04 - Wireless Vulnerabilities

WIRELESS LAN SECURITY

Contents

- Reconnaissance Attacks
- DoS Attacks
- Authentication Attacks
- WEP Keystream and Plaintext Recovery
- WEP Key Recovery Attacks
- Attacks on EAP Protocols
- Rogue APs
- Ad-Hoc Mode Security

Reconnaissance Attacks

- Attackers can both capture and transmit wireless signals provided they are within range.
- to discover and analyze the targets of the attack.
- to determine what protocols and security mechanisms are being used.

Sniffing and SSIDs

- Sniffing refers to eavesdropping packets.
- In the wireless medium, sniffing is undetectable.
- SSIDs are broadcast in beacons from APs and in probes from stations.
- Most vendors allow SSID broadcasts to be turned off, but several tools sniff SSIDs from association packets.

Sniffing Tools

- 2 key functions: packet capture and useful packet analysis and display.
- determine what capabilities a network has
- discover interesting information
- crack WEP keys
- determine whether a network is configured correctly
- determine whether attacks are taking place

DoS Attacks

- refers to an attempt to disrupt the function of a service.
- physical destruction of network equipment
- use all of a network's bandwidth
- deny a particular person from using the service

Disassociation and Deauthentication Attacks

- exploit the unauthenticated nature of 802.11 management frames.
- Any station can spoof a disassociate or deauthenticate message, pretending to be another station.
- By repeatedly sending these frames, an attacker can keep one or more stations off a network indefinitely.

Authentication Attacks

- DoS attacks can achieve only limited goals. Network access can provide an attacker with much greater benefits.
- The original 802.11 specification defines a rather broken authentication mechanism to limit which stations can connect to the network.
- The IEEE has introduced new authentication mechanisms based on 802.1x and EAP.

Shared-Key Authentication Attacks

- Shared-key authentication is easy to forge and leaks keystream information.
- By simply XORing together the challenge and the response, an attacker can figure out a chunk of keystream corresponding to that IV. He simply encrypts whatever challenge is thrown at him with this keystream, and he is authenticated.

MAC Address Spoofing

- Several vendors' APs have the ability to limit which stations can connect based on the MAC address.
- time-consuming to configure
- unlikely to be used other than by small sites
- Several 802.11 card drivers allow users to specify whatever MAC address they want.

