Intrusion Prevention Systems: Architectures and Tools

Mohammad A. R. Abdeen

Islamic University of Madinah, Madinah, Saudi Arabia

Summary
Cyber security is an ever-heated topic as the rate of cyber-crime has increased significantly in the last few years. According to a report released by the University of Maryland in 2018 that cyber-attacks are happening on a "near constant time". The study stated that there is approximately one attack every 39 seconds on every computer in the world. The estimated total cost of cyber-crime is over $1 trillion dollars in 2018 and is expected to exceed $2 trillion in 2019 [2]. These facts have exerted an enormous pressure on governments, organizations and individuals worldwide to pacify, detect, and prevent those attacks. Intrusion prevention Systems (IPS) are central to computer and network cyber security. Despite the use of firewalls and virus scans, many attacks make it to the network largely due to human errors [3]. IPSs work on real-time to detect and take a defensive measure before the malware makes its way through the computer or the network. The way IPSs work is that they scan the incoming and the outgoing packets to/from computers or networks on real-time. If a suspicious packet is detected its either dropped or the entire connection is terminated. There are various ways/techniques used by IPSs to scan the data. In this work we will discuss the signature, the profile, and the stateful protocol methods. We will also discuss the deployment of those prevention methods, weather on a host, on a network or as wireless IPS. At the end of this work we will be reviewing the available systems for IPSs including the open-source ones. Examples of such systems include Snort, OSSEC, and Suricata. A comparison of those systems and their pros and cons will be included.

Key words:
Intrusion Detection, Intrusion Prevention, Open source software

1. Introduction

Intrusion Prevention Systems

Today, computer connectivity has proven indispensable. Isolated computers are today seen as an astray in a no man's land. With the sharp climb in the amount of data in just about any topic whether specialized or general available on the Internet, the access of this data became an everyday practice. On top of this is the numerous and rather uncountable applications from social media, online taxi (Uber), mobile applications, to online shopping made today's life without an Internet connectivity next to impossible. With every joy there is pain. With this blessing of connectivity and richness in data access and applications, came a huge risk of breaching security on the personal and organization levels. Many attacks on private and government have been reported in the last two decades that made addressing the issue of network security a pressing need. Some of the well-known attacks is the attack on Yahoo servers and the stealing of over 3 Billion user account information [12]. Many scholars in the industry as well as the research community dedicated much time to develop innovative methods to take these security problems. The start of the solution to this problem is to be able to identify or rather called detect an attack. Router are network devices that are used to provide connectivity to home networks. Routers are connected form one side to the Internet and from the other side to the home network. Today's routers are equipped with a functionality called a "firewall". A Firewall is a unit that acts as a security guard on the incoming traffic to the network. It prevents against intrusions and suspicious actions that might damage the network nodes or storage. Firewalls can be implemented as a software component or a hardware unit. For larger networks, other solutions that are far more comprehensive, effective, and sophisticated have been developed. As an example, the McAfee network security platform (NSP) can support up to 32 million connections and uses intelligent methods to detect intrusions [9]. Other solutions are also available where they can discover potential attacks on higher layers [14].
Figure 1 shows the physical and logical topology of the Intrusion Prevention System.

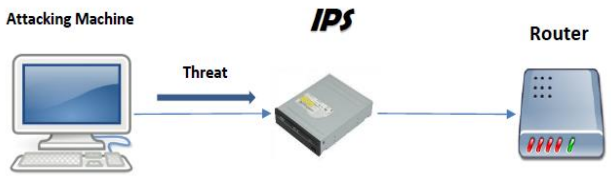

Fig. 1 Physical and logical Topology of the Intrusion Prevention System

2. Intrusion Prevention System (IPS)

The intrusion prevention system is a network security and threat prevention technology that examines network traffic flow to detect and prevent any possible exploitation of vulnerabilities. Malicious users, as an example, target

Manuscript received November 5, 2019
Manuscript revised November 20, 2019

either applications or services to disrupt and possibly gain control of a machine or a specific application running on the targeted machine. A successful intruder could potentially interrupt or completely disable the targeted application. The intruder might also succeed in gaining access with full permissions to the compromised application. A good IPS system is able to prevent a detected threat immediately. The IPS examines every packet and a decision is made if the packet is to be allowed into the network or dropped. Incriminated packets are discarded and the process results in some delay to ensure that secure packets are not mistakenly dropped. Figure 2 below shows the architecture and data paths. Designs are composed of two layers: data layer and control layer. The control layer controls the packet and flows of data layers.

