ZFONE SECURITY ANALYSIS OF VIDEO CALL SERVICE USING GENERAL NEWORK DESIGN PROCESS METHOD(GNDP)

Bayu Priyatna[1], April Lia Hananto[2], Rozahi Istambul[3]

Abstract---*VoIP (Voice over Internet Protocol) is one of the services implemented in wireless local area networks. However, VoIP that uses wireless technology as a media data stream Video Call service has a high risk of being tapped by sniffing attacks [2]. To avoid this from happening, you can add a security system to the service, one of which is to use Zfone security. Adding a security system will affect the work of the Video Call service on the quality of service. The author uses the General Network Design Process (GNDP) study method. After testing security by cropping images, Zfone affects the security of video calls on WLAN by turning conversations between client images black. Although Zfone managed to secure from eavesdropping on video calls, Zfone also had an impact on the deterioration of the quality of the Video Call service.*

Keywords---*VoIP, WLAN, Zfone, Network Security, Tapping Image, Quality of Service, GNDP.*

I. INTRODUCTION

To avoid this from happening, you can add a security system to the service, one of which is to use Zfone security. Adding a security system will affect the work of the Video Call service on the quality of service. The author uses the General Network Design Process (GNDP) study method. After testing security by cropping images, Zfone affects the security of video calls on WLAN by turning conversations between client images black. Although Zfone managed to secure from eavesdropping on video calls, Zfone also had an impact on the deterioration of the quality of the Video Call service [1]. One of the technologies used today is VoIP. Voice over Internet Protocol (VoIP) is a technology that allows long-distance voice conversations through internet media [2]. In addition to conducting long-distance conversations over the internet, VoIP has a service that can carry out chat messages and even make video calls.

VoIP can also be implemented on a Local Area Network (LAN) or abbreviated as VoIP LAN. VoIP LAN networks are usually implemented on cable networks and combined with Public Switch Telephone Network (PSTN) networks. The development of network technology, the existence of VoIP LAN that uses cable began to move using wireless network technology, namely wireless [8].

The use of wireless networks as a medium for the flow of data makes VoIP services can be used in several communication technology tools such as personal computers, laptops, and smartphones [3].

*[1,2] Information Systems Study Program
School of Engineering and Computer Science
Universitas Buana Perjuangan Karawang[1,2]
Widyatama University[3]
[1] Email: aprilia@ubpkarawang.ac.id
[2] Email: bayu.priyatna@ubpkarawang.ac.id*

The use of VoIP technology that is implemented on WLAN networks with video call services contained in the VoIP facility is an excellent solution in conducting conversations at an affordable cost compared to the VoIP service associated with PSTN [11].

The use of VoIP technology with video call services is very beneficial for users, but efficient communication and affordable costs in terms of security are not so considered [9]. Therefore compilation of video call services that are connected to WLAN is still very vulnerable in terms of security because this network works by spreading a lot of radio frequency signals, thus allowing parties who take access to enter the network and filter the ongoing communication [10].

This needs to be addressed because it is a very important matter concerning user privacy [5]. Based on this, what can be done is to add a security system to the WLAN network. By using Zfone software that uses the Zimmermann Real-Time Transport Protocol (ZRTP) protocol as its executor. The use of Zfone is an alternative method for security by encrypting the data traffic of a WLAN [6]. Using Zfone software, data packages must go through several security stages before being sent and arrive at their destination.

II. RESEARCH METHODS

This study uses the General Network Design Process (GNDP) method with 6 stages [12]. as follows:

1. Assess needs and costs

The initial stages of the General Network Design Process (GNDP) there are two main things as follows:

a. This stage explains what is needed by the user by doing this research. The availability elements that must be achieved in this research are video call service security and Quality of Service WLAN network system.

b. This stage is the stage for the budget required in this research both from hardware (hardware) and software (software).

2. Choosing topology and technology

This stage is the stage for the selection of topology and technology used in this research. In this study using star topology. The wireless network in this study uses infrastructure mode, presented in Figure 1.

