International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

http://ijpsat.ijsht-journals.org
Vol. 9 No. 2 July 2018, pp. 266-271

The VoIP Security Analysis and Tools in uLaw and GSM Protocol

IGN Mantra
Informatics Engineering
Perbanas Institute, Indonesia

Teguh Prasetyo Mulyo
Informatics Engineering,
Pancasila University, Indonesia

Abstract – **Web-based software development The VoIP technology allows users to be able to communicate on the Internet Protocol (IP) network with each other more efficiently, but VoIP technology has a weakness in information security. Security of the intended information is the security of user conversations that can be recorded by irresponsible parties. The Aspect of integrity, VoIP security system can be seen from the side of users, the original sound quality of voice conversation. The aspect availability, sound is not lost when transmitted or shipping and the aspect of confidentiality, voice must be secured either encrypted or disguised, so it is not known with certainty what sounds and who is talking. This paper is testing and analysis the VoIP, secure or nosecure and sound quality on the open source platform. One of any methods that can be used is using VPN, the security method VPN is to create tunneling or create a special path between users of the service with the server, to ensure the data sent by the user to the destination without any intruders that take or change the data conversation and encryption at the time of sending data as well as decrypting on data recipient. There are not many communication protocols used in Indonesia, the selection of uLaw and GSM as research objects because GSM has become the main protocol used, while ulaw as a comparison other than GSM. These two protocols can be obtained the conclusion that GSM and uLaw as an address secure tools in the implementation of VoIP security in Indonesia telecommunication.**

Keywords – **VoIP Security; Data Security; Sound Quality; VPN, uLaw; GSM.**

I. INTRODUCTION

The development of technology Voice over Internet Protocol (VoIP) is currently growing rapidly. This is supported by the use of network technology that can be connected with various types of data, whether in the form of text, sound, and video or various applications that can be used freely. The core of VoIP technology utilization is the Internet Protocol Private Branch Exchange (IP PBX) that can centrally manage communications between users.

The current development of VoIP, making IP PBX services today more diverse, ranging from paid IP PBX services developed by enterprise application providers, or IP PBX services based on open-source. One of the most widely used IP PBX software is Asterisk. The main problem that will happen to VoIP is the security and quality of service. One example of threats to VoIP is that anyone on the network can record or manipulate data communications made by the user if done without going through the process of encryption.

II. THE RESEARCH PROBLEMS

1. How To secure the talk on Asterisk services?
2. Is the OpenVPN can secure Asterisk services?
3. How is the Asterisk's quality of service when passing tunneling and encryption on OpenVPN.
4. How to select of VoIP tools in protocol communication ?

III. RESEARCH OBJECTIVES

1. To know and testing the quality of VoIP services and security when using the encryption and tunneling techniques available on OpenVPN.

Corresponding Author: IGN Mantra

2. To analyze changes in the performance of VoIP services before and after using OpenVPN services using delay, jitter and packet loss parameters.
3. To test the security of services on VoIP systems.
4. To select of VoIP tools in protocol communication.

IV. LIMITATIONS OF THE PROBLEM

1. The quality of VoIP services and security at the moment.
2. The using an asterisk as a telephone exchange.
3. The codec used and analyzed uLaw and GSM.
4. The protocol used is SIP.
5. Tunneling and encryption using the OpenVPN service found on Linksys LRT214.
6. The parameters used during use delay, jitter, and packet loss are tested on wireshark software.

V. RESEARCH METHODS

Experimental research can be defined as a systematic method for building relationships that contain causal phenomena. Experimental research is a core method of research model that uses a quantitative approach. In the experimental research method, the researcher must perform three requirements: controlling activities, manipulating activities, and observation. In the experimental research method, the researcher divides the object or subjects under study into 2 groups ie treatment group that get treatment and control group that did not get treatment.

The steps :

1. Analysis, At this stage, two types of analysis are analyzed, ie problem and needs analysis.
2. Design, At this stage is done designing the network architecture and services used in this study.
3. Implementation, At this stage is the installation and configuration of software and hardware.
4. Testing, At this stage will be tested on the network and system.

VI. DISCUSSIONS

Based on the previous discussion that has been described, then made the modeling system before implementation and testing done. Modeling is needed to know the planning and design of quality service testing process against Passive Eavesdropping and Message Flooding attacks. Compared using the parameters that have been determined based on the provisions of the international telecommunications regulatory body ITU.

