Multilayer Secured SIP Based VoIP Architecture

Basma Basem, Atef Z. Ghalwash, and Rowayda A. Sadek

Abstract—**VoIP faces many emerging attacks and threats. securing SIP based VoIP is a major challenging task, hence confidentiality, integrity, availability, as well as authenticity must be provided. Focusing on three main critical attacks targeting SIP based VoIP infrastructure, which are Denial of service (DoS), man-in-the middle attack, and Authenticity based attacks. In this paper the main contribution is providing a secure efficient multilayer security architecture based on open source applications (snort, snortsam and iptables, as well as OPENVPN Tunnel), The architecture provides a secure reliable VoIP services for the enterprise network, that have been deployed based on asterisk PBX. The proposed security architecture aims to prevent the mentioned critical attacks, to provide CIAA security services, by proposing an adaptive rule based queuing polices. QoS is a major challenge, the paper also provides an enhancement for the proposed architecture to minimize the delay for more efficient secure communication, as well as preventing zero day attacks by exploiting method and updating Snort DB with attack signatures. QoS factors have been measured using OPNET simulators. The proposed architecture gives promising results when it comes to attacks prevention with 0.01% better performance results compared to previous work.**

Index Terms—**VoIP, snort, OPEN VPN, firewall, iptables, OPNET 17.**

I. Introduction

Voice over Internet Protocol (VoIP) is a set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across Internet. A VoIP system is usually cheaper to operate than an equivalent office telephone system with a private branch exchange and conventional telephone service, since it uses the Internet. Moreover, VoIP takes advantage of this ubiquitous carrier technology to disseminate voice data packets to and from machines. VoIP requires signaling protocol such as SIP, H323, and MGCP, which is responsible for end user registration, thus enabling end-user to setup, disconnect and control the calls and telephony features. RTP is the carrier speech transmission, it is an IETF standard. Meanwhile, RTCP is an RTP control protocol aims to provide feedback on QoS, by sending periodic statistics information to the participants in a streaming multimedia session. VoIP software at end-user nodes is responsible for digitizing, encoding, streaming, decoding, and playing out the voice signal [1]. First, the voice signal is sampled and digitized, then encoded with one of the available codec as (G. 711, G.7231.1, and G.729). Voice signal is packetized and transmitted using RTP/UDP/IP. At the receiver end-user data is de-packetized and forwarded to a jitter buffer, which smoothes out the variation delay or jitter in the network, the voice is then reconstructed and delivered to the recipient.

SIP is an IETF specified protocol for initiating a two-way communication session. It is considered by some to be simpler than H.323 [2], [3], though it is now the largest RFC in IETF history. SIP is text based and an application level protocol that can be carried by TCP, UDP, or SCTP. UDP is mostly used to decrease the overhead and to increase the speed and efficiency.

Since VoIP uses the Internet Protocol (IP) to transfer voice data, so it inherits same threats, risks and vulnerabilities of the Internet, added to threats targeting the SIP signaling protocol [4]. SIP is a text based client-server protocol similar to the HTTP, and this text-based nature can cause weakness and arising vulnerabilities. Therefore, SIP messages open many opportunities for possible attacks such as; spoofing, hijacking, message tampering, and the use of malicious SIP messages that can cause a major impact leading to unauthorized access or Denial of Service (DoS).

The main proposed contribution in this paper lies in providing a new efficient secure integrated Multilayer Secured SIP Based VoIP Architecture. Providing defense against DoS, eavesdropping and zero day attacks. The proposed architecture covers three categories of Security techniques that have been developed based on their function

1) Security Enabling [Encryption and Authenticity]
2) Security protection [Firewall, aiming to protect from external threats]
3) Security Violation detection techniques (Such as IDS/IPS and monitoring events]

VoIP architecture Scenario aims to secure the perimeter network, internal Network, as well as user agents from external attacks and threats, while providing confidentiality for remote user agents over untrusted network, guaranteeing integrity in transit.

There are number of research efforts that tried to provide VoIP security [5], Previous work and studies have been categorized into "Single-layer security defense" vs. "Multilayer security defense", not all CIA security services was covered in previous work, main interest was DoS attacks, although eavesdropping, spoofing and hijacking attacks have a major impact as well, yet neglected. Also intrusion prevention system wasn't used, so the network was compromised to attacks and threats, delay in blocking action response rather than automated driven policy response, lacking protection against zero day attacks.

The proposed Multilayer Secured SIP Based VoIP Architecture is achieved by securing all of VoIP protocol

Manuscript received June 21, 2014; revised September 4, 2014.

Basma Basem is with the Arab Academy for Science, Technology & Maritime Transport, Computer Engineering Department, Egypt (e-mail: basmabasem@hotmail.com.com).

Atef Z. Ghalwash and Rowayda A. Sadek are with the Faculty of Computers and Information, Helwan University, Egypt (e-mail: {atef_ghalwash, rowayda_sadek}@yahoo.com).

DOI: 10.7763/IJCTE.2015.V7.1002

stack layers, providing availability, confidentiality and authenticity for media and signaling. Moreover proposed an enhanced queuing mechanisms, implemented in a rule based policies, providing a better QoS and a minimum delay. The proposed rule based Queuing mechanism also prevents flooding attacks, many researchers shown that effect of flood based DoS attack can be reduced if system has a good queuing mechanism. The proposed architecture has been implemented in virtualization environment, performance result analysis was measure by OPNET simulation tool, indicating performance analysis while deploying different types of VPN, with rule based priority queuing policy.

Risk Assessment was performed on the proposed VoIP architecture, in order to do a gap analysis and risk treatment. Protection against zero day attacks, and new vulnerabilities have been considered, thus proving an efficient secure end-to-end communication.

This paper is organized as follows, Section II presents a classifications and an overview of SIP threats taxonomy along with the arising attacks. Section III briefly presents mitigation methods and previous related work. Section IV states the proposed multilayer secured SIP architecture. Section V describes the simulation configuration, and result analysis. Finally, the last section presents the conclusion and provides some insights to future work.

II. SIP Threats Taxonomy and Attacks

There have been many threats and attacks arising in VoIP infrastructure sourced from the internal and the external network. Those threats and targeted attacks violate the CIA triad [5], [6]. Man in the middle attacks such as call eavesdropping, call recording, and voice mail tampering, are violating confidentiality. Altering messages while transmission is violating the integrity. DoS floods, Buffer overflow attacks, Worms and viruses are violating the availability of the services offered by the VoIP infrastructure, and finally violating Authenticity by registration hijacking, and caller ID spoofing.

