Agenda

- Mr. Michael Disabato, Senior Analyst, Burton Group – "Wi-Fi Protected Access: Locking Down the Link"
- Send your questions via "Chat"
- Followed by a panel with
  - Michael Disabato, Panel Moderator
  - David Cohen – Chairman, Wi-Fi Alliance Marketing Security Task Group
  - Jesse Walker – Network Security Architect, Intel
  - Dorothy Stanley - System Architect, Agere Systems
  - Gene Chang – Vice President, Strategic Business Development, Funk Software

Wi-Fi Protected Access™: Locking Down the Link

Michael Disabato
Senior Analyst
Burton Group
mdisabato@burtongroup.com
www.burtongroup.com
June 11, 2003

Burton Group DRIVING NETWORK EVOLUTION™

Agenda

- Wired Equivalent Privacy (WEP)
- The Promise of Wi-Fi Protected Access™ (WPA)
- Implementation Issues
- Wi-Fi Protected Access 2 (WPA2)
- Recommendations & Conclusions
- Q & A

Wired Equivalent Privacy (WEP)

What is WEP?

- WEP was designed to secure the radio link
- Wired Equivalent Privacy (WEP) uses the RC4 encryption algorithm devised by Ron Rivest (the "R" in RSA) of RSA Security, Inc.
  - Symmetric-key stream cipher
  - Variable length key
- WEP uses 64-bit shared keys
- Initialization Vector (IV) is 24 bits of the key and sent as plain text

Wired Equivalent Privacy (WEP)

WEP has been shown to have some serious weaknesses

- A single key is used for all access points and client radios
- Keys can be recovered with easily available utilities
- Recovered keys expose the network to attacks or passive monitoring
- Lack of automated key management contributes to infinite static key lifespan in large networks
- When WEP was available it was not always turned on

Wired Equivalent Privacy (WEP)

And if that wasn't enough…

- WEP provides no forgery protection
- WEP provides no replay protection
- WEP misuses the RC4 encryption algorithm and allows weak key attacks
- WEP uses the Initialization Vector as part of the key, and when the IV wraps around, data can be easily recovered

Wired Equivalent Privacy (WEP)

Key Recovery Attacks

- Based on weaknesses in the key scheduling algorithm, utilities (AirSnort, WEPCrack) have been developed that are able to recover static WEP keys
- Common features of these utilities:
  - Collection of data for attack can be done passively
  - Once the secret key is recovered all traffic can be read until the key is changed
  - Less than 20,000 packets encrypted with the same key are required for this to work
  - Send and receive traffic is used in the attack
  - TCP ACK packets add to the traffic count and allow a known plain text attack

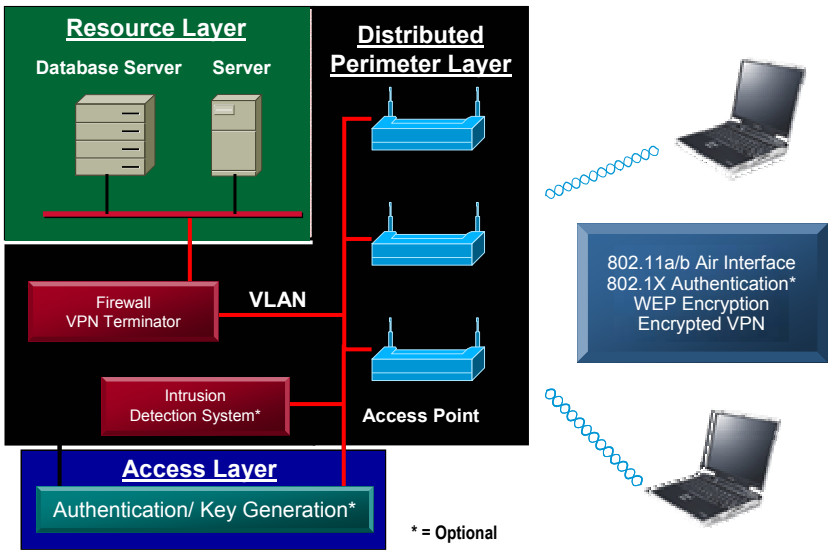
Wired Equivalent Privacy (WEP)

