Advanced Access Control to Information Systems: Requirements, Compliance and Future Directives

Faouzi Jaidi

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.69329

Abstract

The swift cadence of Information and Communication Technologies (ICT) is at the origin of a new generation of open, ubiquitous, large-scale, complex, and heterogeneous information systems (IS). Inextricably linked with this evolution, a number of technical, administrative, and social challenges should be urgently addressed. Security and privacy in critical IS are recognized as crucial issues. The access control is well adopted as a typical solution for securing sensitive resources and ensuring authorized interactions within IS. The chapter deals mainly with the thematic of advanced access control to IS and particularly to relational databases. We present a synthesis of the state of the art of access control that encloses a study of research advancements and challenges. We introduce and discuss requirements and main characteristics for deploying advanced access control infrastructures. Then, we discuss the problem of the conformity of concrete access control infrastructures, and we propose a conformity management scheme for monitoring the compliance between low-level and high-level policies. Finally, we provide and discuss proposals and directives to enhance provably secure and compliant access control schemes as a main characteristic of future IS.

Keywords: information systems security, access control, database security, conformity, security policy

1. Introduction

Nowadays, Information and Communication Technologies (ICTs) developments bring out significant security concerns related to the deployment and operation of IS. In fact, in today's IS infrastructures characterized by their criticality, openness, complexity and heterogeneity (such as e-commerce, e-government, and e-health care), security and privacy are recognized as crucial issues. Ensuring a high level of security with a minimal overhead is the main goal of research activities. Among several security mechanisms, it is commonly agreed that the access control is a strong driving force and is well adopted as a typical solution for ensuring a high level of protection of critical infrastructures. This mechanism is fundamental to ensure higher confidentiality and integrity of sensitive data and services within IS. It helps in a structured manner—*generally enforced according to an access control policy with reference to a security policy*—to define and organize accesses and interactions within a specific system. The standing of the access control in the protection of critical resources has been well studied in literature. Several mechanisms, approaches, and models have been proposed to structure, specify, and enforce access rights. As a part of this chapter, we review in an exhaustive manner and discuss access control advancements. We highlight the evolution of access control infrastructures from traditional solutions to fine-grained solutions.

Despite the great advancements, several requirements and concerns need to be addressed for defining and setting up efficient and reliable access control infrastructures. Indeed, specifying and enforcing a trustworthiness access control infrastructure, ensuring its coherence, and monitoring its conformity have now become complicated and even puzzling activities. Moreover, it is commonly agreed that effective and proficient administration and management of access control infrastructures are recognized as main issues, while mastering these tasks is crucial as it would help to guarantee a higher security of IS. We study and discuss basic requirements for deploying advanced access control infrastructures. We discuss the problem of the conformity of concrete access control infrastructures, and we propose future directives to enhance provably secure and compliant access control schemes as a main characteristic of future IS.

The remainder of this chapter is structured as follows. In Section 2, we introduce and review access control advancements. In Section 3, we study and discuss main access control challenges for IS. In Section 4, we focus on advanced access control to IS. We study the main requirements for deploying advanced solutions, and we propose a compliance management solution. We present future directives to enhance provably secure and compliant access control schemes. Finally, Section 5 concludes the chapter.

2. Access control advancements: from traditional approaches to fine-grained access control

2.1. Introduction to access control

The access control is defined as any physical/logical mechanism by which a system controls and manages the access and the use of its resources. This mechanism allows the system to grant or revoke privileges for active entities (subjects) to access to or to perform some actions on passive entities (objects). The mechanism is also identified as authorization service or reference monitor that generally enforces access control policies.

An access control policy—*in general defined in the context of a security policy*—corresponds to the sets of rules and practices that regulate within a specific system how different resources (data and services) are operated, managed, and distributed. A security policy has to identify for a specific system the security objectives and the associated threats [1]. The policy acts mainly on three levels or aspects: administrative, physical, and logical. In the administrative level, we focus on the organizational security and the corresponding administrative procedures within the organization. In the physical level, we need to define the necessary procedures and means to protect the set of resources from physical risks and accesses. Finally, in the logical level, we define legitimate and authorized actions a user can perform. This level contains a set of security mechanisms such as the identification, authentication, and access control.

2.2. The generic model of access control

The generic model to control access to resources in the context of databases (as an example) is defined according to **Figure 1**. (**1**) A subject (an active entity) requests access to a database object (a passive entity) to perform some actions. (**2**) The authorization service checks the set of rights granted to the subject by the defined access control policy. (**3**) Then, an access decision (grant or revoke) is accorded to the subject.

2.3. Access control models

The emphasis on access control for ensuring high protection of critical infrastructures has been extensively justified in literature. The three main reference models have been defined: discretionary, mandatory, and role-based access control (RBAC) models. The wide deployment and great success of the standard role-based access control model have initiated several research works leading to the definition of advanced models for a fine-grained access control.