VII. THE FRAMEWORK MODEL

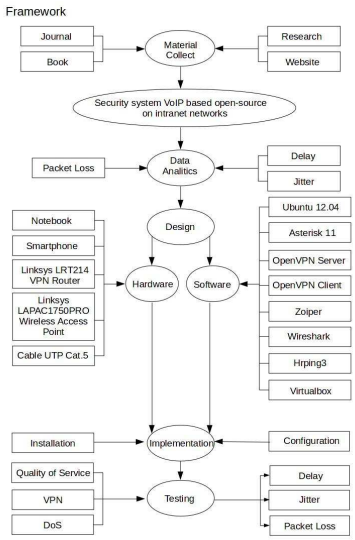

Fig. 1. Frame Model of Security VOIP system

Tests conducted to facilitate an explanation of how the communication process occurs in VoIP with attention to parameters jitter, delay, and packet lost. The purpose of the test is to know the potentials that can be tailored to the needs of development, planning, and test documents using scenarios to make observations as well as detect the impact of the actions taken.

In this test will be considered the quality of VoIP service at the time and has not been through the process of encryption, and how the condition of VoIP service when exposed and not exposed to passive attacks eavesdropping and massage flooding. In this test there are 5 nodes consisting of 1 notebook installed virtual machine, 1 wireless access point, 1 vpn router, and 2 workstations. Modeling the system is needed, kakrena can facilitate the process in describing the testing process undertaken, the following is the flow of testing performed.

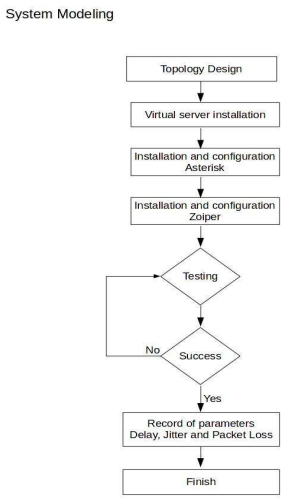

Fig.2. System Modeling

A. Network Topology Modeling

In topology network modeling, topology star used with router as the concentrator of each network connected to the network. Star topology is chosen because it is easier to develop and if there are constraints on one node on the network, does not affect the performance of the network or other nodes connected to the network.

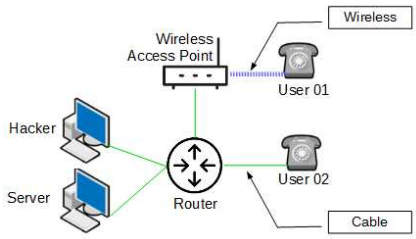

Fig.3. Network Topology

B. Testing Scenario

In this test scenario like the one made in Figure 3.1 with one VoIP server, one router, one wireless access point, two workstations and one attacker. The creation of this test scenario aims to provide an explanation and knowledge of the tests conducted and run in the current study.

In addition, this test is expected to produce data that can be analyzed from each scenario, the data include delay, jitter and packet loss. The test scenario consists of four conditions, among others:

1. Scenario 1

In scenario one run VoIP testing with one user condition and user two doing communication relationship using uLaw and GSM codec with no encryption and no DoS attacks, which are done alternately 30x with 30 second call duration.

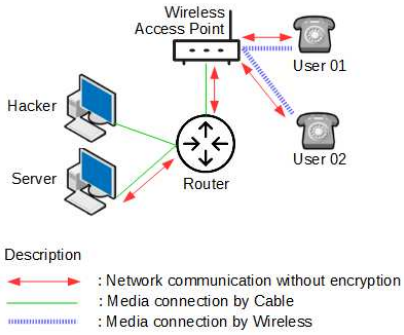

Fig. 4. Testing Scenario 1

2. Scenario 2

In the second scenario, a VoIP test with one user and two user conditions performs a communication relationship using the uLaw and GSM codecs on the encrypted communication path using OpenVPN and without any DoS attacks, which are performed alternately 30x with a 30 second call duration.

