Learning from the Past: a Survey of VoLTE Vulnerabilities

Son Nguyen Truong Pham
sntpham@uwaterlo.ca
University of Waterloo
Waterloo, Ontario, CA

ABSTRACT

Long-Term Evolution (LTE) was first commercially used in 2009 and brought many new implementations into the world. After three years, in 2012, Voice over LTE (VoLTE) service was rolled out to improve the quality of voice calls and reduce the complexity of the Circuit Switch (CS) service. About a decade later, 5G New Radio (NR) was introduced, significantly improving data rates, and opening a new horizon for AI, autonomous vehicles, and Virtual Reality. With the advent of 5G, VoNR (Voice over NR) technology also became available to the public. However, the differences between VoNR and VoLTE for end users are not identical, as the quality of VoLTE is already mature and further improvements in data rates are not necessary for voice calls. Looking ahead, VoLTE will continue to be in service for a long time, covering a vast number of users and applications including car, IoT, health, and mobile devices. Therefore, vulnerabilities are crucial for both users and operators if they are not addressed and resolved properly.

1 INTRODUCTION

Before studying the VoLTE topic and associated acronyms, let's explore things around us for a minute. Imagine you are craving sweet treats from a famous bakery. There is a catch - the bakery has an alarm system, which will call a guard when it detects an intruder. Furthermore, it can operate in adverse conditions without electricity and WiFi. To assist with that feature, it should have a battery and cellular module. Recently, news that mentioned 2G/3G service would be halted in 2022 caught your attention. Things seem to become clear; you start to connect the dots and conclude that the system might use LTE with VoLTE enabled for establishing phone calls. How can we get the cookies without being busted? You try to ask ChatGPT; however, it is not allowed to teach you how to exploit any system. Eventually, you come up with an idea to *jam the cellular module* and found the methods on the IEEE or ACM website. Next, imagine after 4 years of hard work at UWaterloo, you get a job at a telecommunication company. And your role involves identifying discrepancies in the charging data. You notice user Bob usually has long voice calls to a specific phone number every day, and the bandwidth Bob's device asking for is abnormal. Bob is suspicious and he might know some vulnerabilities of the system.

As you see, these examples touch upon potential exploits associated with VoLTE. Other exploits are more severe, which are addressed in this survey paper. Now, let's return to VoLTE.

Looking back, I purchased my first Samsung S3 in 2013, and my operator AT&T offered HD Voice service or VoLTE in 2014. Based on experience, one thing I notice is that the time takes to establish a call between 1X and VoLTE is longer than VoLTE itself. Also, the sound in 1X is not clear compared to its successor.

Then, amidst the chaos of the pandemic, isolation, remote work, and TikTok, the fifth-generation wireless technology emerged. 5G Non-Standalone technology was impressive as it uses dynamically shared spectrum (DSS) with the existing LTE network to increase bandwidth and enhance speed. Besides NSA, there is a "steroid" version called Standalone (SA), or 5G mmWave, which operates on upper-frequency bands ranging from 20-40GHz. Higher frequency adds tremendous data rates. In 2021, a download speed recorded on a Samsung S21 device via the Ookla app reached about 2 GB/s at an urban mall in Los Angeles. One limitation is that the device needs to be close to the cell (10-20 meters). Coupled with this, faster speed induces heating and draining batteries on mobile devices.

Voice over 5G is referred to as VoNR, which operates on the SA network and does not rely on the LTE structure. In contrast, NSA will fall back to VoLTE whenever a phone call is made. Subsequently, VoLTE will fall back to Circuit Switched (CS) through CS FallBack (CSFB) if the recipient binds to a 2G or 3G network.

While there are distinctions between VoNR and VoLTE, the latter will continue to be in service for a long time. Despite many third-party apps offering seamless communication via VoIP, customers still prefer VoLTE based on its simplicity as a carrier's default feature. The dominant popularity of VoLTE is the first reason to compose this paper. The next reason is to review and understand the foundation of VoLTE so we can improve 5G and develop 6G. Finally, the last reason is to inform readers about the existing vulnerabilities. Although there is a broader survey paper for threats and attacks in LTE that also includes VoLTE[10], you might find a different perspective in this paper.

To keep coherence throughout the paper, most abbreviations and capitalized words are limited to avoid disrupting the reading flow.

In section 2 of this paper, the technical background, we'll first explore the architecture of LTE and IMS (IP Multimedia Subsystem). Moving on to section 3, "Attack methods," we'll classify attacks based on their final targets, namely, attacks against the user and attacks against the operator. We also include a discussion on the trade-off of the current design. Lastly, we draw conclusions and wrap up in section 4.