2.3.1. The discretionary access control (DAC) model

The discretionary access control (DAC) model has appeared mainly with Lampson [2] in the 1970s who defined the structure of the access control matrix based on the subject, object, and action notions. The model allows to restrict the access to objects on the basis of the identity of the subjects and/or the groups of subjects. In the DAC model, the owner of a specific resource fixes itself the access rights to the resource for all users of the system. Moreover, a subject who has an access authorization is able to pass this permission (perhaps indirectly) to other

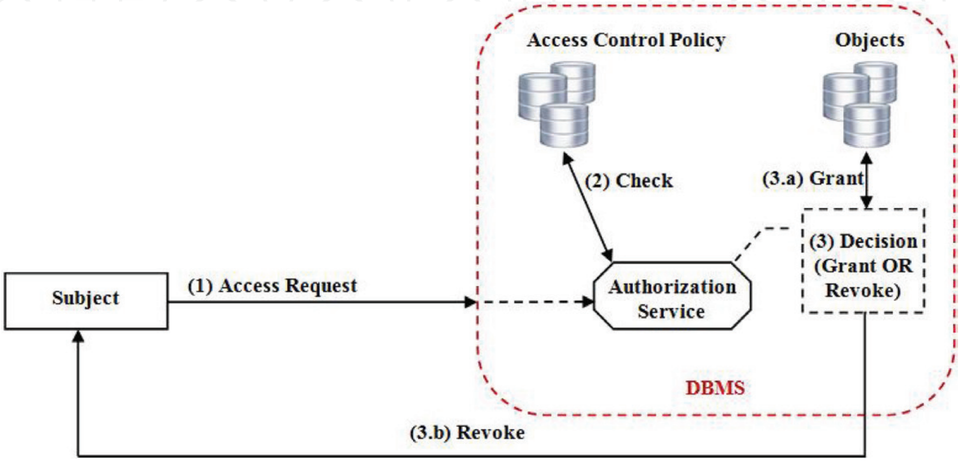

Figure 1. The generic model of access control.

subjects. The controls are discretionary in the sense that the management of access rights is left to the discretion of the users.

2.3.2. The mandatory access control (MAC) model

The mandatory access control (MAC) [3, 4] model controls access to resources on the basis of the notion of security level. It associates a confidentiality level to each subject and object. The set of subjects and objects is classified according to corresponding confidentiality levels, and authorized actions are derived based on associated levels. In this model, the system manages directly user rights based on the corresponding security information (confidentiality levels) assigned to users and objects. This model was motivated by the need of providing higher security by preventing unauthorized accesses and protecting resources from Trojan horses.

2.3.3. The role-based access control (RBAC) model

The role-based access control (RBAC) model [5, 6] controls access to resources on the basis of the concept of roles assigned to users. A role represents a function within an organization. The model defines access rights to resources based on the roles assigned to users. A variety of RBAC conceptual models had been defined. The core model (noted $RBAC_0$) defines, for any system, the minimum requirements to support the access control based on roles. The *hierarchical RBAC* (noted $RBAC_1$) extends RBAC_0 with the concept of role hierarchy. The *constrained RBAC* (noted $RBAC_2$) extends RBAC_0 with the notion of constraints. Constraints are a set of restrictions defined on RBAC components, such as static separation of duty, dynamic separation of duty, prerequisite, and cardinality constraints. The global model called *consolidated model* (noted $RBAC_3$) contains both of the hierarchy and the constraint concepts. It includes RBAC_1 and RBAC_2 models and consequently the RBAC_0model.

2.3.4. Fine-grained access control (X-BAC) models

To structure access rights and to meet specific application needs, numerous extensions have been proposed for the RBAC family, called X-based access control models. The ORBAC [7] model represents a main extension defined as a conceptual and industrial framework to meet security needs for sensitive healthcare communications. RBAC+ is a dynamic model to enforce fine-grained access control to web databases. The model extends the standard model with the notions of application, application profile, and sub-application session. The GEO-RBAC [8] model has been proposed to take into account spatial contextual information. It is motivated by security requirements of location-based services and mobile applications as well as the increased concern for the management and sharing of geographical information in strategic applications like environmental protection and homeland security [8]. The temporal RBAC and the generalized temporal-RBAC extensions [9] are defined to take into account temporal contextual information and to constrain the use of permissions to specific temporal periods. Several other extensions that define the concepts of teams (Team-BAC), tasks (task-LAC), lattice (Lattice-LAC), organizations (Organization-BAC), or contexts (Context-LAC) have been also defined to structure rights. The concept of attribute-based access control (ABAC) organizes access based on the evaluation of attributes. RBAC extensions are defined for a fine-grained access control policy specification to meet new security challenges.

Content-based access control is a particular case of fine-grained access control specific to database systems. In this type of access control, access decisions (to authorize or to deny an access request) are based mainly on the content of the data to be accessed.

2.4. Synthesis

The main discretionary access control model expressed through access matrices has been widely used and implemented in several applications in the commercial and academic fields, such as in Unix/Linux operating systems. Nonetheless, the management of permissions list is tedious and prone to errors in the case of a large number of users and permissions. Moreover, this model is difficult to administer in the case of large infrastructures and is vulnerable to Trojans.

In order to improve and strengthen access control to critical resources, several research works gave rise to other models, mainly the MAC model based on the definition and exploitation of security levels. In this context, the early defined approaches have proposed to organize the set of security levels in a strict order. Then, the obligation to refine and relax this constraint made it possible to organize the security levels according to lattices. The notion of lattice allows structuring the security levels according to a hierarchy that gives more freedom to administrators in the modeling of access control policies. This makes the MAC models well adapted to highly structured IS that require a high confidentiality, namely, military systems or sensitive enterprise systems. However, in the case of large-scale organizations, it is too rigid to apply the MAC model since it is difficult to classify a huge number of objects and subjects in a predefined number of security levels. Moreover, database management systems (DBMS) that adopt only the MAC model as a unique access control solution had a little commercial success due to their rigidity and the strict hierarchy they impose on users and objects.

