



Issues in Wireless Security (WEP, WPA & 802.11i)

**Presented to the 18th Annual Computer
Security Applications Conference
11 December 2002**

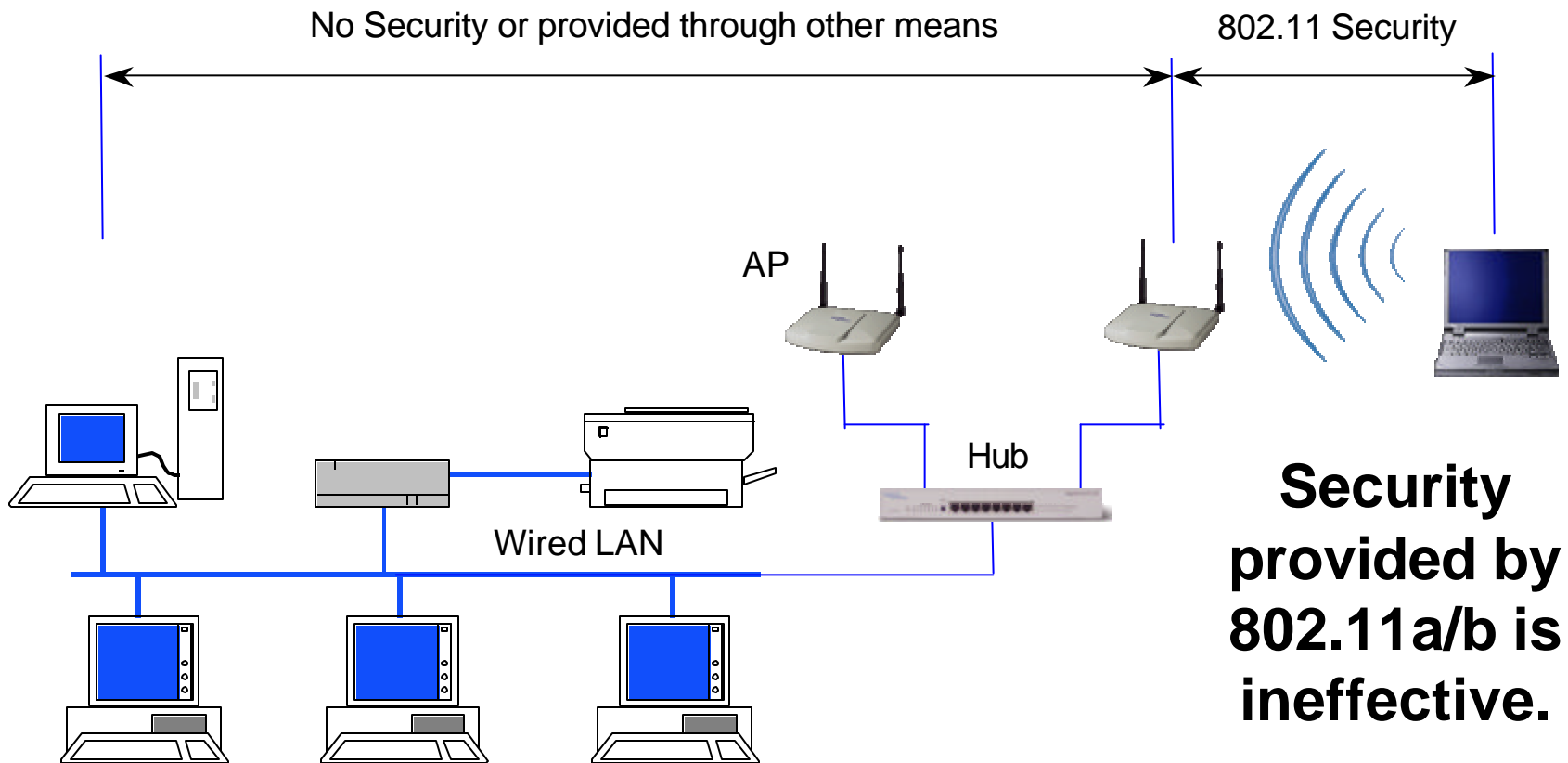
Brian R. Miller, Booz Allen Hamilton

Overview

- ▶ Examine current wireless security provided by Wired Equivalent Privacy (WEP)
- ▶ Examine the wireless industry's response to the issues of WEP and the Wi-Fi Alliance's interim solution Wi-Fi Protected Access (WPA)
- ▶ Examine the security provided by the 802.11 Tgi standard
- ▶ Summary

