Trust Management Approach for Securing the Services Access: Telecom Operators Collaborations in IMS Network

Nawal Ait Aali, Amine Baina and Loubna Echabbi

Laboratory of Telecommunications Systems, Networks and Services
National Institute of Posts and Telecommunications (INPT), Rabat, Morocco
E-mail: aitaali@inpt.ac.ma; baina@inpt.ac.ma; echabbi@inpt.ac.ma

Received 10 December 2018; Accepted 03 September 2019;
Publication 13 September 2019

Abstract

IP Multimedia Subsystem (IMS) network presents a new generation in the telecommunication infrastructure by providing a variety of services whatever the used technologies. Therefore, to make the customers satisfied, their telecom operator provides them several services according to their attached user profile (subscription type). However, some services are not hosted by the home operator; the service providers are responsible to present these services to the customers. In this case, the operator contacts the concerned provider for requesting the access to the desired services. In fact, this access may arise some security issues which affect the customer privacy and the services security. In this paper, we project our approach, Tr-OrBAC, in the context of collaboration between service providers and telecom operators. We discuss the case when the customer wishes to access to a service hosted by an external service provider. We present the encountered security problems. Then, we depict and we detail the functioning of our approach to resolve these problems.

Keywords: IMS network, trust management, collaboration, trust criteria, privacy, telecom operator, service provider, decision making, AHP.

Journal of Mobile Multimedia, Vol. 15_1&2, 51–70.
doi: 10.13052/jmm1550-4646.15123

1 Introduction

From the emergence of the Information and Communication Technologies until the next generation [1], there has been a real revolution in regards to the services offered to people around the world. This revolution is characterized by a set of technologies that will ensure the communication between the social actors (individual and collective) and their contact with the outside world (local, national and international). In this context, the telecoms operators have appeared, their main concern is to make their customer satisfied by offering them several services. Among these services, we cite:

- Stay connected to the Internet at high speeds due to the appearance of new generations (3G, 4G…) [2, 3];
- Continue to access to the desired services (calls, messaging, connection, file transfer, streaming, conference…) offered by the Home Operator or a Service Provider;
- Maintain the communication with other customers when moving in several places without any interruption (roaming) [4].

Moreover, the customers don't benefit the same services (it depends on the type of their subscription with their operator) and they don't belong all to a single telecom operator. Also, each customer chooses a type of access network (UMTS, GSM, Ethernet, WI-Fi…) that depends on his/her needs and requirements without forgetting that he/she has a wide selection of terminals; we talk about smart phones, laptops, tablets, TVs, digital phones and also the traditional analog phones…. This diversity of the used terminals, the offered services and the access networks arose to the customers some problems concerning the management of communications when different technologies are used. To solve this problem, a group of telecommunications companies were released a new technology: It is the ***IMS (IP Multimedia Subsystem)*** network [5].

The objective behind the creation of IMS network is the convergence to a single architecture, which facilitates to different customers the access to several services, regardless of their access networks and their used terminals. These services are hosted by the telecom operator as their providers. When they are not available at the home operator, this latter asks the access from the provider. To achieve the customer access to the desired service, a set of transactions [6] is required between the home operator and the service provider by creating a collaborative system. This collaboration can produce serious results in terms of security; firstly, the sensitive and personal data of different customers may be shared, and then they may be reused illegally. Secondly, the customer who asks the service access can commit unethical behaviors when accessing to the desired service. In this context, the security of the information customers and the protection of desired services become a necessity. We face, thus, a big challenge, how can we secure the resources and services that are accessed by external customers? How can we ensure successful collaboration between the telecom operators and the service providers by respecting their requirements and constraints? And how can we respect the privacy and the confidentially of different customers asking the services access?

In this paper, we focus on presenting the security challenges in different stages: (1) establishing collaboration, (2) controlling access to different services and resources, (3) respecting the customer privacy, (4) managing and evaluating the reliability of the customers who ask the access. Thus, we present our trust model: Tr-OrBAC [7]; It was developed mainly to ensure the security of the collaborative systems within Critical Infrastructures (CI) [8]. In particular, we focus on this article to present and interpret how this model is practical in the IMS network security and especially in the context of collaboration between the telecom operators and the service providers.

Before presenting the application of our model in the IMS network security, some points must be discussed and presented. Therefore, the rest of this paper is organized as follow: In Section 2, we present the IMS architecture and its different layers, also the followed process to access to the services. Section 3 details several security requirements, according to the collaboration context in the IMS network and then we discuss some previous works. The Section 4 is reserved to recall the principle of our approach Tr-OrBAC and presents the different preliminaries constituting the proposed solution. While our objective is to secure the collaboration in the IMS network, we focus, in the Section 5, on demonstrating and interpreting the feasibility of our approach in the IMS network. For this purpose, we present a concrete example of collaboration between the telecom operator and the service provider. At the end, the Section 6 is dedicated to conclude the paper and present our perspectives.

