International Journal of Advance Research in Science and Engineering
Vol. No.8, Issue No. 12, December 2019
www.ijarse.com
IJARSE
ISSN 2319 - 8354

5G Authentication Protocol

Rajesh Yadav

Computer Science Deparmtment, BML Munjal University, Gurgaon, India

Abstract: *Mobile network fundamental security concepts are authentication and key management as both mutual authentication as well as keys derivations for signaling and user data is their responsibility. We have gone through many generations of cellular networks and every generation has defined at least one method of authentication,4G technology has EPS-AKA and 5G has 5G-AKA, EAP-AKA as well as EAP-TLS. This paper gives an overview of 5G-AKA protocol which is used for authentication in 5G networks.*

Keywords: 5G, AKA, authentication

1 Introduction

In the core network of 5G, service-based architecture i.e. SBA has been proposed. As a part of it, new service requests as well as new entities have been defined for 5G networks. These entities are security anchor function, authentication server function, unified data management and subscription identifier de-concealing function.

During the process of authentication, Security Anchor Function i.e. SEAF works as middleman between user equipment and home network. Authentication request from user equipment can be accepted or rejected, but it depends on the home network of user equipment to come to a decision.

Authentication Server Function i.e. AUSF performs user equipment authentication, it takes the decision for authentication based on backend service for authentication data computation as well as keying materials in case 5G-AKA or EAP-AKA is used. Data management has different functions like authentication processing function as well as credential repository to select the method of authentication depending on identity of subscriber as the policy which is configured, it then computes authentication data and keying material for authentication server function if required[1].

Subscription concealed identifier is being decrypted by the subscription identifier de-concealing function for obtaining the long-term identity like the subscription permanent identifier for example IMSI. In case of 5G networks, encryption is being done before transmitting the long-term identity over the radio interfaces, for this public key encryption is used for protecting the SUPI. As a result of this, SIDF only has access to the private key attached with a public key which is distributed to user equipment for the encryption of their SUPI's. 5G authentication framework is being introduced in the next section and 5G-AKA protocol is being explained in detail.

2 5G Authentication Framework

For making 5G authentication in open as well as access network agnostic(like both 3GPP networks, no-3GPP networks such as cable and Wi-Fi networks(See Fig.1), a unified authentication framework has been defined. Extensible authentication protocol authentication works between user equipment(EAP peer) and the

authentication server function(EAP Server) through SEAF(functioning as an EAP pass-through authenticator) when EAP is used(EAP-AKA or EAP-TLS)

In case of over untrusted authentication, a new entity i.e. non-3GPP interworking function (N3IWF) is needed to work as a virtual private network server for allowing user equipment to access 5G over untrusted, non-3GPP networks through IPsec (IP Security) tunnels[2].

Using one authentication execution, many security contexts can be established for allowing the user equipment to move from a 3GPP access network to a non-3GPP network without any need to go through re authentication process.

