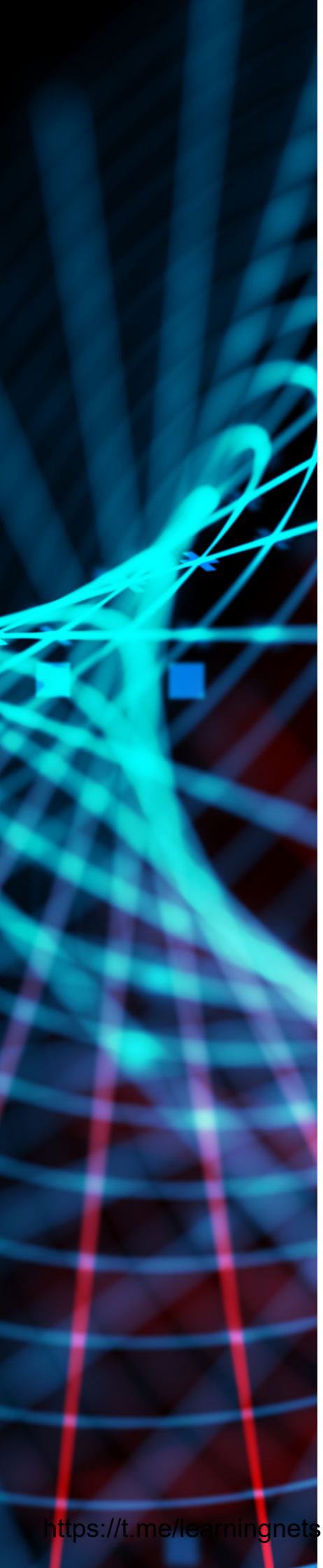

:: Positive Technologies
Telco cybersecurity trusted advisor
5G Standalone core security research
positive-tech.com

Contents



1. Executive summary

This report presents our findings regarding the 5G Standalone core. Our objective was to analyze the security of the network architecture, interaction of network elements, and subscriber authentication and registration procedures.

Key elements of network security include proper configuration of equipment, as well as authentication and authorization of network elements. In the absence of these elements, the network becomes vulnerable. Exploitation of vulnerabilities may lead to a number of consequences, including:

- Subscriber denial of service due to exploitation of vulnerabilities in the PFCP protocol
- Registration of new attacker-controlled network functions
- Subscriber denial of service due to mass deregistration of network elements
- Disclosure of subscriber unique identifier (SUPI)
- Disclosure of subscriber profile information
- Creation of Internet sessions by attackers at subscriber expense

To prevent the consequences of such attacks, operators must employ timely protection measures, such as proper configuration of equipment, use of firewalls on the network edge, and security monitoring.

2. Introduction

5G mobile networks are gradually being rolled out by operators worldwide. Widespread adoption will allow users and devices to benefit from all the advantages of 5G, such as enhanced mobile broadband (eMBB), ultra-reliable and low-latency communications (URLLC), and massive machine-type communications (mMTC).

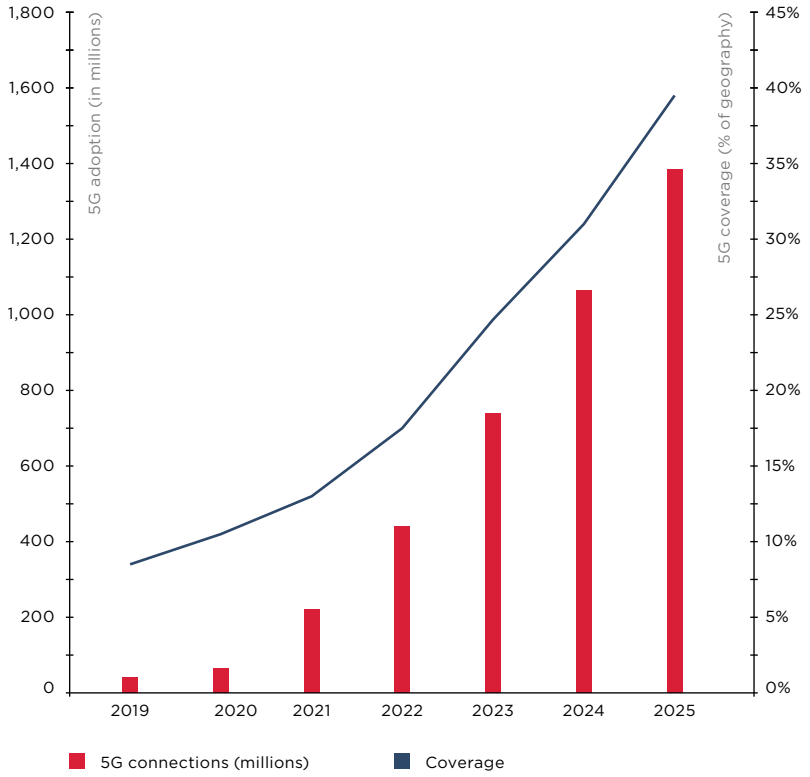


Figure 1. Expected growth in 5G subscribers [1]

Deployment of a network capable of delivering all the expected functionality is a complex and expensive process. That is why 3GPP specifications describe two possible tracks for 5G development:

- Non-Standalone (NSA) refers to an interim implementation that relies on existing LTE radio and 4G core components as the base for selectively adding 5G components on top.
- Standalone (SA) is a network implementation mode that uses only new components, such as 5G New Radio (5G NR) and 5G Core Network (5GC).

This research focuses on the SA mode of 5G network deployment. The implementation is based on Rel 15 3GPP with the OpenAPI Specification providing detailed descriptions of each interface.