2 IP Multimedia Subsystem (Ims) Network

In this section, we present the IMS architecture and its different layers, then, we detail the process of the services access by a customer by detailing different steps and the role of several IMS entities.

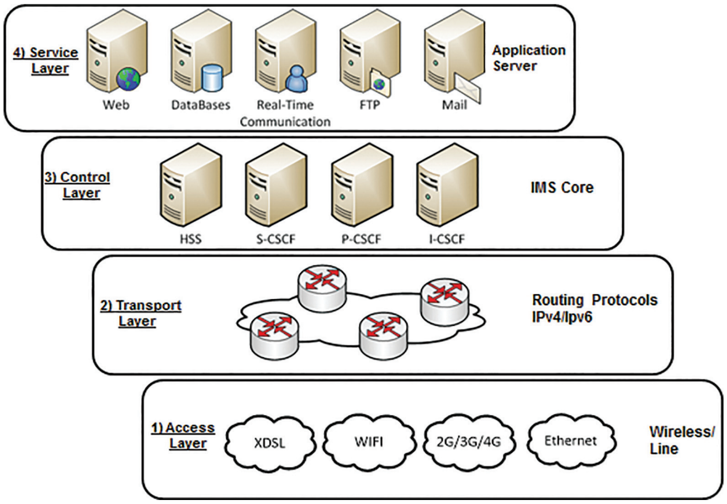

Figure 1 IMS architecture.

2.1 Presentation and Architecture

As previously presented, the objective of the IMS network is to provide multimedia services to customers, independently of the access network and terminals that are used by these customers. To achieve this goal, the IMS architecture consists of four layers [9]: physical layer (access), transport layer, session layer (control) and application layer. Each layer has its functionalities, entities and protocols . . . we present this architecture briefly from the bottom to top as described in Figure 1.

Access Layer: The first layer in the IMS architecture is the access layer; it presents a key element that ensures the connectivity of the customer with the IMS network. Also, it contains a set of access networks allowing customers to choose how to connect to the network by using a terminal of their choice.

Transport Layer: This layer is responsible for the transport of data between different customers. It is based on IP protocol (IPv4/IPv6).

Control Layer: In order to manage the different operations within the IMS network, a management and control layer is required. It is responsible for authentication, signaling, traffic transfer, access rights management. In order to perform all these operations, the presence of a set of entities is necessary, we talk about: ***HSS (Home Subscriber Server) and Call Session Control Function (CSCF)*** entities.

Service Layer: (Application Server): This layer contains several servers which provide to the customers the different multimedia services.

2.2 The Service Access Process

The customers subscribed to the telecom operators choose several services presented by their operator and they can access them according to their subscription type. However, they can request other services which are hosted by the service providers. In both cases, the validation of a set of steps is necessary in order to access to the desired service as shown in the Figure 2.

When the customer wants to access a service (1), first, he/she must authenticate in the network. To do this, the P-CSCF (Proxy CSCF) entity is used to interface the client and the network by establishing a connection (2). This entity (P-CSCF) sends messages from the customer to the I-CSCF (Interrogating CSCF) entity (3) which looks for the S-CSCF (Serving CSCF) to which the customer can connect (4). In this sense, the S-CSCF contacts the HSS

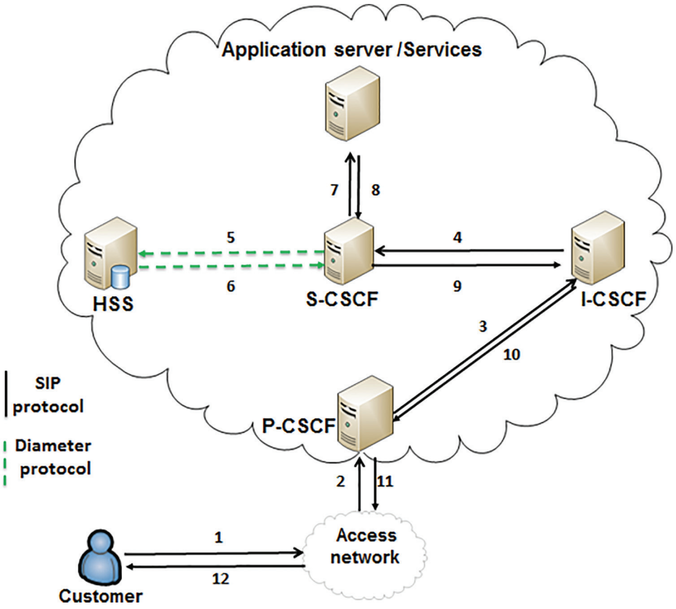

Figure 2 Service access process.