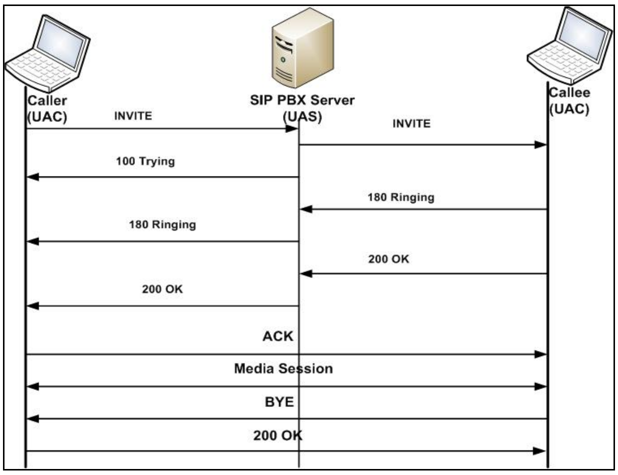
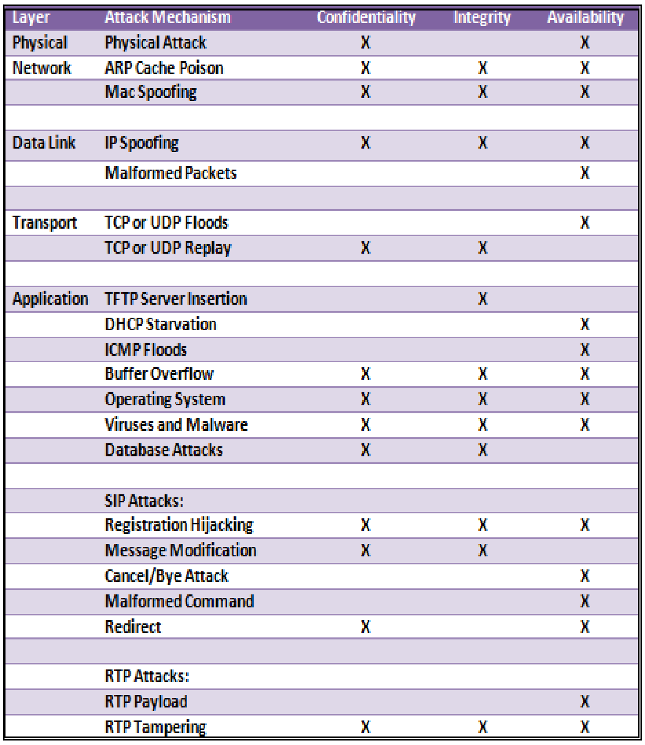


Fig. 1. SIP registration.

Launching an attack in SIP based VoIP infrastructure is performed after certain steps are performed, such as; Foot printing, reconnaissance, scanning and enumeration, thus discovering available alive hosts that use SIP as a signaling protocol. Then launching the attacks can be easily successful if there is no proper security controls applied for VoIP infrastructure. Those attacks aim to manipulate the use of Normal Registration Session affecting either User Agent Client (UAC), or User Agent Server (UAS) which is SIP based UAS in this case. Fig. 1 shows the flow of SIP registration.

Launching a Denial of Service attack in a SIP based environment violates the availability, thus preventing users from making VoIP calls. There are two common strategies to launch a DoS attack, either by exploiting the software vulnerability or by depleting resources at the target host. This attack is performed by canceling user calls which is BYE, and CANCEL attack. Moreover by flooding the SIP PBX Server which is INVITE or REGISTER attack by sending a large number of packets which the target accepts and tries to process, causing either delay or dropping any legitimate traffic.



Layer	Attack Mechanism	Confidentiality	Integrity	Availability
Physical	Physical Attack	X		X
Network	ARP Cache Poison	X	X	X
	Mac Spoofing	X	X	X
Data Link	IP Spoofing	X	X	X
	Malformed Packets			X
Transport	TCP or UDP Floods			X
	TCP or UDP Replay	X	X	
Application	TFTP Server Insertion		X	
	DHCP Starvation			X
	ICMP Floods			X
	Buffer Overflow	X	X	X
	Operating System	X	X	X
	Viruses and Malware	X	X	X
	Database Attacks	X	X	
	SIP Attacks:			
	Registration Hijacking	X	X	X
	Message Modification	X	X	
	Cancel/Bye Attack			X
	Malformed Command			X
	Redirect	X		X
	RTP Attacks:			
	RTP Payload			X
	RTP Tampering	X	X	X

Fig. 2. CIA violations.

SIP is vulnerable to RTP media injection, so it is easy to manipulate and can lead to some major dangerous impact, thus violating the integrity. Man in the middle attack can be launched by ARP Poisoning, so the attacker receives all the RTP traffic as well as the Registration credentials, thus violating confidentiality, this is known as eavesdropping. Successful exploitation of vulnerability by a threat can lead to possible attacks that have huge impact on assets availability, confidentiality, and integrity. Fig. 2 shows a classification of attack mechanisms targeting the corresponding TCP/IP layers, and the resulting violations of the CIA security mechanism [4].

Major Security threats, are Eavesdropping, DoS, Packet Spoofing, Replay attacks and message integrity. This paper aims is to implement Multilayer VoIP Security in SIP based infrastructure, providing CIA Security mechanism, thus mitigating Denial of Service, Eavesdropping and

Registration manipulation Attacks.

III. Mitigation Methods and Related Work

Multiple Mitigation methods have been discussed based on SIP based threats, and attacks. Then discussing previous related work, which is categorized into Single-layer security defense, and Multilayer security defense.

A. Mitigation Methods

SIP attacks mitigation methods have been addressed in [5], [6]. Focusing on the targeted attacks as clarified in the previous section. SIP security is provided in a multilayer security defense; evolving a Multilayer secured SIP based VoIP architecture. Those layers are divided into Network Layer, Transport Layer and Application Layer. Those layers are compromised to man in the middle attacks, Denial of Service and fake registration attacks.

Firstly, *Eavesdropping* is the unauthorized interceptions of voice packets; this can be mitigated by encrypting the transmitted data. Encryption can be achieved by the use of Tunnels across public networks. Tunnels are by topology “point to point” virtual connections between a network ingress point and a network egress point. At the ingress point, data is encapsulated using encryption, while at the egress point, data is DE-encapsulated into the original source format. Tunnels can be established across a private Metropolitan Area Network (MAN) or a Wide Area Network(WAN), such as Optical Ethernet, Frame Relay, Leased Line, etc., or across the public Internet. In this way, most VoIP traffic, except for virtual private networks (VPN), will not traverse a public network such as the Internet. This is done by establishing a virtual point-to-point connection through the use of dedicated connections and applying encryption. Such as IPIP, GRE, TLS/SSL and IPSEC based VPN that provides a secure communication for data as it transits through the unsecure public network [7], [8].

Tunneling over WANs eliminates the risk of exposing a network to intruders, which comes with opening ports on a firewall to allow VoIP to flow through. Therefore tunnels provide secure transport of the VoIP traffic over the public network. A secure voice network which employs end-to-end encryption will introduce more latency. This is the major disadvantage in this approach. Latency is a very important issue as users will not accept long call setup times, delay in conversation, or choppy voice quality (jitter). Participants in a conversation will begin to talk over each other as latency increases above 200ms.

