SCTE·ISBE CABLE-TEC EXPO 2019 NEW ORLEANS, LA SEPT. 30-OCT. 3

2019 Fall Technical Forum SCTE·ISBE • NCTA • CABLELABS

Security Analysis Of 5G Mobile Networks

A Technical Paper prepared for SCTE•ISBE by

Tao Wan
Principal Architect
CableLabs
858 Coal Creek Circle, Louisville, CO 80027
303.661.3326
t.wan@cablelabs.com

Mansour Ganji
Lead Security Architect
Rogers Communications
8200 Dixie Rd, Brampton, ON, CA, L6T 4B8
647.289.4679
mansour.ganji@rci.rogers.com

Table of Contents

List of Figures

List of Tables

Introduction

Cellular mobile networks have evolved from 2G to 5G over the past three decades. Mobile services offered by 2G, 3G, and 4G networks have always been voice calls and data network access. The introduction of 5G has changed this protocol by providing the communication technologies for many more use-cases tailored for each specific requirement. More specifically, 5G will provide network connectivity not only for human-to-human communications but also for human-to-machine, and machine-to-machine communications. 5G user equipment will fall into a broad range of devices where at one end they are fully-fledged computers, and at the other end they are single-purpose and resource-constrained IoT devices.

Because of the potentially significant impact on our society by 5G, its security is of critical importance and must be treated systematically. Researchers from both industry and academia have been working on improving security in 5G for a while. For example, the 3GPP SA3 working group has been studying and defining security specifications for 5G systems since 2017. Academic researchers are also helping to identify flaws in 5G specifications and are proposing enhancements. In this paper, we conduct a summary of security threats to 5G and prior generations of mobile networks and discuss how some of these threats are being addressed by the 3GPP 5G security standard.

Threats against cellular mobile networks can be generally classified into three categories: threats against user equipment or subscribers, threats against radio access networks, and threats against mobile core networks. In this paper, we focus on threats against subscribers. More specifically, we consider how subscriber security can be attacked by exploiting design constraints or flaws in control channels including broadcasting, paging and dedicated unicasting channels.

Due to the fact that neither broadcasting nor paging messages are authenticated in 5G (release 15) and prior generations, they are subject to spoofing, enabling many of the attacks against subscribers. Unicasting messages may or may not be security protected. Unprotected unicasting messages are also subject to spoofing and can be exploited to attack subscribers.

Through a summary of security threats against and defenses by 5G networks, we hope that a realistic understanding of expected 5G security can be established across the networking community, and hopefully among the general public as well.

Background

A cellular mobile network including 5G consists of user equipment (UE), access networks and core networks (see Figure 1).

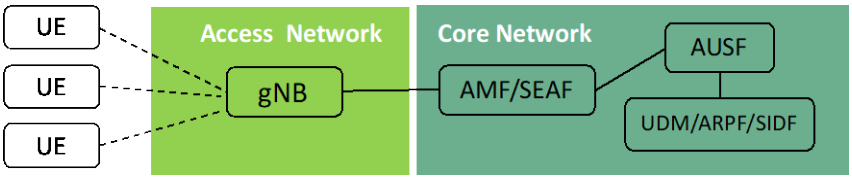

Figure 1 - Simplified 5G System Architecture

A UE is a device connecting to the cellular network to consume the services offered by the network,e.g., voice calls and data network access. A UE usually consists of an application processor running a general-purpose OS such as Android, and a baseband processor running mobile network protocol stacks (e.g., LTE

or 5G). A UE often contains a Universal Integrated Circuit Card (UICC) hosting at least a Universal Subscriber Identity Module (USIM) application, where a cryptographic key is stored and shared with the subscriber's home network and is the basis for mutual authentication of the UE and the network.

