On an Access Control Model enhancement for the 5G System

Luis Suárez, David Espes, Frédéric Cuppens, Philippe Bertin, Cao-Thanh Phan, Philippe Le Parc
IRT b<>com - Cesson-Sévigné, France
{Luis.Suarez; David.Espes; Frederic.Cuppens; Philippe.Bertin; Cao-Thanh.Phan; Philippe.Le-Parc }@b-com.com

***Abstract*—The realization of communication services over 5G needs resource sharing as a way to achieve network coverage. To do so, it is necessary to consider security access mechanisms to regulate how interconnections are made. The existing models do not address all the needs inherent to the 5G architecture, such as access control mechanisms, multi-tenancy, multi-domain and multiple security levels. This position paper presents the state of the art of access control models and their application in 5G networks. Then, points out problems that are not addressed and establishes the conditions that such access control scheme must obey in order to be suitable for its utilization in the 5G system.**

***Index Terms*—Security, Access Control Model, 5G, intra-slice, RBAC, DTE, BLP**

I. Introduction

5G is envisioned as the new architecture that is going to make possible the implementation of new telecommunication use case scenarios. A key quality that must be considered is their security. Related to 5G, security is addressed from the service point of view, on top of the existing services of the 5G System (5GS), but there is no clear access control model for the entities that are inside the 5GS. Moreover, since these entities can be provided by different stakeholders, dissimilar security levels are applied according to their own internal rules, policies and security requirements. The need for interconnection of components poses the risk of being exposed to threats from other players, and in consequence, a secure interaction should be guaranteed to minimize the security risks. The challenge is how to manage the interaction between those entities, given multiple providers, functions and security attributes that specify them. Even though there exist several access control models applied in information technology that are imported into the telecommunications industry, their properties cannot be directly applied to the 5G system. In order to support our claim, this short paper is organized as follows: Section II investigates how existing access control models can apply to 5GS use cases. Section III points out the shortcomings of existing approaches to then, in Section IV state the ideal access control components required for the 5G System. Concluding remarks are given in Section V.

II. Approach and architectures

Access control models answer the need to provide secure access to resources. Traditional access control models and new approaches to 5G networks are reviewed in the next subsections.

A. Traditional access control models

Role Based Access Control (RBAC) leverages on the **role** concept as a way to group job functions. **Users** and **permissions** are assigned to the roles via assignment relations, as detailed in [1].

Domain and Type Enforcement (DTE) is an enhanced version of Type Enforcement, which specifies policies in a high-level language (instead of using tables) and provides implicit security attributes for objects [2]. The implementation made over the Linux kernel [3] considers that **Type** can be assigned to objects and **Domain** to processes. The DTE policy restricts access between domains and from domains to types.

Lattice-based access control model was developed to address the way information flows in a computer system. It mostly covers confidentiality, and also applies to integrity. Under this category, we find some representative models, such as: **(a)** *Bell-LaPadula (BLP)* which is a state-machine model for information flow and access control. BLP covers confidentiality only, and the secure state is permitted according to a specific security policy as it is detailed in [4]. **(b)** *Denning's lattice model* [5] states the importance to secure information flow among Security Class (SC) in a computer system. The model is built over three components: **(i)** the SC, **(ii)** a flow relation on pairs of SC, and **(iii)** a binary class-combining operator on SC. Using those components, Denning formulates some axioms, which are detailed in [5].

B. Access control implementations for 5G

Some publications seek to apply Multi Layer Security (MLS) to telecommunication networks. For example, in [6] authors propose a modified BLP security model to be used in a 5G/Internet of Things (IoT) use case. Their security model considers a scheme to label data based on the secrecy level and category, as well as capability token that rules the access scheme. In [7], authors also use BLP in the private cloud environment in order to change the security level of an object dynamically.

Authors in [8] address the security in IoT in relation to the complex data flows. Even if a strict approach using Denning's lattice model can be implemented, authors prove that using a partial order model can achieve security and more flexibility. These two works are important since it is necessary to have a secure interaction between the IoT environment and the 5G network that provides connectivity and access to telecommunication services.

In [9] authors analyze the issue of confidential information carried by video signals transmitted by objects in a Vehicular Ad-Hoc Network (VANET) that use 5G networks. In addition to cryptography to ensure secure communication, the scheme uses enhanced RBAC to allow only authorities to view video files residing in the storage system.

Authors in [10] propose to enhance the Topology and Orchestration Specification for Cloud Applications (TOSCA) modeling language with security parameters, which can be deployed on VNF services with embedded security countermeasures.

