Authentication in 4G and 5G - Case Study

by . .

Submission date: 11-Jul-2021 12:23PM (UTC-0400)
Submission ID: 1618203766
File name: Authentication_in_4G_and_5G_-_Case_Study.docx (323.39K)
Word count: 1740
Character count: 10051

Authentication Process in 4G and 5G

ITE – 511 – Wireless and Mobile Networks

7/11/2021

Table of Contents

1. Introduction

Organizations provide Authentication for their network to restrict the access from unauthorized users from using their premises, including overall network, websites, computer systems, databases, and other network-based applications or services. Mobile authentication is also necessary as network authentication, in which the identity of a user can be verified by using the mobile phone through one or more authentication processes. The network technologies are most important in mobile networking authentication. The cellular network technologies can be categorized into 2G, 3G, 4G, and 5G. The primary concept of cellular network security is that Authentication occurs between the user and the network through cryptographic key management and Authentication. The authentication method will change as per the generation of the cellular networks. This case study compares the authentication process in 4G and 5G cellular networks.

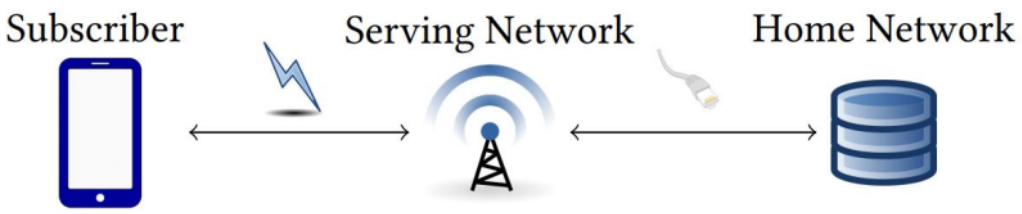
2. Importance of Authentication in Mobile Networks

The approximate number of mobile subscribers in the world becomes two-thirds of the total population, which means two of three are using any one of the mobile networks. Moreover, the subscribers are connecting the SIM cards through any of the mobile networks. Therefore, users' communication through these cellular networks must be secured and achieved using mutual Authentication between the users and the cellular network carrier. Users can make their mobile secured by using the following methods:

- By using passwords for the applications.
- By using digital certificates which include encrypted data.
- By using OTP (One Time Password) authentication through SMS.
- By using biometric authentications such as facial, iris, voice, or fingerprint.

The cellular network carriers also use authentication methods on the other side by ensuring that the communication is genuinely secured and varies from network generation such as 4G and 5G. For example, in 4G, EPS-AKA is the authentication method is used, whereas, in 5G, three authentication methods are used; 5G-AKA, EAP-AKA, and EAP-TLS. In short, the AKA (Authentication Key Agreement) protocols are used in both 4G and 5G networks.

The security breaches and the cyber-attacks are increased every quarter of each year, especially in this COVID-19 pandemic situation. The traditional security methods are not enough to manage the new cyber attacking methods, and these attacks are mainly focused on mobile devices and remote workers. Most people store their personal information, including passwords and other confidential data, kept on mobile devices. In the 2G or 3G networks, the security issues have originated either lack of authentication protocols or the confidentiality of the messages passing through the networks. For this reason, the Authentication of mobile devices and cellular networks are equally important and to resolve these issues. The AKA protocols are used in 4G and 5G networks. Whenever a new mobile device is added to the mobile network, the cryptographic key stored in the USIM application is also shared with the Home Network. The architecture of a standard cellular network is given below:



3. Authentication Process in 4G

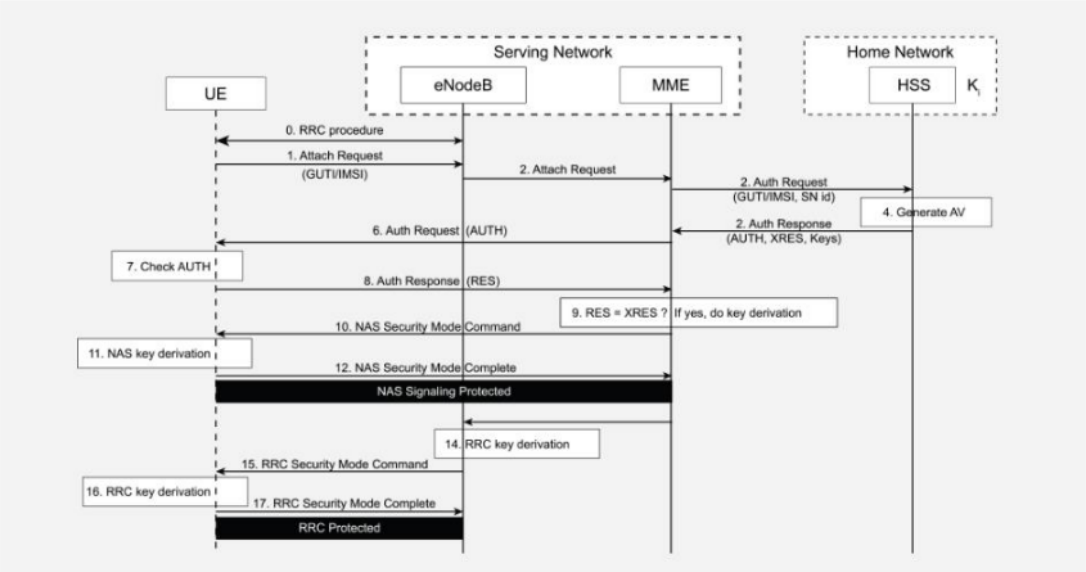
The fourth-generation network, 4G, uses Radio interfaces through Radio Access equipment used to communicate with the Serving Network with the UE. The Home Network, in which the mobile device is registered, contains a Home Subscriber Server (HSS), consisting of user authentication details and other user credentials. In addition, an IP Network is used for the communication between the Serving Network and the Home Network. The authentication method used in the 4G network is 4G EPS-AKA.

3.1 4G EPS-AKA

3.1.1 Working of EPS-AKA:

The eNodeB in the Serving Networks sends an Attach Request to the MME after completing the Radio Resource Control (RRC) procedure by the UE and triggering the EPS-AKA protocol in the 4G network. Then, the MME in the serving network will send an Authentication Request to the

HSS in the Home Network. The Authentication Request will contain the UE identity and the serving network identifier. Next, the HSS performs the cryptographic operations based on the secret keys, generates Authentication Vectors (AV), and sends them back to the MME Authentication Response. After getting the Auth Response from the HHS, the MME sends an Authentication Request to the UE, which includes the Auth token, and the UE verifies the Auth token and sends an authentication response to the MME. The MME then validates the Auth response with the expected response, and if both of them are equal, it derives the key to protect the subsequent NAS signal messages. Then the NAS signals are protected, and the MME derives a RRC key and send to the UE so that the RRC gets protected. This is the whole procedure for the Authentication and protection of the network in 4G.



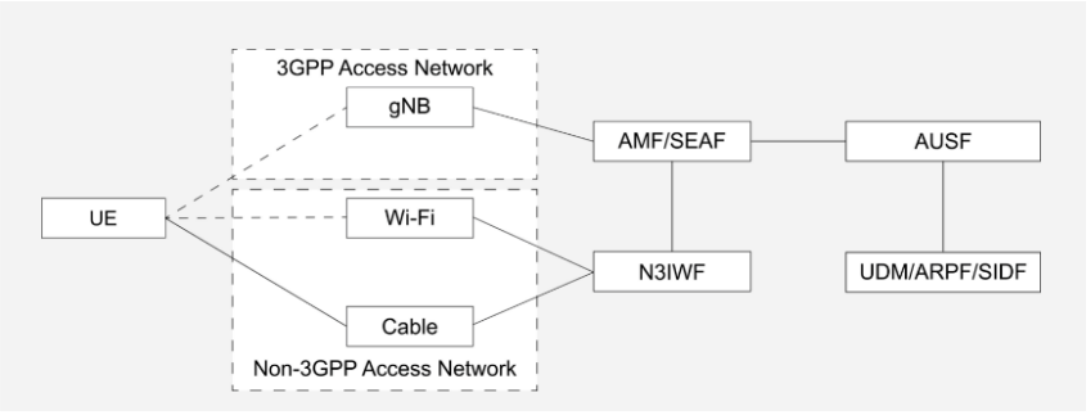
4. Authentication Process in 5G

The core concept of the 5G core network is the Service-Based Architecture, and the new entities and new service requests are defined in it. Some of the new entities are SAF, AUSF, UDM, and SIDF. The Security Anchor Function (SAF) in 5G authentication can act as a middleman and reject the unwanted Authentication from the UE. The Authentication Server Function (AUSF) can make decisions on the authentications in the background. The Unified Data Management (UDM) can

