Cisco.com

WLAN Security Solutions

ISSA Brussels

March 13th 2003

Franjo Majstor
Consulting Engineer
Cisco Systems, Inc
fmajstor@cisco.com

© 2003, Cisco Systems, Inc.

Agenda

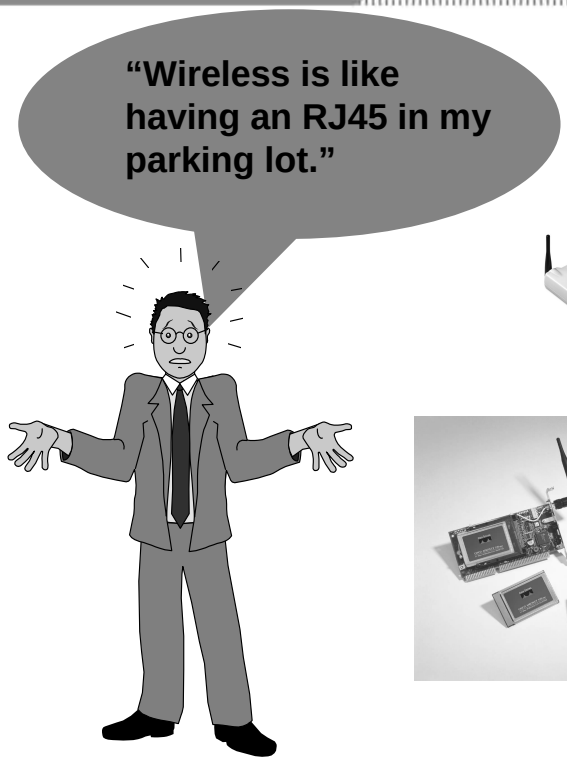
- **WLAN Technology Introduction**
  - **802.11 alphabet**
- **WLAN Security Issues**
  - **Exposures**
- **WLAN Security Solutions**
  - **WEP RC4 Enhancements (TKIP & MIC)**
  - **WPA (SSN)**
  - **802.1x and EAP(s)**
- **WLAN & VPN**
- **Q&A**

© 2003, Cisco Systems, Inc.

WLAN Technology Introduction

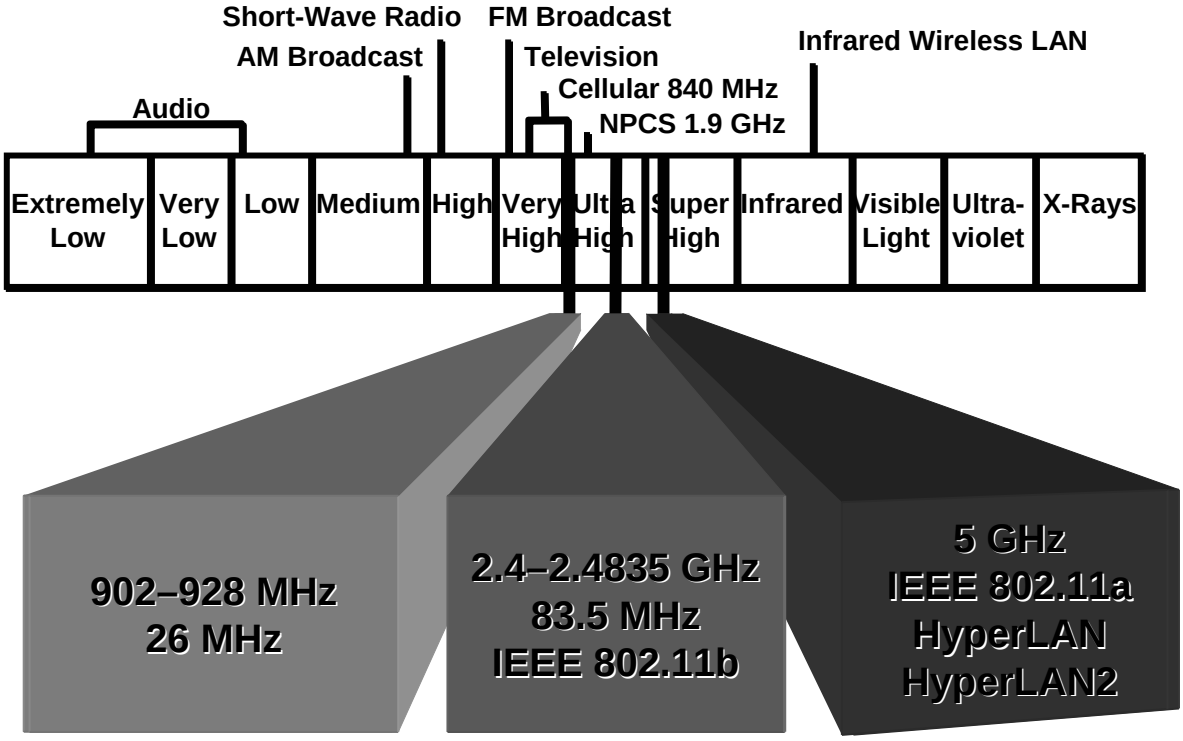
© 2003, Cisco Systems, Inc.

Wireless LAN components



© 2003, Cisco Systems, Inc.

ISM Unlicensed Frequency Bands



© 2003, Cisco Systems, Inc.

IEEE 802.11b history overview

- 802.11b standard: Ratified September 1999
  - Focused on MAC layer definition
  - Selected WEP, based on RC4 algorithm, for encryption
  - Made 40-bit WEP optional
- WECA: 40-bit WEP part of Wi-Fi™ compliance
- 802.11 Task Group I (802.11i) has worked to expand WLAN security standards to address weaknesses in 802.11 security

© 2003, Cisco Systems, Inc.

IEEE 802.11 Standard “alphabet”

- 802.11a - 5GHz- ratified in 1999
- 802.11b - 11Mbps 2.4 GHz- ratified in 1999
- 802.11g - Higher Data rate (>20 Mbps) 2.4 GHz
- 802.11d - Additional regulatory domains
- 802.11e - Quality of Service
- 802.11f - Inter-Access Point Protocol (IAPP)
- 802.11h - Dynamic Frequency Selection and Transmit Power Control mechanisms
- 802.11i - Authentication and security

© 2003, Cisco Systems, Inc.

Agenda

- WLAN Technology Introduction
- WLAN Security Issues
- WLAN Security Solutions
- WLAN and VPN
- Q&A

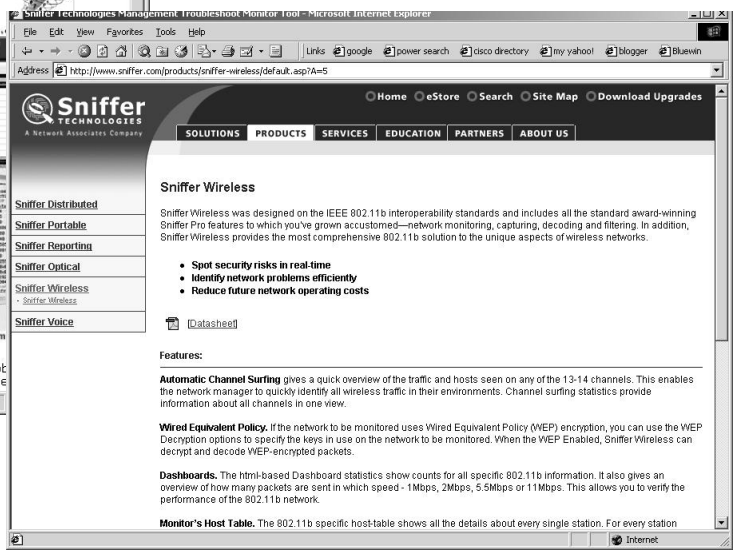
© 2003, Cisco Systems, Inc.

WLAN Security Issues

© 2003, Cisco Systems, Inc.

Sniffing 802.11 WLAN

www.wildpackets.com



www.sniffer.com

© 2003, Cisco Systems, Inc.

Wireless LAN Security Issues

THE WALL STREET JOURNAL.

© 2001 Dow Jones & Company, Inc. All Rights Reserved.

VOL. CCXXXVII NO. 25 WEDN ★★★ MONDAY, FEBRUARY 5, 2001 WSJ.com ····

Hackers Can Penetrate Wireless Network

By Jared Sandberg
Staff Reporter of The Wall Street Journal

A group of respected security research-

ple, brought to light by network-security specialists around the globe. Mr. Goldberg himself found a significant flaw in the

rel." He adds that the IEEE is working on future versions that won't be vulnerable.

connect to networks using simple radio antennas in their laptop or desktop PCs. The technology, also called Wi-Fi, is sold by many vendors but was popularized by Apple Computer Inc. under the name AirPort and is quickly being deployed in networks at a growing number of businesses, college campuses, hotels and airports. By the end of 2001, an estimated 10 million Wi-Fi radios will be deployed, according to research firm Cahners In-Stat. Starbucks Corp., for instance, plans to use the technology to allow latte quaffers to noodle around the Internet.

The weakness is another reminder of the difficulty in implementing effective network security.

chief scientist at Zero Knowledge Systems

Hacking into WEP

"War Driving"

Credit: KNTV San Jose

© 2003, Cisco Systems, Inc.

