Formalization of a security access control model for the 5G system

Luis Suárez, David Espes, Frédéric Cuppens, Philippe Bertin, Cao-Thanh Phan, Philippe Le Parc

Formalization of a security access control model 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 race for implementing communication services over 5G has already begun. For this, network coverage is needed and resource sharing is a way to achieve it. Therefore, each provider enforces its own security requirements. Under this scenario, it is necessary to consider security access mechanisms and policy rules, to regulate how interconnections are made between the shared network functions and how to allow specific traffic. The existing models do not address all the needs inherent to the 5G architecture, such as multi-tenancy, multi-domain and multiple security levels.**

To solve this challenge, this paper defines a novel access control model for 5G, leveraging on the best characteristics of traditional access control models used in operating systems and cloud scenarios. The security properties in our model obey the functional requirements within the 5G system as well as towards the customers. The actions and type of traffic of the system can be specified and enforced via an access control policy.

Besides addressing the 5G system, our innovation is general enough to be applied over other types of architectures, proving its scalability and capability to incorporate more security features.

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

I. Introduction

5G is envisioned as the new architecture that is going to make possible the implementation of new telecommunication use case scenarios. The actual connectivity scheme provided by 4G, that focuses on the mobile broadband use case, does not scale to other applications that have tighter constraints in latency, bandwidth or massive connectivity [1].

One key component that must be considered when implementing services is security. Related to 5G, there are projects that address security 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.

To tackle this problem, we focus on the access control mechanism by which Network Functions (NF) will have to comply in order to access another NF inside the 5G Core (5GC). A mechanism to guarantee only the essential interactions between them is required.

There is an extensive research activity about the different access control models. The ones that are most used are Role-Based Access Control (RBAC) [2], Attribute-Based Access Control (ABAC) [3], Domain and Type Enforcement (DTE) [4], and lattice-based such as the ones proposed by Bell La Padula [5] and Denning [6]. Each one of them has its own properties and mechanisms that seek to control access from subjects to objects. Their properties can be applied to several use cases, for example, in access control to documents that have different classification levels, file systems and operating systems that manage shared pools of information. However, due to the characteristics of a 5G mobile network, their properties cannot be directly applied to this use case.

Choosing a single model is not enough to tackle the complexity to govern the secure access control of the 5GS. Our contribution is important because it selects the best qualities from the models, taking into account that the chosen qualities depend on the target architecture and the properties that we would like to enforce.

Our contributions, which are based on these fundamental models, are: **(i)** search for the best approach to implement secure access control inside the 5GS from the current models; **(ii)** create a security access control model that complies with the 5GS scenario requirements; and **(iii)** provide the proper mathematical definition for the model.

The paper is organized as follows: Section II investigates how existing access control models can apply to 5GS use cases. Section III describes the components that are needed in a secure access control model for the 5GS. Section IV provides the description of the global access control model. Section V describes the auxiliary concepts needed to glue its components together. Interactions inside the 5GS are presented in Section VI. Section VII outlines the advantages of our proposed model compared to the existing ones. In Section VIII we draw concluding remarks about this work.

II. Approach and architectures

Access control models constitute an area of major research due to the necessity to provide secure access to resources. In the following subsections, we will review their most important qualities.

A. Traditional access control models

Among the traditional access control models, the most representative are Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Domain and Type Enforcement (DTE), and Lattice-based access control. The following subsection explains briefly each one of them.

1) RBAC: It is based on the premise that the ability (or need) to access information may depend on the job function of the entity that seeks access. RBAC leverages on the **role** concept as a way to group job functions and, is based on that role that authorizes actions. The role is the mechanism to restrict the impact of the actions of a user. Besides the role, RBAC uses the concept of **users** and **permissions**, which are assigned to the roles via assignment relations, as detailed in [7]. It is interesting to consider the role as an aggregation concept, that is used to handle permissions at a higher level, easing management of the users, via their roles. Other advantages are to have hierarchies in roles, provide least privilege and separation of duties and the use of object classes as a mechanism to avoid assigning permission to specific objects [8].

2) ABAC: This model controls access to objects by making an evaluation of the attributes of entities (objects and subjects), the intended operations and the environmental conditions on which resides the access request [3]. Attributes have a hierarchical structure and the inclusion of more attributes enables to have more possible rules to express policies. ABAC permits the creation of access rules without specifying individual relationships between each subject and each object. When adding new subjects, rules and objects do not need modification as subjects are assigned to the correct attributes.

