Cisco.com

WLAN Security Solutions

NGI Zagreb

May 23rd 2003

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

Agenda

Cisco.com

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

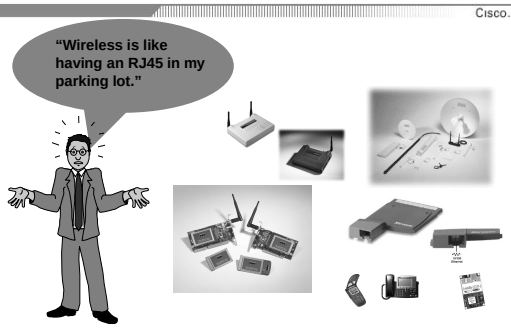
 Cisco.com

Cisco.com

WLAN Technology Introduction

Wireless LAN components

Cisco.com



 Cisco.com

WLAN "Alphabet Soup": IEEE 802.11 Standards Activities

Cisco.com

- **802.11a: 5GHz, 54Mbps**
- **802.11b: 2.4GHz, 11Mbps**
- **802.11d: Multiple regulatory domains**
- **802.11e: Quality of Service (QoS)**
- **802.11f: Inter-Access Point Protocol (IAPP)**
- **802.11g: 2.4GHz, 54Mbps**
- **802.11h: Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC)**
- **802.11i: Security**
- **802.11j: Japan 5GHz Channels (4.9-5.1 GHz)**
- **802.11k: Measurement**

 Cisco.com

Agenda

Cisco.com

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

 Cisco.com

WLAN Security Hierarchy

Cisco.com

Open Access
No Encryption, Basic Authentication

Public "Hotspots"

Basic Security
40-bit or 128-bit Static WEP Encryption

Home Use

Enhanced Security
802.1x, TKIP Encryption, Mutual Authentication, Scalable Key Mgmt., etc.

Enterprise

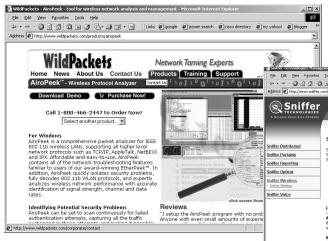
Remote Access

Virtual Private Network (VPN)

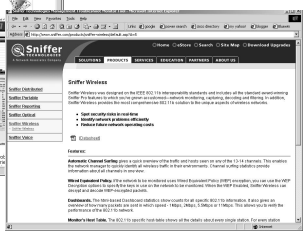
Business Traveler, Telecommuter

Sniffing 802.11 WLAN

Cisco.com



www.wildpackets.com



www.sniffer.com

Wireless LAN Security Issues

Cisco.com

THE WALL STREET JOURNAL.

Hackers Can Penetrate Wireless Network

Hacking into WEP

"War Driving"

Credit: KNTV San Jose

Wardriving …

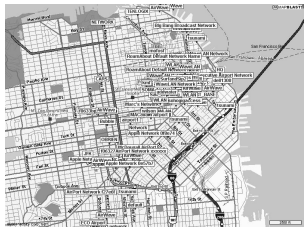
Cisco.com

… 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

Media Attention to Rogue APs Wardriving

Cisco.com

War Driving (wôr drī'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

Warchalking

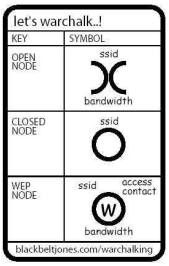
Cisco.com

Warchalking

Cisco.com

Media Attention to Rogue APs WarChalking

Cisco.com



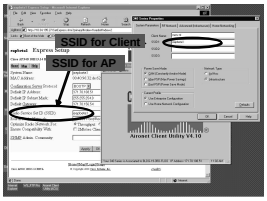
What is Warchalking?

