International Journal of Applied Research 2016; 2(12): 431-435

ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 5.2
IJAR 2016; 2(12): 431-435
www.allresearchjournal.com
Received: 01-10-2016
Accepted: 02-11-2016

U Sinthuja
MSc. M. Phil, Assistant Professor AJK College of Arts & Science Coimbatore, Tamil Nadu, India

A Meena
MSc. M. Phil Assistant Professor AJK College of Arts & Science Coimbatore, Tamil Nadu, India

Correspondence
U Sinthuja
MSc. M. Phil, Assistant Professor AJK College Of Arts & Science Coimbatore, Tamil Nadu, India

Status of VoLTE attacks, security issues & challenges

U Sinthuja and A Meena

Abstract
Unlike previous 3GPP wireless technologies, LTE has no circuit-switched bearer to support voice, This has led to operators leveraging the existing 2G/3G networks with VoLTE methods like Circuit Switched Fallback (CSFB) and Voice over LTE via Generic Access (VoLGA) Until this migration occurs, LTE-capable handsets need to revert to 2G or 3G for voice calls: an approach that is not ideal in the long term. In this work, examines on VoLTE security and several vulnerabilities in both its control-plane and data plane functions and challenges.

Keywords: Long term evolution, VoLTE attack, voice over LTE via generic access

1. Introduction
Introduction of LTE, CSFB and VoLGA were discussed below.

1.1 LTE
Voice is a simple utility service, yet vital to both mobile operators and phone users. It has been a killer application to mobile networks for decades. As the infrastructure upgrades to Long Term Evolution (LTE), the fourth-generation (4G) mobile technology, voice service is also going through its fast evolution. This solution to the 4G network is called VoLTE (Voice over LTE).
Multimedia applications are driving data usage in the cellular networks. Long Term Evolution (LTE) and its true fourth generation manifestation, Long Term Evolution-Advanced (LTE-A), are technologies that operators are deploying, or planning to deploy, to help them tide over this evolutionary trend. Having evolved from Universal Mobile Telecommunications System (UMTS), the specifications are known as the evolved UMTS Terrestrial Radio Access network (E-UTRAN). The first version of LTE was released by 3GPP as release 8. With LTE a move has been made towards a complete IP network consisting of the Evolved Packet Core (EPC), the Radio Access Network (RAN) and the interconnection. The main goal of LTE is to provide a high data rate, low latency and packet optimized radio access technology supporting flexible bandwidth deployments. OFDM, used in downstream, allows simultaneous access by a number of users, MIMO, improves reception by use of multiple antennas and SC-FDMA is used in the Uplink to assign radio resources to multiple users.

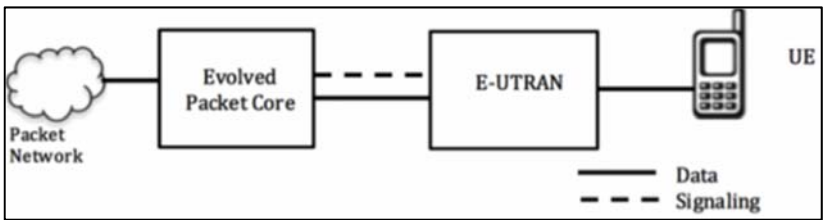

Fig 1: LTE architecture

The User Equipment (UE) includes functionalities of a Mobile Terminal (MT) that is responsible for call functions, a Terminal Equipment (TE) for data streams and Universal Subscriber Identity Module (USIM). The USIM stores network identity and user information.

The Radio Access Network (RAN) part of the LTE is called the Evolved UMTS Radio Access Network (E-UTRAN). It handles communication between the UE and the Evolved Packet Core (EPC) and consists of the base stations called eNodeBs (eNBs).
The Evolved Packet Core (EPC) or System Architecture Evolution (SAE) is the new all-IP core defined by 3GPP in Release 8.
It performs, among others, network access control, mobility management, security and network management functions. The subscriber information is stored in the Home Subscriber Server (HSS).