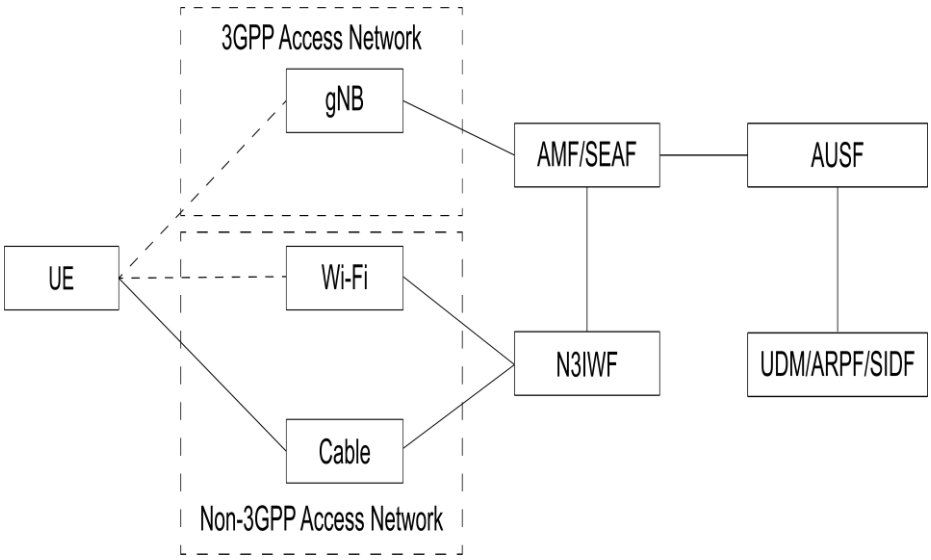

figure 1 – 5g authentication framework

2.1 5G-Authentication and Key Agreement

New authentication-related services are being defined in 5G technology, like the AUSF goes through Nausf_UE authentication to provide authentication service and unified data management goes through Nudm_UE authentication. For the sake of simplicity, authentication request and authentication response are used as generic messages without referring to the real authentication service names. Also, an authentication vector includes a set of data, but only a subset is shown in Fig. 2.

International Journal of Advance Research in Science and Engineering
Vol. No.8, Issue No. 12, December 2019
www.ijarse.com
IJARSE
ISSN 2319 - 8354

figure 2 – 5g-aka authentication procedure

After receiving any signaling message from user equipment, the SEAF may start the authentication procedure in 5G-AKA. It needs to be noted that the user equipment has to send the SEAF a temporary identifier (a 5G-GUTI) or an encrypted permanent identifier (a SUCI) if a 5G-GUTI has not been allocated by the serving network for the UE.SUPI is being encrypted to form SUCI, this encryption uses home network public key. Therefore, permanent identifier of user equipment for example, the IMSI is always sent in encrypted form over 5G radio network. Over prior generations such as 4G[3], this feature is a major security improvement.

An authentication request to the AUSF is being sent by SEAF to initiate the authentication, AUSF verifies the authorization of serving network which is requesting the authentication service. An authentication request to UDM/ARPF is being sent by AUSF in case of success. If AUSF provides the SUCI, then SIDF will be invoked to decrypt the SUCI to obtain the SUPI, which is further used to select the authentication method configured for

the subscriber. In this case, it is 5G-AKA, which is selected and to be executed.5G-AKA is being started by UDM/ARPF by sending the authentication response to the AUSF with an authentication vector having AUTH token, an XRES token, the key KAUSF, and the SUPI if applicable (e.g., when a SUCI is included in the corresponding authentication request) among other data[4].

The AUSF computes a hash of the expected response token (HXRES), stores the KAUSF, and sends the authentication response to the SEAF, along with the AUTH token and the HXRES. Note that the SUPI is not sent to the SEAF in this authentication response. It is only sent to the SEAF after UE authentication succeeds.

The SEAF stores the HXRES and sends the AUTH token in an authentication request to the UE. The UE validates the AUTH token by using the secret key it shares with the home network. If validation succeeds, the UE considers the network to be authenticated. The UE continues the authentication by computing and sending the SEAF a RES token, which is validated by the SEAF. Upon success, the RES token is further sent by the SEAF to the AUSF for validation. Note that the AUSF, which is in a home network, makes the final decision on authentication. If the RES token from the UE is valid, the AUSF computes an anchor key (KSEAF) and sends it to the SEAF, along with the SUPI if applicable. The AUSF also informs UDM/ARPF of the authentication results so they can log the events, e.g., for the purpose of auditing[5].

Upon receiving the KSEAF, the SEAF derives the AMF key (KAMF) (and then deletes the KSEAF immediately) and sends the KAMF to the co-located Access and Mobility Management Function (AMF). The AMF will then derive from the KAMF (a) the confidentiality and integrity keys needed to protect signaling messages between the UE and the AMF and (b) another key, KgNB, which is sent to the Next Generation NodeB (gNB) base station for deriving the keys used to protect subsequent communication between the UE and the gNB. Note that the UE has the long-term key, which is the root of the key derivation hierarchy. Thus, the UE can derive all above keys, resulting a shared set of keys between the UE and the network[6].

