users'

interactions should be seamlessly collected, encrypted and stored in a server, in such a way that those users could query and recover such information afterwards.

As we can observe in Fig. 1, the events collection can be done from multiple sources (e-mail, webpages, files, e-Health data, etc.) and using a number of different devices (PC, smartphone, tablet, sensors, smart TV, etc.).

Hence, the architecture definition has to take into account the support of a huge variety of possible kinds of events, easily allowing the development of extensions in such a way that the architecture could be adapted to the current and future users' needs.

In the presented architecture, as we can see in Fig. 2, we establish a differentiation between (i) the client side, where the end users generate and later visualize their different interactions (i.e. events), and (ii) the server side, where the interactions information is securely and privately maintained, so it could be remotely accessed. The following subsections introduce each of these differentiated sides.

### 5.1. Client side

The client side components have two main functionalities. On the one hand, they are in charge of gathering, filtering and encrypting the interactions that the users do with the different services. On the other hand, they are in charge of searching, recovering and decrypting the stored information so it could be visualized in any of the users' devices. Additionally, the client side requires some sort of communicating functionality with the server side so that the encrypted information could be sent to and received from the server.

To perform the client side functionalities, we have defined the following components, as shown in Fig. 2.

- *Interactions gatherer*: This component is in charge of collecting data from the different interactions that the end users have with the numerous services in their daily life. Such data might come from plugins/add-ons installed in different applications. For example, a web browser could send the information of the websites visited by the end users.
- *Event manager*: This component receives and processes the information of the interactions which have been gathered by the previous module. It instantiates the appropriates data structures, i.e. events, representing the information of the interactions in a common format to be processed by the rest of the components.
- *Encryption and decryption agent*: This component encrypts the generated events before sending them to the server. This encryption could create some meta-information in order to allow efficient searches over the events. In a similar way, it decrypts the events recovered from the server, which are the result of a query performed by the end user.
- *Network Interface*: This component acts as the communication interface with the server side, sending collected and encrypted events to be stored in the server, and receiving the encrypted events from the server as a result of a user's query. Some sort of caching mechanism can be included to avoid continuously flooding the server with new gathered events.
- *Visualizer*: This component is responsible for allowing the user to perform advanced queries on a variety of devices such as PC, laptop, smartphone, and smart TV, based on a number of parameters like keywords, time, location, participants, etc. Moreover, it presents the results of those queries in a friendly fashion.
- *Searches handler*: This component is in charge of building a query out of the searching criteria given by the end users, in order to recover information about their past events. For example, it could ask for certain relevant keywords or specify an approximate date of the event. This module could enrich the search by adding, removing or substituting keywords within the query.

### 5.2. Server side

The server side is mainly focused on storing the information received by the user in such a way that it could be queried and transmitted in an efficient way. The functionalities of the server side can be also grouped into two categories. On the one hand, the server is in charge of receiving, organizing and storing the encrypted interactions of the users. On the other hand,

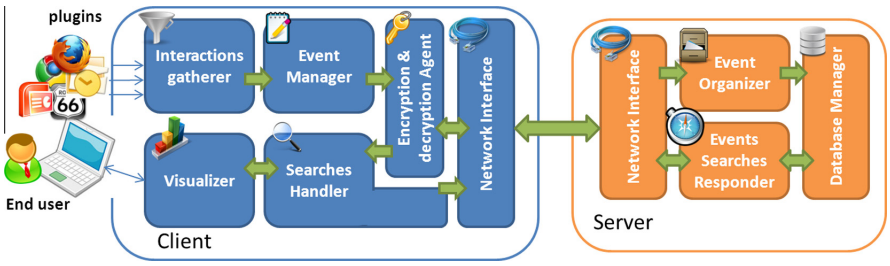


**Fig. 2.** High-level architectural components (client side and server side).

the server is in charge of recovering and selecting the interactions according to the queries received from the client. To perform such functionalities we have defined the following components included in the server side (shown as well in Fig. 2):

- *Network Interface*: As in the case of the client, the server also has a Network Interface component in charge of communicating with the client side. This module receives both the encrypted events from the client, as well as the queries to retrieve those events. In return, it provides the client with the encrypted events obtained after enforcing the user's query.
- *Event Organizer*: This component is in charge of processing and managing the received encrypted events. It prepares the data to be stored allowing a quick and efficient searches later on. For example, it could create and maintain some indices to organize the events.
- *Database Manager*: This component is responsible of appropriately storing the encrypted events. Advanced databases techniques should be applied here to ensure an efficient storage and further retrieval of the data.
- *Event Searches Responder*: The Event Searches Responder receives queries and performs a selection of events based on those queries, recovering the events from the Database Manager. The selection might be sorted based on the relevance with regards to the performed query. The encrypted retrieved events are sent to the client through the Network Interface.

### 5.3. Capturing and recovering data

Next we present the workflows and the involved architectural components in the two main processes considered as part of this solution, namely: data capturing process and data recovery process.

- *Data capturing process*: The capturing process, as depicted in Fig. 3, starts with the gathering of all the user's interactions with the "digital world" (PC, laptop, smartphone, smart TV, e-Health, etc.). After filtering and completing the received information of the interactions, an appropriate event is created out of them containing meaningful meta-data to be used in forthcoming searches. The events are encrypted accordingly and sent to the server. The server receives such events and creates adequate indices for fast recovery before actually storing them.
- *Recovery process*: In turn, the recovery process shown in Fig. 4 starts with the creation of a query out of the search criteria provided by the user, and sending it to the server. The server receives the query and retrieves those events matching with the given query, sorts them according to their relevance to the query, and sends them back to the client, which in turn, decrypts the events, sorts them (clustering, relating, etc.) according to certain criteria (topic-wise, time-wise, etc.) and finally presents them to the user in a friendly manner.

According to the previous description of this proposed architecture, we can note that this is opened enough to support different current and new services (e.g. data industry), endpoint technologies (for gathering information), safe-storage mechanisms, interaction with service and identity providers and integration with IoT architectures. Hence, this architecture can embrace also the sources of personal information mentioned for the tools in Table 1, and could also include local servers (network shared) like repositories to find user information. Finally this architecture covers all the steps pointed in Section 3, namely: gathering, organizing, storing and visualizing, and in this way it also fits and overcomes the scope in terms of processes (collecting, storing, holding, linking, searching and listening) mentioned in Table 1.