1.2 Circuit Switched Fallback (CSFB)

CSFB has been standardized by 3GPP for providing circuit switched voice services to UE connected to E-UTRAN by reusing GSM/UMTS infrastructure. To deploy this method, the operator should have GSM/UMTS deployment in the LTE coverage areas, or have arrangement with other operators having such deployments. When an LTE subscriber makes or receives a voice call, CSFB hands over the UE to 2G/3G network. This method favors the existing operators who have paid for the spectrum and already invested in 2G/3G infrastructure. New operators with no cellular deployment would have to make expensive arrangements with existing operators

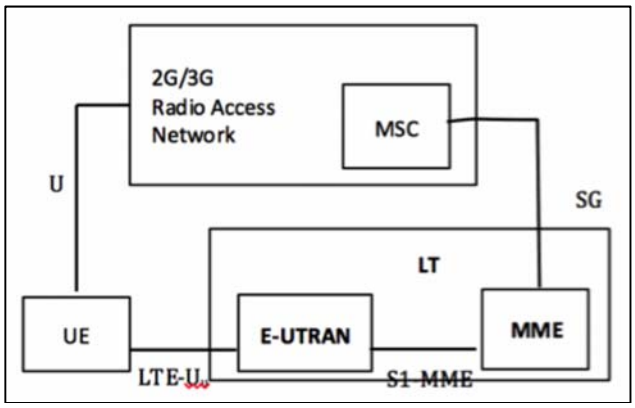

Fig 2: CSFB architecture

Both LTE and the legacy network need changes to implement CSFB. It can be seen that there are new SG interfaces between the LTE network (MME) and the MSC of 2G/3G network. These are used for mobility management and paging procedures between Enhanced Packet Service (EPS) and CS domain. Other than this, UE, MME, MSC and E-UTRAN have to support additional functionalities. The UE should support attach to the MME in LTE as well as the MSC in 2G/3G network. The MME requires additional functionality of maintaining the SGs association towards the MSC.
The MME also needs to derive the Visitor Location Registrar (VLR) number of the MSC to contact when the UE attaches to the LTE network and also maintain the tracking area lists appropriately. The legacy MSC requires maintaining the combined attached status of the UE and page the UE over SGs association when a paging request for incoming call is received for the UE in LTE.

1.2.1 Advantages of CSFB

- Ease of implementation
- The sunk cost in the legacy 2G/3G infrastructure is utilized
- CSFB sustains roaming services

1.2.2 Disadvantages of CSFB

- Due to delays associated with fallback and recovery, call set up latency is worse than the original 2G/3G networks
- 2G/3G network may not be available in all macro/micro cells of the LTE leading to patchy service
- Operators who do not have legacy deployment cannot implement CSFB
- When switching over to CS voice connection, all LTE data sessions will be dropped

1.3 Voice over LTE via Generic Access (VoLGA)

VoLGA is based on the existing 3GPP Generic Access Network (GAN) standard used by cellular operators to extend coverage of cellular with Wi-Fi offload. GAN standard extends 3GPP coverage by allowing dual mode mobiles, which can access the 3G services over Wi-Fi. The GAN idea is to introduce a gateway between Wifi and 3GPP network, which transfers the signaling between the terminal and the 3GPP et work. The purpose of GAN is to extend mobile services over a generic IP access network. With VoLGA operators can integrate LTE stepwise, using 2G or 3G infrastructure. Moving between the two network technologies is fully transparent to the user.

1.3.1 Advantages of VoLGA

- Allows UE to access voice using CS domain and data service using LTE simultaneously
- Unlike CS fallback, the data call is not dropped on handover to CS network
- The VoLGA solution caters to other CS services like SMS
- It doesn't impact existing core network nodes like the MME, the SGSNs or the MSCs
- Emergency and other regulatory services are also supported

1.3.2 Disadvantages of VoLGA

- It has not been standardized by 3GPP
- It requires a GAN based dual mode terminal with SRVCC capability
- VANC is an additional expense. To support roaming, the visited network also needs to deploy VANCs

There are no changes to the existing LTE network, RAN or the MSCs of the legacy network. This allows rapid development even in a multi-vendor MSC environment. All circuit switched services can be used over LTE. To implement VoLGA, a gateway called VoLGA Access Network Controller (VANC) is required. The VANC securely supports the interface to the MSC of a GERAN network or Iu-CS interface to a MSC of UTRAN network and is seen as a Base Station Controller (BSC) by these networks.

