ISSN 2047-3338

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

Noorul Ameen[1], Vincy Salam[2] and Anil Sagar[3]
[1,3]CERT-India, Department of Information Technology, New Delhi, India
[2]TKMIT, Kollam, Kerala, India
[1]noorul.ameen@mit.gov.in, [2]vincysalam2007@gmail.com, [3]anil@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.

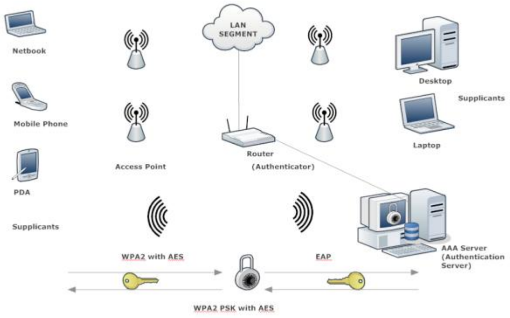


Fig. 1: Wi-Fi Architecture in Enterprise Networks

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

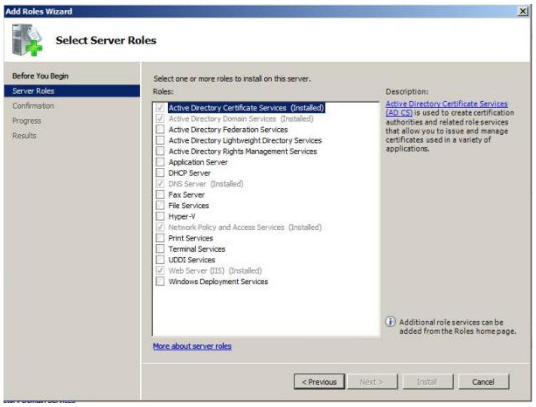
Supplicants: Wireless Client Machines

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.

Step1: Configure Active Directory Domain Services

Step 2: Configure Active Directory Certificate Services



Select one or more roles to install on this server.

Roles:

☑ Active Directory Certificate Services (Installed)
☑ Active Directory Domain Services (Installed)
☐ Active Directory Federation Services
☐ Active Directory Lightweight Directory Services
☐ Active Directory Rights Management Services
☐ Application Server
☐ DHCP Server
☑ DNS Server (Installed)
☐ Fax Server
☐ File Services
☐ Hyper-V
☑ Network Policy and Access Services (Installed)
☐ Print Services
☐ Terminal Services
☐ UDDI Services
☑ Web Server (IIS) (Installed)
☐ Windows Deployment Services

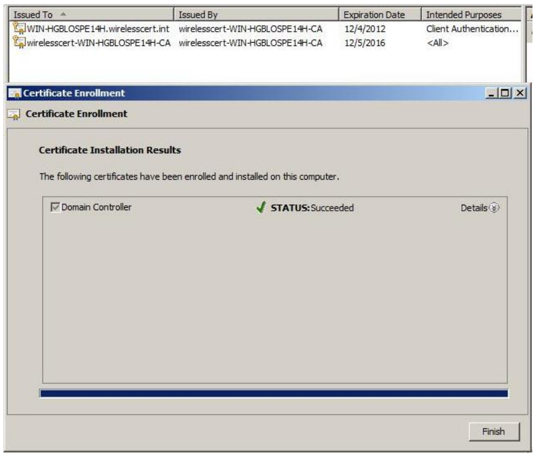
Description:

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Additional role services can be added from the Roles home page.

Fig. 2: Active Directory Certificate Services installed

Step3: Set up the Certificate required by PEAP (Protected EAP) for Authentication Server



Issued To	Issued By	Expiration Date	Intended Purposes
WIN-HGBLOSPE14H.wirelesscert.int	wirelesscert-WIN-HGBLOSPE14H-CA	12/4/2012	Client Authentication...
wirelesscert-WIN-HGBLOSPE14H-CA	wirelesscert-WIN-HGBLOSPE14H-CA	12/5/2016	<All>