3) DTE: It is an enhanced version of Type Enforcement, a table-oriented Mandatory Access Control (MAC) mechanism. Its improvement compared to Type Enforcement, consists in the specification of policies in a high-level language (instead of using tables) and providing implicit security attributes for objects [9]. DTE uses the concepts of **Domain** (which is an invariant access control attribute) and **Type** (which is an invariant attribute) as principal components in the model, regulating their interactions. The implementation made over the Linux kernel [4] considers that **Type** can be assigned to objects and **Domain** to processes. The DTE policy restricts access between domains and from domains to types. In this model, it is useful to ponder the domain concept, as a mechanism to provide segmentation of the resources and border authorization control point to allow the execution of actions on it.

4) Lattice-based access control: This model was developed to address the way information flows in a computer system. It mostly covers confidentiality, and also applies to integrity [10]. Under this category, we find some representative models, such as:

- Bell-LaPadula (BLP): it is a state-machine model for information flow and access control. BLP covers confidentiality only (integrity is achieved when BLP is extended by BIBA model [11]), and the secure state is permitted according to a specific security policy. This policy is summarized in three principles: simple security property; star property and strong star property, as it is detailed in [12]. Apart from only covering confidentiality, and considering its parameters as an ordered set, it provides no native way to manage (that is, change the assignment and modification) of the classification categories. The MAC and information flow approach is interesting under this model, but its security functions only considers the security level of the subject and object.
- Denning's lattice model: The most representative model under this category is the one described by Denning [6], in which she states the importance to secure information flow among Security Classes in a computer system. She leverages on the use of lattices to formulate concisely the security requirements to then aid to formulate the enforcement mechanisms. The model is built over three components: **(i)** the Security Classes, **(ii)** a flow relation on pairs of Security Classes, and **(iii)** a binary class-combining operator on Security Classes. Using those components, Denning formulates some axioms, which are detailed in [6]. The lattice approach is exigent, and is built on a strong categorization and hierarchy. Nonetheless a more malleable approach is needed, due to the fact that our target systems would consist of a dissimilar number of objects that do not have a strict hierarchy relationship to constitute a lattice as an ordered set.

B. Access control implementations for 5G

According to the explored literature, access control implementations cover **(i)** at the application level: IoT systems, connected vehicles, medical oriented scenarios and document management; **(ii)** at the resource level: they consider cloud scenarios, security under NFV MANO environment and traffic segmentation using Software Defined Network (SDN).

Some publications seek to apply Multi Layer Security to telecommunication networks. For example, in [13] 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 [14], the authors propose a Multi Layer Security model based on BLP to avoid leakage of information from internal users in the private cloud environment. This is a key feature to have the ability to change the security level of an object dynamically.

In [15], the authors deal with the secure distribution of workloads in the cloud by transforming the workloads, and detecting possible breaches in the inter-cloud communication. The transformation process involves awareness of the nature of the data in the workflow, the location of the clouds along with their security level.

Authors in [16] 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.

Authors in [17] argue that authorization to access documents in a network is usually enforced at the server side. But since the network is used by actors with different clearances, malicious users can access unauthorized content by attacking the network directly.

In [18] authors seek to allow or deny the interactions between virtual objects in the IoT environment that uses publish/subscribe mechanisms for communication. They use RBAC to control the administrator's configurations on Virtual Objects. The policies specify which Virtual Objects are allowed to publish to which topics, and likewise which Virtual Objects can subscribe to which topics. 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.

Authors in [17] developed an Access Control Application on a SDN controller to classify the information flows and separate them by implementing VLANs, one for each group of users with similar security clearance.

In [19] authors analyze the issue of confidential information carried by video signals transmitted by objects in a Vehicular Ad-Hoc Network that uses 5G. 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. In a similar way, authors in [20] use RBAC principles to provide assurance in access to Body Area Networks that collect health information about a patient. Their quest is to address the situation in which a person without the required role can access the patient's data via a 5G network in order to save a life. Their proposed Emergency-aware RBAC resides on a Personal Trusted Gateway that regulates the access to external actors into the Body Area Network.

Authors in [21] propose to enhance the Topology and Orchestration Specification for Cloud Applications (TOSCA) modeling language with security parameters. The idea is to leverage on the SDN paradigm to use these parameters and, via an access control model, deploy services on Virtual Network Function (VNF) with embedded security countermeasures. Their approach conceives a security orchestrator with an access control meta model that can specify different access control models according to the needs of each tenant.

C. Discussion

Reviewing the traditional access control models, RBAC incorporates the role as limiting concept to the operations available to a user, but it would be desirable to have more advanced attributes as ABAC. However, using ABAC requires the specification of environmental conditions, which is information that is not associated with any specific subject or object. Examples of conditions are the day of the week or the load of an entity. For our study, these conditions do not apply directly to the interactions between the entities in the 5GS. 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 the recent works, most of them are about regulating access control for the applications that run on top of the 5G network (IoT, Vehicular Ad-Hoc Network, or medical environments).

The access control model approach on the TOSCA model proposes its application on 5G networks, but it does not take into account: **(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. These are added-value ideas in our contribution.

