ANALYSIS QUALITY OF SERVICE ON VOIP APPLICATION BASED ON MODIFIED IAX2 PROTOCOL FOR EAVESDROPPING DETECTION

Irwan Alnarus Kautsar[1, *)], Supeno Djanali[2]
1) Informatics Engineering, Information Technology Faculty,
Institute Technology of Sepuluh Nopember
irwanak@cs.its.ac.id
2) Informatics Engineering, Information Technology Faculty,
Institute Technology of Sepuluh Nopember
supeno@its.ac.id

ABSTRACT

VoIP implementation for Next Generation Network is an alternative way for communication through internet, as an audio streaming or video streaming. Another way deploy VoIP service use asterisk Server, with IAX2 protocol.

This paper analyze IAX2 protocol, IAX2 is one general protocol use in VoIP technology used for connecting with other asterisk Server and have many susceptible security issues.

This aim of this work present quality of service, possibility threats, secure mechanisms and deploying based on modified IAX2 protocol for eavesdropping detection, on OPNET Simulator.

The result show in this research, delay a packet captured in IAXServer1 and IAXServer 2 is between 0.00001 and 0,00002 sec. based on table[8], VoIP Apllication with modified miniframe is in good quality.

Keywords*: VoIP, Asterisk, IAX2.*

INTRODUCTION

By Ram Dantu et al, VoIP is third generation after PSTN and cellular phone. It possible many people build own VoIP/proxy server.

Asterisks is one open source PBX/VoIP/Proxy server and use IAX2 protocol for control and transmit streaming data or communication between Asterisk server.
In this paper will present mechanism eavesdropping detection use MAC Address from router that route the packets.

Contribution from this research is give reference mechanism for implementing IAX2 protocol with eavesdropping detection in future works.

Our paper presented as follows: Section 2 contain brief review of the possible VoIP threats, IAX2 theory, present a detailed approach of a mechanism eavesdropping detection. Section 3 overviews the result, section 4 concludes the paper and future works.

ISBN : 978-602-97491-4-4

METHODE

IAX2 Protocol

IAX2 (Inter Asterisk Exchange version 2) is native protocol in Asterisk. The advantages using IAX2 Protocol, is bypassing NAT and use only single port 4569 for transmitting media and control message.

IAX2 protocol contain two session, signaling and media flow transmission session. General IAX2 protocol signaling or call setup is shown (Figure 1).

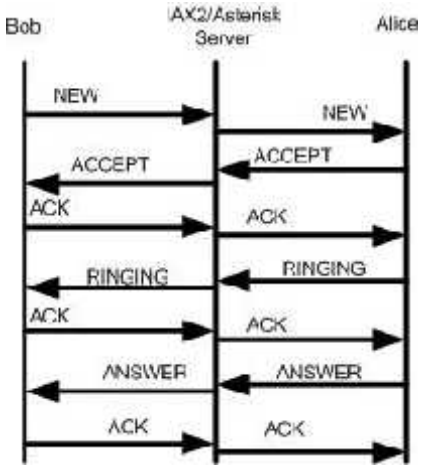


Figure 1. IAX2 Signaling/Call setup Protocol.

For media flow transmission session, is flow 4 byte header called IAX2 Mini frames (labeled M in Figure 2) and flow Full Frames periodically (F(t)) (labeled M in Figure 2) for synchronization.

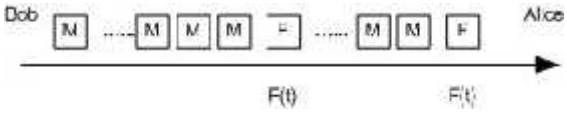


Figure 2. IAX2 Signaling/Call setup Protocol.

For frame contained in mini frame shown in Figure3.