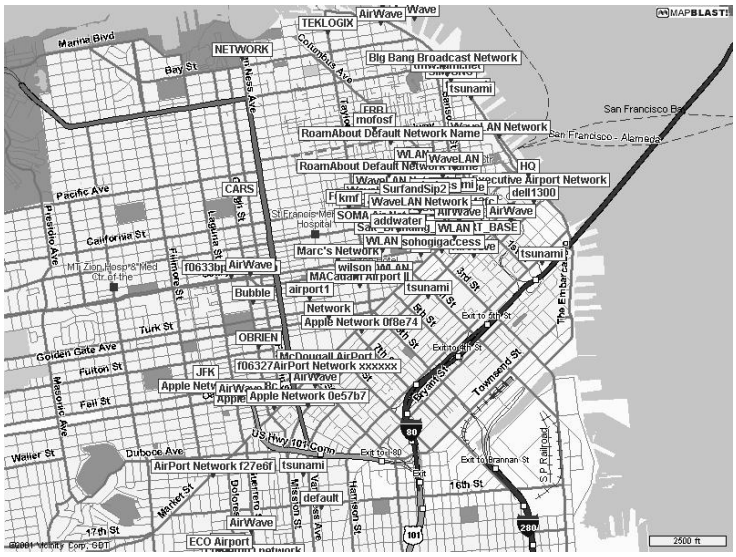
Wardriving …

… is possible as it has been proven by "War driving" exercise in SFO:

= cruising with a car + laptop + WLAN card

+ GPS scanning for (unprotected) 802.11 wireless networks.

+ Perl script to log the SSID, AP's MAC address, best S/N ratio and location (GPS).



www.personaltelco.net/index.cgi/WarDriving

© 2003, Cisco Systems, Inc.

Media Attention to Rogue APs Wardriving

War Driving (wôr dri'vin) ***v.***

1 Driving around looking for unsecured wireless networks.

- term coined by Pete Shipley

- **12,600 hits on google for wardriving**
- **Most wardrivers use NetStumbler to find, map (using GPS), and upload locations of discovered APs to online database**
- **NetStumbler is a free download for Windows and WinCE**

http://www.wirelesscentral.net/aprod/STUM-ANTW.html?ns

Pringles can Antenna
- **12 Dbi Gain**
- **45 minutes to construct**
- **$6.45 total cost**

http://www.oreillynet.com/cs/weblog/view/wlg/448

© 2003, Cisco Systems, Inc.

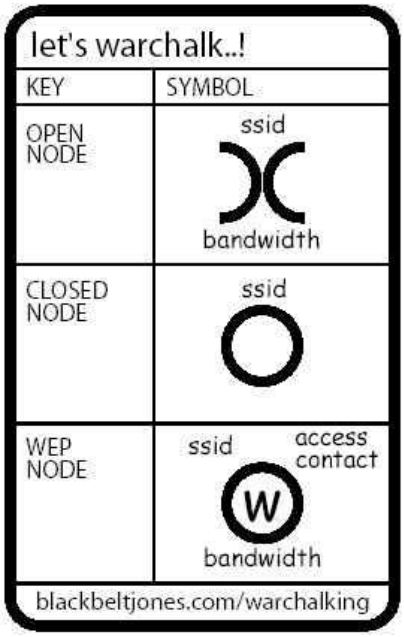
Warchalking

© 2003, Cisco Systems, Inc.

Warchalking

© 2003, Cisco Systems, Inc.

Media Attention to Rogue APs WarChalking



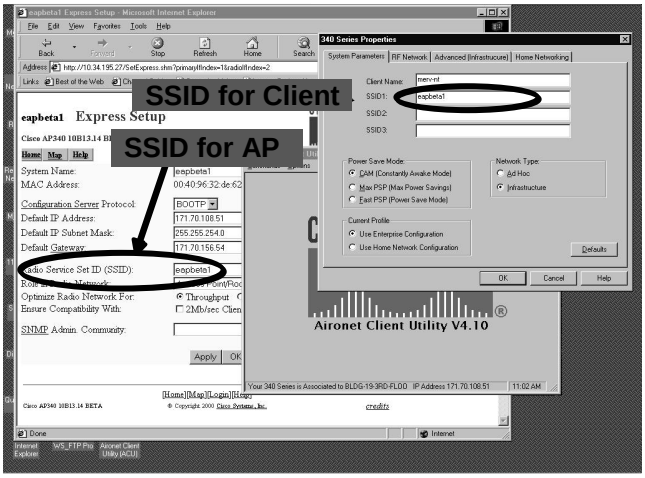
What is Warchalking?

- Warchalking is the process of looking for wireless computer networks and making chalk marks to indicate their locations so that others can more easily find them.
- http://www.warchalking.org/
  - Online community containing descriptions and photos of warchalked sites
- 12,100 hits on Google for "warchalking"

© 2003, Cisco Systems, Inc.

Service Set Identifier (SSID) in 802.11b

- **32 ASCII character string**
- **Sent in the clear**
- Commonly used feature for WLAN identification
- May be advertised or manually pre-configured at the station



- Serves to logically segment the users and Access Points that form part of a Wireless subsystem.
- **<u>Is NOT a security feature!</u>**

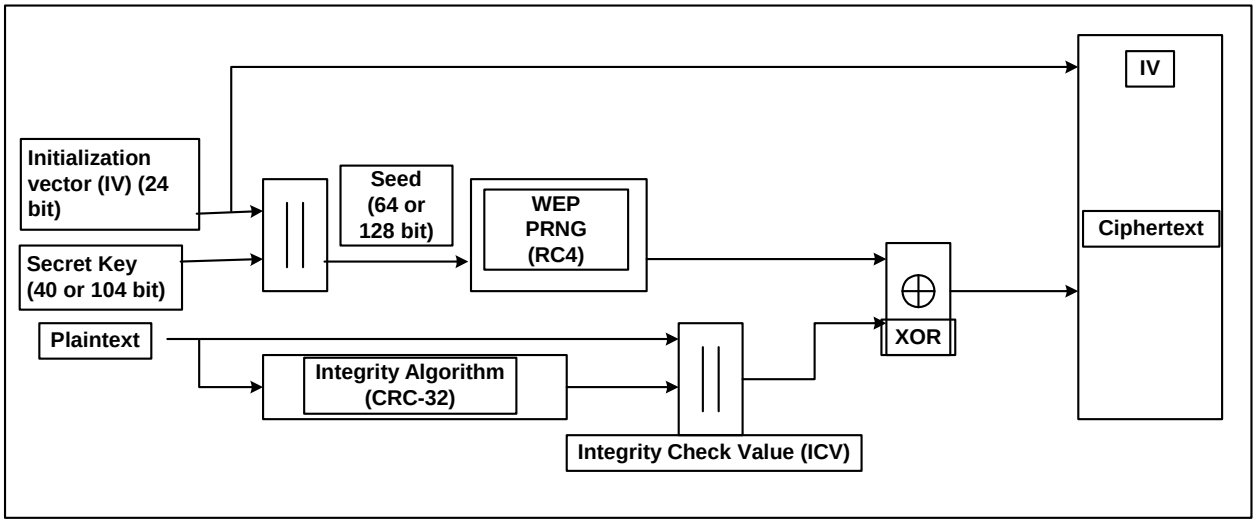
© 2003, Cisco Systems, Inc.

Wire Equivalent Privacy (WEP)

- **Uses the RC4 stream cipher of RSA Data Security for encryption.**
- **RC4 Keystream = (24 bits IV , WEP Key)**
- **Key must be shared by both the encrypting and decrypting endpoints.**
- **IEEE 802.11b has chosen to use 40-bit keys. Several vendors Cisco support 128-bit WEP encryption with their WLAN solutions. Cisco in HW (3 % degradation only)**
- **Key distribution or key negotiation is not mentioned in the standard.**

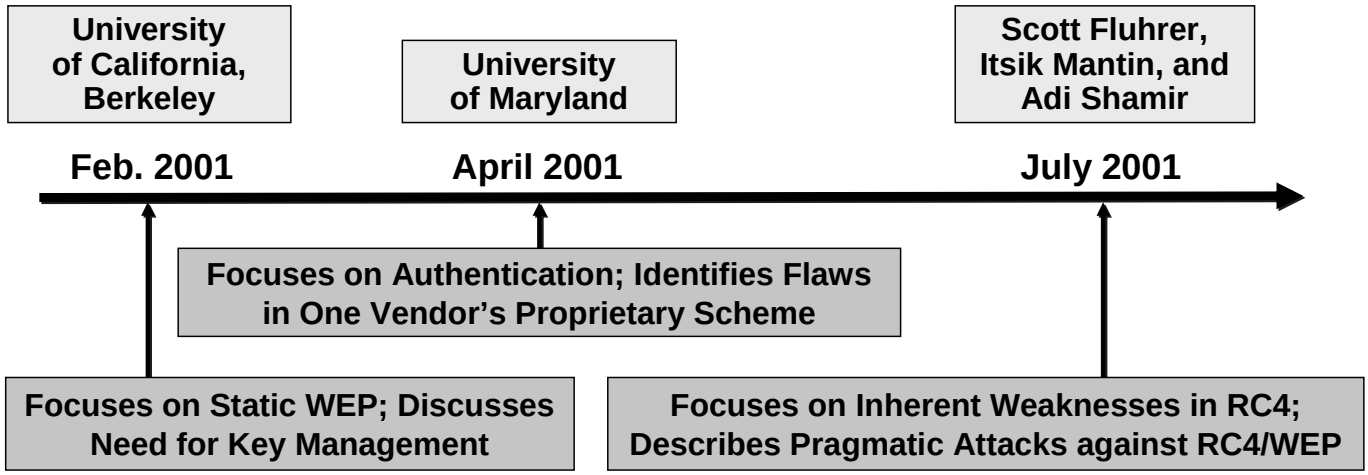
© 2003, Cisco Systems, Inc.

802.11b WEP Encryption



© 2003, Cisco Systems, Inc.