It is deduced that choosing a single model is not enough to tackle the complexity to govern the secure access control of the 5GS. Our contribution is important because it selects the best qualities from the security models, taking into account that the chosen qualities depend on the target architecture and the properties that we would like to enforce. Next section will demonstrate the needed criteria to create an access control model for the 5GS.

A summary of the key characteristics of the discussed access control models is presented in Table I.

III. New Secure Access Control Model for the 5GS

This section presents the key elements needed to build a secure access control model for the 5GS. For this, the Service Based Architecture specified by 3GPP in [22] is used, which specifies the principal NF that are considered to provide a 5G service.

To address the access control model problem for the 5GS, it is necessary to identify commonalities on the components (in order to create domains of interest), identify the roles that the NF play in the 5GS, identify subjects, objects and characteristics that help to establish a classification for them.

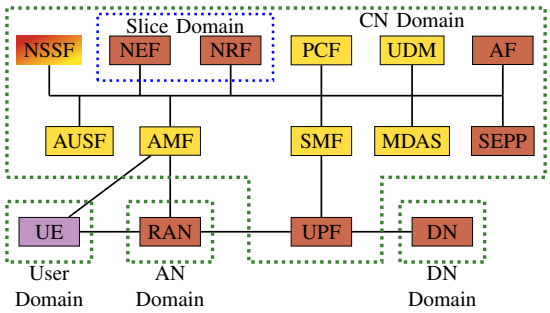

Fig. 1. Simplified 5G System architecture with Roles and Domains [22].

TABLE I
COMPARISON BETWEEN SECURITY MODELS

Model	Description	Qualities for 5G	Missing qualities for 5G
RBAC	• Possibility to interpret RBAC as a MAC model. • Permissions assigned to roles. • Users are assigned to the role. • The role limits the operations available to a user.	• No Access Control List (ACL) as Discretionary Access Control (DAC). • Security functions depend on a much richer set of parameters: user, roles and the permission to the roles, providing a less-restrictive control.	• Does not have advanced attribute functions as ABAC.
ABAC	• The access control decision is based on the attributes of requester and object, environment conditions and the set of policies (in terms of attributes and conditions).	• Attribute list can be expanded as needed, leading to richer rule specification.	• The environmental conditions, which is one important quality, does not match the communication scenario of the 5GS.
DTE	• Originally proposed as an integrity mechanism. • Types can be assigned to objects and domains to processes. • The DTE policy restricts access between domains and from domains to types. • The domain limits the operations available to a subject. • A process belongs to exactly one domain at any particular time.	• The entry point program (inside the domain statement in DTEL) is a mechanism to verify access rights into a domain. • Works based on the principle of least privilege.	• Does not implement roles. • A type is a set of objects which, from the security point of view, are no further differentiated.
BLP	• Motivated to enforce confidentiality. • MLS approach, based on security clearance and security classification. • Uses MAC to enforce information flow policies.	• The security parameters conform an unmutable lattice, which is an ordered set. • Incorporate sensitivity level and the need-to-know (categories).	• Concerned with how data flows from one level to another. • Does not cover integrity. • Security functions depend only on the security level of subject and object. • State of the system depends of few parameters, in consequence it is more restrictive.
Denning	• Considers the concept of flow of information from one security class to another. • Every object is assigned a SC, or label.	• Via ordered security classes (SC) we can have a hierarchy of security classes. • It is a relational model, rather than state-transition based.	• Compared to BLP, only covers sensitivity level, via security classes.

A. Roles

Each NF performs a function that can be categorized into roles. Roles can be used to describe the function of the NF in the 5GS. Roles are important because they help to limit the impact of the actions of the NF that has that role assigned. With this, granularity in access control based on the 5G architecture is achieved. We identify three major role categories for the NF that reside on the control plane: *Customer* (in purple), *Service* (in red) and *Governance* (in yellow) as shown in Figure 1. Notice that certain elements can have more than one role, as the case of the Network Slice Selection Function (NSSF), which has Service and Governance functions.

The reason for choosing these role categories is rooted in the need to grant access to the user into the network, provide a service and finally manage all the 5G system as a whole. It is possible to elaborate further into the specifics for each entity, ending with the assignment of the precise NF to a concrete role. The rational for the role assignment of each NF is as follows:

1) Customer: refers to subjects that request the service. It can be an end user via a mobile device or a Communication Service Customer that has its own customer base, like a Mobile Virtual Network Operator.
2) Service: Figure 2 shows the division scheme for this role category. The different NF inside the 5G Service Based Architecture are divided according to their purpose from a service point of view. Some of them provide a common service to customers and the 5GS, others provide security services, monitoring utilities or traffic routing.
3) Governance: Figure 3 shows the NF role assignment to this category. The NF are classified whether they have to do directly with the Life Cycle Management of the Communication Service (ComSer), of the network slice, or it deals directly with the user. This role has further sub-categories: policy, session, access and authorization for the users, each one of them managing an aspect of the user that accesses the 5GS.