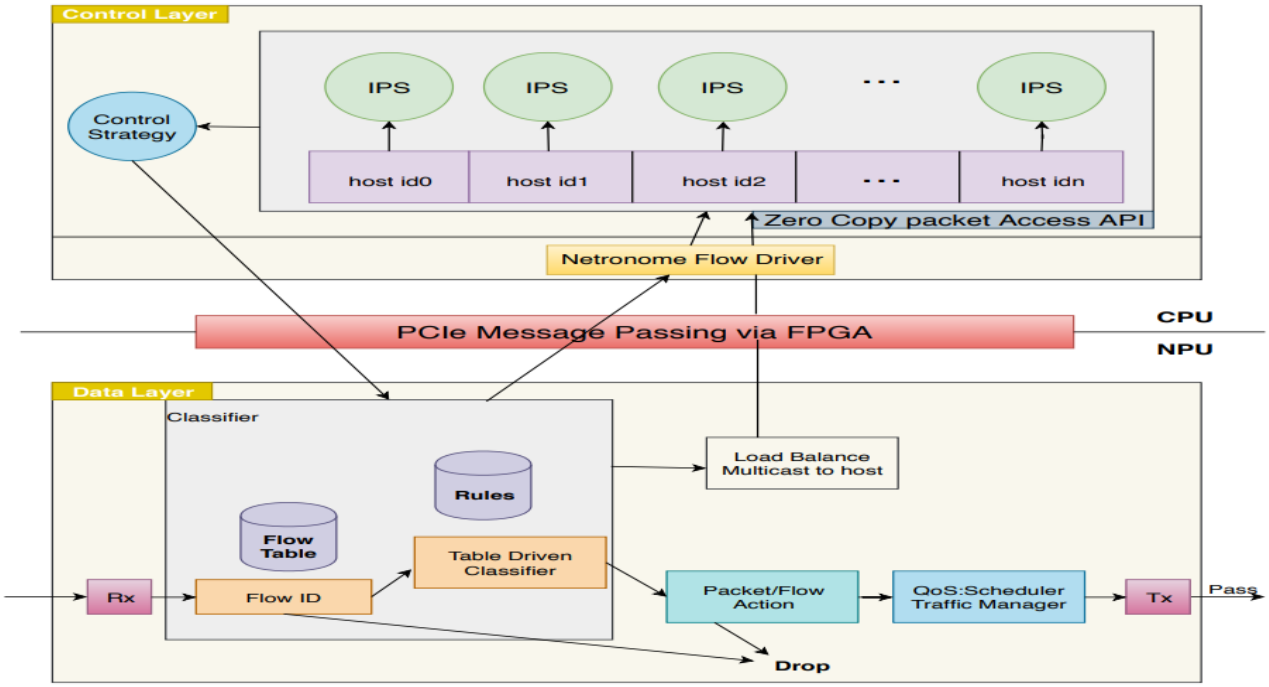

Fig. 2 The Architecture and Data Path of an IPS based for a multicore processor [22]

The IPS often sits directly behind a firewall and provides a complementary layer of analysis that checks for dangerous content. Unlike its predecessor the Intrusion Detection System (IDS) is a passive system that scans traffic and reports back on threats. The IPS, however, is placed in-line (in the direct communication path between source and destination), and is actively analyzes and takes automated actions on all traffic entering the network. These actions include specifically [17]:

1. Dropping the malicious packets
2. Blocking traffic from the source address environment
3. Resetting the connection

As an in-line security component, the IPS must work efficiently to avoid degrading network performance. It must also work fast enough due to the fact that exploits can occur in near real-time. The IPS must also detect and respond accurately, so as to eliminate threats and minimize false positives (legitimate packets misread as threats).