Papers on WLAN Security

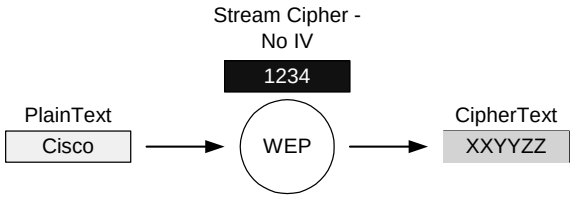


> "In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks we describe…"

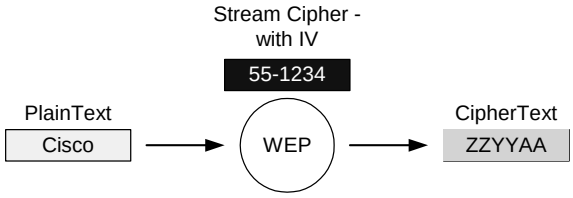
University of California, Berkeley Report on WEP Security, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

© 2003, Cisco Systems, Inc.

What is an IV?



Without an IV, the plaintext will always produce the same ciphertext. An eavesdropper will be able to 'see' patterns and predict plaintext



With the IV, the ciphertext will change as the IV changes, so it will be more difficult for an eavesdropper to 'see' patterns and predict plaintext

- **Same plaintext packet should not generate same ciphertext packet**
- **IV is random 24 bits long string (24 bits + 104 bits WEP key = 128 bits) and changes per packet**

© 2003, Cisco Systems, Inc.

WEP: AirSnort "Weak IV" Attack

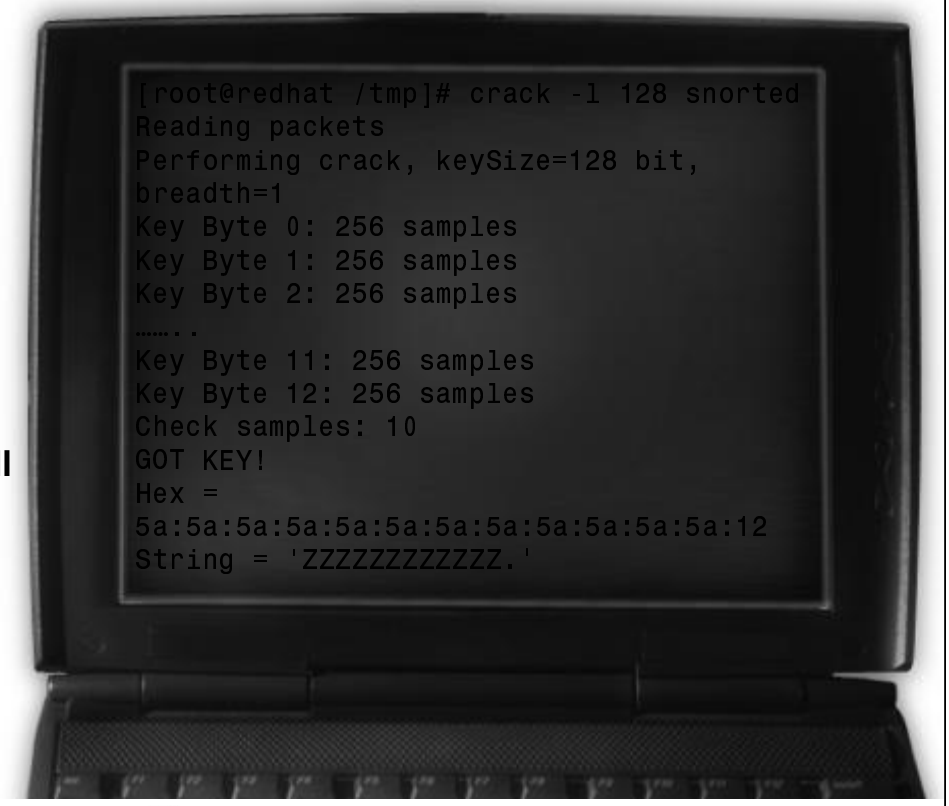
- **Attack is based on Fluhrer/Mantin/Shamir paper**
- **Initialization vector (IV) is 24-bit field that changes with each packet**
- **RC4 Key Scheduling Algorithm creates IV from base key**
- **Flaw in WEP implementation of RC4 allows creation of "weak" IVs that give insight into base key**
- **More packets = more weak IVs = better chance to determine base key**
- **To break key, hacker needs 100,000-1,000,000 packets**

WEP frame

© 2003, Cisco Systems, Inc.

Airsnort

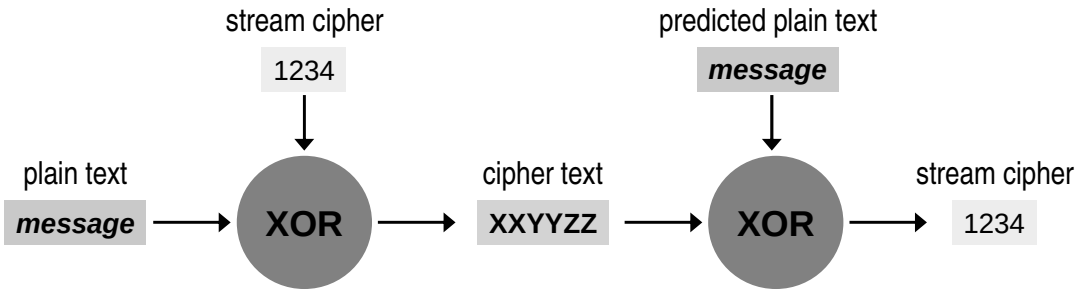
- Capture enough packets
- Crack phase
- For every byte of the key, there are 256 weak IVs.
- 13 key bytes * 256 = 3315 packets to get all weak keys
- You do not need sometimes all of the weak keys to break the WEP key



© 2003, Cisco Systems, Inc.

WEP: Bit-Flipping and Replay Attack

- Hacker intercepts WEP-encrypted packet
- Hacker flips bits in packet and recalculates ICV CRC32
- Hacker transmits to AP bit-flipped frame with known IV
- Because CRC32 is correct, AP accepts, forwards frame
- Layer 3 device rejects and sends predictable response
- AP encrypts response and sends it to hacker
- Hacker uses response to derive key (stream cipher)



© 2003, Cisco Systems, Inc.

Limitations of 802.11 Security

Authentication

- Authentication is device-based, not user-based
- Client does not authenticate network
- Existing authentication databases are not leveraged

Key management

- Keys are static
- Keys are shared among devices and APs
- If adapter or device is stolen, all devices and APs must be rekeyed

RC4-based WEP keys

- Encryption algorithm is vulnerable to attack
- Message integrity is not ensured

© 2003, Cisco Systems, Inc.

Agenda

- WLAN Technology Introduction
- WLAN Security Issues
- WLAN Security Solutions
- WLAN and VPN
- Q&A

© 2003, Cisco Systems, Inc.

WLAN Security Solutions

© 2003, Cisco Systems, Inc.

Addressing the Limitations: 802.11i

Authentication

- Authentication is device-based, not user-based
- Client does not authenticate network
- Existing authentication databases are not leveraged

Key management

- Keys are static
- Keys are shared among devices and APs
- If adapter or device is stolen, all devices and APs must be rekeyed

802.1x

RC4-based WEP keys

- Encryption algorithm is vulnerable to attack
- Message integrity is not ensured

TKIP and AES

© 2003, Cisco Systems, Inc.

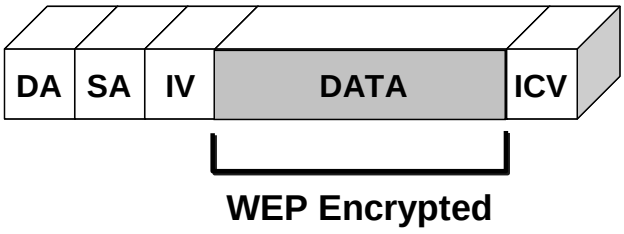
Security Enhancements for RC4 based WEP

- **Security Enhancements to Strengthen RC4-Based WEP Keys:**
  - **Message Integrity Check (MIC)**
  - **Key Hashing or Temporal Key (TK) of TKIP**
  - **Linear Initialization Vector (IV) Sequencing**
  - **Broadcast Key rotation**

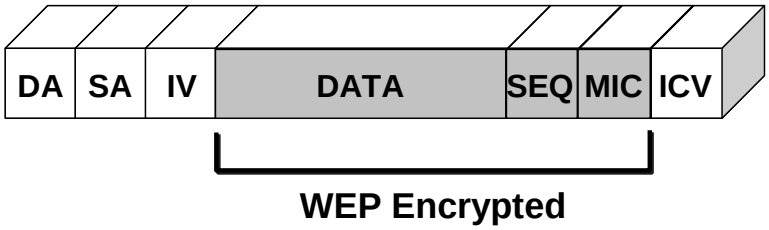
© 2003, Cisco Systems, Inc.

