IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

Unauthorized Access Point Detection in Wireless LAN

Mr. Amol S. Papade[1], Mr. Vikas E. Pansare[2], Mr. Rohit D. Patil[3], Prof. S. S. Gore[4]

Department of Computer Engineering, Jaihind College of Engineering, Kuran SPPU, Pune[1, 2, 3, 4]

Abstract: Illegal Access Point called as Rogue Access Point (RAP) is an access point that has been installed on a secure network without explicit authorization from a system administrator Wireless Networks has big security threat called Rogue access points. If care is not taken and if this network threats are not detected and mitigated on time, this will result into the serious network damage and data loss. Every organization should give priority for Finding and avoiding rogue wireless access points. Rogue access points, if undetected, can be an open door to sensitive information on the network. Many data raiders have taken advantage of the undetected rogue access points in enterprises to not only get free Internet access, but also to view confidential information. Most of the current solutions to detect rouge access points are not automated and are dependent on a specific wireless technology. The approach is an automated solution which can be installed on any router at the edge of a network. Rogue Access Point detection is a two step process starting with discovering the presence of an Access Point in the network and then proceeding to identify whether it is a rogue or not. The presence of Rogue Access Point (RAP) is major security concern in wireless network. If this kind of security threat is alive into WLAN, it results into leakage of confidential information to outside network. In our implementation, we have make used of clock skew of wireless LAN access point as its fingerprint to detect the fake APs. Fingerprinting will act as unique identification like human fingerprint work. The major objective of using the clock skew interval for detecting the fake AP is to overcome the limitation of existing approach. Existing methods for detection of fake AP has limitation of detecting MAC address spoofing.

Keywords: Wireless LAN, Rogue Access Point (RAP), Media Access Control (MAC), Internet Protocol (IP).

I. INTRODUCTION

The main objective of this project is to develop software with functionality of Rouge Access Point Detection & Counter Attack using Advanced Internet Proxy. The contribution of this project is a novel approach to detect Rogue Access Points in a network.

- A rogue access point (AP), also called rogue AP, is any Wi-Fi access point that is installed on a network but is not authorized for operation on that network, and is not under the management of the network administrator.
- In this project proxy is playing an important role. This proxy server will run on server machine. The client will run the project. There is one more class that run and fetches the all machine details. These details are then store at database. While checking whether the request is authorized or unauthorized, proxy crosses check with database and as per details it will give the access to internet.
- At that time check for the IP spoofing too. In computer networking, IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system. That means in this project, we are checking whether two machines has same IP, if yes then one of them must be fake. For this we are storing all machine details in database.
- An authorized user can have internet access and unauthorized is unable to access the internet. The admin will handle the things, such as allow or deny the particular user, block the port number, view the login details etc.
- Rouge Access Point Detection & Counter Attack is desktop application. In which, we are going to detect access point first and check whether this AP are rouge access points.
- Here we are also detecting the IP Spoofing. For this the machine details like IP address, Media Access Control(MAC) address , Hard Disk Serial number etc. are stored at database and when request come it should go through proxy and then proxy will check that request is authorized or not. If it is rouge then the port number of that particular client will be blocked. So that it won't have access in future.

II. NEED

The main objective of this project is to develop software with of Rouge Access Point Detection and Counter Attack using Advanced Internet Proxy. The contribution of this project is a novel approach to detect Rogue Access Points in a network.

1. Rogue devices are an increasingly dangerous reality in the insider threat problem domain. Industry, government, and academia need to be aware of this problem and promote state-of-the-art detection methods.
2. Rogue access points, if undetected, can be an open door to sensitive information on the network. Many data raiders have taken advantage of the undetected rogue access points in enterprises to not only get free Internet access, but also to view confidential information. Most of the current solutions to detect rouge access points are not automated and are dependent on a specific wireless technology.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

3. Rogue AP exposes internal networks to the outside world, making it easy for people to bypass security measures.

III.ARCHITECTURE

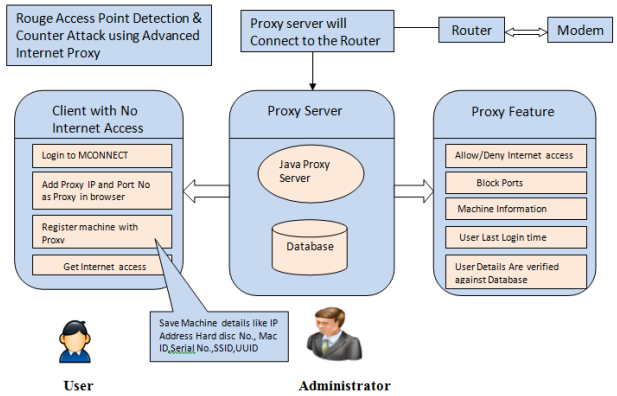

Fig. System Architecture

The system architecture is depicted in Figure 1 and was implemented as a client-server architecture using off-the-shelf commercial hardware and an open-source Wi-Fi sniffer .A modified version of was built and installed in a number of monitors as clients. These clients measure AP data transmission and signal characteristics. They then report their measurements to the server which detects and locates rogue APs if present.
Client monitors, whose locations are set in the table below the map. The identified rogue APs are shown on the right hand side table, and represented by the orange dots on the map.

IV. ALGORITHM

1. MD5 encryption algorithm

A message-digest algorithm is also called a hash function or a cryptographic hash function. It accepts a message as input and generates a fixed-length output, which is generally less than the length of the input message. The output is called a hash value, a fingerprint or a message digest.