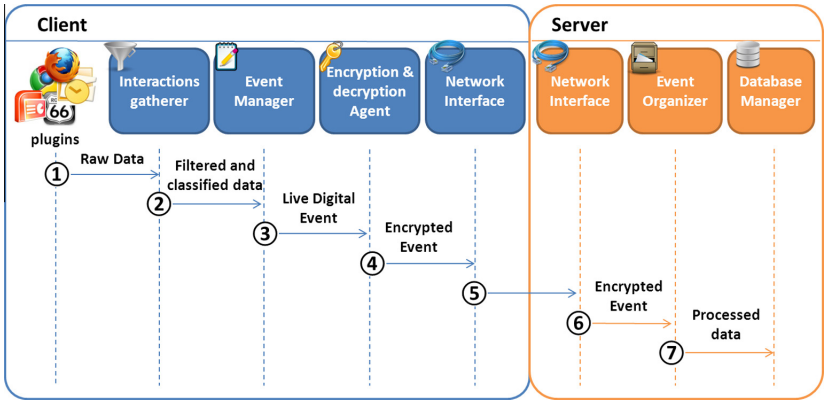


**Fig. 3.** Sequence diagram depicting the data capturing process in live digital/remember digital.

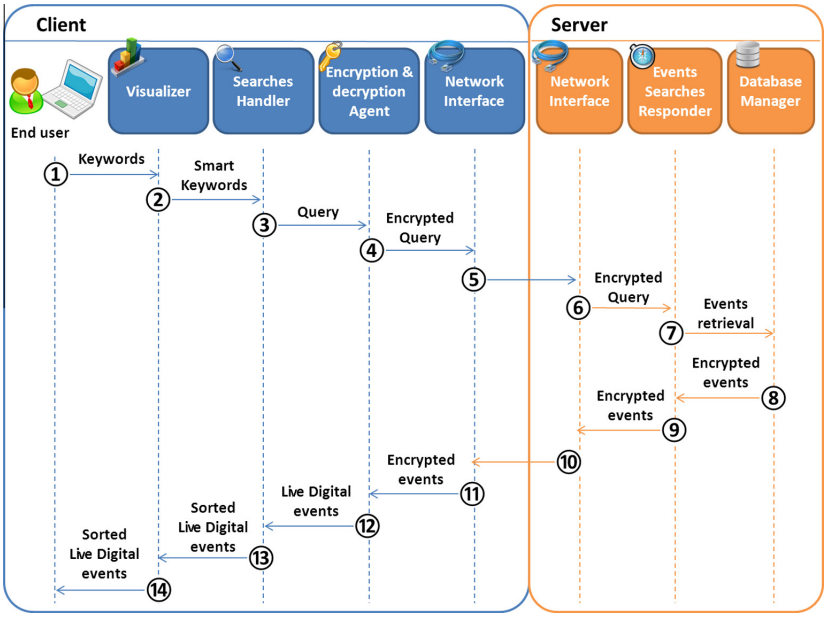


**Fig. 4.** Sequence diagram depicting the data recovery process in live digital/remember digital.

## 6. Use case: health care

As a clear example where Life Digital solutions may be extremely welcome and useful, we have picked an e-Health scenario which is a real concern in many countries nowadays. Particularly, in-home patient monitoring is related usually to a distributed environmental sensor scenario, tracking continuously movement, temperature, humidity, pressure, luminosity and sound, together with more specific features as blood pressure, pulse, body temperature and respiratory rate, which are associated to a human being who dwells a facility. Every time the human moves around, the facility generates data that reflects the changes in the environment and in her body. Global initiatives such as AAL (Ambient Assisted Living) [41] emphasized the importance of focusing on house facilities for elderly people or people with disabilities.

Like AAL, there are other initiatives based on activities for supervising and monitoring human being health. Thus for instance, [42] provides a complete chapter of a myriad of projects to this respect. In this context, it is perfectly acceptable a set of imminent new smart devices around the facility which produce information about the use of its services, such as (i) a smart TV offering broadcast shows, games or movies, (ii) a smart refrigerator with a record of consumed pre-filtered liquid by dispenser, environmental conditions of the food, kind of stored items and items pending for purchase, (iii) a smart shower with a registry of water environmental conditions and use time, or (iv) a food schema assistant registering the compatibility of ingested food by the user, amongst many other possibilities.

All this information can be gathered composing a consolidated information database, which feeds a system that acquires and analyzes different statistics of habits and behavior. For example space occupation, movements, reactions due to exposition to environmental factors, body reactions to food, emotional reactions to contents, etc. These statistics may be used to identify patterns and relations between behaviors, make a tracking of environmental and physical health, and finally to get a record to improve early disease detection and treatment.

Taking into consideration the aforementioned reasons, the presented Life Digital solution in this scenario would bring numerous benefits on helping and assisting the monitored patients. The automatic and seamless recording of the large amount of generated data would endow them with the capabilities to keep a close track of their evolution, amongst other advantages. Likewise, this system would ease the work of their care givers and care providers, enabling them to develop user-tailored treatments (services) which at the end would result more effective for the patient.

Yet, notwithstanding the above, we are probably talking about one of the most private and sensitive data-sets of end users (their health-related data). Therefore, the appropriate advanced privacy-preserving mechanisms need to come into play, in order to actually protect the sensitive user's data from unauthorized accesses. Such unauthorized accesses could come either from the server storing the events itself, or from third parties. The former case could be tackled by properly encrypting the

data, while the latter situation requires of advanced access control mechanisms deciding who has access to what at each moment.

## 7. Conclusions

With the work presented in the paper at hand, we have identified new opportunities and markets around live digital. Live digital may be used to increase productivity at work by reducing the time to find required data, to prove what we did and consequently what we did not do, to assist elderly people and a long etcetera. We have provided an architecture which may be used to address this new challenge. We have also identified the vast set of challenges and problems which are still open for live digital to become a reality. Specially, challenges in security and privacy may be absolutely necessary to appropriately protect the personal data. As future steps, we have in mind to address a complete strategic plan to tackle each of the challenges identified in this contribution, step by step, by means of research works to contribute in each of the issues identified. For example, we are investigating new data-centric encryption schemes, new encryption-aware processing techniques, encryption-aware indexing or purpose-based access to information.