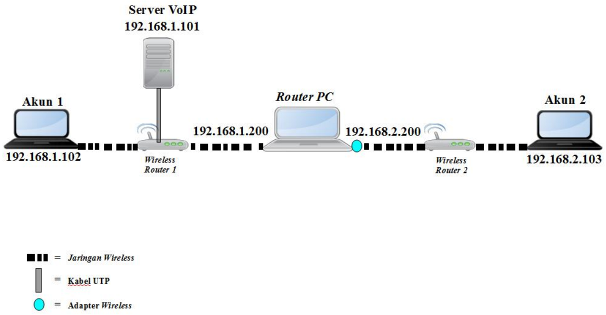


Figure 1. VoIP Network Topology
Using WLAN

1. Workload model

This stage is determined by what systems are charged to the network that has been created by researchers. In this study, two systems are charged, namely, the VoIP system using WLAN and VoIP using WLAN.

2. Simulate behavior under expected load

This stage simulates a network system that has been determined at the workload model stage. At this stage, the Quality of Service is also measured against the VoIP system using WLAN.

3. Perform a sensitivity test

At this stage, the security system is implemented on a VoIP system using WLAN testing. The security used in this system is data encryption, the authors use Zfone software. Zfone uses the ZRTP protocol to encrypt data on the transport protocol used by the VoIP system using WLAN.

4. Process design as needed

At this stage, it is the result of the analysis carried out in the previous stages. At the stage also redesigned if needed to get optimal results [4].

III. RESULTS AND DISCUSSION

1. Call flow process

PAt this stage, it is explained about the process of a video call from the beginning of the video call until the end of the video call. Following are the results of testing the call flow process on a VoIP WLAN system without security and a VoIP WLAN system with Security:

a. VoIP without security

The following are the results of the process flow of the VoIP WLAN system without security presented in Figure 2.

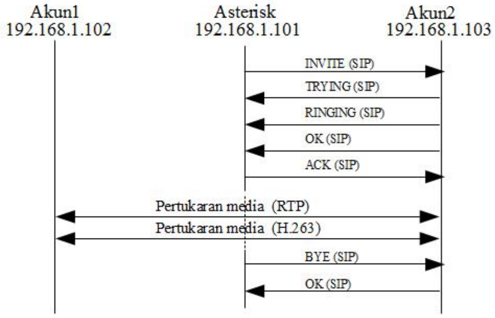


Figure 2. illustrates the process of initiating a video call flow

b. VoIP WLAN with security

Following are the results of the call flow process on the WLAN + ZRTP VoIP system presented in Figure 3.

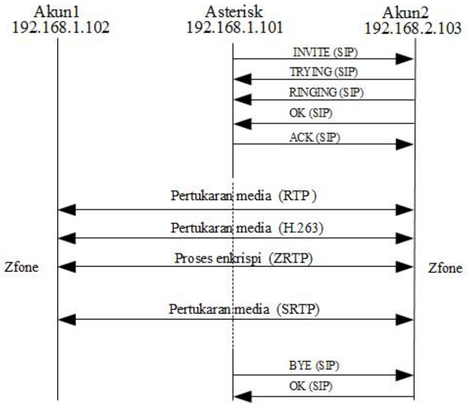


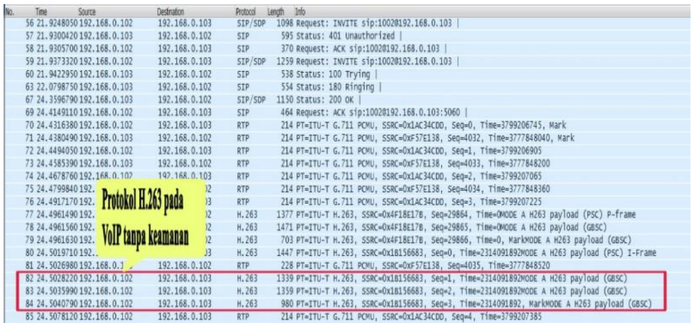
Figure 3. Illustration of the process of initiating VoIP video call flow with security

