Attribute Based Access Control for IoT Devices in 5G Networks

Sascha Kaven and Volker Skwarek

HAW Hamburg

Abstract

The deployment of 5G technology has the potential to usher in a new era for the internet of things (IoT). The introduction of new use cases, such as massive machine-type communications (mMTC), referring to a large number of IoT devices, resulting in the increasing importance of 5G as the basic communication infrastructure for IoT. However, the increasing connectivity of IoT devices coincides with a number of risks to security. Many IoT sensors have limited resources and, therefore, cannot perform the complex security measures required to protect them from attacks and data loss. Furthermore, IoT networks are very scattered, distributed and dynamic, so decentralised security measures are required. To address these challenges, this poster proposes the integration of attribute-based access control (ABAC) into the 5G service-based architecture. This approach aims to prevent unauthorized access to IoT devices at the network level, thereby alleviating the computational burden on resource-constrained IoT devices. By implementing ABAC, the proposed solution offers a more efficient method for managing access control within the IoT landscape in the context of 5G networks.

Introduction

The fifth generation of mobile communication networks (5G) offers a wide range of new use case scenarios. While the previous connectivity schema 4G focuses on the mobile broadband use case, 5G differs by not only providing faster speed, higher bandwidth, and lower latency but also supporting more use cases, such as enhanced mobile broadband (eMBB), massive machine-type communications (mMTC), and ultra-reliable low-latency communications (uRLLC). As a result, 5G is gaining an increasingly central role in basic communication infrastructures, especially for smart-x-applications and critical infrastructures. However, the increasing need for the interconnection of components also poses security risks. The predominantly decentralized structure of smart-x-applications and the requirements for IoT sensors contradict the security requirement of minimum exposure, according to which external access to a system must be minimized. In order to counteract the increased risk of being exposed to threats from other players, complex security measures need to be implemented. However, one of the most significant issues with IoT devices is their limited computing and battery capacity, which leads to security implications because they cannot perform the complex security measures required to protect them from attacks and data loss.

Although traditional access control systems, such as Mandatory Access Control (MAC) and Role-Based Access Control (RBAC), can offer a certain level of protection for IoT devices, Attribute-Based Access Control (ABAC) provides enhanced security in a specific aspect: its ability to react on dynamically changing authentication requirements and environmental conditions of IoT devices, which are further referred to as resources coyne2013abac. A resource defines a set of rules and a list of identity attributes required for the authorization - and these attributes may even change over time. Traditional access control mechanisms are ill-suited for IoT networks. These approaches pose significant challenges in terms of maintenance and scalability [2], making them inadequate for effectively managing access control within the complex and rapidly evolving IoT landscape. A relatively modern approach is Attribute Based Access Control (ABAC), where access rights are set based on attributes of the subject, object and environment to access the resource. Examples of this could be attributes such as the role of the subject, the location of the device, and the type of request.

In order to counteract the resource bottleneck on IoT devices, access control should not be performed on the IoT devices but rather in the network before a session is established between the subject and the resource. This makes it possible to block unauthorized users before establishing a connection to the IoT device. The approach presented in this poster is intended to link ABAC with 5G, aiming to integrate the new functions as seamlessly as possible into the existing 5G core and to extend the existing network functions (NF).