(Home Subscriber Server) database to retrieve customer information through the Diameter protocol (5, 6) in order to authenticate the customer, to verify his/her access rights and to provide him/her services (7) according to his/her user profile. Once the user profile is established, the response propagates in the opposite direction until the client (8, 9, 10, 11, and 12) who obtains an IP address and can access to the desired service.

We note that the Diameter Protocol is used to ensure the communication between HSS and S-CSCF while the SIP (Session Initiation Protocol) is used between the CSCF entities and between the S-CSCF entity and the application Server.

The IMS architecture is therefore rich in terms of entities, functionalities, protocols and roles. This variety of components and functionalities requires the establishment of a security system enabling both the security of services and the confidentiality of customer data. In this context, we present in the next section the different security requirements, according to the collaboration between the operators and the services providers.

3 Security Requirements in the Collaborative Systems Within IMS Network

3.1 Security Requirements and Needs

The Telecommunication Infrastructure, as well as any Critical Infrastructure, is based on the establishment of collaboration (collaborative systems) between telecom Operators and Service Providers in order to present the desired services to the customers. As we have presented in our previous paper [10], the Collaborative systems are defined by a set of organizations that are working together to achieve the necessary operations in order to ensure the continuity and the development of the Critical Infrastructure. These organizations collaborate in a single system but each one of them has its own resources, services, information systems, security policies.... In this context and in order to succeed the collaboration between telecom organizations in the context of the IMS network, they must be flexible while allowing sharing resources and services in a secure way. To achieve a satisfactory level of the security in the collaborative systems in the IMS network, we must respect and consider a set of requirements and constraints.

- **Security of the organizations:** each organization (telecom operator and services provider) has its own resources and services which contain sensitive and confidential information and data. In this context, these organizations are worried to protect their entities against any threats.

- **Security of different exchanges between telecom organizations:** During the collaboration, some types of data are exchanged between telecom organizations such as the requested service, the customer information. Due to their Criticism, different exchanges must be protected by a security protocol.
- **Autonomy and access control** [11]**:** each telecom organization controls the access to its resources and services. Thus, it needs to be more autonomous while applying the security policies and making the collaboration decision [12] regarding the requester customer and the desired service.
- **Detection of malicious activities** [13]**:** The different collaborated organizations are managed by human being. Therefore, during the collaboration and due to human nature, different competitors may generate malicious activities in order to destroy the information systems of other telecom organizations. So, each telecom organization must be able to detect the malicious activities and entities before starting the collaboration.
- **Trust Management** [14]**:** Trust is an important factor between telecom organizations when establishing the collaboration. Thus, each organization must evaluate the reliability of the customers desiring to access to its services based on their behavior and reputation.

After enumerating different security requirements in the IMS network, we discuss in the next subsection the satisfaction of these requirements related to our context which is the collaboration between the telecom operators and the service providers.

3.2 Related Work

To make their customers satisfied, the operators present a set of services according to their costumer's subscriptions. In this sense, two main approaches are discussed: walled-garden and open-garden.

In the walled-garden approach [15], also called: closed model, the operators host the available services to their customers without contacting other services providers. The great advantages behind the exploitation of this approach lies in the security aspect; the operator evaluates itself the customer user profile which is stored in the HSS entity. This profile is then attached to the authorized services which will be accessed by the customer by using the Initial Filter Criteria. In this case, the customer information (history) is not disclosed by other operators or agents. In addition, the home operator stores the customer history which allows judging his/her behavior. Thus, the operator is aware of the customers who can commit malicious activities during the access to the desired services. As a result, this approach ensures the protection of the customer privacy, the protection of the hosted services and their availability to the authorized customers.

However, this protection loses when the customer wishes to access to services which are not available at his/her home operator. In this case, the operator contacts the services providers to ensure the customer access to the desired services according to his/her user profile. This approach is called the open-garden [16]. Actually, this approach brings several advantages regarding the customer's satisfaction [17]; the home operator seeks what service provider hosts the desired service. But, the major problem encountered is the security. In one hand, the service provider does not know the behavior of this customer nor his/her history. Thus, this access may damage the service. In the other hand, the service provider needs to discover the customer information which may contain personal information. Thus, the sharing of the personal information does not respect the customer privacy. Therefore, how can we secure the customer data and his/her personal information, and, at the same time, how can we protect the accessed services from malicious activities of the customer?

To answer these questions, we present in the following section our proposed solution: the Tr-OrBAC approach. It was mainly developed to protect the collaborative systems within Critical Infrastructure. And, we aim in this paper to demonstrate its feasibility in order to remedy the cited security issues in the IMS network.