B. Domains

Besides a division by functionality, the 5GS can be divided into administrative areas. Usually this segmentation is called a domain. A domain is a grouping of network entities according to physical or logical aspects that are relevant for a 5G network [23]. Relevant aspects can include type of functionality, trust, (geographical) location, among others. The division of the 5GS into the proposed domains is shown in Figure 1.

From an *end-to-end* point of view, the well-known division of a mobile network into Access Network (AN), Core Network (CN) and Data Network (DN) is reusable under this context. Nonetheless, it is necessary to consider that a communication service can be provided via verticals, and by itself, it can have NF that belong to each of these domains. In consequence, a

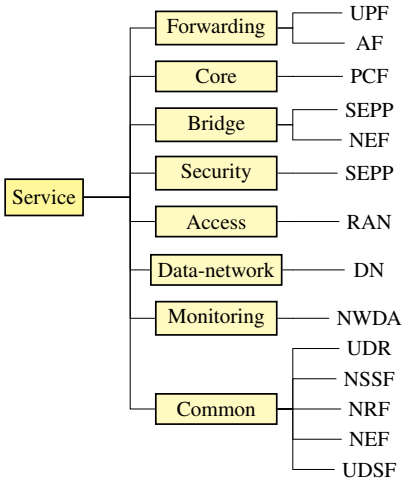

Fig. 2. Hierarchy for the service Role category in the Service Based Architecture.

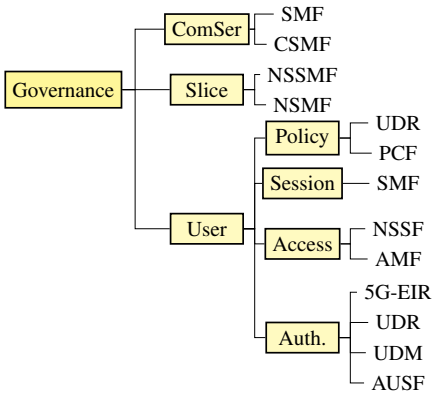

Fig. 3. Hierarchy for the Governance role category in the Service Based Architecture.

slice domain is proposed in addition to the other ones, with its own divisions in AN, CN and DN.

Other important consideration refers to the quantity of NF that belongs to the CN, which can be very high. In consequence, it is necessary to break down this domain into smaller ones. Leveraging on the 5G Service Based Architecture, the proposition is to divide the CN into **(i)** sub-domains that hold NF internal to the CN, named CN-I; **(ii)** sub-domains for the NF that are exposed to other external domains, called CN-E; and **(iii)** sub-domains that have NF with governance capabilities, named CN-G. Finally, the users and industry verticals are found in a generic *Consumer* domain, for example, smartphones, IoT devices or Mobile Virtual Network Operators. Figure 4 provides the graphical description of the domains for the proposed security model.

C. Subjects and objects

Inside the CN, we must consider the communication between NF, since their interconnection and interaction is needed in order to have the complete information to provide a service. As a consequence, the proposed model considers *subjects* performing as the active entity, initiating an interaction with a passive entity; and *objects* that offer a service and are waiting for a request, as a passive entity.

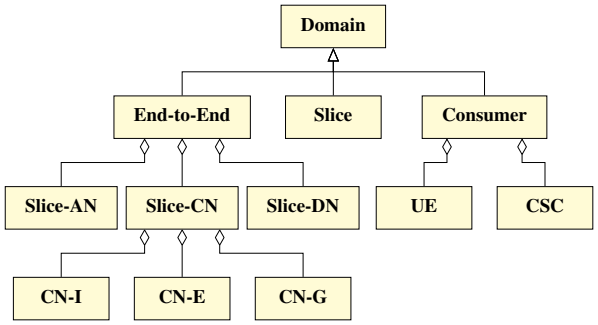

Fig. 4. Domain hierarchy for the proposed security model

D. Which model to apply?

As shown in Section II we have several models for controlling access to a system. From them, we find relevant **(i)** the **role** concept as a mechanism to efficiently manage the actions and permissions to subjects under the same function; **(ii)** the **domain** concept as a way to further confine interactions and group entities that have the same qualities, administrative management and policies; and the differentiation between **(iii) subjects** and **(iv) objects** as division of the interacting parties.

These concepts lead to the choice of using RBAC and DTE models as foundation for the proposed secured access control mechanism for the 5GS.

The challenge is to merge the most representative and useful components from these two models. There are similarities on the way they define role and type, users and subjects, objects and passive entities. There are concepts that are unique to each model (like the ones referring to session and domain), nonetheless the commonalities pave a way to construct a model that picks the best from RBAC and DTE, which we call, Role and Domain Access Control (RDAC).