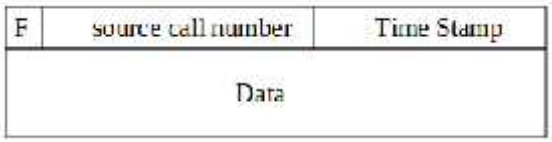
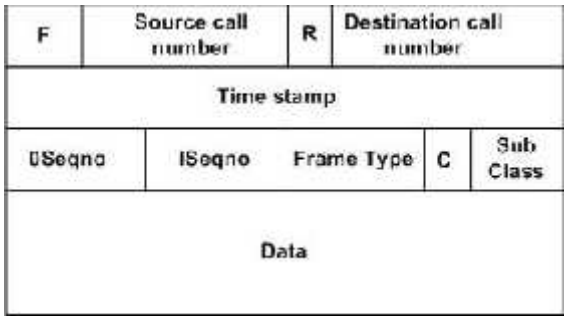


Figure3. IAX2 mini frame.

Mini frame use for media transmission, so mini frame send sequential not periodical.

ISBN : 978-602-97491-4-4

A full frame (Figure 4) is periodical in F(t)(Figure2) and contain much bit, so modified a mini frame is suitable, although signaling session is use Full frame.



IAX2 Protocol Threat

Because IAX2 protocols use single port 4569, attacker can sniff or eavesdrop packet trough that port. The eavesdropping attack clearly demonstrated by Rajagopalan[3], by using tool called Unsniff. Another threat based on[2] that related about packet modification is :

1. Denial on Service

A attacker send ACK packet to IAX Server with simultaneous, so can make IAX Server busy. The Effect is IAX Server can't establish connection.

2. VoIP Spam

A Attacker send fake personal information that need to be confirmed. The effect is user can give

The threat above can prevent and handle, if we know who's on the network, and which computer eavesdrop IAX2 packet.

Eavesdropping detection

Every packet is through port 4569, so every router is by passing in that port and by (Ram Dantu et al)[2] a proposed solution for eavesdropping is port-based MAC Address, also router communicate by MAC address, so packet can get an MAC Address a router/computer that MAC Address open port 4569. This can use additional overhead/bit header on mini frame to store key. So the new mechanism for eavesdropping detection can present in two session, signaling and media transmission.

1. Signaling Session

This session used for implementation routing protocol. By Fig, Bob send packet 1.1 for collect routing table that route packet to Alice. Alice send ACK + key for Bob to inform that packet 1.1 receive.

When packet 1.2. receive, Bob send packet 1.2 to get MAC address based on routing table from 1.1, so IAX Server send packet1.1 to completely routing table need for Bob. Packet 1.3 use to get MAC Address that packet routed.

ISBN : 978-602-97491-4-4

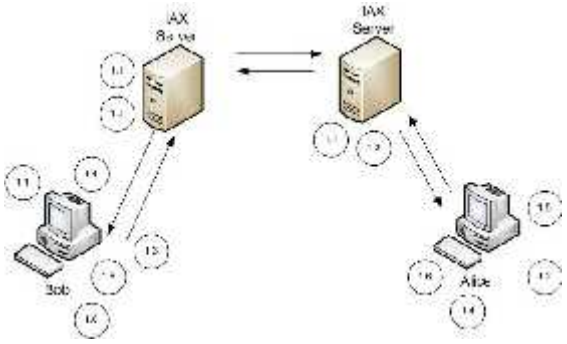


Figure 5. Signalling session by Bob, Alice and router.

The detailed mechanism of Figure 5. Signalling session by Bob, Alice and router, is show in Table1.

Table1. Tabel Activity Signalling Session

Activity ID	activityName	IAX2 Server	Bob, Alice
1.1	Get Routing Table	1	0
1.2	ACK+ key	0	1
1.3	Get MAC Address	1	0
1.4	ACK + MAC + key	1	1
1.5	Send Frame	1	1
1.6	Receive Frame	1	1

2. Media Flow Transmission Session

After routing table created, and get MAC Address, Bob and Alice know which computer is safe to send packet. The information store in bit Signaling data in modified mini frame (figure3).

