Wi-Fi is everywhere!

Wi-Fi Protected Access™

Networld + Interop

April 29, 2003

David Cohen

Chair, Security Committee
Wi-Fi Alliance

Agenda

- What is the Wi-Fi Alliance?
- What is Wi-Fi Protected Access (WPA)?
- History: The problem with WEP and other solutions
- WPA's technology parts
- WPA's design goals
- How WPA works
  - Enterprise
  - Home and SOHO

Agenda

- Deploying WPA
  - Enterprise
  - Home & Small Office
- WPA Certification
- Wi-Fi Security Timeline
- Summary
  - Key takeaways
  - Where to get more information
- Panel
- Q&A

The Wi-Fi Alliance

- The Wi-Fi Alliance (formerly WECA) is a nonprofit organization formed in 1999 to ***certify interoperability*** of IEEE 802.11 products and to ***promote*** Wi-Fi as the global, wireless LAN standard across all market segments.
- There are nearly 700 Wi-Fi CERTIFIED products to date

What is Wi-Fi Protected Access? (WPA)

- Powerful, standards-based, interoperable security technology for Wi-Fi networks
- Strong data protection – encryption
- Strong access control – user authentication
- Subset of the 802.11i draft standard and will maintain forward compatibility
- Software upgradeable to the nearly 700 Wi-Fi Certified products

History of Wi-Fi Security - WEP

- The 1997 IEEE 802.11 spec called for an optional security mechanism called Wired Equivalent Privacy, or WEP
- WEP had modest goals
  - Baseline security
  - Comply with US export guidelines at the time
- WEP had problems even before it was "broken"
  - One static key
  - Manual distribution of keys
  - No user authentication

History of Wi-Fi Security - WEP

- In 2001, several research papers pointed to WEP's cryptographic weaknesses
- Led to development of software tools to break WEP
- WEP still offered basic level of security, and remained useful for casual, home use (most never even used it)
- Not appropriate by itself for securing a busy corporate network

History of Wi-Fi Security - alternatives

- Some vendors responded with their own proprietary solutions
  - Some good, some not
  - But all were proprietary to that specific brand of gear
- Virtual Private Network (VPN)+ Wi-Fi
  - Effective, but:
  - Expensive (overkill), not what VPN’s were designed to do, or what their ROI’s promised
  - Still not interoperable
- 802.1X + WEP (Dynamic WEP)
- Market was calling for strong, interoperable Wi-Fi security

The Industry Responds

- In late 2001, the Wi-Fi Alliance, in conjunction with IEEE 802.11 TGi, began an effort to develop strong, standards-based, interoperable Wi-Fi security to market quickly
- The result of that effort is Wi-Fi Protected Access
- WPA announced October 31, 2002
- First round of WPA products announced today

WPA’s technology parts

- User authentication
  - 802.1X + Extensible Authentication Protocol (EAP)
- Encryption
  - Temporal Key Integrity Protocol (TKIP)
  - 802.1X for dynamic key distribution
  - Message Integrity Check (MIC) a.k.a. “Michael”
- WPA = 802.1X + EAP + TKIP + MIC
- Pre-Shared Key for SOHO authentication