- 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"

Service Set Identifier (SSID) in 802.11b

Cisco.com

- **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.
- **Is NOT a security feature!**

Wire Equivalent Privacy (WEP)

Cisco.com

- **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.**

Papers on WLAN Security

Cisco.com

University of California, Berkeley — **Feb. 2001** — Focuses on static WEP; discusses need for key management

University of Maryland — **April 2001** — Focuses on authentication; identifies flaws in one vendor's proprietary scheme

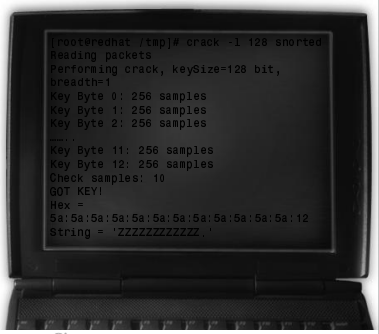
Scott Fluhrer, Itsik Mantin, and Adi Shamir — **July 2001** — Focuses on inherent weaknesses in RC4; describes pragmatic attacks against RC4/WEP

* "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

Airsnort

Cisco.com

- **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**



Limitations of 802.11 Security

Cisco.com

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

Agenda

Cisco.com

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

Addressing the Limitations: 802.11i

Cisco.com

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

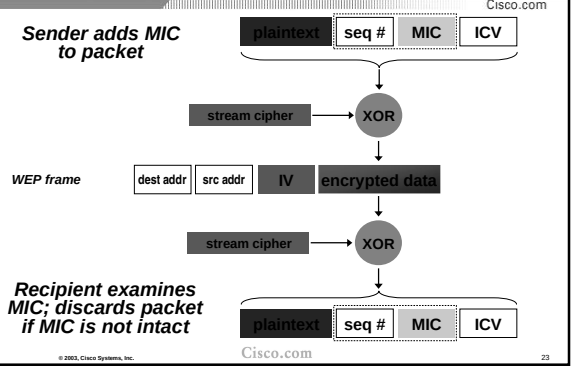
Security Enhancements for RC4 based WEP

Cisco.com

- 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

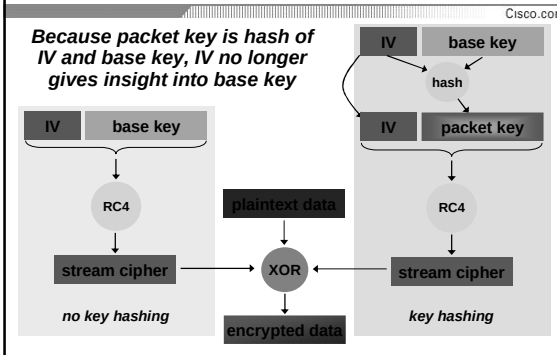
Message Integrity Check (MIC)

Cisco.com



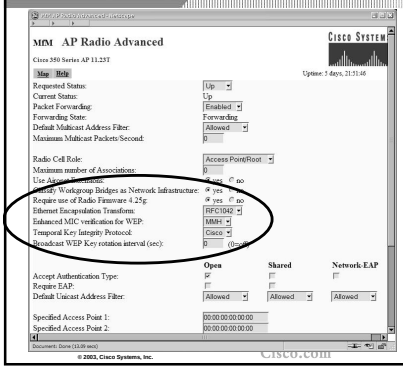
TKIP: Key Hashing (Per-Packet Keys)

Cisco.com



WEP enhancements - TKIP/MIC

Cisco.com



- **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

Linear IV Sequencing

Cisco.com

- **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**

Broadcast Key Rotation

Cisco.com

- **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)**

IEEE 802.1x Defined

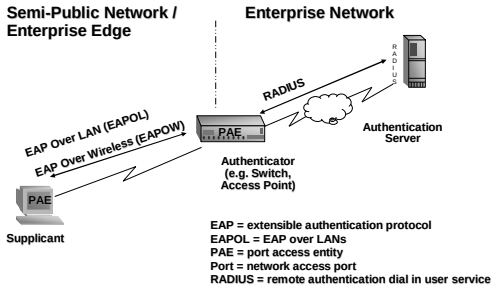
Port based network access control

Cisco.com

- **802.1x is an IEEE Standard for Port Based Network Access Control**
- **Falls under 802.1 NOT 802.11**
- **NETWORK standard, not a wireless standard**
- **Provides Network Authentication, NOT encryption**
- **Improved authentication: different methods**
- **Works on 802.3 LAN switch or 802.11b WLAN AP**
- **To be used for centralized user administration**

IEEE 802.1x Terminology

Cisco.com



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

EAP Defined - RFC 2284

Cisco.com

- **Extensible Authentication Protocol is a extension of CHAP/PAP within PPP**
  - **Support multiple "authentication" schemes:**
    - **plain password hash (MD5)**
    - **token cards**
    - **GSS-API (Kerberos)**
    - **TLS (based on X.509 certificates)**