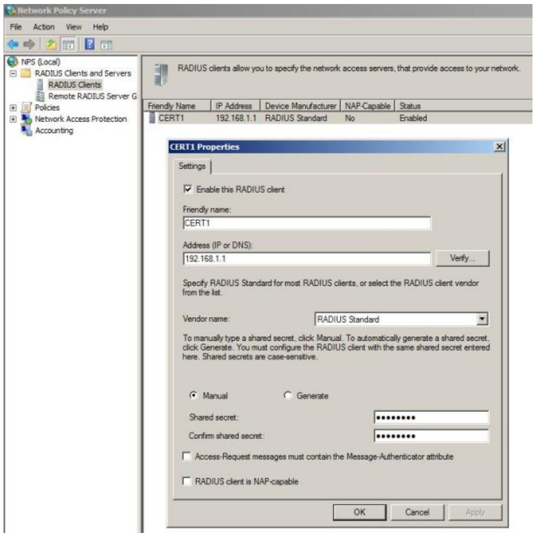
Certificate Installation Results

The following certificates have been enrolled and installed on this computer.

☑ Domain Controller ✓ STATUS: Succeeded

Fig. 3: Certificate Enrollment Status for WIRELESSCERT Domain

Step 4: Configure Network Policy and Access Services Role and RADIUS



Network Policy Server

File Action View Help

NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server G
Policies
Network Access Protection
Accounting

RADIUS clients allow you to specify the network access servers, that provide access to your network.

Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status
CERT1	192.168.1.1	RADIUS Standard	No	Enabled

CERT1 Properties

Settings

☑ Enable this RADIUS client

Friendly name: CERT1

Address (IP or DNS): 192.168.1.1 Verify...

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name: RADIUS Standard

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ••••••••

Confirm shared secret: ••••••••

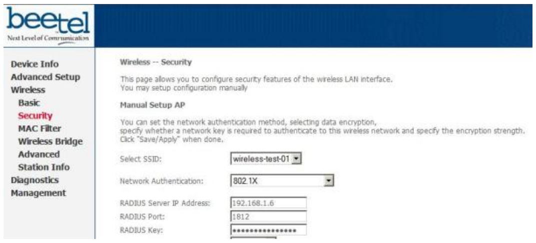
□ Access-Request messages must contain the Message-Authenticator attribute

□ RADIUS client is NAP-capable

OK Cancel Apply

Fig. 4: Radius Clients Configured with shared secret

Step 5: Configure Wireless Controllers and or APs in IEEE 802.1X security mode with shared secret. Prefer WPA2 Enterprise with AES**.**



beetel
Next Level of Communication

Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info
Diagnostics
Management

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually

Manual Setup AP

You can set the network authentication method, selecting data encryption,
specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Save/Apply" when done.

Select SSID: wireless-test-01

Network Authentication: 802.1X

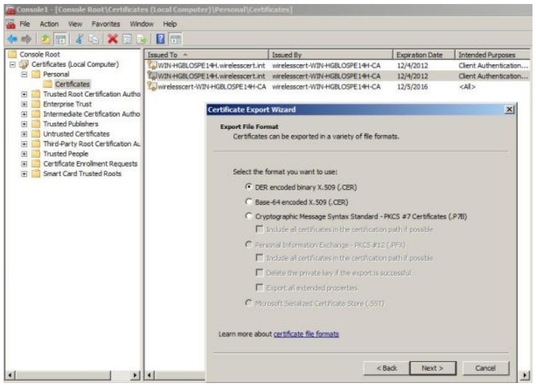
RADIUS Server IP Address: 192.168.1.6

RADIUS Port: 1812

RADIUS Key: •••••••••••••••

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

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



Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

File Action View Favorites Window Help

Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Autho
Enterprise Trust
Intermediate Certification Autho
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Au
Trusted People
Certificate Enrollment Requests
Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes
WIN-HGBLOSPE14H.wirelesscert.int	wirelesscert-WIN-HGBLOSPE14H-CA	12/4/2012	Client Authentication...
WIN-HGBLOSPE14H.wirelesscert.int	wirelesscert-WIN-HGBLOSPE14H-CA	12/4/2012	Client Authentication...
wirelesscert-WIN-HGBLOSPE14H-CA	wirelesscert-WIN-HGBLOSPE14H-CA	12/5/2016	<All>

Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)
○ Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
□ Include all certificates in the certification path if possible
□ Delete the private key if the export is successful
□ Export all extended properties
○ Microsoft Serialized Certificate Store (.SST)