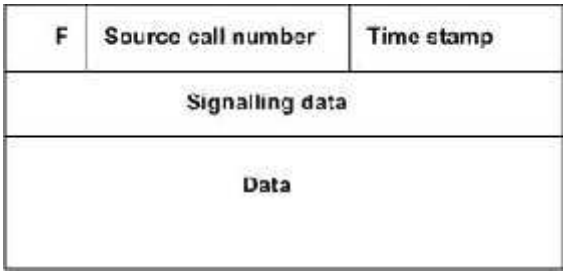


Figure 6 . Modified Miniframe

On Figure3. A Modified on mini frame contain overhead/bit header for signaling data, which store a routing table and MAC address that packet routed.

When eavesdropper try to join in. Attacker MAC Address to be listed in ARP table. IAX Server Scan open port in listed MAC Address in ARP Table, when scanned port 4569, Attacker or client send ACK and key that received in packet 1.4. IAX Server get ACK and checked granted key, if not listed in key granted table, then attacker/client suspect eavesdropping.

ISBN : 978-602-97491-4-4

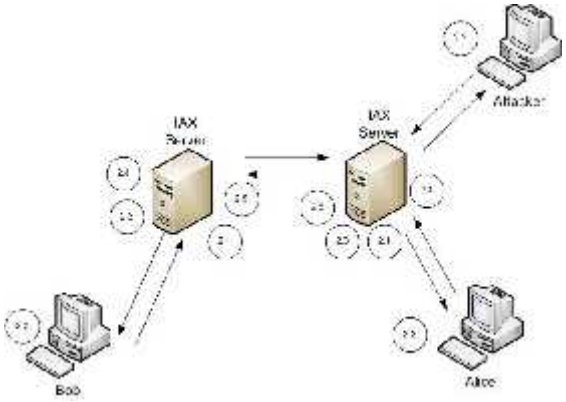


Figure7. Signaling Session by Bob, Alice, Router and Attacker.

Detailed activity and mechanism in signaling session by bob, alice, router and attacker, is shown at Table 2.

Table2. Activity Signalling Session

Activity ID	Activity Name	Bob	Attacker
2.1	Scan Open Port	1	0
2.2	Send ACK + Key	0	1
2.3	Get ACK + Key	1	0
2.4	Check Granted Key	1	0
2.5	Eavesdrop Detection	1	0

IAX2 Protocol mini frame modified for key use for eavesdropping detection to get additional information each route that packet transmitted.

By build key chain at signaling session and authenticate at media transmission session can compare and compute a state that there is eavesdropping activity or none.

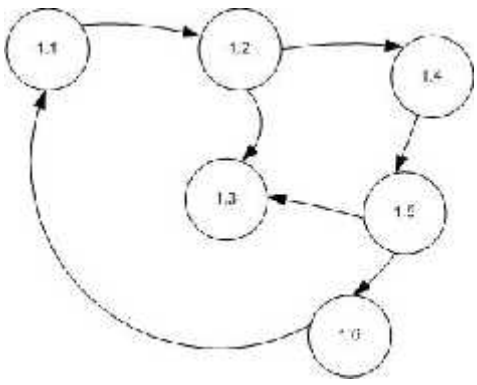


Figure 8 . Packet Activity Signalling Session

ISBN : 978-602-97491-4-4

A state for get routing table is first step must client/server in signaling session (Figure 8), and the importance is Packet 1.3 after packet 1.2 and packet 1.5 send.

State for media transmission session, a IAX Server start eavesdropping detection with packet 2.1 that scanning port. The result is IAX server directly know an active client that join to IAX Server, with key that given in previous session, IAX Server can detect a client/attacker that try to eavesdrop (Figure 9).