Secondly, *Denial-of-Service*: Prevention of access to a network service by targeting SIP PBX server or voice gateway. This can be mitigated by implementing a security control such as intrusion detection/prevention Systems IDS/IPS. The major difference between IDS and IPS is that IPS’s are implemented inline in order to allow/deny incoming or outgoing traffic while IDS’s are mainly used for monitoring and logging purposes that lead to detect malicious attacks and customize rules to prevent those attacks by sending a RESET packet. An IDS/IPS operates in two main modes either in signature based or in anomaly based.

Intrusion Detection Systems (IDS) use either a statistical anomaly analysis technique that determines normal network activity like what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is anomalous (not normal), or a signature based analysis that monitors packets in the Network and compares with preconfigured and predetermined attack patterns known as signatures. The issue is that there will be a lag between the time where the new threat discovered and the time where the signature is applied in IDS for detecting the threat. During this lag time, the IDS will be unable to identify the attack [9].

Thirdly, Authenticity based Attacks, this attack can be performed by Registration Hijacking, where the attacker replace the legitimate registration of the victim with his address. Media Session Hijacking Spoofed messages from Attacker may be delivered to either one of the VoIP end points to redirect the media to another end point or by Server Impersonating, where the attacker trick the victim into communicating with the rogue proxy set up by the attacker [10].

B. Single-Layer Security Defense

The DoS flooding counter-measure mechanism was implemented by detecting the open SIP sessions using cumulative sum method. Attack prevention was based on observation of the connection setup messages (INVITE) and positive replies (200 ok). Both should roughly be equal at any given time, so when suddenly the ratio changes, it's likely to be a DoS attack. The approach was mainly used to detect general TCP SYN flooding attacks. This method is an anomaly based detection that was used to protect end-user terminals (UA) only.

In Ref. [6] a state based data mining IDS was presented to detect SIP message flow tampering and DoS flooding attacks by correlating SIP and RTP network events. Both SIP and RTP traffic were monitored and individual events were generated from the monitored packets. Events were pre-defined characteristics that can be extracted from received messages, e.g. session tear down event, jitter event,...etc.. Signature detection was applied for these events to determine, if the target is currently being attacked. In the framework implementation of IOS, the authors proposed to place IDS’s directly to all relevant UAs where IDS’s were placed in front of agents (UA).

The authors developed a DoS flooding mitigation mechanism dubbed “Pike” that rate-limits incoming traffic on a per-host basis. This method is listed as an example for the various rate-limiting software mechanisms available as add-ons for SIP servers or in commercial security solutions. The algorithm counts all incoming requests per IP address in a defined time frame. Whenever a fixed upper limit is reached, further messages from the offending IP address are not processed for a limited time [11].

The authors suggest implementing their mechanism within a NIDS (dubbed “Application-Layer Attack Sensor”) placed in front of the SIP proxy of the network to be protected. For attack mitigation, the sensor has a connection to the SIP proxy, to instruct it when it should throttle down or temporarily block requests [12].

The authors [13], [14] present a signature-based solution to protect SIP network elements from message payload tampering attacks. They suggest the employment of signature patterns (based on the SIP grammar) to distinguish well-formed messages from malformed ones, similar to computer virus signature descriptions. Specifically, any SIP message which does not correctly conform to the SIP grammar is identified as malformed.

C. Multilayer Security Defense

The authors [15] propose a signature-based message integrity checker and DoS flooding preventing mechanisms based on the Snort IDS [16]. Passing SIP messages are checked for known malicious content, e.g. SQL code injection [17]. Similarly to [11], single-source message flooding is detected by a threshold message counter, and further messages below this threshold are dropped. Additionally, signatures for general IP-based attacks not related to SIP are applied.

The authors [18] present an IDS concept based on a Bayes inference model [19] for detecting multiple types of attacks. The IDS considers SIP signaling attack classes, including multiple-source DoS flooding, SPIT, password cracking and vulnerability scans. Bayesian inference, as used in this work, is a statistical inference in which posterior observations are used to update the probability that a prior hypothesis may be true. Here the authors have developed a Bayes network tree where monitored network events relate to posterior observations. The prior hypothesis states that the traffic belongs to one of the introduced attack classes. The authors define multiple monitoring parameters, like the number of ACK messages in waiting state, request and response distribution in one sampling interval, etc. Each defined parameter is given a probabilistic value for each attack class, this was theoretical work.

The authors [11] present a holistic multilayer IDS system to detect multiple different attacks based on a honeypot setup and network event correlation. A honeypot SIP setup is deployed to lure malicious users with the intention of conducting SPIT or phishing attempts to use this setup. Once in the honeypot, senders are classified and cannot access the real SIP network later on. An event correlator is used for DoS message flooding, and message flow tampering detection. The event correlator is the same pattern-based setup as proposed by [15]. Likewise, attacks are detected with similar signatures. Additionally, the authors propose anomaly-based detection by generating individual SIP user profiles and detecting deviation from this profile. Flooding attacks are detected by monitoring for short inter-arrival times of requests, or by detecting open sessions by monitoring for missing ACK messages. This method does not provide prevention features, however the authors recommend blocking identified users in the honeypot or flooding requests detected by the event correlator.

The authors [19] present a combination of the work of [12], [13] and [17]. They use a layered approach with two layers. The first countermeasure layer consists of a message checker as proposed by [12], [13]. The second layer consists of a cross-protocol state machine specification as proposed by [20]. The authors use this system to target the same threats with the same methods.

IV. The Proposed Architecture

The paper proposes a multilayer security approach in SIP based VoIP infrastructure. It focuses mainly on Denial-of-Service, and Eavesdropping, which is a sort of man-in-the-middle attacks. Previous deployed solutions lacks providing media and signaling security, also it neglected zero day attacks and new vulnerability arising. As shown in Fig. 3, it illustrated the proposed security architecture in details, three categories of Security techniques have been developed based on their function

1) Security Enabling [Encryption and Authenticity]
2) Security protection [Firewall, aiming to protect from external threats]
3) Security Violation detection techniques (Such as IDS/IPS and monitoring events]

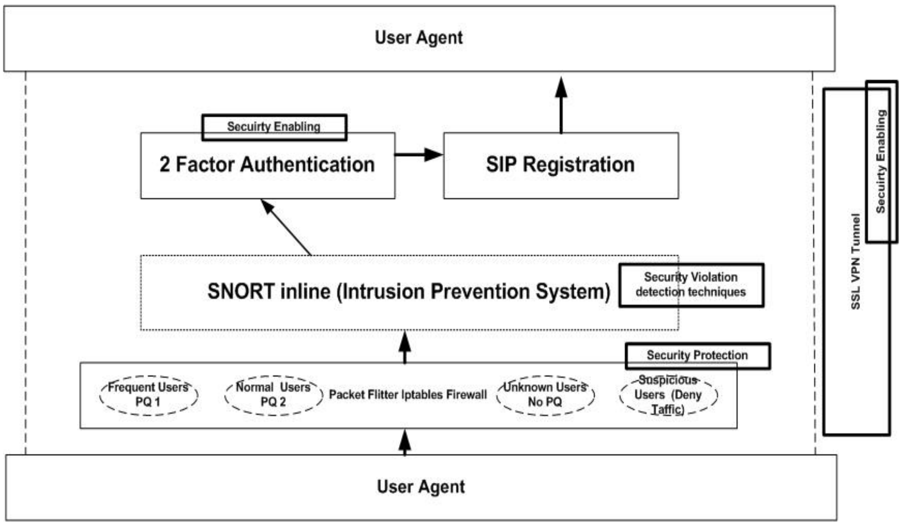


Fig. 3. The proposed architecture.