Message Integrity Check

WEP Frame - No MIC



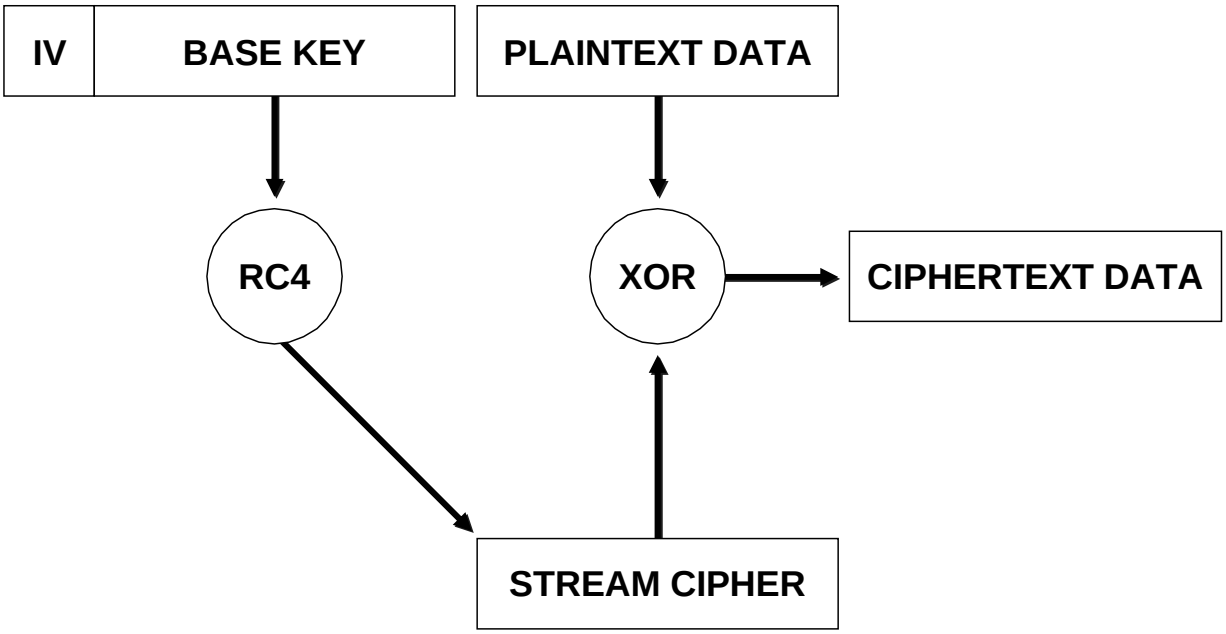
WEP Frame - MIC



© 2003, Cisco Systems, Inc.

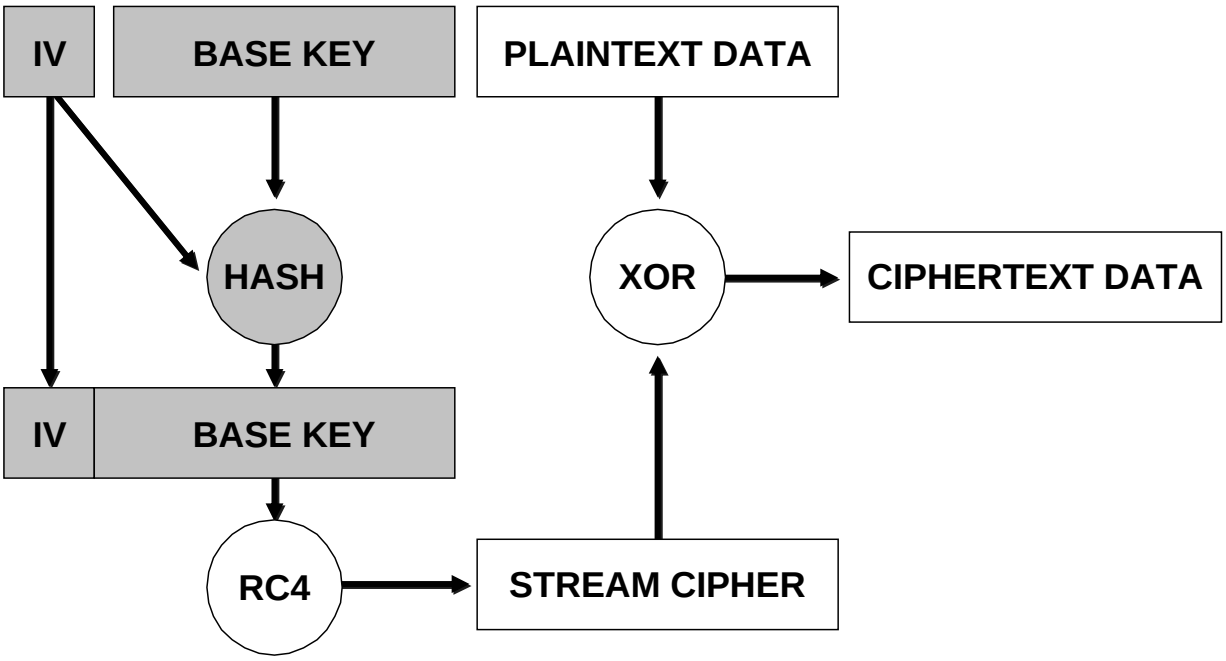
IV Key Hashing/Temporal Key

WEP Encryption Today



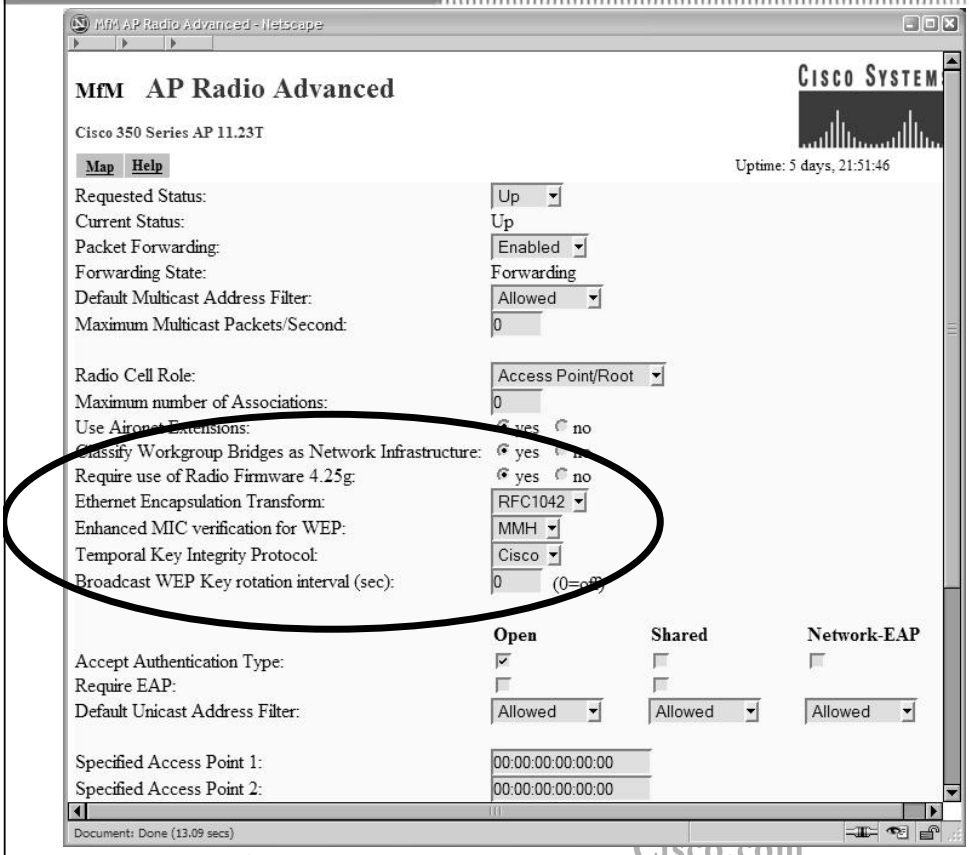
© 2003, Cisco Systems, Inc.

IV Key Hashing/Temporal Key



© 2003, Cisco Systems, Inc.

WEP enhancements - TKIP/MIC



- **WEP Security enhancements:**

- TKIP (Temporal Key Integrity Protocol) hashing to address WEP key vulnerabilities

- MIC (Message Integrity Check) to address bit flipping and replay attacks

© 2003, Cisco Systems, Inc.

Linear IV Sequencing

- **Instead of random collision times, move through the IV listing in a linear fashion**
- **Broadcast key must be rotated before utilizing the entire IV space (~min 2.03h, optimal 10h)**
- **Added benefit is that if packet is using the previous IV, it will be rejected because the transmitter is expecting the next linear IV**

© 2003, Cisco Systems, Inc.

Broadcast Key Rotation

- Static Broadcast Key is vulnerable to FMS attack over time
  - Similar to static WEP Keys
- Using Broadcast Key rotation will prevent static WEP users from functioning correctly.
- Broadcast Key = Hash (seed, ap_mac_addr, #boots)

© 2003, Cisco Systems, Inc.

Static WEP vs. EAP-TLS vs. EAP-Cisco

Attack	WEP	EAP-TLS	IV Hashing	MIC	Broadcast Key Rotation	EAP-Cisco Wireless (LEAP)
IV Reuse/Collision	✗				✓	
CRC32 bit-flipping	✗			✓		
CRC32 replay	✗			✓		
Authentication forging	✗					✓
FMS Attack	✗		✓			
Rogue AP	✗					✓
Dictionary attack	✗	✓				

© 2003, Cisco Systems, Inc.

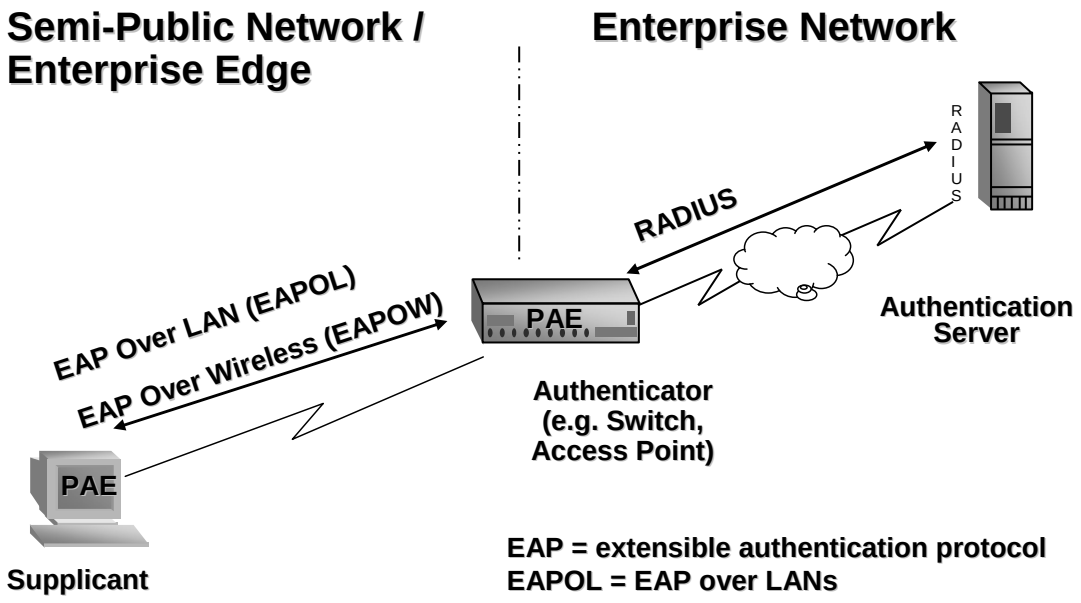
IEEE 802.1x Defined

Port based network access control

- 802.1x is an IEEE Standard in progress for Port Based Network Access Control, EAP based
- Falls under 802.1 NOT 802.11
- NETWORK standard, not a wireless standard
- Provides Network Authentication, NOT encryption
- Improved authentication: username/password
- Works on 802.3 LAN switch or 802.11b WLAN AP
- To be used for centralized user administration
- Is PART of the 802.11i draft

© 2003, Cisco Systems, Inc.