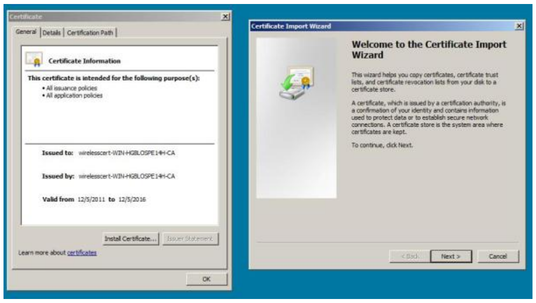
Learn more about certificate file formats

< Back Next > Cancel

Fig. 6: Selecting the export file format

Client Side Configurations:

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



Certificate

General Details Certification Path

Certificate Information

This certificate is intended for the following purpose(s):
- All issuance policies
- All application policies

Issued to: wirelesscert-WIN-HGBLOSPE14H-CA

Issued by: wirelesscert-WIN-HGBLOSPE14H-CA

Valid from 12/5/2011 to 12/5/2016

Install Certificate... Issuer Statement

Learn more about certificates

OK

Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

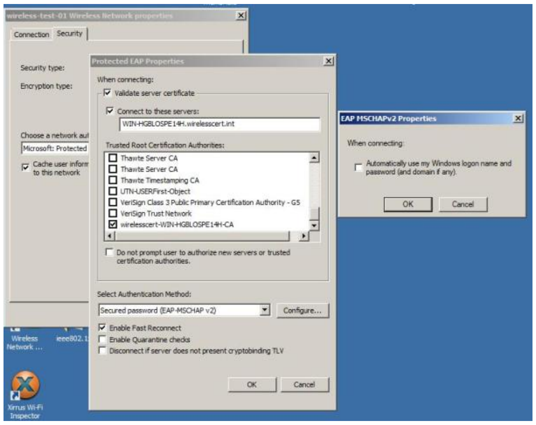
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

< Back Next > Cancel

Fig. 7: Installing Certificates in Client Side

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



wireless-test-01 Wireless Network properties

Connection Security

Security type:

Encryption type:

Choose a network aut

Microsoft: Protected

☑ Cache user inform to this network

Protected EAP Properties

When connecting:

☑ Validate server certificate

☑ Connect to these servers:

WIN-HGBLOSPE14H.wirelesscert.int

Trusted Root Certification Authorities:

□ Thawte Server CA
□ Thawte Server CA
□ Thawte Timestamping CA
□ UTN-USERFirst-Object
□ VeriSign Class 3 Public Primary Certification Authority - G5
□ VeriSign Trust Network
☑ wirelesscert-WIN-HGBLOSPE14H-CA

□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2) Configure...

☑ Enable Fast Reconnect
□ Enable Quarantine checks
□ Disconnect if server does not present cryptobinding TLV

OK Cancel

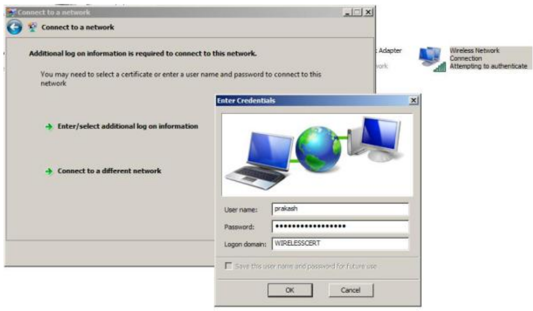
EAP MSCHAPv2 Properties

When connecting:

□ Automatically use my Windows logon name and password (and domain if any).

OK Cancel

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



Connect to a network

Connect to a network

Additional log on information is required to connect to this network.

You may need to select a certificate or enter a user name and password to connect to this network

→ Enter/select additional log on information

→ Connect to a different network

Enter Credentials

User name: prakash

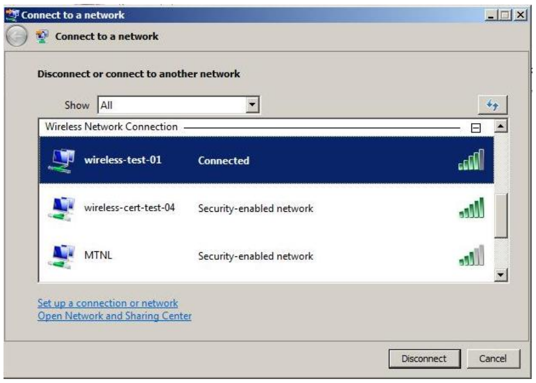
Password: •••••••••••••••••

Logon domain: WIRELESSCERT

□ Save this user name and password for future use

OK Cancel

Fig. 9: Login with proper Domain credentials



Connect to a network

Connect to a network

Disconnect or connect to another network

Show All

Wireless Network Connection

wireless-test-01	Connected
wireless-cert-test-04	Security-enabled network
MTNL	Security-enabled network