2. Type of transport protocol

Based on the type of transport protocol used by the VoIP WLAN system before and after using a security.

a. VoIP WLAN without security

Following are the results of testing the type of transport protocol for VoIP systems without WLAN security, presented in Figure 4 and the frame shape that carries the transport protocol is presented in Figure 5.



```
No.  Time      Source         Destination    Protocol Length Info
56 21.9248050 192.168.0.102  192.168.0.103  SIP/SDP  1098 Request: INVITE sip:1002@192.168.0.103 |
57 21.9300420 192.168.0.103  192.168.0.102  SIP       595 Status: 401 Unauthorized |
58 21.9305700 192.168.0.102  192.168.0.103  SIP       370 Request: ACK sip:1002@192.168.0.103 |
59 21.9373320 192.168.0.102  192.168.0.103  SIP/SDP  1259 Request: INVITE sip:1002@192.168.0.103 |
60 21.9422950 192.168.0.103  192.168.0.102  SIP       538 Status: 100 Trying |
63 22.0798750 192.168.0.103  192.168.0.102  SIP       554 Status: 180 Ringing |
67 24.3596790 192.168.0.103  192.168.0.102  SIP/SDP  1150 Status: 200 OK |
69 24.4149110 192.168.0.102  192.168.0.103  SIP       464 Request: ACK sip:1002@192.168.0.103:5060 |
70 24.4316380 192.168.0.102  192.168.0.103  RTP       214 PT=ITU-T G.711 PCMU, SSRC=0x1AC34CDD, Seq=0, Time=3799206745, Mark
71 24.4380490 192.168.0.103  192.168.0.102  RTP       214 PT=ITU-T G.711 PCMU, SSRC=0xF57E138, Seq=4032, Time=3777848040, Mark
72 24.4494050 192.168.0.102  192.168.0.103  RTP       214 PT=ITU-T G.711 PCMU, SSRC=0x1AC34CDD, Seq=1, Time=3799206905
73 24.4585390 192.168.0.103  192.168.0.102  RTP       214 PT=ITU-T G.711 PCMU, SSRC=0xF57E138, Seq=4033, Time=3777848200
74 24.4678760 192.168.0.102  192.168.0.103  RTP       214 PT=ITU-T G.711 PCMU, SSRC=0x1AC34CDD, Seq=2, Time=3799207065
75 24.4799840 192.                      2   RTP       214 PT=ITU-T G.711 PCMU, SSRC=0xF57E138, Seq=4034, Time=3777848360
76 24.4917170 192.                      3   RTP       214 PT=ITU-T G.711 PCMU, SSRC=0x1AC34CDD, Seq=3, Time=3799207225
77 24.4961490 192.                      2   H.263    1377 PT=ITU-T H.263, SSRC=0x4F18E17B, Seq=29864, Time=0MODE A H263 payload (PSC) P-frame
78 24.4961560 192.                      2   H.263    1471 PT=ITU-T H.263, SSRC=0x4F18E17B, Seq=29865, Time=0MODE A H263 payload (GBSC)
79 24.4961630 192.                      2   H.263     703 PT=ITU-T H.263, SSRC=0x4F18E17B, Seq=29866, Time=0, MarkMODE A H263 payload (GBSC)
80 24.5019710 192.                      3   H.263    1447 PT=ITU-T H.263, SSRC=0x1B156683, Seq=0, Time=2314091892MODE A H263 payload (PSC) I-Frame
81 24.5026980 192.168.0.1    192.168.0.102  RTP       228 PT=ITU-T G.711 PCMU, SSRC=0xF57E138, Seq=4035, Time=3777848520
82 24.5028220 192.168.0.102  192.168.0.103  H.263    1339 PT=ITU-T H.263, SSRC=0x1B156683, Seq=1, Time=2314091892MODE A H263 payload (GBSC)
83 24.5035990 192.168.0.102  192.168.0.103  H.263    1359 PT=ITU-T H.263, SSRC=0x1B156683, Seq=2, Time=2314091892MODE A H263 payload (GBSC)
84 24.5040790 192.168.0.102  192.168.0.103  H.263     980 PT=ITU-T H.263, SSRC=0x1B156683, Seq=3, Time=2314091892, MarkMODE A H263 payload (GBSC)
85 24.5078120 192.168.0.102  192.168.0.103  RTP       214 PT=ITU-T G.711 PCMU, SSRC=0x1AC34CDD, Seq=4, Time=3799207385
```