IEEE 802.1x Terminology



EAP = extensible authentication protocol
EAPOL = EAP over LANs
PAE = port access entity
Port = network access port
RADIUS = remote authentication dial in user service

© 2003, Cisco Systems, Inc.

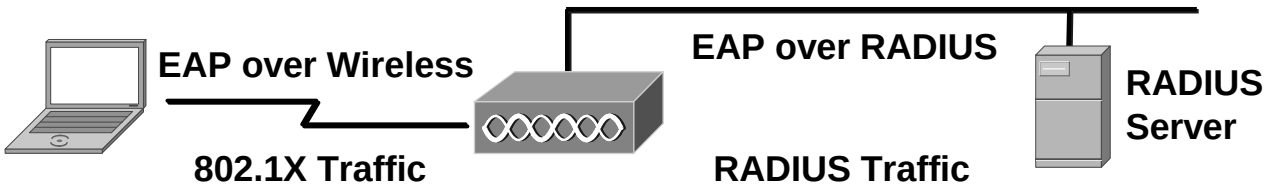
What Is EAP?

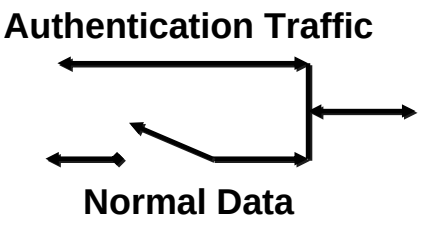
- EAP - The Extensible Authentication Protocol
- A flexible protocol used to carry arbitrary authentication information
- Typically rides on top of another protocol such as 802.1x or RADIUS (could be TACACS+, etc.)
- Specified in RFC 2284
- Support multiple "authentication" types:
  - Plain password hash (MD5) (not mutual)
  - OTP Tokens (not mutual)
  - TLS (based on X.509 certificates)
  - And EAP-Cisco Wireless!!

© 2003, Cisco Systems, Inc.

Before EAP Starts

802.11 Association Complete; Data Blocked by AP



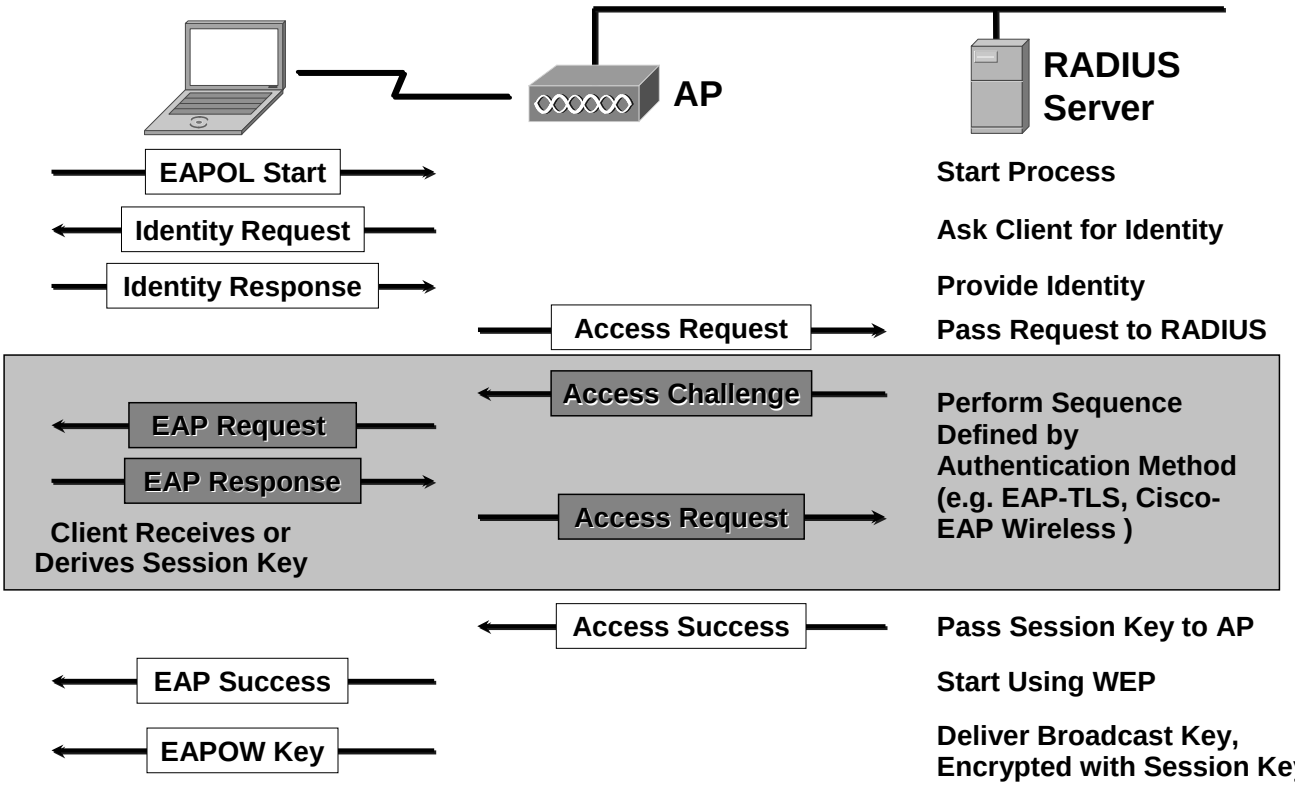


AP "Encapsulates" 802.1x Traffic into RADIUS Traffic, and Visa Versa

AP Blocks Everything but 802.1x-to-RADIUS Authentication Traffic

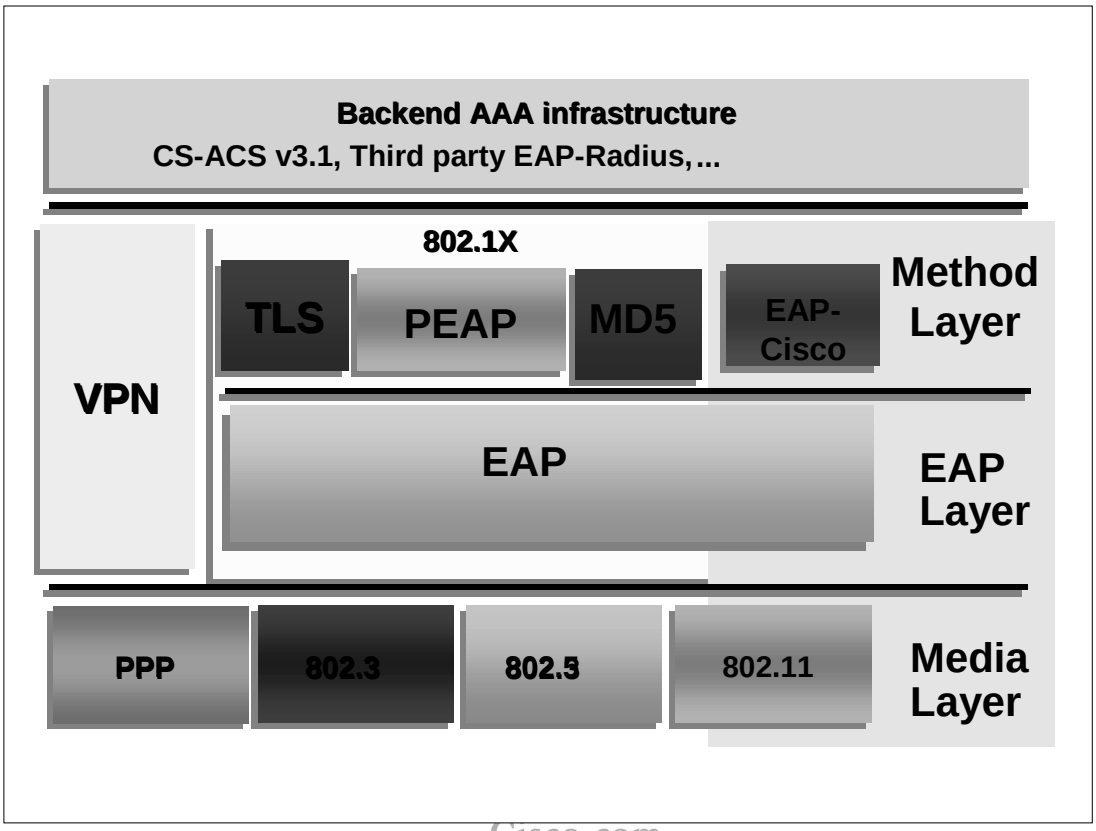
© 2003, Cisco Systems, Inc.

802.1x/EAP Steps



© 2003, Cisco Systems, Inc.

