Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Network Security by Controlled Access in WLAN

Amogh Bhongale
Department of Computer Engineering
AISSMS College of Engineering
Pune, Maharashtra, India

Mehak Koul
Department of Computer Engineering
AISSMS College of Engineering
Pune, Maharashtra, India

Susmit Bansod
Department of Computer Engineering
AISSMS College of Engineering
Pune, Maharashtra, India

Unmesh Dandekar
Department of Computer Engineering
AISSMS College of Engineering
Pune, Maharashtra, India

S. V. Athawale
Department of Computer Engineering
AISSMS College of Engineering
Pune, Maharashtra, India

Abstract— The incredible rise in the deployment of 802.3(LAN) and 802.11(WLAN) has been observed for the sake of recompenses like improved scalability and mobility of computer networks. This provokes illicit minds thus creating an indispensable issue of security. IP address and MAC address can play an important role in identifying such culprits. There are many such tools using which IP and MAC address can be easily spoofed. This is the basis for the delivery of network security techniques like IPS (Intrusion Prevention System). We propose this paper in which the approach is to first scan the complete network with the help of predefined applications or commands. To check and verify that everyone who is logging into the network is authorized user or not, we propose a new parameter which will be unique to each user.

Keywords— 802.3; 802.11; IP; MAC; IPS

I. INTRODUCTION

The world becomes a single large entity because of the huge usage of Internet these days. Internet has indeed become one of the basic needs for any human being. On the timeline of development of technologies in computer networks, there was an era in which Internet was accessed through physical wired connections but now-a-days, there is no pocket which does not have Internet in it. This has become possible just because of the stupendous rise in the development of wireless networks. To setup a wireless network is extremely easy. There is no need of a cable to pull, holes to drill, just bung in your wireless Access Point (AP), wireless connection manager be required to associate routinely, and you are online. sorry to say, but every other person who finds a place inside a broadcast range of your AP is also online along with you, and here trouble for you starts. Risks which have been identified from the use of Wireless Networks have shown that the five aims viz., security, confidentiality, veracity, availability, legitimacy and non-repudiation cannot be met. Methodology must be taken into account such as IP addresses, MAC addresses, SSID, WEP for defence. These techniques are used to provide a standard level of security. Even valuable information such as user account and plain password can easily be analyzed which will in turn lead to a chaotic wireless network environment. The present 802.11 WLAN encryption methods including WEP, WPA and WPA2 are all weak and insufficient. The wireless networks can also become vulnerable because of MITM (Man in the Middle). The sensitive information in the communication process is prone to deterioration if an unauthorized (rogue) Access Point (AP) is introduced into the wireless networks. Such innumerous issues put forth a challenge to the security of wireless networks and hence impel a new security technology known as Intrusion Prevention System (IPS). An Intrusion Prevention System is used in network security. It provides rules and policies for network traffic for alerting system or network administrators to block suspicious traffic, but allows the admin to take the necessary action upon being alerted. So the main proposition of our paper is to provide an efficient and reliable approach to detect and eliminate unauthorized hosts which try to sell out the security and confidentiality of wireless networks thereby enhancing the security and reliability of WLAN.

II. RELATED WORK

We have reviewed attacks on different top-level domains for year 2011. The total number of attacks occurred were 17306 out of which 9839 were only under .in domain only.