Even though historical access control models have introduced the concepts and generic principles of access control, the concern to impose strict access control rules has led to the definition of the notion of structured intermediate levels between subjects and permissions. The general principle of the new models is to introduce a new level of indirection (defined by roles) between users and permissions. The main purpose of this new concept is to facilitate the administration of access control policies. Indeed, in role-based access control models, it is not necessary to update the whole access control policy when adding a new subject (user), and it is sufficient to assign it rights through one or more roles. Thus, the use of this intermediate entity (role) reduces considerably administrative errors and contributes to master difficulties and complexities in the management of access rights through the mechanism of inheritance between roles. This model of access control has received a particular attention by the research community and has become in its simplest or most complex form the most used model [10]. This huge success has made from this model a standard for access control [11]. This led to the elaboration of multiple models and derivations for this family of access control named X-BAC for the definition of a fine-grained access control.

In order to highlight the main advancements of access control, we present in **Table 1** a comparative study and analysis of the discussed access control models and mechanisms with reference to their approaches, applications, and capabilities.

From a security perspective, we present in **Table 2**, a summary of security analysis of the discussed access control models and mechanisms that identifies the relative strengths and weaknesses of existing approaches and their security vulnerabilities.

Features	**DAC**	**MAC**	**RBAC**	**Fine-grained models (exp. ABAC)**
Context of application	Commercial and academic fields: Unix/Linux operating systems	Suitable to highly structured IS: military systems and intelligent environments	Various IS	Specific to particular applications
Implementation	Access control matrix\access control and capability lists	Security levels for subjects and objects	Roles and authorization constraints	Specific mechanisms (exp. ABAC: attributes)
Sensitivity	No fine-grained access control	No fine-grained access control	No fine-grained access control	Fine-grained access control specific to particular applications
Policy updates	The policy update is costly	The policy update is costly	The policy update is simple	The policy update is simple
Policy management and administration	Tedious management, prone to errors, and difficult to administer	Requires a higher management to account and update security levels	Easier than previous models	Easier than previous models
Advantages	Flexibility of usage Enforces the sharing of information	Multilevel security Ensures higher integrity Well-adapted to highly structured IS	Includes the advantages of historical models Intermediate levels between subjects and permissions Hierarchy of roles and constraints Adapted to complex and distributed areas	Fine-grained controls Respond to specific access control needs Solve RBAC limits Focus on other concepts than roles (exp. attributes in ABAC) Higher flexibility Adapted to complex, distributed, open, and dynamic areas
Disadvantages	Problem of scalability No distinction between users and subjects Security problems	Too rigid to apply Problem of scalability	Not suitable to dynamic environments Static access control Requires roles engineering Does not support contextual rules	Difficulty in compliance management More complex to implement than RBAC

Table 1. Comparative study of access control models.

Features	**DAC**	**MAC**	**RBAC**	**Fine-grained models (exp. ABAC)**
Performance and integrity	Low: possibility to settle insecure rights	High: based on security level	High	Very high
Access decision	Ownership	Centralized	Centralized	Centralized
Vulnerability	Vulnerable to malicious programs such as Trojan horses and covert channels	Vulnerable to covert channels	Vulnerable to inner threats, particularly administrative threats	Vulnerable to inner threats, particularly administrative threats
Flexibility	Flexible	Rigid	Flexible	Higher flexibility
Security separation of duties	Does not support	Does not support	Static and dynamic separation of duties	Static and dynamic separation of duties
Constraints and conditions	Does not support	Does not support	Constraints and condition enforcement	Constraints and Conditions enforcement
Inference (indirect access)	Fail to deal with inferences	Fail to deal with inferences	Fail to deal with inferences	Requires specific study to each model
Transitivity	No control on transitive access flow	Transitivity is controlled	Transitivity is controlled	Transitivity is controlled
Least privilege and delegation of rights	Supports	Does not support	Supports	Supports

Table 2. Security analysis of access control models.

3. Access control to databases

3.1. Mechanisms

In a database context, a number of mechanisms can be enforced in a cooperative manner for ensuring the control of legitimate accesses and preventing unauthorized accesses. The diversity of access control mechanisms for database systems illustrates on the one hand the importance of the access control for protecting sensitive data and services and on the other hand the difficulty and the complexity of defining a reliable access control solution. We present in the following a list of the principal access control mechanisms for database systems.

- *Passwords*: a database management system allows to associate passwords for the identification of users and to enforce passwords for the activation of roles.
- *Privileges*: a database management system allows defining a set of privileges for managing the empowerment of users. It provides system privileges and object privileges that allow users performing specific actions across the system and accessing database objects.
- *Views*: a view represents an important and very useful mechanism for restricting access to data. It is a most common mechanism adopted by database management systems to support content-based access control.