New WLAN Security Framework



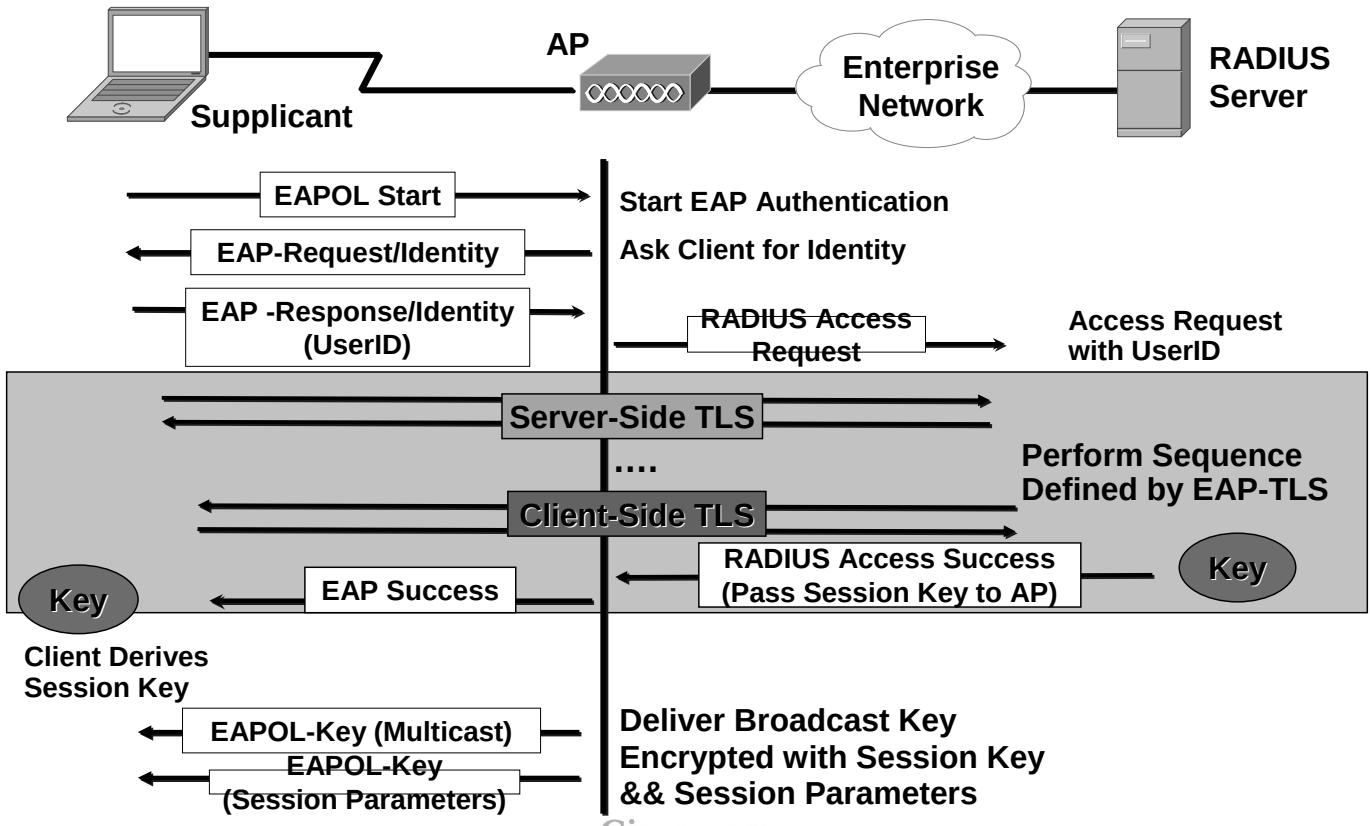
© 2003, Cisco Systems, Inc.

802.1x Extensible Authentication Protocols

- **EAP-MD5 (Message Digest 5)**
  - Is supported in Win 2K/XP and, soon, other Windows versions
  - Does *not* provide *mutual* authentication *nor WEP key derivation*
- **EAP-Cisco Wireless, or LEAP**
  - Is supported by Cisco Aironet client adapters on Windows, CE, Linux, Mac OS, and DOS
  - Has been licensed to other vendors
- **EAP-TLS (mutual EAP-TLS)**
  - Is supported in Win 2K/XP and, soon, other Windows versions
  - Requires *client certificates* and *server certificates*
- **PEAP**
  - Is supported in XP and, soon, other Windows versions
  - Uses server-side TLS, which requires *only server certificates*
- **EAP-TTLS**
  - Is supported by Funk Software's Odyssey
  - Uses server-side TLS

© 2003, Cisco Systems, Inc.

EAP-TLS Authentication



© 2003, Cisco Systems, Inc.

What is PEAP?

- *PEAP* = Protected EAP (Extensible Authentication Protocol)
- 802.1x - based authentication protocol based on EAP
- Leverages server-side EAP-TLS using digital certificates
- Supports a variety of different client authentication methods, including log-on passwords and one-time passwords (OTPs)
- Based on a RFC Draft jointly submitted by Cisco Systems, Microsoft and RSA Security to the IETF
- Initial support on Windows XP and Cisco W2K/XP client

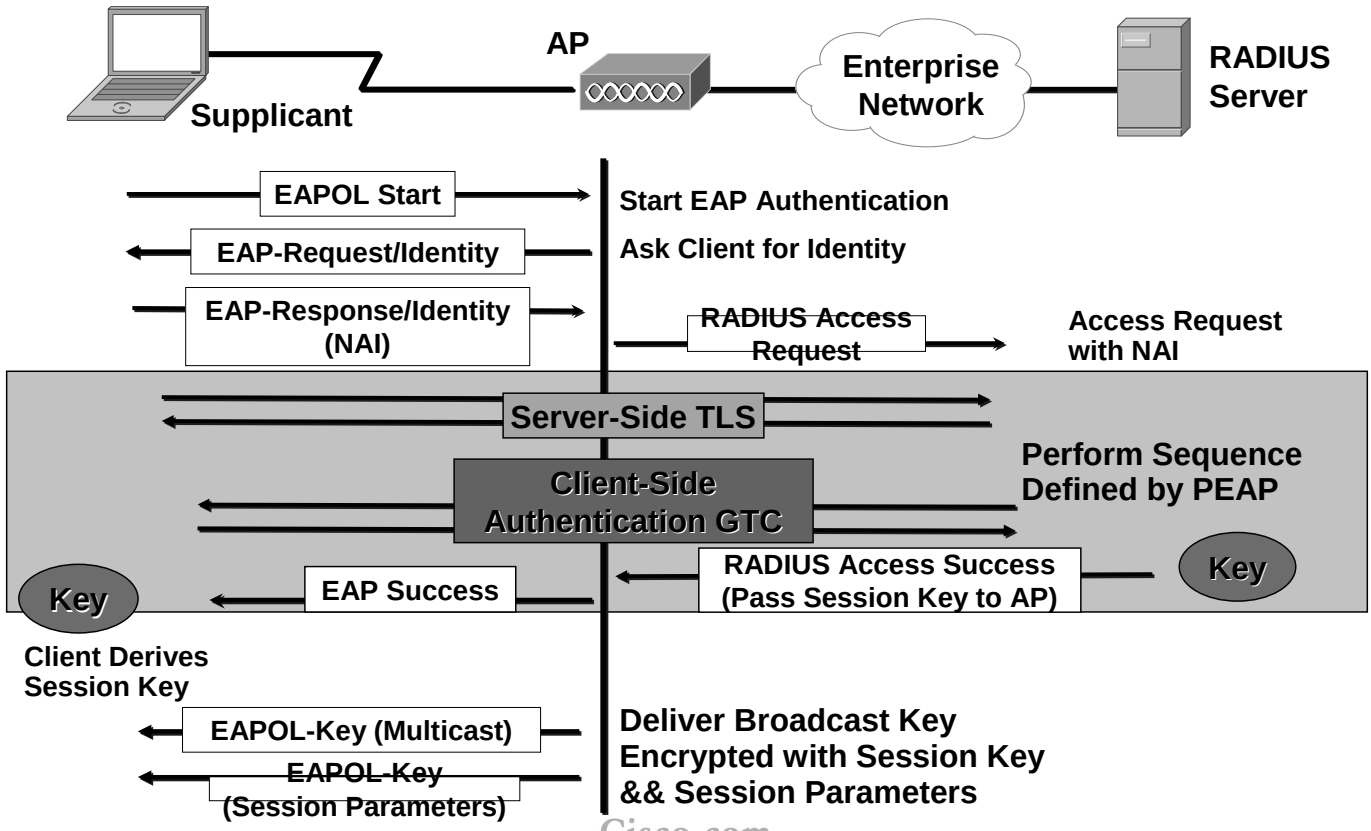
© 2003, Cisco Systems, Inc.

