Enterprise Wireless Fidelity Implementations Using Port Based Network Access Control (IEEE 802.1X)

Noorul Ameen¹, Vincy Salam² and Anil Sagar³

¹,²CERT-India, Department of Information Technology, New Delhi, India
²TKMIT, Kollam, Kerala, India
¹noorul.ameen@mit.gov.in, ²vincysalam2007@gmail.com, ³anil@mit.gov.in

Abstract-- Enterprise Wireless Fidelity implementations have complicated requirements for Authentication, Authorization, Accounting (AAA) and detection of unauthorized access. Recent incidents show that unsecured implementations invite severe risk to enterprise network and data (especially for financial and critical sectors). In this paper a secure implementation is proposed which addresses most of the possible threats in enterprise arena. The system is based on IEEE 802.1X port based NAC. The System is having Authentication, Authorization and Accounting/Auditing Features.

Index Terms-- Wi-Fi, EAP, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), RADIUS and 802.1X

I. INTRODUCTION

Wi-Fi (Wireless Fidelity) devices - well known for their portability, flexibility and increased productivity are based on IEEE 802.11 standard. IEEE 802.11 WLAN, or Wi-Fi, is the most widely accepted broadband wireless networking technology, providing the highest transmission rate among wireless networking technologies. Today’s Wi-Fi devices, based on IEEE 802.11a and 802.11g provide transmission rates up to 54 Mbps; a new standard IEEE 802.11n is there which supports up to 600 Mbps. The transmission range of a typical Wi-Fi device is up to 100-250m, where its exact range varies depending on the transmission power, the surrounding environments, and other factors. The 802.11 devices operate in unlicensed bands at 2.4 and 5 GHz, where the exact available bands depend on each county. In order to connect the device to another network (usually wired) Wireless Access Point (base station) or Wireless Router is required. It can relay data between wired devices and wireless devices in the network.

Since radio waves can penetrate through walls there is a great chance of unauthorized access to the network and data. Because of its broadcasting nature, anybody can sniff the network for valuable credentials. If the network is not properly secured the attacker will get sufficient data to launch an attack. In brief the following cases may happen:

i) The attacker may search for available wireless networks in the close proximity. If the Access Point (AP) is open, not having any user name, password the attacker can avail the network without any authorization.

ii) The attacker can directly log in to the Access Point remotely using default credentials and configure the device in whatever way he wants for unauthorized access, denial of service, DNS redirections, Man in the Middle attacks etc.

iii) The attacker can sniff the network for configuration details such as SSID (Service Set Identifier), BSSID (Basic Service Set Identification), encryption used, channel used etc. He can capture sufficient packets to launch an attack.

iv) The attacker can install a fake Access Point and lure (like advertising free internet access) users to connect to the rogue AP.

v) The attacker can disrupt the normal functioning of the network.

vi) A vulnerable AP may also be exploited with malicious code to further attack Access Points over LAN and WAN.

Authentication, Authorization and Accounting (AAA) are the issues to be considered while securing wireless networks in enterprises. IEEE 802.1X may be one of the best options for this purpose. Since it is a protocol it can be implemented in any arena, independent of Operating Systems and applications.

A). IEEE 802.1X Port Based Network Access Control

It provides AAA futures and is based on Extensible Authentication Protocol (EAP). The authentication is provided by either establishing a point to point connection or preventing access from the port if the authentication fails.

There are mainly three participants in the 802.1X authentication process. A supplicant, authenticator and authentication server. The supplicant is a software on a client device, the authenticator is a wired Ethernet switch or wireless access point, and the authentication server is generally a RADIUS (Remote Authentication Dial in User) database. The supplicant provides user credentials such as username, passwords to the authenticator, then it is forwarded
to the authentication server for verification. If the credentials are valid the supplicant is allowed to access the resources.

RADIUS is a UDP protocol specially used in distributed environments. It provides security management and statistics collection in remote computing environments with dial in users. Security information and statistics like bytes transmitted and received are stored in a central location, known as the RADIUS server. RADIUS clients communicate with the RADIUS server to authenticate users.

II. RELATED WORK

Wireless Local area networks are vulnerable because of insecure implementation. Vulnerable Protocol (primitive implementation of WEP) implementations will make situations more dangerous. A layered Approach should be followed to secure WLANs [1], [7], [8], [9].

III. OUR MODEL

Securing Wireless Networks can be viewed in different aspects. Security best practices may be developed with the home user perspective, Enterprise network implementations and for mobile telecommuters.