An access network is usually based on radio technologies, although other types of access networks including wireline access technologies are supported,e.g. in 5G (release 16). Radio access networks (RAN) manage radio resources between the UE and the next generation NodeB (gNB) to provide connectivity between the UE and the rest of the networks. 5G radio resources can be organized into local channels, including a Broadcasting Control Channel (BCCH), Paging Control Channel (PCCH), Common Control Channel (CCCH), Dedicated Control Channel (DCCH) and Dedicated Traffic Channel (DTCH).

5G core networks consist of virtualized network functions communicating with each other using web-based service requests and responses. The adoption of service-based architecture and virtualization technologies by 5G also result in the introduction of new network entities in 5G core networks, including Security Anchor Function (SEAF), Authentication Server Function (AUSF), Unified Data Management (UDM), Authentication credential Repository and Processing Function (ARPF) and Subscription Identifier De-concealing Function (SIDF).

Threats against Broadcasting

A broadcast channel is used by the network (e.g., gNB) to broadcast system information for the UE to select and connect to the network. In 5G, gNB broadcasts a Master Information Block (MIB) and a number of System Information Blocks (SIB), some of which are always transmitted periodically, and others are only transmitted on-demand by UE. MIB contains physical layer information required by UE to establish radio links with gNB to receive the first SIB for cell selection. SIB1 contains information for UE to connect to a network including PLMN identifiers, track area code, cell identifier, etc. SIB2 to SIB5 contain information about cell re-selection, SIB6 to SIB8 contain public warning information (e.g., earthquake and tsunami warnings) and SIB9 contains information about time (e.g., UTC time and local time).

All user equipment needs to engage with all broadcast messages from all available eNB/gNB radio towers. This is to choose the network that it wants to connect to and then choose the frequency and channel that the base station is mandating it to use.

Since broadcasting messages are intended for all devices in an area, they are transmitted in clear text. Further, they are not authenticated for origin, nor protected for integrity in 5G (release 15) and prior generations. Therefore, all broadcasting messages are subject to spoofing and tampering. We consider four types of possible attacks:

First, the cell selection information can be forged to lure UE away from a legitimate cell, e.g., to a fake base station. More specifically, a fake base station can intercept all broadcast information from a legitimate gNB and rebroadcast the same information with higher power and with some modified elements (e.g., tracking area code) to fool the UE that it has entered a new tracking area and then reselect the fake cell. This is a known issue and has been actively exploited, e.g., to send fake short messages for fraud purposes [10, 11, 15].

Second, SIB3 to SIB5 contain a black list of cells which UE should not select. If this list is forged and cached, the UE may be subject to denial of service attacks if all available cells in an area are included in a faked blacklist. This attack has not been reported before and it is not clear how practical it is.

Third, SIB6 to SIB8 contain public warning information, which if spoofed may cause a public disturbance and instability. This is a known attack and has been demonstrated in LTE by broadcasting fake presidential alerts to a crowd [12] and it is applicable to 5G (release 15).

Fourth, SIB9 contains timing information, which can be spoofed to influence the time setting in UE. Since time is also critical to security, particularly in public key certificate validation (e.g., validating if a certificate has expired), spoofed timing information may lead to other attacks. We have not seen such an attack yet, but it is certainly possible.

Threats against Paging

One of the requirements for the handset is to stay in a dormant mode while not actively using the network. This is both to reduce the battery consumption and also to minimize the network resource usage. While in this state, if there's an incoming call or a message to be delivered to the UE, the mobile network first pages the subscriber over its last known tracking area. Paging messages are sent over the paging channel in clear text without any authenticity or integrity protection. To protect user privacy, the subsriber's permanent identifier (SUPI) is not included in any paging messages in 5G. Instead, a Global Unique Temporary Identifier (GUTI), namely 5G-GUTI, is used.

5G-GUTI is assigned to the UE by the network (i.e., AMF) in the following situations [3]: 1) upon receiving a Registration Request message of types: a) initial registration; b) mobility registration update; and c) periodic registration update; 2) upon receiving a Service Request message in responding to a paging message. In this case, a new 5G-GUTI is sent to the UE by a UE Configuration Update Procedure. Note that in all cases, a new 5G-GUTI are also sent out to UE after NAS security context has been activated. An operator may implement a more frequent change of 5G-GUTI.

