Volume 3, Issue 9, September 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

IPS for Wireless LANs at Layer 3

Prof S V Athawale *

Department Of Computer Engineering& Pune
Pune, India

Prof Dr D N Chaudhari

Professor and Dean, Computer Engineering,
JDIET & Amaravti, India

Abstract— ***Wireless network is one of the fastest growing interests in today's modern world. Communication and data transfer over internet have seen a phenomenal rise in the recent years. This is where malicious attackers try to breach into the wireless network as it is easy to compromise. The IP and MAC address can be spoofed with the tools available. However, it is not a topic of interest for many to secure wireless networks. We propose our paper to secure wireless networks using more than one parameter to make it difficult to break-in the security. We use IP address, MAC address and SSID to identify the authorized users in the Wireless network and prevent the unauthorized ones from accessing network by focusing on network payload, time complexity and latency.***

Keywords— ***Intrusion Prevention System (IPS), Wireless LAN, IP Address, MAC Address, Secure Set Identifier (SSID)***

I. INTRODUCTION

Network security is one of the major issues for many people around the world. Data security is one thing on which no one would compromise. With the increase in network usage for many important purposes, many malicious attackers try to breach in the security for their cruel purposes. All this have been a major issue for many. The level of security that system offers is not sufficient because of the tremendous development in malicious and spiteful software like Trojans, key loggers and root kits. The drawbacks inherent in current defenses have led to rise in a new category of network security known as Intrusion Prevention Systems (IPS). An Intrusion Prevention System is a network device/software that goes deeper than a firewall to identify and block network threats by assessing each packet based on the network protocols in the network layer, the context of the communication and tracking of each session.

Intrusion Prevention Systems (IPS) can be considered as an extension of firewalls with extra security. A considerable improvement upon firewall technologies, IPS makes decisions for access control based on application content, not on IP address or ports as traditional firewalls had done. IPS is a down to business defense mechanisms designed to detect malicious packets within normal network traffic and stop intrusions dead, blocking the aberrant traffic automatically before it does any damage rather than simply giving an alert as, or after, the malicious load has been delivered. Intrusion prevention systems were invented independently to resolve ambiguities in passive network monitoring by placing prevention systems in-line on the network monitoring and the incoming packets based on certain prescribed rules (which can be tweaked by the security administrator) and if any bad passage is detected, the same is dropped in real-time. It is helpful to sense and prevent attacks like DoS/DDoS attacks, vulnerability detection, brute force attacks protocol anomaly detection and prevention unidentified attacks. IPS technologies are typically session based and traffic flow is examined based on session flow. To cut a long story short, the most essential thing you should remember about system security is to start with prevention [1]. Threats to WLAN are numerous and destructive. WLANs are not only susceptible to TCP/IP-based attacks, they are also subject to a variety of 802.11-specific threats [1]. Because of the importance in providing ubiquitous services and the inherent vulnerability due to broadcast nature of the wireless medium, the wireless local area networks (WLANs) are being targeted of a variety of attacks [2].

II. RELATED WORK

In the last few years, researchers have been actively exploring many mechanisms to ensure the security of control and data traffic in wireless networks. These mechanisms can be largely categorized into the following classes—authentication and integrity services, protocols that depends on path variety, protocols that use specific hardware, protocols that require explicit acknowledgments or use statistical methods, and protocols that overhear neighbor communication[3]. The unauthorized users are deployed in secure WLANs without permission or knowledge of the network administrator. The presence of such unauthorized users poses severe threats to the WLAN security as it could compromise security of the entire wireless LAN network. This problem has been in existence ever since WLANs have become popular in commercial applications.

III. INTRUSION PREVENTION SYSTEM

Nowadays the development of network security technology involves three stages. These stages are: Firewall, IDS (Intrusion Detection System) and IPS (Intrusion Prevention System). An intrusion prevention system is a good solution for improving network security to integrate the advantages of firewall and IDS properly. It can not only detect malicious attempts at accessing, operating through the network, but also react to block or prevent those activities in real-time. So an IPS combines the blocking capabilities of a firewall with the deep packet inspection of IDS, and mostly it can still prevent the attack from being successful. In June 2003, Gartner Incorporated released a report entitled "Intrusion Detection Is Dead. Long Live Intrusion Prevention !" In this document, Gartner vice president of research Richard Stiennon said: "Intrusion prevention will replace intrusion detection. Enterprises should delay new large investments in intrusion detection systems which have failed to provide additional security until intrusion prevention systems emerge that provide a stronger defense against 'cyber attacks'[6]. There are different intrusion prevention systems well applied in wired network, but implementing a wireless IPS encounters many difficulties. In WLAN environment, attackers or intruders can discover more ways to intrude a wireless system, so that wireless networks are vulnerable to such intrusions. Under wireless condition, IPS has additional deployment requirements as well as some unique features specific to WLAN threats [4].