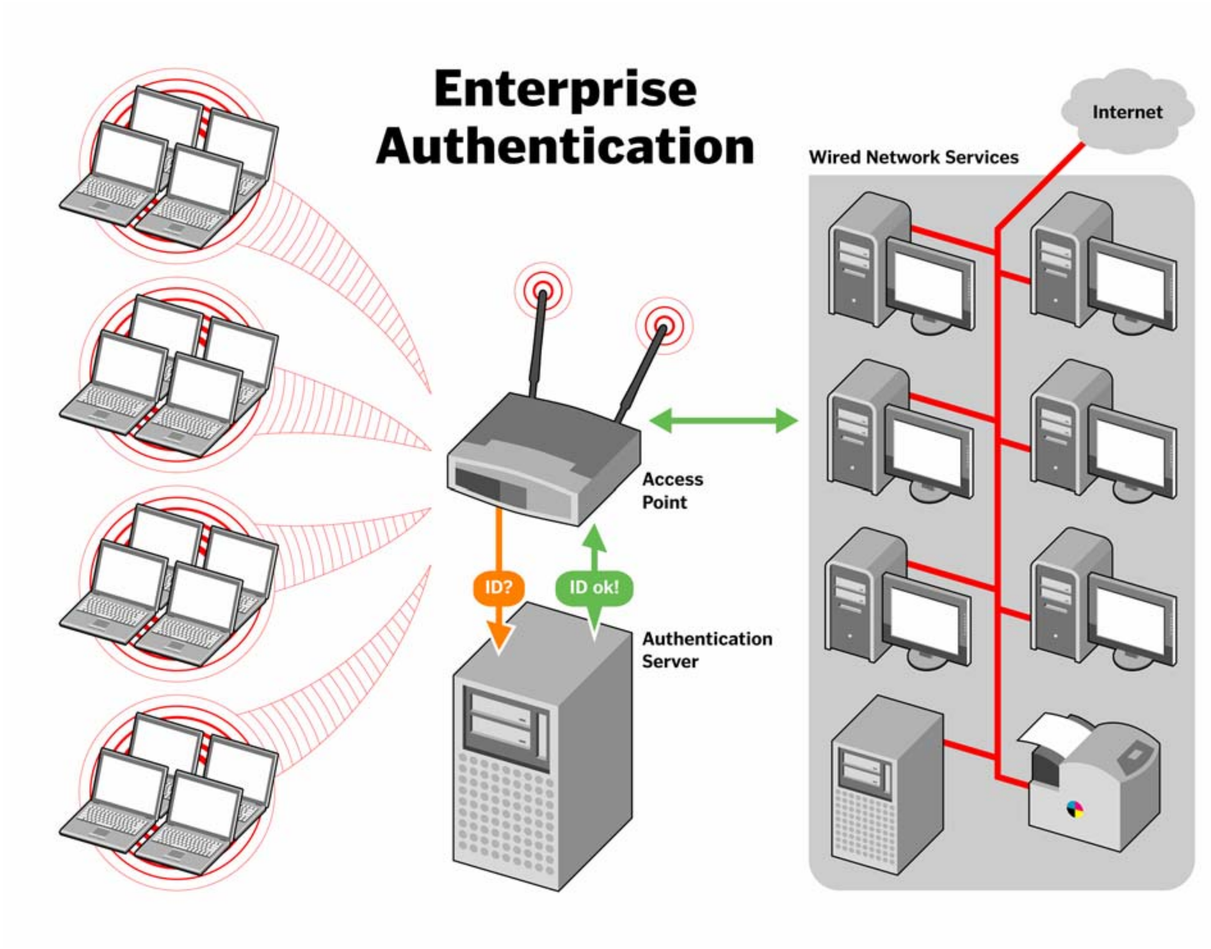
WPA Design Goals

Resolve WEP's cryptographic weaknesses	✓	Cryptographers have verified this
Add user authentication	✓	EAP/802.1X & PSK
Be applicable to the nearly 700 Wi-Fi CERTIFIED products on the market	✓	Designed as software upgrade
Be available in 2003	✓	Here today
Be certified interoperable	✓	Certification announced today

WPA – Exceeding goals

- Automatic key distribution ☑
- Per user, per session, unique master keys ☑
- Unique per packet encryption keys ☑

How WPA Works - Enterprise



How WPA Works - Enterprise

- Step1. Client associates with Access Point (AP)
- Step 2. AP blocks LAN access until client is authenticated
- Step 3. Client provides credentials to authentication server.
  - If not authenticated, client stays blocked from LAN
  - If authenticated, process continues
- Step 4. Authentication server automatically distributes encryption keys to AP and client
- Step 5. Client joins LAN, encrypting data back and forth with AP