Figure 4 H.263 protocol on a WLAN VoIP system without security

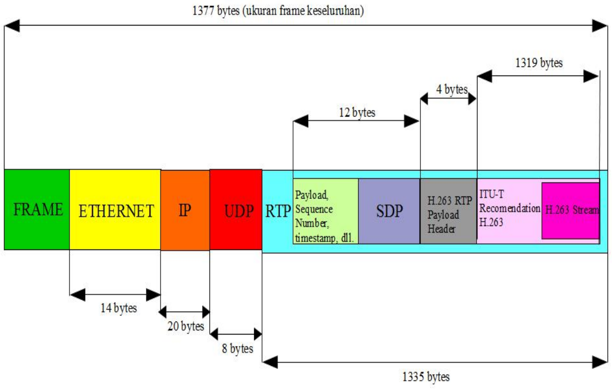
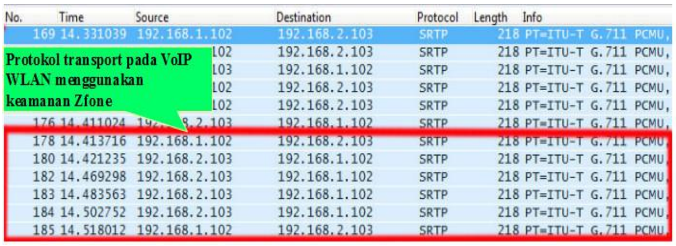


Figure 5 The frame form of VoIP transport protocol without security

b. VoIP WLAN with security

The following results of testing the type of transport protocol VoIP WLAN system with security, are presented in Figure 7 and the frame shape that carries the transport protocol is presented in Figure 8.



```
No.     Time        Source          Destination     Protocol Length Info
    169 14.331039   192.168.1.102   192.168.2.103   SRTP     218 PT=ITU-T G.711 PCMU,
                            102     192.168.2.103   SRTP     218 PT=ITU-T G.711 PCMU,
                            103     192.168.1.102   SRTP     218 PT=ITU-T G.711 PCMU,
                            102     192.168.2.103   SRTP     218 PT=ITU-T G.711 PCMU,
                            102     192.168.2.103   SRTP     218 PT=ITU-T G.711 PCMU,
    176 14.411024   192.    8.2.103 192.168.1.102   SRTP     218 PT=ITU-T G.711 PCMU,
    178 14.413716   192.168.1.102   192.168.2.103   SRTP     218 PT=ITU-T G.711 PCMU
    180 14.421235   192.168.2.103   192.168.1.102   SRTP     218 PT=ITU-T G.711 PCMU
    182 14.469298   192.168.2.103   192.168.1.102   SRTP     218 PT=ITU-T G.711 PCMU
    183 14.483563   192.168.2.103   192.168.1.102   SRTP     218 PT=ITU-T G.711 PCMU
    184 14.502752   192.168.2.103   192.168.1.102   SRTP     218 PT=ITU-T G.711 PCMU
    185 14.518012   192.168.1.102   192.168.2.103   SRTP     218 PT=ITU-T G.711 PCMU
```

Protokol transport pada VoIP WLAN menggunakan keamanan Zfone

Figure 7 Transport protocol on VoIP WLAN with security.