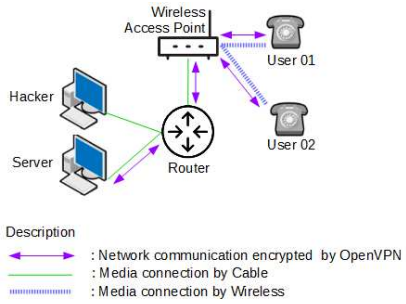

Fig.5. Testing Scenario 2

3. Scenario 3

In the third scenario, VoIP testing with one user and two user conditions performs a communication relationship using the uLaw and GSM codecs on the unencrypted communication path and there is a DoS attack towards the VoP service on the server which is performed alternately 30x with a 30 second call duration.

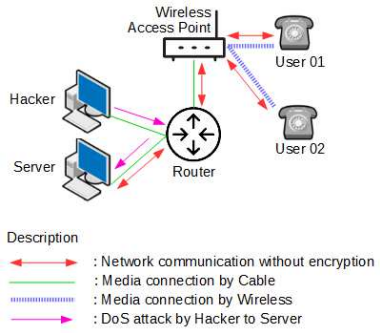

Fig.6. Testing Scenario 3

4. Scenario 4

In the fourth scenario, a VoIP test with one user and two user conditions performs a communication relationship using the uLaw and GSM codecs on the encrypted communication path using OpenVPN and there is a DoS attack toward the VoIP service on the server that is performed alternately 30x with a duration of 30 seconds call

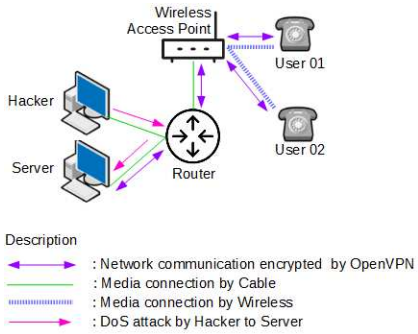

Fig.7. Testing Scenario 4

C. Implementation and Results

1. Make a Call

Based on the previous discussion in chapter 3, on the installation and configuration of zoiper on android, installation and configuration of asterisk. So in this section will be implemented from the process of calling the user extension 102 of user 101 using zoiper on android, where extensions 101 and 102 have been registered on the asterisk system. Here's a look at when extension 101 calls to extensions 102 and 102 receives calls from extension 101.

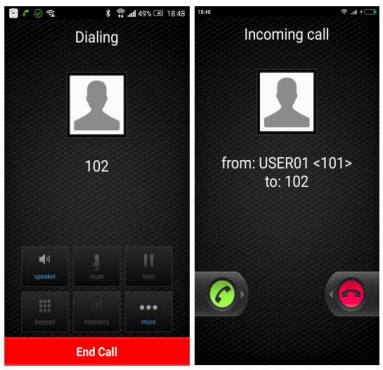

Fig.8. 101 success to call 102

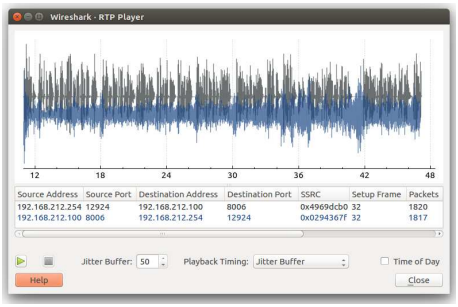

Fig.9. Playback on codec G.711

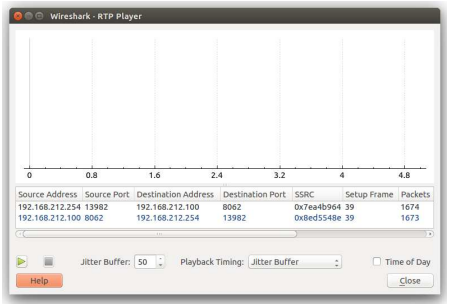

Fig. 10. Playback on codec GSM

Table.1. Data test result of Scenario 1, No Encrypted and DoS attacks –uLaw.