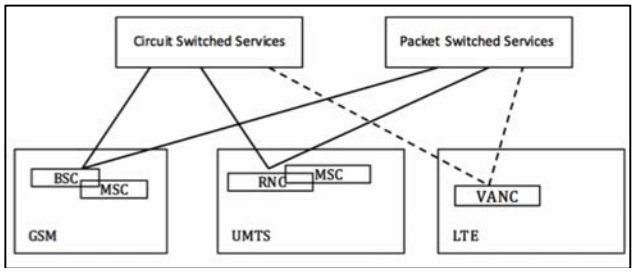

Fig 3: VoLGA architecture

The VANC has the ability to interact with the LTE network and request QoS for VoLGA voice calls. It connects to the LTE through the SGi interface, which carries both data and signaling traffic to the P-GW towards the Serving Gateway (S-GW) and hence seen as an application function by the SGW/PGW. The VANC also includes a security gateway function that terminates a secure remote access tunnel from each UE providing mutual authentication, encryption and integrity protection for signaling traffic.

2. New Security Issues

Here, review of VoLTE and then identify its potential vulnerabilities and also describe the attack model.

2.1 VoLTE Primer

VoLTE is projected as the primary voice solution to the LTE users. It migrates the legacy, circuit-switched (CS) voice service to the packet-switched (PS) design. Network architecture for VoLTE. Figure 1 depicts a simplified architecture to support VoLTE. Two subsystems are involved. The first is the PS delivery subsystem (top), which exists before VoLTE is enabled. Its role is to offer the PS connectivity to and from mobile devices, thus accommodating versatile data services.

The core component is the 4G gateway, which forwards packets, akin to edge routers in the Internet. It also provides certain control utilities such as policy enforcement and data volume billing. The second is the IP Multimedia Subsystem (IMS, bottom), which supports IP telephony and multimedia services. It consists of two key elements: the media gateway and the signaling server. The former is to deliver multimedia (*e.g.*, voice) traffic to VoLTE users or traditional telephony users. The latter is to perform call control functions among the device, the media gateway and the 4G gateway.

How VoLTE works? As illustrated in Figure 1, each VoLTE call requires two communication sessions. The control-plane session is to exchange the call signaling messages through the popular Session Initiation Protocol (SIP); it is established and remains active as long as the VoLTE feature is on. The data-plane session handles the voice packet delivery, *e.g.*, via the Internet Real-time Transport Protocol (RTP); it is established on demand by the control session. Note that no dedicated communication channel (circuit) is reserved between the caller and the callee.

Instead, all the voice traffic and signaling messages are carried in packets and delivered over IP. As a result, the 4G gateway not only relays data packets to/from the Internet for ordinary mobile broadband services, but also routes packets on both control and data planes between the device and the IMS core

2.2 Potential Vulnerabilities

Ultimately, voice and data operate in the same, connection-less

IP network. However, this paradigm shift is double-edged, exposing LTE networks and users to unanticipated vulnerabilities. In this paper, we look into three security aspects.

1. How to trick VoLTE to gain PS data access, despite its designated role for voice? Technically, this relates to the access control fences to VoLTE at the device and the network.
2. How to learn private, critical information on voice calls from VoLTE? Note that VoLTE is IP based and more open and accessible than the legacy CS call service.
3. Will the voice-related policies and operations (*e.g.*, voice billing and QoS control) work well in the VoLTE context? If not, what are the imposed threats to LTE? Our study covers three aspects of VoLTE operations: control plane, data-plane, and the coordination between control and data planes. Such security issues span the device, the 4G Gateway and the IMS core. In the following sections, we disclose how the currently employed or newly developed mechanisms fail to harden VoLTE against attacks and how they are exploited to menace data services (*§*3) and voice calls (*§*4).

2.3 Attack Model and Methodology

The presumed attacker is a mobile user, whereas the victims can be the network operator or/and other mobile users. The adversary uses a commodity smartphone rooted to gain full programmability. However, (s) he has no remote access, at least no privileged access to the victim phones. In some attacks (*i.e.*, data DoS, over billing and voice DoS), an unprivileged malware is required to monitor basic activities and information (*e.g.*, when the data transfer starts and the IP information of network interfaces) on the victim phones. The voice DoS also requires the malware to generate spam traffic. In all cases, the attacker has no control over the carrier network. The network is not compromised. To validate vulnerabilities and attacks, we conduct experiments in two top-tier US carriers denoted as OP-I and OP-II1. They together represent almost 50% of market share. Note that VoLTE functions on only a few recent models, because it requires phone hardware and software upgrades (its rollout in US started in 2014). Both rooted and unrooted ones are tested. We focus on the Android OS but we believe that the identified issues are applicable to any other OS. The results also apply to both carriers unless explicitly specified.