A. Security Enabling

Security Enabling, Authenticity is provided by a two factor authentication mechanism which authenticates user based on username, password, as well as layer 2 MAC address of user agent. While the registration procedure of user agent with

Asterisk PBX, authentication is granted by providing a valid username and password, as well as comparing layer 2 MAC address to the MAC that was already bounded to that particular user agent. This layer of security also prevents some integrity based attacks.

User agent credentials are stored in the database in encrypted format, rather than in clear text. Media and signaling encryption are provided by the use of OpenVPN, thus providing confidentiality for user agents while initiating/receiving VoIP calls, transmits traffic over an SSL-based VPN improves call quality due to UDP VoIP packet encapsulation of SIP & RTP, OpenVPN encrypts data using simpler encryption protocol with a smaller key, then using that key for short time, after key expired a new key is generated randomly and exchanged securely using RSA encryption, the point of this is to highlight the fact that RSA key is only used periodically for re-establishment of data encryption channel. OpenVPN can build tunnel on either TCP or UDP, in this research, UDP Tunnel has been used to provide fast traffic transmissions.

B. Security Protection

Security Protection, Aims to secure perimeter from external attacks and threats, such as DoS, this layer of security is achieved by deploying an inline snort [intrusion prevention system] located right after a firewall [IPtables], which filters traffic and only passes through allowed traffic based on configured rules that are applied in queuing mechanisms method that have been configured by making rule based priority queuing Firewall is first layer of defense that protect against attacks, its located between private and public network as internet, it is a bottleneck for network traffic because when designed properly no traffic can enter or exit LAN without passing through firewall.

There are many types of firewalls such as packet filter firewall, proxy firewall and stateful event monitor, in this research packet filter firewall is used. Network level firewall (packet filter firewall) is a router device which forwards packets from one network to another, but it also filter packets flow through it and decides whether to deny or accept that traffic.

Packet filter firewall describes a method for analysis and tracking of sessions to distinguish between the beginning of the session and the end of the session depend on examine packet headers, such as source and destination IP addresses, source and destination ports and protocol type. Rule based priority queuing has been deployed on firewall, rules are categorized into three rules for frequent users, normal users, and unknown users. Queuing mechanism also prevents flooding attacks, many researchers shown that effect of flood base d DoS attack can be reduced if system has a good queuing mechanism [6].

C. Security Violation

Security Violation detection techniques, Intrusion prevention system is used for this layer of protection, IPS operates in three different phases, which are Detection phase, Correlation phase, and automated policy driven response phase. Detection phase where intrusions are detected by the configured sensor, there are two intrusion detection methods, anomaly detection and misuse detection, misuse detection methods use information about known security policy, know vulnerabilities and know attacks to VoIP systems, this approach compares network activity or system audited data to a database of known attack signatures, or other misuse indicators, resulting a pattern matches that produce alarms and various sorts of Reponses, when a comprehensive and up to date set of attack signature is used, thus knowing by correlation phase during which system gathers data from multiple sites before intelligently correlate gathered information. To avoid prohibitive numbers of false positives, and reactivity implied by signature base detection system.

Automated policy driven response phase is appropriate action that needs to be taken in case of correlation process detects a probable intrusion, the response could be reject, drop or alert, signature based detectors determine the likelihood of an attack issuing an alert. A robust automated response system is deployed to reduce human error and respond to intrusions accurately in a fraction of time required for manual response, also automated response system responds quickly enough to thwart active attacks in real time using optimal Reponses.

Finally, performing regular security and vulnerability scanning using Tool as Nessus, in order to identify vulnerabilities that needs to be patches and fixed, an ensure of zero day attacks detection, by exploiting every vulnerability and add attack signatures in IPS database.

There are three common queuing disciplines that can be analyses, they are first-in-first-out (FIFO) queuing, priority queuing (PQ) and weighted-fair queuing (WFQ) [21], the basic principle of FIFO queuing is that the first packet that arrives at a router is the first packet to be transmitted. An exception here happened if a packet arrives and the queue is full, then the router ignores that packet at any conditions. The principle idea of PQ queuing depends on the priority of the packets, a highest priority are transmitted on the output port first and then the packets with lower priority and so on. When congestion occurs, packets with lower-priority queues will be dropped. The only problem with these packets is that has lower-priority in queue.

D. Laboratory Setup and Architecture

The proposed multilayer secured SIP based VoIP architecture aims to prevent eavesdropping, denial of service and fake registration attacks, providing an efficient security mechanism by deploying rule based priority queuing policies, as well as protecting VoIP infrastructure from zero day, and new emerging attacks. The VoIP components, namely, UAC, UAS, and Asterisk PBX [22], [23], are used to manage and establish calls. SNORT [24] inline component is used to prevent Denial of Service, in addition to filter and block malicious traffic. For penetration testing and security assessment, Backtrack [25] mainly focuses on SIP based attacks and exploits.

The First Layer uses a firewall. In this case Linux OS the iptables was used. This firewall can be configured using a set of rules/commands resulting in flexible way of filtering the unwanted traffic. Rule based priority queuing mechanism can be very helpful in defending against DDoS attacks. Queuing is done on firewall, in this paper the proposed rule based queuing policies substitutes the regular PQ on firewall. rule based has been implemented from scratch, enhanced, and adapted to provide higher security levels, where it categorized packets into fourrule based priority policies: Frequent users, normal users, unknown users, and suspicious users as shown in Fig. 3, the highest priority is the frequent users list, then normal user list. Only INVITE and REGISTER requests are allowed from unknown users, by using this filtering rule at firewall other types of SIP requests can be eliminated The use of temporary user list ensures that unknown legitimate users can become authenticated without any difficulties, the firewall queuing, user list and frequent user list are updated regularly which maintains a good QoS for legitimate users during flood attack. The traffic of suspicious user list is denied from passing through network.

The second layer of the proposed approach is deploying an Intrusion Prevention System (IPS). Snort Intrusion Prevention Systems, as in Fig. 4, it inspects the packets and decides, based on set of rules, whether or not they are malicious. If a packet matches an attack signature then an alert is generated. The Intrusion Prevention System can manipulate or drop those packets or it can also perform IPS alerting tasks. The proposed solution includes a firewall and IPS to provide a more secure VoIP system, as in Fig. 5.

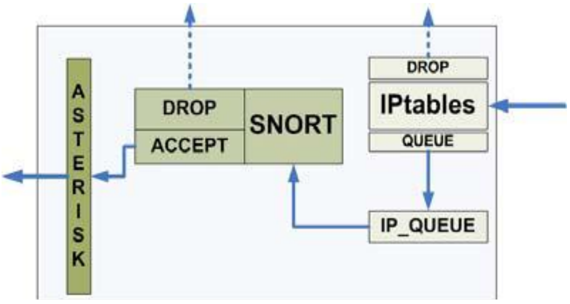


Fig. 4. SNORT and IPtables.

