




Wireless LANs

Understanding WLAN Security



Wireless LAN Security Threats

"War Drivers"	Hackers	Employees
Find "open" networks; use them to gain free Internet access	Exploit weak privacy measures to view sensitive WLAN information and even break into WLANs	Plug consumer-grade APs and gateways into company Ethernet ports to create own WLANs
		

Mitigating the Threats

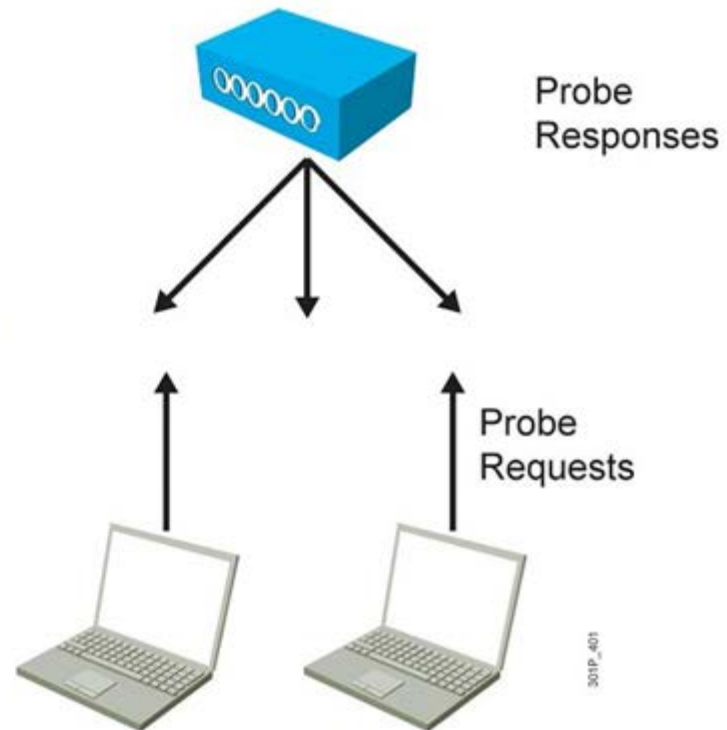
Control and Integrity	Privacy and Confidentiality	Protection and Availability
Authentication	Encryption	Intrusion Prevention System
Ensure that legitimate clients associate with trusted access points.	Protect data as it is transmitted and received.	Track and mitigate unauthorized access and network attacks.