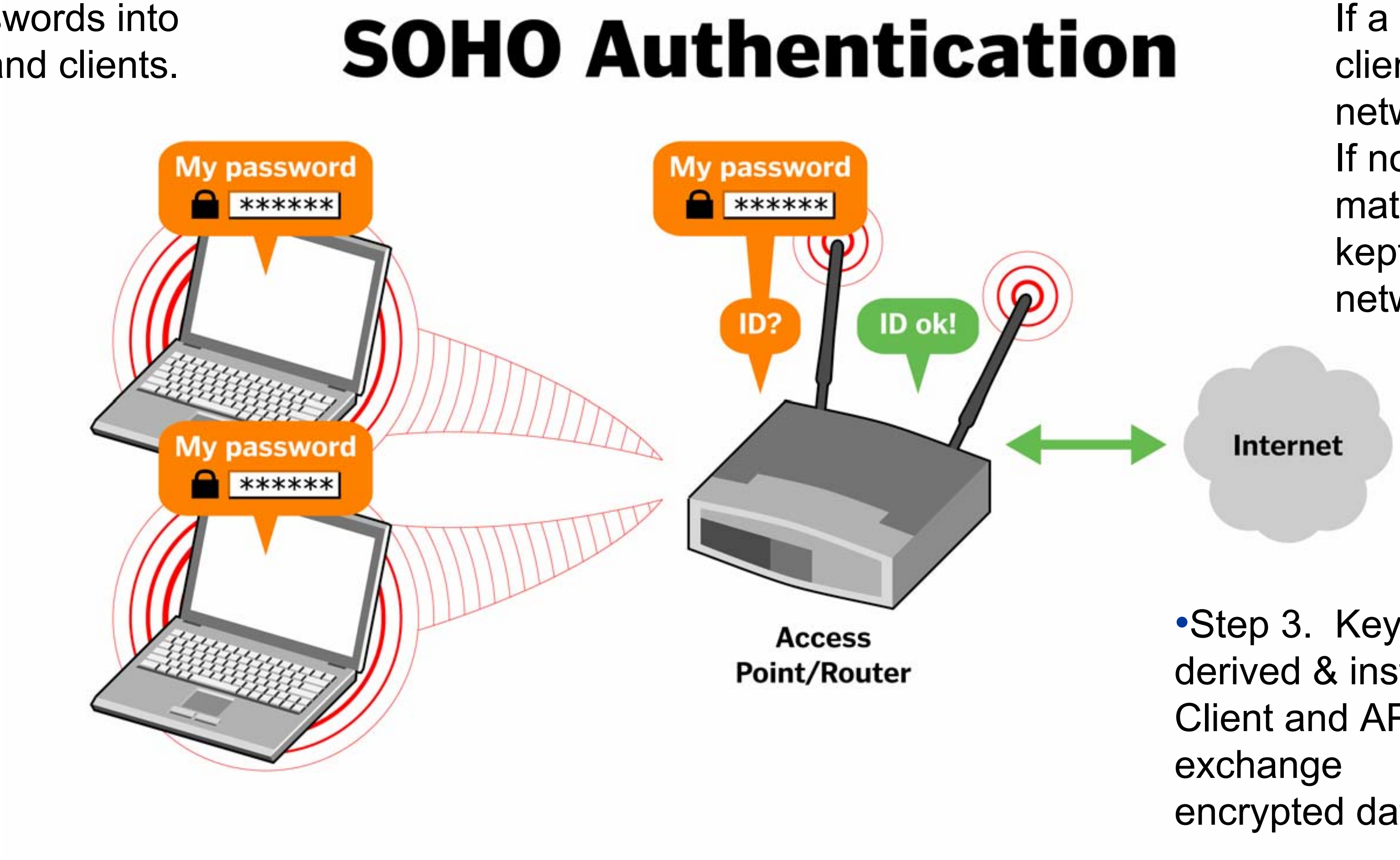
How WPA Works - SOHO

Step 1. Enter matching passwords into AP and clients.

Step 2. AP checks client’s password.

If a match, client joins network.

If not a match, client kept off network.



- Step 3. Keys derived & installed. Client and AP exchange encrypted data.

How WPA Works – SOHO

- Authentication is simplified to a matching password
- Encryption is *identical* to enterprise encryption

Deploying WPA – Enterprise - Hardware

- Authentication server, typically RADIUS
  - Common in LE for remote user access
- WPA enabled Access Points
  - WPA at ship, or
  - Upgraded to WPA
- WPA enabled clients
  - WPA at ship, or
  - Upgraded to WPA

Deploying WPA – Enterprise - Software

- Authentication server (RADIUS)
  - Strong EAP type such as TLS, TTLS, PEAP
- WPA enabled Access Points
  - 802.1X
  - TKIP
- WPA enabled clients
  - 802.1X
  - TKIP
  - Supplicant to support EAP/ 802.1X