IV. Global description of the model

This section describes the components of the proposed model, called RDAC, which combines the best qualities of RBAC and DTE access control models. The intention is not to have a unified model with all components of RBAC and DTE, but to consolidate the required concepts according to the needs of the 5G use case. The mathematical definitions use a simple convention: the capital letter means that it refers to a set and the lowercase letters refers to the components of the set. For example, $\mathcal{O}$ refers to a set of objects, being $\mathcal{O}$ composed of three objects o_1, o_2, o_3.

The global architecture is shown in Figure 5 as an UML diagram. The included components are subject, session, role, domain, object, Security Constraint, action and permission.

The components will be described in more detail in the following subsections.

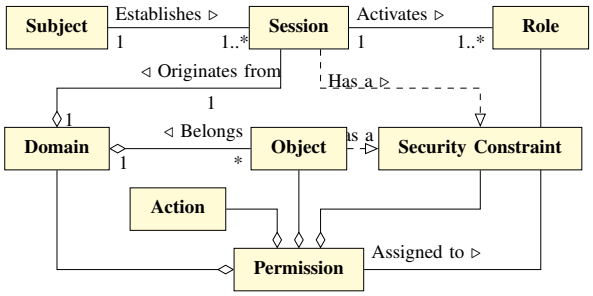

Fig. 5. UML representation of the RDAC model.

A. Entities: subjects and objects

Entities denote the generic name of the actors that interact in our model. From this class, we can differentiate an entity called **subject** (which can be VNFs or a person) and **Objects**, which represent the assets to protect. Objects are conceived as subjects, but in their construction they are composed of an additional standby component that represents their ability to receive requests, to then provide a response in return. Figure 6 presents the concept of entity as an UML diagram. Entities can be built from a finite but unbounded number of elements, defined as: $\mathcal{E} = \{e_1, e_2, ..., e_n\}$.
Subjects $\mathcal{SU}$ and objects $\mathcal{O}$ would be represented as sets: $\mathcal{SU} = \{su_1, su_2, ..., su_n\}$; $\mathcal{O} = \{o_1, o_2, ..., o_n\}$. $\mathcal{SU}$, $\mathcal{O} \in \mathcal{E}$.

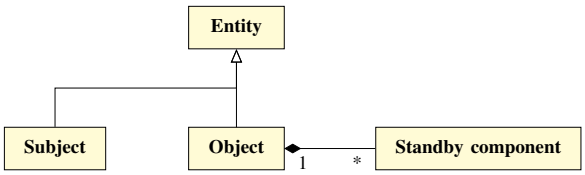

Fig. 6. UML representation of the entities: subject and object.

B. Roles

A role is defined as "a job function in an organization that describes the authority and responsibility conferred on a user assigned to the role" [7]. As shown in Section III, the role is specified as a set consisting of: $\mathcal{R} = \{$Customer, Service, Governance$\}$. Likewise, their constituting sub-roles are also part of this set. The concept of hierarchy is used to create levels of importance for the roles. The Role Hierarchy is defined as: RH $\subseteq \mathcal{R} \times \mathcal{R}$; which is a partial order in $\mathcal{R}$.

C. Security Constraint

Security Constraint is a set of type-value pairs symbolized by Φ. This set is represented as $\Phi = \{\phi_1, \phi_2, ...\phi_n\}$ each one defining a security quality, which are useful to measure the security characteristics of an object. Examples of the types that can be represented cover the security level of an object, its confidence level or whether the object is shareable or not. In order to exploit the information covered by Φ, it is necessary to define two functions: **(i)** *Type*(ϕ_n), which will provide the name of the security property; and **(ii)** *Value*(ϕ_n), which will provide the value of the respective property. This approach makes Φ extensible to any security characteristic and will be useful in order to establish comparison of the Security Constraint between objects in the policy decision point. Each type will have a comparison operator to compare two elements of the same type, as will be shown in Section V-D.

D. Session

Sessions constitute a mapping between a subject, a domain, a Security Constraint ϕ and the activated subset of the set of roles the user is assigned to [7]. One example to illustrate this concept is the *PDU session*, which is represented as a bearer (in the 4G case) or as a flow (in the 5G case). Another example corresponds to the request-response interaction between NF in the Service Based Architecture used by 5G. In our proposed model, subjects, as active entities, would establish sessions to perform an interaction with objects. A subject can establish multiple sessions, conforming a set: $\mathcal{S} = \{s_1, s_2, ...s_n\}$. A session is defined as $\mathcal{S} = \mathcal{R} \times \mathcal{SU} \times \mathcal{D} \times \Phi$.