Here we propose a framework for securing Enterprise WI-FI implementations. The framework is based on IEEE 802.1X port based network Access Control and it solves most of the problems of Authorization, Authentication and Accounting. An Intrusion Detection System (IDS) may be incorporated in this framework which will identify the prevalent threats.

A case study regarding this is depicted in this paper.

The experimental setup includes the following configurations.

Authentication Server: MS Windows Server 2008 (An open source Server OS having authentication server functionality like Ubuntu, may also be used).

Authenticators: Routers/Access Points-Beetel 450BXI Router

Supplicants: Wireless Client Machines

Network Policy Server (NPS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy in Windows Server 2008. As a RADIUS server, it performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless and Virtual Private Network (VPN) connections. NPS replaces Internet Authentication Service (IAS) - the MS Windows 2003 Server implementation of RADIUS.

The implementation includes configuring Active Directory Domain Services, Active Directory Certificate Services, Configure Network Policy and Access Services Role and RADIUS, Router level configurations and Client level configurations. A step by step methodology is explained in this document.

**Step 1:** Configure Active Directory Domain Services

**Step 2:** Configure Active Directory Certificate Services

![Fig. 2: Active Directory Certificate Services installed](image-url

**Step 3:** Set up the Certificate required by PEAP (Protected EAP) for Authentication Server

![Fig. 3: Certificate Enrollment Status for WIRELESSCERT Domain](image-url

**Step 4:** Configure Network Policy and Access Services Role and RADIUS
Step 5: Configure Wireless Controllers and or APs in IEEE 802.1X security mode with shared secret. Prefer WPA2 Enterprise with AES.

Step 6: Export CA Certificate to install it into Client Computers

Client Side Configurations:

Step 8: Copy the CA Certificate generated in the Step 7 (in .crt format) to client machine and install

Step 10: Manually create a Network profile with WPA2 with AES. Edit the PEAP properties and validate the Server Certificate

Fig. 4: Radius Clients Configured with shared secret

Fig. 5: Beetel 450BXI Router configured in 802.1X Network Authentication with Shared Key (same as Radius server)

Fig. 6: Selecting the export file format

Fig. 7: Installing Certificates in Client Side

Fig. 8: PEAP Properties with Secured password Authentication Method (EAP-MSCHAP v2)

Fig. 9: Login with proper Domain credentials

Fig. 10: Successfully connected
AAA features:

By configuring the Enterprise Wi-Fi network using IEEE 802.1X we will get the following features:

i). Proper Authentication: The Authentication is done through IEEE 802.1X RADIUS and EAP with WPA2/AES. It also includes digital certificate, user name(s) and passwords, secure tokens etc.

ii). Authorization: Proper Authorization can be set to the users in the domain.

iii). Accounting: Relevant activities of the user are logged in the Authentication Server.

For example in our test scenario the activities are properly configured and logged.

Detection of rogue Access points:

Rogue access points are mainly of two categories. Internal rogue access points installed by employees and external rogue access points. Different approaches can be considered for detection of rogue access points. The [4] discuss the detection by analyzing traffic characteristics at the edge of a network. The model is based on two classifications.

i). Identify the traffic whether it is originating from a Ethernet traffic or WLAN traffic.

ii). identify whether a host is connected to a rogue access point by analyzing the frequency of access of a particular port and the increase in cross-port communication. If a host shows a remarkable increase in the above two statistical categories it is assumed that host is connected to a rogue access point.


Intrusion Detection System:

Here we will discuss different threats and possible counter measures in enterprise networks.

IV. CONCLUSION

In summary, Enterprise Wireless Networks should have the following salient security features.

- Change the default Admin Password on all the Access Points (APs).
- Implement a policy on Authentication, Authorization, Accounting(AAA) and Encryption
• Prefer WPA2/802.11i (Wi-Fi Protected Access) instead of WEP (Wired Equivalent Privacy) as the encryption standard
• Authenticate the users with authentication protocols like 802.1X, RADIUS and EAP.
• Use MAC address filtering at the access points.
• Keep the logging feature of the wireless devices enabled.
• Log all devices activities and check log files regularly.
• Disable WAN access on the AP.
• Use Wireless Intrusion Detection Systems and vulnerability assessment tools for detecting rogue APs and vulnerabilities in wireless networks.
• Update the firmware and drivers of Access Points, wireless interfaces regularly.

V. ACKNOWLEDGMENTS

We would like to thank our advisor Dr. Gulshan Rai for his valuable support and suggestions. We also thank our colleagues Mohammed Akram Khan, Krishna Kumar, Abhilash and Subrahmani Babu for their technical support.

REFERENCES