4 Tr-OrBAC Approach: A Security Framework for IMS Network

4.1 Tr-OrBAC Architecture

The objective behind establishing the collaborative systems between organizations is to ensure their successful and their continuity. The principle of these systems is based on resources and services sharing between users and agents belonging to several organizations in order to perform the necessary operations. Thus, each user may access to the desired services of other organizations. Due to the security issues, each organization must evaluate the reliability of these users before giving them the access to their own services.

In this context, the Tr-OrBAC approach is based on the trust evaluation of the users. This evaluation is based on three trust criteria: satisfaction, reputation and recommendation [12]. The cited criteria permit to calculate

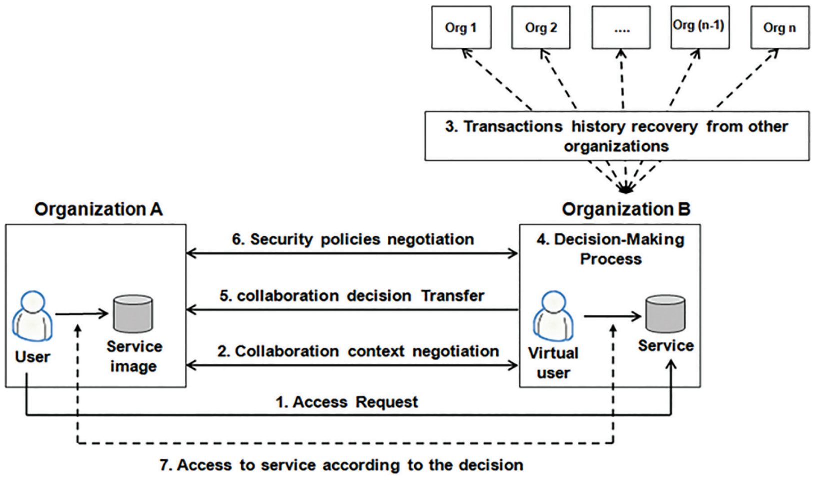
Org 1
Org 2
....
Org (n-1)
Org n
3. Transactions history recovery from other organizations
Organization A
Organization B
6. Security policies negotiation
4. Decision-Making Process
5. collaboration decision Transfer
User
Service image
2. Collaboration context negotiation
Virtual user
Service
1. Access Request
7. Access to service according to the decision

Figure 3 Global architecture of Tr-OrBAC solution.

a global trust score by using the AHP (Analytic Hierarchy Process) multi-criteria analysis method [18]. In fact, the AHP method allows us to attribute to each criterion a coefficient that indicates its importance according to the desired service (as we will explain in the next section).

The calculated trust score allows the provider organization to make the collaboration decision and to choose the appropriate access type for the requester user. Then, The calculated trust score permits to generate the trust rules which are based on the OrBAC model [19]. Figure 3 presents the global architecture of Tr-OrBAC solution. It consists of seven major steps, in general, to establish the collaboration between two organizations A and B.

- **Step 1 (Access Request):** An access request is sent to the Organization B asking for the service access.
- **Step 2 (Collaboration context negotiation):** The two organizations A and B negotiate and discuss the access to the service and the necessary requirements to ensure this access.
- **Step 3 (Transactions history recovery):** The organization B contacts other organizations which have already established the collaboration with the organization A in order to recovery the necessary information to evaluate the reliability of the requester.

- **Step 4 (Decision making process):** After discussing the collaboration context and recovering the necessary history files, the organization B evaluates the requester reliability based on his/her history in order to choose the appropriate access type. In this sense, we analyse the history files according to three trust criteria satisfaction, reputation and recommendation. The objective behind this analysis is to make the collaboration decision which presents the access type. In order to achieve this step, we use the AHP method for the multi-criteria analyses method.
- **Step 5 (Collaboration decision transfer):** In this step, the organization B transfers the established decision to the organization A.
- **Step 6 (Trust rules negotiation):** The two organizations negotiate the generation of the trust rules for the requester. The generated trust rules indicates the access type attributed to the user.
- **Step 7 (Access to service according to the decision):** The last step presents an answer to the first step and it achieves the collaboration process by giving the access to the desired service according to the established decision.

In fact, when we presented the different steps of our solution in [12], we mentioned that the service provider has the right to access to the customer history to evaluate his/her behavior. However, for confidentiality reasons and customer privacy [20], his/her history should not be shared between his/her operators and other telecom organizations. In this sense, the shared information must not be personal or sensitive. But, in this paper, we assume that this information are shared but they don't contain any sensitive information.

