Security: A Trust Perspective
22nd Oct 2020

End to end Security in 5G NR
by
Satish Jamadagni
Vice Chairman, TSDSI
A recent report from Cybereason:

The implications of a individuals, companies, non state actors or nation-states "infiltrating into the deepest segments of providers’ network, including some isolated from the internet," enabling hackers to "compromise critical assets and steal communications data of specific individuals" are extremely significant. It suggests almost open access for intelligence harvesting.

Cybereason also pointed out that "even though the attacks targeted specific individuals, any entity that possesses the power to take over the networks of telecommunications providers can potentially leverage its unlawful access and control of the network to shut down or disrupt an entire cellular network as part of a larger cyber warfare operation."
Typical Attack Types

Summary

- Location Tracking,
- Eavesdropping, SMS interception
- Fraud, Denial of Service
- Credential theft, Data session hijacking
- Unblocking stolen phone
- One-time password theft and account takeover for Telegram, Facebook, Whatsapp

- There is a constant evolution and fine tuning of those attacks ongoing
Securing 5G / LTE Networks
Typical attack in a non “cloudified” network

- Target User Location
- Target User Call redirection / replication
- Target User Call recording

HOW DOES ONE GO ABOUT – ENTRY POINTS

- SS7 /SIGTRAN
- DIAMETER
- Direct HSS approach (Home HSS to AS to Target HSS)

Best entity to target
HSS

IPX

TSDSI Tech Deep Dive Conference 2020
Security in 5G
Why is it more important

5G has 200 times more access points for hackers than existing networks, experts have warned.

- Next-generation 5G mobile networks are expected to connect millions of things, be they self-driving cars in need of real-time data or cows with collars that monitor livestock health. But the vast number of connections and the updated network architecture vastly expand the number of access points for hackers to attempt cyberattacks. 5G networks have 200 times more attack vectors, or paths to gain access to a network, compared to their 4G predecessors. The whole attack surface has really multiplied.

- Telecoms’ existing networks aren’t immune to cyberattacks, as an example an Asian mobile operator that detected a security breach last May which was 240 days after malicious actors entered its system. The difference with 5G is the magnitude of access points connected to the network especially some Internet of Things devices can be hacked in 15 minutes. 5G networks are also more reliant on software, edge computing and cloud-native architecture, creating a huge increase in the interconnections.

Typical Cloud Attacks

Attackers are leveraging the cloud to make their attacks more effective, while enterprises are failing to protect themselves against attacks on their cloud infrastructure. Attackers are using cloud resources to host malware and using advanced architecture such as microservices to stay ahead of their targets. As an example, attackers also use single sign-on authentication services such as OATH to compromise users' social media accounts and then use that access to get into enterprise software-as-a-service (SaaS) applications, just as previously email was used to gain access to the enterprise. Once inside an enterprise cloud, all data will be compromised.

5G Core is going to be based fully on cloud infrastructure and as such the 5G core is very vulnerable.
The first half of 2020 saw an increase in attacks and threats directed at Operational Technology (OT) and Internet of Things (IoT) networks, especially from IoT botnets, according to a report from Nozomi Networks.

Ransomware attacks in particular are raising. According to a recent report from SonicWall, ransomware attacks increased globally by 20 percent in the first half of 2020. The Foreign exchange company Travelex was attacked by the REvil ransomware that put its website and mobile app offline and left customers without access to their travel money. The company reportedly paid $2.3 million in Bitcoin to the hackers to bring their systems back online, and it has since filed for bankruptcy in early August.
IOT Security
Smart City example

The IoT Security Challenge – the Smart City as an Example

gsma.com/iotsecurity
Introduction to Security in 5G NR

NSA – Non Stand Alone

In December 2017, the Non-Standalone (aka. NSA) specifications for 5G new radio (NR) were approved, followed in June 2018, by the Standalone. Security from a NSA and SA are considered

The key feature of Non-Standalone is the ability to utilize existing LTE and EPC infrastructure. EN-DC (E-UTRAN New Radio – Dual Connectivity) uses LTE as the master radio access technology, while the new radio access technology (i.e. NR) serves as secondary radio access technology with User Equipment's (UEs) connected to both radios.

Except for capability negotiation, security procedures for EN-DC basically follow the specifications for dual connectivity security for 4G.
In SA, the trust model in the UE is reasonably simple: there are two trust domains”

1. The tamper proof universal integrated circuit card (UICC) on which the Universal Subscriber Identity Module (USIM) resides as trust anchor

2. The Mobile Equipment (ME). The ME and the USIM together form the UE.

The network side trust model for roaming and non-roaming cases are shown in the next slide.

Currently, i.e. in the 3GPP 5G specification, the AMF (Access and Mobility Management Function) is collocated with the SEcurity Anchor Function (SEAF) that holds the root key (known as anchor key) for the visited network.