3. Mobile network diagram

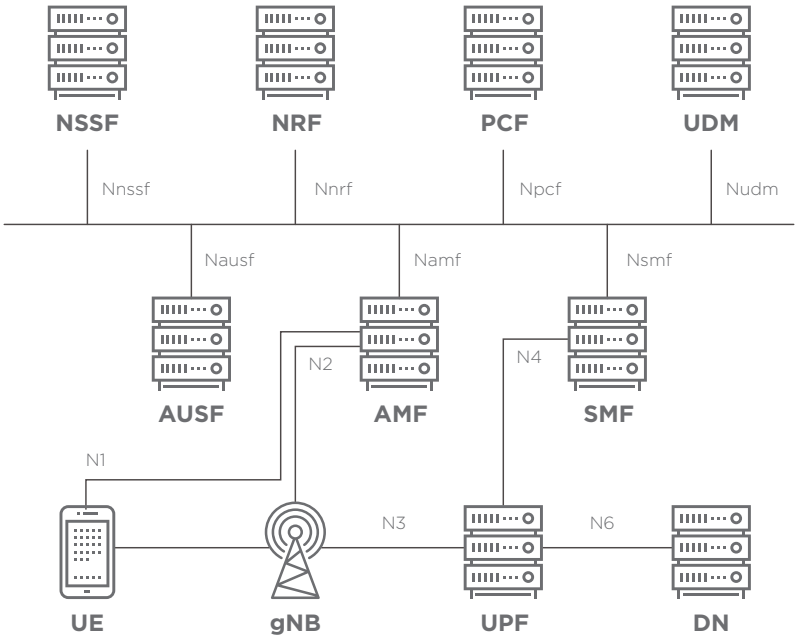


Figure 2. Architecture of the tested network

The tested network includes the basic components needed for serving subscribers, such as:

- Access and Mobility Management Function (AMF), which is responsible for subscriber registration on the network, NAS signaling exchange via the N1 interface, subscriber connection management, and subscriber location management.
- Session Management Function (SMF), which is responsible for creating, updating, and deleting sessions, managing the tunnel between the access network (AN) and User Plane Function (UPF), selection of the UPF gateway to be used, allocation of IP addresses to subscribers, and interaction with the Policy Control Function (PCF).
- User Plane Function (UPF), which is responsible for connecting the subscriber to the Internet, handling GTP-U packets, assigning policy rules, and setting quality of service parameters.
- Network Repository Function (NRF), which is an evolutionary enhancement to the Domain Name Server (DNS). The NRF maintains a repository of the profiles of NF instances available on the network. When enabled, each network function must write in the NRF its status, capabilities, and supported options.
- User Data Management (UDM), which is responsible for managing user profile data and user IDs, as well as for generating authentication credentials.
- Unified Data Repository (UDR), which is a database that stores and allows extraction of subscriber-related data.

- Authentication Server Function (AUSF), which acts as authentication server for 3GPP and non-3GPP access.
- Policy Control Function (PCF), which assigns policy rules to user terminals using data from the UDR.
- Network Slice Selection Function (NSSF), which selects the network slicing instance when user equipment is registered on the network depending on the equipment's type, location, and other factors.

The 5G architecture supports two types of interaction between network functions: interface-based and service-based. The first type demonstrates interaction between network function services described as point-to-point interaction (for example, the N11 interface). This interface-centric approach is well known from previous generations of networks. The service-based architecture is a new way to address the mobile network architecture. It also includes interface-based elements, as can be seen in the diagram (Figure 2). In the upper part of the diagram, network elements are connected by a single bus, with which an authorized control plane (CP) network function can access the services of another NF.

According to the specification, the service-based architecture uses the HTTP/2 protocol and REST API for interaction between all services. This solution makes the system more flexible and significantly facilitates its description. In addition to HTTP/2, fifth-generation networks also use the GTP-U and PFCP protocols. The GTP-U protocol is used to carry user plane (UP) traffic from the (R)AN to the UPF via the N3 interface. The N4 interface also uses the PFCP protocol for interaction between the control plane and user plane on the SMF and UPF. This solution is logical, since all traffic control and management functions have moved to the SMF.

However, this stack of technologies in 5G potentially opens the door to attacks on subscribers and the operator's network. Such attacks can be performed from the international roaming network, the operator's network, or partner networks that provide access to services. Later in this report, we will detail the network core threats that we found on the 5G deployment testbed.

4. PFCP protocol

PFCP (Packet Forwarding Control Protocol) is used on the N4 interface between the control plane and the user plane. With the help of this protocol, the SMF establishes a PFCP session on the UPF to manage the GTP tunnel that provides Internet access to the subscriber. All subscriber settings consist of a number of rules responsible for the PDR (Packet Detection Rule), FAR (Forwarding Action Rule), QER (QoS Enforcement Rule), URR (Usage Reporting Rule), BAR (Buffering Action Rule), and MAR (Multi-Access Rule Handling). Each subscriber is assigned its own unique PDR rules, and the session is identified with the help of an assigned SEID (Session Endpoint Identifier).

To manage subscriber connections, three procedures are available in the PFCP protocol (Session Establishment, Modification, and Deletion), which establish, modify, and delete GTP-U tunnels on the N3 interface between the UPF and gNB. The full procedure for establishing a subscriber session is described in item 4.2.4 of this document. In the meantime, we will focus on the N4 interface. Testing of this interface revealed potential attack scenarios against an established subscriber session.

4.1. Denial of service via Session Deletion Request

The first attack scenario consists of sending a Session Deletion Request packet to the UPF (Figure 3). The request contains only the subscriber session identifier (Figure 4). As a result, packet data transmission to the victim's device will stop, but the connection to the network will remain.