Set up a connection or network
Open Network and Sharing Center

Disconnect Cancel

Fig. 10: Successfully connected

AAA features:

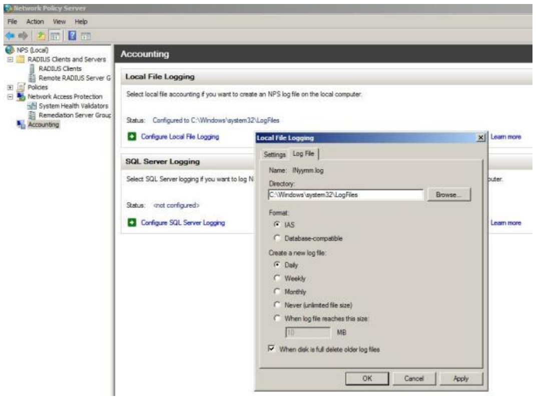
By configuring the Enterprise Wi-Fi network using IEEE 802.1X we will get the following features:

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.



Accounting

Local File Logging

Select local file accounting if you want to create an NPS log file on the local computer.

Status: Configured to C:\Windows\system32\LogFiles

Configure Local File Logging

SQL Server Logging

Select SQL Server logging if you want to log N ... puter.

Status: <not configured>

Configure SQL Server Logging

Local File Logging

Settings | Log File

Name: INyymm.log

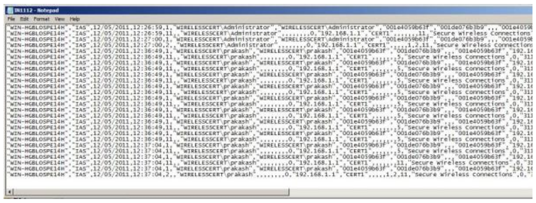
Directory: C:\Windows\system32\LogFiles

Format:
● IAS
○ Database-compatible

Create a new log file:
● Daily
○ Weekly
○ Monthly
○ Never (unlimited file size)
○ When log file reaches this size: 10 MB

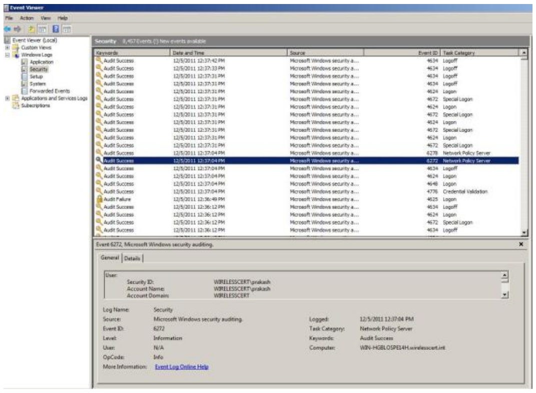
☑ When disk is full delete older log files

