Wireless Security

An Exercise in Imagination

- Materials needed: Laptop wireless card and GPS, Netstumbler, Airsnort, Ethereal
- An attacker would first use Netstumbler to drive around and map out active wireless networks
- Netstumbler not only has the ability to monitor all active networks in the area, but it also integrates with a GPS to map AP’s

An Exercise in Imagination

- At this point, the attacker has chosen his target; most likely a business
- Netstumbler can tell you whether or not the network is encrypted
- If encrypted, park the car, start up Airsnort, and leave it be for a few hours
- Airsnort, given enough time, will passively listen to traffic and figure out the encryption key

An Exercise in Imagination

- Once the encryption key is compromised, it is a trivial process to connect to the network, and if there wasn’t an encryption key at all, well then ….
- An attacker would next use Ethereal (or the packet sniffer of your choice) to listen to the network traffic, analyze, and plan further attacks

That's it…the network is compromised

- Most wireless networks are no more secure than this, many are **less** secure
- Hundreds of business's, schools, airports, and residences use wireless technology as a major point of access to their networks
- Growth of demand for Wireless LANs (WLAN) is increasing dramatically

Basic 802.11b Overview

- 802.11b was IEEE approved in 1999
- Infrastructure Mode or Ad Hoc
- Utilizes 2.4GHz band on 15 different channels (only 11 in US)
- 11mbit shared among all users on access point
- Cheap!!!

Built in Security Features

- Service Set Identifier (SSID)
- Differentiates one access point from another
- SSID is cast in ‘beacon frames’ every few seconds.
- Beacon frames are in plain text!
- First layer of security

Do’s and Don'ts for SSID’s

- Default SSID’s are well known (Linksys AP’s default to linksys, CISCO defaults to tsunami, etc) so change them immediately.
- Don’t set your SSID to something that will give away information.
- Do change the settings on your AP so that it does not broadcast the SSID in the beacon frame.

Associating with the AP

- Access points have two ways of initiating communication with a client
- Shared Key or Open Key authentication
- Open key allows anyone to start a conversation with the AP
- Shared Key is supposed to add an extra layer of security by requiring authentication info as soon as one associates

How Shared Key Auth. works

- Client begins by sending an association request to the AP
- AP responds with a challenge text (unencrypted)
- Client, using the proper WEP key, encrypts text and sends it back to the AP
- If properly encrypted, AP allows communication with the client

Is Open or Shared Key more secure?

- Ironically enough, Open key is the answer in short
- Using passive sniffing, one can gather 2 of the three variables needed in Shared Key authentication: challenge text and the encrypted challenge text

Wired Equivalent Protocol (WEP)

- Primary built security for 802.11 protocol
- Uses 40bit RC4 encryption
- Intended to make wireless as secure as a wired network
- Unfortunately, since ratification of the 802.11 standard, RC4 has been proven insecure, leaving the 802.11 protocol wide open for attack

A closer look at WEP

- Weakness in RC4 lies within the Initialization Vector (IV)
- The IV is a random 24bit number (2^24)
- Packets sent over the network contain the IV followed by the encrypted data
- RC4 combines the IV and the 40bit key to encrypt the data
- Two known attacks against this!

Taking a look back on WEP

- WEP is flawed by a technology weakness, and there is no simple solution to fix it
- Increasing key length will only help against a brute force attack. The IV is the weakness in this protocol, so increasing key length is going to help minimally (the difficulty of cracking the key increases linearly as apposed to exponentially)
- Attacks against WEP are passive and extremely difficult to detect

Security beyond 802.11 specifications

- For a secure wireless network, you MUST go above and beyond the 802.11a/b/g security measures.
- At this point, there are many measures you can take to secure a wireless network. All have their pro's and con's, and of course some work better than others
- The Goal: a secure network that is easy to deploy and maintain.