2 BACKGROUND

Figure 1: Background RoadMap

In this section, we begin by looking at the components inside a phone. After that, we'll explore the main parts of the core network responsible for call processing. As we go through each part, various protocols used in the network are introduced. Finally, we'll have an overview of the first three layers of the LTE protocol stack.

2.1 User Equipment

User equipment (UE) refers to any VoLTE-enabled device that contains a unique identification.

Universal Subscriber Identity Module (USIM) is software loaded inside a physical card or UICC. When inserted into a mobile device, this card enables access to data and voice services. Currently, the latest version of UICC is eSIM, which is soldered directly into the device. It has two main functions. The first function is to verify the user. And another function is to store a unique user identity known as the IMSI [2].

International Mobile Subscriber Identifier (IMSI) is a unique number stored in both the USIM and subscriber servers. It consists of a maximum of 15 digits. The first three digits are for the mobile country code (MCC), which describes the home country of the subscriber. The next 2 to 3 digits represent the mobile network code (MNC) for network operators such as Bell, Vodafone, or AT&T. The remaining digits make up the mobile subscriber identification number (MSIN), providing further individual identification.

Public land management number (PLMN) is the combination of MCC and MNC.

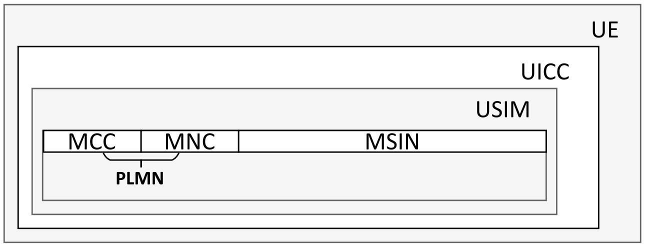

Figure 2: User Equipment Components

2.2 Core Network

In the core network, our primary focus will be the Evolved packet core (EPC) and the Internet multimedia subsystem (IMS); however in this paper, some attacks involve 2G/3G, so we will discuss a few blocks from previous generations here as well.

2.2.1 *Evolved Packet Core.*

Evolved NodeB (eNB, eNodeB) is the first node in the network that communicates with UE and is referred to as the Radio Access Network (RAN).

Mobility management entity (MME) works as a control center in EPC.

Home subscriber service (HSS) stores user-unique information like IMSI in a central database.

Home location register (HLR) performs a function similar to the HSS, but it is used in 2G/3G mobile networks.

2.2.2 *IP media subsystem.*

IP media subsystem (IMS) As a novel component in LTE, the IMS network optimizes voice and video streaming services while efficiently managing resources. IMS utilizes the Session Initiation Protocol (SIP).

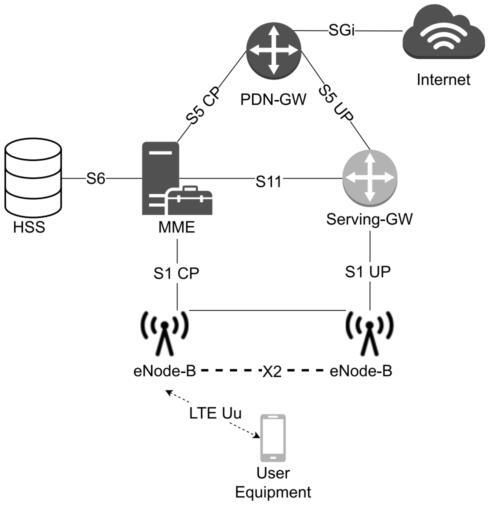

Figure 3: Core Network Components

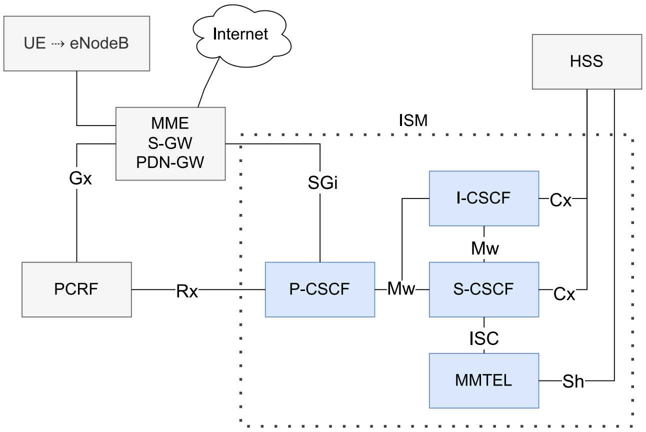

Figure 4: IP Media Subsystem Components

Policy and Charging Rules Function (PCRF) acts as an agent between the IMS and the core by setting rules and applying charging policies to customers. These rules can include promotion packages such as "Free Netflix data" or "Free Facebook browsing."