- *Triggers*: triggers allow to automatically enforce access restrictions as well as security rules. They especially allow enforcing authorization constraints mainly pre- and post-authorization constraints.
- *Stored* procedures: stored procedures may be used in order to define privileges associated with a user's job functions and to ensure that access to data and services are performed according to the defined rules.
- *Encryption mechanisms*: a number of encryption mechanisms contribute to access control for databases. They concern several applications, such as password encryption, data encryption, digital signature, authorization tickets, etc.
- *Access control policies*: it consists on enforcing access control policies based on different models such as DAC, MAC, RBAC, etc. Indeed, database management systems provide mechanisms based on different access control models allowing the management of access rights.
- *Specific mechanisms*: this type of mechanisms is context dependent and specific to every DBMS. As an example, we cite the component Oracle Database Vault that allows restricting access to sensitive data even for database administrators.

3.2. Policy enforcement

In a database context, enforcing an access control policy consists in deploying within a database system, generally in a distributed manner, the schema of the access control policy. This distribution of the policy between different active components of the system ensures a better management of access requests and operations of the database resources. In fact, an access control policy is often spread over several levels. (i) The first level is defined by the database management system itself. Indeed, a DBMS makes it possible to define and store in its depository (data dictionary) a set of information and access rules allowing it to control and manage access to data. (ii) The second level is defined by application servers that allow restricting access to applications and data. (iii) The third level is relative to the application part. Indeed, the software application can manage itself the level of accreditation of users, and it connects to the database under its own logical identity and decides which information the users can consult, modify, etc. (iv) The fourth level belongs to the set of privileges associated to different actors of the system and defined in the directories of users and operating systems of the IS.

3.3. Challenges

Even though, the access control is becoming increasingly important for protecting sensitive data in critical systems; several issues are recognized as crucial challenges in today's access control infrastructures. In fact, the efficient and secure administration and management of access control infrastructures, the safety analysis of access control models, and the risk assessment in access control systems are recognized as fundamental issues. Moreover, setting up a trustworthiness environment of access control and monitoring its compliance and coherence have emerged as complicated and confusing tasks. Indeed, in unreliable and untrustworthy environment, the administration of access control policies considered as a fundamental security aspect generally raises a critical analysis problem when the process of administration is distributed and/or potentially untrusted users contribute to this process. As a consequence, collusion attempts and inner threats may take place to generate crucial and invisible breaches to circumvent the access control policy. Moreover, an administrator via its administrative privileges has power increasingly disputed when the safety of data is threatened [12]. Given that administrative roles are naturally powerful, if they are not used in cautious manner, a malicious administrator or a powerful user can corrupt the policy and create other breaches difficult to identify.

In database context, most of existing DBMS use the *closed-world policy* as a main authorization model. Under this circumstance, whenever a user tries to access a database object and no authorization rule is found, the access is denied. Hence, the lack of authorizations is interpreted as no authorization. Nonetheless, this policy has a major drawback since it does not prevent the user from receiving the required authorization some times in the future [13]. Moreover, most of existing DBMS act as a *black box*, and it is difficult for administrators and security architects to identify the actual state and the compliance level of the concrete policy enforced by the DBMS. Recently, researchers are convinced of the urgency of this topic given the challenges of securing data. A few attempts addressed the topic of reverse engineering of access control policies to externalize the low-level schema of an access control policy enforced by a relational DBMS [14, 15].

4. Advanced access control

Advanced access control solutions should provide an efficient and flexible access control with a reasonable (minimal) overhead for ensuring a higher protection of private data and sensitive resources. From a security perspective, we consider that a reliable and trusted access control infrastructure for future information systems should take into account several requirements and should provide a minimum of security features.

4.1. Requirements

4.1.1. Confidentiality and integrity

In critical systems, it is compulsory to consider and treat sensitive data and services as confidential resources which integrity should be preserved. In this context, the confidentiality and the integrity of the IS resources must be preserved, and a main requirement for the access control system is that it should not allow in any way illegal accesses and unauthorized exploitation of the system resources.

4.1.2. Privacy

In open and untrustworthy environments, preserving the privacy of different users and actors in a critical system is highly required. The access control solution should consider the protection of private data as well as the preservation of a high level of secrecy as main objectives.

4.1.3. Authenticity

The authenticity of the actors of the system is an important aspect that needs to be taken into account by the access control solution. Ensuring the authenticity in the system relies principally on the validation of the origins and the identities of the different actors of the system. In order to ensure a high level of authenticity, the access control system should dispose of reliable identification and authentication mechanisms such as cryptographic and digital signature.

4.1.4. Robustness

The access control system must ensure a high level of robustness in the sense that inappropriate and unauthorized accesses should not be expected. The access control rules have to be rigorous enough to authorize desired accesses and prevent illegal accesses. The robustness of the access control as a crucial question is described with the levels of confidentiality and privacy provided by the system.

4.1.5. Flexibility

In critical infrastructures, such as healthcare and commercial systems, emergency accesses should be preserved by the access control system. In this case, the access control system must integrate flexible controls as regards to emergency cases. The flexibility needs to be integrated in a smooth and transparent manner to permit emergency accesses based on a delegation of rights or an overriding of access privileges.

Moreover, revoking access privileges is an important aspect that should be considered by access control solutions. Indeed, the access control system should be flexible in the sense that it should allow revoking access rights in an easy manner especially in critical situations when users abuse the trust and threaten the IS.