3. Techniques Used By the IPS

The IPS uses some techniques on data collected from the data stream flowing from/to a computer network. The following sections details those techniques.

3.1 The Signature Technique

A Signature based method is one in which a protective action is triggered if the incoming traffic contains a specific “signature” or follows a given pattern. As an example, if the coming traffic contains a given string such as /usr/passwd or performs a given action that is not performed during the normal system operations such as accessing the shell command (which is not a common

practice in graphical operating systems such as Windows). Accordingly, an IPS system needs to scan the incoming network traffic packet by packet searching for such signatures. The known signatures are normally stored in the system a priori in a database, which means that new attacks will not be detected until they actually occur. There are two types of the signature method of IPS; the atomic and the stateful methods. In the atomic method, the IPS system checks each packet individually without paying any consideration to the context of this packet. In other words, the prior and the following packets are not checked. In the stateful technique however, each packet is checked and an action is triggered if a given pattern is notices on several packets in a sequence. An example of the stateful signature is the denial-of-service attack which is detected if the analysis of a sequence of packets yielded the same command (and that matched a known attack that is stored in the database). Some examples of signature matching include also looking into an email subject or a file attachment name or user authentication patterns [13]. The advantage of the atomic is that it is simple and easy to use even if the number of registered attacks is large since the previous state needs not be stored. Upon identifying new attack signatures, the database needs to be updated.

3.2 The Profile Technique

In the profile method, an initial secure and controlled network is setup and the IPS collects a pattern of data stream flowing to and from that system or network. This pattern is treated as a baseline profile and the real-time data stream patterns are compared against it. If a real-time data stream pattern that is found to be suspiciously different from the baseline profile, it is treated as an attack and accordingly preventive action is taken. A standard baseline profile can represent normal behavior of things such as network connections, users, applications, and hosts. For example, if a real-time data stream is observed to be accessing a crucial system file that wasn't accessed when the baseline profile was generated in the controlled environment, this attempt is treated as malicious [13].

3.3 The Stateful Protocol Technique

Stateful means the system is a state aware: The same input can produce different output based on other information in the system, such as information stored from earlier or data collected from other sources.

The stateful traffic analysis is the process of profiling normal protocol activities as a sequence of events while each packet in the traffic is not treated in isolation from the previous and the following packets. The resulting profile is labeled as the normal profile and incoming packets are compared to it during the traffic analysis process. If a deviation is noticed then a corrective action is triggered by the IPS. Various IPS vendors developed universal profiles that specify how a protocol should or should not be used [13]. The word stateful in a stateful protocol means that IPS system records and keeps track of the of the states of the transport, the network and the application. Traffic analysis using stateful IPS yields the capture of unexpected sequence of events such as the issuing of a given sequence of commands (that are recorded to be malicious) or a given command that is issued out of context (if another command should have been issued first)

4. IPS Deployment Options

Deploying an IPS system (also known as IDPS, Intrusion Detection and Prevention Systems) means how and where to install it and get it to work on a computer system. There are two distinct deployment methods for an IPS; the host-based and the network-based. The following sections give some details about each deployment method.

4.1 Host Based IPS

As the name indicates, a host-based intrusion prevention system consists of a software program that is installed on individual servers of the network. The IPS can be thought of as intrusion detection system and a firewall. An intrusion detection system logs malicious activities and alerts user of their possible occurrence. A host-based IPS has preprogrammed policies and rules that it compares traffic to. Any violation to these rules triggers an action by the IPS. Such action can be in the form of blocking all traffic form a suspicious IP address or block the incoming traffic from to that port. The IPS proactively protect a computer system form malicious attacks. Despite their higher cost, HIPS provide a viable reliable intrusion prevention system. The following sections presents some commercially available IPS systems.

