Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 6, Issue, 04, pp.6221-6224, April, 2014

INTERNATIONAL JOURNAL
OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

DETECTING AND ELIMINATING ROGUE ACCESS POINTS IN IEEE-802.11 WLAN- USING RESERVE PROXY SERVER METHODOLOGY

*Yogesh Kapadi, Suchita Khobragade, Priya Bhujbal and Krupa Shaha

Department of Computer Engineering, Sinhgad Institute of Tech., Lonavala. (PU), India

ARTICLE INFO

Article History:
Received 26th January, 2013
Received in revised form
24th February, 2014
Accepted 10th March, 2014
Published online 23rd April, 2014

Key words:
WLAN,
Internet access,
Rogue access points,
Data raiders.

ABSTRACT

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. 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. In this paper, we present a rogue access point detection approach. The approach is an automated solution which can be installed on any router at the edge of a network. The main premise of our approach is to distinguish authorized WLAN hosts from unauthorized WLAN hosts connected to rogue access points by analyzing traffic characteristics at the edge of a network. Simulation results verify the effectiveness of our approach in detecting rogue access points in a heterogeneous network comprised of wireless and wired subnets. 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. This Methodology has the following outstanding properties:
1. It doesn’t require any specialized hardware ;
2. The proposed algorithm detects and completely eliminates the RAPs from network;
3. It provides a cost-effective solution. The proposed technique can block RAPs as well as remove them from the networks both in form of Unauthorized APs or as a Rogue clients Acting as APs. *Key words:* Rogue Access Point, Wireless LAN, Wireless Security, etc.

INTRODUCTION

Problem Description

A rogue AP is an unauthorized access point plugged into a corporate network, posing a serious security threat to enterprise IT systems. Rogue APs are typically installed by employees in work places for convenience and flexibility. Although users could leverage common security measures such as Wired Equivalent Privacy (WEP) to protect their network communications, such measures may not be consistent with the corporate security policies and they are often inefficient. For example, researchers have identified design laws in WEP, which can be easily exploited to recover secret keys. Rogue AP exposes internal networks to the outside world, making it easy for people to bypass security measures. Rouge 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. 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. Rogue AP exposes internal networks to the outside world, making it easy for people to bypass security measures.

There are few researches already performed in this field, to detect and block the Rogue Access Points, but none of them is comprehensive. Most of them need to have a dedicated piece of software or hardware, or even some special qualified employees for performing different scans, or even some additional burden is given to the current employee for regular scanning of their vicinity for checking any unauthorized access points actively working around them. Here we propose a fully automated concept (without any manual intervention) of detecting and eliminating RAPs by applying the Reserve Proxy Server methodology onto the network.

In present methodology there are many limitations like as If RAP is not properly handeled, it could lead from minor network fault to serious network failure. Most solutions are not automated, they are dependent. It fails to provide adequate security. One could easily break into a wireless network with minimal setup, a laptop & a wireless card. The presence of

***Corresponding author: Yogesh Kapadi**
Department of Computer Engineering, Sinhgad Institute of Tech., Lonavala. (PU), India.

RAP always resulted into the important information leakage or damage.

Purpose

The main objective of this project is to develop software with functionality of Rouge Access Point Detection & Elimination. The contribution of this project is a reserve proxy server methodology approach to detect Rogue Access Points in a wireless Network.

Project Scope

A rogue AP is an unauthorized access point plugged into a corporate network, posing a serious security threat to enterprise IT systems. Rogue APs are typically installed by employees in work places for convenience and flexibility. Although users could leverage common security measures such as Wired Equivalent Privacy (WEP) to protect their network communications, such measures may not be consistent with the corporate security policies and they are often inefficient. For example, researchers have identified design laws in WEP, which can be easily exploited to recover secret keys. Rogue AP exposes internal networks to the outside world, making it easy for people to bypass security measures. Rouge 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.

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.

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

Implementation Plan

In algorithm there is the three important factors that is proxy, server and client.

Proxy: 1. All hosts have to go through proxy server.
2. Proxy will detect hosts MAC_ID, SSID, IP Address, Hard disc serial no and requested port no as per incoming requests.
3. Host policies and rules are stored in the MYSQL database on proxy server.

4. Proxy will check the host policy and process the request accordingly.

5. User gets the internet access if he is an authorized user otherwise gets the error message.

6. Proxy Features are: a. Allow/Deny Internet Access. b. Block Incoming/Outgoing Ports. c. Catch Machine Information. d. Maintain user login information. e. Detect Rouge Access Point.

7. Some of the different ways in which IT managers can populate the authorized list are: a. Authorized MAC. b. Authorized SSID. c. Authorized Vendor. d. Authorized Media Type. e. Authorized Channel.