PEAP Authentication Process

- Two Phase Authentication:
  - Phase 1: Server side TLS authentication is performed to create an encrypted tunnel (similar to SSL)
  - Phase 2: Methods such as Generic Token Card (GTC) are used to authenticate the Client to the Server
- PEAP requires Server side certificate only (whereas EAP-TLS requires both Server and Client side certificates)

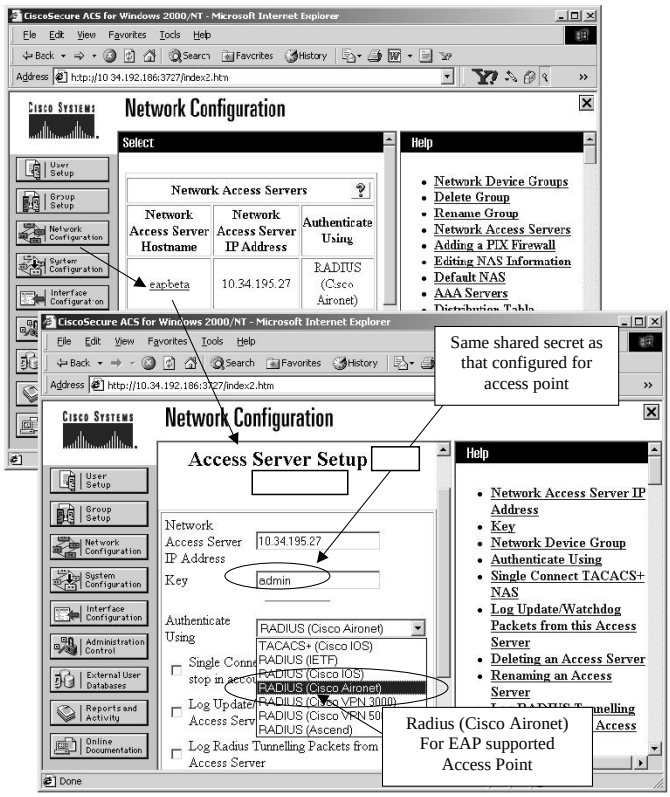
© 2003, Cisco Systems, Inc.

PEAP Authentication Overview



© 2003, Cisco Systems, Inc.

What is the role of the RADIUS Server



- **WEP key is calculated by the RADIUS server, only after the authentication is completed**
- **The key is passed to access point for THAT single authenticated client; this is a *session* key**
- **Client calculates the same WEP key**
- **Key is *never* transmitted over RF**

© 2003, Cisco Systems, Inc.

How Often to Change Key

- Every time a client roams to a new AP, it will go through the same authentication and get new WEP session key
- RADIUS server will also require a new authentication / key at a pre-defined time interval (Attribute 027, Session -Timeout)
- This provides different and totally unique WEP key to each client

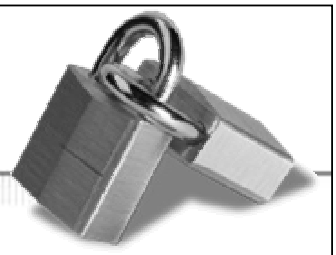
© 2003, Cisco Systems, Inc.

802.1x EAP Authentication Comparison

	LEAP	PEAP	EAP-TLS
Multi-Operating System Support	Yes	No	No
Single Sign On For Windows Log-In	Yes	No*	Yes
Dynamic WEP Key and Mutual Authentication	Yes	Yes	Yes
Static Password Support	Yes	Yes	No
One Time Password Support	No	Yes	No
SERVER Certificate Required	No	Yes	Yes
CLIENT Certificate Required	No	No	Yes
Layer 3 Roaming Support	Yes	Yes	Yes
MS Windows Password Change	No	Yes	No
Microsoft Backend DB Support	Yes	Yes	Yes
LDAP/NDS Backend DB Support	No	Yes	Yes

© 2003, Cisco Systems, Inc.

IEEE 802.11i Security



- grouper.ieee.org/groups/802/11/Reports/tgi_update.htm
  - Fixes to WEP:
  - TKIP (Temporal Key Integrity Protocol)
    - Text/hash function/MIC
  - AES proposals (new HW)
    - All MIC/IV Hash/IV Sequencing/Rapid Rekey to informative text
    - Replace next generation of WEP with TKIP

- www.wi-fi.com (Wi-Fi Aliance, ex. WECA - Wireless Ethernet Compatibilty Alliance):
  - SSN (Safe Secure Networks)
  - WPA (Wi-Fi Protected Access)

© 2003, Cisco Systems, Inc.

Addressing the Limitations: 802.11i

Authentication
- Authentication is device-based, not user-based
- Client does not authenticate network
- Existing authentication databases are not leveraged

Key management
- Keys are static
- Keys are shared among devices and APs
- If adapter or device is stolen, all devices and APs must be rekeyed

RC4-based WEP keys
- Encryption algorithm is vulnerable to attack
- Message integrity is not ensured

802.1x + TKIP and AES = SSN = WPA

© 2003, Cisco Systems, Inc.

WPA - Wi-Fi Protected Access

- What? WPA = 802.1x + TKIP
  - A non-802.1x option exists for home/SOHO products
- Why?
  - 802.1x and TKIP are key elements of 802.11i
  - Industry is tired of waiting for 802.11i to be ratified
  - Responding to push from Microsoft, Wi-Fi Alliance agreed to incorporate WPA into Wi-Fi compliance testing
- When?
  - Optional testing begins in February 2003
  - WPA compliance is needed for new Wi-Fi certification beginning in August 2003
- Result: WPA is new industry baseline for WLAN security

www.wi-fi.com/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf

© 2003, Cisco Systems, Inc.

Agenda

- WLAN Technology Introduction
- WLAN Security Issues
- WLAN Security Solutions
- WLAN and VPN
- Q&A

© 2003, Cisco Systems, Inc.

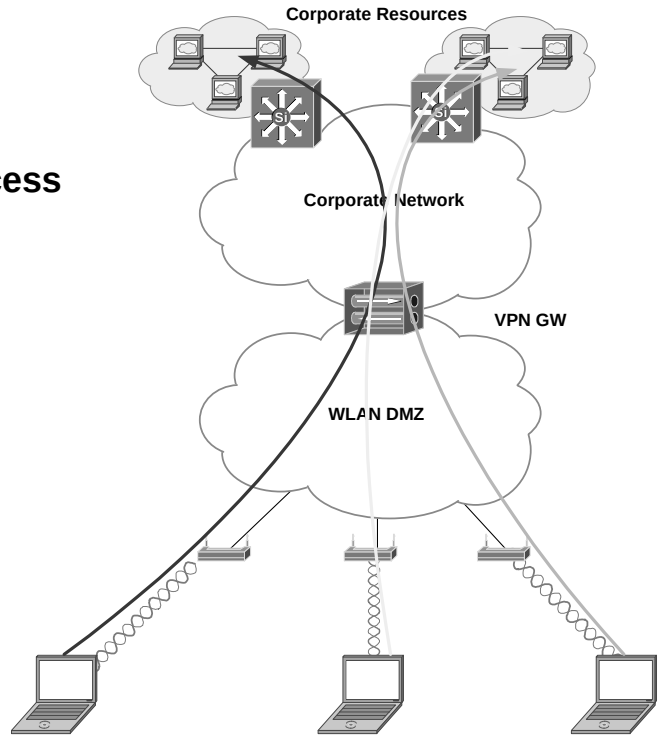
WLAN and VPN

© 2003, Cisco Systems, Inc.

VPN over WLAN Infrastructure

Definitions and Scope:

- **VPN = IPsec based VPN**
- **WLAN = 802.11 based access**



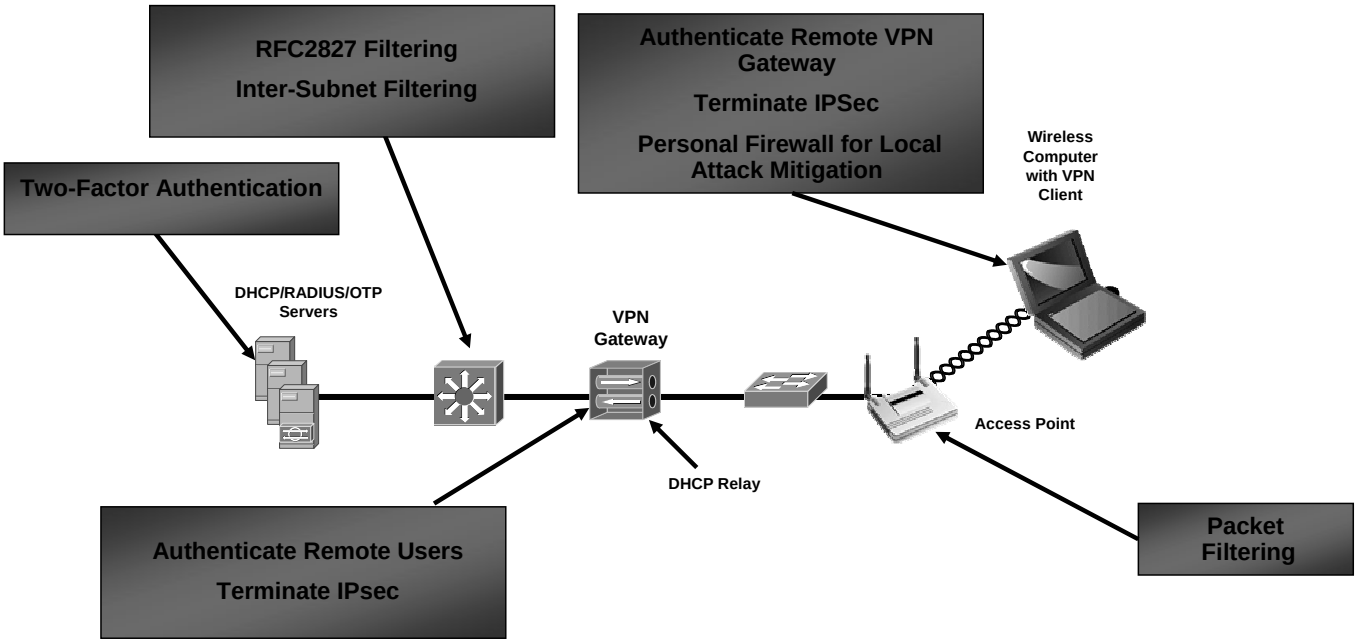
© 2003, Cisco Systems, Inc.

When to use VPN over WLAN?

- In mixed client environments
- Where security is more important that performance or usability
- Home office, remote telecommuters, medium design, large scale designs...

© 2003, Cisco Systems, Inc.

