Politeia
Ano XIX – 2022, pp. 113-120

5G & Cybersecurity

JOAQUIM M. DA CUNHA VIANA
Universidade Autónoma de Lisboa, Autonoma TechLab
https://orcid.org/0000-0002-7574-7235
DOI: https://doi.org/10.57776/j8m2-6d09

Resumo: As comunicações 5G estão previstas para alterar o ambiente de comunicação num futuro próximo. A interacção entre equipamentos com escassa ou mesmo nenhuma interferência humana introduzirá novas vulnerabilidades de segurança, algumas das quais não estão, muito provavelmente, sequer previstas neste momento. Tendo isso em mente, o projecto 3GPP está a tentar pôr em prática várias normas para que os utilizadores possam sentir-se mais confiantes quanto à privacidade dos seus dados.

Palavras-chave: 5G; cibersegurança; tecnologia new radio

Abstract: 5G communications are previewed to change de communication's environment in the near future. Interaction between pieces of equipment with scarce or even no human interference shall introduce new security vulnerabilities, some of which are, most likely, not even foreseen at this moment. With that in mind the 3GPP project is trying to put in place several standards so that users may feel more confident about their data privacy.

Keywords: 5G; Cybersecurity; new radio

Resumen: Se prevé que las comunicaciones 5G cambien el entorno de la comunicación en un futuro próximo. La interacción entre equipos con escasa o incluso nula interferencia humana introducirá nuevas vulnerabilidades de seguridad, algunas de las cuales, muy probablemente, ni

Joaquim M. da Cunha Viana
Universidade Autónoma de Lisboa – jviana@automoma.pt
Submetido em: 13/06/2021. Aceite em: 31/03/2022

siquiera están previstas en este momento. Teniendo esto en cuenta, el proyecto 3GPP está tratando de establecer varios estándares para que los usuarios puedan sentirse más seguros sobre la privacidad de sus datos.

Palavras-clave: 5G; ciberseguridad; tecnología new radio

Introduction

Historically, information systems security has been seen by management as a mere cost. Nowadays pandemic, forcing the adoption of a work from home paradigm brought to attention the possibility of hacking attacks and consequent losses for organizations.

Concurrently, the 5G network and Internet of things appearance and evolution – which is expected to drive an exponential growth in telecommunications, are two other factors that may lead to a more open mind and awareness by the entities responsible for the management of organizational structures.

According to (Combs, 2021), it is highly predicable that by the year 2025, 53% of the world population will be covered by this technology. This kind of evolution will, no doubt, lead to a significant effort by the telecommunications service's suppliers, not only to guarantee their networks availability but also to try to assure their customers that, communications between terminal equipment's will happen with as much security as possible.

(Bartock, 2020) states that the National Cybersecurity Center of Excellence (NCCoE) of the United States Department of Defense is developing "an effort in collaboration with industry to secure cellular networks and, in particular, 5G deployments.

The scope of this project is to leverage the 5G standardized security features which are defined in 3GPP standards to provide enhanced cybersecurity capabilities built into the network equipment and end-user devices." **(p. 3)**

Main Cybersecurity Goals

- **Authenticity**
  To guarantee that anyone participating in a communication is, effectively, who he/she claims to be.

- **Confidentiality**
  Every communication flowing through the network can only be accessed by the entity it is directed to and by no one else.
- **Integrity**
  Any message exchanged between any two partners should not be susceptible to alterations during its path from the emitter to the receiver.
- **Availability**
  Every equipment integrating the communications infrastructure must be available whenever its services are needed.
- **Nonrepudiation**
  Messages exchanged between two partners should not be subject to repudiation by any of them. This is an absolutely essential request for being able to evaluate both emitter and receiver responsibilities.
- **Access control**
  The network should be access by users according to their levels of authorizations.

User Equipment Security Features

With these goals in mind, (Craven, 2020) reinforces that "*5G security standards include requirements for users' equipment primarily their tablets and smartphones and the base stations in a 5G network There is an emphasis on confidentiality, integrity, and replay protection in 5G security standards*".

Still according to (Craven, 2020), these pieces of equipment must include features to guarantee authentication, confidentiality and user's and communication's control data integrity, as well as safe storage and processing of the subscribers' credentials and, finally, but not less important, than all the before mentioned requests, the privacy of these subscribers.

Network Security Features

5G base stations are called **gNB**, which is short for next generation **NodeB**.

These stations should be able to assure: Subscription authentication, user equipment authorization, network authorization services by the home

network, access network authorization, confidentiality of user and signaling data as well as integrity of user and signaling data.