E. Domain

The domain structure was presented in Section III, which is defined as a set: $\mathcal{D} = \{$Consumer, End-to-end, Slice$\}$. The domain concept can be considered as a form of boundary that, associated with permissions, contributes to add granularity to decide what is permitted. The permissions depend on from which domain a session originates and the domain to which an object belongs. The domain concept considers hierarchies as a way to create levels of importance. Domain Hierarchy is defied as: DH $\subseteq \mathcal{D} \times \mathcal{D}$; which is a partial order in $\mathcal{D}$.

F. Actions

Actions are procedures that are used by subjects via sessions in order to perform operations on objects. In the 5G Service Based Architecture, services are exposed by the 5GC NF and, in order to interact with them, some procedures are specified in the control plane [22] such as: $\mathcal{A}_{cp} = \{$ Request, Response, Subscribe, Notify, ServiceDiscovery $\}$. This reasoning can be enhanced by considering user plane actions $\mathcal{A}_{up}$ (which are not covered by 3GPP). Stateful traffic should be considered, due to the nature of most applications utilized by the users.

G. Permission

Describes the ability to perform an operation on a protected object or resource. A permission $\mathcal{P}$ is defined as:
$\mathcal{P} = \mathcal{R} \times \mathcal{D} \times \mathcal{A} \times \mathcal{O} \times \Phi$.

H. Policy

Contains all the access control rules that govern the interaction between subjects (via a session) and objects. This paper deals with policies that describe the case of the 5GC delivered as a self-contained slice, i.e., its internal domain interactions (between AN, CN, DN) and interaction with the user domain. The specificity is because besides the 5GC, the approach can be generalized to describe interactions inside a slice for any service, e.g., IoT, connected vehicle, etc. Policies, represented by Π, are defined as a set of permissions.

V. Auxiliary concepts for the global model

Section IV described each of the components of the global access control model. In order to merge them it is necessary to have tools to build relationships between them. We define messages, assignment operations, functions and a Compliance operator to do so.

A. Messages

Within the global model described in Section IV the action concept was presented. It contains the global operations that can be performed without considering its implementation. In order to specify the parameters of those actions, a message m $\in$ M is defined. m contains information such as IP address, logical ports, protocol and other information necessary to have a concrete message. In other words, the message is a subset of actions, but with the specification of parameters. For example, to request a subscription for an event:
a = Subscribe; a $\in$ A; m = Subscribe (o, *event*); $m \in$ M.
m describes the subscription for an *event* from an object o.

B. Assignment operations

The assignment operation relate the elements of two components of the model, that is, map their interaction. The considered assignment relations are:

1) Permission to role assignment relation: PR $\subseteq \mathcal{P} \times \mathcal{R}$; contains all pair (p, r) for which p $\in \mathcal{P}$ and r $\in \mathcal{R}$.
2) Object to domain assignment relation: OD $\subseteq \mathcal{O} \times \mathcal{D}$; contains all pair (o, d) for which $o \in \mathcal{O}$ and d $\in \mathcal{D}$.
3) Session to domain assignment relation: SD $\subseteq \mathcal{S} \times \mathcal{D}$; contains all pair (s, d) for which $s \in \mathcal{S}$ and d $\in \mathcal{D}$.

C. Functions

Are used to perform the mapping between the components that belong to the proposed model. For example, the Session to Role assignment is specified as sRole: $\mathcal{S} \rightarrow 2^R$.

There are functions that are used inside the policy, in order to find information inside them. The functions are:

1) Subject(D): return a concrete set of subjects in domain D.
2) Object(D): return a concrete set of objects in domain D.
3) Session(su): return a set of session $s \in$ S instantiated by a subject *su* $\in$ D.
4) Permission(π): find a policy π that has an allowed permission.
5) Message(su, o): return the set of messages that goes from *su* to an object *o*.
6) Procedure(m): return the name of the action that is contained in the message structure.
7) Action(π): validate the set of actions allowed by the policy π.

D. Compliance Operator

Our model requires the definition of a Compliance operator, symbolized by $\cong$. It is used when validating whether the Security Constraint of the subject is coherent with the Security Constraint specified for an object in the policy.

Property 1: The Compliance operator $\cong$ means that it is preferred to access an object that has a greater or equal value in a security parameter compared to the one in the origin:
$\forall\ \phi_{s1}, ..., \phi_{sn} \in \Phi_s, \exists\ \phi_{o1}, ..., \phi_{on} \in \Pi \mid \mathit{Type}(\phi_{si}) = \mathit{Type}(\phi_{oi}) \wedge \mathit{Value}(\phi_{si}) \geq \mathit{Value}(\phi_{oi}) \Rightarrow \Phi_s \cong \Phi_o$

The rationale of this operator is that for each pair in the source entity (session) ϕ_{si}, it needs to exist a pair of the same type in the destination entity (object) ϕ_{oi}. The $\geq$ symbol, the *greater or equal to* operator, provides a way to compare quantitatively the values of the attributes. For the specific use case of the 5GC, the value of the property of the source Security Constraint has to be equal or superior to the value of the property of the destination Security Constraint.

