Report for Lab 4

By: Sneha Shukla

Important: I was unsuccessful in installing the emulator for this lab after trying several times and also consulted other students of the class and they also faced the same problem.

Vulnerability in 802.11 WEP Security Protocol

- WEP is the privacy protocol specified in IEEE 802.11 to provide wireless LAN users protection against casual eavesdropping. WEP stands for "Wired Equivalent Privacy" referring to the intent to provide a privacy service to wireless LAN users similar to that provided by the physical security inherent in a wired LAN.

Weakness: Key Management and Key Size

Key management is not specified in the WEP standard, and therefore is one of its weaknesses, because without interoperable key management, keys will tend to be long-lived and of poor quality. Most wireless networks that use WEP have one single WEP key shared between every node on the network. Access Points (APs) and client stations must be programmed with the same WEP key. Since synchronizing the change of keys is tedious and difficult, keys are seldom changed.

Weakness: The Initialization Vector (IV) is Too Small

WEP's IV size of 24 bits provides for 16,777,216 different RC4 cipher streams for a given WEP key, for any key size. Remember that the RC4 cipher stream is XOR-ed with the original packet to give the encrypted packet which is transmitted, and the IV is sent in the clear with each packet. The problem is IV reuse. If the RC4 cipher stream for a given IV is found, an attacker can decrypt subsequent packets that were encrypted with the same IV, or, can forge packets. This means that you don’t need to know the WEP key to decrypt packets if you know what the key stream was used to encrypt that packet. They sound like similar problems, but it’s actually much easier to discover the key stream than it is to discover the WEP key.

Weakness: The Integrity Check Value (ICV) algorithm is not appropriate

The WEP ICV is based on CRC-32, an algorithm for detecting noise and common errors in transmission. CRC-32 is an excellent checksum for detecting errors, but an awful choice for a cryptographic hash. Better-designed encryption systems use algorithms such as MD5 or SHA-1 for their ICVs. The CRC-32 ICV is a linear function of the message meaning that an attacker can modify an encrypted message and easily fix the ICV so the message appears authentic. Being able to modify encrypted packets provides for a nearly limitless number of very simple attacks. For example, an attacker can easily make the victim’s wireless AP decrypt packets for him. Simply capture an encrypted packet stream, modify the destination address of each packet to be the attacker’s wired IP address, fix up the CRC-32, and retransmit the packets over the air to the AP. The AP will happily decrypt the packets and forward them to the attacker. (The attack is slightly more complex than that, but to keep this paper short, we’ve skipped some of the details.) The biggest problem with IV and ICV-based attacks is they are independent of key size, meaning that even huge keys all look the same. The attack takes the same amount of effort.

Weakness: WEP’s use of RC4 is weak

RC4 in its implementation in WEP has been found to have weak keys. Having a weak key means that there is more correlation between the key and the output than there should be for good security. Determining which packets were encrypted with weak keys is easy because the first three bytes of the key are taken from the IV that is sent unencrypted in each packet. This weakness can be exploited by a passive attack. All the attacker needs to do is be within a hundred feet or so of the AP.

Weakness: Authentication Messages can be easily forged

802.11 defines two forms of authentication: Open System (no authentication) and Shared Key authentication. These are used to authenticate the client to the access point. The idea was that authentication would be better than no authentication because the user has to prove knowledge of the shared WEP key, in effect, authenticating himself. In fact, the exact opposite is true: if you turn on authentication, you actually reduce the total security of your network and make it easier to guess your WEP key.

Vulnerabilities in 802.11 WPA/WPA2 with PSK

WPA2 stands for Wireless Fidelity Protected Access 2 – Pre-Shared Key. It allows home users or small offices to secure their network without using an enterprise authentication server.

How does WPA2-PSK work?

WPA2-PSK requires a router with a passphrase, with a length between 8 to 63 characters, to encrypt the data in the network. It uses a technology named TKIP, i.e., Temporal Key Integrity Protocol, that requires network SSID and the passphrase to generate unique encryption keys for each wireless client.

WPA2-PSK (AES) is more secure than WPA2-PSK (TKIP), but WPA2-PSK (TKIP) can be used with older devices that are not WPA2-PSK (AES) enabled devices.