MD5, as well as MD2 and MD4, follows a design principle proposed by Merkle and Damagard. Its basic idea is to do hash in a block-wise mode. In a word, MD5 consists of two phases: padding phase and compression phase. In the padding phase, some extra bits (1 to 512bits) are appended to the input message. The result bits is congruent to 448 mod 512. Then the length of the initial message is transformed to a 64-bit binary- string (if the length is greater than 2^{64}, the lower 64-bit is used) and this 64 bits is added to the tail of the message too. So the padding phase ends with a bit stream that consists of one or more 512-bit blocks. In the compression phase, a compression function is used on each 512-bit block and generates a 128-bit output. The output is always involved in the calculation of next round.

For convenience, we describe the algorithm through the following five steps:

(a) Add padding bits behind the input message

This step is to elongate the initial message and make its length be congruent to 448 mod 512. First, a single bit "1" is appended to the message. Then, a series of "0" bits are appended so that

Length (the padded message) ≡ 448 mod 512

For example, suppose the initial message has 1000 bits. Then this step will add 1 bit "1" and 471 bits "0". As another example, consider a message with just 448 bits. Since the algorithm doesn't check whether the initial length is congruent to 448 mod 512, one bit "1" and 511 bits "0" will be appended to the message. Therefore, the padding bits' length is at least one and at most 512.

(b) Add a 64-bit binary-string which is the representation of the message's length

Here, please pay attention to the meaning of the 64-bit binary-string. You shouldn't regard it as first 64 bits of the initial message. It is indeed the binary representation of the length of the initial message. For example, suppose the message is 1000bits long. Its 64-bit binary representation would be 0x00000000000003E8. If the message is very long, greater than 2^{64}, only the lower 64 bits of its binary representation are used.

(c) Initialize four 32-bit values

These four 32-bit variables would be used to compute the message digest. We denote them by A, B, C, D. Their initial values are:

A = 0x67452301
B = 0xEFCDAB89
C = 0x98BADCFE
D = 0x10325376

(d) Compress every 512-bit block

(e) Generate the 128-bit output

There are four rounds and sixteen steps in each round.

2. Rouge Access Point Detection Algorithm

All web requests goes through the common proxy server. If the proxy detects that the machine details exist in the database and IP is spoofed then the machine is declared to be a rouge access point.

V. OPERATION

A rogue access point (AP), also called rogue AP, is any Wi-Fi access point that is installed on a network but is not authorized for operation on that network, and is not under the management of the network administrator. In this project proxy is playing an important role. This proxy server will run on server machine. The client will run the project. There is one more class that run and fetch the all machine details. These details are then store at database. While checking whether the request is authorized or unauthorized, proxy crosses check with database and as per details it will give the access to internet.
At that time check for the IP spoofing too. In computer networking, IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of concealing the identity of the sender or imperson- ating another computing

DOI 10.17148/IJARCCE.2015.41182

system. That means in this project, we are checking whether two machines has same IP, if yes then one of them must be fake. For this we are storing all machine details in database.

An authorized user can have internet access and unauthorized is unable to access the internet. The admin will handle the things, such as allow or deny the particular user, block the port number, view the login details etc.

V. ADVANTAGES

1. The presence of an Access Point in the network
2. Check whether the client is authorized
3. Checking for an IP Spoofing
4. Block Port numbers where IP spoofing occurs.

VI. CONCLUSION AND FUTURE SCOPE

It is very easy to set up a successful rogue AP, this will result in major security problem. We have existing techniques for detecting rogue AP, but that technique has certain kinds of limitation. Disadvantage of manual Radio Frequency is that. RF scanning requires more time and it is tedious, which Detect rogue AP only, when scanning is applied. RF scanning method is also do impact on the costing and also it is not so effective and accurate. Automatic scanning depend on signs of APs (viz. MAC address, SSID, etc.) which is ineffective when a rogue AP spoofs signatures. But our approach, rogue AP detection with clock skew method overcome this drawbacks and prove effective and robust method of detecting rogue access point. We have mainly focused on identifying wireless vulnerabilities and security threats for the end users and finding solution to combat them.

REFERENCES

[1] TUNG M. LE1, REN PING LIU2, AND MARK HEDLEY2 "ROGUE ACCESS POINT DETECTION AND LOCALIZATION"

[2] PROF.DR.P.B.MANE "ILLEGAL ACCESS POINT DETECTION USING CLOCK SKEWS METHOD IN WIRELESS LAN".

[3] Mrs. Sachin Shetty, Min Song "Rogue Access Point Detection by Analyzing Network Traffic Characteristics" Department of Electrical and Computer Engineering Old Dominion University, Liran Ma Computer Science Department The George Washington University

[4] Liran Ma, Amin Y. Teymorian, Xiuzhen Cheng "A Hybrid Rogue Access Point Protection Framework for Commodity Wi-Fi networks "Department of Computer Science The George Washington University,

[5] Amran Ahmad, Suhaidi Hassan " Detecting Rogue Access Point (RAP) using Simple Network Management Protocol (SNMP) " College of Arts and Sciences

[6] V. S. Shankar Sriram1, G.Sahoo3 "Detecting and Eliminating Rogue Access Points in IEEE-802.11 WLAN - A Multi-Agent Sourcing Methodology" Department of Information Technology, Birla Institute of Technology, Mesra, Ranchi, India sriram@bitmesra.ac.in1, drgsahoo@yahoo.com3