3. Proof-of-Concept Attacks

There three proof-of-concept attacks:

(i) free data service;

(ii) data DoS;

(iii) data overcharging.

(i) Free-data attack

Clearly, the above loopholes can be exploited to gain free external (Mobile-to-Internet) and internal (Mobile-to Mobile) data access. Note that the free external service works for only OP-I, but the free internal service is feasible for both. Take the OP-I as an example. The attacks work as follows. The adversary leverages ICMP tunneling to deliver data through the signaling bearer, since the ICMP packets

are always allowed to be forwarded by the 4G gateway to the Internet or another mobile phone.

Each data packet is encapsulated as an ICMP packet by using Raw Socket. Moreover, the routing table needs to be updated with the routing rules of designated destinations, so the ICMP packet can be sent via the signaling bearer to the destinations. These two operations can only be performed on a rooted phone. In the external case, we deploy a tunneling server out of mobile networks to run ICMP tunneling. In the internal case, the ICMP tunneling is between two VoLTE phones.

(ii) Data DoS Attack

This attack aims to shut down any on going data service at the victim by leveraging higher-priority access yielded by VoLTE-exploited data transfer. The attacker injects high rate spamming traffic through its signaling bearer, to the victim phone's signaling bearer. It can grab all the downlink bandwidth of the victim's data service, thereby causing data DoS. Note that the attacker and the victim are not charged on this spamming traffic, which is carried by the signaling bearers.

This requires an unprivileged malware on the victim device, which detects whether any data service starts, similar to the off-path TCP hijack attack. Once the victim starts any data service, this malware will send a message to an attacker server or an attack phone, leaking the IP address of the VoLTE interface. Afterwards, the attacker starts to inject high-rate spamming data to this IP. In the cases of rush-hour traffic (*e.g.*, 11am-1pm at a campus restaurant), it is observed that the data bearer throughput can be restrained to be zero, under a 10Mbps VoLTE-exploited flow.

(iii) Overcharging Attack

The attacker can make the victim suffer excessive overcharge through injecting data from its signaling bearer into the victim phone's *data-service bearer*. There is only one difference from the above DoS attack. The DoS attack spasm data toward the victim phone's *signaling bearer*.

The chosen victim is an individual phone user, targeted or randomly picked. Given the victim's IP address, we uncover this data spamming can occur without consent from the victim. The IP address can be learned from a phishing Website or an unprivileged malware. Compared with other spamming attacks this threat readily by passes the firewall and security boxes. This is because they are always deployed at the border of mobile networks to prevent malicious traffic from the Internet. However, the spamming caused by VoLTE purely relies on the internal traffic without reaching the Internet. In one run in OP-I, the overcharged volume reached 449 MB, still showing no sign of limit.

4. Challenges of VoLTE

There are many challenges of LTE. While 3GPP has standardized IMS based VoLTE for voice over LTE and SRVCC for call continuity, IMS adoption has been very slow mainly because of the cost issues. Mass deployment of IMS is nowhere in sight putting a question mark on wide adoptability of VoLTE. Among the non-IMS techniques, CSFB introduces call latency as the signaling load on HLR increases.

4.1 Technology challenges

The operators yearn for clarity on standards in supporting voice over LTE. Of the commonly used technologies, CSFB and VoLGA, only the former has been ratified by 3GPP. The operators using VoLGA face the prospect of inter-RAT incompatibility and possible hurdles in migration to GSMA VoLTE. Non-enthusiastic IMS deployment makes it difficult for VoLTE to proliferate. There are many new protocols related to IMS like IPv6, Sig Comp, IPSec and P-headers that makes matters worse. Integration of the LTE protocol stack with the IMS control layer is to be taken care of and end-to-end IMS signaling must be tested over the LTE access network.

Another issue is implementation of mobility between the packet switched LTE and the circuit switched networks. SRVCC should provide the user experience comparable with the roaming experience in the 2G/3G networks. Regulations in most countries require emergency calls to be provided. While in LTE areas with legacy networks this can continue to be provided over these networks but in LTE areas with no IMS the solution may not be trivial. While there is no easy solution, end-to-end IMS signaling over an LTE transport mechanism, addresses the challenges posed by integration of the LTE protocol stack with the IMS control layer and all its various protocols.