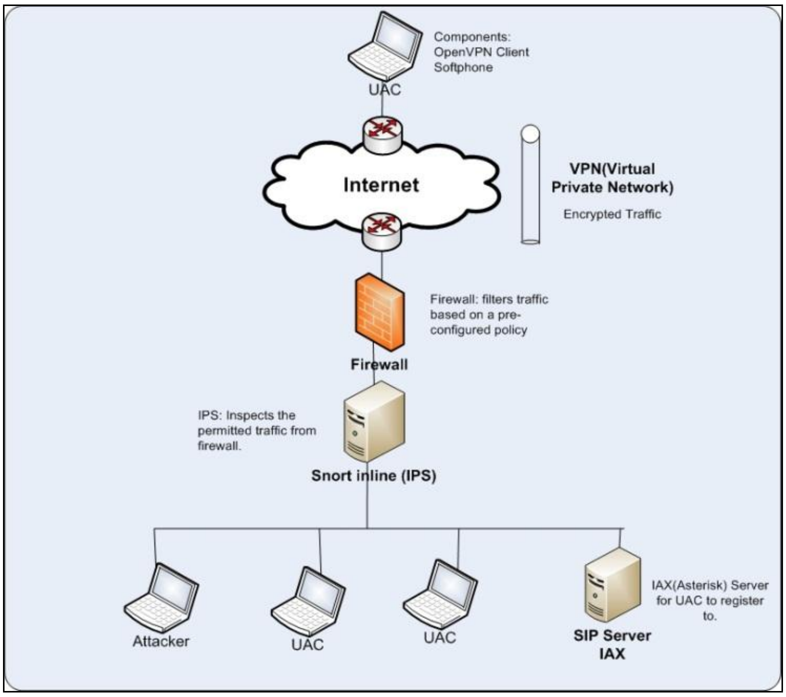


Fig. 5. Multilayer secured SIP based VoIP architecture.

The DROP/DENY rules were applied for traffic from the external network as well as for the messages that could be identified with no doubt as being malicious: The secured system was then tested. Results indicate that UDP flooding is alerted successfully from external network. While alerts were generated, flooding with INVITEs from the internal network was still possible, but attacks from the external network were successfully stopped. Issues involving forged REGISTER, BYE messages proved to be handled harder. Snort successfully blocks attacks that involved erasing or high jacking contacts using false REGISTER messages.

The third vital layer of the approach is Virtual private network, which is implemented by Open VPN server v2.2.0 running in server mode for creating a SSL/TLS based VPN tunnel with local site VPN ensuring authentication, confidentiality, and integrity.

Authentication for outgoing calls is an entirely separate process and always happens on pre-call basis, the user has to register by a two factor authentication method, a UAC has to provide a valid password and it also verifies the layer 2 MAC address bounded to that UAC.

As shown in Fig. 5, the proposed multilayer secured SIP on an end-to-end connection. The impact of security mechanism or the perceived quality of voice communications evaluated by means of suited OPNET simulation tools that allow to simulate different traffic conditions and bandwidth availability, Tunneling all VoIP traffic over VPN, with firewall in order to investigate and filter the incoming and outgoing packets against SIP based attacks and threats malicious traffic. The Results are simulated using OPNET modeler as clarified and shown below. The main QoS consideration specific to IPsec VPN’S are additional bandwidth required by IPsec encryption and authentication.

In Fig. 6, shows the architecture model used, and simulated using OPNET Modeler. The results analyze the impact of performance with different types of encapsulation and VPN, while implementing rule based priority queue in the firewall. The main factors affecting the quality of service are latency, Jitter and packet loss. Jitter: can be defined as a non-uniform packet delays while throughput is measured by the amount of successful data delivery over a specific period. The end-to-end delay is total amount of delay including codec delay, network delay as well as play out delay. Packet end-to-end delay less than 150 ms is considered good while a delay less than 400ms is considered acceptable [26].

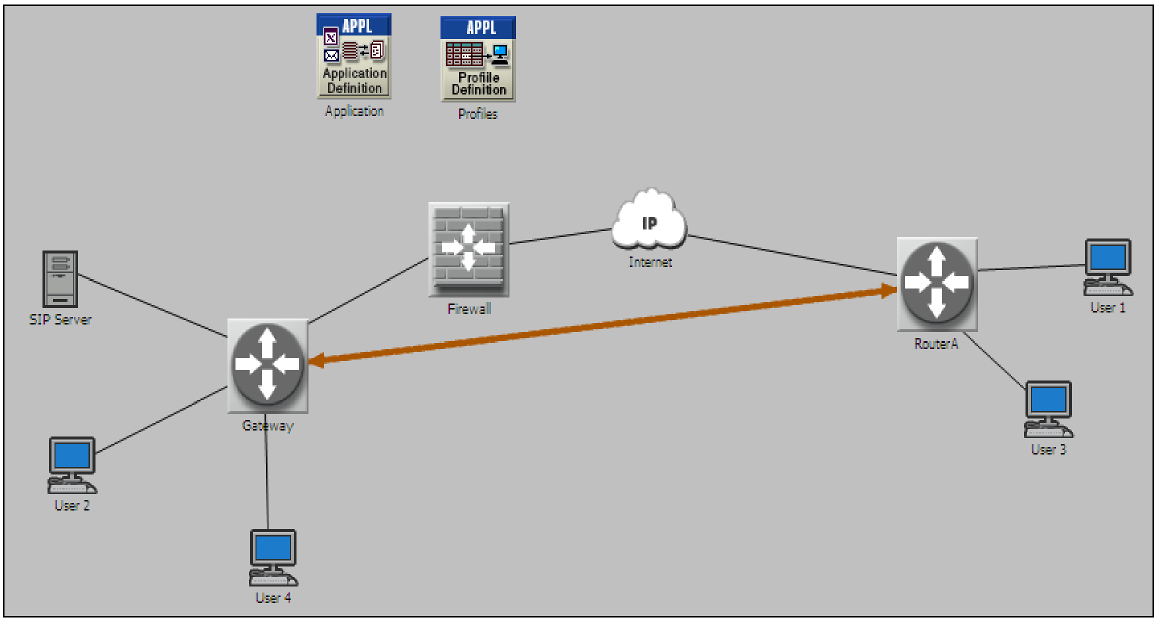


Fig. 6. The network topology.

V. Simulation Configuration and Results

As shown in Fig. 6, a VPN constructed as a gateway-to-gateway model where two remote users use the internet for VoIP communication via a firewall. Two types of VPNs are considered in the topology for a comparison test (IP VPN and GRE VPN) where test results are recorded with and without rule based priority queuing firewalls policies.