WEP Keystream and Plaintext Recovery

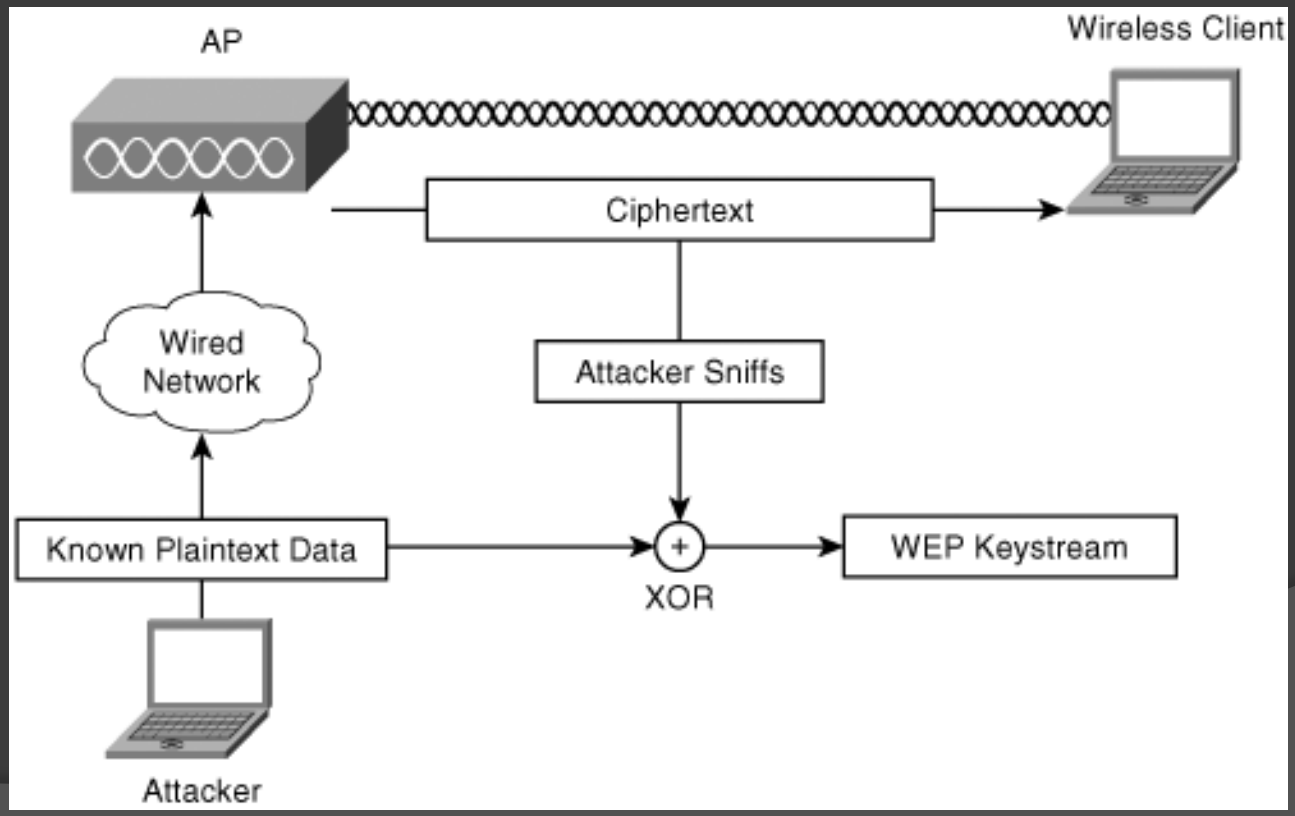
- 2 means of breaking WEP-encrypted data:
  - to discover the key itself
  - to discover all possible keystreams that a key can generate.
- RC4 encryption involves XORing the keystream (K) with the plaintext (P) data to produce the ciphertext (C). An attacker can always know C because it is broadcast. Thus, if an attacker knows P, he can get K. After he has K, he can recover P in future jackets.

Keystream Dictionaries

- The security of RC4 depends in part on not repeating the same keystream. using the IV to permit 2^{24} possible keystreams for each key.
- One method is to wait for repeated keystreams, known as a *collision*, which reveals information about the data and the keystream.
- Another method is to know some or all of the data that was encrypted, called a *known plaintext attack*.

Known Plaintext Attack

- Attacker Sends Known Plaintext to Client, Sniffs the Resulting Ciphertext, and XORs the Two to Recover the Keystream.



IV Collisions

- After a small fraction of the possible IVs have already been broadcast, it becomes difficult for a random algorithm not to rebroadcast one.
- When you do have an IV collision, it is relatively easy to compromise the data in those two packets.
- If the data is compromised, the keystream corresponding to that IV can also be compromised. This can help an attacker build up a dictionary of keystreams.

Traffic Injection: Choosing Your Own IVs

- The original 802.11 specification unfortunately allows a sender to choose his own IV and does not prohibit reuse of IVs.
- An attacker can just repeatedly reuse the same IV for which he has the keystream and inject an unlimited number of packets into a network.

Packet Decryption

- To decrypt packets from keystreams, an attacker needs a dictionary of most or all keystreams.
- After the attacker has a complete dictionary, he can decrypt every packet sent with that WEP key. This is equivalent to having the WEP key itself.

WEP Key Recovery Attacks

- One of the juiciest targets for an attacker targeting a WEP-protected WLAN is recovering the WEP key.
- Several attacks have been developed that compromise WEP keys.
- The most serious of these is the Fluhrer-Mantin-Shamir (FMS) attack, which allows a passive sniffer to recover WEP keys with as little as nine minutes of sniffing.