## References


[1] Carroll JM. Human computer interaction (HCI), The interaction design foundation, Aarhus, Denmark; 2013.
[2] Liu Y, Zhou G. Key technologies and applications of internet of things. In: 2012 Fifth international conference on intelligent computation technology and automation (ICICTA). IEEE; 2012. p. 197–200.
[3] Camarillo G, Garcia-Martin M. The 3G IP multimedia subsystem (IMS): merging the Internet and the cellular worlds. Wiley; 2011.
[4] Finkenzeller K. RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication. Wiley; 2010.
[5] Al-Ofeishat H, Mohammad A. Near field communication (NFC). IJCSNS 2012;12(2):93.
[6] Porcino D, Hirt W. Ultra-wideband radio technology: potential and challenges ahead. IEEE Commun Mag 2003;41(7):66–74.
[7] Sahinoglu Z, Gezici S, Gvenc I. Ultra-wideband positioning systems: theoretical limits, ranging algorithms, and protocols. Cambridge University Press; 2011.
[8] Sveda M, Trchalik R. Zigbee-to-internet interconnection architectures. In: Second international conference on systems, 2007. ICONS'07. IEEE; 2007. p. 30.
[9] Yin H, Long B, Wang N. Power line carrier-based networking technology of the internet of things. Adv Mater Res 2012;516:1414–8.
[10] Pan J, Paul S, Jain R. A survey of the research on future internet architectures. IEEE Commun Mag 2011;49(7):26–36.
[11] Sanvido F, Díaz-Sánchez D, Almenárez-Mendoza F, Marín-López A. A survey on security in future internet and cloud. In: AFIN 2011, The third international conference on advances in future internet; 2011. p. 35–40.
[12] Gemmell J, Bell G, Lueder R. MyLifeBits: a personal database for everything. Commun ACM 2006;49(1):88–95.
[13] Hodges S, Williams L, Berry E, Izadi S, Srinivasan J, Butler A, et al. SenseCam: a retrospective memory aid. UbiComp 2006: Ubiquit Comput 2006:177–93.
[14] Bang-Jensen J, Gutin G. Digraphs: theory, algorithms and applications. Springer; 2008.
[15] Cole B. Search engines tackle the desktop. Computer 2005;38(3):14–7.
[16] Noda T, Helwig S. Benchmark study of desktop search tools. Best practice report 1.0. University of Wisconsin-Madison E-Business Consortium. Madison, WI 53706; 2005.
[17] Yahoo! Desktop Search, Official Product WebPage; 2013 <http://info.yahoo.com/privacy/us/yahoo/desktopsearch/>.
[18] Inside Google Desktop, Official Product WebPage; 2013 <http://desktop.google.com>.
[19] Copernic Desktop Search – The best Desktop Search Tool, Official Product WebPage; 2013 <http://www.copernic.com/en/products/desktop-search/>.
[20] Huttunen J. Locate32, Official Product WebPage; 2013 <http://locate32.cogit.net/>.
[21] Kim P. E-model: event-based graph data model theory and implementation. Ph.D. thesis, Georgia Institute of Technology.
[22] Giunchiglia F, Kim P. Lifelog data model and management: study on research challenges.
[23] Godoy D. One-class support vector machines for personalized tag-based resource classification in social bookmarking systems. Concurr Comput: Pract Exper 2012;24(17):2193–206. http://dx.doi.org/10.1002/cpe.2892.
[24] Kabir M, Mahmood A, Mustafa A. K-means clustering microaggregation for statistical disclosure control. In: Kumar AM, Selvarani R, Kumar TVS, editors. Proceedings of international conference on advances in computing. Advances in intelligent systems and computing, vol. 174. India: Springer; 2012. p. 1109–15.
[25] Sànchez J, Urrutia J, Ripoll E. Trade-off between disclosure risk and information loss using multivariate microaggregation: a case study on business data. In: Privacy in statistical databases. Springer; 2004. p. 519.
[26] Solé M, Muntés-Mulero V, Nin J. Efficient microaggregation techniques for large numerical data volumes. Int J Inform Secur 2012;11:253–67. http://dx.doi.org/10.1007/s10207-012-0158-5.
[27] Kontaxis G, Polychronakis M, Markatos E. Minimizing information disclosure to third parties in social login platforms. Int J Inform Secur 2012;11:321–32. http://dx.doi.org/10.1007/s10207-012-0173-6.
[28] Ardagna CA, De Capitani di Vimercati S, Foresti S, Paraboschi S, Samarati P. Supporting privacy preferences in credential-based interactions. In: Proceedings of the 9th annual ACM workshop on privacy in the electronic society, WPES 10. New York, NY, USA: ACM; 2010. p. 83–92. http://dx.doi.org/10.1145/1866919.1866931.
[29] Kontaxis G, Polychronakis M, Markatos E. Sudoweb: minimizing information disclosure to third parties in single sign-on platforms. Inform Secur 2011:197–212.
[30] Dey A, Weis S. Pseudoid: enhancing privacy in federated login. In: Hot topics in privacy enhancing technologies; 2010. p. 95–107 <http://www.pseudoid.net>.
[31] Corena J, Ohtsuki T. Secure and fast aggregation of financial data in cloud-based expense tracking applications. J Netw Syst Manage 2012;20:534–60. http://dx.doi.org/10.1007/s10922-012-9248-y.
[32] Yaseen Q, Panda B. Insider threat mitigation: preventing unauthorized knowledge acquisition. Int J Inform Secur 2012;11:269–80. http://dx.doi.org/10.1007/s10207-012-0165-6.
[33] Bogdanov D, Niitsoo M, Toft T, Willemson J. High-performance secure multi-party computation for data mining applications. Int J Inform Secur 2012;11:403–18. http://dx.doi.org/10.1007/s10207-012-0177-2.
[34] Bethencourt J, Song D, Waters B. New techniques for private stream searching. ACM Trans Inf Syst Secur 2009;12(3):16:1–16:32. http://dx.doi.org/10.1145/1455526.1455529.
[35] Cao N, Wang C, Li M, Ren K, Lou W. Privacy-preserving multi-keyword ranked search over encrypted cloud data. In: INFOCOM, 2011 proceedings IEEE; 2011. p. 829–37. http://dx.doi.org/10.1109/INFCOM.2011.5935306.