Call session control function (CSCF) Most IMS systems are software-based, and CSCF is one of them. It consists of three distinct blocks to manage call transmission and reception: the proxy, interrogating, and serving blocks.

Proxy-CSCF is the first contact point in IMS that acts as a SIP proxy, forwarding SIP messages from the user to other neighboring blocks.

Interrogating-CSCF provides the contact point for all calls to access subscribers within a network, determines the S-CSCF by searching the subscriber server, and assigns the S-CSCF to the UE in the registration process.

Serving-CSCF controls the SIP registration and SIP proxy. Based on the function described above, the S-CSCF can be considered as a controller within the CSCF.

Multimedia telephony (MMTEL) handles other features of voice calls, such as voicemail, waiting tone, and group calls.

2.2.3 *Call Switch Fall Back.*

Call Switch Fall Back (CSFB) is a method used to combine LTE and 3G voice calls. In CSFB, we have similar blocks as in LTE. Here are the blocks mentioned in this paper:

- **Media Switching Center (MSC)** acts similarly to MME.
- **SGs** is the interface that connects MME and MSC, helping both blocks stay in sync and store a copy of the combined Tracking Area (TA) for LTE and Location Area (LA) for 3G.

2.2.4 *Protocols.*

Session Initiation Protocol (SIP) A text-based protocol used to initiate and tear down call flows.

Diameter Protocol Replacing SS7 blocks in LTE and is mainly used in charging functions.

Real-Time Protocol (RTP) Used to transport voice data.

Packet Data Convergence Protocol (PDCP) Compresses, adds authentication and transmits data to upper layers.

Non-Access Stratum (NAS) Protocol Provides procedures for mobility and security control between UE and MME. The mobility field includes methods such as Attach, Detach, Tracking Area Updates, and Service Requests. For security, instead of using UE's unique number IMSI, NAS allocates another ID for UE called GUTI.

GPRS Tunneling Protocol (GTP) Originally used in the Gn interface of the General Packet Radio Service (GPRS), it carries over to the user plane of the S1 interface in LTE. Additionally, GTP helps forward user data packets during handover between eNodeBs.

2.3 Protocol Stacks

Physical layer is the base level in the communication stack and plays a crucial role in transmitting and receiving signals. It involves the modulation and demodulation of the signal, as well as handling various modulation schemes such as quadrature amplitude modulation (QAM) or binary phase shift keying (BPSK). The main physical components in this layer include the transmitter, receiver, converter, amplifier, and antenna.

The scope of this paper is limited to VoLTE; however, jamming in this layer is worth mentioning. The attack is conducted by sending high power at the target frequency. Normally, UE will try to camp on the strongest signal. If an adversary transmits high-power signals, the UE will ignore real cell towers and camp instantly on the fake cell [18]. As a result, this will cause a denial of service on the UE itself. Although there is no way to stop the attack unless the jamming ceases, a network administrator can easily detect this signal by measuring the incoming signal strength with a directional antenna. This practice is sometimes referred to as "fox hunting" or "transmitter hunting," and it's an exciting game among ham radio communities and RF enthusiasts[13].

Data link layer often pairs with the physical layer. Its role is to improve security and prepare data for the upper layers. Within this layer, three protocols are used:

- **Medium access control (MAC)**: Identifies different users with RNTI (Radio Network Temporary Identifier).
- **Radio link control (RLC)**: in charge of packaging the data and retransmission.
- **Packet data convergence protocol (PDCP)**: PDCP compresses and transfers data to the upper layer. It also provides authentication.

Network layer serves as a controller in the communication stack and consists of three sub-layers: the Non-Access Stratum (NAS), Radio Resource Control (RRC), and IP. Among those three, NAS handles device mobility, while RRC manages the rest.

2.4 Authentication and Encryption

LTE uses Authentication and Key Agreement (AKA), which is a challenge and response method using a symmetric key algorithm.

ESP-AKA has two variants:

- MILENAGE is a function in esp-aka.
- TUAK is the improvement of Milenage.