802.1x Extensible Authentication Protocols

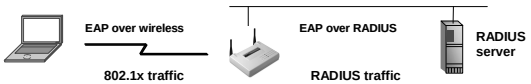
Cisco.com

- **EAP-MD5 (Message Digest 5)**
  - Supported in Win 2K/XP and, soon, other Windows versions
  - Does ***not*** provide ***mutual*** authentication ***nor WEP key derivation***
- **EAP-Cisco Wireless, or LEAP**
  - Supported client in WinXP/2K/NT/ME/98/95/CE, Linux, Mac, DOS.
  - Provides ***mutual*** authentication and ***WEP key derivation***
- **EAP-TLS (mutual EAP-TLS)**
  - Supported in Win 2K/XP and, soon, other Windows versions
  - Requires ***client certificates*** and ***server certificates***
- **PEAP**
  - 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

Before EAP Start

Cisco.com

802.11 association complete; data blocked by AP

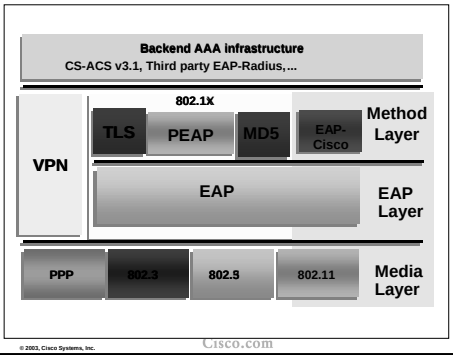


AP encapsulates 802.1x traffic into RADIUS traffic, and visa versa

AP blocks everything but 802.1x-to-RADIUS authentication traffic

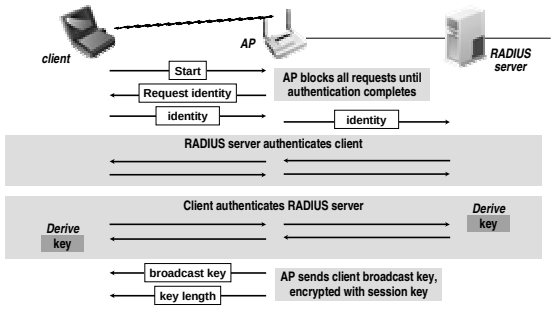
New WLAN Security Framework

Cisco.com



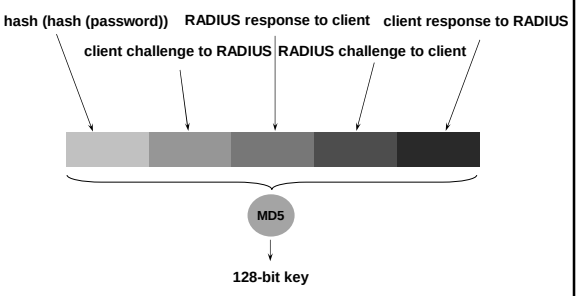
EAP Step: Key Derivation

Cisco.com



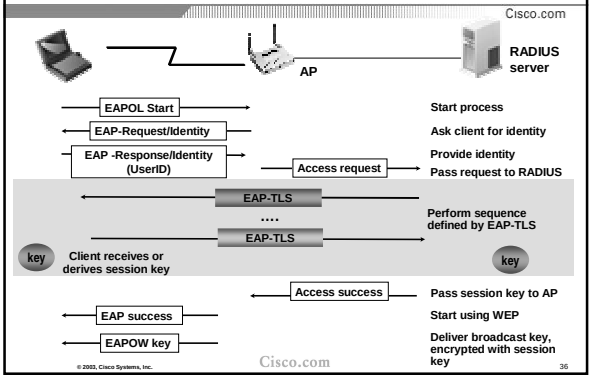
Cisco EAP Wireless (LEAP) Session Key Derivation

Cisco.com



EAP-TLS

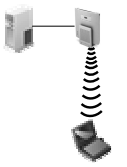
Cisco.com



What is PEAP?

