COURSE SAMPLE: WLAN SECURITY

Wireless LAN Threats and Vulnerabilities

- War-drivers survey for poorly protected LAN's.
- Conventional hackers may use a Wireless LAN as an easy means of access.
- Unauthorised Wireless LAN's may be deployed by employees, but typically have weak or no security.
- A rogue access points can be used in an active attack to attract and monitor traffic or to mount denial of service.

1.1 WLAN Security

1.1.1 Wireless LAN Threats and Vulnerabilities

Because no physical access is required to connect to a wireless LAN, they can provide an access mechanism for attackers wanting to target networks. The usual attacks, including theft of resources, theft of information, and Denial of Service (DoS) attacks are all possible.

In particular, the following threats should be considered:

- War-drivers look for unprotected or weakly protected wireless LANs by surveying an area, on foot or in a vehicle. Once a suitable network is identified with scanning tools, the attacker can connect and gain free Internet access, or potentially mount further attacks against the network.
- Conventional hackers who want to target the corporate network to which a wireless LAN attaches may use the wireless LAN as an easy means of access
- Unauthorised wireless LANs can easily be deployed by employees or other trusted staff, as a quick expedient to allow access to the corporate network; however these typically have weak or no security, and can allow easy access to an attacker.
- Rogue access points are bogus access points set up to masquerade as legitimate parts of the corporate network. Such as access point can attract clients and either sniff their traffic, or create a DoS attack by making locations on the legitimate network inaccessible.

A combination of strong mutual authentication of clients with APs, strong encryption of traffic travelling over the air interface, and techniques to spot or block bogus APs such as VLAN port security and Intrusion Detection Systems (IDS) can protect against these threats.

Wireless LAN Security Standards

Name	Year Standardised	Key Distribution	Device Authentication	User Authentication	Encryption
Wired Equivalent Privacy (WEP)	1997	Static	Yes (weak)	None	Yes (weak)
The interim Cisco solution while awaiting 802.11i	2001	Dynamic	Yes	Yes (802.1x)	Yes (TKIP)
Wi-Fi Protected Access (WPA)	2003	Both	Yes	Yes (802.1x)	Yes (TKIP)
802.11i (WPA2)	2005+	Both	Yes	Yes (802.1x)	Yes (AES)

1.2 Security Standards

1.2.1 Wired Equivalent Privacy (WEP)

Standards for security of wireless LANs have developed over the last several years. Early security protocols (specifically Wired Equivalent Privacy (WEP)), used a rather weak authentication and encryption scheme which proved breakable with moderate resources. WEP should not be used if possible, and should instead be replaced by one of the Wifi Protected Access/802.11i implementations.