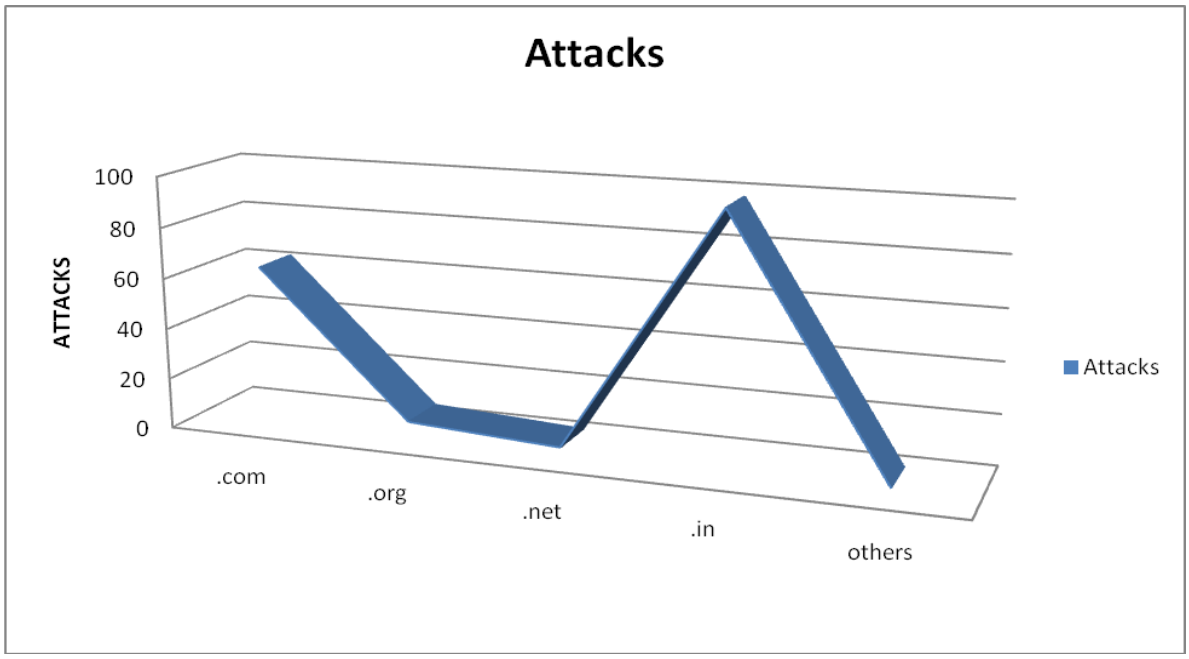

Fig. 1 Indian websites defaced during 2011 (Top Level Domains)

We also have reviewed the open proxy servers existing in India which do not hold any type of security. In all 3294 open proxy servers were tracked in the year 2011.