When a user connects to the router, the user provides a password to authenticate their identity and, as long as the password matches, the user is connected to WLAN.

With WPA2-PSK, users can secure their data, transmitted through the wireless channel between a router and other network devices. It is the latest generation of Wi-Fi security where the key is shared between connected devices. WPA2-PSK is also known as WPA2 Personal.

Is WPA2-PSK vulnerable?

WPA2-PSK is designed for small offices and home networks to allow users to trust the network they are connected to. WPA2-PSK is secure but shares a password to all the users connected to the network, leading to snooping on the network by the attacker.

WPA2-PSK is also found in airports, public hotspots, or universities as it is easy to implement and requires only one password. But if your WPA2-PSK gets compromised, an attacker can easily get access to your network and is capable of doing the following malicious activities:

- Switch Spoofing
- Spanning Tree Protocol (STP) Attacks
- Dynamic Host Configuration (DHCP) Spoofing
- Media Access Control (MAC) Spoofing
- Double Tagging
- Address Resolution Protocol (ARP) Spoofing.

Using a single password for network access requires good faith to keep the password secret on every user’s device. The reason for this is that if one user gets compromised, then all users can be hacked.

Brute force attacks like dictionary attacks can be performed, and an attacker can decrypt all the device traffic if it obtains the Pre-Shared Key and captures the key handshake while a user joins the network.

Security Assessment of 802.1X Port-Based Authentication Protocols

What is 802.1x important?

- Authenticate devices connected to switch ports.
- When authentication fails:
    - No or limited network access
- When authentication succeeds:
    - Access is granted
- Access can be restricted by using (downloadable) access lists

802.1x Benefits

- Visibility:
    - Clients are authenticated
    - Identity can be used for security audits   and forensics
- Security:
    - Strongest authentication methods should be used

- Transparency:
    - No involvement of end-user

802.1x Components

- Supplicant
- Authenticator
- Authentication Server

802.1x EAP Authentication Methods

Method	Identification
EAP-TTLS	Any authentication
EAP-TLS	Certificate
EAP-MSCHAPv2	Password
PEAP-EAP-TLS	TLS + Certificate
PEAP-MS-CHAPv2	TLS + Password

EAP-TLS Authentication

- No user identity protection
- Active Directory Domain Services
- Active Directory Certificate Services
- Network Policy Server (RADIUS server)
- 802.1x capable devices
- Client (Windows XP/Vista/7/8)
- Certificate based authentication for users or computers
- Provides mutual authentication
- No dependency on the password of the user
- Protected by public key cryptography
- Network Policy Server must have a certificate
- Wired client must have a certificate

EAP-TTLS Authentication

- Extends TLS by creating a secure tunnel
- Encapsulation EAP in TLS
- Can be used as proxy
- Client does not need a certificate
- Only server authentication
- Protection against eavesdropping and mitm
- Windows Server 2012 and Windows 8

EAP-MSCHAPv2 Authentication

- Password based authentication for users or computers
- User or computer account must be member of the domain
- Easier to deploy
- Provides mutual authentication
- Network Policy Server must have a certificate
- Wired or wireless clients does not need a certificate

PEAP

- Used TLS to enhance security by protecting authentication traffic (EAP-MSCHAPv2 or EAP-TLS) between the wired client and the RADIUS server.
- Does not specify the authentication method
- Wired client authenticates the RADIUS server
- Protection against packet injection between wired client and RADIUS
- Fast reconnect (no re-authentication when the client moves between wireless access points)

- Not supported with EAP-MD5
- Does not support guest authentication (blank username and password)
- Support for smart cards

PEAP-MS-CHAPv2

Configure Wired Clients

- Wired AutoConfig Service
- Configure 802.1x Manually
- Configure 802.1x via Group Policy

Types of Authentication

- User Authentication

Specifies that when users are not logged on to the computer, authentication is performed by using the computer credentials.

- Computer Authentication

Authentication is always performed by using only the computer credentials

- Guest Authentication

Allows connection to the network that are regulated by the restrictions and permissions that are for the guest account