International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 03 | March - 2023 Impact Factor: 7.185 ISSN: 2582-3930

An Investigative Approach to identify Loop Hole and Data Leak vulnerabilities in a World's Largest Greenfield VoLTE Mobile Network Operator JIO through Network Packet Dissection and Penetration

Saravanan. S
Paging911@gmail.com

ABSTRACT

Apply Digital forensic technique to diagnose the cyber security threat to the Advanced IP based Mobile telephony Networks. Indian Telecom Market having a huge subscriber base. The Market adapts the new technology Long Term Evolution (LTE), VoLTE, IP Multimedia Subsystem. Hacking the Mobile Network is a major threat to the telecom ecosystem impacts the subscribers and operator seriously. The paper illustrates investigation on the strategy to Dissect and penetrate into JIO's Network to identify the loop holes and data leaks in the Network pipe. Using the loop holes, the network may subject to attacks, hijacked, data stealth. We have followed out a grey hat technique to an extent, to continue the process and explore network nodal entry gaps to access the systems and flood anonymous traffic in to the network. We may require the Network operator's permission to dig deeper, investigate further provide an authenticated report. The research and the reports of this paper is carried out by thorough understanding of user limits privileges provided by the network to a normal subscriber. It's very clear the access is open to every subscriber and not crossed the network boundary limits. The investigation results bring an alarm to telecom network and its stake holders. With recent advancements like 5G, WSN, IOT, IoE, SDN-NFV the stakeholders keep increasing and expanding brings industrial convergence. With this aspect the stakeholder's groups of telecom imbibes a huge impact across the industries and normal life. This research approach is just a sample on JIO's Network, this can be carried out on all the Networks in the Indian Market or global Market to ensure no gaps in their network security. The idea is to sniff packets in the network through user agents like Mobile phones and do a deep packet investigation along with the understanding of network interfaces and protocols. Identify the gaps in the Core networks interfaces and the entities in the Network through call flow scenarios PS Mobile originating/ Terminating call and SMS tracing. The paper describes the initial phase of Dissecting and penetrating the Network. By having the operators Permission, we may drill down deeper investigation in this approach and analyses the crucial impacts, damage and Collateral damages to their Network.

KEYWORDS

Cyber Security, Digital Forensic, Mobile Network security, Network Penetration, Packet sniffing, Deep Packet Inspection.

1 RESEARCH METHODOLOGY

The Research Methodology followed in this project is as follows.
The communication channels are broadly classified in to two types a, Signalling Channel and b, Media Channel. According to the 3GPP, IETF standards All the authentication procedures happens over signalling channel and the network allows the subscriber to use the network for transferring user plane data/media over media channel. Dissection and Penetration into the network via Media channel is simpler rather than considering Signalling Channel. The Methodology followed here in the project is illustrated below. Hacking the Core Network Interfaces is difficult. Hence, we have taken the media channel gap available in the communication link and explore further media channel of the JIO Network using Sniffing mechanism, packet tracing, Deep packet inspection and used other open source Tools. we have discovered the Loops holes to attack the Nodes of the Reliance JIO Network. General Idea is till the LTE the tunnel gets established followed by the PGW which discovers and communicates the P-CSCF for the VoLTE Services. Capturing any SIP protocol messages may be a suspicious message travelled to the IMS CORE from the LTE/EPS Network. Capturing those SIP messages may lead to explore and investigate further loop holes about the network

2. TOOLS REQUIRED

The tools required for the paper is as follows. The test bed diagram is illustrated in

- User Equipment-OBI Mobile phone with Android OS 4G phone
- Sim cards with JIO Network Access
- tpacketcapture android App installed on UE
- Wireshark, calosoft apps for sniffing in Laptop
- https://www.iplocation.net
- NMAP scanner

3 TEST BED:

The Test bed contains the Mobile phone with the JIO SIM Card, Enable tethering on a laptop.

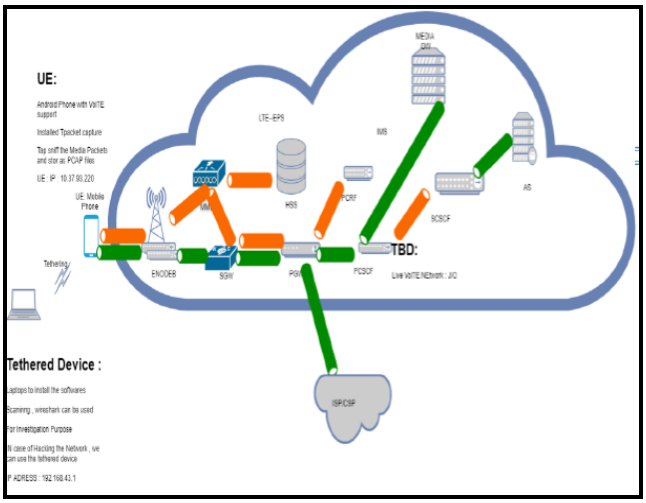

Figure 1. Test Bed - Architecture

4 NETWORK TAPS:

User Agent is the TAP. In this experimental approach, the Network tapping has been achieved by sniffing packets in the user agent, A VoLTE mobile phone. Here the signaling channel and the authentication procedures can be bypassed by having the appropriate sim cards.

Sniffing the packets in the Mobile Phones and the observing the Network call flow scenarios, where the Nodes can be identified and spotted through the digital Forensic investigation like DPI and IP scanning.