1.2.2 Wifi Protected Access (WPA)

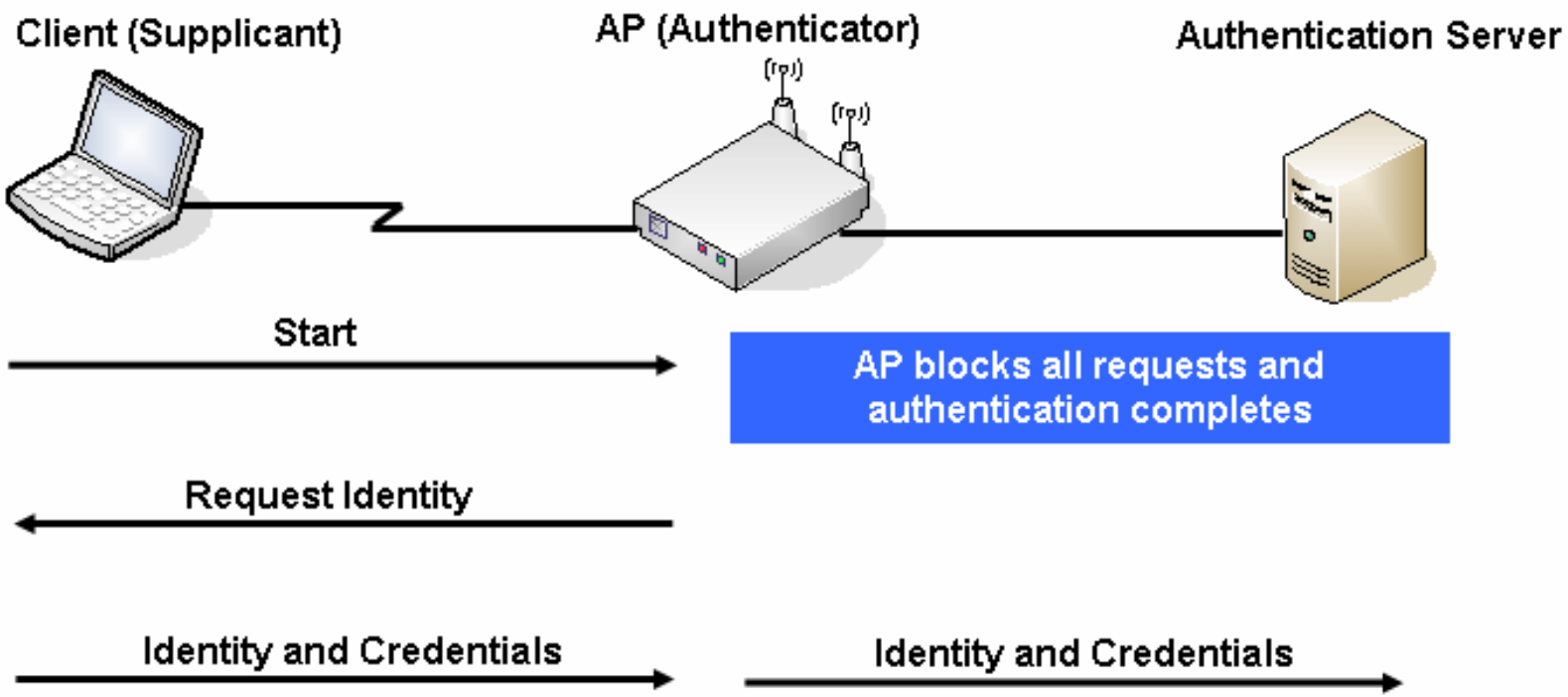
The WiFi Alliance is an industry body formed to promote the adoption and interoperability of wireless LAN systems. Ahead of ratification of a full IEEE standard to improve on WEP, they produced a pre-standard security framework called Wifi Protected Access (WPA), which made some assumptions about how the final IEEE standard would be written, and simplified its operation in certain ways. It improved over WEP in several key ways, and was widely adopted by vendors of Wireless LAN products:

- It allowed dynamic authentication of devices, rather than the static authentication using Pre-Shared Keys (PSK) used by WEP
- It allowed dynamic key generation, exchange and update, rather than the static key of WEP

1.2.3 WPA2 and 802.11i

The 802.11i standard was ratified in 2005, and is functionally similar to WPA and a Cisco interim solution which is itself rather like WPA. One powerful addition was the inclusion of the Advanced Encryption Standard (AES) in the IEEE approach, providing high-grade cryptographic protection for traffic over the air interface.

802.1x on a WLAN



1.2.4 802.1x Authentication in Wireless LANs

IEEE 802.1X is an IEEE standard for port-based Network Access Control; it is part of the IEEE 802 (802.1) group of protocols. It provides authentication to devices attached to a wired or wireless LAN port, and is supported in Cisco and numerous other wireless LAN APs. It is based upon the Extensible Authentication Protocol (EAP) defined in RFC 3748.

Upon detection of a new client connection (the supplicant), the port on the access point (authenticator) is enabled and set to the "unauthorized" state. In this state, only 802.1X traffic will be allowed; other traffic, such as DHCP and HTTP, will be blocked at the data link layer. The authenticator sends an EAP-Request identity to the supplicant, and the supplicant should respond with an EAP-response packet that the authenticator can forward to the authenticating server. The authenticating server can accept or reject the EAP-Request; if it accepts the request, the authenticator will set the port to the "authorized" mode and normal traffic will be allowed. When the supplicant logs off, it should send an EAP-logoff message to the authenticator. The authenticator will then set the port to the "unauthorized" state, once again blocking all non-EAP traffic.