No Encrypted and DoS attacks – uLaw						
Number	Forward			Reserved		
	Delay (ms)	Jitter (ms)	Packet Loss(%)	Delay (ms)	Jitter (ms)	Packet Loss(%)
1	23.01	0.14	0	34.86	0.23	0
2	22.87	0.13	0	23.42	1.08	0
3	24.07	0.23	0	33.98	11.68	0
4	23.85	0.16	0	40.53	11.65	0
5	23.61	0.2	0	34.06	11.96	0
6	24.08	0.18	0	36.39	11.45	0
7	23.88	0.21	0	41.98	11.19	0
8	22.79	0.19	0	39.65	11.79	0
9	24.04	0.21	0	38.42	11.12	0
10	22.56	0.15	0	35.36	11.86	0
11	24.19	0.25	0	36.76	11.05	0
12	23.01	0.17	0	23.01	11.16	0
13	27.99	0.25	0	37.69	1146	0
14	24.5	0.24	0	34.71	11.23	0
15	24.14	0.25	0	41.2	11.77	0
16	26.18	0.18	0	40.27	10.97	0
17	24.11	0.72	0	34.52	11.95	0
18	25.04	0.18	0	38.86	11.73	0
19	34.47	11.33	0	22.56	0.16	0
20	23.82	0.19	0	34.86	11.64	0
21	24.07	0.23	0	33.84	11.79	0
22	24.17	0.22	0	41.92	11.54	0
23	24.28	0.2	0	34.93	11.07	0
24	23.05	0.2	0	35.27	12.14	0
25	23.73	0.21	0	40.23	11.66	0
26	24.04	0.23	0	34.14	11.58	0
27	23.71	0.24	0	34.32	11.81	0
28	24.13	0.22	0	37.77	11.32	0
29	24.07	0.2	0	33.74	11.37	0
30	23.19	0.2	0	41.74	11.73	0
Median	**24.355**	**0.59033333**	**0**	**35.6996667**	**48.256**	**0**

Table.2. Data test result of Scenario 1, No Encrypted and DoS attacks – GSM

No Encrypted and DoS attacks – GSM						
Number	Forward			Reserved		
	Delay (ms)	Jitter (ms)	Packet Loss(%)	Delay (ms)	Jitter (ms)	Packet Loss(%)
1	23.51	0.19	0	34.79	11.76	0
2	22.99	0.15	0	36.36	9.16	0
3	23.92	0.15	0	35.53	11.89	0
4	27.71	0.19	0	34.4	11.69	0
5	23.02	0.21	0	42.06	11.08	0
6	23.22	0.22	0	34.73	11.69	0
7	24.05	0.2	0	34.22	11.18	0
8	25.28	0.22	0	34.58	11.47	0
9	24.19	0.21	0	33.87	11.4	0
10	23.54	0.17	0	34.89	11.23	0
11	23.46	0.17	0	39.64	11.48	0
12	23.67	0.18	0	33.75	12.2	0
13	24.15	0.22	0	33.8	11.85	0
14	23.1	0.19	0	35.45	11.52	0
15	23.82	0.17	0	35.84	11.61	0
16	23.95	0.21	0	35.84	11.41	0
17	23.65	0.21	0	40.94	10.97	0
18	23.5	0.17	0	34.45	11.44	0
19	23.14	0.16	0	40.76	11.24	0
20	24.29	0.19	0	40.66	12.13	0
21	25.89	0.21	0	44.6	11.81	0
22	24.16	0.19	0	39.54	10.93	0
23	24.82	0.21	0	36.38	11.58	0
24	24	0.18	0	39.12	11.02	0
25	25.43	0.17	0	33.98	11.95	0
26	23.98	0.21	0	34.97	11.18	0
27	22.55	0.16	0	36.53	10.32	0
28	24.73	0.21	0	34.1	12.19	0
29	23.92	0.23	0	34.63	11.48	0
30	24.16	0.21	0	34.41	10.79	0
Median	**24.06**	**0.192**	**0**	**36.494**	**11.3883333**	**0**

2. Scenario 2 and Result

In a second test scenario where the server and user are encrypted using OpenVPN, it is not possible to capture the data condition. Jitter, Delay and Packet loss are not captured by wireshark either on the uLaw codec or GSM codecs, can only be captured by OpenVPN headers as they pass through the network. But communication between users with the server still running.

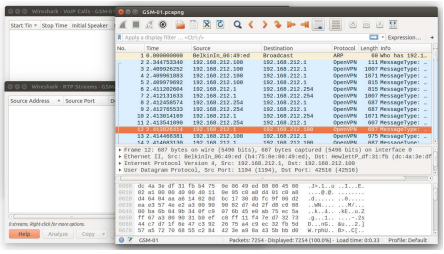

Fig.11. OpenVPN Transmissions.