Dynamic Key Change – A Quick Fix

- WLAN vendors implemented a key management fix to make up for WEP's weaknesses
- A unified WEP fix was needed that was vendor neutral and Wi-Fi interoperable
- All the implementations required an authentication server (RADIUS or AAA)
- No WEP enhanced authentication method was available for small sites and home networks

Wired Equivalent Privacy (WEP)

WEP Secured WLAN



Agenda

Wired Equivalent Privacy (WEP)

The Promise of Wi-Fi Protected Access™ (WPA)

Implementation Issues

Wi-Fi Protected Access 2 (WPA2)

Recommendations & Conclusions

Q & A

The Promise of WPA

What is WPA?

- Wi-Fi Protected Access (WPA) is a response by the WLAN industry to offer an immediate, strong security solution
- WPA is intended to be:
  - A software/firmware upgrade to existing access points and NICs
  - Inexpensive in terms of time and cost to implement
  - Cross-vendor compatible
  - Suitable for enterprise, small sites, home networks
  - Runs in enterprise mode or pre-shared key (PSK) mode
- WPA is a subset of the 802.11i draft standard and is expected to maintain forward compatibility with the standard

The Promise of WPA

Enterprise Mode

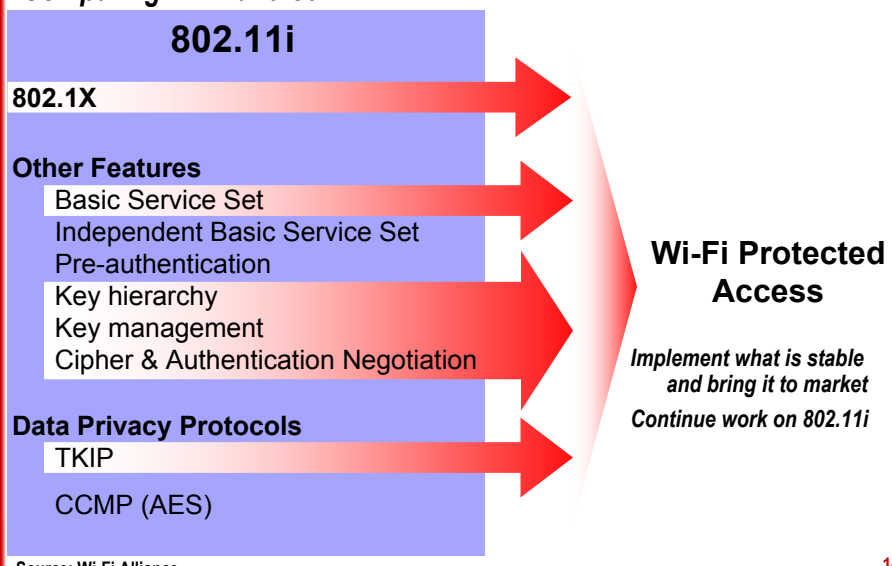
- Requires an authentication server
- Uses RADIUS protocols for authentication and key distribution
- Centralizes management of user credentials

Pre-Shared Key Mode

- Does not require authentication server
- "Shared Secret" is used for authentication to access point

