	WEP	TKIP	CCMP
Cipher Key Size(s)	RC4 40- or 104-bit encryption	RC4 128-bit encryption, 64-bit authentication	AES 128-bit
Key Lifetime Per-packet key	24-bit wrapping IV Concatenate IV to base key	48-bit IV TKIP mixing function	48-bit IV Not needed
Integrity Packet Header	None	Source and destination addresses protected by Michael	CCM
Packet Data Replay detection	CRC-32 None	Michael Enforce IV sequencing	CCM Enforce IV sequencing
Key Management	None	IEEE 802.1X	IEEE 802.1X

	WEP	WPA	WPA2
Encryption Analyzability	Relatively easy	Difficult	Impossible
Generation of key	Simple	Complicated	Complicated
Update function of key	N/A	Available	Available
Encryption engine	RC4	RC4	AES
Integrity Mechanism	N/A	Available	Available

	Cisco LEAP with TKIP	EAP-TLS with TKI	EAP-PEAP with TKIP	IPsec-based VPN
Key length (in bits)	128	128	128	168/128, 192, 256
Encryption algorithm	RC4	RC4	RC4	3DES/AES/other
Packet integrity	CRC-32/MIC	CRC-32/MIC	CRC-32/MIC	MD5-HMAC/ SHA-HMAC
Device authentication	No	Certificate	No	PSK/certificate
User authentication	Username/password	Certificate	Username/password	Username/ password or Certificate
Certificate requirements	None	RADIUS server/ WLAN client	RADIUS server	Optional
Additional hardware	No	Certificate server	Certificate server	IPsec Concentrator
Per-user keying	Yes	Yes	Yes	Yes
Protocol support	Any	Any	Any	IP unicast / any with L2TP
Open standard	No	Yes	IETF draft RFC	Yes

TABLE 1 COMPARISON OF DIFFERENT WI-FI PROTECTION MECHANISMS

Table 1. Main features of WEP, WPA, and WPA-2

	WEP	*WPA*	*WPA-2*
Authentication	N/A	IEEE 802.1X/ EAP/PSK	IEEE 802.1X/ EAP/PSK
Cryptographic algorithm	RC4	RC4	AES
Key size	40 O 104 bits	128 bits	128 bits
Encryption method	WEP	TKIP	CCMP
Data integrity	CRC32	MIC	CCM
Keys for packets	No	Yes	Yes
IV length	24 bits	48 bits	48 bits