Fig. 11: Configuring Network Policy Server with proper Accounting



```
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:26:59,1,"WIRELESSCERT\Administrator","WIRELESSCERT\Administrator","001e4059b63f","001de076b3b9",,,"001e4059
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:26:59,11,,"WIRELESSCERT\Administrator",,,,,,,,0,"192.168.1.1","CERT1",,,,,,,11,"Secure Wireless Connections
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:27:00,1,"WIRELESSCERT\Administrator","WIRELESSCERT\Administrator","001e4059b63f","001de076b3b9",,,"001e4059
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:27:00,2,,"WIRELESSCERT\Administrator",,,,,,,,0,"192.168.1.1","CERT1",,,,,1,2,11,"Secure Wireless Connection
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:36:49,1,"WIRELESSCERT\prakash","WIRELESSCERT\prakash","001e4059b63f","001de076b3b9",,,"001e4059b63f","192.16
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:36:49,11,,"WIRELESSCERT\prakash",,,,,,,,0,"192.168.1.1","CERT1",,,,,,,5,"Secure Wireless Connections",0,"311
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:36:49,1,"WIRELESSCERT\prakash","WIRELESSCERT\prakash","001e4059b63f","001de076b3b9",,,"001e4059b63f","192.16
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:36:49,11,,"WIRELESSCERT\prakash",,,,,,,,0,"192.168.1.1","CERT1",,,,,,,5,"Secure Wireless Connections",0,"311
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:36:49,1,"WIRELESSCERT\prakash","WIRELESSCERT\prakash","001e4059b63f","001de076b3b9",,,"001e4059b63f","192.16
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:36:49,11,,"WIRELESSCERT\prakash",,,,,,,,0,"192.168.1.1","CERT1",,,,,,,5,"Secure Wireless Connections",0,"311
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:36:49,1,"WIRELESSCERT\prakash","WIRELESSCERT\prakash","001e4059b63f","001de076b3b9",,,"001e4059b63f","192.16
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:36:49,11,,"WIRELESSCERT\prakash",,,,,,,,0,"192.168.1.1","CERT1",,,,,,,5,"Secure Wireless Connections",0,"311
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:36:49,1,"WIRELESSCERT\prakash","WIRELESSCERT\prakash","001e4059b63f","001de076b3b9",,,"001e4059b63f","192.16
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:36:49,11,,"WIRELESSCERT\prakash",,,,,,,,0,"192.168.1.1","CERT1",,,,,,,5,"Secure Wireless Connections",0,"311
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:36:49,1,"WIRELESSCERT\prakash","WIRELESSCERT\prakash","001e4059b63f","001de076b3b9",,,"001e4059b63f","192.16
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:36:49,11,,"WIRELESSCERT\prakash",,,,,,,,0,"192.168.1.1","CERT1",,,,,,,5,"Secure Wireless Connections",0,"311
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:36:49,1,"WIRELESSCERT\prakash","WIRELESSCERT\prakash","001e4059b63f","001de076b3b9",,,"001e4059b63f","192.16
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:36:49,11,,"WIRELESSCERT\prakash",,,,,,,,0,"192.168.1.1","CERT1",,,,,,,5,"Secure Wireless Connections",0,"311
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:36:49,1,"WIRELESSCERT\prakash","WIRELESSCERT\prakash","001e4059b63f","001de076b3b9",,,"001e4059b63f","192.16
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:36:49,11,,"WIRELESSCERT\prakash",,,,,,,,0,"192.168.1.1","CERT1",,,,,,,5,"Secure Wireless Connections",0,"311
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:37:04,1,"WIRELESSCERT\prakash","WIRELESSCERT\prakash","001e4059b63f","001de076b3b9",,,"001e4059b63f","192.16
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:37:04,11,,"WIRELESSCERT\prakash",,,,,,,,0,"192.168.1.1","CERT1",,,,,,,5,"Secure Wireless Connections",0,"311
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:37:04,1,"WIRELESSCERT\prakash","WIRELESSCERT\prakash","001e4059b63f","001de076b3b9",,,"001e4059b63f","192.16
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:37:04,11,,"WIRELESSCERT\prakash",,,,,,,,0,"192.168.1.1","CERT1",,,,,,,11,"Secure Wireless Connections",0,"31
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:37:04,1,"WIRELESSCERT\prakash","WIRELESSCERT\prakash","001e4059b63f","001de076b3b9",,,"001e4059b63f","192.16
"WIN-HGBLOSPE14H","IAS",12/05/2011,12:37:04,2,,"WIRELESSCERT\prakash",,,,,,,,0,"192.168.1.1","CERT1",,,,,1,2,11,"Secure Wireless Connections",0,"
```