4.1.1 Storm Watch

OKENA's [4] Storm Watch uses a intelligent agents and works at the kernel based. It hocks into the kernel and intercepts system calls and captures suspicious behavior. It can be installed on servers and workstations. Storm watch does not adopt the signature approach and does not require a prior knowledge of an attack profile. It uses proactive rather than reactive approach to prevent an intrusion before it occurs. It prevents malicious behaviors such as buffer overflow, network warms, Trojan hours and SYN flood attacks. Storm watch has four components that work on various aspects of the system. As an example, one components works on the file system and its function is to intercept file reads/writes requests. Another component works at the network level and interceptor packet events at the driver or transport levels. The other two components

are the Configuration and the execution space interceptors which work at the Windows registry level or on files for the Unix based system and the memory writes respectively

4.1.2 Entercept

Entercept is a host-based intrusion prevention system that was acquired by McAfee in 2004. Entercept works on the operating system and the application level to detect threats. It can detect unauthorized access to critical files, directories, or registry keys and applications. Due to the nature of its operation, Entercept introduces delays and some performance degradation to the server it hosts. This delay, however, is the price to pay for preventing possible malicious attacks. The delay is claimed to have no noticeable effect at the user side.

4.2 Network Based Intrusion Prevention System

The network intrusion prevention system (NIPS) differs from the host-based in that it is installed in-line as opposed to being installed on a host. It therefore interjects the incoming traffic to the network and hence is able to analyze it at the packet level. An NIPS has two main components, a pattern matching engine and a subliminally classification engine. Figure 3 shows a diagram of the NIPS.

Fig. 3. The Network-Based Intrusion Prevention System

The way that the NIPS works is that it analyzes each packet searching for known signatures stored in the NIPS database. Several vendors exist for NIPS such as Cisco, Intel, HP, McAfee, Juniper Networks and IBM. As an example, Cisco provide the IOS NIPS with features such as the ability to store up to 7000 signatures that are downloadable form their website.
Due to the nature of its functionality, the NIPS introduces delay to the network due to the time consumed in checking every packet against thousands of signatures. NIPS therefore need to possess high performance computation capability and are usually in the form of hardware chips. A Ternary Content Addressable Memory (TCAM) chips are usually used to run IPS algorithms. The work by [21] presents a Routing TCAM (RTCAM) pattern matching algorithm where the TCAM chip is used to store the signatures.

4.3 Wireless IPS

Wireless intrusion prevention systems (WIPS) provides protection for wireless networks against rouge wireless access points. It is deployed in either a software application or in the form of a hardware device. The WIPS scans the wireless radio spectrum for unauthorized activities. It checks the MAC address of devices connected to the network against unauthorized devices. Some attackers might be able to spoof the MAC address of an authorized device and in these cases the WIPS uses fingerprinting techniques to weed out any of those devices. A device fingerprint is a characteristic of the emitted radio signal of a given device that cannot be regenerated by an intruding device. The WIPS consist of three main components: 1) wireless sensors that are spread across the wireless network and that are arranged in a way to cover the entire active wireless space of the network. These sensors scan the wireless spectrum automatically searching for possible intruders. Usually users define their own operating policies for the wireless network. 2) A WIPS server that centrally analyses the packets from the sensors and correlates them with the predefined wireless policy and classifies that threat if it is. The server is either alerted of the threat or it acts automatically if the policies are defined as such. 3) A console that provides a user interface for reporting or administrative purposes. The aforementioned method of deploying the WIPS is called an overlay WIPD. Another way to deploy WIPS is by integrating the searching for rouge packets into the wireless access point. This method is called the ”time-slicing WIPS”. This method require that the access point does a double duty which requires a more sophisticated hardware. A yet third method to deploy the WIPS is called the ”integrated WIPS”. In this method, the sensors are integrated into the authorized access points and continually search the spectrum for unauthorized access point [17].

5. Available IPS Systems

5.1 Commercial

There are several vendors for commercial IPS systems that offer the service with various flavors. The list of vendors include communications giants such as Cisco and Huawei. Other vendors also exist such as McAfee, IBM, Trend

Micro and Wins. The following is a list of the products offered by those vendors.

