On an Access Control Model enhancement for the 5G System

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

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, {firstname.lastname}@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.

Introduction

- In 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.
- 5GS entities can be served by different providers: 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.
- Current access control models do not address these requirements, their properties cannot be directly applied to the 5G system.
- **Objective**: state the qualities of an access control mechanism suitable for the 5G System.

Current approaches

Traditional methods:

- Role Based Access Control (RBAC): role concept to group job functions. Users and permissions are assigned to the roles.
- Domain and Type Enforcement (DTE): a Type can be assigned to objects and a Domain to processes.
- Lattice-based: analyzes how information flows in a computer system, using Security Classes.

Usage on new use cases:

- IoT: restrict access by labeling data.
- V2x: confidentiality to video information.

5G System use case is not addressed.

Problems in current approaches

- Lack of granularity to reflect the 5G S architecture.
- Little support for diversity of attributes.
- Need for segmentation capabilities and limit actions.
- Hard definition of security classes and clearances: The 5GS is complex enough.

Lack of 3GPP guidance:

- Restrict inner interactions between 5G System components.
- Supervise the interactions among those components: actions, messages, restrict and segment the influence between them.

Ideal Access Control model for the 5GS

Take consideration of the Service Based Architecture (SBA)

- Network functions.
- Offered services.
- Deployment planes.
- Traffic and messages.

The 5G System is end-to-end:

- Interactions between access, core and data network
- Amount of entities that interact in a domain.

Include external and internal actors.

- And the interactions between the service provider and external stakeholders.

Conclusions

We selected the best qualities from traditional access control models, which are needed in an access control mechanism in order to be used in the 5GS:

- Roles.
- Domains.
- Sessions.
- Context for the 5G procedures.

These key characteristics guarantee that several security properties can be specified according to the needs of the communications service provider.
Their usage enforces security within the 5G system and offer more secure services to users and verticals.

b<>com
UBO Université de Bretagne Occidentale
IMT Atlantique Bretagne-Pays de la Loire École Mines-Télécom