WEP

802.11 WEP Security is Inadequate



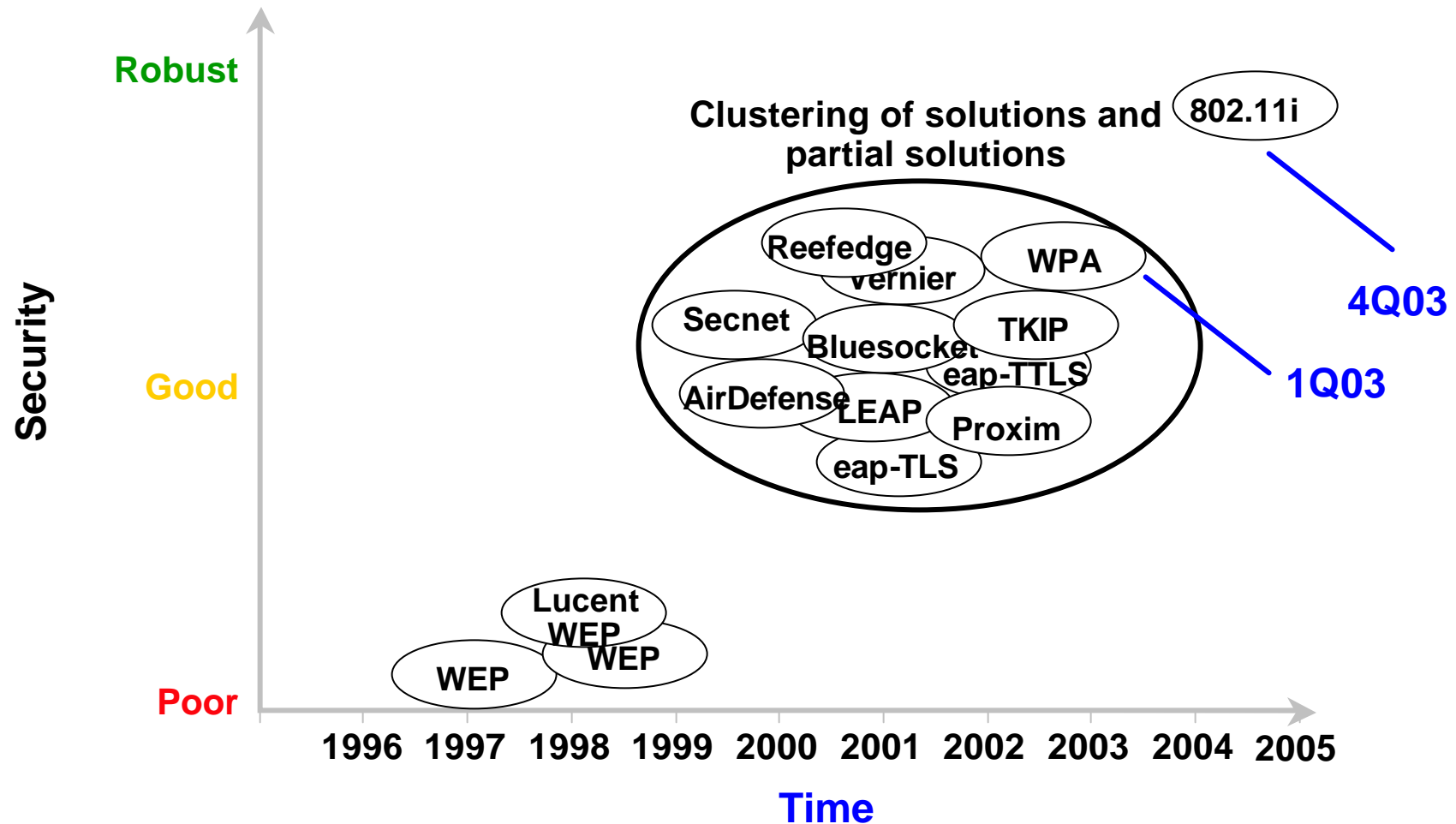
Key Problems With 802.11 Wireless LAN Security (WEP)

- ▶ Repeat in key stream which allows easy decryption of data for a moderately sophisticated adversary. (Short IV)
- ▶ Weak implementation of the RC4 algorithm leads to an efficient attack that allows key recovery
- ▶ Subject to brute force attacks (Short Keys)
- ▶ Easily compromised keys (Shared keys/No Key management)
- ▶ Message modification is possible
- ▶ No user authentication occurs
- ▶ Subject to Man in the Middle attacks
- ▶ Organizations are becoming hesitant to deploy 802.11 wireless technology due to weak security