The Promise of WPA

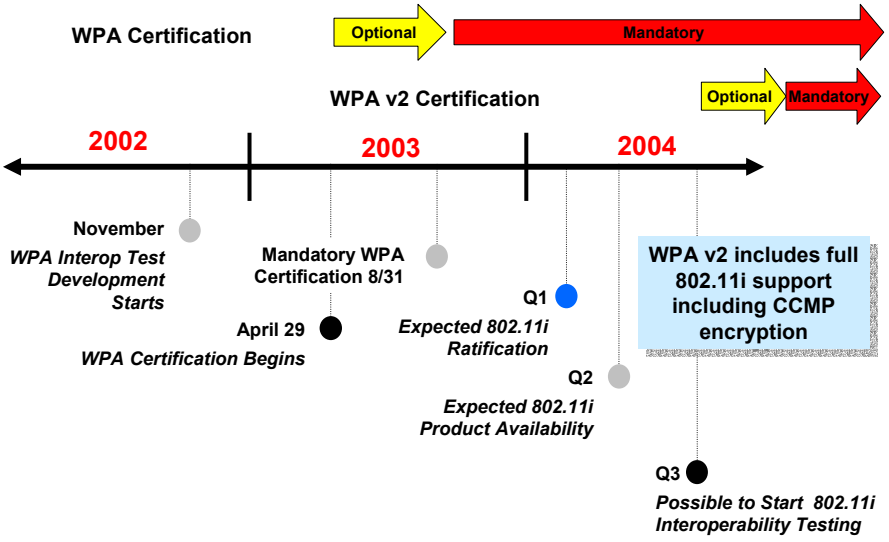
Comparing WPA and 802.11i



Source: Wi-Fi Alliance

The Promise of WPA

Wi-Fi Alliance Security Roadmap



The Promise of WPA

How WPA Addresses the WEP Vulnerabilities

- WPA wraps RC4 cipher engine in four new algorithms
  1. Extended 48-bit IV and IV Sequencing Rules
     - 2^{48} is a large number! More than 500 trillion
     - Sequencing rules specify how IVs are selected and verified
  2. A Message Integrity Code (MIC) called Michael
     - Designed for deployed hardware
     - Requires use of active countermeasures
  3. Key Derivation and Distribution
     - Initial random number exchanges defeat man-in-the-middle attacks
  4. Temporal Key Integrity Protocol generates per-packet keys

The Promise of WPA

WPA Summary

- Fixes all *known* WEP privacy vulnerabilities
- Designed and scrutinized by well-known cryptographers
- Pragmatic sacrifice of best possible security to minimize performance degradation on existing hardware
- Will work in home, small business, and enterprise environments

Agenda

Wired Equivalent Privacy (WEP)

The Promise of Wi-Fi Protected Access™ (WPA)

Implementation Issues

Wi-Fi Protected Access 2 (WPA2)

Recommendations & Conclusions

Q & A

Implementation Issues

Pre-Shared Key Mode Issues

- Needed if there is no authentication server in use
- If shared secret becomes known, network security may be compromised
- No standardized way of changing shared secret
- Significantly increases the effort required to allow passive monitoring and decrypting of traffic
- The more complex the shared secret, the less likely it will fall to dictionary attacks

Implementation Issues

Migration from WEP to WPA

- Enterprise:
  - Select EAP types and 802.1X supplicants to be supported on stations, APs, and authentication servers
  - Select and deploy RADIUS-based authentication servers
  - Upgrade APs with WPA software and firmware
  - Upgrade client stations with WPA software and firmware
- Small Office/Home Office:
  - Upgrade the APs with WPA software and firmware
  - Upgrade client stations with WPA software and firmware
  - Configure pre-shared key (PSK) or master password on the AP
  - Configure the PSK on client stations

Implementation Issues

Migration from WEP to WPA

- Existing authentication systems can still be used
- Moving to WPA is “all or nothing”
- WPA replaces WEP
- WPA 2 replaces RC4 with AES
- All access points and client radios will need new firmware and drivers
- Some older NICs and access points may not be upgradeable
- Once enterprise access points are upgraded, home units will need to be, if they were using WEP

Agenda

Wi-Fi Protected Access 2

- Uses the Advanced Encryption Standard (AES)
  - AES selected by National Institute of Standards and Technology (NIST) as replacement for DES
  - Symmetric-key block cipher using 128-bit keys
  - Generates CCM Protocol (CCMP)
    - CCMP = CTR + CBC + MAC
      - CTR = Counter Mode Encryption
      - CBC/MAC = Cipher Block Chaining/Message Authentication Code
- Hardware accelerated and will require replacement of most access points and some NICs
- Certified equipment due in late 2004

Wi-Fi Protected Access 2 (WPA2)