4.1.6. Non-repudiation

In order to pass up incidents linked to user's irresponsibility and negligence, it is recommended that the access control system has to integrate non-repudiation mechanisms such as auditability. This helps mainly in auditing illegal access and collusion attempts that allows strengthening the system with the corresponding prevention rules and controls.

4.1.7. Administration, management, and compliance

An access control system has to remain compliant and coherent with regard to the validated requirements without alterations. The necessity of integrating flexible controls in the system should not be at the origin of the non-compliance situations. In this context, we verify that a secure and efficient management of the access control infrastructure is a main requirement that has a wide impact on the quality of the system. Indeed, a faulty access control policy, a miss-configuration of the policy, or flaws in the policy and system deployment can result in serious vulnerabilities. A reliable management helps to precisely capture the security properties and needs that access control should adhere to bridge the gap of abstraction between the access control policy and the corresponding mechanisms.

4.2. Compliance management

The traditional life cycle of an access control policy defines three main phases: the specification, the verification, and the implementation of the policy. Then, the policy evolves with reference to maintenance and administrative tasks, following the evolution of security needs. Throughout its life cycle, the policy can undergo confused alterations: (i) It may record illegal updates and non-compliant changes with regard to its original specification. This generally occurs following an intrusion attempt or an illegal delegation of rights. (ii) It may contain incoherent and conflicting access control rules. This generally occurs following inner threats and collusion attempts and particularly in case the policy is defined by using more than a unique model of access control that leads to redundancy, inconsistency, and contradiction in the expression of the policy. We consider that the identification of the discrepancies between the abstract level of the access control policy (the specification) and its concrete level is crucial since correct operation and enforcement of access control policies by corresponding applications rely on the hypothesis that the specifications are correct and valid.

In large-scale, open and untrustworthy environments, the administration and management of an access control policy (considered as main security aspects) generally raise a critical analysis problem in case of a distributed administration of the policy, and/or potentially untrusted users (in most cases represent malicious administrators) contribute to the administration process. As a consequence, collusion attempts and inner threats may take place to generate crucial and invisible breaches to circumvent the policy. In fact, a faulty access control policy, a miss-configuration of the policy, or flaws in the policy and system deployment can result in serious vulnerabilities. In a database management system (DBMS) context, we easily check that as business and private data is exposed to several security threats and attacks, an access control policy is also subject to the same dangers [16]. According to *Imperva Application Defense Center* reports in 2013 and 2015, *Excessive and Unused Privileges* and *Privilege Abuse* are identified as most critical threats in top 10 database security threats.

Moreover, in the context of healthcare and e-healthcare systems (as a typical critical infrastructures), access control solutions should be rigorous to ensure a higher protection and flexible to treat emergency cases. We check that the simultaneous coupling of two necessary but contradictory objectives (robustness and flexibility) has a direct influence and a wide impact on the compliance of the deployed access control policy [17].

Our proposal to address issues related to the deployment and management of access control policies extends the traditional life cycle of access control policies with pertinent phases that we consider as necessary activities for ensuring the trustworthiness and the compliance of security policies. We consider three main levels of compliance management of access control infrastructures like illustrated in **Figure 2**. The first level concerns the management of the conformity between security and functional needs and the specification and design of the access control system. Indeed, a main requirement in the deployment of the access control infrastructure is specifying security and business needs, mastering, and validating its basics and expressiveness. Then, evolving the policy according to new security and business needs is highly required to maintain coherence between security needs and the high-level policy.

The second level concerns the management of the compliance between the specification of the policy and its concrete implementation. This level ensures the identification of faulty access control policy, miss-configurations or flaws in the policy and the system that can result in serious vulnerabilities. To ensure a high level of trustworthiness, it is highly recommended to proceed with verifying the conformity between the specification and the first implemented instance of the policy and particularly before the concrete exploitation of the system. The third level concerns the management of the compliance between the high-level policy as a reference model and any concrete instance of the policy. This helps detecting illegal updates and non-compliant changes in the concrete instance with regard to its original specification. It allows also identifying incoherent and conflicting access control rules occurred following inner threats and collusion attempts.

To ensure an efficient and secure deployment and management of reliable access control policies, we cover three key security aspects like illustrated in **Figure 3**. (i) The specification, verification, and implementation of the policy invariants, (ii) the validation of a concrete (implemented) instance of the policy regarding its original specification, and (iii) the adjustment and optimization of the access control policy schema. In fact, the goal during