Cisco.com

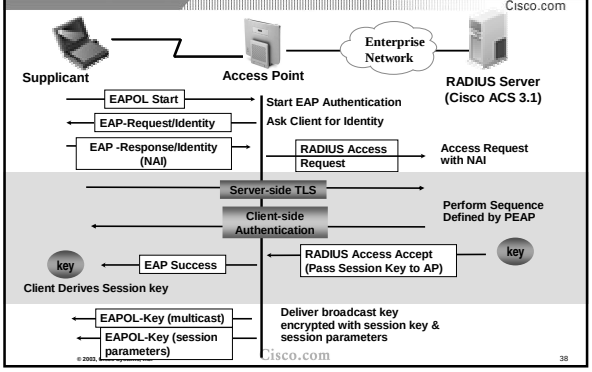
- ***PEAP*** **= Protected EAP (Extensible Authentication Protocol)**
- **802.1x - based authentication protocol based on EAP**
- **Leverages server-side EAP-TLS using digital certificates**
- **Supports a variety of different client authentication methods, including log-on passwords and *one-time passwords*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



Cisco Systems RSA Security Microsoft

PEAP - Two Phase Authentication

Cisco.com



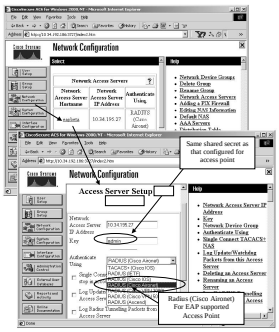
Client support for 802.1x

Cisco.com

	802.1x	LEAP (using Cisco Aironet drivers)	Cisco PEAP (using Cisco Aironet Drivers)	Microsoft PEAP (using OS drivers)
Cisco Products				
Cisco Aironet NICs	now	now	5.05.001	n/a
Cisco Aironet APs	now	now	11.23T	firmware upgrade to AP
CiscoSecure ACS	now	now	3.1	3.2
Operating Systems	(using OS drivers)			
Windows XP	now	now	now	now
Windows 2000	now	now	once MSFT releases EAP-TLS supplicant on other OSs	~ Q2-Q3 '03
Windows NT	now	now	once MSFT releases EAP-TLS supplicant on other OSs	~ Q2-Q3 '03
Windows 98	now	now	once MSFT releases EAP-TLS supplicant on other OSs	~ Q2-Q3 '03
Mac OS	MAC OS X	now	-	-
Solaris	www.open1x.org	n/a	-	-
Linux	www.open1x.org	now	-	-
User Databases (w/ CiscoACS AuthServer)				
CiscoSecure ACS	n/a	now	3.1	3.2
MSFT Backend Database	n/a	now	currently in beta	currently in beta
OTP	n/a	n/a	now	n/a
3rd-Party RADIUS Server	n/a	now	now	n/a
Kerberos	n/a	n/a	not committed	n/a
LDAP	n/a	n/a	now	n/a
NDS	n/a	n/a	now	n/a

What is the role of the RADIUS Server

Cisco.com



- **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**

How Often to Change Key

Cisco.com

- **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**

802.1x EAP Authentication Comparison

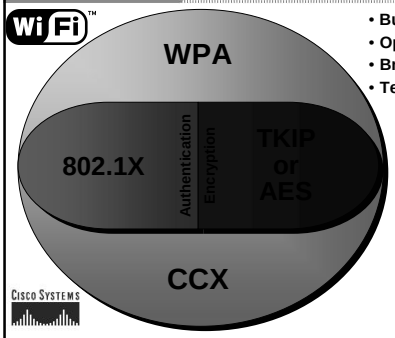
Cisco.com

	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

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/48-bits IV/EAP
  - AES proposal (new HW)
- www.wi-fi.com (Wi-Fi Alliance, ex. WECA - Wireless Ethernet Compatibility Alliance):
  - WPA (Wi-Fi Protected Access)
    - Text/hash function/MIC/48-bits IV/EAP

Enterprise-Class WLAN Security: The Cisco Wireless Security Suite



- Built on Standards
- Optimized for Enterprise
- Broad Adoption
- Tested for Interoperability

WPA
Wi-Fi Protected Access
TKIP
Temporal Key Integrity Protocol
AES
Advanced Encryption Standard
CCX
Cisco Compatible eXtensions

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 = WPA

Wi-Fi Protected Access (WPA)

- WPA is the biggest thing to happen to WLAN security since Cisco LEAP
- Cisco has supported the base technologies of WPA longer than any other vendor
- All new products after Aug.'03 MUST have WPA
  - Existing products are grandfathered
- 802.11i-standard TKIP + 802.1x authentication
- There is a non-802.1X version of WPA for home use which is unsuitable for enterprises