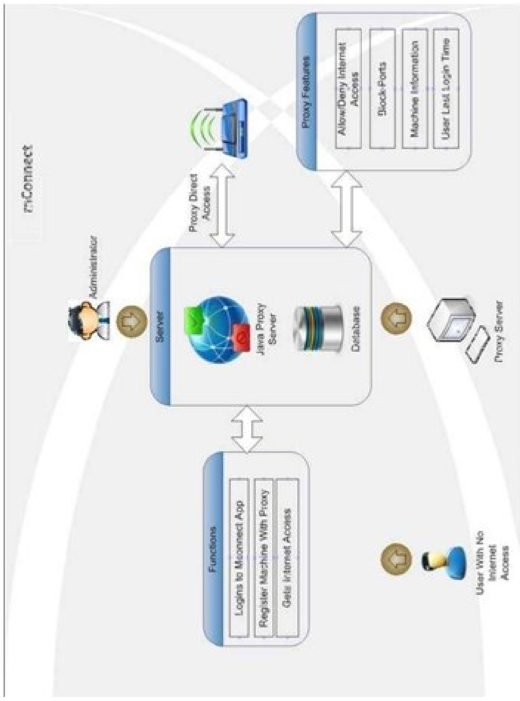


Fig.1. System Architechture

Server :

1. Admin can view login details. 2. Admin can define rules for the host and allow/deny them for internet access. 3. Admin can add ports to incoming/outgoing port list.

Client :

1. Client has to Start Application.

2. Login with your credentials. 3. Set the proxy IP and port no in browser proxy Hit web URL to connect to.

Working of System

There are three main parts in this system i.e. client, proxy server and server. In System connection firstly proxy server sends the request for establishment of connection with the server. Then server accepts the request and establishes the connection with proxy server and informed to proxy server.
When new client wants to use WLAN it must require the software setup. If there is new client then he should go through the registration process. Firstly client fills registration details and sends this information to proxy server. Then proxy server automatically fetches the client machine details and forward to the server. At server side, server cross check the all details if that details not present in the system then in that case server adds that details in the database repository. Then again cross checking with the server take place. If details are verified then machine get the permission to network access. Then client

sends the IP, URL and Port request to the proxy server. Then proxy server sends these details to the server. When server accepts the request then it sends the acknowledgement and authorization to the proxy server then proxy server sends authorization to the client. In this way the working of the system take place.

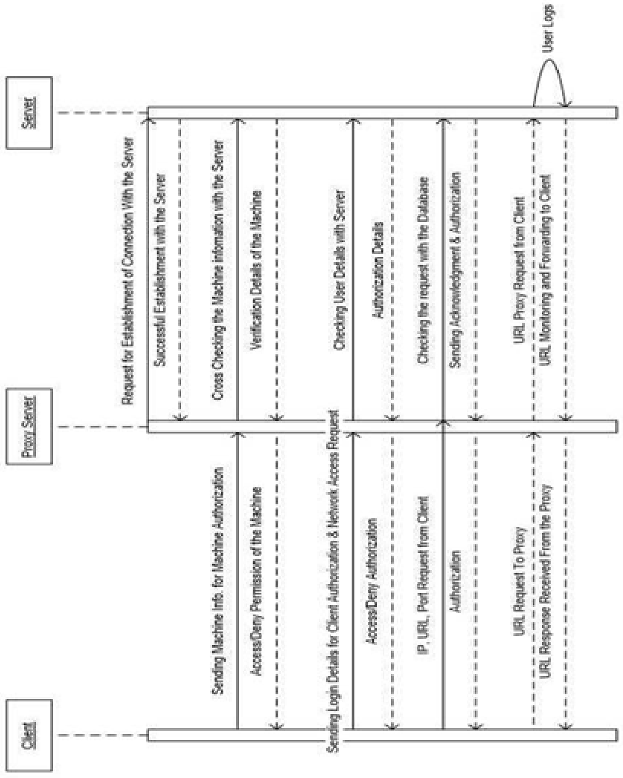
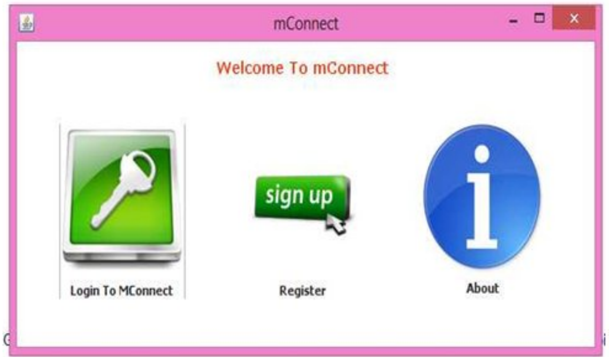