Scenarios Modes of deployments:

1) No Security controls are implemented
2) IP tunnel without Firewall
3) GRE Tunnel without Firewall
4) IP tunnel with Firewall
5) GRE Tunnel with Firewall

In the prescribed topology, a remote user (located off the premise) that requires the use of the VoIP services while he is connected through the Internet cloud.

A. Configuration Parameters

1) Workstation

Throughout the simulation, a wlan_wkstn_adv node model is used to represents a workstation with client-server applications running over TCP/IP and UDP/IP. The workstation supports one underlying WLAN connection at 1Mbps, 2Mbps, 5.5Mbps and 11Mbps. The workstation requires a fixed amount of time to route each packet, as determined by the “IP forwarding rate”. Packets are routed on a first-come-first serve basis and may encounter queuing at the lower protocol layers, depending on the transmission rates of the corresponding output interfaces.

2) Server

An Ethernet server. Model is used as a server node with applications running over TCP/IP and UDP/IP. This node supports one underlying Ethernet connection at 10Mbps, 100Mbps, or 1 Gbps.

3) Switch

An Ethernet 16_port switch is used. The switch implements the spanning tree algorithm in order to ensure a loop free network topology. In addition, the connections can be at 10Mbps, 100Mbps, or 1000Mbps.

4) Subnet

A single network object that contains other network objects (links, nodes, and other subnets) is used. Sub-networks allow us to simplify the display of a complex network through abstraction. It also helps us in logically organize network model.

5) Firewall

The firewall, which can also be seen such as concentrator VPN, follows the model OPNET "ethernet2_slip8_firewall". It thus contains two interfaces Ethernet, those who interest us here, but also 8 interface series, unused in this case. It is characterized by the same parameters (CPU/Workstations, ARP/Wireless Router, IP: Ethernet /Server). Since the most common WLAN usage is considered, the wireless speed was configured at 11Mbps with the random CSMA/CA DCF access mode [27].

B. Result Analysis

Below are the results of OPNET simulations. A comparison between different deployment scenarios with different security measures have been implemented as mentioned in the previous section, the time needed to set up a call. The minimum time was recorded if no security controls were applied. IP VPN with a firewall took 0.047 sec to set up a call while the same set up took 0.057 sec, in case of GRE VPN.

Fig. 7 and Fig. 8 show that the five deployment scenarios are relatively the same while sending and receiving traffic, hence there is no packet loss.

In Fig. 9, end user delay variation, which represents the variance among end to end delays for voice packets and is measured from the time it is created to the time it is received, it shows that GRE VPN with firewall took the highest packet delay variation and GRE without firewall took less time, indicating the small delay impact of the use of firewall. The least end Delay Variation is IP VPN with firewall.

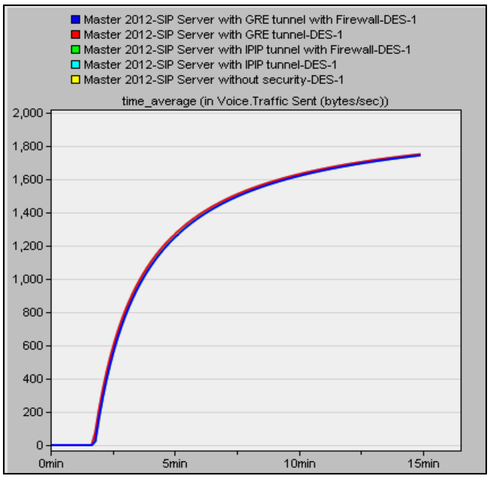


Fig. 7. Traffic sent.

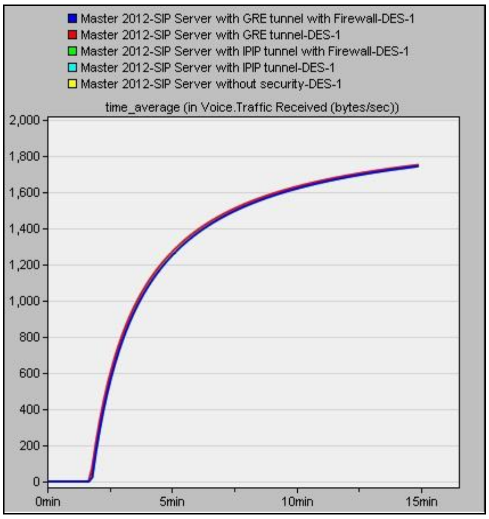


Fig. 8. Traffic received.

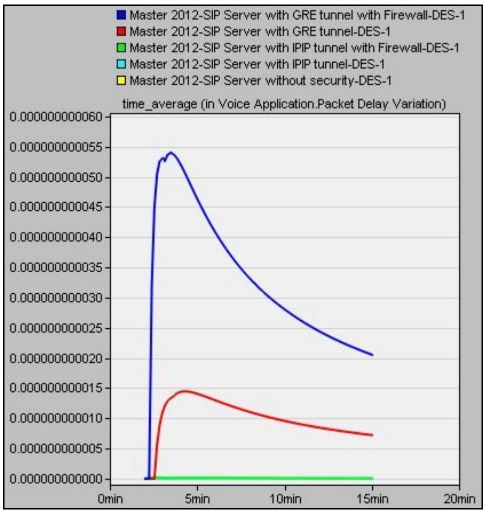


Fig. 9. End user delay variations.

Fig. 10 shows that GRE VPN with firewall had the highest packet delay variation and GRE without Firewall took less time, indicating the impact of the use of GRE tunnel, since a lot of encryption overheads. The least end user packet delay is IP VPN with firewall as shown.

The results of Fig. 11 gives a significant observation, that GRE VPN with a firewall showed the highest end-to-end delay compared to IP VPN with firewall that recorded a less end-to-end delay.

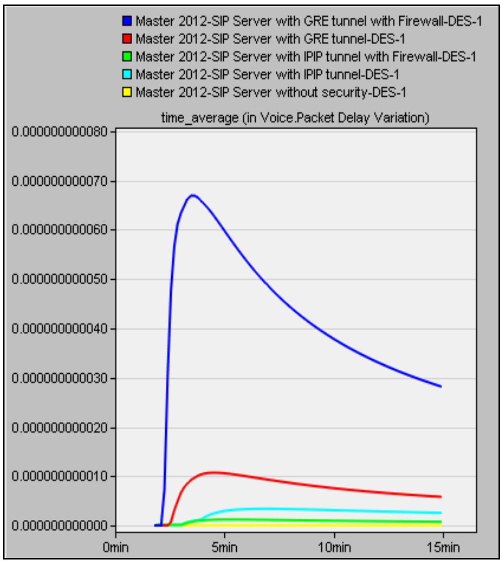


Fig. 10. Packet delay variations.