Dictionary-Based Key Attacks

- run all the words in a dictionary through the WEP key-generation algorithm
- operates on a file of captured packets
- First the tool finds a WEP-encrypted packet
- Then it tries to decrypt the packet using WEP keys based on all the dictionary words it has.
- If the integrity check vector of the packet is correct, the tool knows it has decrypted the packet correctly and has found the right WEP key.

The Fluhrer-Mantin-Shamir Attack

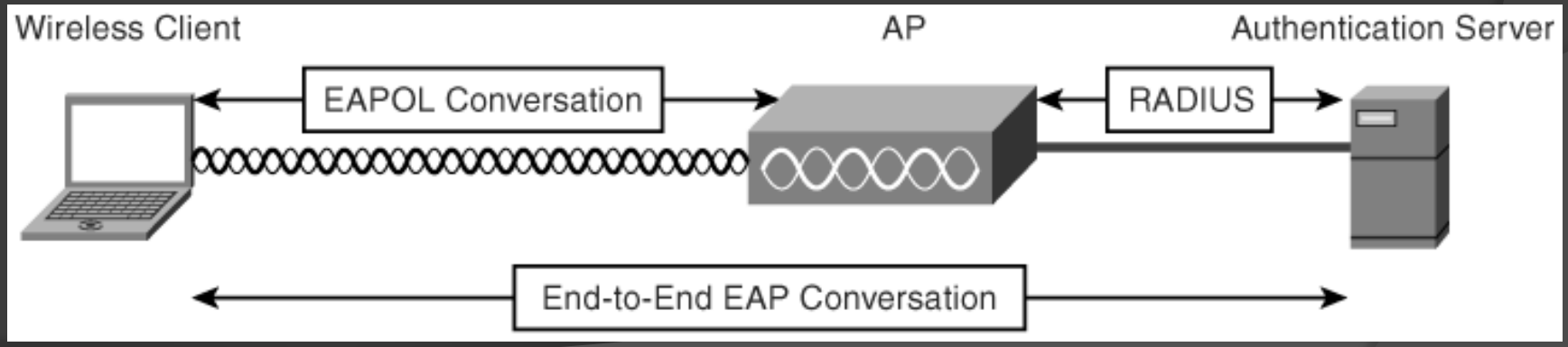
- rooted in a flaw in the key scheduling algorithm (KSA) of the RC4 encryption protocol
- a small portion of the key is slightly more likely to end up in the keystream than other values.
- The attack relies on gathering large amounts of encrypted data and looking for the packets in which the key has the weak structure.
- The more packets he gathers, the higher the assurance that he has in fact cracked the key.

Attacks on EAP Protocols

- All these protocols involve a back-end authentication server (AS), with the AP acting mostly as a conduit for the authentication messages.
- An attacker can watch the traffic and attempt to gain useful information, or
- become a participant, impersonating the client, the server, or both, as an MitM.

Summary of 802.1x and EAP

- 802.1x is a protocol designed to provide security on network ports. It uses EAP to exchange authentication information.