Hiding the SSID

- As stated earlier, the SSID is by default broadcast every few seconds.
- Turning it off makes it harder to figure out a wireless connection is there
- Reading raw packets will reveal the SSID since even when using WEP, the SSID is in plain text
- Increases deployment difficulty

MAC address filtering

- MAC address filtering works by only allowing specific hardware to connect to the AP
- Management on large networks unfeasible
- Using a packet sniffer, one can very easily find a valid MAC address and modify their OS to use it, even if the data is encrypted
- May be good for small networks

Virtual Private Networking (VPN)

- Deploying a secure VPN over a wireless network can greatly increase the security of your data
- Idea behind this is to treat the wireless network the same as an insecure wired network (the internet).

Deploying a VPN

- First, choosing a good secure VPN is essential, as the network will now be only as secure as the VPN itself.
- For companies already using a VPN for access to their networks over the internet, using the same VPN will greatly reduce costs
- The VPN client software must be setup on each client individually

Deploying the VPN continued…

- A secure firewall device should be setup at the point where the wireless network meets the wired network, allowing only the secure encrypted data into the wired network
- All traffic is then tunneled over the wireless network and into a VPN concentrator on the wired network

VPN is not the final solution

- Increases the amount of setup needed for each client
- VPN's are proprietary solutions, cost of deployment will vary on the size of the network
- VPN's only secure the connection to the wired network, an intruder still has full access to the wireless LAN!

VPN problems continued…

- The VPN is only as secure as each client. Compromising a client will lead to access to the wired network
- 802.11b networks that use VPN's are susceptible to piggy backing, denial of service attacks, along with any attack against the specific VPN
- VPN's require encapsulation, and thus increase overhead and decrease performance.

802.1X: A solution at last, maybe…

- 802.1X is an IEEE standard that enables layer 2 (MAC address layer) authentication and key management on IEEE 802 LAN's.
- Not limited or specific to 802.11 networks
- 802.1X is not an alternative to 802.11 or WEP, it works along with the 802.11 protocol to manage rotation of keys and authentication for WLAN clients

How authentication takes place

- A client requests access to the AP
- The AP asks for a set of credentials
- The client sends the credentials to the AP which forwards them to a RADIUS (Remote Authentication Dial-in Service) server for authorization
- The exact method for supplying credentials is not defined in 802.1X itself

Extensible Authentication Protocol (EAP)

- 802.1X utilizes EAP for it's authentication framework
- Developers may create their own methods to pass credentials
- Since it is an extensible protocol, there are a vary wide variety of available authentication methods: one time passwords, certificates, smartcards, etc

A few more benefits of 802.1X

- 802.1X does not use encapsulation, and thus has zero per packet overhead
- Because 802.1X integrates well with other open standards such as RADIUS, it is often easy and cost efficient to deploy
- Any RADIUS server (such as Windows 2000 IAS) that supports EAP can be used to manage an 802.1X network

more benefits of choosing 802.1X…

- Access points only need a firmware upgrade to enable 802.1X
- On the client side, 802.1X can be enabled with an updated driver for the NIC
- Nearly transparent setup for the client depending on the EAP you choose
- Depending on the EAP you choose, you can have a very secure wireless LAN!

A closer look at a few common EAP's

- EAP-MD5 is a simple EAP implementation
- Uses and MD5 hash of a username and password that is sent to the RADIUS server
- Has no dynamic key generation or key management, so the WEP key can still be found out through the methods described earlier
- Authenticates only one way
- It does keep attackers from using the network directly however

EAP-LEAP (Cisco Wireless)

- Like MD5-LEAP, it uses a Login/Password scheme that it sends to the RADIUS server
- Each user gets a dynamically generated one time key upon login
- Authenticates client to AP and vice versa
- Can be used along with RADIUS session time out feature, to dynamically generate keys at set intervals
- Only guaranteed to work with Cisco wireless clients

EAP-TLS by Microsoft

- Instead of a username/password scheme, EAP-TLS uses certificate based authentication
- Has dynamic one time key generation
- Two way authentication
- Uses TLS (Transport Layer Security) to pass the PKI (Public Key Infrastructure) information to RADIUS server
- Compatible with many OS's
- Hard to implement unless you do it exactly how Microsoft specifies

PEAP by Microsoft and Cisco

- A more elegant solution!
- Very similar to EAP-TLS except that the client does not have to authenticate itself with the server with a certificate, instead it **can** use a login/password based scheme
- Much easier to setup, does not necessarily require a PKI