[36] Glisson W, Storer T, Mayall G, Moug I, Grispos G. Electronic retention: what does your mobile phone reveal about you? Int J Inform Secur 2011;10(6):337–49.
[37] Sengupta A, Mazumdar C, Bagchi A. A formal methodology for detecting managerial vulnerabilities and threats in an enterprise information system. J Netw Syst Manage 2011;19(3):319–42.
[38] Ahmed M, Al-Shaer E, Taibah M, Khan L. Objective risk evaluation for automated security management. J Netw Syst Manage 2011;19(3):343–66.
[39] Cascarano N, Ciminiera L, Risso F. Optimizing deep packet inspection for high-speed traffic analysis. J Netw Syst Manage 2011;19(1):7–31.
[40] Dólera Tormo G, López Millán G, Martínez Pérez G. Definition of an advanced identity management infrastructure. Int J Inform Secur 2012;19(2):1–28. http://dx.doi.org/10.1007/s10207-012-0189-y.
[41] Costa R, Carneiro D, Novais P, Lima L, Machado J, Marques A, et al. Ambient assisted living. In: 3rd Symposium of ubiquitous computing and ambient intelligence 2008. Springer; 2009. p. 86–94.
[42] Rashvand HF, Alcaraz Calero JM. Smart sensing architectures. John Wiley and Sons, Ltd.; 2012. p. 480, http://dx.doi.org/10.1002/9781119941354.ch3.

**Daniel Díaz López** is a PhD student in computer engineering from the University of Murcia. His research interests include management and federation of identity, security in cloud computing and privacy. At the time of writing this paper he was student research assistant at NEC Laboratories Europe, Heidelberg, Germany. He received an MSc in computer engineering from the University of Murcia.

**Ginés Dólera Tormo** is a research scientist in the security group at NEC Laboratories Europe, Heidelberg, Germany. He is pursuing his PhD at the University of Murcia. His research interests include authorization, authentication and identity management, user-centric technologies and trust management. He received an MSc in computer science from the University of Murcia, Spain.

**Félix Gómez Mármol** is a senior research scientist in the security group at NEC Laboratories Europe, Heidelberg, Germany. His research interests include authorization, authentication and trust management in distributed and heterogeneous systems, security management in mobile devices and design and implementation of security solutions for mobile and heterogeneous environments. He received an MSc and PhD in computer engineering from the University of Murcia.

**Jose M. Alcaraz Calero** is Lecturer on Networks at University of the West of Scotland, United Kingdom. His research interests include authorization, authentication and trust management in distributed and heterogeneous systems, cloud computing and big data. He hold an MSc and PhD in computer engineering from the University of Murcia.

**Gregorio Martínez Pérez** is an associate professor in the Department of Information and Communications Engineering of the University of Murcia. His research interests include security, privacy and management of IP-based communication networks. He received an MSc and PhD in computer engineering from the University of Murcia.

# Bibliography


[1] R. Shirey, RFC4949 - Internet Security Glossary, Version 2, IETF - Informational Memo (2007).

[2] ISO/IEC 13335-1:2004 Information technology – Security techiques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management, International Standard, edition 1 (November 2004).

[3] Ministry of Finance and Public Administration - Spanish government, MAGERIT version 3.0. Methodology for Information Systems Risk Analysis and Management. Book I - The Method, http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html, edition 1 (July 2014).

[4] R. Kainda, I. Flechais, A. Roscoe, Security and usability: Analysis and evaluation, in: ARES '10 International Conference on Availability, Reliability, and Security, 2010, 2010, pp. 275–282.

[5] L. Zapata, Development of a Model for Security and Usability, Master Thesis, Universidad Politécnica de Madrid (July 2013).

[6] NIST/NSA Privilege Access Management Workshop Collaboration Team, Nist IR 7657 - A Report on the Privilege (Access) Management Workshop, annex B: A Survey of Access Control, NIST Internal Report, National Institute of Standards and Technology (March 2010).

[7] M. Goodyear, J. Louis, Defining the security domain, http://www.educause.edu/ir/library/powerpoint/SPC0669A.pps (April 2006).

[8] J. Chen, Y. Wang, X. Wang, On-demand security architecture for cloud computing, Computer 45 (7) (2012) 73–78.

[9] Verizon Communications, Data Breach Investigation Report (DBIR) 2015, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf.

[10] European Comission, Digital Security: Cybersecurity, Privacy and Trust, Call H2020-DS-2014-1, DS-02-2014,

http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/1050-ds-02-2014.html, Official WebPage (December 2013).

[11] European Comission, HORIZON 2020 Work Programme 2014-2015 - Secure Societies - Protecting freedom and security of Europe and its citizens, http://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/main/h2020-wp1415-security_v2.0_en.pdf (July 2014).

[12] Department of Homeland Security, Science and Technology Directorate Review 2014, http://www.dhs.gov/sites/default/files/publications/DHS_ST_Review_2014-508_1.pdf, report (August 2014).

[13] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, version 1.0 (February 2014).

[14] R. W. McGraw, Risk-adaptable access control (radac), in: Privilege (Access) Management Workshop, NIST-National Institute of Standards and Technology-Information Technology Laboratory, NIST, 2009, gaithersburg, Maryland, USA.

[15] ISO/IEC 27001 Information technology - Security techiques - Information security management systems - Requirements, International Standard, edition 2 (October 2013).

[16] ISO/IEC 27005 Information technology - Security techiques - Information security risk management, International Standard, edition 2 (June 2008).

[17] D. Díaz, G. Dólera, F. Mármol, G. Pérez, Managing XACML systems in distributed environments through Meta-Policies, Computers & Security 48 (0) (2015) 92 – 115.

[18] D. Díaz, G. Dólera, F. Mármol, G. Pérez, Dynamic counter-measures for risk-based access control systems: An evolutive approach, Future Generation Computer Systems (-).

[19] D. Díaz, G. Dólera, F. Mármol, J. Calero, G. Pérez, Live digital, remember digital: State of the art and research challenges, Computers & Electrical Engineering 40 (1) (2014) 109 – 120, 40th-year commemorative issue.

[20] R. Sawilla, D. Wiemer, Automated computer network defence technology demonstration project (ARMOUR TDP): Concept of operations, architecture, and integration framework, in: 2011 IEEE International Conference on Technologies for Homeland Security (HST), 2011, pp. 167–172.

[21] R. Caralli, R. Danyliw, J. Spencer, CSIRT Requirements for Situational Awareness, Tech. rep., Carnegie Mellon Software Engineering Institute (January 2014).

[22] DHS, Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture Report - (CAESARS), Tech. rep., Department of Homeland Security - Federal Network Security Branch (September 2010).

[23] Verizon Communications, Data Breach Investigation Report (DBIR) 2014, http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf, Security Report (2014).

[24] A. Anderson, H. Lockhart, SAML 2.0 profile of XACML v2.0, http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-saml-profile-spec-os.pdf, OASIS Standard (February 2005).

[25] A. Anderson, XACML profile for role based access control (RBAC), OASIS Access Control TC committee draft 1 (2004) 1–13.