Attacks exploiting the paging messages can be classified into three categories: 1) location tracking; 2) denial of services; and 3) SUPI disclosure.

First, paging messages can be capatured and used to determine the coarse-grained location of a UE upon the observation of the presence of an UE identifier of interest. Depending on the size of the area to which paging messages are sent, tracked location can be large or small. For example, in 4G/LTE, a UE can be tracked to an area of 2 km^2 (the size of an LTE cell) when the smart page is implemented. Since a paging area may become even smaller in 5G, location tracking can be more precise. Although the use of a temporary identifier (e.g., 5G-GUTI) with frequent changes can mitigate a location tracking attack, other flaws can still make it possible. For example, Torpedo (tracking via Paging message distribution) [4] exploits side channel information to track the user's location.

Second, paging can be exploited to deny the service of a UE. For example, an adversary can listen to the paging channel and respond to a paging request quickly so that the response from a victim is ignored by the network. In this case, the victim will not be able to receive its service (e.g., an incoming call or a text message). The attacker can also forge false paging signals and send them to the victim's handset device. Depending on the LTE or a 5G baseband modem on the target's phone, the forged messages may push the handset into a detached state. And if the attackers can continuously send the forged messages, they can cause a DoS attack on the victim.

Third, paging messages may disclose some information about a UE's SUPI even though 5G-GUTI is used and changed frequently. For example, it is discovered in [4] that an IMSI is used to calculate a paging occasion [16] which can leak the last 7 bits of the IMSI. This flaw is fixed in the next version of TS 38.304 [17].

Threats against Unicasting

Threats against unicasting messages can be further classified based on the states of the UE in the process of authentication. More specifically, we classify such threats into three sub-categories, namely, threats against unicasting prior to authentication; threats against the authentication protocol itself, and threats against unicasting messages after authentication.

1. Pre-Authentication

The 3GPP standards contain specifications for securing the communication channel between user equipment and the network. But in all of the releases before 5G (Rel.15), they come into play only after the device has been authenticated and the security context has been built. Encrypting traffic between user equipment and the network needs a key, and that key would only be built during the security context creation. Therefore, every communication before that stage had to be made in clear-text. This issue has always been a challenge as this leaves space for eavesdropping on the communication channel and obtaining information that is sensitive in nature. The most important piece of data that can be revealed during this stage is the IMSI (International Mobile Subscriber Identification) which is unique to every subscriber. Obtaining IMSI is a big privacy concern as it allows tracking the subscribers' location. Besides, many of the attacks using DIAMETER signaling protocol require the attacker to know the victim's IMSI beforehand. So disclosing the IMSI opens the door to many more attacks. Although 3GPP had included using of temporary subscriber identifications like TMSI (Temporary Mobile Subscriber Identification) and GUTI (Globally Unique Temporary Identifier), there are some attacks reported to be run successfully that could force the user equipment to disclose the IMSI during a clear-text communication. [3]

This has been improved in the latest 3GPP technical specifications for 5G by adding an asynchronous encryption covering the whole authentication process. With this approach, the network operator will use a public-private key pair and the public portion of the key will be pre-provisioned on every subscriber's UICC (Universal Integrated-Circuit Card). The subscriber identifier has been renamed to SUPI (Subscriber Universal Public Identifier) in the recent 3GPP release document and it is encrypted before being transmitted over the air interface. The encrypted identity is called SUCI (Subscriber Universal Concealed Identifier) and is the main part of the information that is being transmitted for the authentication period [3].

Prior to the authentication and key agreement, certain RRC layer messages need to be exchanged between the UE and the network, which are subject to spoofing and tampering. Two examples of such RRC messages are RRC_UECapabilityEnquiry and RRC_UECapabilityInformation. Some NAS messages (e.g., NAS Service Reject) may also be sent out to UE prior the establishment of security context. Those unprotected messages can be exploited to attack both the UE and the network.

