CISCO SYSTEMS

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

Cisco.com

WLAN Security Threats & Solutions

WLN 2003
Third International
Workshop on Wireless Local Networks
Bonn, Oct 21st 2003

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

© 2003, Cisco Systems, Inc.

Agenda

Cisco.com

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

© 2003, Cisco Systems, Inc.
Cisco.com

WLAN Technology Introduction

Wireless LAN components

Cisco.com

© 2003, Cisco Systems, Inc.
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

© 2003, Cisco Systems, Inc.
Cisco.com

WLAN Security Issues

Sniffing 802.11 WLAN

Cisco.com

www.wildpackets.com

www.sniffer.com

© 2003, Cisco Systems, Inc.
Cisco.com

Wireless LAN Security Issues

Cisco.com

THE WALL STREET JOURNAL.

Hackers Can Penetrate Wireless Network

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

Hacking into WEP

"War Driving"

Credit: KNTV San Jose

© 2003, Cisco Systems, Inc.
Cisco.com

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 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

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

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
•23,700 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
University of Maryland — April 2001
Scott Fluhrer, Itsik Mantin, and Adi Shamir — July 2001

Focuses on authentication; identifies flaws in one vendor's proprietary scheme

Focuses on static WEP; discusses need for key management

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

WLAN Security Solutions

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

- Initialization Vector (IV) - a counter that increments with each frame
- IV is hashed with base WEP key
- Result is a new 'Packet' WEP key
- *The Packet WEP key is hash of IV and base key, so IV no longer gives insight into base key*

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

Before EAP Start

Cisco.com

802.11 association complete; data blocked by AP

New WLAN Security Framework

Cisco.com

EAP Defined - RFC 2284

- 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

- 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

EAP Step: Key Derivation

EAP-TLS

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)
- 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

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

EAP Types Comparison

	LEAP	EAP-TLS	EAP-PEAP
Server Authentication	Password	Certs/PKI	Certs/PKI
Client Authentication	Password	Certs/PKI	Password[1]
Single Sign on	Yes	Yes	No[2]
Vulnerable to Password Attack	No[3]	No	No
OTP/LDAP Support	No	N/A	Yes
Additional Infrastructure	No	Yes/CA	Yes/CA

[1] Not limited to password schemes
[2] MS native supplicant supports SSO w/EAP-MS-CHAPv2
[3] Requires strong passwords

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)
    - SW part only (hash/MIC/48-bits IV + EAP)

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 + TKIP and AES = WPA

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

© 2003, Cisco Systems, Inc.

Wi-Fi Protected Access (WPA)

- WPA is being incorporated into Wi-Fi testing
  - Mandatory Wi-Fi certification starting August/2003
- Wi-Fi Protected Access is a subset of 802.11i draft
- Addresses all currently known security problems with WEP
- Allows software upgrade on already deployed 802.11 equipment

Overview: http://www.wi-fi.com/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf
Q&A: http://www.wi-fi.com/OpenSection/pdf/Wi-Fi_Protected_Access_QA.pdf

© 2003, Cisco Systems, Inc.

Wi-Fi Protected Access (WPA)

- Components of WPA:
  - Authenticated key management using 802.1x:
    - EAP authentication and Pre-Shared Key (PSK) authentication
    - EAP-TLS and RADIUS are the nominated EAP test mechanism
  - TKIP: per-packet keying
  - Message Integrity Check (MIC)
  - Unicast and broadcast key management
  - IV expansion: 48 bit IVs
  - Migration mode - coexistence of WPA and non-WPA devices

© 2003, Cisco Systems, Inc.

802.11i/WPA
EAP Authentication Overview

© 2003, Cisco Systems, Inc.

WPA Key Hierarchy - Unicast Keys

- 802.1X auth derives 256 bit Pairwise Master Key (PMK)
- PMK is expanded and fragmented into 5 transient keys:
  - 128 bit EAPOL encryption key
  - 128 bit EAPOL-MIC key
  - 128 bit temporal encryption key
  - (2) 64 bit bidirectional
  - 64 bit MIC keys

© 2003, Cisco Systems, Inc.

WPA Key Hierarchy - Broadcast Keys

- AP derives Group Master Key (GMK)
- GMK is expanded and fragmented into 3 transient keys:
  - 128 bit temporal encryption key
  - (2) 64 bit bidirectional
  - 64 bit MIC key

© 2003, Cisco Systems, Inc.

Pre-shared Key (PSK) Authentication

Improvement on WEP Static Key; the PSK Is Only Used for Key Generation, Not for Encryption

802.11 Security Capabilities Discovery

Enhanced 802.1X Key Mgmt (Generate and Install PTK and GTK)

Data Protection

© 2003, Cisco Systems, Inc.

WLAN and VPN

VPN over WLAN Infrastructure

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

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

© 2003, Cisco Systems, Inc.

Generic VPN WLAN Design

© 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.

WLAN Security White Papers

Wireless LAN Security & the Cisco Wireless Security Suite

Cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf

SAFE for Wireless
(version 2)

Cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.pdf

or Cisco.com/go/SAFE

© 2003, Cisco Systems, Inc.

Questions?

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

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-03.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

© 2003, Cisco Systems, Inc.

Thank you!

WLAN Security Threats & Solutions

fmajstor@cisco.com

Cisco Systems

Empowering the Internet Generation℠