4.2 Implementation challenges

Standards for voice services over LTE based on 3GPP IMS architecture are still maturing. It would take time for the subscriber base on LTE to be anywhere close to 2G/3G networks. It is, therefore, expected that the operators would look for interim solutions before moving on to full-fledged IMS architecture. For operators this makes economic sense. In the interim the operators would deploy CSFB, VoLGA or even OTT solutions.

The data may be migrated sooner to the LTE because of built in efficiencies offered by LTE for data operations. New operators who have obtained spectrum from the digital dividend and do not have any legacy networks face difficult situation. If they do not wish to go for OTT solutions for the fear of customer dissatisfaction, they would have to make expensive sharing arrangements with other operators. Even the existing 2G/3G operators who do not have Generic Access Network and do not wish to commit investment in IMS would have to go for CSFB. If the operators have GAN and are prepared to invest in VANC would still have to maintain their legacy networks.

4.3 User satisfaction challenges

Performance of the network for critical real-time services needs to be tested with real-time audio and video quality measurement tools. Network impairment simulation may be carried out to test voice call quality by inserting errors in the application data stream. While moving to more advance technology like LTE, customers expect the service quality to be better than what they get today. While this may be true for data services where customers can see faster video downloads, the same cannot be said for voice services. Depending on the voice over LTE solution deployed by the operator, there may be delay in call set up and degradation in quality. The service providers would therefore face a difficult choice in the short and long term. Since IMS based VoLTE has the support of 3GPP, the operators may be forced to have a roadmap towards full IMS services. The

VoLGA forum supports GSMA VoLTE initiative, which recognizes VoLGA as the interim solution.

5. Conclusion

In this paper we deliberate upon technical details of various VoLTE technologies, their upsides and downsides and the situations in which they could be deployed. The concept of CSFB and VoLGA also defined with architecture and its pro's and con's. LTE proof –of-attack types discussed with vulnerabilities. Challenges of VoLTE have been extended with the theme of technology-wise, implementation wise and the satisfaction of the user-side.

6. References

1. Voice over LTE: Status and Migration Trends Lav Gupta, lavgupta (at) wustl.edu.
2. Insecurity of Voice Solution VoLTE in LTE Mobile Networks Chi-Yu Li∗, Guan-Hua Tu∗ University of California, Los Angeles.
3. How Voice Calls Affect Data in Operational LTE Networks. Guan-Hua Tu, Chunyi Peng, Hongyi Wang, Chi-Yu Li, Songwu Lu University of California, Los Angeles, CA 90095, USA {ghtu, chunyip, hywang, lichiyu, slu}@cs.ucla.edu.
4. [alcatel12] Voice over LTE-The New Mobile Voice, Strategic whitepaper, Alcatel Lucent, 2012.
5. [alcatel09] The LTE network Architecture, White Paper, Alcatel Lucent, 2009.
6. [anritsu13] Addressing the Challenges of VoLTE Implementation, Briefing note, Anritsu, 2013.
7. What is voice over LTE, Ericsson press backgrounder. 2014.
8. Itsuma Tanaka, Takashi Koshimizu, Overview of GSMA Voice over LTE Profile, Technology Report, NTT DOCOMO, 2012.
9. Itsuma Tanaka, Takashi Koshimizu, Overview of GSMA Voice over LTE Profile, Technology Report, NTT DOCOMO, 2012.
10. 3GPP. TS23.107: Quality of Service concept and architecture, 2014.
11. Peng C, Li C, Tu G, Lu S, Zhang L. Mobile Data Charging: New Attacks and Countermeasures. In CCS. 2012.
12. Fitchard K. Voice calls over 4G LTE networks are battery killers, 2012. http://gigaom.com/2012/11/28/volte-calls-consumer-twice-thepower-of-2g-voice-calls
13. CNET. Competitive wireless carriers take on at&t and verizon, 2012.
14. The smart VoLTE solution fast route to carrier grade voice, Whitepaper, Samsung, 2013.
15. Peng C, Li C, Tu G, Lu S, Zhang L. Mobile Data Charging: New Attacks and Countermeasures. In CCS. 2012.
16. Louvros APS, Gkioni A. Voice over LTE (VoLTE): Service Implementation and Cell Planning Perspective. In System-Level Design Methodologies for Telecommunication, Springer, 2014, 43-62.
17. Traynor P, McDaniel P, La Porta T. On Attack Causality in Internet-Connected Cellular Networks. In USENIX Security, 2007.