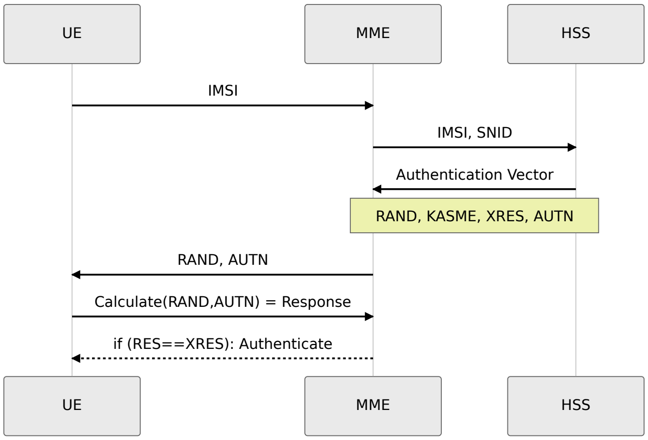

Figure 5: Authentication Flow

Below is summarize of the authentication process.

1. UE → MME: The User Equipment (UE) sends its identity (IMSI) to the serving MME.
2. MME → HSS: The MME then sends IMSI and its network identity SNID to the Home Subscriber Service (HSS).
3. HSS → MME: Using those two inputs, the HSS generates an authentication vector, which includes a random number (RAND), a local master key (KASME), an expected response (XRES), and an authentication token (AUTN).

(4) MME → UE: From the received vectors, the MME forwards only RAND and AUTN to the UE.
(5) UE → MME: After receiving the authentication token and random number, the UE calculates the response value using those.
(6) MME: Finally, the authentication is successful if the calculated response value (RES) matches with XRES in the MME.[3]

3 METHODS OF ATTACKS

After combining more than 10 research papers, the most common attack in VoLTE is Denial of Service. Besides, some interesting attacks include spoofing, location disclosing, resource exhaustion, and bypassing the charging function. All will be discussed in this paper by the order of vulnerable blocks.

During a simple call flow, SIP is used to set up a call. It carries SDP that contains codex codes, timing, and other relevant details. Once a session is established, media is transferred via RTP; however, to determine the destination, UE interacts with HSS (Home Subscriber Server) to ask for identity. During that time, it undergoes a security check using Authentication and Key Agreement (AKA) and UE is checked again when it initiates a phone call. This procedure is prone to DDoS attacks[6].

3.1 Attacks on Session Initiation Protocol (SIP)

The call session control function uses SIP to manage call flow. Since SIP is a text-based protocol, it is prone to alteration attacks if the operators don't protect it with proper authentication schemes.

3.1.1 USER.

Denial of Service (DoS) From an attacker's point of view, if we want to conduct a DoS attack on a target or operator, we will look for blocks that send repeated messages (1) or blocks that send messages and wait for a response (2). Another trick we often use on our friend's phone is trying to type the wrong password to lock the phone for hours (3). These attacks bear similarities to SIP attacks.

(1) **Amplification attack** When the UE wants to establish a call, it will send a SIP Register to the CSCF. Then, the control system will challenge the UE for authentication with a 4xx auth message. The UE accepts the challenge and sends the nonce in the 401 message to the SIM's CPU. The CPU will solve the nonce and send back authentication info via a Response message. The flow is described in the diagram below.
So, what if we don't send back a response? According to [7] and posts from Stack Overflow [1] (assuming Stack Overflow is a practical source for engineers and students), the CSCF will repeatedly send 401 Unauthorized messages to the UE, causing a denial of service on the UE. However, according to the 3GPP document, the controller stops after 70 messages due to the limit set in the max-forward field. This limitation is not mentioned in [7]. Eventually, the adversary can target any victim if the IMSI, phone number, and IP of the end-user are obtained. This attack is similar to (1) that mentioned above.
(2) **Silent call attack**

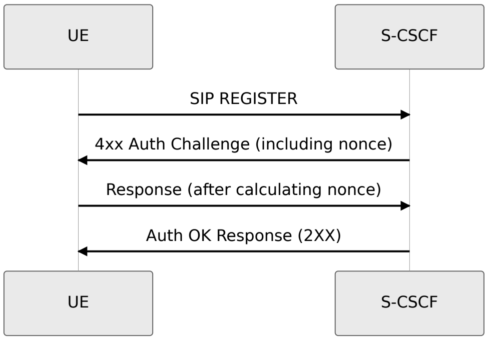
UE
S-CSCF
SIP REGISTER
4xx Auth Challenge (including nonce)
Response (after calculating nonce)
Auth OK Response (2XX)
UE
S-CSCF