Wireless IPS

Wireless LAN is subject to a variety of threats. At the present time, there are the following dangerous threats to WLAN [7]. First, because WLAN uses radio waves, this wireless technology provides a convenient way of connecting lots of computers to a network without using wires. By reason of the openness of wireless network, an attacker using the wireless card and Wi-Fi detection tool can easily discover any access point all around. For instance, war-driving using Net Stumbler will present attackers with the network identification, wireless channel, and encryption information and so on. After locating a wireless network, attackers can try to exploit it.

Second, 802.11 WLAN is also subject to DoS (Denial of Service) attack, in which the attacker attempts to make the target network unable to serve its legitimate users. Hackers can launch malicious DoS attacks by authentication flood, association flood, de-authentication flood, disassociation flood and so forth. These attacks are so effective against wireless networks that the normal users can not access WLAN successfully.

Third, although 802.11 WLAN supplies a series of encryption and authentication methods such as WEP, WPA and WPA2, these methods are both weak and insufficient. WEP encryption provides data integrity checking for wireless packets, but research has indicated that 64-bit and 128-bit WEP key can be both easily decrypted via Backtrack tool. Even if WPA/WPA2 authentication is utilized on WLAN, an attacker can also potentially decrypt the key via Aircrack tool.

Last, all WLAN devices are equipped with MAC addresses installed for the wireless interface. But many tools can allow a hacker to spoof the MAC address to pose as an authorized AP thereby getting the victim stations associate to him. MAC hiding is the first step in creating a MITM (Man in the Middle) attack or an attack known as "evil twin". Some important data such as password and account can be revealed through eavesdropped packet. Thus, it is very much necessary to secure MAC address as well.

To aid in the detection and defense of these potential wireless threats, WLAN should employ an intrusion prevention system, which must be a very good solution to reduce false positives and improve detection performance[4].

OBJECTIVES OF THE PAPER

Many surveys reveal that the top eight threats experienced are viruses, system penetration, DoS, insider abuse , spoofing, data/network sabotage, and un-authorized insider access.

Although majority of them use firewalls it is apparent that firewalls are not always effective against many intrusion attempts. The average firewall is intended to reject clearly suspicious traffic - such as an attempt to telnet to a device when corporate security policy forbids telnet access completely - but is also designed to allow some traffic. Our aim is to detect and prevent intrusion in the wireless network. We propose our system for the host base scenario. A host-based IPS monitors the characteristics of a single host and the events occurring within that host for doubtful activity. Examples of the types of characteristics a host-based IPS might monitor are wired and wireless network traffic (only for that host), system logs, file access, system and application configuration changes and running processes and modification.

We are proposing the system which primarily focuses on the following aspects:

 Identifying security policy problems:

An IPS can provide some degree of quality control for security policy implementation, such as duplicating firewall rule sets and alerting when it sees network traffic that should have been blocked by the firewall but was not because of a firewall configuration error and when an unauthorized user is tracked.

 Documenting the existing risk to an organization:

IPSs log information about the threats that they notice. Understanding the frequency and characteristics of attacks against an organization's computing resources is helpful in identifying the appropriate security measures for resource protection. The data can also be used to instruct management about the threats that the organization faces.

To prevent individuals from breaking security policies:

If individuals are alert that their actions are being monitored by IPS technologies for security policy violations, they may be less likely to commit such violations because of the risk of detection.

 Recording information related to observed events.

Information is usually recorded locally, and might also be sent to different systems such as security information and event management (SIEM) solutions, centralized logging servers and enterprise management systems [5].

 Notifying security administrators of important observed events.

This notification, known as an alert, occurs through several methods, including the following: messages, pages, e-mails on the IPS user interface, Simple Network Management Protocol (SNMP) traps, syslog messages, and user-defined programs and scripts. A notification message typically includes only basic information regarding an event; administrators need to access the IPS for additional information [5].

- **Producing reports.**

Reports summarize the monitored events or provide details on particular events of interest [5]. Our main objective is to prevent intrusions in the host based systems using various parameters like IP Address, MAC Address and SSID to secure networks by focusing on network payload, time complexity and latency.

SYSTEM SCENARIO AND WORKING

A host-based IPS monitors the characteristics of a single host and the events occurring within that host for doubtful activity. Examples of the types of characteristics a host-based IPS might monitor are wired and wireless network traffic (only for that host), system logs, in succession processes, file access and alteration, and system and application design changes.

Components

This section describes the major components of typical host-based IPSs and illustrates the most common network architectures for these components. It also provides recommendations for selecting which hosts should use host-based IPSs. This section also describes how host-based IPSs can affect a host's internal architecture, such as intercepting process calls.

Typical Components

Most host-based IPSs have detection software known as agents installed on the hosts of interest. Each agent monitors activity on a single host and if IPS capabilities are enabled, also performs prevention actions.

The agents transmit data to management servers, which may or may not use database servers for storage. Consoles are used for supervision and monitoring.

Some host-based IPS products use dedicated appliances running agent software instead of installing agent software on individual hosts. Each piece of equipment is positioned to monitor the network traffic going to and from a particular host. Technically, these equipments could be considered network-based IPSs, because they are deployed inline to monitor network traffic. However, they usually observe activity for only one specific type of application, such as a database server or Web server, so they are more specialized than a standard network-based IPS. Also, the software in succession on the appliance often has the same or similar functionality as the host-based agents. Therefore, host-based IPS products using appliance-based agents are included in this section.

