CISCO SYSTEMS

1

Cisco.com

WLAN Security

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

© 2003, Cisco Systems, Inc.

2

Agenda

Cisco.com

- WLAN Security Issues
- WLAN Security Solutions
  - -TKIP & MIC
  - - WPA (SSN)
  - - 802.1x/EAP - PEAP
- WLAN & VPN
- Q&A

© 2003, Cisco Systems, Inc.

Cisco.com

3

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.

"War Driving"

Hacking into WEP

Credit: KNTV San Jose

© 2003, Cisco Systems, Inc.

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

© 2003, Cisco Systems, Inc.

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

© 2003, Cisco Systems, Inc.

Warchalking

Cisco.com

© 2003, Cisco Systems, Inc.

Warchalking

Cisco.com

© 2003, Cisco Systems, Inc.

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"

© 2003, Cisco Systems, Inc.

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 static WEP; discusses need for key management

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

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

© 2003, Cisco Systems, Inc.

Wireless LAN Security Issues

Cisco.com

Issue
- Access control: Anyone in AP coverage area can get on WLAN
- Privacy: Wireless sniffer can view all WLAN data packets

802.11 Solution
- Use WEP to encrypt all data transmitted between client and AP
- Without WEP key, user cannot transmit or receive data

© 2003, Cisco Systems, Inc.

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

© 2003, Cisco Systems, Inc.

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

© 2003, Cisco Systems, Inc.

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 + **TKIP and AES** = **SSN = WPA**

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

© 2003, Cisco Systems, Inc.

WEP: AirSnort "Weak IV" Attack

Cisco.com

- 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

dest addr	src addr	IV	encrypted data

WEP frame

© 2003, Cisco Systems, Inc.

TKIP: Key Hashing (Per-Packet Keys)

Cisco.com

Because packet key is hash of IV and base key, IV no longer gives insight into base key

© 2003, Cisco Systems, Inc.

WEP: Bit-Flipping and Replay Attack

Cisco.com

- 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.

TKIP: Message Integrity Check (MIC)

Cisco.com

Sender adds MIC to packet

Recipient examines MIC; discards packet if MIC is not intact

© 2003, Cisco Systems, Inc.

WPA - Wi-Fi Protected Access

Cisco.com

- 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.

Cisco and WPA

Cisco.com

- Current capabilities of Cisco Aironet products
  - Have supported 802.1x since December 2000 - via LEAP
  - Have supported pre-standard TKIP implementation since December 2001
- Cisco plans
  - Continue to support all 802.1x types, including LEAP, as well as pre-standard TKIP
  - Ensure WPA compliance, primarily by adding support for standard TKIP
- Result: Cisco continues WLAN security leadership

* Not committed

© 2003, Cisco Systems, Inc.

802.1x for 802.11

Cisco.com

- Part of 802.11i draft standard
- Supported by Cisco since December 2000
- Extensible and interoperable – Supports:
  - Different authentication methods, or types
  - New encryption algorithms, including AES as a replacement for RC4
- Key benefits
  - Mutual authentication between client and authentication (RADIUS) server
  - Encryption keys derived after authentication
  - Centralized policy control, where session timeout triggers reauthentication and new key

© 2003, Cisco Systems, Inc.

New WLAN Security Framework

Cisco.com

© 2003, Cisco Systems, Inc.

802.1x Extensible Authentication Types

Cisco.com

- 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.

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)
- 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

Cisco.com

- 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 - Two Phase Authentication

Cisco.com

© 2003, Cisco Systems, Inc.

Cisco PEAP SW Information

Cisco.com

- Required software versions:
  - AP SW 11.23T or higher
  - PEAP Supplicant FCS - September, 2002
    - Cisco ACU 5.05.001 for MS Windows 2K/XP
  - Cisco Secure ACS Version 3.1: December, 2002
  - Or MS Win XP/SP1

© 2003, Cisco Systems, Inc.

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	not announced	not announced
Solaris	www.open1x.org	n/a	not announced	not announced
Linux	www.open1x.org	now	not announced	not announced
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

© 2003, Cisco Systems, Inc.
Cisco.com

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 WEP2 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.
Cisco.com

VPN over WLAN Infrastructure

Cisco.com

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

© 2003, Cisco Systems, Inc.
Cisco.com

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...

© 2003, Cisco Systems, Inc.

Large Enterprise VPN WLAN Design

Cisco.com

© 2003, Cisco Systems, Inc.

VPN AP 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

© 2003, Cisco Systems, Inc.

IPsec VPN vs Static WEP vs EAP-Cisco

Cisco.com

	LEAP-Cisco	IPSec	Static WEP
Key Length (bits)	128	168	128
Encryption Algorithm	RC4	3 DES	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.

Questions?

Cisco.com

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

References

Cisco.com

Cisco.com/go/aironet

Cisco.com/go/SAFE

IETF RFC's (www.ietf.org/rfc/):
- **RFC 2869 - RADIUS Extensions**
- **RFC 2284 - PPP Extensible Authentication protocol**
- **RFC 2716 - PPP EAP TLS Authentication Protocol**

IETF drafts (www.ietf.org/internet-drafts/):
- **draft-josefsson-pppext-eap-tls-eap-05.txt**
- **draft-kamath-pppext-eap-mschapv2-00**
- **draft-ietf-eap-otp-00.txt**

IEEE 802.11i:

grouper.ieee.org/groups/802/11/Reports/tgi_update.htm

© 2003, Cisco Systems, Inc.

Thank you!

Cisco.com

WLAN Security

fmajstor@cisco.com

CISCO SYSTEMS

EMPOWERING THE INTERNET GENERATION℠

www.cisco.com

38