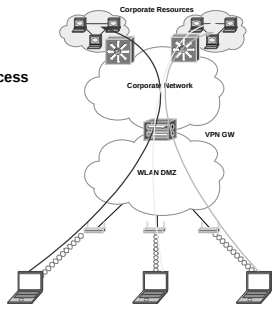
www.wi-fi.com/OpenSection/protected_access.asp

Agenda

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

VPN over WLAN Infrastructure

Definitions and Scope:
- VPN = IPsec based VPN
- WLAN = 802.11 based access



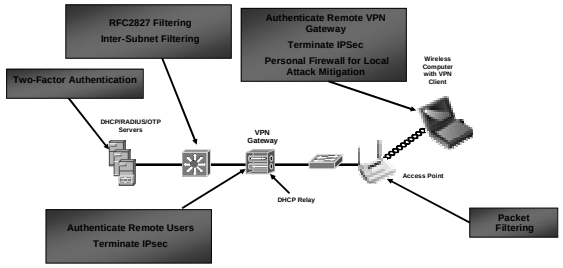
When to use VPN over WLAN?

Cisco.com

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

Generic VPN WLAN Design

Cisco.com

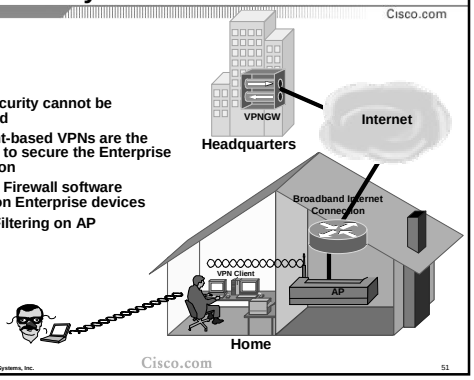


Cisco.com/go/SAFE

Enterprise Day Extender/Telecommuter

Cisco.com

- **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**



Access Point Filtering on RF side

Cisco.com

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

WLAN Security White Papers

Cisco.com

Wireless LAN Security & the Cisco Wireless Security Suite


A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite

www.cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a00800b469f.shtml

SAFE for Wireless
(updated Mar.'03)

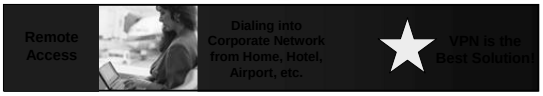
SAFE:
Wireless LAN Security in Depth

www.cisco.com/application/pdf/en/us/guest/netsol/ns128/c654/ccmigration_09186a008009c8b3.pdf

***or* Cisco.com/go/SAFE**

VPN Security for WLANs

Cisco.com



VPN/WLAN On Campus - Pros

- **Familiar**
  Is in use at most enterprises
  Makes user interface consistent for both WLAN & remote access
- **Trusted for authentication & privacy**
  Supports central security management
  Ensures 3DES encryption from client to concentrator
- **Compatible with wide range of client devices from multiple vendors**

VPN/WLAN On Campus - Cons

- **Cost:** Requires VPN concentrators behind APs
- **Performance:** Client software encryption lowers throughput
- **Roaming:** Roaming between VPN concentrators forces application restarts
- **QoS:** All traffic is IPSec traffic; no QoS, multicast, or multiprotocol support
- **Client Devices:** Not supported on phones, scanners, or other specialized devices
- **Convenience:** Additional steps required beyond Windows logon

Agenda

Cisco.com

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

Questions?

Cisco.com

References

Cisco.com

- 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

IETF:

- EAP: www.ietf.org/rfc/rfc2284.txt
- TLS: www.ietf.org/rfc/rfc2246.txt
- EAP TLS: www.ietf.org/rfc/rfc2716.txt
- EAP TTLS: draft-ietf-pppext-eap-ttls-02.txt
- PEAP : draft-josefsson-pppext-eap-tls-eap-06.txt

IEEE:

- 802.1x: grouper.ieee.org/groups/802/1/pages/802.1x.html
- 802.11i: grouper.ieee.org/groups/802/11/Reports/tgi_update.htm

Thank you!

Cisco.com

WLAN Security Solutions

fmajstor@cisco.com