select the authentication method utilizing the subscriber entity and policies. Public key encryption is used in 5G, and Subscription Identifier De-concealing (SIDF) can decrypt the codes using the private keys of UE. Three authentication methods are used in the authentication framework in 5G: 5G-AKA, EAP-AKA, and EAP-TLS.

3.2 5G Authentication Framework

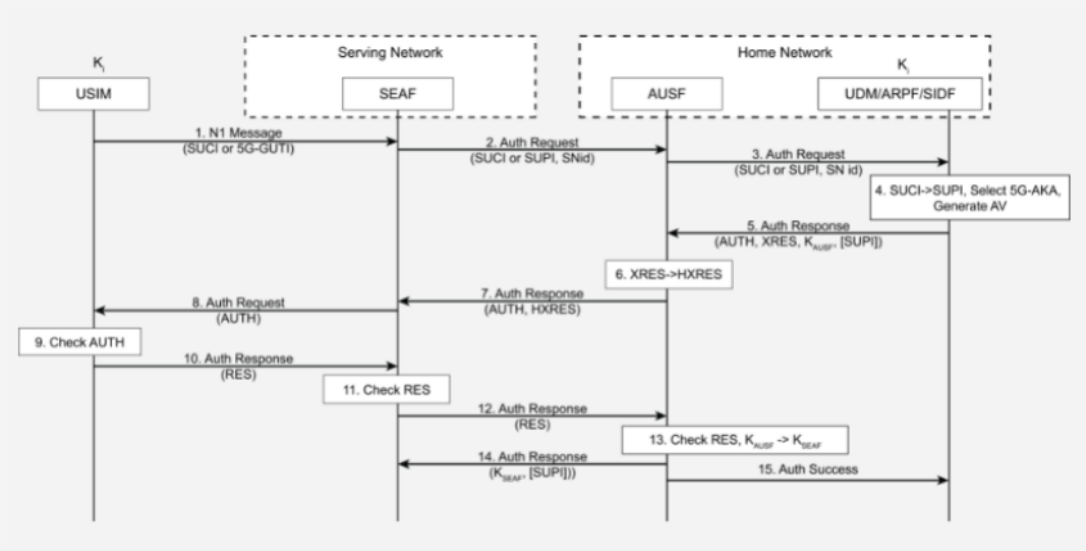
In the 5G network authentication, a unified authentication framework can be used to access the network securely. An Extensible Authentication Protocol (EAP), either EAP-AKA or EAP-TLS, is used to authenticate the UE and the AUSF. For a trusted authentication 3GPP, from gNB, the SEAF or AMF is used for the Authentication between UE and AUSF. For authentication from a non-trusted resource such as Wi-Fi or Cable, the N3IWF is used for the authentication process. It will allow the user to access the network without re-authentication for the next time. The Authentication Framework of 5G is shown below:



3.3 5G-AKA

The 5G network introduces new services related to Authentication and is more accessible than 4G. The USIM sends the message to the SEAF in the Service Network, and the SEAF will starts the authentication process in the 5G. SEAF sends an Authentication request to AUSF in Home Network, and it will request the Authentication from the UDM/ARPF and to USIM. The UE will validate the Authentication with the private key provided by the Home Network and respond to SEAF. The SEAF will check the response and send it back to the AUSF. After getting the Authentication Response from the SEAF to AUSF, it will generate the hash of the expected

response and authenticate with sending the key as a response. The following figure shows the authentication procedure in 5G-AKA.



3.4 EAP-AKA

Another authentication method used in 5G networks is EAP-AKA which is based on a cryptographic key. This protocol is also based on mutual Authentication between UE and Home Network. The EAP messages are contained in the NAS messages and are different from the 5G_AKA. The EAP messages are exchanging between UE and AUSF through the SEAF without having an authentication in SEAF.