2. Authentication

The authentication process in 5G continues to use an AKA algorithm like the previous 3G and LTE generations; the algorithm is called 5G AKA. There are two new authentication methods that have been added to the list and they are EAP-AKA' and EAP-TLS (only in Non-Public network or isolated deployment). Choosing which authentication method to utilize will be a decision made by the home network.

As mentioned earlier, the authentication process has improved from the previous generations. One of the big improvements is adding the home network's public key to the process. With the subscriber (UE) having the home network's public key, it can start encrypting sensitive authentication data such as SUPI right from the beginning of the authentication process. The second improvement is reducing the trust in the serving network for authenticating the roaming subscriber. In the previous network generations, the serving network had the option to fake the presence of a subscriber, thus tricking the home network into updating a subscribers' location, dropping the legitimate security context and running a DoS as a result, or even redirecting SMS and connecting to a malicious or compromised serving network. The new advances in 5G roaming authentication prevent all these issues because the home network will not authenticate a roaming subscriber, unless it implicitly receives the data that it expects from the subscriber in the authentication process. It is only after this stage that the home network passes the encryption and integrity checking keys to the serving network along with the SUPI. [6]

However, these improvements require the channel between the home network and the serving network to be authenticated and encrypted as it now passes sensitive information like K_{SEAF}. Since this is a design consideration rather than a 5G specification, we will not dive deeper into this context.

There are also a number of papers [4,5,6] which find some security issues with the 5G authentication and key agreement protocols. Those issues include information disclosure from side channel, race condition exploitation, and improper protection of SQN. 3GPP is working on to mitigate some of those issues.

3. Post-Authentication

There are certain unicasting messages that cannot be protected due to design limitations, even after security contexts have been established and are in use between UE and the network after a successful authentication and key agreement. Those messages can be sent out in clear texts with neither confidentiality nor integrity protection. Thus, they are subject to spoofing and tampering attacks. These messages include:

Table 1 - Messages to be sent and received out of authentication context

Network to UE	UE to Network
IDENTITY REQUEST	IDENTITY RESPONSE
AUTHENTICATION REQUEST	AUTHENTICATION RESPONSE
AUTHENTICATION RESULT	AUTHENTICATION FAILURE
AUTHENTICATION REJECT	SECURITY MODE REJECT
REGISTRATION REJECT	REGISTRATION REQUEST
DEREGISTRATION ACCEPT	DEREGISTRATION REQUEST DEREGISTRATION ACCEPT
SERVICE REJECT	

These messages are not confidentiality or integrity protected as they may sometimes need to be communicated out of the security context. But, this leaves a possibility for an attacker to spoof either the subscriber or the network and cause a service disruption to a subscriber. If the attacker is in a position to continuously send a malformed message to the subscriber or to the AMF, they can run a targeted DoS against a specific subscriber. [13]

This also applies to the emergency service requests where both confidentiality and integrity need to be set to "null" due to the nature of the call.

Conclusion

There has been significant improvement in 5G authentication in comparison to the previous cellular network generations. Nevertheless, there are still areas that are susceptible to potential attacks or misuses. Most of the cases where a vulnerability still exists are information exchanges that can or should be allowed without a security context in place. These are messages that are supposed to be available to all subscribers in an area or channels to be present for emergency communications. The current trust model for cellular mobile networks is based on isolated trust within each individual service provider. In other words, there are many trust trees in the communications industry and each tree has a root within a specific service provider. Outside that trust tree, the subscribers and service providers have no choice but to interact with "untrusted" entities that have the potential to be malicious. With this model, any improvements in the authentication process and trust establishment will remain a localized attempt and will not help with the global trust.