Figure 6: Simple Call Flow

An adversary can perform a stealthy attack by establishing a call and then hanging up without exposing the ringtone or missed call on the target device.
The attack is carried out by sending a Cancel before the SIP UPDATE message. As a result, the target device's battery will be drained quickly since it is switched from idle to a voice call state. It would be even more intriguing if the author experiments with this method using a video call to compare the draining rate with a voice call [19].
Similar to this attack, in the paper [9], adaptive learning is used to continuously denial of service callee, making it unable to initiate a call. The exploitation is found by analyzing technical documents using Natural Language Processing.
(3) **PingPong attack** Another attack method is ping-pong. The attacker calls the target from a 2G/3G network, preventing the target from switching back to LTE. This attack limits the usage of data on the target device [19]. By making multiple calls, the attacker can also block other incoming calls to the target device.
(4) **Terminate a coming call** An attacker can send a Bye message to terminate an ongoing call when they know the IPs of both S-CSCF and the victim. However, if the terminal is equipped with caller-ID recognition, the attacker cannot send a Bye message because the caller-ID of the Bye message must correspond to the call-ID of the Invite message used for call initiation. As we know, the caller-ID is unique for each call session [12].
(5) **Mute call attack**
Different from the above attack, this exploit represents another aspect of call processing. Imagine a taxi company where SIP acts as a dispatcher, taking orders from customers, while RTP acts as the taxi driver, transporting customers from one place to another. In this case, the attacker attempts to congest the street, which is the VoLTE signaling bearer. Consequently, due to heavy traffic, RTP gets stuck; this marks the end of our very very bland analogy. In the real world, RTP runs over UDP.
To flood the bearer, we first need to find the session ID by scanning packets after the SIP BYE. This method is mentioned in [8], "V7: Side-channel Leakage by Improper Coordination." When a call is ended, the SIP BYE message is sent

to the Proxy server. From there, the Proxy server releases its voice bearer and forwards the SIP message to the Serving server. During that time, the Serving server may still be sending UDP packets while the voice bearer is closed. As a result, the stranded UDP packets will reach VoLTE's interface, and a malicious app can scan those packets to reveal the session ID.

The next puzzle is finding the RTP/RTCP ports. To do this, we can send UDP packets to various ports and compare the times. The shortest time indicates an open port for RTP/RTCP. After this step, we begin flooding the bearer with UDP. Furthermore, the paper criticizes the lack of adaptive algorithms in QoS control, as it always allocates the highest level to VoLTE which is QCI=1 (1). Moreover, the bearer is not secure enough (2). These issues (1) and (2) can lead to data usage without charge. And congratulations! We are almost reaching 6 pages. Thank you for continuing to read up to this part. Next, we will explore information leakage, impersonate attacks, and conclude this SIP section with attacks on the core network.

Information leakage

(1) **Location tracking**
The attacker can send an Invite Request and expect a 200 OK response from the target. The P-Access-Network-Info in the 200 OK messages will disclose the location information of the callee [12].

(2) **Disclosing device type**
By comparing the call response time, the attacker can identify if a device is non-IoT/IoT or a device that uses a phone number or non-phone number [20].

Impersonation attack

(1) **Voice phishing** Sometimes, repeating things can make us bored; however, it is a good way to retain long-term memory. SIP is text-based and can be edited easily. An attacker can pretend to be someone else by changing the phone number [11, 12].

(2) **Using victim credits for call services** The carriers charge customers based on Invite, Update, and Bye messages. If an attacker uses the victim's info to make a call, the victim may be charged for that usage [12].

3.1.2 OPERATORS.

Denial of Service (DoS)

(1) **Resource exhaustion on IMS** Proxy-CSCF is the first contact point in LTE, responsible for transmitting SIP messages from the terminal to the IMS block. It also filters out malformed SIP messages. If there is an enormous load on the P-CSCF, the system may not be able to provide service as expected [12].

Information leakage

(1) **Disclosing IMS network equipment IP** Thankfully, paper [12] is quite useful as it covers most of the SIP attacks. Whenever we send a SIP Register, the network may send back a 200 OK response. The S-CSCF IP address is attached to that message for routing purposes. An attacker can use that IP address as a starting point to scan or guess other components in the IMS network.

3.2 Attacking on Gprs Tunneling Protocol (GTP)

Please don't be surprised; we still use GTP in LTE and 5G. Attacks on GTP are quite interesting, but many of them are not related to VoLTE, so we'll go over it quickly.

3.2.1 USER.

Denial of Service (DoS)

(1) **Dos with Create Session** Before sending data, the user sends a Create Session message to the P-GW, requesting resources for building a tunnel. An attacker can send a Create Session message with the target's TEID to the core network. As a result, the P-GW will allocate resources for the attacker, causing the target to not receive any services from the network [11].