4.2 Tr-OrBAC Tools

Tr-OrBAC approach is based on three major phases, starting with the determination of the trust criteria until the generation of the trust rules. In this section, we aim to detail these phases which are: Trust evaluation using trust criteria, multi-criteria analysis methods and trust rules generation.

a. Trust evaluation using trust criteria

In order to evaluate the reliability of different users before giving them the access to the desired services, the service provider is based on three trust criteria: satisfaction, reputation and recommendation. We define in our Tr-OrBAC approach these criteria which are used to establish our mathematical model for trust evaluation [10].

- Satisfaction

The satisfaction of a set of entities towards the behavior of an entity is expressed by the ratio of the number of successful accesses to the total number of accesses (successful and unsuccessful), taking into account the novelty of the accesses and the novelty of collaborations. In fact, the new collaborations are more important than the old ones because they contain new conditions, requirements, needs, activities and services, etc. For this reason, an attenuation function h(i) [21] must be added to the calculation of satisfaction in order to indicate the impact of time on the satisfaction evaluation.

- Reputation

The reputation of an entity increases through its honest participation in the trust evaluation of other entities, also, through the provision of its services to any reliable requester entity if needed. In this sense, an entity is considered well reputed if it is honestly active in a collaborative system

- Recommendation

In some cases, the entities recommend and choose one of them to perform an activity which is considered critical and sensitive; this entity must be well reputable within the collaborative system. As defined "the recommendation is simply an attempt to communicate the reputation and reliability of a party from one community context to another" [22]. To this end, the recommendation to an entity must come from a set of entities that are themselves deemed reliable and reputable.

As we have presented, the details and the calculation of the different trust criteria are presented and detailed in our published article: Trust Management in Collaborative Systems for Critical Infrastructure Protection [10].

As these criteria don't have the same importance which depends on the collaboration context and the criticality of the desired services, it is necessary to use some methods which take into account the criteria analysis and the importance of each criterion in order to make the collaboration decision. For this, we use the AHP (Analytic Hierarchy Process) method for multi-criteria analysis. The AHP permits us to calculate the total trust score of the requester.

b. AHP for collaboration decision making

As we presented in the introduction, our objective is to secure the services accessed by a customer of other organizations, this customer can have one type of access among three possible according to his/her trust score. We talk about: Permission, Recommendation and Prohibition access. Also, the calculation

Table 1 The numerical assessments and their linguistic meaning [24]

Numerical Assessment	Linguistic Meaning
• 1	• Equal important
• 3	• Moderately more important
• 5	• Strongly more important
• 7	• Very strongly important
• 9	• Extremely more important
• 2, 4, 6, 8	• Intermediate values of importance

of the global trust score requires the combination of the trust criteria values whose importance changes according to the desired service.

Therefore, when several accesses are possible, we should choose the appropriate one between them according to the cited criteria, and the decision becomes difficult. It is in this context that the multi-criteria analysis methods have been proposed in order to facilitate the decision making. Several methods exist in our context; we implement our model using the AHP method.

The principle of this method (in our model) is to assign to each criterion a value indicating its importance relative to other criteria according to the desire service, as presented in Table 1. Next, each alternative or choice (in our case is the access type) is presented by a value indicating its importance compared to the other alternatives; and this comparison is made with respect to each criterion. Then, a set of calculation is done using the AHP method to choose the best alternative which has the greatest coefficient. The details of this method and also an example of application are presented in [12, 23].

After evaluating and calculating the different criteria and making the collaboration decision, the service provider generates the appropriate trust rules to secure the desired service from the customer access according to his/her reliability.

c. Trust rules

The trust rules in our proposed model are based on the OrBAC model [19]. This latter was developed primarily to manage the security rules within an organization when the number of resources, users, and actions increases. In our model, we use the principle of OrBAC model to manage the access between organizations, making it a collaborative model by integrating the concept of trust into the generated security policies. This integration is translated into a variable indicating the trust score of the user which requests the access to the service. We present an example of the trust rule as:

Permission (‘Org’, ‘Role’, ‘View’, ‘Activity’, ‘Context’, ‘Trust-score’).

This means that the organization ***'Org'*** permits the requester user to use the ***'Role'*** in order to access to the desired service ***'View'*** to perform an ***'Activity'*** in the predefined ***'Context'***. This user has the trust level: ***'Trust-score'***. More details about the OrBAC model, its principle and its different components are presented in [19].

After presenting the proposed solution and the IMS security issues regarding the collaboration, we reserve the next section to present the implementation of our solution in the IMS network, and then we interpret each step of our solution to demonstrate its feasibility.

5 Application of Tr-OrBAC in the IMS Network

As we mentioned earlier in this paper, our goal is to secure the collaboration between the service provider and the operator in the IMS network. So, the aim of this part is to present the process of securing the collaboration between the different actors by applying our approach Tr-OrBAC. After that, we will interpret each phase of collaboration.