The 802.1x authentication

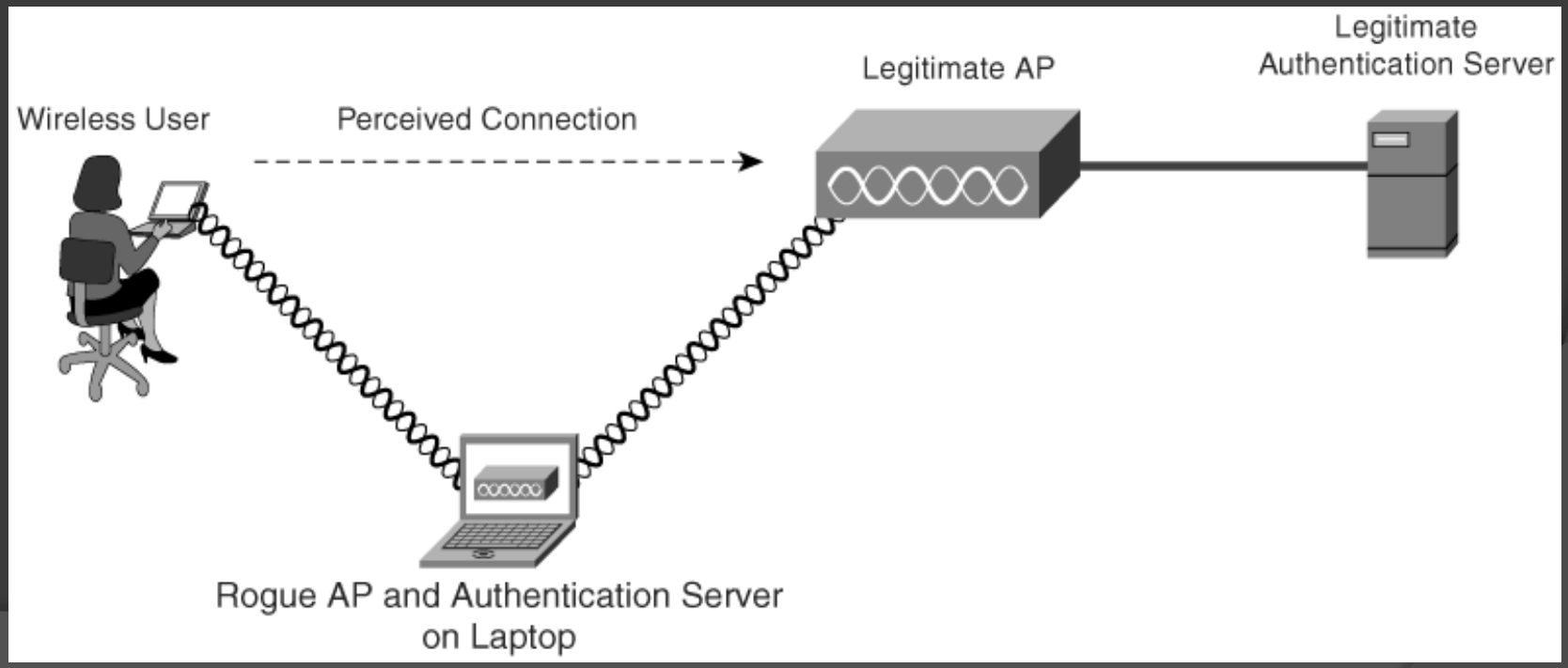
1. The client requests access.
2. The AS and client exchange messages so that the server can verify the client's identity. This might be mutual, with the client verifying the server, too.
3. When the AS is satisfied that the client has authenticated, it instructs the AP to let the client onto the network.
4. Optionally, the AS might pass additional information to the AP.

Dictionary Attack on LEAP

- The AS sends a challenge, and the client must perform a calculation based on the challenge and the password to prove that it knows the password.
- LEAP's major weakness is the use of MS-CHAPv1 in an unencrypted form for authentication.
- An attacker first must sniff both the challenge and the response of a LEAP authentication. He can then run through all the words in a dictionary and attempt to obtain the response to match the challenge.

PEAP Man-in-the-Middle Attack

- In PEAP, the client and AS set up an encrypted tunnel and then do one of several possible authentication exchanges within the tunnel.



PEAP Man-in-the-Middle Attack

- 2 key requirements:
  - The client must validate the server certificate.
  - The inner, protected authentication method must not be used outside of PEAP in a form where the attacker can sniff it.
- if the client fails to validate the server's certificate, an attacker could put up a rogue AP and AS and steal the client's credentials.

Rogue APs

- Rogue APs are unauthorized APs in a network.
- The MitM attacks require the attacker to set up a rogue AP.
- An attacker can set up a rogue AP to pose as a legitimate AP and gather user account information.

Ad-Hoc Mode Security

- In ad-hoc mode, a group of users who agree on an SSID and a channel can form a network with no AP.
- The security implications of this scenario are potentially serious because each user can be attacked by any of the other users in the network.
- Thus, personal firewalls are essential in ad-hoc networking.