- McAfee Network Security Platform by McAfee.
- FirePOWERTM Next-generation IPS (NGIPS) by Cisco.
- IBM Security Network Intrusion Prevention System by IBM
- TippingPoint Next-Generation Intrusion Prevention System by Trend Micro [5]
- Sniper IPS by Wins [6]
- NIP6000 Next-Generation Intrusion Prevention Systems by Huawei.

In this section a brief coverage of some of the systems listed above.

5.1.1 The CISCO Adaptive Security Appliance

Cisco provides commercial device family called the Adaptive Security Appliance (ASA). The device comes with its embedded software that combines firewall, anti-virus, intrusion prevention and virtual private network capabilities. Various device sizes are offered depending on the size of the target network and the traffic involved. The core software of the device is based on Linux operating system [11].

5.1.2 FirePOWERTM Next-generation IPS (NGIPS)

In 2013, Cisco invested over $2.7 billion to acquire SourceFire, a leading next generation firewall (NGFW) producer. Initially there were two interfaces for the firewall, one for the ASA and another for FirePower of SourceFire. Eventually Cisco decided to merge the two interfaces and produce the FirePower threat defense. The Next-Generation intrusion prevention system (NGIPS) is the new intelligent solution for intrusion prevention. It continuously collects information about the operating systems, mobile devices, files, application and users. This enables the device to provide necessary contextual information regarding preventing possible threats. This NGIPS provides protection against known and unknown threats. Its main features are:

- IPS rules that recognize and block attack traffic that target network vulnerabilities.
- Tightly integrated defense against advanced malware incorporating advanced analysis of network and endpoint activity
- Sandboxing technology: this technology uses a large number of behavioral indicators to identify evasive and zero-day attacks.

5..1.3 McAfee Network Security Platform

The McAfee network security platform is, as claimed by its vendor, a next generation IPS. Unlike the traditional signature-based methodology, the McAfee network security platform works with layered signature-less technology that detects threats that has never been seen before. It also uses user data, device data and application data to provide contextual analyses and combines it with real time McAfee Global Threat Intelligence feeds to protect against unknown threats. The platform can scale up to 40 Gbps. Some of the features of this system are listed below:

- Advanced threat prevention: by providing outbound SSL decryption and Mobile threat reputation and cloud analysis.
- Botnet and malware callback protection: by providing DNS sinkholing and Heuristic bot detection.
- DoS and DDoS prevention by providing host-based connection limiting.

5.2 Free Software

5.2.1 The Multi Router Traffic Grapher (MRTG)

The Multi Router Traffic Grapher is graphics based free software that is used to monitor and measure the traffic load on a given network. Its is licensed under the GNU GPL. It is written in Perl and works on Linux/Unix or Windows operating systems. It also work on Netware Systems. The data generated by this software is embedded into HTML files and can be viewed from any web browser. By default MRTG works for IPv4, but can be enabled to work for IPv6 [7].

5.3 Open Source Software

There exist numerous open source systems for intrusion detection and prevention. These systems support windows and/or Linux operating systems. Some of these systems are host based (HIDS) while others are NIDS. The following are some examples of existing such systems:

5.3.1 Open Source Security (OSSEC)

This is one of the most popular intrusion detection systems and is owned by Trend Micro is currently maintained by AtomiCorp. This system is available on Unix like systems (Linux – Solaris - AIX) and is freely available. OSSEC consists of multiple components. The main ones are the Manager and the agents. The manager is a central entity that receives and analysis events and syslogs from the agents. It stores the rules, decoders and major configurations. The agents are small program(s) that are installed on the devices to be monitored Agents collects information from the hosting device and forwards it to the manager for analysis and correlation. These agents have small memory footprint and CPU utilization thereby not

overloading the hosting device. Agents connect to the manager on UDP port 1514. OSSEC can be integrated with a variety of firewalls, switches and routers and can receive logging info from these devices. Examples of devices supported are Cisco routers, Cisco PIX, Juniper routers and others.