5.1 Securing the Services Access in the Services Providers

In general, the customer wants to access to a service which is hosted by his/her operator or another service provider. In the case where the service is available at the operator, the security of the customer's data and the availability of the services are ensured. However, the problem is that when the service is no longer available from the operator but it is hosted by an external provider. In this context, the operator contacts the service provider in order to negotiate the customer's access to the desired service.

On the one hand, the provider must evaluate the reliability and the behavior of the customer before providing him/her the access to the service. And on the other hand, the operator must not disclose the customer data and information according to the regulations and contract between the customer and the operator. We are thus faced with a major challenge concerning the trust negotiation between the telecom operator and the service provider whose objective is to satisfy the customer and maximize the provider's profit. In this context, we apply our approach: Tr-OrBAC to resolve the cited security issues.

5.2 Integration of the Proposed Solution in the IMS Network

To demonstrate the feasibility of our solution in the IMS network, we present in this section a scenario illustrating the application of the cited solution in

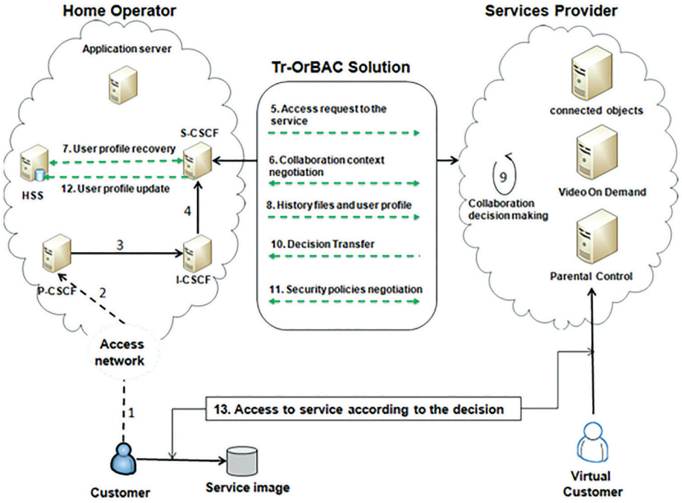

Figure 4 Integration of Tr-OrBAC solution in the IMS network.

the context of the collaboration between the telecom operator and the service provider. Figure 4 describes a global description of the solution integration.

The customer sends the access request to the desired service that is hosted by an external provider. This request is shared in the IMS network between the various CSCF servers (1, 2, 3, 4) until the S-CSCF which contacts the concerned provider in order to establish the collaboration (5, 6). In this sense, the S-CSCF recovers the user profile and the customer history from the HSS (7) in order to send the necessary information to the provider (8).

The chosen service provider evaluates the reliability of the customer based on his/her former collaborations regarding access to various services (9). For each type of service requested, the trust criteria will be calculated according to the level of importance of each criterion. And the decision of collaboration will be taken which presents the type of access attributed to the customer. Once the decision is made, it will be communicated to the operator (10) and the trust rules will be applied for the requester customer (11). Note that after the evaluation of the reliability of the customer, the user profile is updated in the HSS (12). Depending on the authorized access, the customer accesses the desired service by creating a service image in the operator, as the service is just hosted by the home operator (13). As customers, all of these steps are carried out automatically.

5.3 Interpretation, Discussion and Synthesis

A customer who wants to access a service that will be hosted by his/her operator or by an external provider must authenticate firstly in the IMS network. If authenticated, the customer will be registered in the network and he/she will have an IP address to access to the IMS network (necessary condition). This step of authentication and registration is ensured by the CSCF entities in the control layer of the IMS network. In our work, we are not concerned with customer authentication, since methods (IMS-AKA, HTTP Digest, GIBA . . .) [25] used until now are considered reliable for customers authentication. In fact, we are interested in how the customer can have access to the desired service and, more specifically, the services that are hosted by external providers (Service Provider).

After the authentication phase, the customer sends a request for access to the service. This request is passed through several entities within the IMS network (P-CSCF, I-CSCF) in order to direct the request to the S-CSCF.

This latter contacts the HSS entity whose role is storing the user data (databases), user profiles and service profiles. If the service is not available at the home operator, the operator looks for the provider which hosts this service. And collaboration establishment phase between the telecom operator and service provider begins.

At the time of collaboration, two contexts are possible depending on the desired service:

- Context 1:

A service hosted by the service provider, but at the time of collaboration, the provider deploys the operator's architecture to present the desired services to customers. In this case, the provider is present in the IMS network and according to the contract signed with the operator; it can have access to the user profile of the customer who is seeking access to the service.