III. Problems in existing approaches

Concerning traditional access control models, RBAC incorporates the role concept as an attribute to restrict the operations available to a user. But it would be desirable to have more advanced attributes as Attribute-Based Access Control (ABAC) to gain more granularity in this control. DTE provides the distinction between objects and processes, proposing the concept of domain as a restriction to limit the operations available to the subject. Nonetheless, its conception is oriented to operating systems, making difficult its implementation in other architecture by its own means. BLP is based on the security clearance and security classification in order to enforce information flow policies. The state of the system depends on few parameters, making it more restrictive when trying to apply it into other use cases. For the general case of lattice-based access control models, the need to establish ordered security classes makes it difficult to adapt to system in which labels are not necessary in a hierarchy.

Regarding telecommunication technologies, most of the research works are about regulating access control for the applications that run on top of the 5G network (IoT and VANET environments). The access control model on the TOSCA model considers its application on 5G networks, but it does not consider: **(i)** the inner interactions between its components according to 3rd Generation Partnership Project (3GPP) standards; and **(ii)** the hierarchies that are needed in order to supervise the access among those components.

From this review, it is deduced that choosing a single model is not enough to tackle the complexity to govern the secure access control of the 5GS. Next Section demonstrates the needed criteria to create an access control model for the 5GS.

IV. Ideal access control model for the 5G System

At the core of the 5G System lies the Service Based Architecture (SBA), specified by 3GPP in [11], which describes the principal Network Functions (NF) that are considered to provide a 5G service. The constituting NF have different roles to play in the architecture, each one differentiated, for example, whether it handles customer requests directly, deals with the service offering or have management functionality. Moreover, even though the SBA lies at the core network, interacting entities can be found on the access network and the data network. This gives a clue that the separation into domains is required as a way to segment the network to ease management and isolate failure domains.

Several stakeholders interact in this architecture, some of them as consumers, others as producers of services. Their assignment to a role and to a domain in the architecture is the key to assure that the requests and actions are valid according to policy. This way, the established sessions between entities are secured and behave according to the rules stated by the standards.

V. Conclusions

Traditional access control models do not fulfill the requirements of the 5G architecture, considering communication between dissimilar entities, distributed over different layers of the architecture and managed by different providers. All of them seeking to provide a concrete communication service to customers and industry verticals.

We argue that the concepts of **role** and **domain** are the ones that help to specify and restrict actions over entities of the 5G system. Derived from these concepts, the established **session** between entities will reside under the scope of a concrete context, which is framed by security properties that delimit the possible 5G procedures that can be executed over a NF.

These key characteristics guarantee that several security properties can be specified according to the needs of the Communication Service Providers (CSP). Moreover, the concepts that are used are general enough to apply to other use cases and architectures. Their implementation constitutes an enabler to enforce security within the 5G Core (5GC) and offer more secure services to users and verticals.

References

[1] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *Computer*, vol. 29, no. 2, Feb. 1996.

[2] K. A. Oostendorp and Badger, "Domain and type enforcement firewalls," in *DISCEX'00*, vol. 1, 2000.

[3] L. Badger and D. F. Sterne, "Practical Domain and Type Enforcement for UNIX," in *IEEE Symposium on Security and Privacy*, 1995.

[4] L. J. LaPadula and D. E. Bell, "Secure computer systems: A mathematical model," Citeseer, Tech. Rep., 1996.

[5] D. E. Denning, "A Lattice Model of Secure Information Flow," *Commun. ACM*, vol. 19, no. 5, May 1976.

[6] O. Salman and A. Kayssi, "Multi-level security for the 5G/IoT ubiquitous network," in *2017 Second International Conference on Fog and Mobile Edge Computing (FMEC)*, 2017.

[7] H. Xue, "A Multilevel Security Model for Private Cloud," *Chinese Journal of Electronics*, 2014.

[8] L. Logrippo and A. Stambouli, "Configuring data flows in the Internet of Things for security and privacy requirements," *11th International Symposium on Foundations and Practice of Security (FPS 2018)*, 2018.

[9] R. Gopi and A. Rajesh, "Securing video cloud storage by ERBAC mechanisms in 5g enabled vehicular networks," *Cluster Comput*, 2017.

[10] Pattaranantakul, "Leveraging Network Functions Virtualization Orchestrators to Achieve Software-Defined Access Control in the Clouds," *IEEE Transactions on Dependable and Secure Computing*, 2018.

[11] 3GPP, "Specification # 23.501," 2018.