5.3.2 Snort

Snort is an open source network intrusion prevention software. Snort is able to perform packet analysis and network monitoring for IP networks. It was created by Martin Roesch in 1998 and now is maintained and developed by Cisco after acquiring SourceFire. Snort is able to prevent against attacks such as buffer overflow, operating system fingerprinting, Denial of Service and many other attacks. The software is written in C programming language and can run on Linux boxes such as Fedora, OpenBSD, and Ubuntu. It can also run on Windows and Centos. Snort comes with a set of rule categories that a system administrator can choose from in order to configure how the system deals with possible threats. Examples of these rules are:

- Blacklist rules: This category includes IP addresses, URLs, and DNS rules that indicate a possibility of malicious behavior.
- file-executable: This category includes vulnerabilities delivered through executable files.
- malware-tools: This category includes rules that identifies tools that can be considered malicious in nature (e.g. LOIC).

There are various ways to deploy Snort. It can either be deployed before or after the firewall. Deploying a Snort sensor before the firewall enables the network administrator to monitor all traffic coming in to the network including possible malicious packets. Installing the sensor right after the firewall shows the traffic after being filtered by the firewall. This arrangement could be used to measure the firewall performance and identify any deficiencies. In many cases and to reduce cost, the Snort sensor is installed on the firewall itself [18]. The following is a list of advantages and shortcomings of Snort [20].

Advantage

- Free to download and is open source.
- Easy to write rules for intrusion prevention.
- It has high flexibility.
- Good community support for solving problems and is under rapid development.

Disadvantage

- It is based on command line. No GUI interface for rule manipulation.
- It is relatively slow in processing network packets.
- Cannot detect a signature split over multiple TCP packets, which occurs when packets are configured in inline mode.

5.3.3 Suricata

The Suricata Engine is a fairly new open-source intrusion detection and prevention engine released in 2010. It is developed by Open Information Security Foundation (OISF), which is a non-profit foundation supported by the US Department of Homeland Security (DHS) and a number of private companies. Suricata is compatible with most operating systems (e.g. Linux, Mac, FreeBSD, UNIX and Windows). The Suricata Engine is available to use under the GPL v.2 license. The operation modes of Suricata are the same as Snort's. It can be used either as an IDS or IPS system. There are no differences when connecting Suricata to the network. Suricata even has basically the same rule syntax as Snort (although not 100%), which means that both systems can use more or less the same rules [19].

Advantage

- This product performs network traffic processing at the seventh layer of the OSI model. This helps enhance its capability to detect malware activities.
- It automatically detects and parses protocols like IP, TCP, UDP, ICMP, HTTP, TLS, FTP, SMB and FTP so that rules apply on all protocols.
- It has some advanced features such as multi-threading and GPU acceleration.

Disadvantage

- This product has less support as compared to other IPSs like Snort.
- It is also complicated in its operation and requires more system resources for full-fledged functionality.

6. Conclusions

Cyber security has been and continues to be an important and central topic for organizations and corporations. If special care, money and enough resources are not dedicated for the purpose of protecting and ensuring the security of the network consequences can be catastrophic. Covering this topic requires the addressing of the detection and prevention aspects of cyber security. Due to their importance and generality, this work is dedicated to cover the intrusion prevention systems. Various systems exist that employ different techniques. Some of these systems

use a "normal" traffic/data pattern as a baseline and deviation from this pattern is considered to signal an intrusion (the profile technique). Other techniques include the signature technique which stores predetermined malicious patters and search the traffic for any similarities. Deployment of IPS can vary. Some of them are host-based while others are network based. Moreover, there exist commercial systems as well as open source systems (such as SNORT). Comparison of these systems, their advantages and disadvantages have been provided in this work.