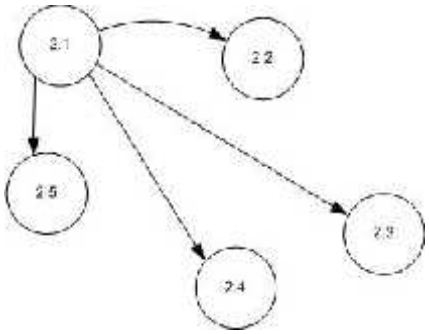


Figure 9 . Packet Activity Signalling Session

Implementation

By using OPNET Simulator a presented topology (Figure 7) shown in (Figure 10).

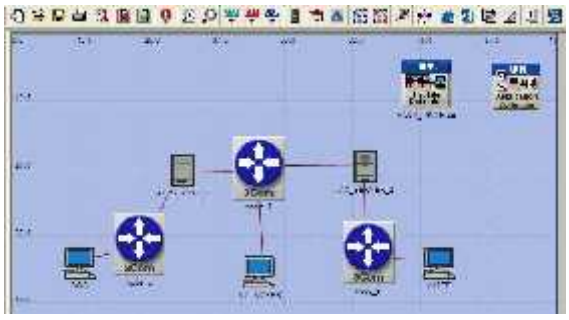


Figure 10 . Topology in OPNET Modeler.

And modified packet state in data link layer IAX2 Server, shown in Figure 11.

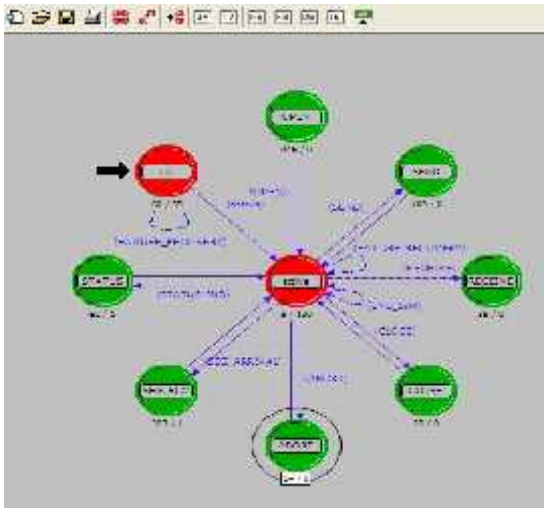


Figure 11 . Data Link Layer IAX2 Server.

ISBN : 978-602-97491-4-4

The parameter for simulation is shown Figure12.

Figure 12 . Data Link Layer IAX2 Server.

RESULT

Another parameter on VoIP service is Quality Of Service (QoS) that contain Jitter, Delay and Throughput. With a modified mini frame and full frame, can analyze that QoS after modified frame signaling and media transmission. For IAX2 Server1 and IAX2 Server2 packet jitter, delay and throughput shown in figure13 and figure14.