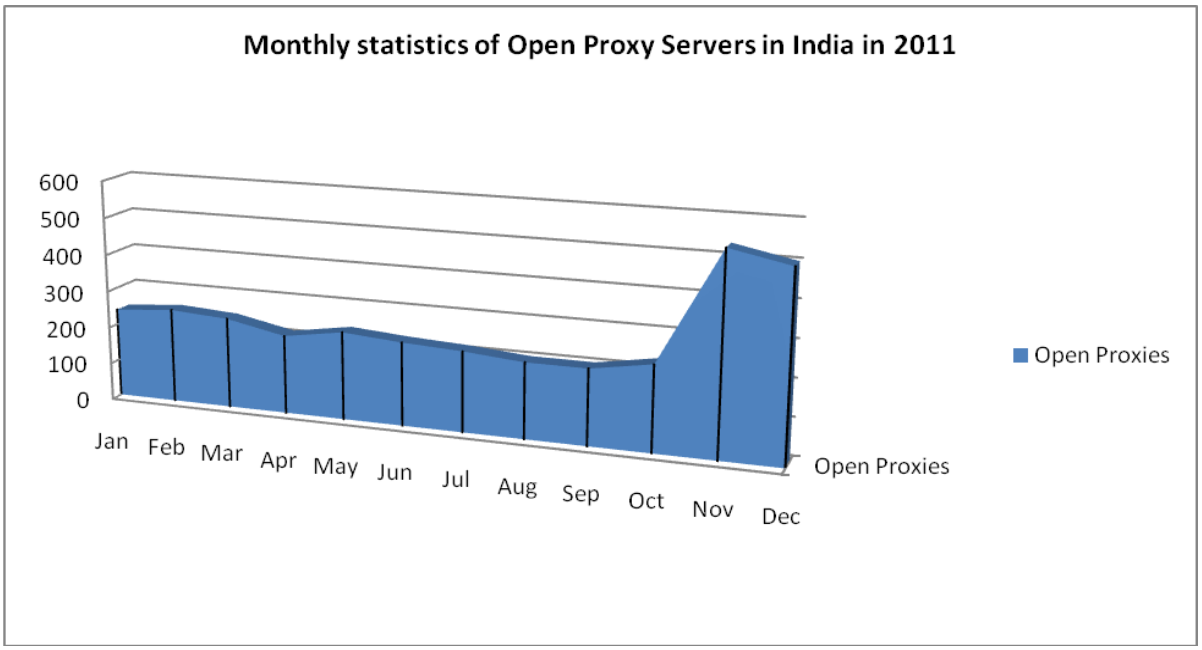

Fig. 2 Monthly statistics of Open Proxy Servers in 2011

The open proxy servers are very dangerous as it unknowingly results in the creation of rouge access points. Rogue Access Points (RAPs) is one of the leading security threats in current network scenario and if not handled properly in time, could lead from minor network faults to serious network failures. Rouge Access Points are the access points which are created without proper authorization. Most of the times authorized users mistakenly create these access points in order to assist the scalability of the network but this may lead to increase in the jeopardy to the network. Rogue APs are present on about 20% of all enterprise networks. Proper security is not maintained in Rogue Access Points due to which they turn out be loopholes to the network. If an illegitimate user is detected in the network, the access point through which he has entered into the network can be detected as rogue access point ([1], [5]).

The management frames which are sent by rogue access points can cause Denial of Service attacks on WLAN and even if the network is protected by top security protocols, they do not seem to accomplish the security measure up to the mark. For implementation, such techniques may require substantial changes in the standard and they do not seem to be useful when an internal node is compromised. Due to making extensive use of cryptography they can prove relatively expensive on mobile hosts [6].

A Toolset can be used to evaluate the performance and effectiveness of wireless intrusion detection techniques. Although some wireless intrusion detection systems (WIDSs) exist in the market, recent studies show that wireless networks are still vulnerable to complex, dynamic, and knowledgeable attacks [10]. There are some techniques in which an active intrusion detection system is installed at each access point which will detect intrusion at access point level. But if the same intruder tries to attack from another AP then all the work done by 1st access point will go in vain. And RAP will create problem for this system [3]. Some more tools are available like Intelligent Mobile Agent in which Mobile Agent System (MAS) must be installed on each machine in the network even if it is client. This leads to an increase in the complexity of the system as MAS needs to be installed on every client [2]. Firewall proves to be a good measure when security holds a priority for outside network but talking about inside network security, it does not seem to be a reliable option. Traditionally, firewalls depend on inside and external network topology. In many cases, systems/devices in an internal network are supervised and used for the attacks. So, firewall alone is not sufficient enough, IPS can use the blocking capacity of firewall and can prevent attacks successfully [4, 9]. Network security depends notably on network type. Wireless mesh network allows fast, easy and inexpensive network deployment however it is more vulnerable to various types of attacks. Stealthy packet dropping can be easily launched against multi hop wireless ad hoc networks ([7], [8]).

III. PROPOSED SYSTEM ARCHITECTURE

In our proposed system the emphasis is on the scanning phase as it stands as a guard to the network, by attending the users who are already logged in, into the network and the ones who want to access internet through the network. Any user, who is trying to access the internet, has to have go-ahead by the administrator. In our case the administrator is the Controller. All the users need to be registered with the controller. In the scanning phase the entire network is scanned and the data in the form of IP address, MAC address and the Unique Key which is provided by the administrator is brought together. Our proposed system will run the scanning of network continuously, so any user who comes into the network and asks for the internet will be detected and thus will be constrained to register with the controller.

The next phase in our anticipated system is report generation which is based on the data that is collected from the scanning phase. In this phase all the IP addresses and the MAC addresses collected are molded into a report and then it is provided to the Controller alias the administrator. The controller checks the report and then based on the data the users are validated, as valid or invalid. The valid users are prompted to provide their unique key, after their IP and MAC addresses are found valid. After providing the Unique Key the user is permitted to utilize the internet, after its entry in the database is found non-conflicting with the other entries in the database. The catalog of invalid users will be kept as a record to avoid any future consequences.