References

[1] University of Mariland Available from:https: //eng.umd.edu/news/story/ study-hackers-attack-every-39-seconds - [Accessed - 21 July 2019]

[2] Juniper Research Available from: https://www.juniperresearch.com/ researchstore/innovation-disruption/ cybercrime-security - [Accessed - 21 July 2019]

[3] Wills Tower Watson Available from: https: //www.willistowerswatson.com/ – [Accessed: 21 July 2019]

[4] Okena Intrusion Prevention Software Available from: https: //www.networkworld.com/article/ 2339500/cisco-acquires-okena.html - [Accessed: 22 Sept. 2019]

[5] Trend Micro Available from: https://www.trendmicro.com/ - [Accessed: 28 Sept. 2019]

[6] Wins Co., Ltd Available from: http://www.wins21.co.kr/en/main/ main.html - [Accessed: 28 Sept. 2019]

[7] Multi Router Traffic Grapher Available from: https://oss.oetiker.ch/mrtg/ - [Accessed: 28 Sept. 2019]

[8] SNORT Software Available from: http://www.snort.com – [Accessed: 3 July 2019]

[9] McAfee Network Security Platform Available from: http://www.mcafee.com – [Accessed: 18 September 2019]

[10] The Open Source HIDS SECurity (OSSEC) Available from: https://www.ossec.net/ - [Accessed: 20 July 2019]

[11] Cisco Corporation Available from: https://www.cisco.com/ - [Accessed: 20 July 2019]

[12] Oath of Vorison Available from: https://www.oath.com/press/ yahoo-provides-notice-to-additional -users-affected-by-previously/ - [Accessed: 18 September 2019]

[13] Dr. K. Prabha1, S. Sudha sree2. (2016) "A Survey on IPS Methods and Techniques" In: International Journal of Computer Science Issues, Volume 13, Issue 2, March 2016.

[14] Filip Hock, Peter Kortis, Slovakia, ˇ (2019)"Commercial and open-source based Intrusion Detection System and Intrusion Prevention System (IDS/IPS) design for an IP networks" In: Conference Paper · November 2015 DOI: 10.1109/ICETA.2015.7558466vember 2016]

[15] The Paloalto Netwrok: What is an intrusion prevention system. Available from: www.paloaltonetworks.com/cyberpedia/ what-is-an-intrusion-preventionsystem-ips - [Accessed: 21 July 2019]

[16] What is DOT com Wireless Intrusion Prevention System. Available from:https://whatis.techtarget.com/ definition/WIPS-wireless-intrusionprevention-system - [Accessed: 21 July 2019]

[17] The basics of Network Intrusion Prevention Systems. Available from: https://searchsecurity.techtarget.com/feature/ The-basics-of-network-intrusionprevention-systems - [Accessed: 21 July 2019]

[18] Best open source network intrusion detection tools, Available from: https://opensourceforu.com/2017/04/best-open-source-network-intrusiondetection-tools/.

[19] Mauno Pihelgas (2012). "A Comparative Analysis of Opensource Intrusion Detection Systems" In: TallInn University of Technology, ITI70LT.

[20] Sonali Nemade, Madhuri A. Darekar, Jyoti Bachhav, Sunanyna Shivthare "A Comparative Study of Intrusion Detection System tools and Techniques" In: International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 8, August 2017.

[21] Weinsberg, Yaron and Tzur-David, Shimrit and Dolev, Danny and Anker, Tal "High performance string matching algorithm for a network intrusion prevention system (nips)" In: 2006 Workshop on High Performance Switching and Routing, 2006.

[22] Yueai, Zhao, Hou Pengcheng, Ling Wang, and Han Suqing. "High-performance Architecture of Network Intrusion Prevention Systems." EAI Endorsed Transactions on Scalable Information Systems 1, no. 3 2014.

Mohammad A. R. Abdeen received the M.S. and Ph.D. degrees in Electrical and Computer Engineering from the University of Victoria, and the University of Ottawa, Canada respectively. He assumed numerous academic and industrial positions in international organizations. He is currently an Adjunct Professor at the University of Ottawa and an Associate Professor at the Islamic University of Madinah, Saudi Arabia**.**