3.2.2 OPERATORS.

Denial of Service (DoS)

(1) **GTP Fuzzing** Similar to an attack on a user, an attacker can use a random TEID to send a Create Session message. If the P-GW detects faults in subscribers, their services will be halted. In an attempt to attack the core from the attackers, carriers can lose customers because P-GW disabling users' services [11].

Information leakage

(1) **Disclosing IP in GTP echo** The method of monitoring GTP is mentioned in the patent "US 8,339,972 B2". GTP echo response will carry the system IP address [11]; however, GTP request also requires the receiver's IP address. The reference in the paper [11] is not available, so our guess is that the attacker needs to build a rainbow table for the IP addresses.

3.3 Attacking on EPS-AKA and non-integrity message

3.3.1 USER.

Denial of Service (DoS)

(1) **Dos with Attach Request message**
To make things less boring, let's explore the fascinating mechanism of our mobile devices. When you turn on your phone, it first searches for cell towers or eNodeBs nearby. Similar to Wi-Fi, a list of cells and signal strength is recorded. To determine which cell to camp on, the device will compare the results with the correct cell ID in its USIM. After that, both the device and the cell tower will exchange configuration information and their capabilities in MIB and SIB messages. Now, we are in the Network layer.
To connect to the internet or use voice call services, UE needs to be authorized by the network. This is when the Attach Request message is used. In Figure 5, at the first step, when UE first boots up, it will send the IMSI to the MME. This is usually a plaintext message. For an active attack, the adversary can craft a new Attach Request message that breaks the security context. So, UE has to send IMSI to MME

again. This presents a potential **information leakage** [5]; however, to avoid repeating info, we incorporate it here. Also in Cheng [5], although Invite, and cancel messages are encrypted with IPsec, they can be decrypted easily with available tools.

Finally, an attacker can use that IMSI to initiate an Attach Request, which causes the real request from the victim to be halted [4, 16].

Man in the middle attack (MITM)

(1) **Fake base station** can obtain Auth and Rand from the network and then ask the target to solve them. Finally, it forwards the target's correct response to the network to impersonate the target.

(2) **Eavesdropping LTE Call** This attack exploits the reuse keystream mechanism of VoLTE. Rupprecht et al [15] use a sniffer to catch downlink messages. After a call is completed, the attacker initiates a new call to reuse the current keystream and other settings on DBR3. After obtaining the keystream, it is XOR-ed with cyphertext to decrypt the message. The root cause of this issue is due to the unencrypted RTP traffic. To fix this we can request Encrypting RTP is not optional in the specification and address the issue in the next release.

3.3.2 *OPERATORS.*

Denial of Service (DoS)

(1) **Exhausting resources** In Figure 5, after forwarding IMSI and SNID, the MME will hold a buffer while waiting for the HSS to provide RAND and AUTH. With a large number of requests, the service will slow down.

3.4 Attacking on CSFB (circuit-switch fallback)

3.4.1 *USER.*

Impersonation attack

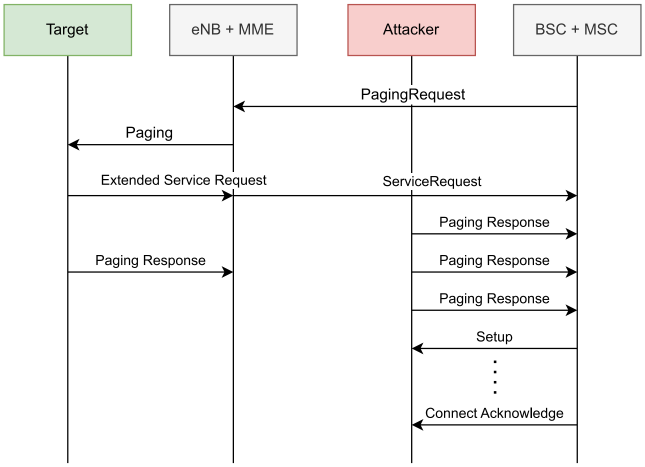

Figure 7: Paging LTE connected device from 2G/3G network

(1) **Impersonate callees** When a 3G caller establishes a call, the agent of the 3G caller, MSC, will send a paging request to the LTE agent, MME. When the UE receives a notification from the MME, it will send back a confirmation message (Extended service request). Subsequently, it will receive an RRC Connection Released message from the eNodeB with information to fall back to 3G or 2G. After that, the UE needs to send back a paging response to the MSC [21].