[26] C. A. Ardagna, S. D. C. di Vimercati, E. Pedrini, S. Paraboschi, P. Samarati, M. Verdicchio, Extending XACML for open web-based scenarios, W3C Workshop on Access Control Application Scenarios, Luxembourg, 2009.

[27] M. Bartel, J. Boyer, B. Fox, B. LaMacchia, E. Simon, XML-Signature Syntax and Processing (Second Edition), http://www.w3.org/TR/xmldsig-core/, W3C recommendation (June 2008).

[28] E. Blasch, É. Bossé, D. Lambert, High-level Information Fusion: Management and Systems Design, Artech House intelligence and information operations series, ARTECH HOUSE Incorporated, 2012.

[29] S. Cantor, J. Kemp, R. Philpott, E. Maler, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard (March 2005).

[30] S. Cantor, F. Hirsch, J. Kemp, R. Philpott, E. Maler, et al., Bindings for the OASIS Security Assertion Markup Language (SAML) V2. 0, OASIS Standard (March 2005).

[31] S. Das, K. Kant, N. Zhang, Handbook on Securing Cyber-Physical Critical Infrastructure, Morgan Kaufmann, 2012.

[32] D. DeCouteau, M. Davis, S. D., Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of Security Assertion Markup Language (SAML) for Healthcare, https://www.oasis-open.org/committees/download.php/29921/xspa-saml-profile-cd-01.doc", OASIS Committee Draft (November 2008).

[33] Y. Demchenko, O. Koeroo, C. de Laat, H. Sagehaug, Extending XACML authorisation model to support policy obligations handling in distributed application, in: Proceedings of the 6th international workshop on Middleware for grid computing, no. 5 in MGC 08, ACM, New York, NY, USA, 2008.

[34] L. Dong, K. Chen, Cryptographic Protocol: Security Analysis Based on Trusted Freshness, Springer, 2012.

[35] D. Ferraiolo, D. Kuhn, R. Chandramouli, Role-Based Access Controls, Artech House Computer Security Series, Artech House, 2003.

[36] I. Foster, What is the Grid? A Three Point Checklist, Journal GRID today 1 (6) (2002) 4.

[37] D. Ganguly, S. Lahiri, Network and Application Security: Fundamentals and Practices, Science Publishers - CRC Press, 2012.

[38] G. Garzoglio, et al., An XACML Attribute and Obligation Profile for Authorization Interoperability in Grids, CS Document 2952-v3, Grids Fermilab (August 2011).

[39] G. Garzoglio, I. Alderman, M. Altunay, R. Ananthakrishnan, J. Bester, K. Chadwick, V. Ciaschini, Y. Demchenko, A. Ferraro, A. Forti, D. Groep, T. Hesselroth, J. Hover, O. Koeroo, C. Joie, T. Levshina, Z. Miller, J. Packard, H. Sagehaug, V. Sergeev, I. Sfiligoi, N. Sharma, F. Siebenlist, V. Venturi, J. Weigand, Definition and Implementation of a SAML-XACML Profile for Authorization Interoperability Across Grid Middleware in OSG and EGEE, Journal of Grid Computing 7 (3) (2009) 297–307.

[40] P. Goyal, S. Batra, A. Singh, A literature review of security attack in mobile ad-hoc networks, International Journal of Computer Applications IJCA 9 (12) (2010) 24–28.

[41] O. Gryb, XACMLight Reference, http://xacmllight.sourceforge.net/, Official Project Web Site (July 2012).

[42] H. H. Hosmer, Metapolicies I, SIGSAC Rev. 10 (2-3) (1992) 18–43.

[43] V. Hu, D. Ferraiolo, D. Kuhn, Assessment of access control systems, NIST interagency report 7316, National Institute of Standards and Technology (September 2006).

[44] J. Hughes, E. Maler, Security Assertion Markup Language SAML v2.0 technical overview, OASIS Working Draft (October 2006).

[45] F. Huonder, Conflict detection and resolution of XACML policies, Master's thesis, University of Applied Sciences Rapperswil (July 2010).

[46] T. Imamura, B. Dillaway, E. Simon, et al., XML Encryption Syntax and Processing, http://www.w3.org/TR/xmlenc-core/, W3C Recommendation (December 2002).

[47] W. E. Kühnhauser, On paradigms for security policies in multipolicy environments, in: In Proceedings of the 11th International Information Security Conference (IFIP/SEC '95), Cape Town, South Africa, Chapman and Hall, 1995.

[48] F. Krief, Communicating Embedded Systems: Networks Applications, ISTE - Wiley, 2013.

[49] A. Kuketayev, XACML version 2.0 conformance tests, version 0.5, https://www.oasis-open.org/committees/download.php/14877/ConformanceTests.html, Non-normative tests - OASIS Consortium (October 2005).

[50] S. Lakshminarayanan, Oracle Web Services Manager, From technologies to solutions, Packt Publishing, Limited, 2008.

[51] M. Lischka, Y. Endo, M. Sánchez Cuenca, Deductive policies with XACML, in: Proceedings of the 2009 ACM workshop on Secure web services, ACM, Chicago, Illinois, USA, 2009, pp. 37–44.

[52] M. Lorch, D. Kafura, S. Shah, An XACML-based Policy Management and Authorization Service for Globus Resources, in: Proceedings of the 4th International Workshop on Grid Computing, IEEE Computer Society, Phoenix, AZ, USA, 2003, pp. 208–213.

[53] E. Lupu, M. Sloman, Conflict analysis for management policies, in: A. Lazar, R. Saracco, R. Stadler (Eds.), Integrated Network Management V, IFIP - The International Federation for Information Processing, Springer US, 1997, pp. 430–443.

[54] E. Martin, T. Xie, T. Yu, Defining and measuring policy coverage in testing access control policies, in: Proc. 8th International Conference on Information and Communications Security - ICICS, Vol. 4307, Springer, 2006, pp. 139 – 158.

[55] T. Moses, et al., eXtensible Access Control Markup Language (XACML) Version 2.0, http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf, OASIS Standard (February 2005).

[56] B. Parducci, H. Lockhart, XACML v3.0 Administration and Delegation Profile Version 1.0, http://docs.oasis-open.org/xacml/3.0/xacml-3.0-administration-v1-spec-cs-01-en.pdf, OASIS Committee Specification (August 2010).

[57] A holistic approach to security policies - policy distribution with XACML over COPS, Electronic Notes in Theoretical Computer Science 168 (0) (2007) 143 – 157, proceedings of the Second International Workshop on Views on Designing Complex Architectures (VODCA 2006).