Short Term Solutions

- ▶ Don't use / Delay implementation of WLANS
 - Federal Government and some commercial users are taking this approach
 - Wait for Wi-Fi Protected Access (WPA)
- ▶ Use proprietary WEP security
 - WEP security with patches- Harder to break but still vulnerable
 - May force a vendor specific solution with poor interoperability
- ▶ Robust Layer 2 Type-1
 - Harris SecNet 11 – NSA Approved for use in U.S government environments with data classified up to secret
 - Provides robust security but prohibitively expensive (Approx \$2500.00 per NIC)
- ▶ Implement VPN for access to the wired network
- ▶ Security switch/gateway with “add-ons” to address other security services

Overview of the Evolution of WiFi Security Solutions/Std (Illustrative only)



Wi-Fi Alliance

Wi-Fi Alliance

- ▶ The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification.
- ▶ In 2001 there were 100 Wi-Fi Certified Products and today there are 500+ Wi-Fi certified products
- ▶ Industry is demanding a more secure wireless environment and can not wait for the 802.11i standard to be ratified next year.
- ▶ Wi-Fi Protected Access (WPA) is Wi-Fi Alliance's response to the need for an immediate solution to the WEP problem and a recognition that the 802.11i standard is still too far off.
- ▶ Security Goal: Implement what is stable in 802.11i and bring it to market in WPA.



WPA

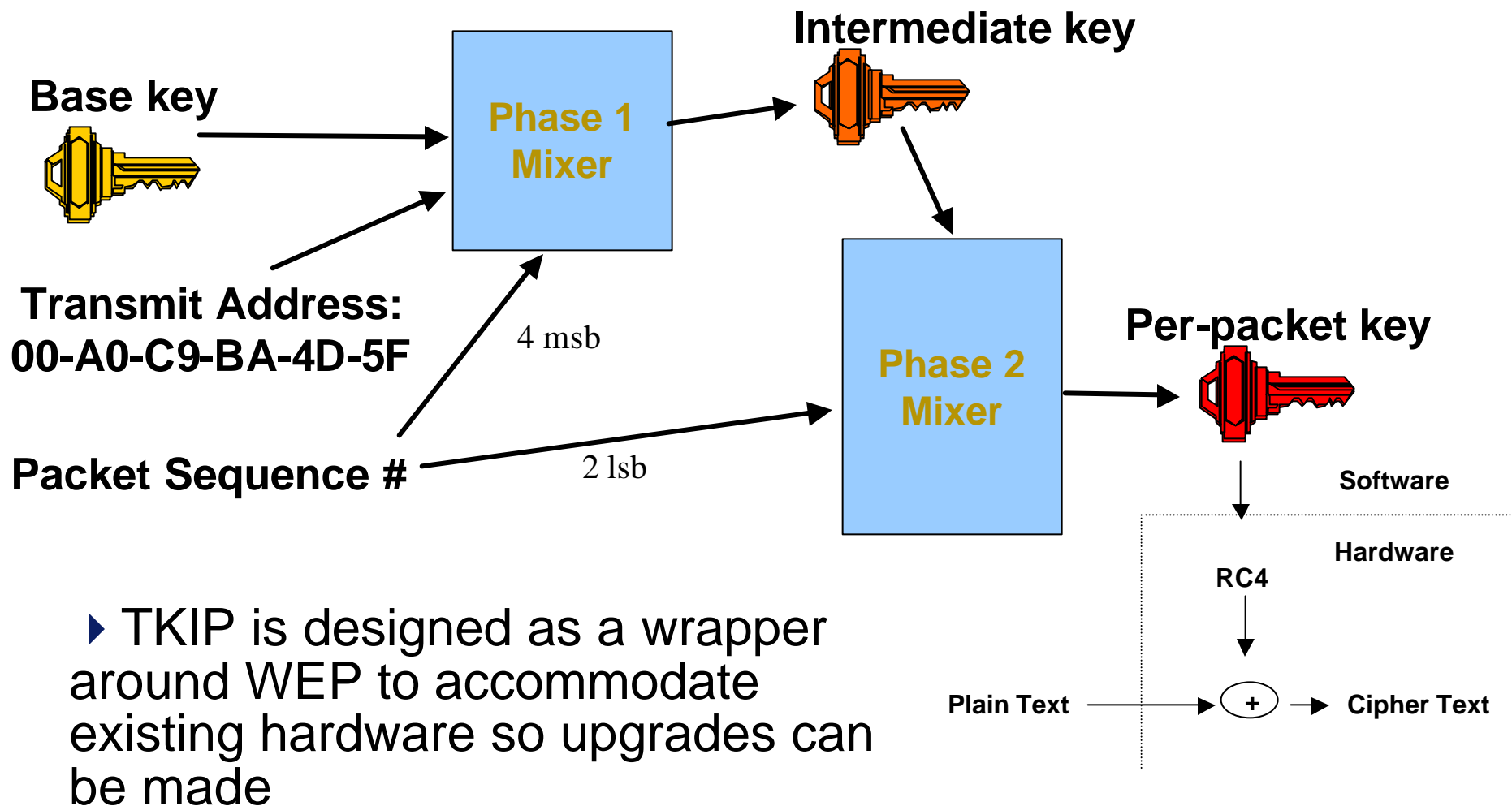
Wi-Fi Protected Access (WPA)