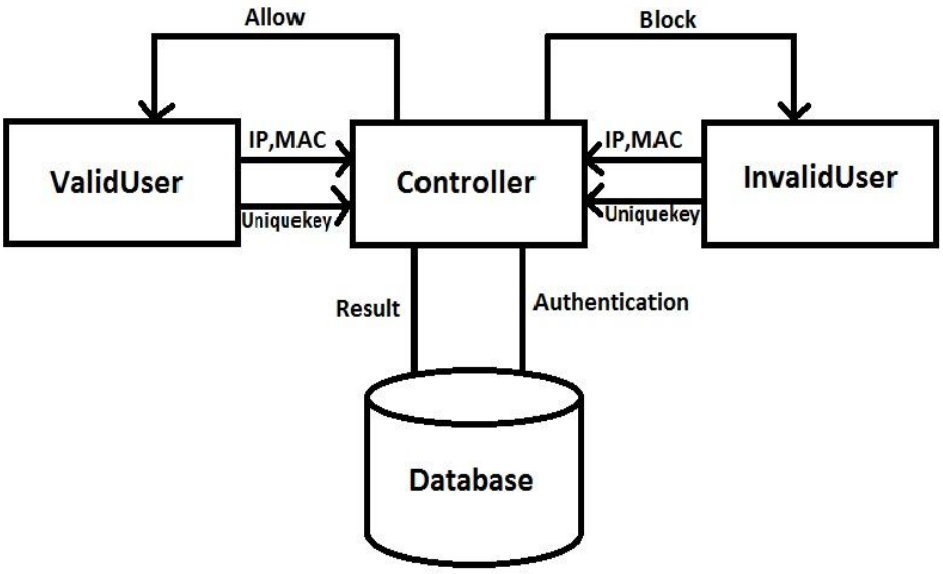

Fig. 3 Proposed System Architecture

A. *Different cases in our system*

Case 1: If the scanned IP and MAC addresses are NOT PRESENT in the database then such client needs to authenticate itself and obtain its own unique key.

Case 2: If the scanned IP and MAC addresses are PRESENT in the database then such client needs to provide its unique key whenever asked for.

Case 3: If any of the scanned parameters (IP or MAC) is found to conflict integrity constraints in the database then such client is assumed to be an intruder and will be blocked.

IV. CONCLUSIONS

This paper commences with the scrutiny of threat to the WLANs, then it overviews the existing intrusion prevention systems and limitations of them that have been tried to overcome. This proposed System keeps check of the entire network and keeps barrier on non invited users with the help of their own identity to prevent illicit usage of internet. Proposed system shall be considered as a model for keeping edge between users and network resources. It is believed the proposed will bring an effective and more reliable approach in network security. The way interest and research is growing its pace in the field of network security so as it is growing for IPS. Each system is abided for its update. In our upcoming considerations we are thinking to develop this system in such a way that along with the Internet even other network resources will have privileged access only.

ACKNOWLEDGMENT

This paper involves number of respected helping hands. We are grateful to Prof. S. V. Athawale for his dedication and valuable guidance. We would like to thank the Department of Computer Engineering, AISSMS COE, Pune for their uninterrupted help and support.

REFERENCES

[1] S.B.Vanjale, Amol K. Kadam and Pramod A. Jadhav, *Rogue Access Point Detecting & Eliminating in IEEE 802.11 WLAN*, International Journal of Smart Sensors and AdHoc Networks (IJSSAN) 2011.

[2] Hitesh Thawani, Vivek Waykule, Saket Raut, Geetsagar Pagare, and Shashi Athawale, *Detection and Elimination of Unauthorized Hosts using MA based WIPS*, International Journal of Computer Application 2013.

[3] Ming Lei, Yang Xiao and Susan V. Vrbsky, *Active Protection in Wireless Networking*, The 4th International Conference on Mobile Ad-hoc and Sensor Networks by IEEE Computer Society 2008.

[4] S. V. Athawale, Himgauri Shejvalkar, Priya Sankpal, Ankita Naik and Ashwini Pawar, *Enhanced Behavior of DF Using Intrusion Detection*, International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 3, March – 2013 ISSN: 2278-0181.

[5] S.V. Athawale and S B Vanjale, *802.11g Rouge Access Point Detection using MA*, International Journal of Computer Science and Communication (ISSN 0973-7391), Volume-II, Number-I of March 2011.

[6] Yaqing Zhang and Srinivas Sampalli, *IPS for Client-based WLANs*, 6th IEEE International Conference on Networking and Communications , Wireless and Mobile Computing 2010.

[7] Sahil seth and Anil Gankotiya, *Denial of service attacks an detection methods in Wireless mesh networks*, International conference on recent trends in Information, telecommunication and computing, 2010.

[8] Issa Khalil and Saurabh Bagchi, *Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure*, IEEE transactions, August 2011.

[9] Samer Fayssal and Byoung Uk Kim, *Performance Analysis Toolset for Wireless Intrusion Detection Systems*, IEEE transactions, 2010.

[10] Guanlin Chen, Hui Yao and Zebing Wang, *An Intelligent WLAN Intrusion Prevention System Based on Signature Detection and Plan Recognition*, Second International Conference on Future Networks 2010.