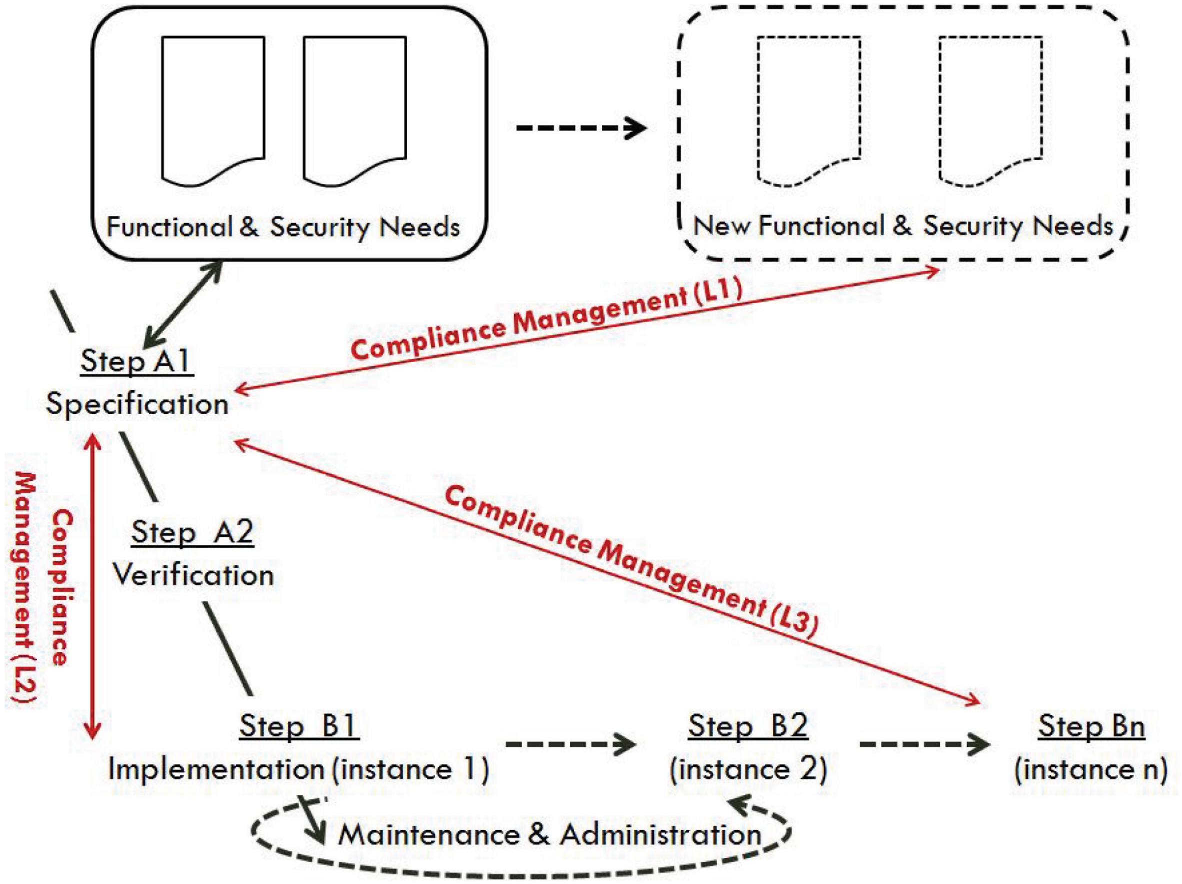
Functional & Security Needs
New Functional & Security Needs
Compliance Management (L1)
Step A1
Specification
Compliance Management (L2)
Step A2
Verification
Compliance Management (L3)
Step B1
Implementation (instance 1)
Step B2
(instance 2)
Step Bn
(instance n)
Maintenance & Administration

Figure 2. Compliance management levels.

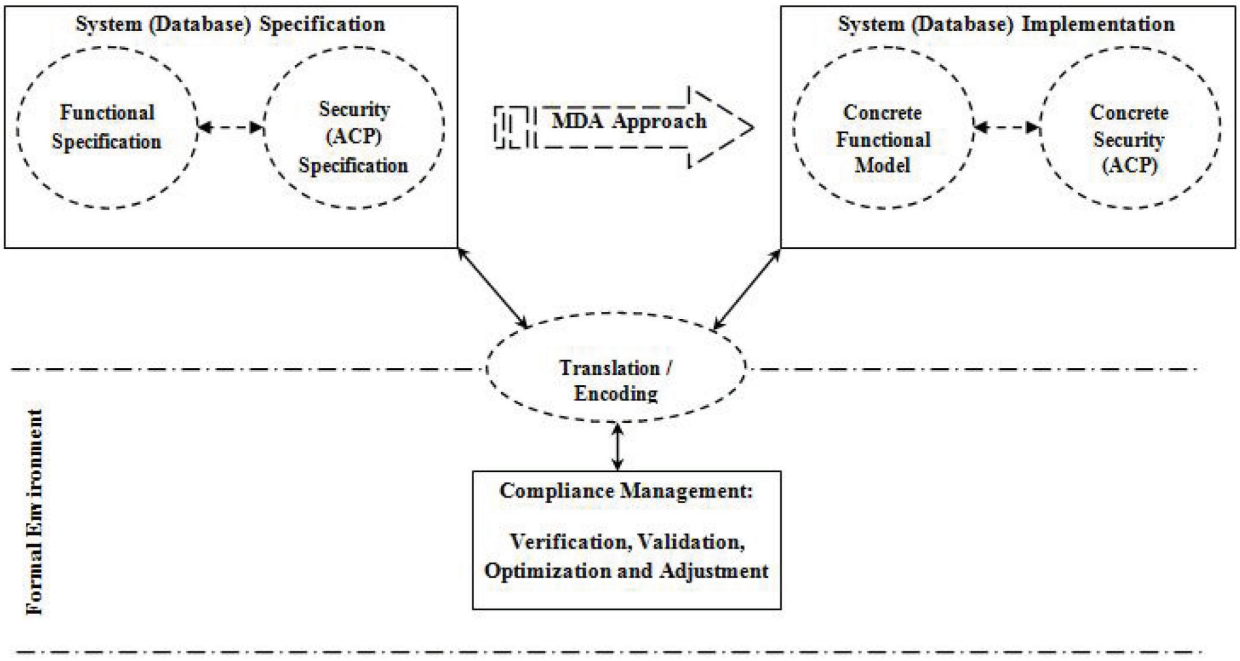
System (Database) Specification
Functional Specification
Security (ACP) Specification
MDA Approach
System (Database) Implementation
Concrete Functional Model
Concrete Security (ACP)
Translation / Encoding
Compliance Management:
Verification, Validation, Optimization and Adjustment
Formal Environment