- ▶ WPA seeks to provide a standards based security solution based 802.11i security features ahead of IEEE ratification
- ▶ Interim security solution that fixes all known WEP vulnerabilities
- ▶ Key features of WPA include:
 - Data Encryption -- TKIP (Temporal Key Integrity Protocol) using RC4 WEP
 - User Authentication -- 802.1X EAP based authentication, PPK
 - Message Integrity -- Michael Message Integrity Check
- ▶ WPA products certified by Wi-Fi alliance are expected to be available Q1 2003

WPA: TKIP Design Requirements

- ▶ Designed so that only software or firmware upgrades are required to use WPA functionality on existing/legacy hardware
- ▶ Must be designed to be used on 33 or 25 MHz ARM7 or i486 already running at 90% CPU
- ▶ Result: TKIP designed to use existing WEP off-load hardware as a part of the encryption process

TKIP Design



WPA Benefits

- ▶ Improved Cryptography
- ▶ Strong Network access control
- ▶ Will Support 802.1x, EAP, EAP-TLS, Radius, and Pre-Placed Keys
- ▶ Key Management
- ▶ Replay Protection
- ▶ Provides for data and header integrity
- ▶ Is expected to provides forward compatibility with full 802.11i standard when it is ratified.

Issues: WPA

- ▶ While TKIP & Michael significantly improve WEP security, design limitations result in cryptographic weaknesses
- ▶ While components have been designed and scrutinized by well-known cryptographers, a pragmatic sacrifice of bullet-proof security to minimize performance degradation on existing hardware.
- ▶ Note: TKIP designers do not expect a potential successful attack on WPA is not expected to be simple or cheap
- ▶ How strong is WPA really?

Recommendation: WPA

- ▶ Migrate existing wireless infrastructure to WPA through software and firmware upgrades when available. (Q1/Q2 2003)
- ▶ Evaluate the sensitivity of data to be transmitted wirelessly and implement wireless networks using WPA accordingly.
- ▶ Look to future products that will support the full 802.11i standard.

802.11i, WPA v2

IEEE 802.11i

- ▶ Long-term security solution for 802.11 wireless LANs
- ▶ Key features include:
 - (WPA) Encryption: TKIP using RC4 – Legacy Device Support
 - (WPA) Message Integrity -- Michael Message Integrity Check
 - Encryption/Message Integrity: AES-CCMP Using Advanced Encryption Standard (AES) – New hardware
 - User Authentication -- 802.1X EAP based authentication, PPK
 - PPK
 - Roaming/Pre Authentication
 - Ad Hoc Networking
- ▶ 802.11i products certified by Wi-Fi alliance are expected to be available Q1 2004

802.11i Benefits

- ▶ Strong Cryptography
- ▶ Support for Legacy Equipment
- ▶ Strong Network Access Control
- ▶ Will Support 802.1x, EAP, EAP-TLS, Radius, and Pre-Placed Keys
- ▶ Key Management
- ▶ Replay Protection
- ▶ Provides for data and Header Integrity
- ▶ Roaming Support