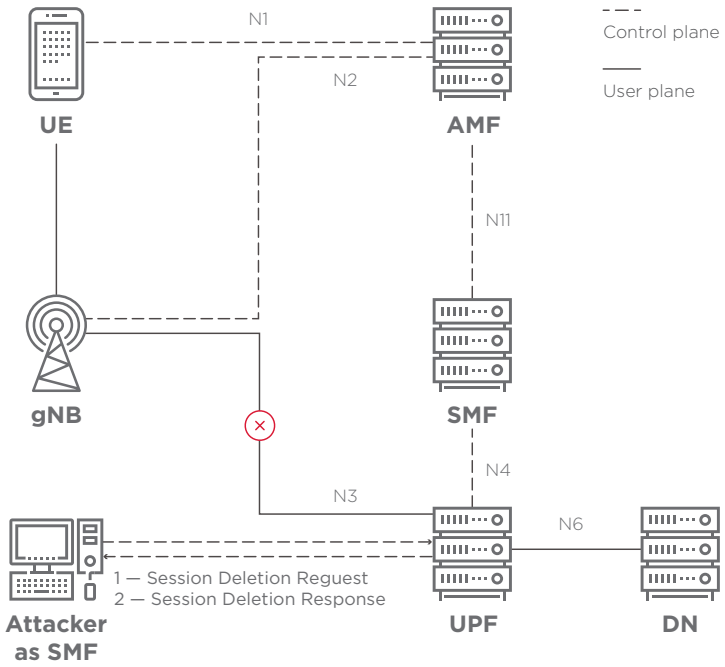


Figure 3. Attack diagram

CVSS v3.1 Vector:
AV:A/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H

Base score:
6.1 (medium)

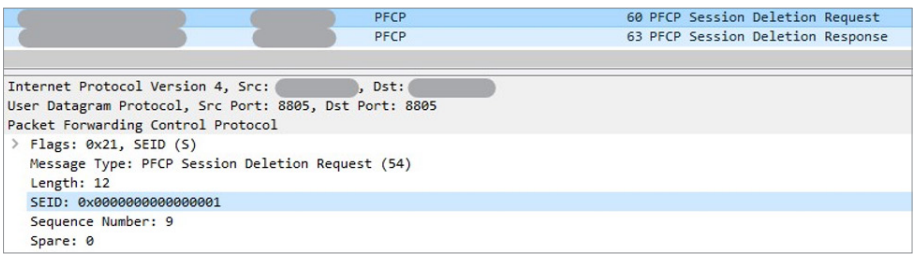


Figure 4. Deletion of subscriber session

4.2. Denial of service via Session Modification Request

In the second scenario, packet handling settings are discarded (Figure 5). Attackers need to send a Session Modification Request containing a DROP flag in the Apply Action field in the FAR rules (Figure 6). If the rules are changed successfully, the FAR rules containing the TEID and IP address of the base station are deleted on the UPF. As a result, the GTP tunnel for the subscriber's downlink data is cut off, depriving the subscriber of Internet access. The GTP-U tunnel can be subsequently restored by sending the required data to the UPF.

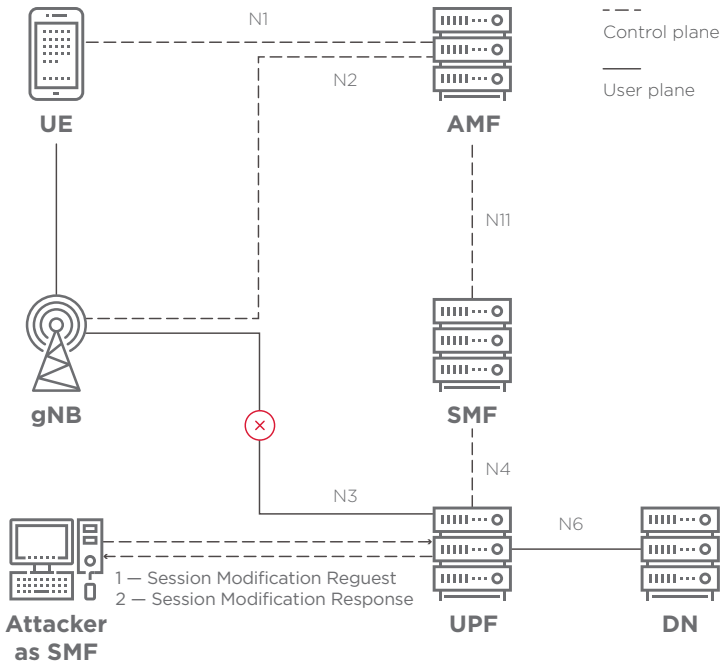


Figure 5. Attack diagram

CVSS v3.1 Vector:
AV:A/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H

Base score:
6.1 (medium)

```
[redacted]  PFCP  92 PFCP Session Modification Request
[redacted]  PFCP  63 PFCP Session Modification Response

Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
User Datagram Protocol, Src Port: 8805, Dst Port: 8805
Packet Forwarding Control Protocol
> Flags: 0x21, SEID (S)
  Message Type: PFCP Session Modification Request (52)
  Length: 46
  SEID: 0x0000000000000001
  Sequence Number: 7
  Spare: 0
> F-SEID : SEID: 0x0000000000000001, IPv4[redacted]
v Update FAR : [Grouped IE]
    IE Type: Update FAR (10)
    IE Length: 13
  > FAR ID : Dynamic by CP 2
  v Apply Action :
      IE Type: Apply Action (44)
      IE Length: 1
    v Flags: 0x01, DROP (Drop)
        000. .... = Spare: 0
        ...0 .... = DUPL (Duplicate): False
        .... 0... = NOCP (Notify the CP function): False
        .... .0.. = BUFF (Buffer): False
        .... ..0. = FORW (Forward): False
        .... ...1 = DROP (Drop): True
```

Figure 6. Discarding packet handling settings

4.3. Redirection of data via Session Modification Request

By using a Session Modification Request, attackers can redirect user traffic from the UPF to an attacker-controlled resource (Figure 7). For this, the attackers need to change the IP address in the Outer Header Creation field (Figure 8). As a result, they can access the downlink data of the subscriber, who will not be aware that the traffic is being intercepted.

