International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

A REVIEW ON SECURITY ISSUES & CHALLENGES OVER VOLTE NETWORK

Humma Shoket[1], Jadeep Singh Aulakh[2]

[1]M.Tech Scholar, [2]Asst. Prof. ,Electronics and Communication & Engineering Department
Amritsar College of Engineering and Technology, Amritsar

ABSTRACT

In previous 3GPP wireless technologies, LTE has no circuit-switched bearer to support voice, This has led to operators investment the present 2G/3G networks with VoLTE strategies like Circuit Switched fallback (CSFB) and voice over LTE via Generic Access (VoLGA) till this migration happens, LTE-capable handsets got to revert to 2G or 3G for voice calls: an approach that's not ideal within the long run. in this work, examines on VoLTE security and a number of other vulnerabilities in each its control-plane and data plane functions and challenges.

I. INTRODUCTION

Voice over Internet Protocol (VoIP) which is also referred to as internet telephony is a technology that transmits voice signal in real time using the internet protocol (IP) over a public internet or private data network. [3]. In a simpler term, it converts voice signal which is analog to a digital signal in your telephone before compressing and encoding it into long strings of IP packets for upward transmission over the IP network to the receiver. At the receiving end, the received IP packets reassembles in order before decompressing and processing through the use of a Digital to Analogue Converter (DAC) to generate the initial signal transmitted. [4] .Its existence is basically based on two fundamental technologies, the telephone and the internet.[5]Identified the sharing of existing infrastructures (convergence) between both data and voice application as some of the VoIP benefits in reducing implementation, management and support cost. The VOIP services in developed countries due to the existence of technologies i.e. 3G, 4G and LTE. VOIP is that the main issue in developing countries due to the absence of those technologies as many main telecommunication firms are stressing on combining their system with VOIP technologies are provided to user at least coast.so that client will get pleasure from these services [2]. VOIP services became terribly notable among medium and little organizations in the main for business method outsourcing firms and decision centers, that uses information and voice services to an excellent extent. many firms are trying to form use of infrastructure which might give the support to VOIP services in a manner such they'll have smart quality of services with lesser revenant prices . decision centers desires Quality of unsuitable infrastructure. A call center utilizes VOIP for having best economic standing however several call center needs to avoid wasting continual prices and initial investment an excessive amount of and find yourself creating terribly unsuitable selections with reference to choice of infrastructure and integration of VOIP service and PSTN . VOIP can not be pretty much as good as PSTN, however a call center ought to be sensible enough to form the correct picks to possess a higher monetary standing. Codec performance is relied on the conditions as

International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

each codec has specific desires. If the acceptable atmosphere isn't equipped the codec can have lower performance and also the result shows an excellent quantity of packet loss and interference.

Figure 1: Structure of Voice over Internet Protocol (VOIP)

The call managing service ought to maintain the amendment codec rely upon traffic and channel things, supported call destination info, with regard to a policy for choice of codec. VOIP service provider and developers of decision managing software package need data on what's an acceptable policy for choice of codec. Many little industries fail within the terribly initial year of deployment because of several reasons are [10]

1 Deficiency of information related to the entities and governing bodies in the area.

2 Unsuitable network architecture.

3 Inappropriate selection of service provider according to the requirements of the business.

4 Selection of unsuitable Codec and tools.

5 Unsuitable handling of IP pooling and Call Manager.

II VOICE OVER LTE VIA IP MULTIMEDIA SUBSYSTEM (VOLTE)

Voice practicality is equipped by the ip multimedia scheme (IMS) during this solution. IMS may be a central specification that's incorporated on high of the LTE network as portrayed in Figure two. The IMS network is primarily used to produce all the fundamental voice facilities that are equipped by the subsisting networks. It additionally facilitates improved transmission services i.e. real time gaming, video conference etc.