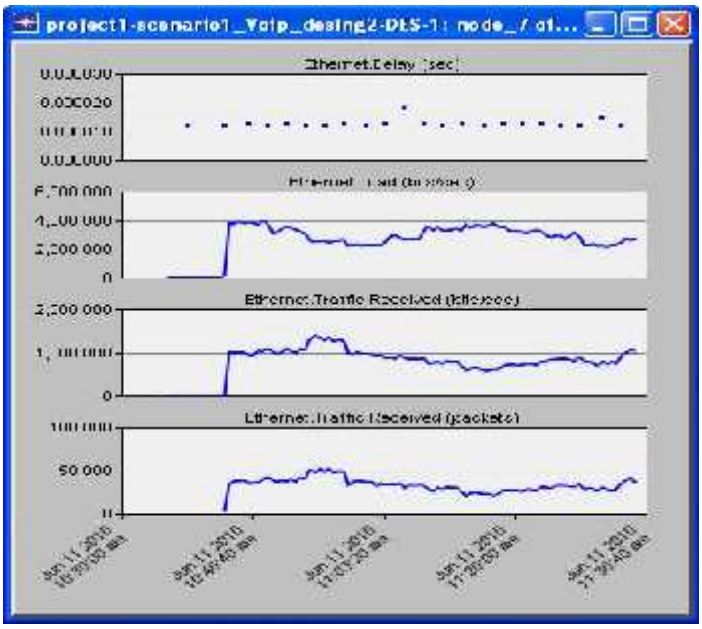


Figure13. Delay in IAX Server1

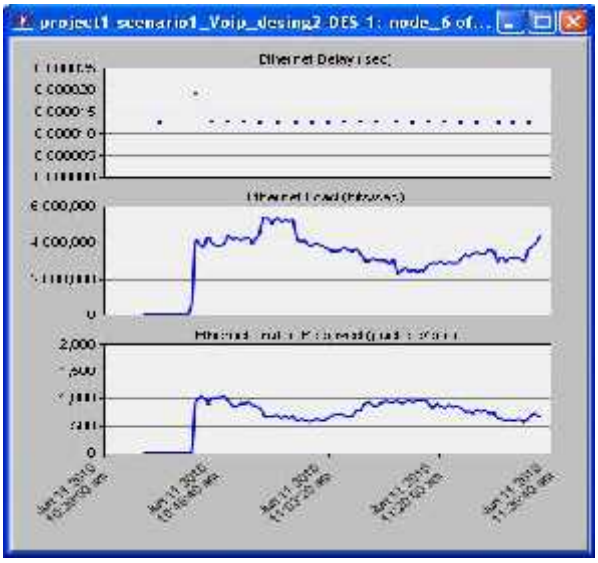


Figure14. Delay in IAX Server2

ISBN : 978-602-97491-4-4

CONCLUSION AND FUTURE WORKS

Delay a packet captured in IAXServer1 and IAXServer 2 is between 0.00001 and 0,00002 sec. based on table, VoIP Apllication with modified miniframe is good quality.

Table 4. ITU Recommendation G.114[8]

Jitter/ Delay (milisecond)	Perameter
0-150	Good
150-400	Good with Sound Transmition Warning
> 400	Poor

With MAC Address and port 4569 that used for IAX2 protocol, and possibility for transmit modified packet with IAX2 protocol, IAX Server can detect active client or attacker that try to eavesdrop. Parameter on VoIP service is Quality Of Service (QoS) that contain Jitter, Delay and Throughput.

With possibility transmit modified packet use IAX2 protocol, a scenario for implementation eavesdropping detection, with clustering intruder/attacker, data preprocessing for detecting anomaly, is available for future works.

REFERENCES

Adams B, Alden J, and Harris N (2009) Hacking VoIP - Protocols Attacks and Countermeasures. No Starch Press.

Dantu R, Fahmi S, and Taylor B, Schulzrinnec H, Joao Cangussu J,(2009) Issues and challenges in securing VoIP. Computers & Security 28 (2009) 743–753.

Rajagopalan V (2006) IAX2 Call Analyzer for Unsniff. Available at: www.unleashnetworks.com/lib/IAX2AnalyzerWhitepaper3.pdf [Accessed: May, 15th 2011].

Spencer M, Miller F.W (2004) IAX Description [Online]. Available at: www.seteurocom.ru/materials/rus/iax.pdf [Accessed: May, 20th 201].

Biermann E, Cloete E, and Venter L.M, ,(2001) A comparison of Intrusion Detection systems. Computers & Security 20 (2001) 676-683.

Kolhar M.S, Abu-Alhaj M.M., Abouabdalla O, Wan T.C, and Manasrah, A.M,(2009) A comparison of Intrusion Detection systems. (IJCSIS) International Journal of Computer Science and Information Security. Vol. 6, No. 3

M. Spencer, B. Capouch, E. Guy, Ed., F. Miller,K. Shumard,(2010) Independent Submission Request for Comments: 5456 IAX: Inter-Asterisk eXchange Version 2. ISSN: 2070-1721

http://www.cisco.com/en/US/tech/tk652/tk698/technologies_white_paper09186a00800a8993.shtml. [Accessed, June, 1st 2011].

ISBN : 978-602-97491-4-4