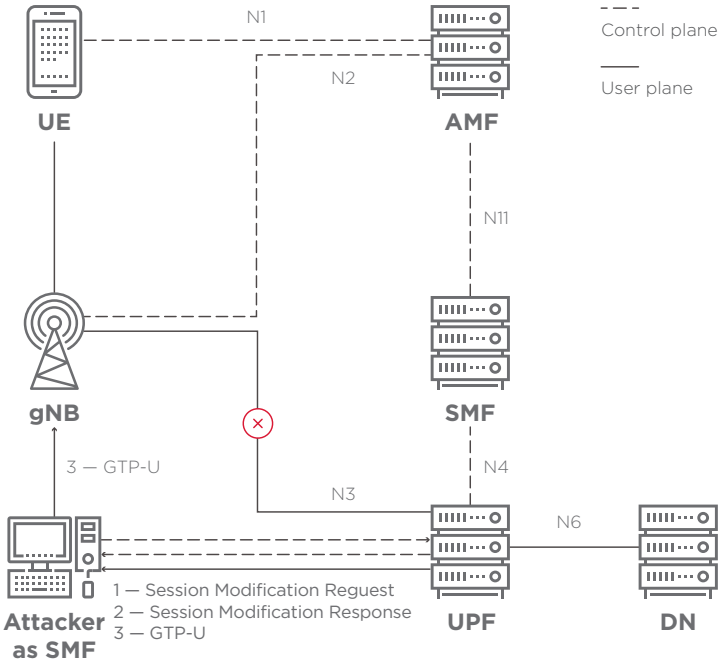


Figure 7. Attack diagram

CVSS v3.1 Vector:
AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Base score:
8.3 (high)

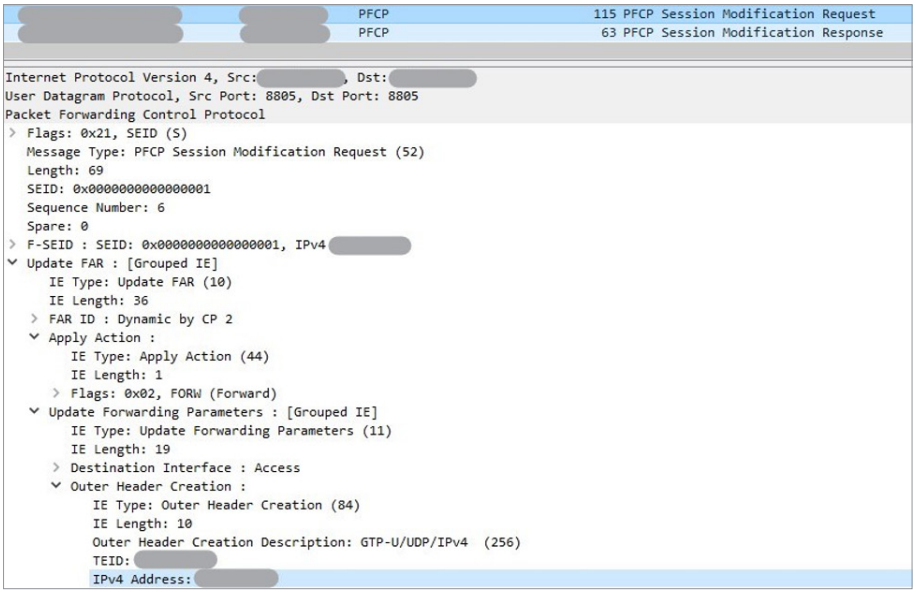


Figure 8. Redirection of data

4.4. PFCP protocol: conclusions

The preceding examples prove the vulnerability of the PFCP protocol. The good news is that this interface is located inside the operator's network. If equipment is configured correctly, external attackers will not get access to the N4 interface. However, operators often make mistakes in network configuration, due to which internal interfaces become accessible from the global network. Such mistakes exist on half of GTP networks that we have tested. [2]

5. HTTP/2 protocol

5.1. NRF

According to the specification, the Network Repository Function is a key service of 5G networks. The NRF is responsible for registering new NFs and storing their profiles. The NRF also receives requests for discovery of available NFs that meet certain criteria.

On the 5G testbed, we studied three procedures:

- Registering a new NF
- Obtaining the NF profile
- Deleting the NF profile

In the tested deployment, none of the components verify the TLS certificate when connecting to each other. No procedure for service authorization is performed on the NRF.

5.1.1. Registering a new NF

A request for registering a new network function contains a profile with description of interfaces and a unique NF number in the Instance ID header (Figure 9).

CVSS v3.1 Vector:
AV:A/AC:L/PR:N/
UI:N/S:C/C:N/I:L/A:H

Base score:
8.2 (high)

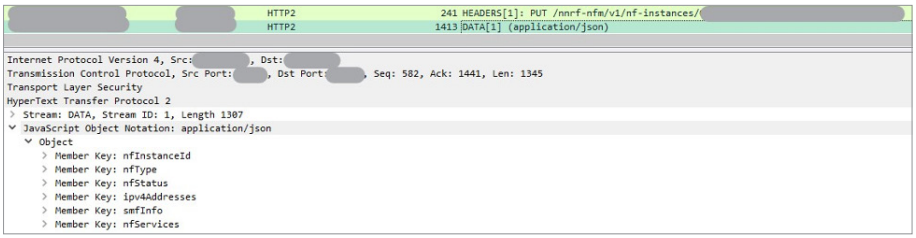


Figure 9. Example of registration of a new NF

If the profile of a legitimate NF is already stored on the NRF, registration of the same network function by an attacker may cause disruption. The attacker will be able to serve subscribers via an attacker-controlled NF and thus access subscriber data.

5.1.2. Obtaining the NF profile

An attacker who obtains the profile of a network function will be able to use it in subsequent attacks that require indicating the Instance ID in the request body (Figure 10).