[58] P. Rao, D. Lin, E. Bertino, N. Li, J. Lobo, An algebra for fine-grained integration of xacml policies, in: Proceedings of the 14th ACM Symposium on Access Control Models and Technologies, SACMAT '09, ACM, New York, NY, USA, 2009, pp. 63–72.

[59] M. Rosen, B. Lublinsky, K. Smith, M. Balcer, Applied SOA: Service-Oriented Architecture and Design Strategies, Wiley, 2012.

[60] M. St-Martin, A verified algorithm for detecting conflicts in XACML access control rules, Master's thesis, University of Ottawa (2012).

[61] Sun Microsystems, Inc, Sun's XACML Implementation, http://sunxacml.sourceforge.net/, Official Project Web Site (June 2006).

[62] J. Vacca, Computer and Information Security Handbook, no. 2, Elsevier Science, 2012.

[63] Q. Wei, J. Crampton, K. Beznosov, M. Ripeanu, Authorization recycling in hierarchical RBAC systems, ACM Transactions on Information and System Security TISSEC 14 (1).

[64] G. Wurster, P. Van Oorschot, A control point for reducing root abuse of file-system privileges, in: Proceedings of the 17th ACM conference on Computer and communications security, ACM, Chicago, Illinois, USA, 2010, pp. 224–236.

[65] OASIS Consortium, XACML References and Products, Version 1.85, https://www.oasis-open.org/committees/download.php/42588/xacmlRefs-V1-85.html, List (June 2011).

[66] S. Yang, Internet-based Control Systems: Design and Applications, Advances in Industrial Control, Springer, 2011.

[67] J. Qian, S. Hinrichs, K. Nahrstedt, Acla: A framework for access control list (acl) analysis and optimization, in: R. Steinmetz, J. Dittman, M. Steinebach (Eds.), Communications and Multimedia Security Issues of the New Century, Vol. 64 of IFIP - The International Federation for Information Processing, Springer US, 2001, pp. 197–211.

[68] A. Liu, E. Torng, C. Meiners, Compressing network access control lists, Parallel and Distributed Systems, IEEE Transactions on 22 (12) (2011) 1969–1977.

[69] S. D. Stoller, P. Yang, M. I. Gofman, C. Ramakrishnan, Symbolic reachability analysis for parameterized administrative role-based access control, Computers and Security, Special Issue on Access Control Methods and Technologies 30 (2 - 3) (2011) 148 – 164.

[70] Y. Jung, J. B. Joshi, Cribac: Community-centric role interaction based access control model, Computers and Security 31 (4) (2012) 497 – 523.

[71] Q. Zhang, Y. Mu, M. Zhang, Attribute-based authentication for multi-agent systems with dynamic groups, Computer Communications, Special Issue of Computer Communications on Information and Future Communication Security 34 (3) (2011) 436 – 446.

[72] B. Cha, J. Seo, J. Kim, Design of attribute-based access control in cloud computing environment, in: K. J. Kim, S. J. Ahn (Eds.), Proceedings of the International Conference on IT Convergence and Security 2011, Vol. 120 of Lecture Notes in Electrical Engineering, Springer Netherlands, Suwon, Korea, 2012, pp. 41–50.

[73] P. Kodeswaran, S. B. Kodeswaran, A. Joshi, T. Finin, Enforcing security in semantics driven policy based networks, Computer Standards and Interfaces, Special Issue: Secure Semantic Web 33 (1) (2011) 2 – 12.

[74] D. Huang, W.-T. Tsai, Y.-h. Tseng, Policy management for secure data access control in vehicular networks, Journal of Network and Systems Management 19 (2011) 448–471.

[75] Q. Ni, E. Bertino, J. Lobo, Risk-based access control systems built on fuzzy inferences, in: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ACM, 2010, pp. 250–260.

[76] R. A. Shaikh, K. Adi, L. Logrippo, Dynamic risk-based decision methods for access control systems, Computers & Security 31 (4) (2012) 447–464.

[77] J. Hintzbergen, K. Hintzbergen, A. Smulders, Foundations of Information Security: Based on ISO27001 and ISO27002, Best practice, Bernan Assoc, 2010.

[78] A. Calder, S. Watkins, IT Governance: An International Guide to Data Security and ISO27001/ISO27002, ITPro collection, Kogan Page, 2012.

[79] T. Sakuraba, K. Sakurai, Proposal of the hierarchical file server groups for implementing mandatory access control, in: Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Palermo, Italy, July, pp. 639–644.

[80] J. Zhang, J. Yao, K. Huang, Research on Access Control Policy for Confidential Information System, Applied Mechanics and Materials 263 (2012) 3064–3067.

[81] S. Kandala, R. Sandhu, V. Bhamidipati, An attribute based framework for risk-adaptive access control models, in: Sixth International Conference on Availability, Reliability and Security (ARES), 2011, pp. 236–241, Vienna, Austria.

[82] Q. Wang, H. Jin, Quantified risk-adaptive access control for patient privacy protection in health information systems, in: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS '11, ACM, 2011, pp. 406–410.

[83] M. E. Orwat, A decision framework for enhancing mobile ad hoc network stability and security, Phd thesis, Naval Postgraduate School Monterey CA (June 2008).

[84] R. A. Shaikh, K. Adi, L. Logrippo, Dynamic risk-based decision methods for access control systems, Computers and Security 31 (4) (2012) 447 – 464.

[85] M. Sharma, Y. Bai, S. Chung, L. Dai, Using risk in access control for cloud-assisted ehealth, in: 14th IEEE International Conference on High Performance Computing and Communication & 9th International Conference on Embedded Software and Systems (HPCC-ICESS), IEEE, 2012, pp. 1047–1052, Liverpool, United Kingdom.

[86] L. Chen, J. Crampton, M. Kollingbaum, T. Norman, Obligations in risk-aware access control, in: 10th Annual International Conference on Privacy, Security and Trust (PST), IEEE, 2012, pp. 145–152, Paris, France.

[87] K. De Jong, Evolutionary computation: A unified approach, in: Proceedings of the 14th Annual Conference Companion on Genetic and Evolutionary Computation, GECCO '12, ACM, 2012, pp. 737–750.

[88] P. Guo, X. Wang, Y. Han, The enhanced genetic algorithms for the optimization design, in: Biomedical Engineering and Informatics (BMEI), 2010 3rd International Conference on, Vol. 7, 2010, pp. 2990–2994.