VI. Inter-domain interactions

Figure 7 depicts the permitted interactions between the domains in the 5GS. They constitute the properties of the security access control model. These interactions are inferred from the the functional model of the 5G architecture [22] and the procedures and NF services [24] specified by 3GPP. The architecture can be characterized as per Definition 1.

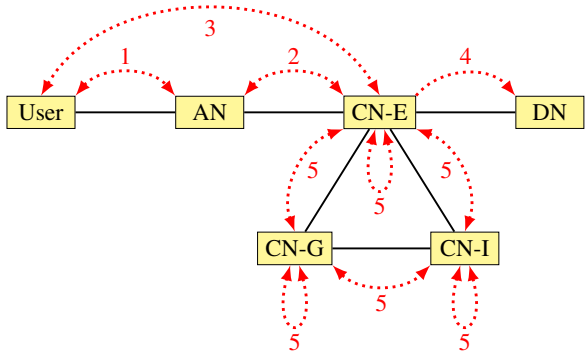

Fig. 7. Permitted inter-domain interaction map for the 5GS.

Definition 1: The inter-domain interactions can be represented as a graph $G = \{V, E\}$ with:
$V = \{$User, AN, CN-E, CN-G, CN-I, DN$\}$ the vertices which are the set of domains.
$E = \{$(User,AN), (AN,CN-E), (CN-E,CN-G), (CN-G,CN-I), (CN-I,CN-E), (CN-E,DN)$\}$ the set of authorized communications.

For instance, the considered interactions are: **(1)** actions between user and AN domains; **(2)** when NF in the AN domain need to communicate with NF in the exposed CN domain; **(3)** where an UE needs to have Non Access Stratum communication with NF in the CN domain (the AN domain acts as a transparent proxy); **(4)** the user generated traffic exits the Communication Service Provider network towards the DN domain; **(5)** covers the case in which a NF requires communication with another NF inside the CN domain.

Some examples of the actions for interaction **(5)** are **(i)** the Network Function Service Framework Procedure, which

includes NF service Registration, update, de-registration, NF to NF service discovery and service status subscribe/notify; **(ii)** procedures and flows for Policy Framework (when Application Functions are involved); and **(iii)** interactions for network slice selection and communication between Communication Service Management Function (CSMF) and Network Slice Management Function (NSMF).

The inter-domain communications are allowed only for links l belonging to E, that is, the set of authorized communications (see Property 2). In addition, there must be no other communications allowed for any link composed of two different domains belonging to V and not belonging to E (see Property 3).

Property 2:

$\forall\ l = (v_i, v_j) \in E \wedge \forall\ su \in Subject(v_i) \wedge \forall\ s \in Session(su) \wedge \forall\ o \in Object(v_j) \wedge \forall\ m \in Message(s, o) \wedge \forall\ r \in Role(s) \Rightarrow \exists\ \pi \in \Pi \mid s \in Session(\pi) \wedge o \in Object(\pi) \wedge \Phi(s) \cong \Phi(\pi) \wedge Procedure(m) \subset Action(\pi) \wedge Permission(\pi) =$ Allow

Property 3:

$\forall\ v_i, v_j \in V \wedge \forall\ su \in Subject(v_i) \wedge \forall\ s \in Session(su) \wedge \forall\ o \in Object(v_j) \wedge \forall\ m \in Message(s, o) \wedge \forall\ r \in Role(s) \mid v_i \neq v_j \wedge l = (v_i, v_j) \nexists E \Rightarrow \exists\ \pi \in \Pi \mid s \in Session(\pi) \wedge o \in Object(\pi) \wedge \Phi(s) \cong \Phi(\pi) \wedge Procedure(m) \subset Action(\pi) \wedge Permission(\pi) =$ Deny

VII. Discussion

RDAC, our proposed access control model, provides advantages compared to existing access control models, under the point of view of its application to the 5GS use case scenario.

It permits to include several functional attributes for the interacting NF, permitting to narrow down the possible actions that can be performed among them. This is an advantage with respect to RBAC, BLP and Denning models which offer less options to manage this quality. Moreover, it permits to establish attributes whose values are not only ordered sets or hierarchical values, but considers also named values that can be compared as a security constraint. Regarding ABAC, the model has to be defined before its usage, rendering it more difficult to configure. In addition, the setup of environmental variables do not match the interactions inside the 5GS. The 5GS is complex enough to add other layer of difficulty.

