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

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.

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

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.

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

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 privacypreserving 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.

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.