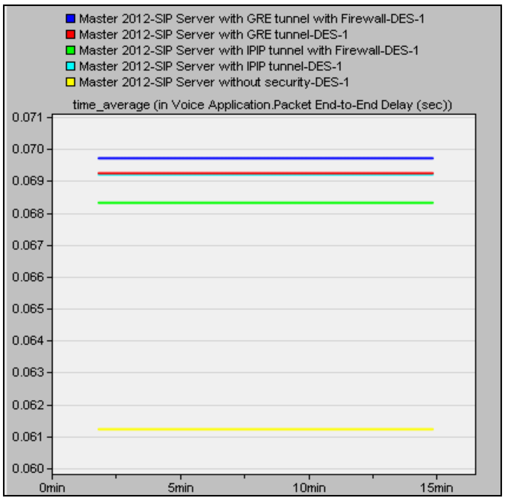


Fig. 11. End-to-end delay.

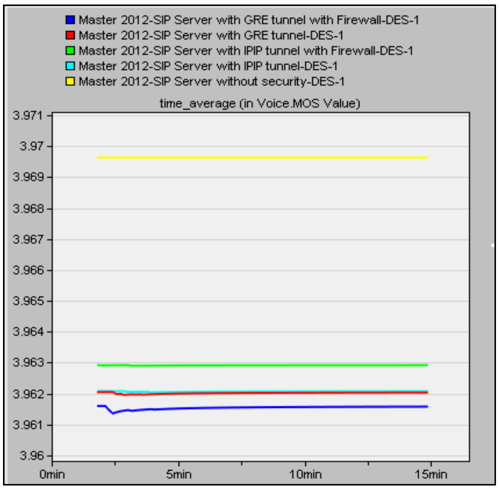


Fig. 12. MOS.

Fig. 12 shows the mean opinion score (MOS). The maximum observed values for MOS for voice traffic was found to be 3.963 for IP VPN with Firewall, while MOS for GRE VPN with Firewall was between 3.961 and 3.962. MOS is used to check which factor affecting the quality of voice its value changes to 1 to 5, the lowest value show the lowest quality of voice and highest value show the best quality of voice [27].

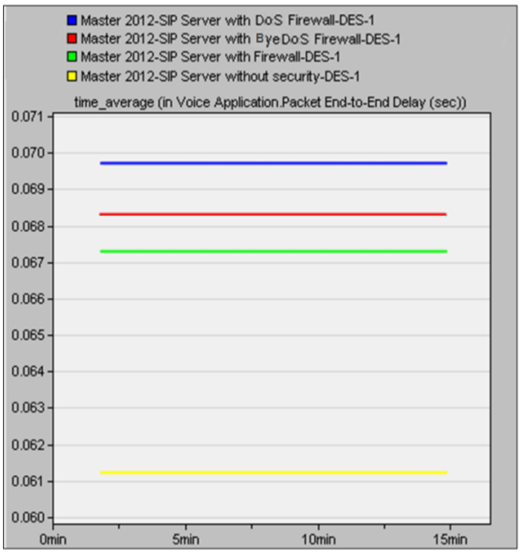


Fig. 13. DoS attack end-to-end delay.

TABLE I: VOIP MEASUREMENTS

Scenario	Voice Volume bytes/sec	Top ETE (End-to-End) Delay	TopETE Delay variation	MOS(Voice mean opinion score)
GRE with FW	Peak traffic received: 1000 Bps	0.069711 sec	User2: 2.0094E-10	3.961599
	Average: 872 Bps		User1: 1.2775E-10	
	Peak traffic sent: 1000 Bps		Average 2.0527E-11	
GRE without FW	Sent: 872 Bps	0.06924 sec	User2: 1.8379E-11	3.962046
	Average: 872 Bps		User1: 3.3971E-11	
	Peak: 872 Bps		Average: 7.2284E-12	
IPIP with FW	Peak traffic received: 1000 Bps	0.068315 sec	User2: 5.7930E-12	3.962923
	Average: 872 Bps		User1: 4.5981E-13	
	Peak traffic sent: 1000 Bps		Average: 8.2970E-14	
IPIP without FW	received: 1000 Bps	0.069198 sec	User2: 1.5761E-11	3.962085
	Average: 872 Bps		User1: 8.5059E-14	
	Peak traffic sent: 1000 Bps		Average: 2.2354E-14	

Fig. 13 shows comparison between rule based queuing firewall end-to-end delay while DoS and Bye DoS Attack, and when there is no Attack.

Table I shows results analysis of QoS for each scenario, showing the impact of different types of VPN used, Comparing results to previous paper results [26], [27]. Delay is maximum when GRE tunnel was implemented. End-to-End delay values in case of firewall and VPN is found to be 0.6158 sec, while it is found to be 0.3836 sec in case of no firewall and in case of with firewall this value found to be 0.1078 sec in paper [28], ETE delay was found 2.43 sec in case of firewall and 2.63 sec for firewall and VPN, and MOS was found to be 3.056.

VI. CONCLUSION AND FUTURE WORK

The proposed multilayer secured SIP based VoIP architecture has been implemented in the VMware Server's virtualization environment. It provides an efficient VoIP security to many layers, as application, network and transport layer, thus providing CIA, as well as protection against DoS, Man-in-Middle attack, and Hijacking. The security system architecture reveals the magical power of Linux as an open source growing technology. SIP based threats, and attacks have been identified, in this paper a rule based priority queue firewall policy have been implemented substituting pre-configured priority algorithm in firewall, it has been showing enhanced QoS and security defense mechanism. OPNET was used to evaluate end-to-end performance analysis of IP and GRE VPN tunneling for VoIP using OPNET modeler, while configuring rule based PQ firewall. The results show the delay impact caused by protocol overhead caused by VoIP encapsulation within VPN, Due to limitations of simulations of IPSEC using OPNET, In other words, the IPSEC parameters are configured however it doesn't affect the graph results; however the results will be very similar to GRE VPN with Firewall.

The results and analysis shows that packet delay variation and packet end-to-end delay for voice increased while using GRE VPN with Firewall, than IP VPN with firewall, main reason behind this is the additional encapsulation time needed as well as IP processing time of the Firewall, moreover the encryption process. On the other hand MOS was not affected by GRE VPN with Firewall; it provides an increasing security levels, meanwhile a reasonable decrease in network performance was observed. It's expected that the use of IPSEC VPN the security level increases however a reasonable decrease in the network performance shall be observed, which will be due to the encryption process and added authentication headers for packets. According to experimental results, it's found that rule based queuing firewall end-to-end delay while under DoS provides good performance and less end-to-end delay.

The proposed architecture ensures to block zero day attacks, by exploiting every vulnerability and adding attack signature in IPS database, also it enhanced performance results by 0.01% compared to previous work, for future work, one can consider Securing VoIP Applications hosted over the cloud, and providing a secure architecture for cloud based applications.

ACKNOWLEDGMENT

The authors would like to thank National Telecommunications Institute (NTI), Egypt, for providing OPNET 17 modeler.

REFERENCES

[1] D. R. Kuhn, T. J. Walsh, and S. Fries, *Security Considerations for Voice Over IP Systems*, National Institute of Standards and Technology, ch. 2, pp. 16-17, January 2005.

[2] H. Schulzrinne and J. Rosenberg, "A comparison of SIP and H.323 for internet telephony," in *Proc. International Workshop on Network and Operating System Support For Digital Audio And Video (NOSSDAV),* Cambridge, England, July1998, pp. 83-86.