Evolution of Wireless LAN Security

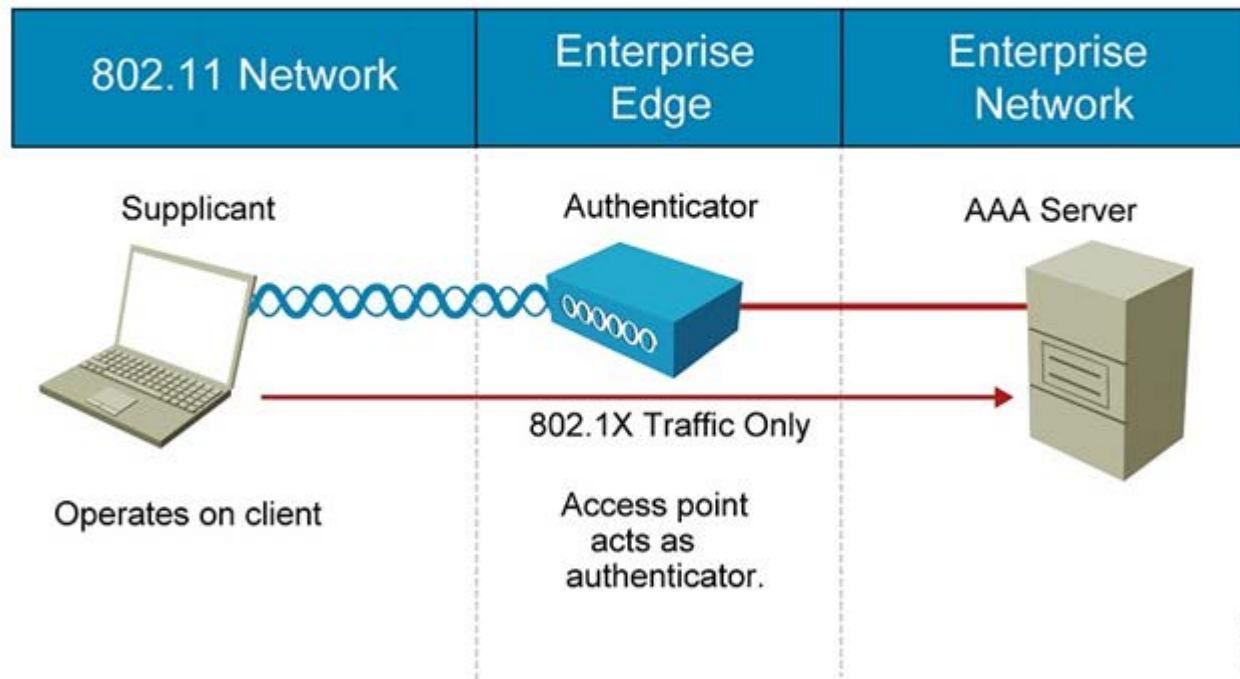
1997	2001	2003	2004 to Present
WEP	802.1x EAP	WPA	802.11i , WPA2
<ul style="list-style-type: none">▪ Basic encryption▪ No strong authentication; open and shared-key▪ Static, breakable keys▪ Not scalable▪ MAC filters and SSID-cloaking also used to complement WEP	<ul style="list-style-type: none">▪ Dynamic keys▪ Improved encryption▪ User authentication▪ 802.1X EAP (LEAP, PEAP)▪ RADIUS	<ul style="list-style-type: none">▪ Standardized▪ Improved encryption; TKIP▪ Strong user authentication (such as LEAP, PEAP, EAP-FAST)	<ul style="list-style-type: none">▪ AES strong encryption▪ Authentication▪ Dynamic key management

Wireless Client Association

- Access points send out beacons announcing SSID, data rates, and other information.
- Client scans all channels.
- Client listens for beacons and responses from access points.
- Client associates to access point with strongest signal.
- Client repeats scan if signal becomes low to reassociate to another access point (roaming).
- During association, SSID, MAC address, and security settings are sent from the client to the access point, and checked by the access point.



How 802.1X Works on the WLAN



301P_402

WPA and WPA2 Modes

	WPA	WPA2
Enterprise mode (Business, education, government)	Authentication: IEEE 802.1X, EAP Encryption: TKIP	Authentication: IEEE 802.1X, EAP Encryption: AES-CCMP
Personal mode (SOHO, home and personal)	Authentication: PSK Encryption: TKIP	Authentication: PSK Encryption: AES-CCMP

WLAN Encryption Types

WEP

- Basic encryption
- Has serious issues

TKIP

- A solution to avoid the problems of WEP
- Part of WPA

AES

- Stronger and the most resource-consuming
- Part of WPA2

VPN

- Encrypted connection between private networks over a public network
- DES, 3DES, AES, SSL

Summary

- It is inevitable that hackers will attack unsecured WLANs.
- The fundamental solution for wireless security is authentication and encryption to protect wireless data transmission.
- WLAN standards evolved to provide more security.
 - WEP
 - 802.1X, EAP
 - WPA
 - 802.11i, WPA2
- Access points send out beacons announcing SSIDs, data rates, and other information in order to support wireless client association.

Summary (Cont.)

- With 802.1X, the access point acts as the authenticator at the enterprise edge, allows the client to associate using open authentication, and provides the path to the authentication server.
- WPA provides authentication support via IEEE 802.1X and PSK.
 - Enterprise mode is a term given to products that are tested to be interoperable in both PSK and IEEE 802.1X/EAP modes of operation for authentication.
 - Personal mode is a term given to products tested to be interoperable in the PSK-only mode of operation for authentication.