3. Scenario 3 and Result

In the third scenario experiment with unencrypted conditions and there was a DoS attack on the server, it was found that the server condition could not respond and the VoIP service was not working at all. Therefore, parameter data delay, jitter and packet loss can not be captured by wireshark.

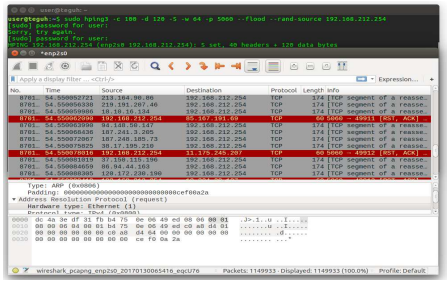

Fig.12. UnEcrypted conditions and DoS Attacks on Server

4. Scenario 4 and Result

In testing the four user scenarios and the server is in an encrypted condition using OpenVPN and getting a DoS attack from hping3. Conditions on DoS attacks without encryption again found server conditions can not respond and instantly VoIP service does not work. OpenVPN can protect VoIP services from passive eavesdropping but can not protect services from DoS attacks.

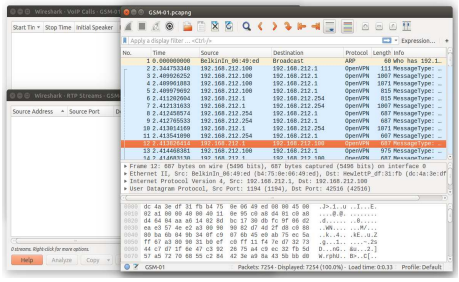

Fig.13. Communication condition with Open VPN

VIII. Conclusion

1. The Quality of service between uLaw and GSM codec, although uLaw codec has 64 kbps rate while GSM codec only 12 kbps. Both services are not significantly different based on test data as follows.

Table 3. Testing Result with *codec uLaw*

Codec uLaw			
Traffic	Delay	Jitter	Packet Loss
Forward	24.35ms	0.59ms	0
Reverse	35.69ms	48.25ms	0

Table 4. Testing Result with *codec GSM*

Codec GSM			
Traffic	Delay	Jitter	Packet Loss
Forward	24.06ms	0.19	0
Reverse	36.49	11.38	0

2. The Scenario 1 is the best testing result, because from the testing scenario 2, 3 and 4, the sound quality and various things about voip encrypted testing do not get satisfactory result or zero result.
3. The OpenVPN can not protect VoIP services from DoS attacks, but it protects VoIP services from passive eavesdropping attacks.
4. The selection of the best tools from the results of research testing above is the utilization of uLaw and GSM protocol as the implementation of voip security in Indonesia telecommunication

REFERENCES

[1] Ahmad Setiawan, Fikri.. Analisa perbandingan kualitas *VoIP* menggunakan *codec* G.711 dan GSM dengan menggunakan metode *fast handover* pada mobile IPv6 (FMIPv6). Universitas Indonesia. 2012.

[2] DC Sicker, Tom Lookabaugh, *VoIP Security : Not an afterthought*, 2004, dl.acm.org

[3] Feilner, Markus. Gaft, Norbert. *Beginning OpenVPN 2.0.9*. Packt Publishing. 2012.

[4] Hartpence, Bruce. *Packet Guide to Voice over IP*. O'REILLY. 2013.

[5] Hung, Patrick C.K, Martin, Miguel Vargas, *Security Issues in VOIP Applications*, Electrical and Computer Engineering, 2006. CCECE '06.

[6] Likhar, Praveen. Shankar, Ravi. Rao M, Keshava. *Securing IEEE 802.11g WLAN using OpenVPN and its Impact Analysis.* 2011.

[7] S McGann, DC Sicker, *An analysis of security threats and tools in SIP-based VoIP systems*, Second VoIP security workshop, 2005-startrinity.com

[8] Sugeng, Einarno. Istiyanto, Jazi Eko. Mustofa, Khabib. Ashari, Ahmad. *The Impact of QoS Changes towards Network Performance*. 2015.

[9] Uskov, Alexander. Byerly, Adam. Heinemann, Colleen. *Advance encryption standard analysis with multimedia data on intel* ® AES-NI architecture. 2016.