Fig. 12: Details of logged in user



Security 9,457 Events (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	12/5/2011 12:37:42 PM	Microsoft Windows security a...	4634	Logoff
Audit Success	12/5/2011 12:37:33 PM	Microsoft Windows security a...	4634	Logoff
Audit Success	12/5/2011 12:37:31 PM	Microsoft Windows security a...	4634	Logoff
Audit Success	12/5/2011 12:37:31 PM	Microsoft Windows security a...	4634	Logoff
Audit Success	12/5/2011 12:37:31 PM	Microsoft Windows security a...	4624	Logon
Audit Success	12/5/2011 12:37:31 PM	Microsoft Windows security a...	4672	Special Logon
Audit Success	12/5/2011 12:37:31 PM	Microsoft Windows security a...	4624	Logon
Audit Success	12/5/2011 12:37:31 PM	Microsoft Windows security a...	4672	Special Logon
Audit Success	12/5/2011 12:37:31 PM	Microsoft Windows security a...	4624	Logon
Audit Success	12/5/2011 12:37:31 PM	Microsoft Windows security a...	4672	Special Logon
Audit Success	12/5/2011 12:37:31 PM	Microsoft Windows security a...	4624	Logon
Audit Success	12/5/2011 12:37:31 PM	Microsoft Windows security a...	4672	Special Logon
Audit Success	12/5/2011 12:37:04 PM	Microsoft Windows security a...	6278	Network Policy Server
Audit Success	12/5/2011 12:37:04 PM	Microsoft Windows security a...	6272	Network Policy Server
Audit Success	12/5/2011 12:37:04 PM	Microsoft Windows security a...	4634	Logoff
Audit Success	12/5/2011 12:37:04 PM	Microsoft Windows security a...	4624	Logon
Audit Success	12/5/2011 12:37:04 PM	Microsoft Windows security a...	4648	Logon
Audit Success	12/5/2011 12:37:04 PM	Microsoft Windows security a...	4776	Credential Validation
Audit Failure	12/5/2011 12:36:49 PM	Microsoft Windows security a...	4625	Logon
Audit Success	12/5/2011 12:36:12 PM	Microsoft Windows security a...	4634	Logoff
Audit Success	12/5/2011 12:36:12 PM	Microsoft Windows security a...	4624	Logon
Audit Success	12/5/2011 12:36:12 PM	Microsoft Windows security a...	4672	Special Logon
Audit Success	12/5/2011 12:36:12 PM	Microsoft Windows security a...	4634	Logoff

Event 6272, Microsoft Windows security auditing.

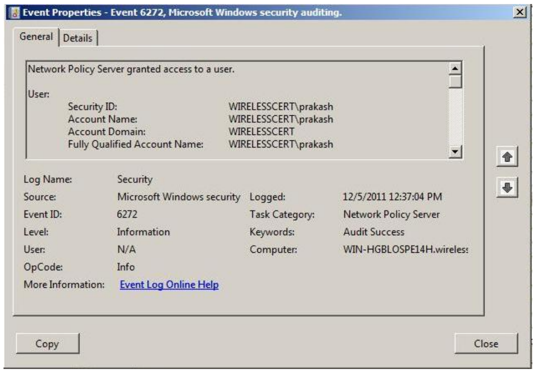
User:
Security ID: WIRELESSCERT\prakash
Account Name: WIRELESSCERT\prakash
Account Domain: WIRELESSCERT

Log Name: Security
Source: Microsoft Windows security auditing. Logged: 12/5/2011 12:37:04 PM
Event ID: 6272 Task Category: Network Policy Server
Level: Information Keywords: Audit Success
User: N/A Computer: WIN-HGBLOSPE14H.wirelesscert.int
OpCode: Info
More Information: Event Log Online Help

Fig. 13: Details of Audit

Intrusion Detection System:

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



Event Properties - Event 6272, Microsoft Windows security auditing.

Network Policy Server granted access to a user.

User:
Security ID: WIRELESSCERT\prakash
Account Name: WIRELESSCERT\prakash
Account Domain: WIRELESSCERT
Fully Qualified Account Name: WIRELESSCERT\prakash

Log Name: Security
Source: Microsoft Windows security Logged: 12/5/2011 12:37:04 PM
Event ID: 6272 Task Category: Network Policy Server
Level: Information Keywords: Audit Success
User: N/A Computer: WIN-HGBLOSPE14H.wireless
OpCode: Info
More Information: Event Log Online Help

Fig. 4: Event properties

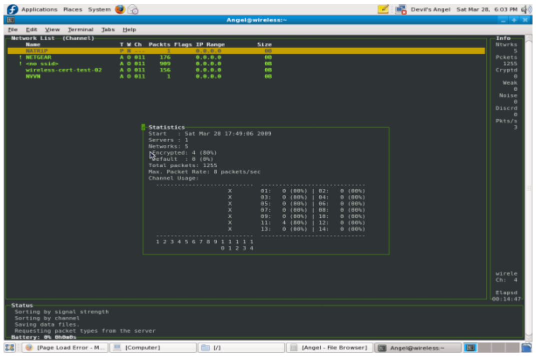
Detection of rogue Access points:

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.