3.5 EAP- TLS

For the limited use cases' Authentication, such as private networks and IoT environments, we can use the EAP-TLS method in the 5G network. The Authentication between the UE and the USM/ARPF through the SEAF utilizing a transparent EAP authenticator and exchange messages between UE and the AUSF. Through the TLS handshaking, both the UE and AUSF validates the pre-shared key for mutual Authentication.

5. Conclusion

For any cellular networks including 4G and 5G, Authentication and critical management will help protect user communications in the networks. However, the Authentication in the 4G and 5G networks are different in many areas, such as 5G supports open framework authentication, which contains a non-AKA-based authentication method (EAP-TLS), and 4G does not support them. Some of the common differences between the 4G and 5G networks are listed below:

- **Speed Upgrades**: The speed of the 5G cellular network is faster than that of 4G LTE.
- **Low Latency**: Latency is the measurement of the time that a signal takes to reach its destination and the latency in 5G is faster than 4G.
- **Enhanced Capacity**: The capacity of the 5G network is 1000 times better than the 4G network.
- **Increased Bandwidth**: The speed and network capacity of the 5G network are faster, allowing the users to transmit a large amount of data than the 4G.
- **Availability of Coverage**: The coverage area for the 5G network will be limited, but it's larger than 4G.

5G network uses the mutual authentication process, making the communication between the user and the network more secure and faster. Furthermore, the public critical encryption method used in the 5G network will help the Authentication more specifically than that of the 4G cellular network. The common difference between the 4G and 5G networks is that the authentication method used in both of them. In 4G, the EPS-AKA is used for the Authentication, whereas in 5G, 5G-AKA, EAP-AKA, and EAP-TLS methods are used for the Authentication. Thus, it means the Authentication in 5G uses open frame works and uses mutual Authentication using the public key encryption method between the UE and the Home Network for the communication. Although, from the above case study, the 5G network is better than the 4G LTE cellular network in terms of Authentication, speed, capacity, latency, etc. in the future, the 5G network will use additional security enhancement for the authentication purpose.

6. References

https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2019/ITUPITA2018/ITU-ASP-CoE-Training-on-/4G%20and%205G%20network%20security%20techniques%20and%20algorithms.pdf

(n.d.). arXiv.org e-Print archive. https://arxiv.org/pdf/1806.10360.pdf

Benefits of 5G technology: 5g features and advantages. (n.d.). Intel. https://www.intel.com/content/www/us/en/wireless-network/5g-benefits-features.html

A comparative introduction to 4G and 5G authentication. (2019, March 7). CableLabs. https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication

Efficient authentication and re-authentication protocols for 4G/5G heterogeneous networks. (2020, May 24). EURASIP Journal on Wireless Communications and Networking. https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-020-01702-8

Network authentication. (n.d.). ScienceDirect.com | Science, health and medical journals, full text articles and books. https://www.sciencedirect.com/topics/computer-science/network-authentication

A survey on authentication and access control for mobile networks: From 4G to 5G. (2019, July 12). Annals of Telecommunications. https://link.springer.com/article/10.1007/s12243-019-00721-x

What is the difference between 4G and 5G. (2021, February 19). [Official] The World's #1 Phone to Phone Transfer Solution | Wondershare MobileTrans. https://mobiletrans.wondershare.com/5g/4g-vs-5g.html?gclid=Cj0KCQjwiqWHBhD2ARIsAPCDzamtU6vOLih2AAtiC01nzrR_mhXI4lgZwqLQDUzX1H-73rkM-g-Dc_waAkbOEALw_wcB

Authentication in 4G and 5G - Case Study

ORIGINALITY REPORT

12%	11%	3%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.cablelabs.com Internet Source	9%
2	Chandra Sekhar Mukherjee, Dibyendu Roy, Subhamoy Maitra. "Chapter 2 Telephony Architecture", Springer Science and Business Media LLC, 2021 Publication	1%
3	S. R. Mani Sekhar, G. Nidhi Bhat, S. Vaishnavi, G. M. Siddesh. "Chapter 12 Security and Privacy in 5G-Enabled Internet of Things: A Data Analysis Perspective", Springer Science and Business Media LLC, 2021 Publication	1%
4	cors.archive.org Internet Source	1%
5	jwcn-eurasipjournals.springeropen.com Internet Source	1%
6	www.coursehero.com Internet Source	1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		