Areas mentioned below differentiates 5G-AKA from EPS-AKA of 4G:

Due to the new service-based architecture of 5G, the authentication entities are different. Specifically, the SIDF is new and in 4G, it does not exist.

Before sending the user equipment permanent identifier to 5G network, public key of the home network is used by user equipment to encrypt it.

The UE always uses the public key of the home network to encrypt the UE permanent identity before it is sent to a 5G network. In case of 4G network, permanent identifier of the user equipment is always sent in clear text to the network, this makes it possible to steal it by a malicious network like a rogue base station of even by a passive adversary over the radio links (if communication over radio links is not protected)[7].

In 5G, final decision on user equipment authentication is being made by the home network(e.g. AUSF). In addition to this, user equipment authentication results are being sent to unified data management for logging purpose. In case of 4G network, only to generate authentication vectors, the home network is consulted during authentication, it does not decide on authentication results.

As compared to 4G, key hierarchy is longer in 5G due to the reason that two intermediate keys are introduced in 5G i.e. KAUSF and KAMF, KSEAF is the anchor key in 5G, equivalent to KASME in 4G.

3 Conclusion

In case of mobile networks, authentication and key management are very important as they are highly responsible for user protection as well as networks, and communication between them. Authentication process in 5G has improved a lot as compared to 4G in a number of areas like unified authentication framework, better UE identity protection, enhanced home-network control, and more key separation in key derivation, however 5G authentication is not without its weaknesses. For example, in case of 5G network, user trackability may still be possible[8].

Support of multiple authentication methods(non-AKA-based methods such as EAP-TLS) and open framework are also other noticeable difference in 5G authentication. Since AKA-based mechanisms have been primary authentication methods supported in 4G and its prior generations, so feature is encouraging.

Different use cases are intended to be supported by 5G,and few of them may be more suitable for non-AKA-based mechanisms. In case of wireless and wireline convergence scenario, user equipment such as a laptop behind a residential gateway may not have a USIM; it would not be able to execute AKA protocols even though it needs to be able to register and connect to the 5G core. In such a case, non-AKA-based methods such as EAP-TLS or EAP-TTLS can be used to authenticate the user to the 5G core. Different use cases are envisioned in 5G technology, by including security enhancements and other authentication methods, future work on 5G authentication could support those use cases.

References

1. Zhenhua Li, Weiwei Wang, Christo Wilson, Jian Chen, Chen Qian, Taeho Jung, Lan Zhang, Kebin Liu, Xiangyang Li, and Yunhao Liu, “FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild,” Proceedings of the Internet Society Symposium on Network and Distributed System Security (NDSS) (February 2017).

2. Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, and Jean-Pierre Seifert, “Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems,” Proceedings of the Internet Society Symposium on Network and Distributed System Security (NDSS) (Feburary 2016).

3. 3GPP, “3GPP System Architecture Evolution (SAE)—Security Architecture” (Release 15), technical specification (TS) 33.401, v15.2.0 (September 2018).

4. 3GPP, “Security Architecture and Procedures for 5G System” (Release 15), technical specification (TS) 33.501, v15.5.0 (September 2018).

5. Byeongdo Hong, Sangwook Bae, and Yongdae Kim, "GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier," Proceedings of the Internet Society Symposium on Network and Distributed System Security (NDSS) (February 2018).

6. Internet Engineering Task Force, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')," Request for Comments (RFC) 5448 (May 2009).

7. David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler, "A Formal Analysis of 5G Authentication," Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18) (October 2018).

8. Sami Tabbane, "4G and 5G networks security techniques and algorithms", ITU PITA Workshop on Mobile network planning and security", 23-25 October 2019.