Each agent is typically intended to protect one of the following:

A server: Besides monitoring the server's operating system (OS), the agent may also monitor some common applications.

A client host (desktop or laptop): Agents designed to monitor users' hosts usually monitor the OS and common client applications such as e-mail clients and Web browsers.

An application server: Some agents perform monitoring for a specific application service only, such as a database server program or a Web server program. This type of agent is also called as an application-based IPS.

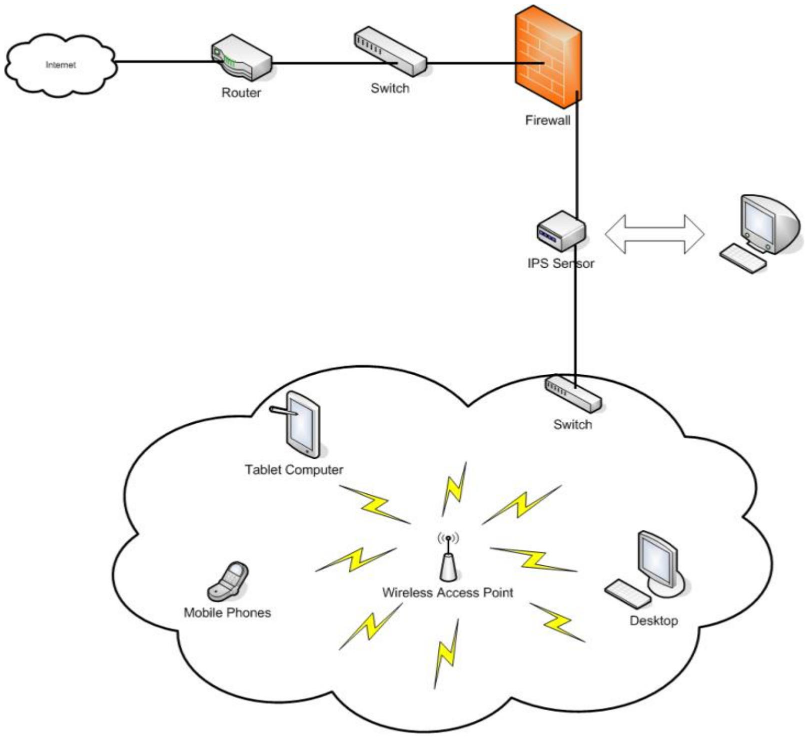

Fig. 1 Architecture of IPS

TABLE I
COMPARISON CHART

Parameter	Existing system	Our system
Time Complexity	O(n) Greedy approach	O (nlogn) Divide and conquer approach
Network Latency	Marginal	Negligible

IV. CONCLUSIONS

The traditional IPS uses the old technique of Centralized RF Scanning, SSID scanning, hence generating lots of network traffic. Also the previous techniques are unable to detect the intrusion which uses internal compromised proxies to hide them. We propose our system to take wireless network security to a higher level by considering various parameters like reduced network payload, low latency and less time complexity which increases the performance of the wireless networks significantly. Our proposed system takes advantage of Divide and Conquer algorithm hence making our system more efficient. The model will make it easier to implement well organized network management system. It can satisfy the need of future computing.

ACKNOWLEDGMENT

First and foremost, I would like to thank Dr. D N Chaudhari for his most support and encouragement. He gently read my paper and offered precious detailed advices on motivate, organization, and the theme of the research paper.

REFERENCES

[1] Guanlin Chen1, 2, Hui Yao1, Zebing Wang1, “Research of Wireless Intrusion Prevention Systems based on Plan Recognition and Honeypot”. 1.School of Computer and Computing Science, Zhejiang University City College, Hangzhou,310015, China. 2.College of Computer Science, Zhejiang University, Hangzhou, 310027, China.

[2] Suman Jana and Sneha K. Kasera, “On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews”, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 3, MARCH 2010.

[3] Issa Khalil, Member, IEEE, and SaurabhBagchi, Senior Member, IEEE “Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasures”, ieee transactions on mobile computing, vol. 10, no. 8, august 2011.

[4] Guanlin Chen1, 2, Hui Yao1, Zebing Wang1 “An Intelligent WLAN Intrusion Prevention System Based on Signature Detection and Plan Recognition”. 1.School of Computer and Computing Science, Zhejiang University City College, Hangzhou, 310015, P.R. China. 2.College of Computer Science, Zhejiang University, Hangzhou, 310027, P.R. China.2010,Second International Conference on Future Networks.

[5] Karen Scarfone PeterMell ”Guide to Intrusion Detection and Prevention Systems (IDPS) “,National Institute of Standards and Technology Gaithersburg, MD 20899-8930 February 2007.

[6] Timothy D. Wickham, “Intrusion detection is dead. Long live intrusion prevention!” www.sans.org/reading_room/whitepapers/detection/1028.php, 2003.

[7] KenHutchison,“Wireless Intrusion Detection Systems,” http://www.sans.org/rr/whitepapers/wireless