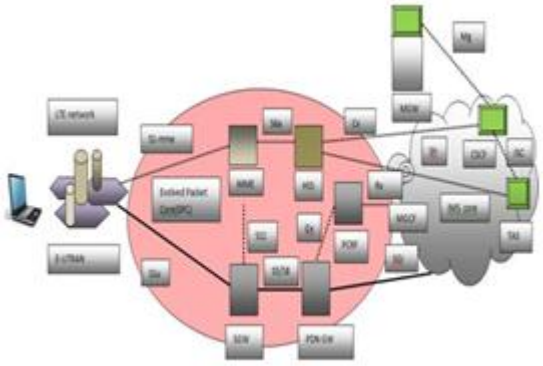


Figure 2: VoLTE

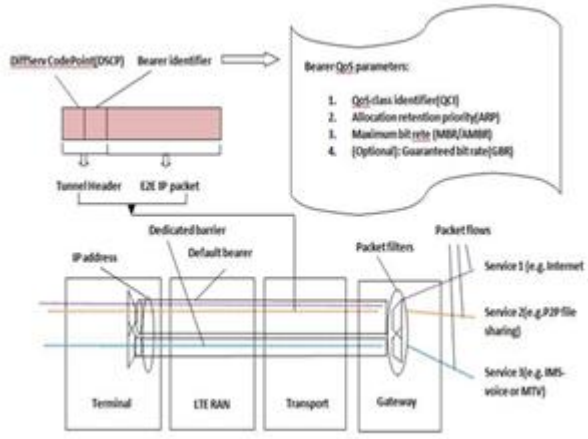
International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

The major good thing about utilizing an IMS primarily based answer is that it uses the LTE design fully rather than using the present Cs networks for providing voice service. The IMS network are often integrated with the inheritance 2G/3G networks then it will offer support to voice decision continuity even once the user moves out of LTE vary. Thus, the user will uses an equivalent facilities in roaming additionally. This resolution is being selected because the long run solution because it will offer improved options to the LTE network and additionally supports combination with the on the market 2G/3G networks.[11]

III. QOS ARCHITECTURE IN LTE

In LTE, the QoS is provided by suggests that of a bearer that unambiguously identifies the packet flow between the user and also the PDN-GW and is liable for the priority that's given to a packet flow across the LTE network. Bearers are established once the booming authentication and registration of the user within the LTE network. The LTE bearer design is shown within the Figure three. Every bearer is related to a Traffic Flow guide (TFT) that is employed to differentiate the categories of packets that flow through it. The TFT will this classification based on one of the subsequent parameters:[11]

- Port numbers
- ToS/DSCP Values
- Source/Destination address
- Protocol (TCP/UDP)



V

Figure 3: QoS Architecture in LTE

IV.NEED AND SCOPE FOR 4G TECHNOLOGIES

1. 4G Ultra high speed internet access - E-mail or general web browsing is available.
2. 4G Data intensive interactive user services - Services such as online satellite mapping will load instantly.
3. 4G Multiple User Video conferencing - subscribers can see as well as talk to more than one person.
4. 4G Location-based services - a provider sends wide spread, real time weather or traffic conditions to the computer or phone, or allows the subscriber to find and view nearby businesses or friends whilst communicating with them.
5. 4G Tele-medicines - a medical provider monitors or provides advice to the potentially isolated subscriber whilst also streaming to them related videos and guides.

6. Develop the IMT-2000 CDMA technologies to make more efficient use of the available frequency spectrum.
7. Evolve the Cellular Network Architecture to suit high levels of mobility and purely packet-switched data.
8. Allow for short-range Ad Hoc networking among wireless devices.
9. Make significant advances on the security and scalability.[8]

V. PREVIOUS WORK

Guan-Hua Tu et al. [2] [2016] has mentioned VoLTE is that the selected voice solution to the LTE network. Its early preparation is in progress worldwide. Volte offers no categorically higher quality than popular VoIP applications altogether tested situations except some engorged eventualities. Given the high value on infrastructure upgrade, VoLTE, in its current type, won't warrant the preparation effort. VOLTE, a light-weight voice solution from that all parties of users, LTE carriers, and VoIP service suppliers could profit.

Jakob Spooner et al. [4] [2016] has mentioned Software Defined Networking is a paradigm still in its emergent stages in the realm of production-scale networks. Centralization of network control introduces a new level of flexibility for network administrators and programmers. Security is a huge factor contributing to consumer resistance to implementation of SDN architecture. Without addressing the issues inherent from SDNs centralized nature, the benefits in performance and network configurative flexibility cannot be harnessed. This paper explores key threats posed to SDN environments and comparatively analyses some of the mechanisms proposed as mitigations against these threats – it also provides some insight into the future works which would enable a securer SDN architecture.