The security architecture is defined in a future proof fashion, as it allows separation of the security anchor from the mobility function that could be possible in a future evolution of the system architecture.
Security – 5G NR
SA – Stand Alone

Access and Mobility Management Function (AMF)
Authentication Server Function (AUSF)
Unified Data Management (UDM)
Authentication Credential Repository and Processing (ARPF)

ARPF is a functional element of the UDM

Source: www.3gpp.org
Security – 5G NR
SA – Stand Alone

• The AUthentication Function (AUSF) keeps a key for reuse, derived after authentication, in case of simultaneous registration of a UE in different access network technologies, i.e. 3GPP access networks and non-3GPP access networks such as IEEE 802.11 Wireless Local Area Network (WLAN).

• Authentication credential Repository and Processing Function (ARPF) keeps the authentication credentials. This is mirrored by the USIM on the side of the client, i.e. the UE side. The subscriber information is stored in the Unified Data Repository (UDR).

• The Unified Data Management (UDM) uses the subscription data stored in UDR and implements the application logic to perform various functionalities such as authentication credential generation, user identification, service and session continuity etc. Over the air interface, both active and passive attacks are considered on both control plane and user plane. Privacy has become increasingly important leading to permanent identifiers being kept secret over the air interface.

• In the roaming architecture, the home and the visited network are connected through SEcurity Protection Proxy (SEPP) for the control plane of the internetwork interconnect.
  • This enhancement is done in 5G because of the number of attacks coming to light recently such as key theft and re-routing attacks in SS7 and network node impersonation and source address spoofing in signaling messages in DIAMETER that exploited the trusted nature of the internetwork interconnect.
Security – 5G NR
Enhancements over 4G

5G brings several enhancements to 4G LTE security, some of the key points are presented in this section:

Primary authentication: Network and device mutual authentication in 5G is based on 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.

Secondary authentication: Secondary authentication in 5G is meant for authentication with data networks outside the mobile operator domain. For this purpose, different EAP (Extensible Authentication Protocol) based authentication methods and associated credentials can be used.
• **Inter-operator security:** Several security issues exist in the inter-operator interface arising from SS7 or Diameter in the earlier generations of mobile communication systems. 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):** The 5G core network is based on a service based architecture, which did not exist in 4G and earlier generations. Thus, 5G also provides adequate security for SBA.

• **Key hierarchy:** The 5G hierarchy reflects the changes in the overall architecture and the trust model using the security principle of key separation. 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 will also bring solutions for the Internet of Things (IoT) in the form of massive Machine Type Communication (mMTC) and Ultra-Reliable and Low Latency Communications (URLLC).

- mMTC relates to very large number of devices transmitting a relatively low volume of non-delay-sensitive data.

Data over NAS (DoNAS) is a control plane cellular IoT optimization that allows the network to transport user data within signaling messages. This feature transports user data or SMS messages via the MME (mobility management entity) by encapsulating them in NAS (non-access stratum) signaling.

One key security benefit of this feature is that the customer/user data is encrypted and its integrity protected using the same mechanism reserved for network signaling, thus ensuring similar levels of protection.

Support of Security for High Reliability by Redundant Data Transmission in User Plane:

Redundant data transmission introduces additional threat surface for attackers to take advantage of the presence of multiple user plane paths. If any one of the two user plane path is compromised, then the whole proposition of URLLC security can collapse. To realize high level of reliability, the 5G system supports confidentiality and integrity protection for user plane data transmitted over multiple paths as the primary feature.

UP Security Policy Handling for Multiple PDU Sessions established for Redundant Data Transmission introduces another aspect from the security perspective.

An attacker may perform jamming on an integrity protected path to prevent forwarding of the user plane data from the gNB to the UPF and simultaneously modify the data on the non-protected path. To address this scenario, two solutions are proposed:

1. Encryption and/or integrity protection of user plane
2. The Master gNB (MgNB) to ensure that the UP security policy is forwarded and used by the Secondary gNB (SgNB) for the two PDU sessions in the redundant data transmission.

3GPP SA3 (security) working group has started the study on security aspect of URLLC since the end of 2018. This work resulted in TR 33.825 [9]. The Normative work is included in the Release 16 (3GPP TS 33.501)
The Hardware Backdoors
Supply Chain Issues

- Sepio Systems' co-CEO, Yossi Appleboum, had recently providing proof of hacked motherboards used in servers, this time at an unnamed US telecommunications company. Due to the sensitive nature of the disclosure and potential impact on business.

- Security researchers have demonstrated how easy it is to place a tiny implant on a hardware motherboard that can interface with the baseboard management controller (BMC). This could allow a hacker to run code or take over other aspects of a hardware communication and power system, providing another means of system access with dangerous consequences.

- The BMC is “a kind of superchip that administrators use to remotely log in to problematic servers, giving them access to the most sensitive code even on machines that have crashed or are turned off”. The BMC has access to and authorization to control and/or interface with various aspects of a hardware system, including power supplies, LAN ports, OS installations, file systems and others. This makes it very difficult to secure and control an attack that leverages it once it occurs and spreads through the hardware and even onto other systems. These hardware implants cost virtually nothing for hackers to implement if they have access to the supply chain and can get them into motherboards. The cost of such “Spy Chips” could be not more than five dollars which is even more worrying.
Thank You

<vicechairman@tsdsi.com>