

AUDITING WIRELESS NETWORKS

Mark Adams, CISSP

Deloitte & Touche

First, a review...

802.11

- **Wireless protocol standard**
 - 802.11 > 2Mbps over 2.4-GHz ISM band
 - 802.11b > 11Mbps over 2.4-GHz ISM band (Wi-Fi)
 - 802.11a > 54Mbps over 5-GHz UNII band
- **Optional security compliance level, Wired Equivalent Privacy (WEP)**

Throughput

■ 802.11a

- Standard: 54 Mbps
- Reality: 25 to 27 Mbps
- Runs on 12 channels
- Not backward compatible with 802.11b

■ 802.11b

- Standard: 11 Mbps
- Reality: 5 to 7 Mbps
- Runs on 3 channels; shared by cordless phones, microwave ovens, and many Bluetooth products

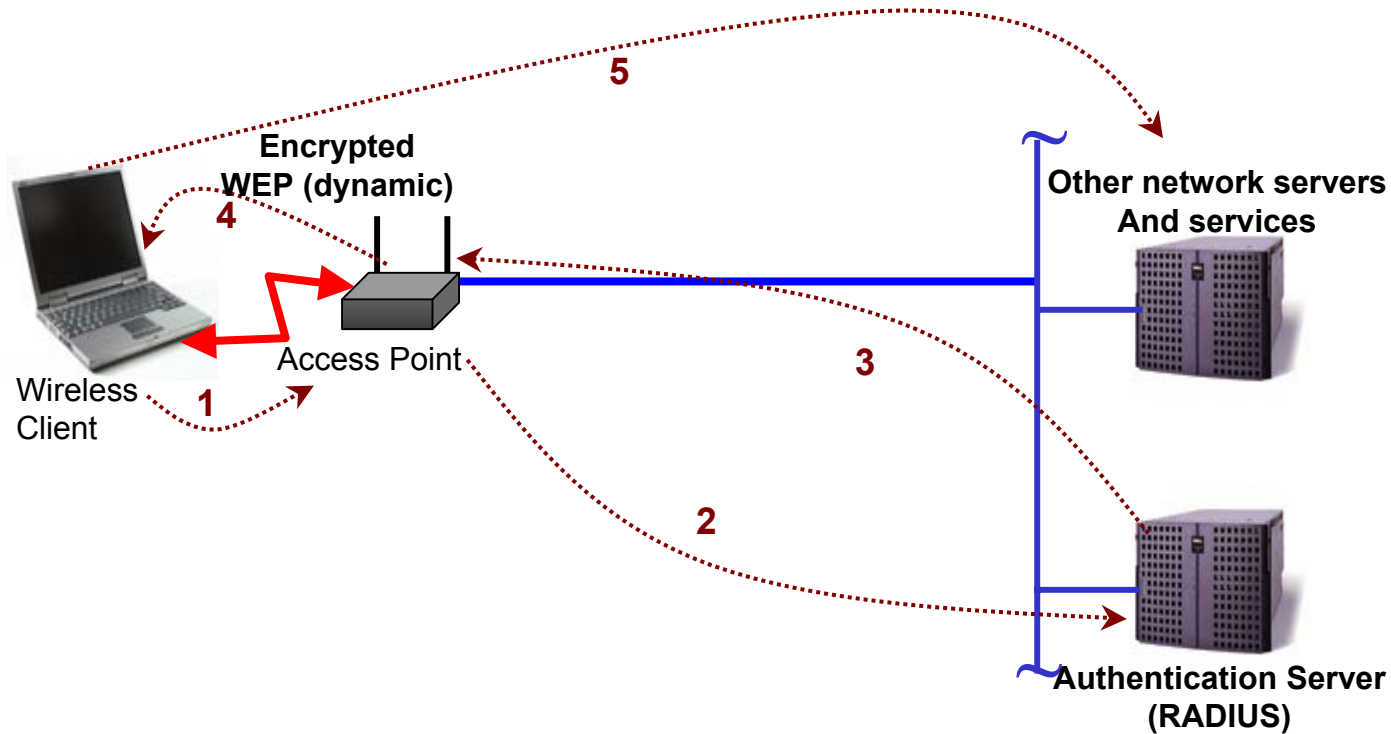
802.11g

- An extension to 802.11b, which will broaden 802.11b's data rates to 54 Mbps within the 2.4-GHz band.
- An 802.11b radio card will interface directly with an 802.11g access point (and vice versa) at 11 Mbps or lower depending on range.
- Final standard likely available by the end of 2002.