Figure 3. Formal approach of compliance management.

the specification phase is to capture the maximum of security needs and to distinguish the invariants that must meet any concrete instance of the access control policy. *Security architects* dispose, during this phase, of security modeling languages that extend classical application modeling languages. Verifying the exactitude of the specification and adopting a *model-driven architecture* (MDA) approach are highly interesting in system development and allow especially reaching the implementation via successive refinements of the verified specification. During the validation phase, the reference stage (the specification) and the concrete instance are facing in a logical framework allowing formal reasoning and compliance demonstration. To do so, two preliminary phases are necessary: a reverse engineering phase that allows generating the schema of the implemented policy and a formalization phase for representing the extracted policy in our formal framework. The optimization phase corrects the redundancy anomalies and helps check the properties of the graph of roles, calculate the power of a role, etc. Obtained results allow the adjustment and the up to date of the corresponding policy.

4.3. Future directives

4.3.1. Compliance management of distributed policies

Today's IS generally comprises several heterogynous components. Securing the IS requires mainly defining and enforcing a global security policy to be distributed on several active components that participate—in a collective manner—to the system security. The *security architect* is responsible for defining a global access control policy (GACP) and for defining the sub-policies (ACP_1, ACP_n) relative to each active component in the system such as firewalls (FW), database management systems (DBMS), application servers (AS), operating systems (OS), enterprise directory services (LDAP), etc.

A global management of the compliance of the global access control policy enforced by the IS consists in monitoring the conformity of all sub-access control policies enforced by active components separately and in verifying the conformity of the global policy taking into account the interactions between those components, like illustrated by **Figure 4**. As a future research direction, a global compliance management process—which integrates compliance management of sub-policies—should be defined and investigated for a global check of the conformity of the global policy taking into account interactions between active components of the system.

4.3.2. Reverse engineering access control policies

The management of the compliance of access control policies within databases relies on a reverse engineering step for externalizing the concrete implementation of a policy from the DBMS. In literature, numerous research works addressed the thematic of retro-conception or reverse engineering in the context of relational databases. This was at the origin of the development of professional tools for databases reverse engineering. Existing tools allow to generate the functional model of a concrete database, while they do not allow to generate the complete security model. In other words, they do not offer the opportunity to extract all the components of persistent access control policies. The reverse engineering procedure is based on the exploitation of the DBMS data dictionary.

Actually, a few research works addressed this important topic and defined reverse engineering techniques for extracting concrete policies from the Oracle DBMS [14, 15]. Even though,

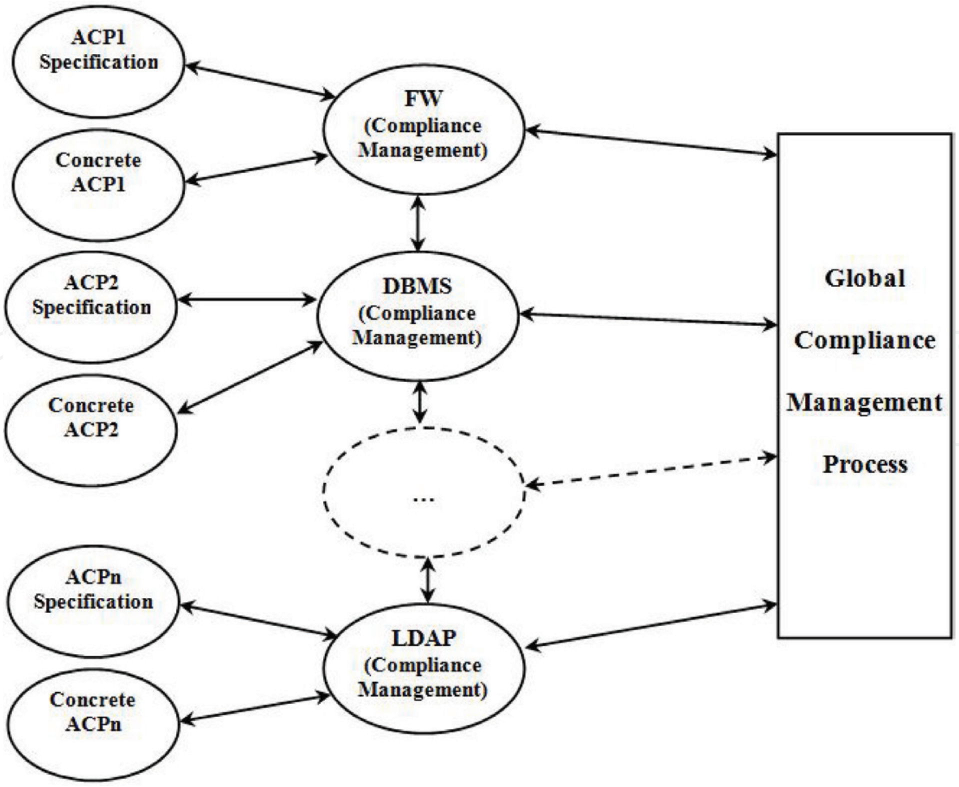

Figure 4. Distributed compliance management.

defined reverse engineering approaches can be generalized, we need specific reverse engineering procedures relative to each DBMS. A main contribution in this thematic is to define specific reverse engineering techniques relative to other familiar database management systems such as Informix, MySQL, etc.