Our proposed model includes the functionality of the NF, that is, the role it plays, and its location in the SBA, serving as a differentiation mechanism for the interacting NF. This differentiation restricts the type of actions that NF can perform and, at the same time, what are the NF allowed to receive as requests. This differentiation constitutes an improvement with respect to DTE and Denning models.

RDAC is aligned to obey the specifications of 3GPP regarding the procedures that a subject must follow in order to gain access to a service in the 5GS. This quality goes beyond typical use cases where interacting entities have limited functions and services in information technology. RDAC goes beyond the notion whether how the data flows, but addresses the need to know if data is authorized to flow in the first place.

Finally, by specifying the actions in the policy, a high control is achieved, in function of the security properties specified via the security constraint, addressing the concrete needs of the 5GS use case scenario.

Even though this work covers the formalization of the model, its implementation is important to provide a proof of concept of the mathematical model. Due to space limits, the experimentation related to the implementation is not shown and will be presented in a forthcoming paper. As said in Section III, it is possible to implement a 5GS using network slices. In consequence, the implementation involves extending the interactions and analyzing the inter-slicing use case.

VIII. Conclusions

This paper addresses a major security concern for Communication Service Providers when faced with resource sharing, being this technique important when deploying 5G services and expanding network coverage.

Each stakeholder has its own internal security policies and security levels, so it is necessary to establish access control mechanisms that incorporate the required elements to restrict and authorize interactions according to those constraints.

Due to the fact that traditional access control models do not fulfill the requirements of the 5G architecture, a new method was created called RDAC. This novel approach picks the best concepts of RBAC and DTE access control models.

With the concept of **role** we restrict actions according to the function of a NF. With the concept of **domain**, we restrict interactions according to the section of the 5G system or stakeholder and whether the **session** created by a *subject* has authorization to establish communication with an **object** in the destination domain. With the objective to bind the aforementioned requirements, the concept of **Security Constraint** was created as a mechanism to specify several security properties.

The proposed **actions**, which leverage on the functional model of the 5GS, specify the appropriate procedures that can be executed over objects, being **permissions** the concept that links these two concepts together. The *property statement* represents the description of the required allowed communication. Finally, the **Compliance operator** is used as a mean to evaluate if the interaction can be authorized using the involved Security Constraints.

Something interesting about the proposed access control model is its extensibility: several security properties can be specified according to the needs of the Communication Service Provider. Moreover, the concepts that are used are general enough to apply to other use cases and architectures.

The usage of this new model lays the foundation for secure resource sharing among the different players involved in providing services over 5G networks. It constitutes an enabler to enforce security within the 5GC and offer more secure services to users and verticals.

REFERENCES

[1] 5G-PPP, "View on 5G Architecture (Version 2.0)," 2017.

[2] D. F. Ferraiolo, J. A. Cugini, and D. R. Kuhn, "Role-Based Access Control (RBAC): Features and Motivations," in *11th Annual Computer Security Applications Conference*, Dec. 1995.

[3] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, "Attribute-Based Access Control," *Computer*, vol. 48, no. 2, Feb. 2015.

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

[5] D. E. Bell and L. J. LaPadula, "Secure Computer Systems: Mathematical Foundations," Mitre Corp Bedford MA, Tech. Rep. MTR-2547-VOL-1, 1973.

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

[7] 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.

[8] R. S. Sandhu and P. Samarati, "Access control: Principle and practice," *IEEE Communications Magazine*, vol. 32, no. 9, Sep. 1994.

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

[10] R. S. Sandhu, "Lattice-based access control models," *Computer*, vol. 26, no. 11, Nov. 1993.

[11] M. Gasser, *Building a Secure Computer System*. New York, NY, USA: Van Nostrand Reinhold Co., 1988.

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

[13] 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.

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

[15] P. Watson, "A Multi-Level Security Model for Partitioning Workflows over Federated Clouds," in *2011 IEEE Third International Conference on Cloud Computing Technology and Science*, Nov. 2011.

[16] 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.

[17] U. Tupakula, V. Varadharajan, and K. Karmakar, "Access Control Based Dynamic Path Establishment for Securing Flows from the User Devices with Different Security Clearance," in *Advanced Information Networking and Applications*. Springer, 2020.

[18] A. Alshehri and R. Sandhu, "Access Control Models for Virtual Object Communication in Cloud-Enabled IoT," in *2017 IEEE International Conference on Information Reuse and Integration (IRI)*, Aug. 2017.

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

[20] V. Oleshchuk and R. Fensli, "Remote Patient Monitoring Within a Future 5G Infrastructure," *Wireless Pers Commun*, vol. 57, no. 3, Apr. 2011.

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

[22] 3GPP, "Specification # 23.501," 2018.

[23] 5G-ENSURE, "Deliverable D2.7 - Security Architecture," Feb. 2016.

[24] 3GPP, "Specification # 23.502," 2019.