Attackers will take advantage of the unauthenticated Paging Response message to impersonate the target user. If the setup procedure is successful, with the Connection Acknowledge message, attackers can now receive the victim's calls and SMS [21].

As an extension of the above attack, the attacker can send a hold message to hold the link established between the caller and callee. After the caller hangs up, the attacker can use that link to originate a call.

(2) **Impersonate caller in 2G** This attack method is applied in a 2G network, where an attacker can impersonate the caller if the CSMO flag is included in the MO call [21].

3.5 Discussion

Many attacks mentioned above are based on unauthenticated or loose error-checking mechanisms. One reason for this is the security negligence in implementation. Additionally, latency can be a contributing factor. In a network with thousands to millions of users, using a more secure authentication method could significantly increase the setup time. Moreover, some of the attacks mentioned above may be considered trivial, and the associated risk might be relatively low.

As users, there are not many ways to protect ourselves from Denial of Service or other attacks. When something strange occurs, such as losing data, or a call being interrupted, our best action is to reboot the device. This action generates a new set of temporary IDs (TMSI, GUTI) and starts a registration procedure again.

Most of the fixes for these issues need to be implemented from the network side. Since most carriers operate as monopolies, it would be interesting to see if there is a group or company that rates the security and privacy of each carrier's network. This approach could create competition among carriers, motivating them to improve their network's security and privacy.

Regarding defense methods, one paper suggests using a lightweight Bayesian model [14]. When traffic on the VoLTE bearer exceeds the threshold, it will signal the network. Besides, we have seen many DoS attacks. The key to those attacks is Caller-ID. So Sheoran et al [17] proposes a mechanism to detect spoofing by implementing Caller-ID validation. In this method, a verification function is added to the IMS block and PGW (PDN-GW) which controls packets from the network to the Internet; it can be found in Figure 3. From IMS to PGW, the function will verify Caller-ID in the Invite message. And in PGW, the function will create, store or delete the Caller-ID. Although the result is decent, 95% successful rate for 0 spoof calls, the average CPU usage is 3.5 times higher than normal. There is still room for improvement.

4 CONCLUSION

There is a need to address current issues in VoLTE through a survey paper. Firstly, to build a better understanding and foundation for future communication systems. Secondly, to detect and analyze any ongoing attacks. And lastly, to resolve any privacy and security issues concerning VoLTE users.

REFERENCES

[1] [n. d.]. How to stop Asterisk from repeating "SIP/2.0 401 Unauthorized" messages — stackoverflow.com. https://stackoverflow.com/questions/36976879/how-to-stop-asterisk-from-repeating-sip-2-0-401-unauthorized-messages. [Accessed 29-07-2023].

[2] 2017. *Global System for Mobile Communications (GSM)*. John Wiley & Sons, Ltd, Chapter 1, 1–70. https://doi.org/10.1002/9781119346913.ch1 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119346913.ch1

[3] Mourad Abdeljebbar and Rachid El Kouch. 2018. Security Improvements of EPS-AKA Protocol. *Int. J. Netw. Secur.* 20 (2018), 636–644. https://api.semanticscholar.org/CorpusID:21706027

[4] Yi Chen, Yepeng Yao, XiaoFeng Wang, Dandan Xu, Chang Yue, Xiaozhong Liu, Kai Chen, Haixu Tang, and Baoxu Liu. 2021. Bookworm Game: Automatic Discovery of LTE Vulnerabilities Through Documentation Analysis. In *2021 IEEE Symposium on Security and Privacy (SP)*. 1197–1214. https://doi.org/10.1109/SP40001.2021.00104

[5] Zishuai Cheng, Mihai Ordean, Flavio D. Garcia, Baojiang Cui, and Dominik Rys. 2023. Watching your call: Breaking VoLTE Privacy in LTE/5G Networks. arXiv:2301.02487 [cs.CR]

[6] James Henrydoss and Terry Boult. 2014. Critical security review and study of DDoS attacks on LTE mobile network. In *2014 IEEE Asia Pacific Conference on Wireless and Mobile*. 194–200. https://doi.org/10.1109/APWiMob.2014.6920286

[7] Eunhye Ko, Seongmin Park, Sekwon Kim, Kyungho Son, and Hwankuk Kim. 2016. SIP amplification attack analysis and detection in VoLTE service network. In *2016 International Conference on Information Networking (ICOIN)*. 334–336. https://doi.org/10.1109/ICOIN.2016.7427126