- Context 2:

New services have been proposed but until now they are still monopolized by their provider which does not deploy the operator's architecture in order to present these services. In this context, the provider has no knowledge about the customer, his/her profile and his/her history. However, it must provide him/her with the service as the "context of collaboration." In this sense, the service provider evaluates the reliability of the customer in order to attribute the appropriate access type.

The customer's trust score is based on the trust criteria that are already discussed. The Service providers offer multiple services with different degrees of criticism, a quality of service that differs from one service to another, and some services require a high level of security. It is in this context that the provider decides the policy to follow in order to establish the trust towards to the customers requesting the service and to determine their trust score. This score is based on the history of the customer registered in the HSS database at their operator.

The principle is that the service provider determines the importance of each trust criterion according to the desired service and it also defines the importance of each type of access, (permission, recommendation and prohibition), to attribute to the customer based on the service.

If the customer has a favorable response to access to the service, so before access, a set of steps is necessary to reconstruct a new user profile containing information about the customer, service access, charging.... This profile will be registered in the HSS entity. Besides, in the service provider side, the customer accesses the service follows a set of trust rules generated by the provider. These rules contain the score indicating the reliability and the trust established for this customer.

In order to manage the customer access to different services, the provider establishes abstract security rules by specifying the role to be assigned to the customer, the service to be accessed, and the activity to be performed on the desired service. The customer trust score calculated is also added to various generated trust rules. This score is intended to justify the activity allowed for this customer. Once the collaboration is taken, the provider can assign the customer at the right role according to his/her trust score.

6 Conclusion and Perspectives

The protection and the security of several collaboration in the IMS network is primarily linked to several requirements that need to be identified and taken into consideration at the time of collaboration. Given the importance of these requirements, we project, in this paper, our proposed trust model Tr-OrBAC in the context of collaboration in the IMS network. This model allows the security of the participants involved in collaboration, while respecting the confidentiality of data and the privacy of customers. In this context, the developed trust model was based on three essential elements, such as trust rules, trust management by proposing trust criteria (satisfaction, reputation and recommendation) and the AHP multi-criteria analysis method which allows the Collaborative decision-making between several actors.

In this paper, we have presented an example of collaboration in the IMS network between the telecom operator and the service provider. In particular, we treated the issue of the customer access to a service hosted by a service provider. The goal was to provide to each customer an access type based on his/her user profile. Finally, this type of access is translated into a set of trust rules.

On the introduction of the IMS in this paper, it was only to process and illustrate how our approach is functional for this type of network by interpreting its application in an example of collaboration context. In our perspective, we intend to deal with a real case of a service accessed by external customers and we will give more details about the implementation of the developed trust model Tr-OrBAC in the IMS network. In this sense, we work actually to implement our approach in a real case study.

References

[1] R. Ratasuk, A. Prasad, Z. Li, A. Ghosh and M. A. Uusitalo, ‘Recent advancements in M2M communications in 4G networks and evolution towards 5G’, in 18th International Conference on Intelligence in Next Generation Networks, pp. 52–57, 2015.

[2] T. Pfeiffer, ‘Next Generation Mobile Fronthaul Architectures’, in Optical Fiber Communication Conference and Exhibition, Los Angeles, CA, USA, 2015.

[3] N. Czernich, O. Falck, T. Kretschmer and L. Woessmann, ‘Broadband Infrastructure and Economic Growth*: Broadband Infrastructure and Economic Growth’, The Economic Journal, vol. 121, no 552, pp. 505–532, 2011.

[4] D. He, C. Chen, J. Bu, S. Chan and Y. Zhang, ‘Security and efficiency in roaming services for wireless networks: challenges, approaches, and prospects’, IEEE Communication Magazine, vol. 51, no 2, pp. 142–150, 2013.

[5] Camarillo, Gonzalo and Miguel-Angel Garcia-Martin, ‘The 3G IP multimedia subsystem (IMS): merging the Internet and the cellular worlds’ John Wiley & Sons, 2007.

[6] Scott, W. Richard, Gerald F. Davis et al., “Organizations and organizing: Rational natural and open systems perspectives”, Routledge, 2015.

[7] N. Ait Aali, A. Baina and L. Echabbi, ‘Tr-OrBAC: A trust model for collaborative systems within critical infrastructures’, 5th World Congress on Information and Communication Technologies (WICT), pp. 123–128, 2015.

[8] C. Alcaraz and S. Zeadally, ‘Critical infrastructure protection: Requirements and challenges for the 21st century’, International Journal of Critical Infrastructure Protection, vol. 8, pp. 53–66, 2015.

[9] E. Belmekki, M. Bellafkih and N. Bouaouda, ‘Efficient light model for securing IMS network’, in 8th International Conference on Intelligent Systems: Theories and Applications (SITA), pp. 1–7, 2013.