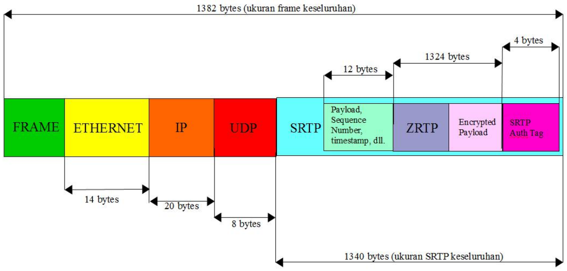

1382 bytes (ukuran frame keseluruhan)
4 bytes
1324 bytes
12 bytes
FRAME
ETHERNET
IP
UDP
SRTP
Payload, Sequence Number, timestamp, dll.
ZRTP
Encrypted Payload
SRTP Auth Tag
14 bytes
20 bytes
8 bytes
1340 bytes (ukuran SRTP keseluruhan)

Figure 8 The form of VoIP transport protocol frames with security.

3. Video tapping results

Tapping is done by stealing data packets which become transport protocols on VoIP systems using WLAN. The transport protocol carries data that contains sound and image media that are generated from conversations conducted by the client. To do this wiretapping, the author uses Wireshark and PC router as executor of wiretapping, as shown in Figure 9.

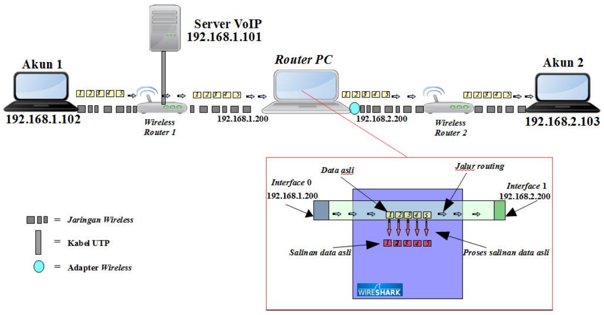


Figure 9 Illustration of the tapping process

a. VoIP WLAN without security

Following are the results of tapping video calls on a WLAN VoIP system without security, presented in Figure 10.

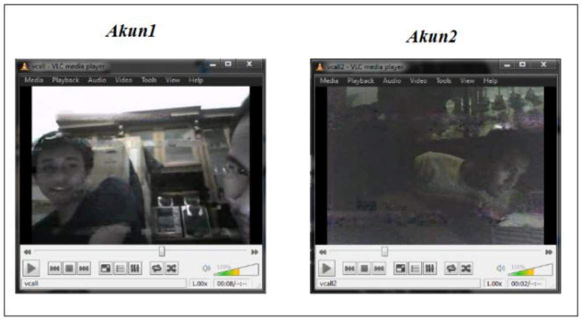


Figure 10 The results of tapping VoIP WLAN images without security

b. VoIP WLAN with SRTP

Following are the results of tapping video calls on a VoIP WLAN system with security, presented in Figure 11.

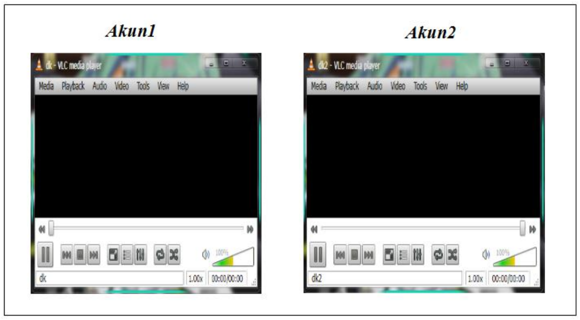


Figure 11 The results of tapping VoIP WLAN images with security

4. Quality of Service Results

Quality of Service testing is carried out five times, testing is done by making calls to account1 to account2. The parameters used are delay, jitter and packet loss. The test was carried out on a VoIP WLAN system without security and a VoIP WLAN system with security.

a. Delay

The following is the delay value in the WLAN VoIP system without security and with security, presented in table 1.