5 RESERCH ANALYSIS:

DNS Queries and Responses can be analyzed. Through the DNS packets captured in the user agent. From analysis, captured the Key Network Entity IP address are 49.44.74.134 and 49.44.65.86 and Jio DNS Server's IP address is 10.45.0.1

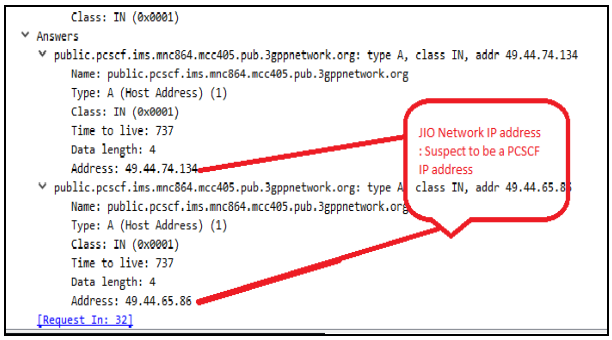

Figure 2: DNS-Packet Analysis

5.1 SIP PACKET ANALYSIS:

Analyzing above suspicious IP address from the DNS packets confirms transports SIP where it belongs to the IMS/VoLTE Network's P-CSCF Node.

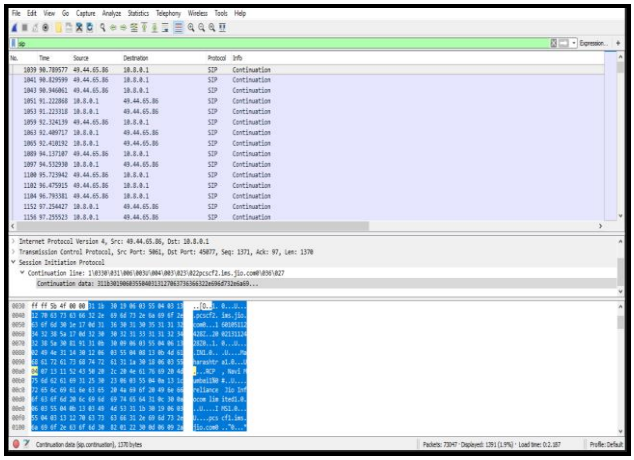

Figure 3: SIP- Packet Analysis

5.2 IP LOCATION -FINDER TEST

To get Confirmed about the location, using the IP address location finder websites the IP address has been tested to find the location and we found results as expected, which belongs to the JIO Network placed in Mumbai region, India

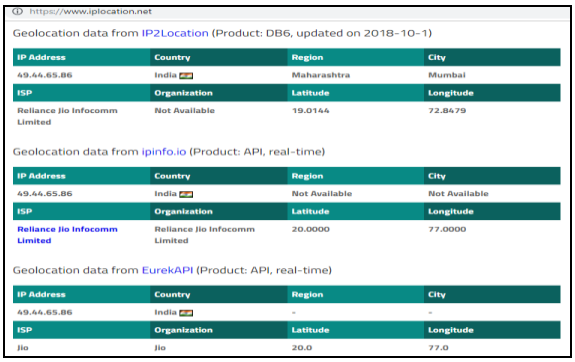

Figure 4: IP-Location Finder Test

5.3 IP-SCANNING TEST:

IP scanning has been carried out in the user agent on Suspected ip address and the complete JIO sub net ip address.

We have Identified the IP address of the JIO networks like CSCF IP address. The Complete Scan results to investigative a next lead. The nodes with IP address start in172 * are the MME and ENODEB Entities.

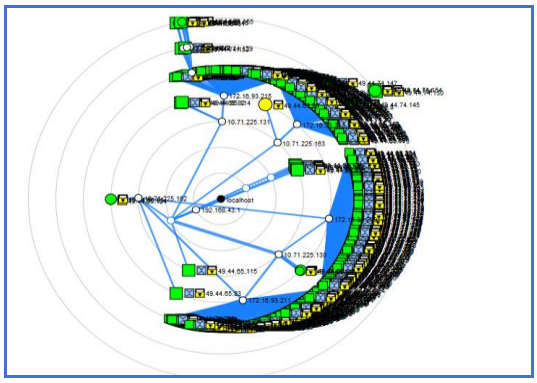

Figure 5: IP Scanning Test

6.Conclusion and Future Works:

The Network Dissection Approach helps to Dissect, penetrate a live mobile network to diagnose the nodal element address and behavior in the network. We diffused and identified the key nodes like Call Session Controlling Function servers (P-CSCF), DNS Servers . The work helps to identify the Key nodes and the other leads to the Secondary nodes like MME, ENODE-B of the network.

Based on the collected information and research results may help to hijacking the Networks, intrude into the network. Further by identifying the nodes like HSS (Home subscriber server) from identify the ports and the Ip address of the diameter traffic helps the hacker to completely hack the subscriber base information from the network. In Similar fashion the threat extents to Billing, Revenue Assurance, all the OSS/BSS, VAS Nodes of the Network.

The research was experimented by bounded to certain limits where subscribers can use the network. To go beyond this and identify the more loop holes and vulnerabilities like Identify the Entire Node of the network, inject Malicious traffic in to the network will give more Guidance to the Network Operators service providers and OEMS. Using the same approach, the mobile phones in the market also be evaluated for security standards through the packet dissection.

At the end the security standards and preventive measures to be taken on the protocol level in the network to avoid such loop holes and vulnerabilities in the network.

REFERENCES

1. GSMA: FCM0.1: VoLTE Service Description and Implementation Guidelines Version 1.1
2. 3GPP TS 23.002 version 12.5.0 Release 1: Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Network architecture
3. 3GPP TS: 33.828 IP Multimedia Subsystem (IMS) media plane security.
4. 3GPP TS 33.401: 3GPP System Architecture Evolution (SAE); Security architecture.
5. 3GPP 33.501: Security architecture and procedures for 5G System
6. https://www.wireshark.org/docs/
7. https://www.colasoft.com/company/case_study.php