The 3rd Generation Partnership Project (3GPP) Releases

> "The 3GPP project unites seven organizations responsible for the development os standards related with the telecommunications systems (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as "Organizational Partners" and provides their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies".
>
> "The project covers cellular telecommunications technologies, including radio access, core network and service capabilities, which provide a complete system description for mobile telecommunications". (3GPP, https://www.3gpp.org/about-3gpp/about-3gpp)

Since 1991 until today, 3GPP has been publishing standards related to mobile communications. In December, 2017 specifications were approved for for the new radio (NR) 5G networks working in "*Non-Standalone*" mode, also known as NSA. Later, in June, 2018 the specifications for "*Standalone*" mode were published, thus, finishing the 5G Phase 1 (3GPP Release 5).

The main characteristic of "Non-Standalone" mode is the possibility of using pre-existent infrastructure fused for "*Long Term Evolution*" (LTE) and "*Evolved Packet Core*" (EPC), as well as the new radio technology based on 5G, without the need for the replacement of previously installed networks.

3GPP 5G Security

5G Phase 1 (3GPP, https://www.3gpp.org/about-3gpp/about-3gpp) introduced several improvements when compared to 4G LTE, namely,

- **Primary authentication**
  This is similar to 4G but there are a few differences.
  - The authentication mechanism has in-built home control (allowing the home operator to know whether the device is authenticated in a given network and to take final call of authentication). In 5G Phase 1 there are two mandatory authentication options:

5G Authentication and Key Agreement (5G-AKA) and Extensible Authentication Protocol (EAP)-AKA', i.e. EAP-AKA
  - Optionally, other EAP based authentication mechanisms are also allowed in 5G – for specific cases such as private networks. Also, primary authentication is radio access technology independent (thus it can run over non-3GPP technology such as IEEE 802.11 WLANs);
- **Secondary authentication**
  Meant for authentication with data networks outside the mobile operator domain. For this purpose, different EAP based authentication methods and associated credentials can be used. A similar service was possible in 4G as well, but now it is integrated in the 5G architecture.
- **Inter-operator security**
  Related to this context, several problems arising from the use of SS7 (Introduction to SS7 Signaling, 2012) and Diameter (Signalling Security in Telecom SS7/Diameter/5G_EU level assessment of the current situation, 2018) in the earlier generations of mobile communication systems had to be addressed.
  To counter these issues, 5G Phase 1 provides inter-operator security from the very beginning.
- **Privacy**
  Subscriber identity related issues have been known since 4G and earlier generations of mobile systems. In 5G a privacy solution is developed that protects the user's subscription permanent identifier against active attacks.
  A home network public key is used to provide subscriber identity privacy.
- **Service based architecture (SBA)**
  This concept did not exist in 4G and in none of the previous generations. 5G also provides adequate security for SBA.
- **Central Unit (CU) – Distributed Unit (DU)**
  A base-station is logically split in CU and DU. With a interface between them. Security is provided for the CU-DU interface. This split was also possible in 4G, but in 5G it is part of the architecture that can support a number of deployment options (e.g. co-located CU-DU deployment is also possible).

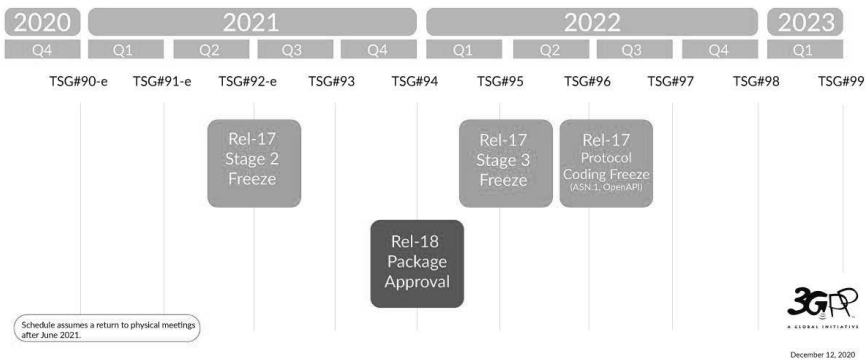
The DUs, which are deployed at the very edge of the network do not have access to any user data when confidentiality protection is enabled. Even with the CU-DU split, the air interface security point in 5G remains the same as in 4G, namely in the radio access network.