Table 1. Delay VoIP WLAN without security and VoIP WLAN with zfone security

No	Testing	VoIPWLAN	VoIPWLAN +Zfone
1	T-1	72,59	78,77
2	T-2	74,07	81,48
3	T-3	100,7	83,64
4	T-4	71,73	73,41
5	T-5	25,58	83,29
Average		**68,93**	**80,12**

b. Jitter

The following is the value of jitter on a WLAN VoIP system without security and with security, presented in table 2.

Table 2. Jitter VoIP WLAN without security and VoIP WLAN with zfone security

No	Testing	VoIPWLAN	VoIPWLAN+ Zfone
1	T-1	1,75	2,50
2	T-2	2,43	1,81
3	T-3	2,58	8,07
4	T-4	2,44	5,74
5	T-5	0,99	3,67
Average		**2,04**	**4,36**

c. Packet Loss

Following is the value of packet loss in a VoIPWLAN system without security and with security, presented in table 3.

Table 3. Packet loss of VoIP WLAN without security and VoIP WLAN with zfone security

No	Testing	VoIPWLAN	VoIPWLAN+ Zfone
1	T-1	0	0
2	T-2	0	0
3	T-3	0	0
4	T-4	0	0
5	T-5	0	0
Average		**0**	**0**

IV. CONCLUSIONS

1. The Zenfone security system has an effect on using video calls on WLAN. At the time of videotaping, the SRTP protocol turns the image of conversations between clients black.
2. The results of the quality of service before using the Zfone security system with the parameters of delay, jitter, and packet loss are as follows:

a. The value of the delay time is 68.93 ms
b. The jitter time value is 2.04ms
c. The packet loss parameter before using Zfone security is 0%

3. The results of the quality of service after using the Zfone security system with the parameters of delay, jitter, and packet loss are as follows:

a. The value of the delay time is 80.12 m s
b. The jitter time value is 4.36ms.

V. RECOMMENDATIONS

So that security is much stronger, the results of this research can be done in combination with other video encryption methods.

REFERENCES

[1] M. Mikrotik, "Ancaman keamanan jaringan pada server untuk membatasi website tertentu menggunakan mikrotik," no. 02, pp. 22–31, 2019.

[2] A. W. Rahman, M. M. Sigalingging, and M. H. Tristanto, "Network Security & Interkoneksi Jaringan Dengan L2tp + Ipsec," 1960.

[3] P. Welishe, B. Weaver, and P. Welishe, "Hantering av informationssäkerhet : en studie om arbetet i praktiken Hantering av informationssäkerhet : en studie om ar- betet i praktiken."

[4] R. J. Solihin, D. Arnaldy, and S. Syafe'i," Analisis Performansi Winconnect Pada Jaringan Pc Cloning Untuk Aplikasi Game Online," *Pseudocode*, vol. 2, no. 1, pp. 20–27, 2015.

[5] Bulgurcu, B., Cavusoglu H., & Benbasat, I., (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and information Security Awareness. MIS Quarterly.

[6] Reynolds (2016). Social Engineering: The art of psychological warfare, human hacking. Persuasion and deception Create Space Interdependent Publishing Platform.

[7] Barrie Sosinsky Networking Bible. United States : Wiley Publishing, 2009 http://www.counterpath.com/assets/files/191/XLite3.0_UserGuide.pdf.

[8] Kamaldila, IlmuKomputer.com, Model Referensi OSI. Diperoleh 5 mei 2014.

[9] Keith W. R, James F. Kurose. Computer Networking : A Top-Down Approach (Sixth Edition). United States : Pearson Education. 2013.

[10] Richard,NS Computer Software and Services P/L Ed Warnicke, Wireshark User's Guide : for Wireshark 1.11. 2013.

[11] Rudi Hartono & Agus Purnomo, S.Si, Wireless Network 802.11. D3 TI FMIPA UNS. 1/1/2011. Diperoleh 12 mei 2014.

[12] Deris Setiawan, Fundamental Internet working Development & Design Life Cycle. 2009.