802.1X is not perfect

- WEP is still a weakness, and only provides weak encryption and no per packet authentication
- Alternative ciphers are on the way (TKIP and WRAP)
- Some EAP's do not require mutual authentication
- Some EAP's are subject to dictionary attacks

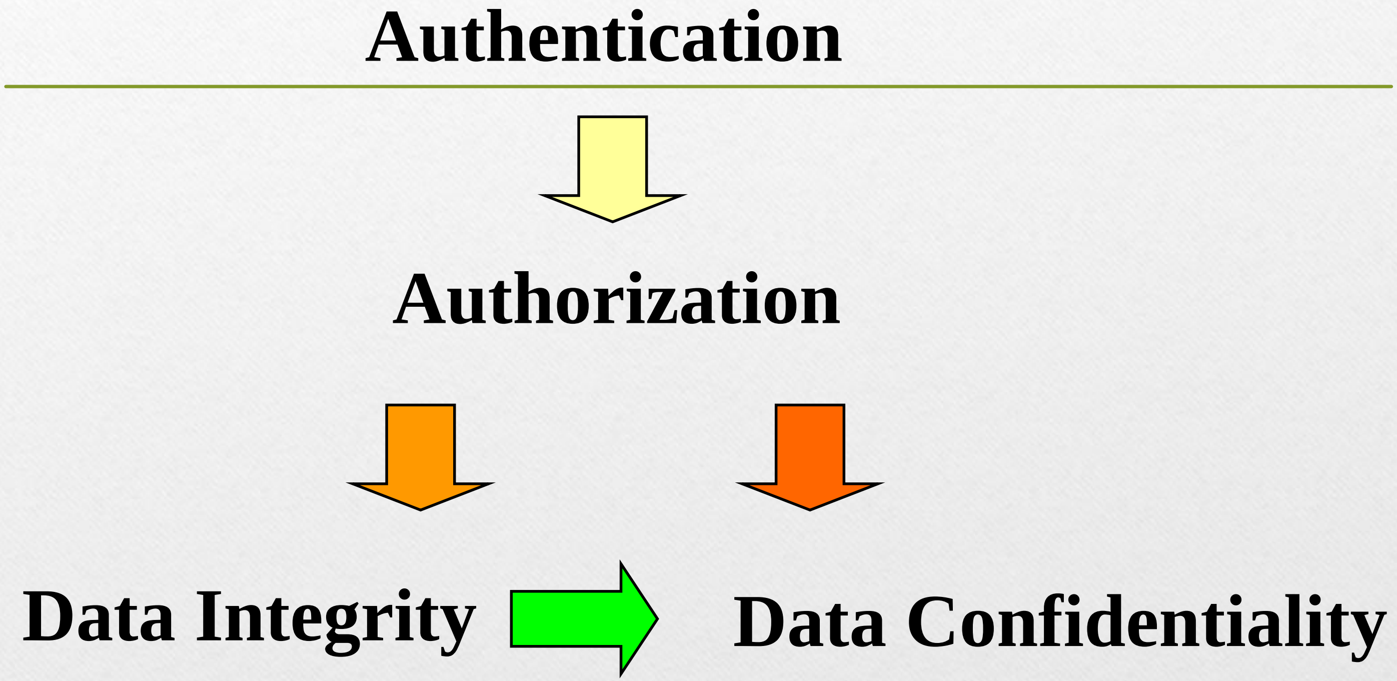
More flaws in current implementations

- 802.1X is vulnerable to many kinds of DOS attacks (spoofing logoff frames, flooding AP with start frames, and other miscellaneous packet spoofing techniques)
- Many EAP's are subject to man in the middle attacks. Recently these were found to include PEAP and EAP-TTLS

Things to keep in mind when securing a WLAN

- All WLAN should be considered insecure, and thus should be treated that way
- Never put a WLAN within the perimeter of your wired LAN’s firewall
- Don't use WEP
- Implement 802.1X with key rotation every 5' to 10‘
- Combine security mechanisms.

Security Service Dependencies



Authentication

Authorization

Data Integrity

Data Confidentiality