- **Key hierarchy**
  5G hierarchy reflects the changes
  - o In the overall architecture
  - o The trust model using the security principle of key separation.
  - o One main difference in 5G compared to 4G is the possibility for integrity protection of the user plane.
- **Mobility**
  Although mobility in 5G is similar to 4G, the difference in 5G is the assumption that the mobility anchor in the core network can be separated from the security anchor. 5G hierarchy reflects the changes.

The 3rd Generation Partnership Project (3GPP) Releases

The present plans for the generation's evolution are defined according to the following:

Figura 1 – https://www.3gpp.org/specifications/67-releases



5G Security in Phase 2

The security goal which are to be implemented during Phase 2 are, among others, the following:

- **Authentication and Key Management for Applications;**
  Similar to the Generic Bootstrapping Architecture (GBA) feature specified for earlier generations (3GPP TS #: 33.220).
  A UE can be registered in, or attached to, the network both over 3GPP or non-3GPP access. UE can still be authenticated and reachable by the network, e.g. over Wi-Fi.
  Key hierarchy in the 5G System includes a new key KAUSF shared between the UE and the home network.(3GPP, ETSI TS 133 535 V16.2.0, 2021).
- **Integrated Access Backhaul (IAB);**
  In a hierarchical telecommunications network, the backhaul portion of the network comprises the intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network.
  To enhance the coverage and boost the performance over the New Radio (NR) technology of 5G allows for deploying lower protocol layer devices such as antennas further away in the field so that better coverage can be provided, given the limitation, in terms of range, of the NR technology. It Includes additional nodes on the "access path" – IAB-donor nodes and IAB nodes(Henda, 2020).
- **Support for Advanced V2X Services (*Vehicle to Everything*)**
  3GPP LTE-V2X PC5 (also known as LTE side-link)
  For V2X, PC5 will support broadcast, groupcast and unicast communications. It is expected to work off coverage and even between UEs that have subscriptions with different operators. Nevertheless, it is not yet clear how KgNB key which is shared between the UE and the network will be established, specifically between UEs potentially out of network coverage. (Henda, 2020).
- **Ultra-Reliable Low Latency Communication Services**
  For applications requiring a high degree of reliability, it was decided by 3GPP to leverage the Dual Connectivity (DC) architecture to realize the support of two parallel paths for the redundant transmission of such application data. (Henda, 2020).

Among the security aspects to consider are the following:

- In case the same key stream is used, an eavesdropper can identify redundant transmission and target the attack to whatever critical application making use of the feature.
- The use of different security policies for each of the user data connection pertaining to the same data transmission may compromise the overall protection. e.g. it may lead to confidentiality protection being activated for one connection but not for the redundant one.

Bibliography

3GPP. (January, 2021). ETSI TS 133 535 V16.2.0. *5G; Authentication and Key Management for Applications (AKMA)*.

3GPP. (s.d.). https://www.3gpp.org/about-3gpp/about-3gpp. *3GPP Home Page*.

Bartock, C. &. (2020). *5G CYBERSECURITY_Preparing a Secure Evolution to 5G.* National Institute of Standards and Technology.

Combs, V. (January, 4, 2021). 5G Prediction: 53% of the world's population will have coverage by 2025. *TechRepublic*.

Craven, C. (June, 10, 2020). 5G Security Standards: What Are They? *https://www.sdxcentral.com/*.

Henda, N. B. (March, 2020). Overview on the Security in 5G Phase 2. *Journal of ICT Standardization*, 2020: Vol 8 Iss 1.

Introduction to SS7 Signaling. (2012). *https://www.patton.com/whitepapers/intro_to_ss7_tutorial.pdf*.

Signalling Security in Telecom SS7/Diameter/5G_EU level assessment of the current situation. (March, 2018). *European Union Agency For Network and Information Security*, pp. https://www.key4biz.it/wp-content/uploads/2018/03/Interconnect-Security-SS7-Diameter.pdf.

Combs, V. (December, 2020). 5G standalone networks may have more vulnerabilities than you think. *TechRepublic*.

Shein, E. (December, 2020). Standalone 5G is more secure than previous network generations. *TechRepublic*.

Wheeler, T. & Simpson, D. (September, 2019). Why 5G requires new approaches to cybersecurity. https://www.brookings.edu/research

Cybersecurity of 5G networks-EU Toolbox of risk mitigating measures (January, 2020). CG Publication. NIS Cooperation Group.

James, P. (September, 2020). 5G Technology and How it will change cybersecurity. https://gbhackers.com

Ivezic, M. & Ivezic, L. (April, 2019). 5G Critical Infrastructure – The most critical of all. https://5g.security/cyber-kinetic