CVSS v3.1 Vector:
AV:A/AC:L/PR:N/
UI:N/S:C/C:H/I:N/A:N

Base score:
7.4 (high)

Figure 10. Obtaining the NF profile

Attackers can then impersonate any network service for other NFs and obtain profile data, such as authentication status, current location, and subscriber settings for network access.

5.1.3. Deleting the NF profile

If an attacker obtains NF profiles and the NRF does not restrict the operations allowed on NF profiles, the attacker could delete such profiles (Figure 11).

CVSS v3.1 Vector:
AV:A/AC:L/PR:N/
UI:N/S:C/C:N/I:N/A:H

Base score:
7.4 (high)

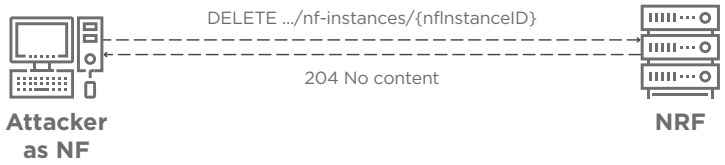


Figure 11. Deleting the NF profile

In case of mass deregistration of the core components, the network will not be able to provide service to subscribers, potentially causing financial losses and reduction in subscriber trust.

5.1.4. Conclusions and recommendations

The described vulnerabilities enable extremely dangerous manipulations on the network, which makes the NRF an important element of the network core. Securing the NRF will help to prevent the majority of other attacks that require NF profile information.

One way to protect from such attacks is to authorize services by verifying TLS certificates when a connection is being established. Adding authorization on the NRF will help services to verify the legitimacy of the sender service when receiving incoming requests.

5.2. Subscriber authentication vulnerabilities

Authentication is crucial in the procedure for registering a subscriber on the network. It serves for mutual authentication between the subscriber terminal and the network. Authentication also provides the KSEAF security key used to encrypt control plane and user plane data.

The 3GPP specification defines two methods of subscriber authentication: 5G-AKA and EAP-AKA'. A network operator selects the authentication method for each device individually. In our research, we analyzed authentication using the 5G-AKA method (Figure 12), which is an extension of EPS-AKA used in 4G networks.

The following sample requests demonstrate that subscriber authentication becomes insecure if the NRF does not perform authentication and authorization of 5G core network functions.

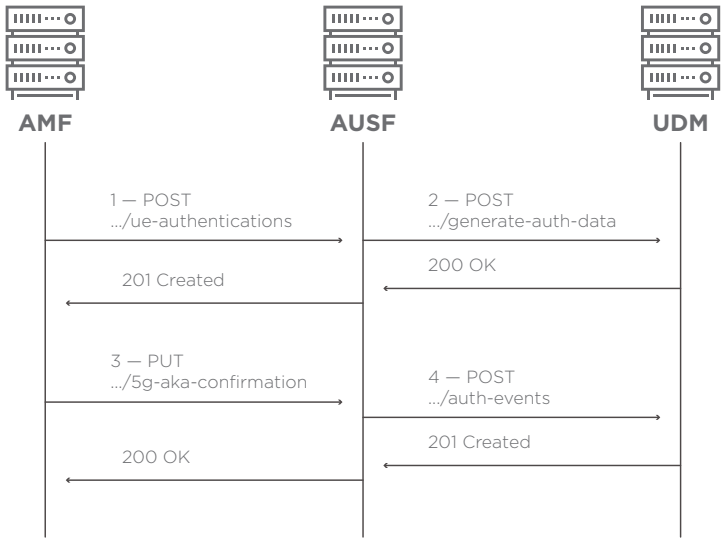


Figure 12. 5G AKA full authentication process

5.2.1. 5G AKA

The first request (.../ue-authentications) initializes authentication. The message contains the user ID (SUPI or SUCI) and name of the serving network. The response returns data together with the HXRES* and resource address to confirm authentication (Figure 13). Attackers can use this procedure to obtain the subscriber authentication vector.

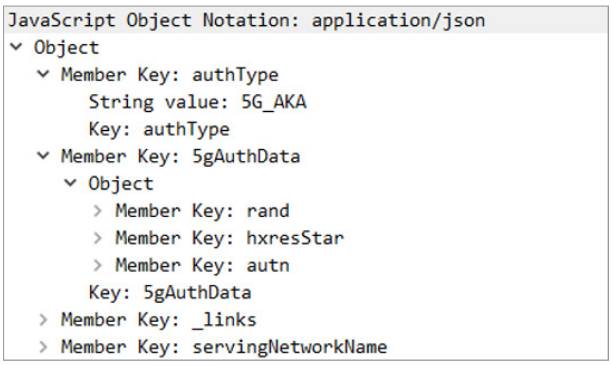


Figure 13. Response to authentication request

As soon as the AMF obtains the authentication vector, it sends the RAND and AUTN parameters to the subscriber, on whose device the RES* is calculated. After obtaining the RES* from the subscriber, the AMF calculates the HRES* hash and performs authentication of user terminal by comparing the HRES* to the HXRES*. If they match, the AMF sends the request .../5g-aka-confirmation, which contains the RES* to confirm authentication. A successful response contains the authentication status, SUPI, and KSEAF (Figure 14). The method itself is not dangerous, since the RES* is calculated on the subscriber's device. However, if the attacker impersonates the AMF and serves the subscriber, this will cause disclosure of the SUPI and fake authentication of subscriber in the network.