[3] K. Siddiqui, M. Kamran, and S. Tajammul, "Comparison of H.323 and SIP for IP telephony signaling," in *Proc. IEEE 4th International Multioptics Conference,* Lahore, Pakistan, Dec. 2001, vol. 5, no. 2, pp. 32-47.

[4] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambrinoudakis, S. Gritzalis, K. S. Ehlert, and D. Sisalem, "Survey of security vulnerabilities in session initiation protocol," *IEEE Communications Surveys & Tutorials*, vol. 8, no. 3, pp. 68-81, 2006.

[5] D. Butcher, X. Y. Li, and J. H. Guo, "Security challenge and defense in VoIP infrastructures," *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews,* vol. 37, no. 6, pp. 1152-1162, Nov. 2007.

[6] S. Ehlert, D. Geneiatakis, and T. Magedanz, "Survey of network security systems to counter sip-based denial-of-service attacks," *Computer and Security*, Elsevier, vol. 29, pp. 225-243, 2010.

[7] A. Malik, H. K Verma, and R. Pal, "Impact of firewall and VPN for securing WLAN," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 5, pp. 407-410, May 2012.

[8] R. Malik and R. Syal, "Performance analysis of IP Security VPN," *International Journal of Computer Applications*, vol. 8, no. 4, p. 5, October 2010.

[9] M. Babu, "Performance analysis of IPSec VPN over VoIP network using OPNET," *International Journal of Advanced Research in Computer Science and Software*, vol. 2, no. 9, pp. 38-42, 2012.

[10] K. Salah and A. Alkhoraidly, "An OPNET based simulation approach for deploying VoIP," *Int. J. Network Mgmt*, vol. 16, no. 3, pp. 159-183, 2006.

[11] B. Iancu. (2003). SER PIKE excessive traffic monitoring module. [Online]. Available: http://www.iptel.org/ser/doc/modules/pike

[12] R. Dantu, S. Fahmy, H. Schulzrinne, and J. Cangussu, "Issues and challenges in securing VoIP," *Computer & Security Elsevier*, vol. 28, no. 8, pp. 743-753, 2009.

[13] M. Nassar, S. Niccolini, R. State, and T. Ewald, "Holistic VoIP intrusion detection and prevention system," in *Proc. Principles, Systems and Applications of IP Telecommunications*, New York, USA, vol. 181, pp. 1-9, July 2007.

[14] D. Geneiatakis, G. Kambourakis, T. Dagiuklas, C. Lambrinoudakis, and S. Gritzalis, "A framework for detecting malformed messages in sip networks," in *Proc. 14th IEEE Workshop on Local and Metropolitan Area Networks (LANMAN),* Chania, Greece, September 2005, vol. 175, pp. 5.

[15] M. Nassar, R. State, and O. Festor, "Intrusion detection mechanisms for VoIP applications," in *Proc. 3rd Annual VoIP Security Workshop*, Berlin, Germany, vol. 179, pp. 3-7, 2006.

[16] D. Geneiatakis, G. Kambourakis, C. Lambrinoudakis, T. Dagiuklas, and S. Gritzalis, "A framework for protecting a sip-based infrastructure against malformed message attacks," *Computer Networks*, vol. 51, no. 10, pp. 2580-2593, July 2007.

[17] D. Geneiatakis, G. Kambourakis, C. Lambrinoudakis, T. Dagiuklas, and S. Gritzalis, "SIP Message Tampering: The SQL code injection attack," in *Proc. 13th International Conference on Software, Telecommunications and Computer Networks*, Split, Croatia, pp. 2-7, September 2005.

[18] M. Roesch, "Snort – Lightweight intrusion detection for networks," in *Proc. 13th USENIX Large Installation System Administration Conference (LISA'99),* Seattle, USA, November 1999, pp. 229-238.

[19] S. M. Stigler, "Thomas Bayes' Bayesian inference," *Journal of the Royal Statistical Society, Series A (General)*, vol. 145, no. 2, pp. 250-258, 1982.

[20] Y.-S. Wu, S. Bagchi, S. Garg, N. Singh, and T. Tsai, "SCIDIVE: A stateful and cross protocol intrusion detection architecture for Voice-over-IP environments," in *Proc. International Conference on Dependable Systems and Networks*, Firenze, Italy, July 2004, pp. 443-442.

[21] H. A. Mohammed, A. H. Ali, and H. Mohammed, "The effects of different queuing algorithms within the router on QoS VoIP application using OPNET," *International Journal of Computer Networks & Communications (IJCNC)*, vol. 5, no.1, pp. 117-124, January 2013.

[22] J. V. Meggelen and J. Smith, *Asterisk the Future of Telephony,* O`Reilly Media, ch. 3, September 2007.

[23] Digium. (2008). Asteriskguru. [Online]. Available: http://www.asteriskguru.com/tutorials/cli_cmd_14.html

[24] SOURCEfire. (2008). Snort.org Intrusion Detection/Prevention System. [Online]. Available: http://www.snort.org/dl/

[25] Backtrack Linux-Penetration testing distribution. [Online]. Available: http://www.backtrack-linux.org/

[26] H. Kazemitabar, S. Ahmed, K. Nisar, A. B. Said, and H. B. Hasbullah, "A comprehensive review on VoIP over Wireless LAN networks," *ISSR Journal*, vol. 2, no. 2, pp. 5-9, 2010.

[27] S. Narayan, S. S. Kolahi, K. Brooking, and S. D. Vere, "Performance evaluation of virtual private network protocols in Windows 2003 environment," in *Proc. IEEE International Conference on Advanced Computer Theory and Engineering,* 2008, pp. 69-73.

[28] A. H. M. Amin, "VoIP Performance measurement using QoS parameters," in *Proc. Second International Conference on Innovation in IT*, 2005, pp. 6-9.

Basma Basem is a network security engineer. She graduated from El Shorouk Academy. She received a cyber-security diploma from Information Technology Institute. She is a M.S student in the Computer Engineering Department at Arab Academy for Science Technology & Maritime Transport, Cairo. Her research interests are in the area of network security, cloud computing security, SIP/VoIP, and information security. She works in a multinational telecommunication company as a senior network security engineer.

Rowayda A. Sadek is an associate professor of Information Technology at Helwan University. She received her Ph.D. degree in 2005 from Alexandria University, Alexandria, Egypt in communication and electronics engineering. She is currently working as an assoc. professor and the head of Information Technology Department, in Faculty of Computer and Information, Helwan University. Her research interests include computer networking and security, multimedia processing for image, audio, video, etc. also multimedia networking, and security as interdisciplinary research.

Atef Z. Ghalwash is with the Faculty of Computers & Information, Computer Science Department, Helwan University, Egypt. He received his MSc degree from the Faculty of Engineering, Cairo University, Egypt in 1980. He was awarded his Ph.D. degree from the Faculty of Engineering, Maryland University, USA in 1988. His research interests include artificial intelligence, expert systems, computer security, DSS and systems developments.