Generic VPN WLAN Design

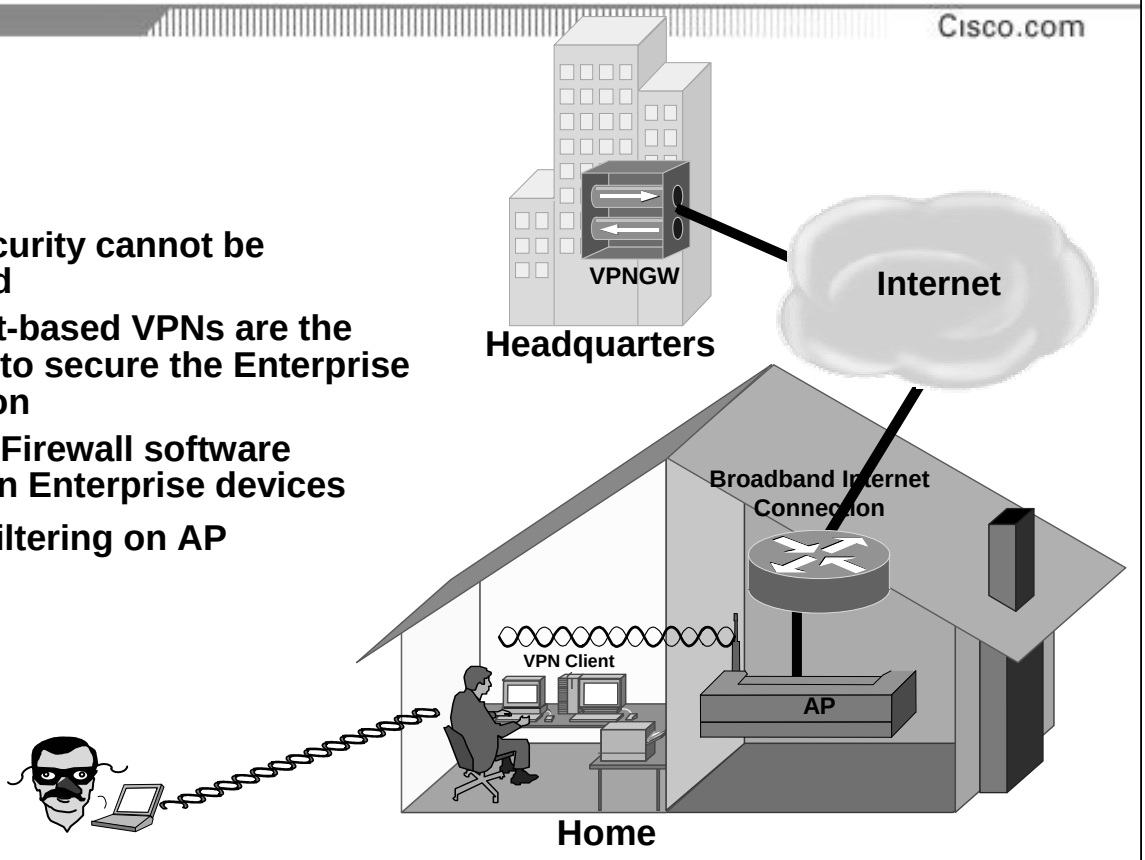


http://Cisco.com/go/SAFE

© 2003, Cisco Systems, Inc.

Enterprise Day Extender/Telecommuter

- Home security cannot be controlled
- SW Client-based VPNs are the best way to secure the Enterprise connection
- Personal Firewall software needed on Enterprise devices
- Use RF Filtering on AP



© 2003, Cisco Systems, Inc.

Access Point Filtering on RF side

Filter type	Protocol	Value	Action
Ethertype	ARP	0x0806	Forward
Ethertype	IP	0x0800	Forward
IP protocol	UDP	17	Forward
IP protocol	ESP	50	Forward
UDP port	BootPC*/ BootPS**	68/67	Forward
UDP port	DNS	53	Forward
UDP port	IKE	500	Forward

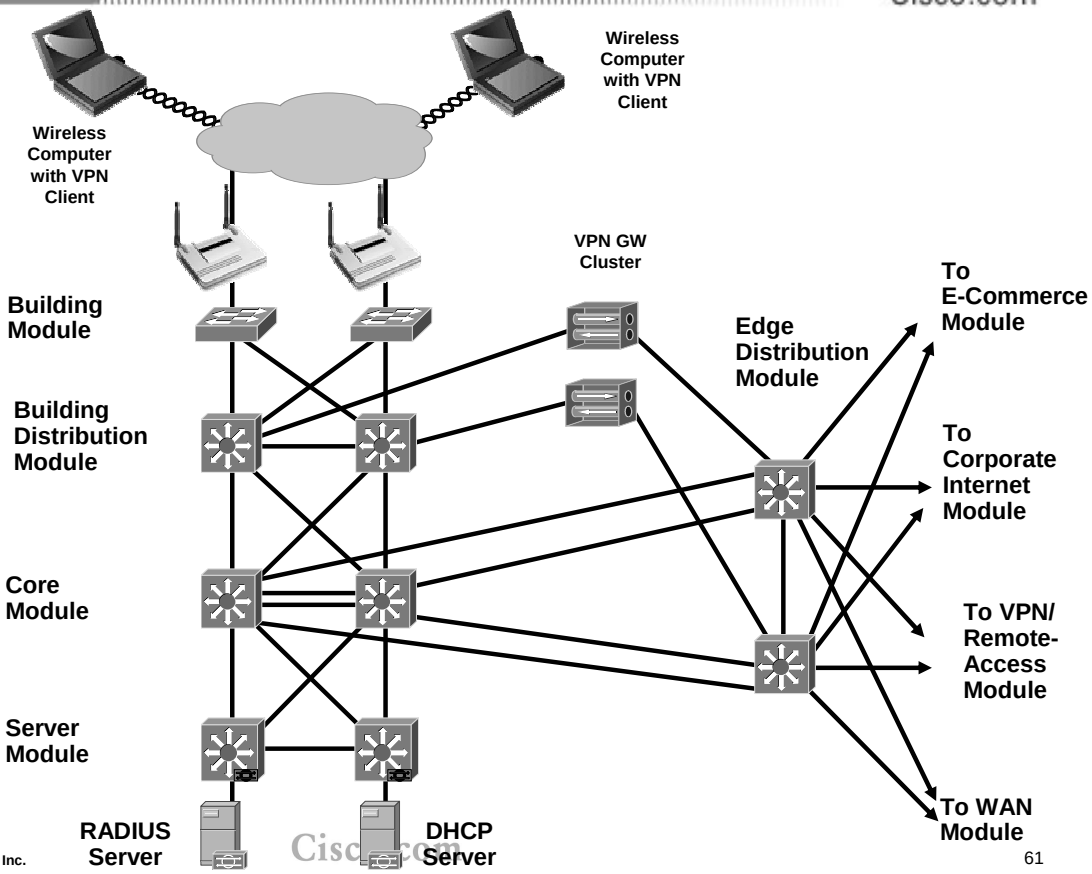
* inbound filter

** outbound filter

© 2003, Cisco Systems, Inc.

Large Enterprise VPN WLAN Design

Cisco.com



© 2003, Cisco Systems, Inc.
Cisco.com

Summary of VPN vs WLAN Security

Cisco.com

	EAP-Cisco Wireless	IPSec	Static WEP
Key Length (bits)	128	168, 128-256	128
Encryption Algorithm	RC4	3DES, AES	RC4
Packet Integrity	CRC32/MIC	MD5-HMAC/SHA-HMAC	CRC32/MIC
Device Authentication	None	Pre-shared secret or Certificates	None
User Authentication	Username/Password	Username/Password or OTP	None
User Differentiation	No	Yes	No
Transparent user experience	Yes	No	Yes
ACL requirements	None	Substantial	N/A
Additional Hardware	Authentication Server	Authentication Server and VPN Gateway	No
Per user keying	Yes	Yes	No
Protocol Support	Any	IP Unicast	Any
Client Support	PCs and high end PDAs. Wide range of OSs supported from Cisco	PCs and high end PDAs. Wide range of OSs supported from Cisco and 3rd Party Vendors.	All clients supported
Open Standard	No	Yes	Yes
Time based key rotation	Configurable	Configurable	No
Client hardware Encryption	Yes	Available, software is most common method	Yes
Additional Software	No	IPSec client	No
Per-flow QoS Policy Management	At access switch	After VPN gateway	At access switch

© 2003, Cisco Systems, Inc.
Cisco.com

Agenda

- WLAN Technology Introduction
- WLAN Security Issues
- WLAN Security Solutions
- WLAN and VPN
- Q&A

© 2003, Cisco Systems, Inc.

Questions?

© 2003, Cisco Systems, Inc.
© 2003, Cisco Systems, Inc. All rights reserved.

References

- 802.11 security flaws description info from Berkley University
  www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf
- Paper from S. Fluhrer (Cisco Systems), I. Mantin and A. Shamir
  www.crypto.com/papers/others/rc4_ksaproc.ps
- An Initial Security Analysis of the IEEE 802.1x Standard
  www.cs.umd.edu/~waa/1x.pdf

- IEEE 802.1x: grouper.ieee.org/groups/802/1/pages/802.1x.html
- EAP: www.ietf.org/rfc/rfc2284.txt
- TLS: www.ietf.org/rfc/rfc2246.txt
- EAP TLS: www.ietf.org/rfc/rfc2716.txt
- PEAP : draft-josefsson-pppext-eap-tls-eap-05.txt
- IEEE 802.11i: grouper.ieee.org/groups/802/11/Reports/tgi_update.htm
- Cisco.com/go/aironet

WLAN Security WP & presentation:
www.employees.org/~franjo/papers/WLAN_Security_pdfWP.zip
www.employees.org/~franjo/slides/ISSA_WLAN_pdf.zip

© 2003, Cisco Systems, Inc.

Thank you!

WLAN Security Solutions

fmajstor@cisco.com