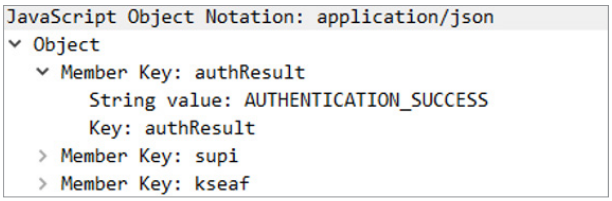


Figure 14. Response to confirmation of authentication

5.2.2. Authentication information retrieval

When sending the .../generate-auth-data request as the AUSF, the attacker needs to specify the subscriber's ID and the name of the serving network. This method allows obtaining the authentication vector together with the RAND, AUTN, XRES*, and KAUSF, as well as the subscriber's SUPI, if the request contained the SUCI (Figure 15). Having obtained this data, an attacker can use special equipment to spoof the base station and serve the subscriber.

```
JavaScript Object Notation: application/json
▾ Object
  › Member Key: authType
  ▾ Member Key: authenticationVector
    ▾ Object
      › Member Key: avType
      › Member Key: rand
      › Member Key: xres
      › Member Key: autn
      › Member Key: ckPrime
      › Member Key: ikPrime
      › Member Key: xresStar
      › Member Key: kausf
      Key: authenticationVector
  › Member Key: supi
```

Figure 15. Response to request for generation of authentication data

5.2.3. Authentication confirmation

The AUSF compares the calculated XRES* to the RES* received from the subscriber, after which it completes the procedure by sending to the UDM a request (.../auth-events) containing the SUPI and subscriber authentication status. When using this method, an attacker who impersonates the AUSF will leave a record on the UDM indicating successful authentication. This record can affect the functioning of other network services.

5.3. Subscriber profile disclosure via UDM

Another important network element is the user data management module (UDM). The UDM provides the following functionality:

- Store user IDs (SUPI values).
- Derive the subscriber's permanent identifier (SUPI) from the subscriber's concealed identifier (SUCI).
- Authorize access based on user profile data (for example, roaming restrictions).
- Manage user registration (storing the serving AMF).
- Maintain continuity of service and sessions by storing the SMFs/DNNs assigned for current sessions.
- Manage delivery of SMS messages.

By design, the Unified Data Repository manages subscriber profile data. An attacker who has access to the relevant interface can connect to the UDM directly or by impersonating a network service, and then extract all the necessary information (Figure 16).

Figure 16. Request diagram

By knowing the subscriber's SUPI, we obtained the following data during testing:

- Subscriber MSISDN
- NSSAI network segment identifier
- User Internet connection parameters
- Location data

CVSS v3.1 Vector:
AV:A/AC:L/PR:N/
UI:N/S:C/C:H/I:N/A:N

Base score:
7.4 (high)

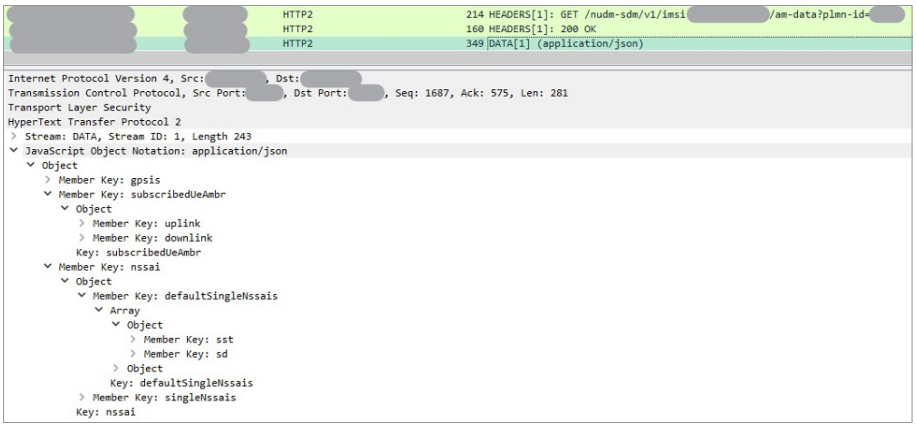


Figure 17. Example of data extraction

Access to such data would severely jeopardize security: it allows the attacker to secretly spy on the subscriber, while the latter will never know what is going on. To protect equipment from such attacks, the same methods are applicable as before: obligatory authentication and authorization for network components.

5.4. PDU session creation

Unlike previous generations, 5G networks enforce clear differentiation between user traffic and control traffic for all protocols. This allows cleanly separating data flaws and optimizing network architecture.

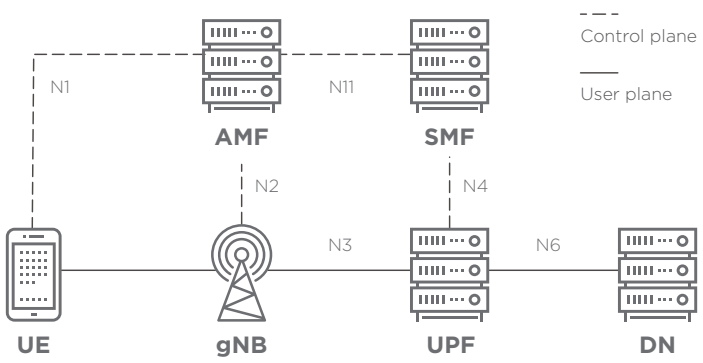


Figure 18. User and control traffic separation

5G networks use PDU sessions for subscriber Internet connections. The subscriber terminal sends a request for connection to the AMF by using the N1 Interface via gNB. After successful subscriber registration, the AMF establishes a connection with the SMF via SM context to manage packet data transfer between the subscriber and the UPF (Figure 19).