[8] Chi-Yu Li, Guan-Hua Tu, Chunyi Peng, Zengwen Yuan, Yuanjie Li, Songwu Lu, and Xinbing Wang. 2015. Insecurity of Voice Solution VoLTE in LTE Mobile Networks. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (Denver, Colorado, USA) *(CCS '15)*. Association for Computing Machinery, New York, NY, USA, 316–327. https://doi.org/10.1145/2810103.2813618

[9] Yu-Han Lu, Chi-Yu Li, Yao-Yu Li, Sandy Hsin-Yu Hsiao, Tian Xie, Guan-Hua Tu, and Wei-Xun Chen. 2020. Ghost Calls from Operational 4G Call Systems: IMS Vulnerability, Call DoS Attack, and Countermeasure. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking* (London, United Kingdom) *(MobiCom '20)*. Association for Computing Machinery, New York, NY, USA, Article 8, 14 pages. https://doi.org/10.1145/3372224.3380885

[10] Silvère Mavoungou, Georges Kaddoum, Mostafa Taha, and Georges Matar. 2016. Survey on Threats and Attacks on Mobile Networks. *IEEE Access* 4 (2016), 4543–4572. https://doi.org/10.1109/ACCESS.2016.2601009

[11] Seongmin Park, Sekwon Kim, Joohyung Oh, Myoungsun Noh, and Chaetae Im. 2014. Threats and Countermeasures on a 4G Mobile Network. In *2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*. 538–541. https://doi.org/10.1109/IMIS.2014.79

[12] Seongmin Park, Sekwon Kim, Kyungho Son, and Hwankuk Kim. 2015. Security Threats and Countermeasure Frame Using a Session Control Mechanism on VoLTE. In *2015 10th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA)*. 532–537. https://doi.org/10.1109/BWCCA.2015.11

[13] Kevin J. Richardson, Harley J. Fernandez, Kirsten R. Basinet, Andrew G. Klein, and Richard K. Martin. 2018. A making and gaming approach to learning about RF path loss and antenna design. In *2018 IEEE Integrated STEM Education Conference (ISEC)*. 247–253. https://doi.org/10.1109/ISECon.2018.8340494

[14] Na Ruan, Qi Hu, Lei Gao, Haojin Zhu, Qingshui Xue, Weijia Jia, and Jingyu Cui. 2016. A Traffic Based Lightweight Attack Detection Scheme for VoLTE. In *2016 IEEE Global Communications Conference (GLOBECOM)*. 1–6. https://doi.org/10.1109/GLOCOM.2016.7841555

[15] David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper. 2020. Call Me Maybe: Eavesdropping Encrypted LTE Calls with REVOLTE. In *Proceedings of the 29th USENIX Conference on Security Symposium (SEC'20)*. USENIX Association, USA, Article 5, 16 pages.

[16] Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, and Jean-Pierre Seifert. 2016. Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. https://doi.org/10.14722/ndss.2016.23236

[17] Amit Sheoran, Sonia Fahmy, Chunyi Peng, and Navin Modi. 2019. Nascent: Tackling Caller-ID Spoofing in 4G Networks via Efficient Network-Assisted Validation. In *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*. 676–684. https://doi.org/10.1109/INFOCOM.2019.8737567

[18] Mika Ståhlberg. 2000. Radio Jamming Attacks Against Two Popular Mobile Networks. https://api.semanticscholar.org/CorpusID:9885139

[19] Guan-Hua Tu, Chi-Yu Li, Chunyi Peng, and Songwu Lu. 2015. How voice call technology poses security threats in 4G LTE networks. In *2015 IEEE Conference on Communications and Network Security (CNS)*. 442–450. https://doi.org/10.1109/CNS.2015.7346856

[20] Sihan Wang, Guan-Hua Tu, Xinyu Lei, Tian Xie, Chi-Yu Li, Po-Yi Chou, Fucheng Hsieh, Yiwen Hu, Li Xiao, and Chunyi Peng. 2021. Insecurity of Operational Cellular IoT Service: New Vulnerabilities, Attacks, and Countermeasures. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking* (New Orleans, Louisiana) *(MobiCom '21)*. Association for Computing Machinery, New York, NY, USA, 437–450. https://doi.org/10.1145/3447993.3483239

[21] Yuwei Zheng, Lin Huang, Haoqi Shan, Jun Li, Qing Yang, and Wenyuan Xu. 2017. Ghost telephonist impersonates you: Vulnerability in 4G LTE CS fallback. In *2017 IEEE Conference on Communications and Network Security (CNS)*. 1–9. https://doi.org/10.1109/CNS.2017.8228629