Chi-Yu Li et al. [6] [2015] has mentioned regarding VoLTE (Voice-over-LTE) is that the selected voice solution to the LTE mobile network, and its worldwide deployment is underway. It reshapes decision services from the normal circuit-switched telecom telephony to the packet-switched net VoIP. Our analysis reveals that, the issues stem from each the device and also the network. The de-vice OS and chipset fail to ban non VoLTE apps from accessing and injecting packets into VoLTE management and information planes. The network infrastructure additionally lacks correct access management and runtime check.

Raphael Horvath et al. [7] [2015] has mentioned Network technologies have continually been a vital a part of success for technologies like cloud computing. However thanks to the slow development of a scalable IT infrastructure, this will result in problems in aggressiveness. The paper reports on the most outcomes of a systematic literature review on challenges and effects of SDN. Attention is additionally given to security problems arising with package outlined networks and also the permanent high demand from the end-user combined with the concern of fixing ancient networks. problems addressing specialized ability were known as another challenge class. Effects of SDN area unit mentioned by process distinctive options of SDN like decoupling hardware from the package and also the world read of the full specification.

Gagandeep Garg et al. [9] [2014] package outlined Networking (SDN) is AN rising networking technology that separates the control-logic of data-flow from networking devices. SDN programmatically modifies the practicality and behavior of network devices using single high level program. It separates management plane and information plane, also provides centralized management. SDN provides many advantages together with,

network and repair customizability, improved operations and higher performance. however there area unit some security problems that require to be taken care of. This paper describes the emergence of SDN as a crucial new networking technology. the most focus is to explore Security problems associated with SDN. Also, the paper reviews and evaluates the salient options of SDN.

V. NEW SECURITY ISSUES IN VOLTE

The likely attacker could be a mobile user, whereas the victims may be the network operator or/and alternative mobile users. The user uses a commodity smartphone rooted to realize full programmability. However, (s) he has no remote access, a minimum of no privileged access to the victim phones. In some attacks (i.e., data DoS, over charge and voice DoS), an unprivileged malware is needed to watch basic activities and information (e.g., once data} transfer starts and also the science information of network interfaces) on the victim phones. The voice DoS additionally needs the malware to get spam traffic. altogether cases, the attacker has no management over the carrier network. The network isn't compromised. To validate vulnerabilities and attacks, we have a tendency to conduct experiments in 2 top-tier us carriers denoted as OP-I and OP-II1. They along represent nearly 500th of market share. Note that VoLTE functions on solely many recent models, as a result of it needs phone hardware and software upgrades (its rollout in us started in 2014). each frozen and unrooted ones area unit tested. we have a tendency to specialise in the robot OS however we have a tendency to believe that the known problems area unit applicable to the other OS. The results additionally apply to each carriers unless expressly specified [12]

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 is exploited to achieve free external (Mobile-to- Internet) and internal (Mobile-to Mobile) information access. Note that the free external service works for less than OP-I, however the free internal service is possible for each. Take the OP-I as an example. The attacks work as follows. The resister leverages ICMP tunneling to deliver information through the signal bearer, since the ICMP packets are forever allowed to be forwarded by the 4G entrance to the net or another mobile phone. Each information packet is encapsulated as an ICMP packet by exploitation Raw Socket. Moreover, the routing table must be updated with the routing rules of selected destinations, that the ICMP packet is sent via the signal bearer to the destinations. These 2 operations will solely be performed on a rooted phone. within the external case, we have a tendency to deploy a tunneling server out of mobile networks to run ICMP tunneling. within the internal case, the ICMP tunneling is between 2 VoLTE phones.[12]

ii)Data Dos Attack

This attack aims to finish off any on going data service at the victim by investing higher-priority access yielded by VoLTE-exploited information transfer. The attacker injects high rate spamming traffic through its

communication bearer, to the victim phone's communication bearer. It will grab all the downlink bandwidth of the victim's information service, thereby causing information DoS. Note that the attacker and also the victim don't seem to be charged on this spamming traffic, that is carried by the communication.[12] This requires an unprivileged malware on the victim device, that detects whether or not any data service starts, just like the off-path transmission control protocol hijack attack. Once the victim starts any data service, this malware can send a message to an attacker server or an attack phone, leaky the ip address of the VoLTE interface. Afterwards, the attacker starts to inject high-rate spamming information to the current scientific discipline. within the cases of rush-hour traffic (e.g., 11am-1pm at a campus restaurant), it's determined that the info bearer throughput are often restrained to be zero, underneath a 10Mbps VoLTE-exploited flow[12]

iii) data overcharging.