802.1x

- Port-based authentication and key distribution
- AP authenticates client by consulting an authentication server (RADIUS or Kerberos) using EAP-MD5 or EAP-TLS
- Supported by Windows XP natively
- Alternative open source client called “Xsupplicant” is also available from the Open1x project

Example of 802.1x Security



- 1) User requests authentication. AP prevents network access**
- 2) Encrypted credentials sent to authentication server (RADIUS)**
- 3) Authentication server validates user, grants access rights**
- 4) AP Port enabled and WEP keys are assigned to client (encrypted)**
- 5) Wireless client can now access general network services securely**

Wired Equivalent Privacy

- Uses the RC-4 40-bit encryption algorithm, although vendors can add proprietary encryption features to their software, taking the encryption level up to 128 bits.
- In February, 2001 three researchers (Fluhrer, Mantin, and Shamir) found four flaws in the WEP protocol.

WEP (cont.)

- Tools like WEPcrack and Aircrack-ng can obtain WEP keys from sniffed wireless traffic
 - Need high-traffic AP, lots of time, and luck
- Attacks on WEP have nothing to do with the key length!
 - The same 24-bit IV is used for both 64- and 128-bit WEP, which is the source of the weakness

Business Issues

- Backward compatibility
- Changing standards
- Bandwidth concerns
- Business case for a wireless LAN?
- Implementation cost
 - Site survey
 - Spectrum Analysis

Business Solutions

- Products that can be upgraded to support new standards
 - Cisco Aironet 1200 series, Agere (Orinoco) AP-2000, Enterasys RoamAbout R2
- Use product with more bandwidth/range
 - U.S. Robotics has boosted the speed of its 802.11b products to 22Mbps; 30% more linear range
- Have trained professionals perform site survey and implementation!!

Secure Protocols

- Extensible Authentication Protocol (EAP)
- Temporal Key Integrity Protocol (TKIP)
- Message Integrity Check (MIC)

Extensible Authentication Protocol (EAP)

- RFC 2284
- Extension to PPP
- Standard support mechanism for authentication schemes like token cards, Kerberos, Public Key, etc.
- Four commonly used EAP methods

Four EAP Methods

■ EAP-MD5

- MD5 hash of username and password
- Does nothing to protect WEP key
- Considered the least secure

■ EAP- Cisco Wireless (LEAP)

- Above and beyond what 802.1x specifies
- Relies on MS-CHAPv1, which has known vulnerabilities
- Only works on Cisco networks

Four EAP Methods

- EAP-TLS (Microsoft)
 - Uses X.509 digital certificates
 - Requires a PKI
 - Very difficult to implement unless AD and Microsoft Certificate Server are being used
- EAP-TTLS (Funk Software)
 - Alternative to EAP-TLS
 - Can use a variety of challenge-response mechanisms
 - Threatened by joint MS – Cisco standard called Protected EAP (PEAP)

TKIP

(a.k.a. WEP key hashing)

- 128-bit shared secret – “temporal key” (TK)
 - Mixes the transmitter's MAC address with TK to produce a Phase 1 key.
 - The Phase 1 key is mixed with an initialization vector (iv) to derive per-packet keys.
 - Each key is used with RC4 to encrypt one and only one data packet.
- Defeats the attacks based on “Weaknesses in the key scheduling algorithm of RC4” by Fluhrer, Mantin and Shamir,”
- TKIP is backward compatible with current APs and wireless NICs

Message Integrity Check (MIC)

- MIC prevents *bit-flip* attacks
- Implemented on both the access point and all associated client devices, MIC adds a few bytes to each packet to make the packets tamper-proof.

802.11i

- Takes base 802.1x and adds several features
- Wireless implementations are divided into two groups: Legacy and New
 - Both groups use 802.1x for credential verification, but the encryption method differs

802.11i

- Legacy networks must use 104-bit WEP, TKIP and MIC
- New networks will be same as legacy, except that they must replace WEP/TKIP with Advanced Encryption Standard – Operation Cipher Block (AES-OCB)
- 802.11i may not be standardized until mid to late 2003

Secure Architecture

- Create a wireless DMZ and have users authenticate through a VPN
 - Put Access Points *in front of* the firewall
 - Treat wireless LAN as an *untrusted* network
- Use RADIUS authentication
- Utilize IPSec/VPN, SSH, SSL, etc.
- Use firmware features like SSID Hiding

Q & A

Markadams@deloitte.com

Audit Items

- Is WEP activated?
- Is dynamic key exchange being used?
- Are NIC and AP firmware up to date?
- Who can reset access points?
- Are access points physically secure?>
- Are APs disabled during non-usage hours?

Cont

- Do APs have strong passwords?
- Are SSIDs being broadcasted?
- Are default SSIDs being used?
- Are cells being properly limited?
- Have access controllers been deployed?
- Are personal firewalls being used?

Cont

- Is VPN technology being used?
- Are static IP addresses being used?
- Is monitoring for rogue APs being performed?
- Is WLAN deployment being controlled?