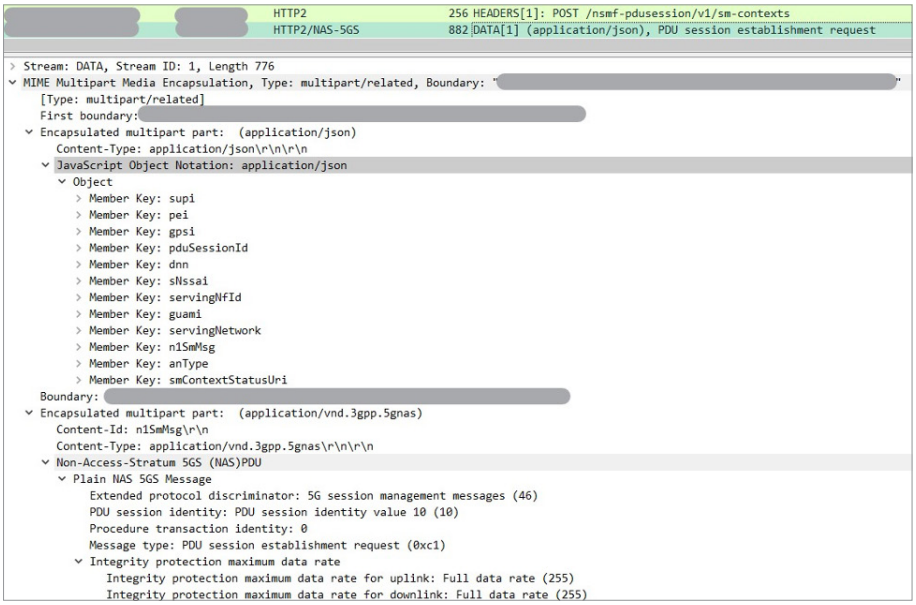


Figure 19. Request for creating context

The request contains general information for subscriber identification; the NAS protocol from the N1 interface is encapsulated separately. Then the SMF obtains data about the parameters of the Internet connection (QoS, AMBR, Data Network Name, and so forth) from the UDM as well as policies and billing rules from the PCF.

The SMF creates a request to establish a PFCP session on the N4 interface in order to send the subscriber session parameters to the UPF. If the session is established, a unique number is returned to the AMF in the Location field of the HTTP/2 header; this number is used to control the context. The SM context data (subscriber IP addresses plus UPF and TEID for Uplink UE) is transmitted to the subscriber device and the base station via the AMF (Figure 20).

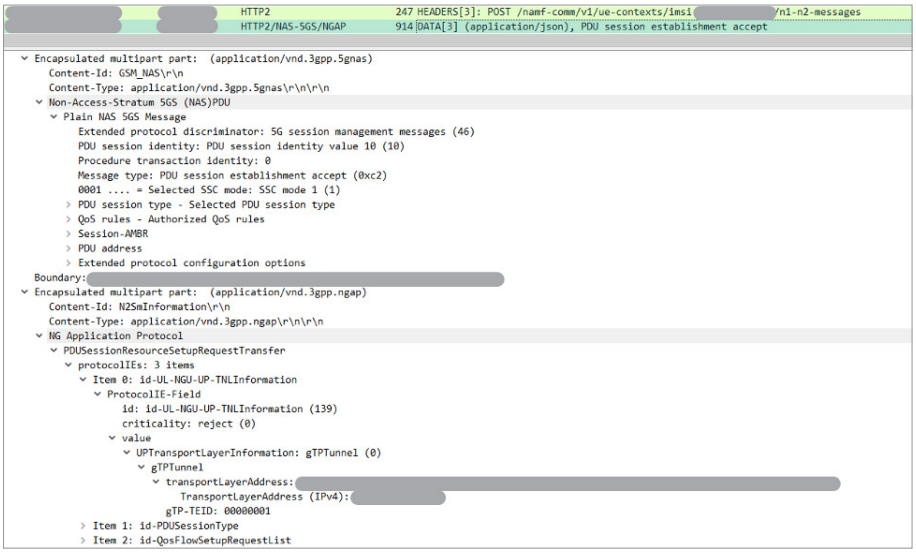


Figure 20. Parameters of the established session

This information is enough to transfer traffic from the subscriber to the network, but the UPF does not yet have information about the base station serving the subscriber, nor has a TEID been assigned for downlink transmission. The AMF sends the required information to update the context by using a unique identifier (Figure 21).

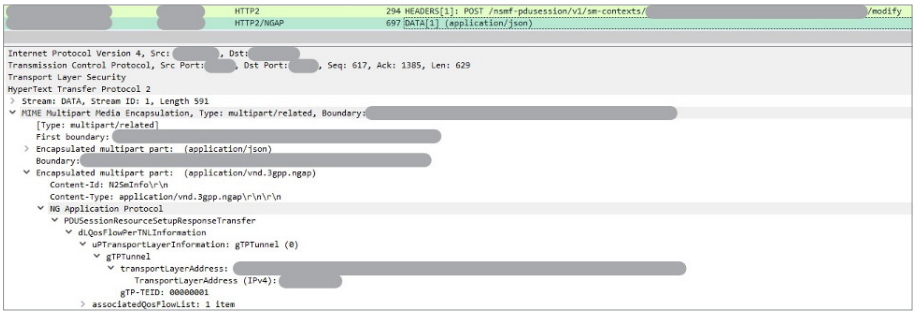


Figure 21. Subscriber session update

CVSS v3.1 Vector:
AV:A/AC:L/PR:N/
UI:N/S:C/C:L/I:H/A:N

Base score:
8.2 (high)

After exchanging these messages, a PDU session is established and the subscriber can connect to the Internet. Further management and session deletion require knowledge of the unique number obtained during session creation. A potential attacker needs to obtain this number to perform an attack, which is rather difficult because all signaling traffic is encrypted.

The attacker can create a new session by impersonating the AMF, using the data of a particular subscriber, and manage this session as described already. As a result, the subscriber will be billed for all traffic used by the attacker.

6. How to protect 5G

Security wise 5G was designed to address the gaps and errors present in the architecture of previous-generation networks. This led to new protection mechanisms based on the following principles:

- Mutual authentication. The sender and recipient must each verify that the other is genuine.
- Zero-trust model. No network component assumes trust in another component, whether inside or outside the MNO.
- Use of encryption on the transport-level connections. This should prevent eavesdropping and modification of transmitted data between endpoints.