Encryption Method Comparison

	WEP	WPA	WPA 2
Cipher	RC4	RC4	AES
Key Size	40 bits	128 bits encryption 64 bits authentication	128 bits
Key Life	24-bit IV	48-bit IV	48-bit IV
Packet Key	Concatenated	Mixing Function	Not Needed
Data Integrity	CRC-32	Michael	CCM
Header Integrity	None	Michael	CCM
Replay Attack	None	IV Sequence	IV Sequence
Key Management	None	EAP-based	EAP-based

Agenda

Wired Equivalent Privacy (WEP)
The Promise of Wi-Fi Protected Access™ (WPA)
Implementation Issues
Wi-Fi Protected Access 2 (WPA2)
Recommendations & Conclusions
Q & A

Recommendations

General

- Conduct a risk assessment for all information that will travel over the WLAN and restrict sensitive information
- Policies and infrastructure for authenticating remote access users can be applied to WLAN users
- Perform regular audits of the WLAN using network management and RF detection tools
- Minimize signal leakage through directional antennas and placement of access points
- Make sure all equipment being purchased can be upgraded to support WPA and WPA 2/AES
- If using Pre-Shared Key Mode consider that the shared secret may become compromised

Recommendations

Should you upgrade to WPA2 with AES after WPA?

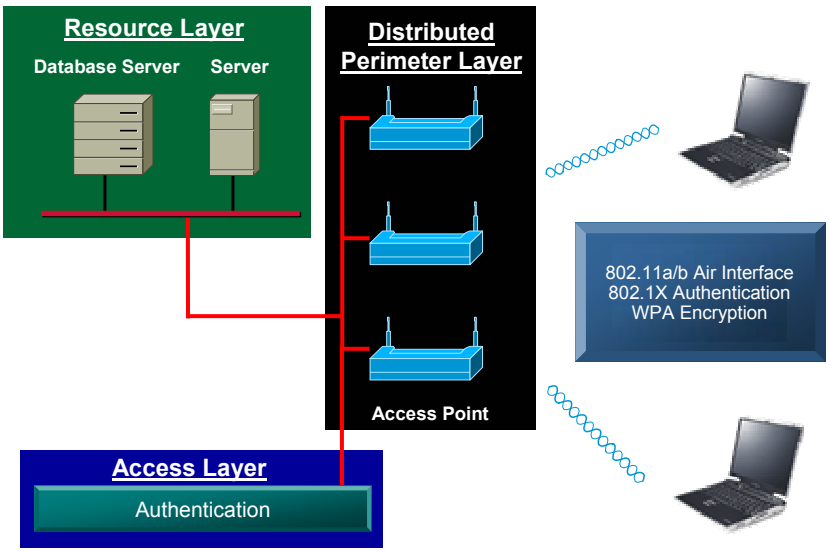
- An investment in new hardware (access points, NICs) may be needed
- Does your risk analysis indicate the extra protection is warranted
- WPA has not been broken (yet)
- Is there a compelling business reason to do so

However…

- WPA has not met the challenge of live traffic
- Network equipment will change over the next few years
- Eventually, RC4 will succumb to Moore's Law

Conclusions

WPA/ WPA 2 Secured WLAN



Conclusions

- WEP is insufficient to protect WLANs today from determined attackers
- WPA resolves all of WEP's known weaknesses
- WPA is a dramatic improvement in Wi-Fi security
- WPA provides an enterprise-class security solution for user authentication and encryption
- WPA is a subset of the 802.11i draft standard and is expected to maintain forward compatibility with the standard
- WPA 2 will provide an even stronger cryptographic cipher than WPA
- Unless there is a significant flaw found in WPA or RC4 is broken, there may be no reason to move to WPA 2/AES in the near future
- Numerous White Papers and additional information is available about WPA on the Wi-Fi WPA website

Q&A

- **Michael Disabato**, Panel Moderator
- **David Cohen** – Chairman, Wi-Fi Alliance Marketing Security Task Group
- **Jesse Walker** – Network Security Architect, Intel
- **Dorothy Stanley** - System Architect, Agere Systems
- **Gene Chang** – Vice President, Strategic Business Development, Funk Software