[89] Extensible access control markup language (XACML) version 3.0, OASIS Standard (January 2013).

[90] S. Pina Ros, M. Lischka, F. Gómez Mármol, Graph-based xacml evaluation, in: Proceedings of the 17th ACM Symposium on Access Control Models and Technologies, SACMAT '12, ACM, New York, NY, USA, 2012, pp. 83–92.

[91] K. M. Kavanagh, M. Nicolett, J. Pescatore, Marketscope for vulnerability assessment, Gartner RAS Core Research Note G 156038.

[92] Product Guide McAfee Risk Advisor 2.7 Software, https://kb.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/23000/PD23685/en_US/MRA_2.7.0_Product_Guide_en-us.pdf, Accessed: April 2014 (2012).

[93] E. Alba, B. Dorronsoro, Cellular Genetic Algorithms, Vol. 42 of Operations research/computer science interfaces series ; ORCS 42, Springer London, Limited, 2008.

[94] A. Moraglio, S. Silva, K. Krawiec, P. Machado, C. Cotta (Eds.), 15th European Conference on Genetic Programming, EuroGP, Vol. 7244 of Lecture Notes in Computer Science, Springer, Malaga, Spain, 2012.

[95] M. Agrawal, P. Mishra, A comparative survey on symmetric key encryption techniques, International Journal on Computer Science & Engineering 4 (5) (2012) 877–882.

[96] S. U. Rehman, M. Bilal, B. Ahmad, K. M. Yahya, A. Ullah, O. U. Rehman, Comparison based analysis of different cryptographic and encryption techniques using message authentication code (mac) in wireless sensor networks (wsn), International Journal of Computer Science Issues (IJCSI) 9 (1) (2012) 96–101.

[97] K. Floyd, J. P. Whelan, A. W. Meyers, Use of warning messages to modify gambling beliefs and behavior in a laboratory investigation, Psychology of Addictive Behaviors 20 (1) (2006) 69–74.

[98] F.-F. Cheng, C.-S. Wu, Debiasing the framing effect: The effect of warning and involvement, Decision Support Systems 49 (3) (2010) 328–334.

[99] S. Ismail, M. Ngadi, New security authentication mechanisms in grid computing web environment, in: International Conference on Research and Innovation in Information Systems (ICRIIS), Kuala Lumpur, Malaysia, 2011, pp. 1–4.

[100] R. Hasan, R. Khan, Interaction provenance model for unified authentication factors in service oriented computing, in: Proceedings of the 4th ACM Conference on Data and Application Security and Privacy, CODASPY '14, ACM, New York, NY, USA, 2014, pp. 127–130.

[101] D. Thorleuchter, D. V. den Poel, Improved multilevel security with latent semantic indexing, Expert Systems with Applications 39 (18) (2012) 13462 – 13471.

[102] K. Tang, T. Chan, R. Yin, K. Man, Multiobjective Optimization Methodology: A Jumping Gene Approach, Industrial Electronic Series, CRC PressINC, 2012.

[103] A. Hopgood, Intelligent Systems for Engineers and Scientists, Third Edition, 3rd Edition, CRC Press, 2012, iSBN=9781466516175.

[104] ISO/IEC 27033-3 Information technology - Security techniques - Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues, ISO Standard (December 2010).

[105] A. N. Khan, M. M. Kiah, S. U. Khan, S. A. Madani, Towards secure mobile cloud computing: A survey, Future Generation Computer Systems 29 (5) (2013) 1278 – 1299, special section: Hybrid Cloud Computing.

[106] J. Arshad, P. Townend, J. Xu, A novel intrusion severity analysis approach for clouds, Future Generation Computer Systems 29 (1) (2013) 416 – 428, including Special section: AIRCC-NetCoM 2009 and Special section: Clouds and Service-Oriented Architectures.

[107] I. Ray, I. Ray, Trust-based access control for secure cloud computing, in: K. J. Han, B.-Y. Choi, S. Song (Eds.), High Performance Cloud Auditing and Applications, Springer New York, 2014, pp. 189–213.

[108] J. O. Fito, J. Guitart, Business-driven management of infrastructure-level risks in cloud providers, Future Generation Computer Systems 32 (0) (2014) 41 – 53, special Section: The Management of Cloud Systems.

[109] W. Han, C. Sun, C. Shen, C. Lei, S. Shen, Dynamic combination of authentication factors based on quantified risk and benefit, Security and Communication Networks 7 (2) (2014) 385–396.

[110] C. Bailey, D. Chadwick, R. de Lemos, Self-adaptive authorization framework for policy based rbac/abac models, in: IEEE 9th International Conference on Dependable, Autonomic and Secure Computing (DASC), Sydney, Australia, 2011, pp. 37–44.

[111] C. Bailey, L. Montrieux, R. de Lemos, Y. Yu, M. Wermelinger, Run-time generation, transformation, and verification of access control models for self-protection, in: SEAMS'14: 9th International Symposium on Software Engineering for Adaptive and Self-Managing Systems, ACM, ACM, Hyderabad, India, 2014.

[112] P.-C. Cheng, P. Rohatgi, C. Keser, P. Karger, G. Wagner, A. Reninger, Fuzzy multi-level security: An experiment on quantified risk-adaptive access control, in: Security and Privacy, 2007. SP '07. IEEE Symposium on, 2007, pp. 222 –230.

[113] U. M. Mbanaso, G. Cooper, D. Chadwick, A. Anderson, Obligations of trust for privacy and confidentiality in distributed transactions, Internet Research 19 (2) (2009) 153–173.

[114] J. M. Carroll, Human Computer Interaction (HCI), The Interaction Design Foundation, Aarhus, Denmark, 2013.

[115] Y. Liu, G. Zhou, Key technologies and applications of internet of things, in: Intelligent Computation Technology and Automation (ICICTA), 2012 Fifth International Conference on, IEEE, 2012, pp. 197–200.

[116] G. Camarillo, M. Garcia-Martin, The 3G IP multimedia subsystem (IMS): merging the Internet and the cellular worlds, Wiley, 2011.

[117] K. Finkenzeller, RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication, Wiley, 2010.

[118] H. Al-Ofeishat, A. Mohammad, Near Field Communication (NFC), IJCSNS 12 (2) (2012) 93.

[119] D. Porcino, W. Hirt, Ultra-wideband radio technology: potential and challenges ahead, Communications Magazine, IEEE 41 (7) (2003) 66–74.