The [5] and [6] use another approach is to use a wireless scanner for the detection purpose. The [5] addresses most of the threats in wireless networks. The [5] uses an open source IDS known as kismet.


Applications Places System
Devil's Angel Sat Mar 28, 6:03 PM
Angel@wireless:~
File Edit View Terminal Tabs Help
[Page Load Error - M...
[Computer]
[/]
[Angel - File Browser]
Angel@wireless:~

```
Network List (Channel)                                                 Info
    Name                     T W Ch  Packts Flags IP Range     Size     Ntwrks
    NATRIP                   P N ---      1       0.0.0.0        0B          5
  ! NETGEAR                  A O 011    176       0.0.0.0        0B     Pckets
  ! <no ssid>                A O 011    909       0.0.0.0        0B       1255
    wireless-cert-test-02    A O 011    156       0.0.0.0        0B     Cryptd
    NVVN                     A O 011      1       0.0.0.0        0B          0
                                                                          Weak
                                                                             0
                                                                         Noise
                                                                             0
                                                                        Discrd
                                                                             0
                                                                        Pkts/s
                                                                             3
             Statistics
             Start    : Sat Mar 28 17:49:06 2009
             Servers : 1
             Networks: 5
              Encrypted: 4 (80%)
              Default  : 0 (0%)
             Total packets: 1255
             Max. Packet Rate: 8 packets/sec
             Channel Usage:
              -------------------------   -------------------------
                                    X     01:   0 (00%) | 02:   0 (00%)
                                    X     03:   0 (00%) | 04:   0 (00%)
                                    X     05:   0 (00%) | 06:   0 (00%)
                                    X     07:   0 (00%) | 08:   0 (00%)
                                    X     09:   0 (00%) | 10:   0 (00%)
                                    X     11:   4 (80%) | 12:   0 (00%)
                                    X     13:   0 (00%) | 14:   0 (00%)
              -------------------------   -------------------------
              1 2 3 4 5 6 7 8 9 1 1 1 1 1
                                0 1 2 3 4
                                                                         wirele
                                                                         Ch:  4

                                                                        Elapsd
                                                                      00:14:47
Status
  Sorting by signal strength
  Sorting by channel
  Saving data files.
  Requesting packet types from the server
Battery: 0% 0h0m0s
```

Fig. 15: The open source tool Kismet, may detect rogue access points and generate alerts

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

[1] [1]. Dinesh Yadav, Anjali Sardana, "Enhanced 3-Way Handshake Protocol for Key Exchange in IEEE 802.11i", IEEE Communications, 2011.

[2] G. Hiertz, D. Denteneer, L. Stibor, Y. Zang, X. P. Costa, and B. Walke, "The IEEE 802.11 universe," IEEE Communications Magazine, vol. 48, pp. 62-70, 2010.

[3] http://www.windowsnetworking.com

[4] Sachin Shetty, Min Song, Liran Ma, "Rogue Access Point Detection by Analyzing Network Traffic Characteristics",1-4244-1513-06/07/$25.00 ©2007.

[5] Larry Pesce, Discovering Rogue Wireless Access Points Using Kismet and Disposable Hardware, GAWN Gold Submission, SANS Institute 2006.

[6] Ibrahim Halil Saruhan, Detecting and Preventing Rogue Devices on the Network, GCIA Gold Certification, SANS Institute 2007.

[7] S. Vinjosh Reddy, K. Rijutha, K. SaiRamani, S. Mohammad Ali, CR. Pradeep Reddy, "Wireless Hacking - A WiFi Hack by Cracking WEP", 2010, 2nd International Conference on Education Technology and Computer (ICETC).

[8] Jyu-Cheng Chen and Yu-Ping Wang, “Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience”, IEEE Radio Communications, Dec 2005.

[9] W.-K. Chen IEEE Standard for local and metropolitan area networks, “Port-based Network Access Control”, IEEE Std. 802.1x, 2001 Edition (R2004).