[10] N. Ait Aali, A. Baina and L. Echabbi, ‘Trust Management in Collaborative Systems for Critical Infrastructure Protection’, *Security and Communication Network,* vol. 2018, p. 1–15, juillet. 2018.

[11] R. S. Sandhu, E. J. Coyne, H. L. Feinstein and C. E. Youman, ‘Role-based access control models’, Computer, vol. 29, no 2, pp. 38–47, 1996.

[12] N. Ait Aali, Y. E. B. E. Idrissi, A. Baina and L. Echabbi, ‘Collaboration decision making based on AHP method in Tr-OrBAC model: Case study’, in 4th IEEE International Colloquium on Information Science and Technology (CiSt), pp. 779–784, 2016.

[13] V. Herrera-Semenets, O. A. Pérez-García, A. Gago-Alonso and R. Hernández-León, ‘Classification rule-based models for malicious activity detection’, Intelligent Data Analysis, vol. 21, no 5, pp. 1141–1154, 2017.

[14] F. Ishmanov, A. S. Malik, S. W. Kim and B. Begalov, ‘Trust management system in wireless sensor networks: design considerations and research challenges’, Transactions on Emerging Telecommunications Technologies, vol. 26, no 2, pp. 107–130, 2015.

[15] A. Chen, N. Feamster and E. Calandro, ‘Exploring the walled garden theory: An empirical framework to assess pricing effects on mobile data usage’, Telecommunications Policy, vol. 41, no 7, pp. 587–599, 2017.

[16] N.-V. Ciobanu, D.-G. Comaneci, C. Dobre, C. X. Mavromoustakis and G. Mastorakis, ‘OpenMobs: Mobile Broadband Internet Connection Sharing’, in Mobile Networks and Management, pp. 244–258, 2014.

[17] D. Kang Y. Park, ‘Review-based measurement of customer satisfaction in mobile service: Sentiment analysis and VIKOR approach’, Expert Systems with Applications, vol. 41, no 4, pp. 1041–1050, 2014.

[18] T. L. Saaty, ‘Decision making with the analytic hierarchy process’, International Journal of Services Sciences., vol. 1, no 1, pp. 83–98, 2008.

[19] A. A. E. Kalam et al., ‘Organization based access control’, in 4th International Workshop on Policies for Distributed Systems and Networks, pp. 120–131, 2003.

[20] A. S. Y. Cheung, ‘Location privacy: The challenges of mobile service devices’, Computer Law & Security Review, vol. 30, no 1, pp. 41–54, 2014.

[21] K. Toumi, C. Andrés and A. Cavalli, ‘Trust-orBAC: A Trust Access Control Model in Multi-Organization Environments’, in *Information Systems Security*, V. Venkatakrishnan and D. Goswami, Éd. Springer Berlin Heidelberg, 2012, pp. 89–103.

[22] S. Ruohomaa and L. Kutvonen, ‘Trust management survey’, in *Trust Management,* Springer, 2005, pp. 77–92.

[23] Y. E. B. El Idrissi, R. Ajhoun and M. J. Idrissi, ‘Multicriteria-Based Decision for Services Discovery and Selection’, in Intelligent Interactive Multimedia Systems and Services, Springer, pp. 41–51, 2010.

[24] G. Işiklar and G. Büyüközkan, ‘Using a multi-criteria decision making approach to evaluate mobile phone alternatives’, Computer Standards & Interfaces, vol. 29, no 2, pp. 265–274, 2007.

[25] M. Maachaoui, ‘Sécurité et performances des réseaux de nouvelle génération’, 12-juin-2015. [En ligne]. Disponible sur: http://ethesis.inp-toulouse.fr/archive/00002996/.

Biographies

Nawal Ait Aali completed her engineering studies in Telecommunication systems and networks at National School of Applied Sciences from 2007 to 2012. Currently, she is preparing her Phd in Computer Science at the National Institute of Posts and Telecommunications (INPT) at Rabat, Morocco. She works in her thesis on the trust management in the collaborative systems for Critical Information Infrastructure Protection.

Amine Baina is Assistant Professor at the National Institute of Posts and Telecommunications Rabat, Morocco, since 2010. He had his PhD in Computer Science in "Access Control for Critical Infrastructures" in 2009 from the Laboratory of Systems Analysis and Architecture in Toulouse. He had his Computer Engineer's degree from the National Engineering School of Bourges, France, in 2005.

Loubna Echabbi is qualified a Senior Lecturer in France, since December 2005 and an Associate member of the team ALCAAP PRISM Laboratory, Versailles. She received her PHD in Algorithms for the allocation and pricing of resources in telecom networks with service guarantees in September 2005. Currently, she is a professor at National Institute of posts and Telecommunications, Rabat, Morocco.