4.3.3. Compliance management of access control policies in the context of object and NoSQL databases

The fact that the concepts and principles of object-oriented and NoSQL databases are completely different from traditional databases (mainly relational databases), the application of traditional security controls is not adequate for providing effective security measures for object-oriented and NoSQL databases. Due to the specificity of object databases, we need—in a future research directive—to define the necessary techniques for monitoring the compliance of implemented access control policies in object-oriented DBMS.

5. Conclusion

Addressing security issues in today's information system requires mainly defining a trustworthy environment of access control. In this chapter, we review the actual state of research in access control to highlight the main advancements and challenges. We introduce and discuss requirements and the main characteristics for deploying advanced access control infrastructures. We illustrate that the management of the compliance of today's access control infrastructures represents a main issue for the deployment of secure systems. To address this thematic, we discuss the problem of the conformity of concrete access control infrastructures, and we propose a conformity management scheme for monitoring the compliance between low-level and high-level policies. Moreover, we highlight some future research directives that comply with the discussed thematic.

Author details

Faouzi Jaidi

Address all correspondence to: faouzi.jaidi@gmail.com

Digital Security Research Unit, Higher School of Communication of Tunis (Sup'Com), University of Carthage, Tunisia

References

[1] Rihaczek K. The harmonized ITSEC evaluation criteria. Computers and Security. 1991; **10**(2):101-110

[2] Lampson BW. Protection. ACM SIGOPS Operating Systems Review. 1974;**8**(1):18-24

[3] Bell D, LaPadula L. Secure Computer Systems: Unified Exposition and Multics Interpretation. MTR-2997 ed. Bedford, MA: Mitre; 1975

[4] Denning DE. A lattice model of secure information flow. Communications of the ACM. 1976;**19**(5):236-243

[5] Cenys A, Normantas A, Radvilavicius L. Designing role-based access control policies with UML. Journal of Engineering Science and Technology Review. 2009;**2**(1):48-50

[6] Sandhu R, Coynek EJ, Feinsteink HL, Youmank CE. Role-based access control models. IEEE Computer. February 1996;**29**(2):38-47

[7] Abou El Kalam A, El Baida R, Balbiani P, Benferhat S, Cuppens F, Deswarte Y, Miège A, Saurel C, Trouessin G. Security models and policies for health and social information and communication systems. In: IEEE 4th International workshop on policies for distributed systems and Networks (Policy 2003); June 2003. Lake Come, Italy: IEEE; 2003

[8] Bertino E, Ghinita G, Kamra A. Access Control for Databases: Concepts and Systems. 3, 1-2. Foundations and Trends® in Databases; 2010. 1-148

[9] Bertino E, Bonatti PA, Ferrari E. Trbac: A temporal role-based access control model. ACM Transactions on Information and System Security. 2001;**4**(3):191-233

[10] Albain T. L'insuffisance du modèle RBAC [Internet]. Available from: http://www.journaldunet.com/solutions/expert/50225/l-insuffisance-du-modele-rbac.shtml [Accessed: 2016]

[11] Sandhu R, Ferraiolo D, Kuhn R. The NIST model for role-based access control: Towards a unified standard. In: Proceedings of the 5th ACM Workshop on Role-based Access Control, Berlin, Germany; ACM, 2000. pp. 47-63

[12] Jaidi F, Labbene Ayachi F. The problem of integrity in RBAC-based policies within relational databases: Synthesis and problem study. In: ACM, editor. The 9th International Conference on Ubiquitous Information Management and Communication ACM IMCOM (ICUIMC); Bali, Indonesia; ACM; 2015. p. 21

[13] Bertino E, Sandhu R. Database security – concepts, approaches and challenges. IEEE Transactions on Dependable and Secure Computing. 2005;**2**(1):2-19

[14] Jaidi F, Labbene Ayachi F. A reverse engineering and model transformation approach for RBAC-administered databases. In: IEEE, editor. 13th International Conference on High Performance Computing & Simulation, HPCS 2015; Amsterdam, Netherlands, IEEE; 2015

[15] Martinez S, Cosentino V, Cabot J, Cuppens F. Reverse engineering of database security policies. In: Proceedings of 24th International Conference on Database and Expert Systems Applications; Springer Berlin Heidelberg; 2013. pp. 442-449

[16] Jaidi F, Labbene Ayachi F. An approach to formally validate and verify the compliance of low level access control policies. In: Proceedings of 2014 IEEE 17th International Conference on Computational Science and Engineering (CSE); Chengdu China, IEEE; 2014. pp. 1550-1557

[17] Jaidi F, Labbene Ayachi F, Bouhoula A. Advanced techniques for deploying reliable and efficient access control: Application to E-healthcare. Journal of Medical Systems. 2016;**40**(12):262