One possible solution for this issue is to follow the same model or models that have been proven to work in the public Internet access area. The trust model built for safe web browsing, for example, could be a good start for more developments in the cellular network. Having global trust anchors endorsed by the home network that all of its user equipments can trust could be a viable solution. In such a model, even the communications that have to be outside subscribers' security context, can still be digitally signed so that the subscriber can verify that a message is coming from "a legitimate service provider" even if it's not its own home network. We hope that 3GPP will embrace digital signature based solutions which can mitigate most of the threats discussed in this paper.

Abbreviations

3GPP	3rd Generation Partnership Program
AKA	Authentication and Key Agreement
AMF	Authentication Management Function
DoS	Denial of Service
EAP	Extensible Authentication Protocol
gNB	Next Generation NodeB
GUTI	Global Unique Temporary Identifier
HN	Home Network
IMSI	International Mobile Subscriber Identity
ISBE	International Society of Broadband Experts
LTE	Long Term Evolution
SN	Serving Network
SUPI	Subscriber Permanent Identifier
SUCI	Subscriber Concealed Identifier
TLS	Transport Layer Security
UE	User Equipment
UICC	Universal Integrated-Circuit Card
SCTE	Society of Cable Telecommunications Engineers

Bibliography & References

[1] 3GPP TS 24.501. “Non-Access-Stratum (NAS) protocol for 5G System (5GS), Stage 3 (Release 15). Jan 2019.

[2] 3GPP TS 38.321. “NR; Medium Access Control (MAC) protocol specification (Release 15). V15.5.0, March 2019.

[3] 3GPP TS 33.501. “Security architecture and procedures for 5G system, (Release 15)”

[4] Hussain SR, Echeverria M, Chowdhury O, Li N, Bertino E. Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information. In 26th Annual Network and Distributed System Security Symposium, NDSS, San Diego, CA, USA, February 2019.

[5] Borgaonkar R, Hirschi L, Park S, Shaik A. New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols. Proceedings on Privacy Enhancing Technologies 2019.

[6] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler. "A formal analysis of 5G authentication." In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS’18), October 2018.

[7] Cremers, Cas, and Martin Dehnel-Wild. "Component-Based Formal Analysis of 5G-AKA: Channel Assumptions and Session Confusion." In 26th Annual Network and Distributed System Security Symposium, NDSS, San Diego, CA, USA, February 2019.

[8] Golde N, Redon K, Seifert JP. Let me answer that for you: Exploiting broadcast information in cellular networks. In Proceedings of the 22nd {USENIX} Security Symposium ({USENIX} Security 13) 2013 (pp. 33-48).

[9] Shaik A, Borgaonkar R, Asokan N, Niemi V, Seifert JP. Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. In 23th Annual Network and Distributed System Security Symposium, NDSS, San Diego, CA, USA, February 2016.

[10] Marc Lichtman, Raghunandan Rao, Vuk Marojevic, Jeffrey Reed, Roger Piqueras Jover. "5G NR Jamming, Spoofing, and Sniffing:Threat Assessment and Mitigation"

[11] Roger Piqueras Jover, Vuk Marojevic. "Security and Protocol Exploit Analysis of the 5G Specifications". IEEE Access Magazine, Volume 7, 2019

[12] Gyuhong Lee et all. “This is Your President Speaking: Spoofing Alerts in 4G LTE Networks”. MobiSys ’19, June 17–21, 2019, Seoul, Korea

[13] 3GPP TS 23.501 V16.0.2 (2019-04). System Architecture for the 5G System; Stage 2 (Release 16)

[14] 3GPP TS 38.331. “NR; Radio Resource Control (RRC) protocol specification (Release 15). V15.5.0, March 2019.

[15] Li, Zhenhua, 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." In Proceedings of NDSS. February 2017.

[16] 3GPP TS 38.304. “NR; User Equipment (UE) procedures in Idle mode and RRC Inactive state (Release 15). V15.0.0, June 2018.

[17] 3GPP TS 38.304. “NR; User Equipment (UE) procedures in Idle mode and RRC Inactive state (Release 15). V15.1.0, September 2018.