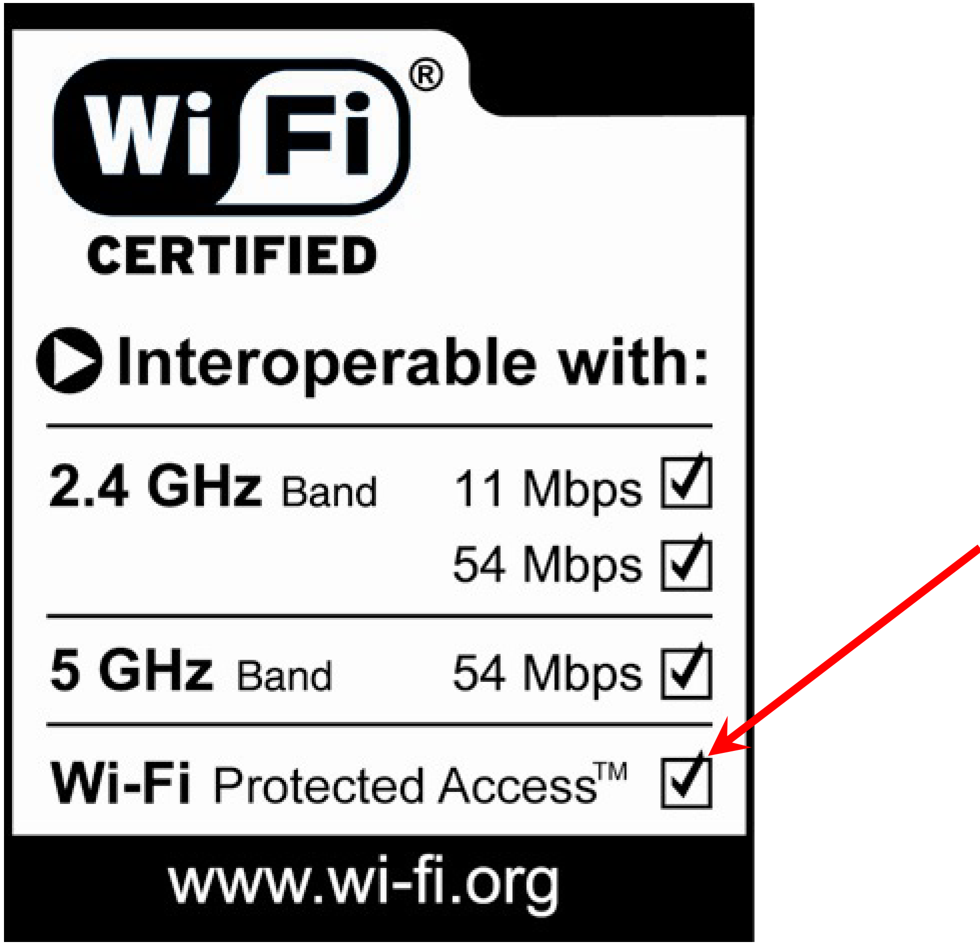
Deploying WPA – SOHO - Hardware

- WPA enabled Access Points or home gateway
  - WPA at ship, or
  - Upgraded to WPA
- WPA enabled clients
  - WPA at ship, or
  - Upgraded to WPA

Deploying WPA – SOHO - Software

- WPA enabled Access Points
  - 802.1X
  - TKIP
- WPA enabled clients
  - 802.1X
  - TKIP
  - Supplicant, or partial supplicant to run 802.1X and PSK
- Runs in Pre-Shared Key (PSK) mode

WPA Certification


Wi Fi ®
CERTIFIED

Interoperable with:

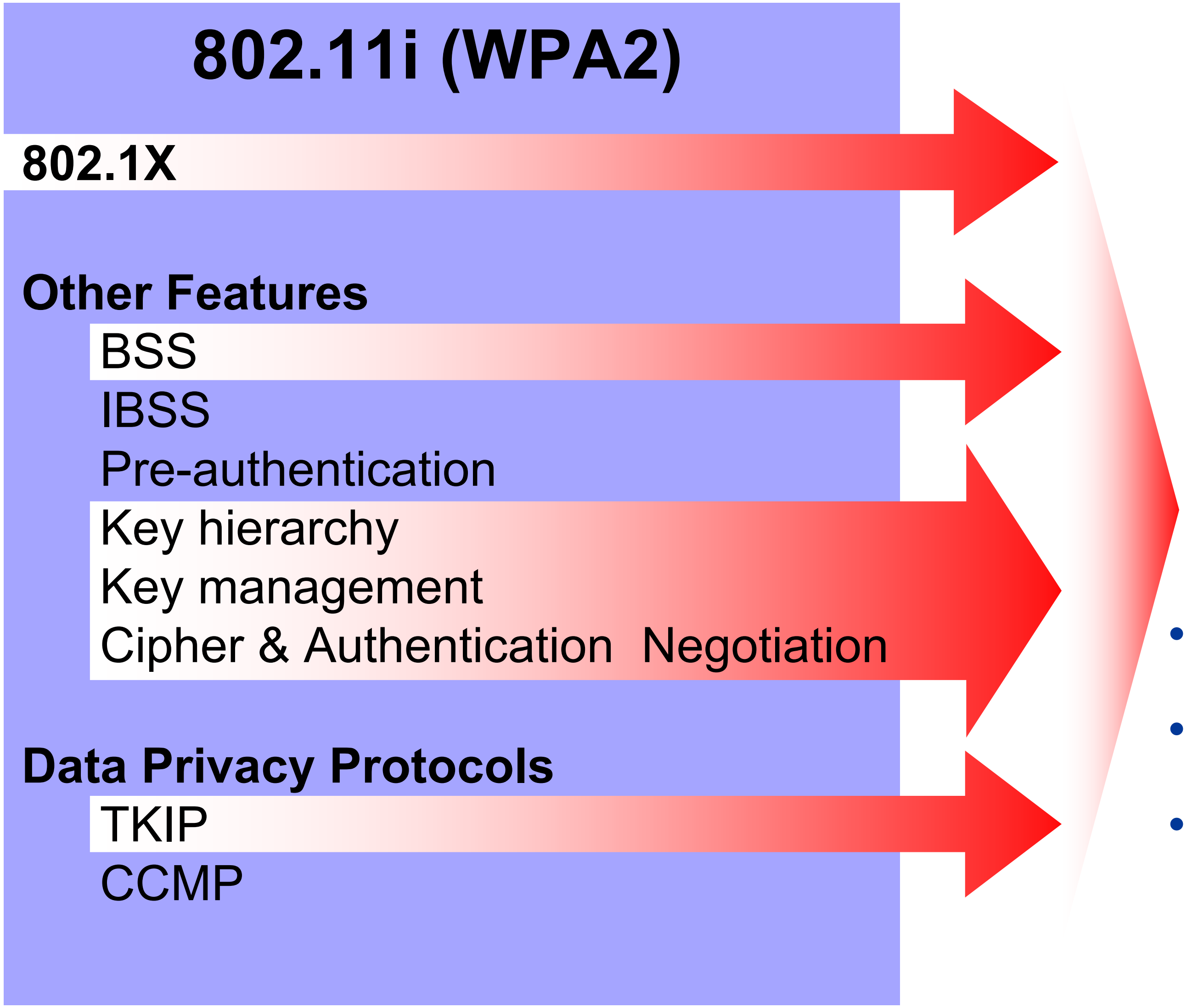
2.4 GHz Band	11 Mbps	☑
	54 Mbps	☑
5 GHz Band	54 Mbps	☑
Wi-Fi Protected Access™		☑

www.wi-fi.org

Wi-Fi Alliance Security Timeline

- 1999 – WEP
- 2003 – Wi-Fi Protected Access (WPA)
- 2004 – WPA2 (802.11i)

WPA is a snapshot of 802.11i (WPA2)



802.11i (WPA2)

802.1X

Other Features

- BSS
- IBSS
- Pre-authentication
- Key hierarchy
- Key management
- Cipher & Authentication Negotiation

Data Privacy Protocols

- TKIP
- CCMP

Wi-Fi Protected Access

- Implement key features today
- Continue work on 802.11i
- Forward and backward compatible

Summary Comparison

	WEP	WPA
Encryption	Flawed, cracked by scientists and hackers	Fixes all WEP's flaws
	40-bit keys	128-bit keys
	Static key – same key used by everyone on the network	Dynamic session keys. Per user, per session, per packet keys
	Manual distribution of keys– hand typed into each device	Automatic distribution of keys
Authentication	Flawed, used WEP key itself for authentication	Strong user authentication, utilizing 802.1X and EAP

Summary

- WPA provides a dramatic improvement in Wi-Fi security
- Enterprise class but suitable for SOHO
- Reasonable deployment costs
- The strong, standards-based Wi-Fi security solution the market has been seeking
- Best of all . . .
- It's here now!
- For more information, go to:

http://www.wi-fi.org/OpenSection/protected_access.asp

Panel discussion and Q & A