.The attacker will create the victim suffer excessive overcharge through injecting data from its sign bearer into the victim phone's data-service bearer. there's solely one distinction from the higher than DoS attack. The DoS attack spasm data toward the victim phone's sign bearer.

The chosen victim is an individual phone user, targeted or randomly picked. Given the victim's ip address, we have a tendency to uncover this data spamming will occur while not consent from the victim. The ip address is learned from a phishing web site or an unprivileged malware. Compared with different spamming attacks this threat pronto by passes the firewall and security boxes. this is often as a result of they're always deployed at the border of mobile networks to stop malicious traffic from the net. However, the spamming caused by VoLTE strictly depends on the interior traffic while not reaching the net. In one run in OP-I, the overcharged volume reached 449 MB, still showing no sign of limit.[12]

VI. CONCLUSION

In this paper we tend to deliberate upon technical details of varied VoLTE technologies, their upsides and drawbacks and also the things during which they might be deployed. The conception of CSFB and volga also outlined with design and its pro's and con's. LTE proof –of-attack varieties mentioned with vulnerabilities. Challenges of VoLTE are extended with the theme of technology-wise, implementation wise and also the satisfaction of the user-side.

REFERENCES

[1] Daeyoung Hyun∗, Jinyoug Kim†, Jaehoon (Paul) Jeong" SDN-Based Network Security Functions for VoIP and VoLTE Services" conference ©2016 IEEE 978-1-5090-1325-8/

[2] Guan-Hua Tu , Chi-Yu Li, Chunyi Peng, Zengwen Yuan, Yuanjie Li, Xiaohu Zhao and Songwu Lu, "VoLTE*: A Lightweight Voice Solution to 4G LTE Networks", Department of Computer Science, ISBN 978-1-4503-4145-5/16/02,2016.

[3]. Anita Singh and Dr. Deepti Sharma, "A Review on Voice over Internet Protocol (VOIP) over LTE Networks", International Journal of Science, Engineering and Technology Research (IJSETR) Volume 5, ISSN: 2278 – 7798, 2016, pp.1527-1531.

[4]. Jakob Spoone and Dr Shao Ying Zhu, "A Review of Solutions for SDN-Exclusive Security Issues", International Journal of Advanced Computer Science and Applications, vol. 7 , 2016, pp. 113-122.

[5] Jinyong Kim, Mahdi Daghmehchi Firoozjaei, Jaehoon (Paul) Jeong, Hyoungshick Kim, and Jung-Soo Park, "SDN-based Security Services using Interface to Network Security Functions", Electronics and Telecommunications Research Institute, Republic of Korea, ISBN :978-1-4673-7116-2, 2015, pp.526-529

[6]. Chi-Yu Li, Guan-Hua Tu, Chunyi Peng, Zengwen Yuan, Yuanjie Li, Songwu Lu and Xinbing Wang, "Insecurity of Voice Solution VoLTE in LTE Mobile Networks", Denver, Colorado, USA, ISBN: 978-1-4503-3832-5/15/10,2015.

[7] Raphael Horvatha, Dietmar Nedbala and Mark Stieningera, "A Literature Review on Challenges and Effects of Software Defined Networking", 2015 , pp.552-561.

[8] Rakesh kumar singh, Ranjan singh "4G cellular technology network architecture and mobile standard, International Journal of Emerging Research in Management And Technology ISSN: 2278-9359 (Volume-5, Issue-12**)**,2016

[9]. Gagandeep Garg, Roopali Garg, "Review On Architecture & Security Issues of SDN", International Journal of Innovative Research in Computerand Communication Engineering, vol.2, ISBN : 2320-9798, 2014, pp.6519-6524.

[10] Dutta, C. and Singh, R. Sustainable IPv4 to IPv6 Transition. International Journal of Advanced Research in Computer Science and Software Engineering, 2012, 2 (10): pp. 298-305.

[11] Anita Singh[1], Dr. Deepti Sharma[2], International Journal of Science, Engineering and Technology Research (IJSETR) Volume 5, Issue 5, May 2016 pp. 1527-1531.

[12] U Sinthuja, A Meena Status of VoLTE attacks, security issues & challenges International Journal of Applied Research 2016; 2(12): pp 431-435