Issues: 802.11i

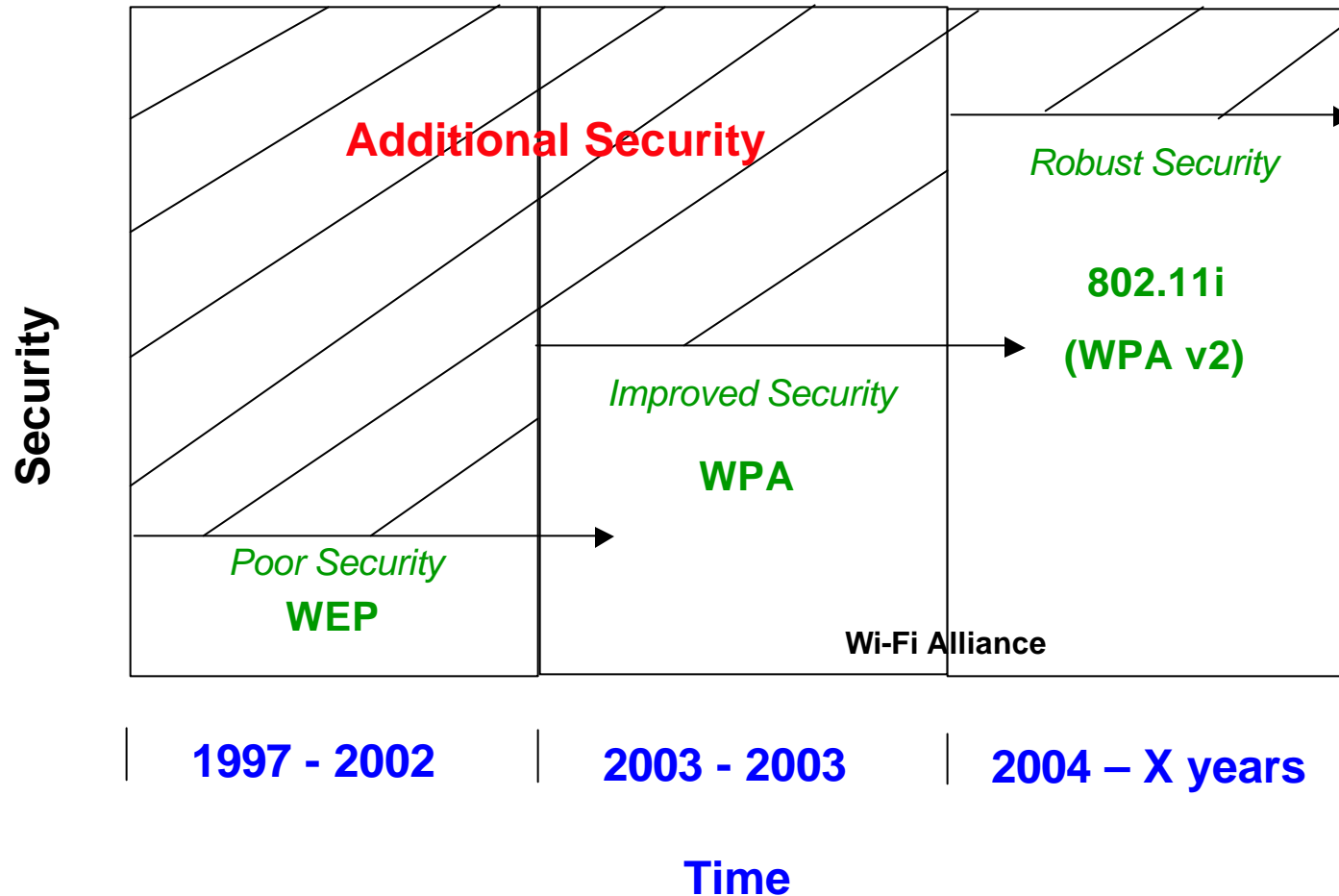
- ▶ May require hardware upgrade due to the processing requirements of AES.
 - Note: Some implementations may take advantage of host processing power and only require a software and/or a firmware upgrade.
- ▶ Consumers may not effectively plan for migration to 802.11i resulting in reliance on WPA longer than advisable.

Recommendations: 802.11i

- ▶ After final ratification of the 802.11i standard, migrate to the standard as soon as feasible. (approximately Q1 2004)
- ▶ Organizations should look to 802.11i for roaming requirements of mobile VoIP and mobile devices.

Summary

Evolution of WiFi Security (Illustrative only)



Conclusion

- ▶ WEP is Broken
- ▶ WPA Provides an interim solution to the WEP problem and long term support for legacy wireless infrastructure. (Q1/Q2 2003)
- ▶ The full 802.11i standard is expected to provide the robust security needed for wireless environments in the future.

| Thank You

Presenter Information

Brian R. Miller

Booz Allen Hamilton, Wireless Security

703/902-5189 (office)

703/328-2719 (cellular)

Miller_Brian_R@ bah.com (email)

| Questions?

		WPA	802.11i
	<u>WEP</u>	<u>TKIP</u>	<u>AES-CCMP</u>
<i>Cipher</i>	RC4	RC4	AES
<i>Key Size</i>	40 or 104 bits	128 bits	128 bits
		encryption, 64 bit auth	
<i>Key Life</i>	24-bit IV, wrap	48-bit IV	48-bit IV
<i>Packet Key</i>	Concat.	Mixing Fnc	Not Needed
<i>Integrity</i>			
<i>Data</i>	CRC-32	Michael	CCM
<i>Header</i>	None	Michael	CCM
<i>Replay</i>	None	Use IV	Use IV
<i>Key Mgmt.</i>	None	EAP-based	EAP-based