User Logs
Server
Proxy Server
Client
Request for Establishment of Connection With the Server
Successful Establishment with the Server
Cross Checking the Machine information with the Server
Verification Details of the Machine
Checking User Details with Server
Authorization Details
Checking the request with the Database
Sending Acknowledgment & Authorization
URL Proxy Request from Client
URL Monitoring and Forwarding to Client
Sending Machine Info. for Machine Authorization
Access/Deny Permission of the Machine
Sending Login Details for Client Authorization & Network Access Request
Access/Deny Authorization
IP, URL, Port Request from Client
Authorization
URL Request To Proxy
URL Response Received From the Proxy

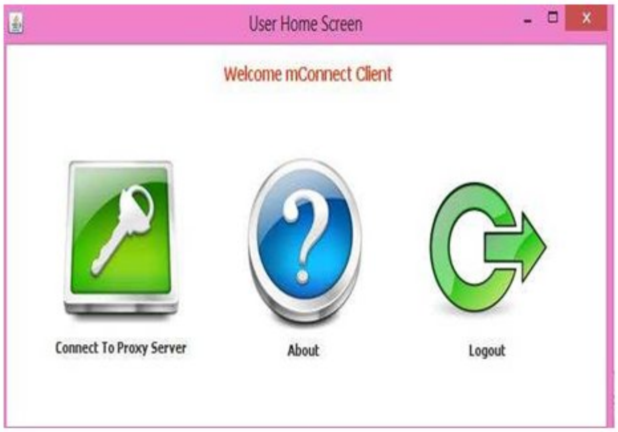
Fig.2. Sequence Flow

Snap Shot

Following fig shows the total initial details of the system. In this if client is new then he should sign up for that he fills all details like user name password then go through secure sign up. If client is old one then he directly login to the system. After login clients details match with the database repository, if details match then he get network access. After that there is logout screen using that user close all process.


mConnect

Welcome To mConnect


User Home Screen

Welcome mConnect Client

Conclusion

This system requires only single detection and elimination algorithm. Wireless Security maintained properly. So Processing of Detection and elimination of RAPs is very fast. Also all solutions are automated, they are independent. This system Doesn’t required an y specialized hardware so it is cost effective. This approach look very efficient, however its efficiency will get evaluate during the practical experiments over real time wireless networks. Here we extended the approach of reserve proxy server based mechanism to detect and prevent the fake access points from the wireless networks.

In above proposed algorithm we added the concepts of proxy server which improves the performance and allows to periodically scan not only new access points but also the existing access points for any unauthorized actions.

REFERENCES

“Air Defense enterprise: a wireless intrusion prvention system.” [Online] Available: http://www.airdefense.net/

“Air Magnet: Enterprise WLAN management.” [Online] Available: http://www.airmagnet.com/

“Air wave: Wireless net work management.” [Online] Available: http://www.airwave.com/

“Rogue Access Point Detection” Automatically Detect and Manage Wireless Threats to Your Network-www. wavelink.com.

Access Point Detection by Analyzing Network Traffic Char acteristics” 1 -4244-151306/07/$25.00©2007 IEEE.

Lanier Watkins, Raheem Beyah, Cherita Corbett ― A Passive Approach to Rogue Access Point Detection‖ 1930-529X/07/$25.00 © 2007 IEEE.

Liran Ma, Amin Y. Teymorian, Xiuzhen Cheng ― A Hybrid Rogue Access Point Protection Framework for Commodity Wi-Fi Net works ‖ published in the IEEE INFOCOM 2008.

Manage Engine White Paper: Wireless Network Rogue Access Point Detection & Blocking

Mohan K Chirumamilla, Byrav Ramamurthy ― Agent Based Instrusion Detection and Response System for Wireless L ANs‖ 0 -7803-7802- 4/03/$17.00 © 2003 IEEE

Net Stumbler, http://www.netstumbler.com.

Sachin Shetty, Min Song, Liran Ma “Rogue

Shankar Sriram, V. S. G. Sahoo, Ashish P. Singh, Abhishek

Kumar Maurya ―Securing IEEE 802.11 Wireless LANs – A Mobile Agent Based Architecture‖ 2009 IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6-7 March 2009.

ShankarSriram V. S., G. Sahoo ― A Mobile Age nt Based Architecture for Securing WLANs ‖ International Journal of Recent Trends in Engineering, Vol1, No. 1, May 2009.

Songrit Srilasak, Kitti Wongthavarawat, Anan Phonphoem "Integrated Wireless Rogue Access Point Detection and Counter attack System" 2008 International Conference on Information Security and Assurance

SongritSrilasak, Kitti Wongthavarawat and Anan Phonphoem, Intelligent Wireless Network Group (IWING) ―Integrated Wireless Rogue Access Point Detection and Counterattack System ‖ published in 2008 International Conference on Information Security and Assurance.

****