ABAC in the 5G services-oriented architecture

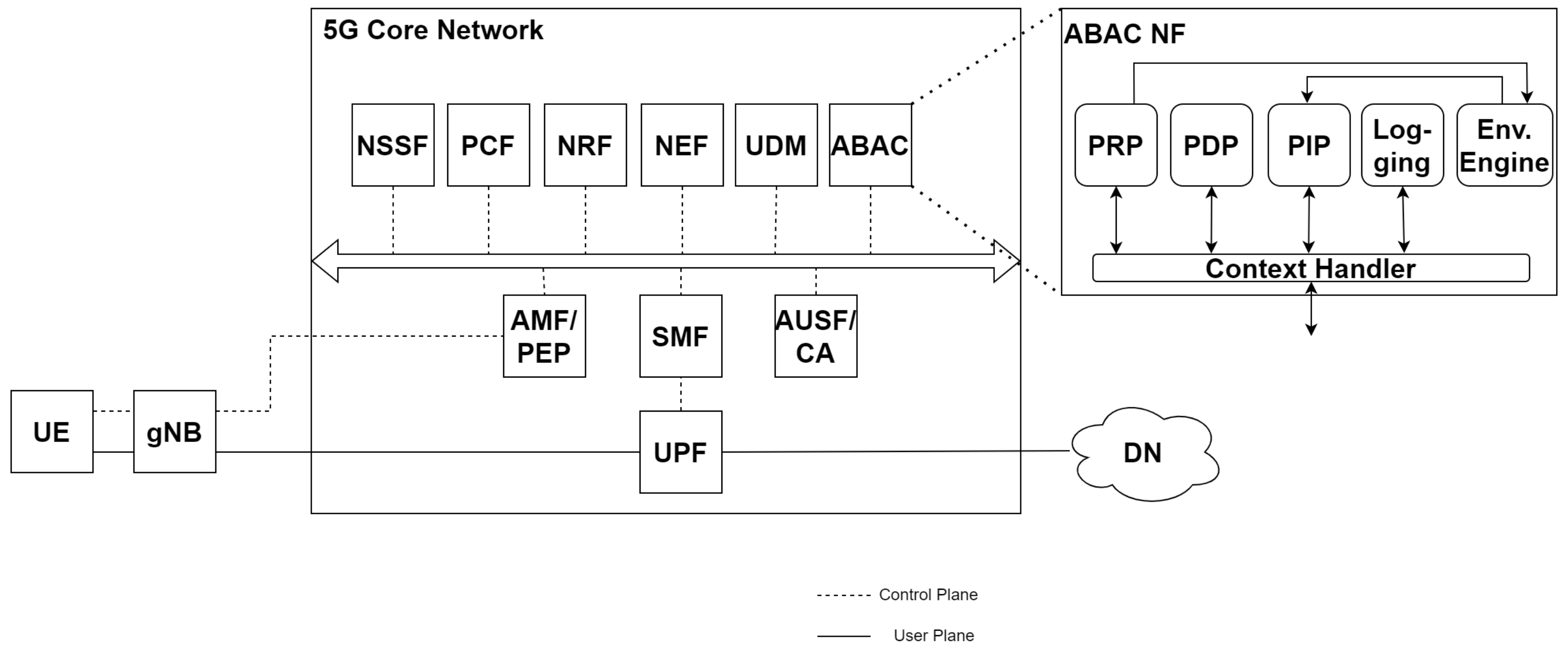

Figure 1. 5G service-oriented architecture extended by ABAC

The 5G service-based architecture, which is defined in [1], forms the basis for the provision of services in the 5G network. The 5G network can be divided into two logical components. The radio access network (RAN) builds the link between the subject and the core network and the 5G core network (5GC) itself. The 5G core network is a critical component of the 5G infrastructure, responsible for advanced mobile services and applications. It provides a high-performance and scalable communication infrastructure that enables end-to-end connectivity for devices, services and applications.

In order to establish a connection to the IoT device a users mobile device (user equipment, UE), such as a cell phone or tablet connects to a 5G wireless base station (gNB) managing the communication between the UE and the core network. The access and mobility management function (AMF) performs operations like mobility-, registration-, connection management, UE-based authentication, etc. Based on the service requested by the UE, AMF selects the respective session management function (SMF) for managing the user session context. The SMF is primarily responsible for interacting with the decoupled data plane, creating, updating and removing protocol data unit (PDU) sessions and managing session context with the user plane function (UPF). The 5G UPF connects the actual data stream between the user and the IoT device.

To protect the IoT devices from unauthorized access, in this approach the access control will already be performed in the process of creating a PDU session between user and IoT device. This makes it possible to prevent an unauthorized access attempt even before the first interaction of the user with the IoT device. However, to achieve this, ABAC components must be integrated into the 5G architecture. Figure 1 shows the 5G service-oriented architecture extended by ABAC.

The policy enforcement point (PEP) is responsible for accepting the access request in ABAC and should therefore be included at an early stage in the access request. Within the 5G network, all requests on the core side are accepted by the Access and Mobility Management Function (AMF). The AMF is responsible for the authentication, registration and distribution of requests. The AMF is also seen as an administrative component within the 5G core and has most of the specified interfaces to other components 3gpp.23.501. For this reason, the AMF is ideally suited to be extended to perform the tasks of PEP.
The remaining ABAC components such as the Policy Decision Point (PDP), which enforces access decisions, and the Policy Information Point (PIP), which manages attribute data, are integrated into a single, cohesive module. The ABAC module is defined as a new NF in the 5G core. Since there is no access control in this form in 5G to date, integrating the various components of the ABAC module into existing NFs would merely avoid the desired separation of duty without offering any significant benefit. Furthermore, if the module were split, the respective interfaces of the NFs would have to be reworked. This could impede adoption, as it would entail a considerable amount of supplementary effort to implement these alterations.
To start an access request in the 5G network extended by ABAC, the user sends a corresponding access request to the network. This access request contains information about the IoT device to which a connection shall be established as well as the attributes of the user. The access request is received in the network by the AMF extended by the PEP functionalities and passed on to the ABAC module. The ABAC module then collects the environment attributes of the corresponding instances necessary for the access decision, as well as the policies necessary for the evaluation. The policies can either be stored in a central repository or decentrally on the individual IoT devices and can be requested by the network if required. As soon as all the information is available, the PDP evaluates the access request and transmits the result to the SMF. If access is granted, the SMF establishes a PDU connection between the user and the IoT device. However, if access is denied, no PDU session is created and the user is thus unable to communicate with the IoT device.

Evaluation

An initial proof-of-concept implementation of ABAC NF as a implementation of the XACML standard was developed to evaluate the evolved concept for integrating ABAC into the 5G service-oriented architecture. In a further step, the developed module will be integrated into the Open5GS open-source core to test the module in real 5G environments. In addition to parameters such as latency and data rate, the focus of the tests will be on preventing attacks on IoT devices. To achieve optimal flexibility and scalability, the entire system will be incorporated into a Kubernetes cluster, facilitating dynamic load management and enabling the system to adapt seamlessly to varying workloads and resource demands.

References

[1] 3GPP.
System architecture for the 5G System (5GS).
Technical Specification (TS) 23.501, 3rd Generation Partnership Project (3GPP), Juni 2022.
Version 17.5.0.

[2] Ed Coyne and Timothy R Weil.
Abac and rbac: scalable, flexible, and auditable access management.
IT professional, 15(03):14–16, 2013.