These principles inspired new mechanisms for securing signaling traffic during drafting of the 3GPP documentation. Starting with 5G potential attackers should face a higher barrier to commit any kind of illegitimate activity: for instance discovering the subscriber permanent identifier (SUPI) over the air with an IMSI catcher; the subscriber concealed identifier (SUCI) should be transmitted when a subscriber registers on the network. The Security Edge Protection Proxy (SEPP) involves traffic filtering mechanisms that will help to prevent attackers from breaching the operator's network via the roaming network. Transport-level encryption can be used to prevent eavesdropping on traffic within the MNO. At the same time, the Oauth 2.0 protocol will enable the network function receiving a message to verify whether the sender (a different NF) has undergone network authorization, which is beneficial if an attacker is attempting to send a message by posing as a legitimate NF.

These examples are only a few of the features incorporated at the specification level for 5GC security. Which is good, but should not be treated as panacea, because real life deployment always involves difficulties, some aspects not fully solved by the moment and finally surprises happen.

That's why even full use of all this functionality will not guarantee that a network cannot be breached from outside.

In this research we demonstrated that the ability to register new attacker-controlled NFs and send various messages to other legitimate services. This was possible because of a lack of service authorization and failure to verify TLS certificates for incoming connections. This is just one specific issue and there possibly many others.

As practice shows, operators frequently make errors in equipment configuration with consequences for security. An important role is played by equipment vendors, which are responsible for the technical implementation of all the architected network protection features. Protection of the network core must be thorough and far-reaching with additional systems for monitoring, control, and filtering, in addition to regular security audits of the MNO network to identify potential risks.

Addressing security issues require a comprehensive approach, which includes on minimum basis the following activities:

1. Assessment
2. Monitoring
3. Protection

First. Security testing is a useful tool to start with – it has a number of benefits. There are thousands of base stations in the world that need security testing for the asset access or radio. It would also benefit to run the testing for the core network, as it is fully exposed to the IPx. Security testing is powerful to run on the virtualization infrastructure, as vendors deliver solutions as a black box and it is difficult to uncover what is inside the infrastructure. It is especially important to run testing for the MEC, as it can lack architectural security, for instance.

Second. Security must also be non-intrusive for the telecom world. To provide the best services, the best speed, security must support the process but not be an obstacle.

One of the ways to start addressing security issues is getting visibility of what's happening inside. Although there are a lot of obstacles and constraints with security that will take a lot of time to overcome, mobile operators should start threat detection and plant response because security monitoring is essential to support secure environment and to provide the rapid detection and possibly the rapid mitigation.

Third. What is important to consider is that there is no need to create proactive protection by building borders—the network and services has already been exposed. Having visibility over the infrastructure is the only way to enforce control and protection. Mobile network operators can have it performed by patching and verification for access networks, or hardening and compliance for virtualization, design review and security requirements for Multi-Access Edge Computing, and traffic filtering and continuous fine-tuning for core networks. However, it is important, not to get confused and associate protection with a function. Protection should be considered as a goal and can be achieved in many ways. From the standpoint of security experts, it is a mission to find most effective, applicable for customer's environment and cost-efficient solution.

The right approach to security should be comprehensive, including using a wide range of professional services which can span over all areas, and cost efficient, because this is the only way for creating trust and assurance in technology. The value given through continuous security support is endless—bringing automation of security testing, having end to end visibility for policy enforcement, ongoing and iterative security for sustaining a secure environment.

7. Conclusion

The number of 5G network users will continue to grow each year. The capabilities of 5G networks allow providing services to all devices based on their functionality. Besides regular subscribers, equipment belonging to businesses and even cities may be connected to the network.

In this report, we have covered only a few examples of exploitation of vulnerabilities by potential attackers. Just as with previous-generation networks, attackers still can penetrate operator networks by means of the international roaming network or partner networks. Therefore, it is vital to ensure comprehensive protection of 5G networks.

Sources

1	The 5G guide. A reference for operators. GSMA, April 2019	gsma.com/wp-content/uploads/2019/04/The-5G-Guide_GSMA_2019_04_29_compressed.pdf
2	Threat vector: GTP Vulnerabilities in LTE and 5G networks 2020	positive-tech.com/storage/articles/gtp-2020/gtp-2020-eng.pdf
3	3GPP TS 23.501	3gpp.org/DynaReport/23501.htm
4	3GPP TS 23.502	3gpp.org/DynaReport/23502.htm
5	3GPP TS 33.501	3gpp.org/DynaReport/33501.htm
6	3GPP TS 29.244	3gpp.org/DynaReport/29244.htm
7	3GPP TS 29.502	3gpp.org/DynaReport/29502.htm
8	3GPP TS 29.503	3gpp.org/DynaReport/29503.htm
9	3GPP TS 29.507	3gpp.org/DynaReport/29507.htm
10	3GPP TS 29.509	3gpp.org/DynaReport/29509.htm
11	3GPP TS 29.510	3gpp.org/DynaReport/29510.htm
12	3GPP TS 29.518	3gpp.org/DynaReport/29518.htm
13	3GPP TS 29.531	3gpp.org/DynaReport/29531.htm

Terms and acronyms

AMBR (Aggregate Maximum Bit Rate): parameter responsible for maximum subscriber data transmission speed

GTP-U (GPRS Tunneling Protocol User Plane): a protocol that describes and transmits data between the radio network and the packet network

KAUSF: an authentication key

KSEAF: a security key

NAS (Non-Access Stratum): a protocol that describes and implements interaction between the user device and the network core

PDU (Packet Data Unit) session: a session for transferring data between a subscriber device and the network

PFCP (Packet Forwarding Control Protocol): a protocol for interaction between network components on the control plane and user plane

QoS (Quality of Service): quality of service parameter

SUCI: Subscriber Concealed Identifier

SUPI: Subscriber Permanent Identifier

TEID: Tunnel Endpoint Identifier