[120] M. Sveda, R. Trchalik, Zigbee-to-internet interconnection architectures, in: Systems, 2007. ICONS'07. Second International Conference on, IEEE, 2007, pp. 30–30.

[121] H. Yin, B. Long, N. Wang, Power line carrier-based networking technology of the internet of things, Advanced Materials Research 516 (2012) 1414–1418.

[122] J. Pan, S. Paul, R. Jain, A survey of the research on future internet architectures, Communications Magazine, IEEE 49 (7) (2011) 26–36.

[123] F. Sanvido, D. Díaz-Sánchez, F. Almenárez-Mendoza, A. Marín-López, A survey on security in future internet and cloud, in: AFIN 2011, The Third International Conference on Advances in Future Internet, 2011, pp. 35–40.

[124] J. Gemmell, G. Bell, R. Lueder, Mylifebits: a personal database for everything, Communications of the ACM 49 (1) (2006) 88–95.

[125] S. Hodges, L. Williams, E. Berry, S. Izadi, J. Srinivasan, A. Butler, G. Smyth, N. Kapur, K. Wood, Sensecam: A retrospective memory aid, UbiComp 2006: Ubiquitous Computing (2006) 177–193.

[126] J. Bang-Jensen, G. Gutin, Digraphs: theory, algorithms and applications, Springer, 2008.

[127] B. Cole, Search engines tackle the desktop, Computer 38 (3) (2005) 14–17.

[128] T. Noda, S. Helwig, Benchmark study of desktop search tools, Best Practice Report 1.0, University of Wisconsin-Madison E-Business Consortium, Madison, WI 53706 (april 2005).

[129] Yahoo! Desktop Search, http://info.yahoo.com/privacy/us/yahoo/desktopsearch/, Official Product WebPage (January 2013).

[130] Inside Google Desktop, http://desktop.google.com, Official Product WebPage (January 2013).

[131] Copernic Desktop Search - The best desktop search tool, http://www.copernic.com/en/products/desktop-search/, Official Product WebPage (January 2013).

[132] J. Huttunen, Locate32, http://locate32.cogit.net/, Official Product WebPage (January 2013).

[133] P. Kim, E-model: event-based graph data model theory and implementation, Ph.D. thesis, Georgia Institute of Technology.

[134] F. Giunchiglia, P. Kim, Lifelog data model and management: Study on research challenges.

[135] D. Godoy, One-class support vector machines for personalized tag-based resource classification in social bookmarking systems, Concurr. Comput. : Pract. Exper. 24 (17) (2012) 2193–2206.

[136] M. Kabir, A. Mahmood, A. Mustafa, K-means clustering microaggregation for statistical disclosure control, in: A. Kumar M., S. R., T. V. S. Kumar (Eds.), Proceedings of International Conference on Advances in Computing, Vol. 174 of Advances in Intelligent Systems and Computing, Springer India, 2012, pp. 1109–1115.

[137] J. Sànchez, J. Urrutia, E. Ripoll, Trade-off between disclosure risk and information loss using multivariate microaggregation: A case study on business data, in: Privacy in Statistical Databases, Springer, 2004, pp. 519–519.

[138] M. Solé, V. Muntés-Mulero, J. Nin, Efficient microaggregation techniques for large numerical data volumes, International Journal of Information Security 11 (2012) 253–267.

[139] G. Kontaxis, M. Polychronakis, E. Markatos, Minimizing information disclosure to third parties in social login platforms, International Journal of Information Security 11 (2012) 321–332.

[140] C. A. Ardagna, S. De Capitani di Vimercati, S. Foresti, S. Paraboschi, P. Samarati, Supporting privacy preferences in credential-based interactions, in: Proceedings of the 9th annual ACM workshop on Privacy in the electronic society, WPES 10, ACM, New York, NY, USA, 2010, pp. 83–92.

[141] G. Kontaxis, M. Polychronakis, E. Markatos, Sudoweb: Minimizing information disclosure to third parties in single sign-on platforms, Information Security (2011) 197–212.

[142] A. Dey, S. Weis, Pseudoid: Enhancing privacy in federated login, in: Hot Topics in Privacy Enhancing Technologies, 2010, pp. 95–107.

[143] J. Corena, T. Ohtsuki, Secure and fast aggregation of financial data in cloud-based expense tracking applications, Journal of Network and Systems Management 20 (2012) 534–560.

[144] Q. Yaseen, B. Panda, Insider threat mitigation: preventing unauthorized knowledge acquisition, International Journal of Information Security 11 (2012) 269–280.

[145] D. Bogdanov, M. Niitsoo, T. Toft, J. Willemson, High-performance secure multi-party computation for data mining applications, International Journal of Information Security 11 (2012) 403–418.

[146] J. Bethencourt, D. Song, B. Waters, New techniques for private stream searching, ACM Trans. Inf. Syst. Secur. 12 (3) (2009) 16:1–16:32.

[147] N. Cao, C. Wang, M. Li, K. Ren, W. Lou, Privacy-preserving multi-keyword ranked search over encrypted cloud data, in: INFOCOM, 2011 Proceedings IEEE, 2011, pp. 829 –837.

[148] W. Glisson, T. Storer, G. Mayall, I. Moug, G. Grispos, Electronic retention: what does your mobile phone reveal about you?, International Journal of Information Security 10 (6) (2011) 337–349.

[149] A. Sengupta, C. Mazumdar, A. Bagchi, A formal methodology for detecting managerial vulnerabilities and threats in an enterprise information system, Journal of Network and Systems Management 19 (3) (2011) 319–342.

[150] M. Ahmed, E. Al-Shaer, M. Taibah, L. Khan, Objective risk evaluation for automated security management, Journal of Network and Systems Management 19 (3) (2011) 343–366.

[151] N. Cascarano, L. Ciminiera, F. Risso, Optimizing deep packet inspection for high-speed traffic analysis, Journal of Network and Systems Management 19 (1) (2011) 7–31.

[152] G. Dólera Tormo, G. López Millán, G. Martínez Pérez, Definition of an advanced identity management infrastructure, International Journal of Information Security 19 (2) (2012) 1–28.

[153] R. Costa, D. Carneiro, P. Novais, L. Lima, J. Machado, A. Marques, J. Neves, Ambient assisted living, in: 3rd Symposium of Ubiquitous Computing and Ambient Intelligence 2008, Springer, 2009, pp. 86–94.

[154] H. F. Rashvand, J. M. Alcaraz Calero, Distributed Sensor Systems, John Wiley and Sons, Ltd, 2012, Ch. Smart Sensing Architectures, p. 480.