EVOLUTION OF WIRELESS LAN SECURITY ARCHITECTURE TO IEEE 802.11i (WPA2)

Moffat Mathews, Ray Hunt
Department of Computer Science and Software Engineering,
University of Canterbury, New Zealand
{ray.hunt@canterbury.ac.nz}

ABSTRACT
Wireless LANs have gone through rapid changes with respect to their security architecture in recent years. One view has been to incorporate WLANs under already existing VPN umbrellas and to view them merely as an alternative access method — thus preserving existing VPN infrastructure. Another view has been to address the security of the airwaves which has been demonstrated to be extremely vulnerable. The evolution of security standardisation based upon the work of the IEEE has evolved from WEP to WPA which introduced new key management and integrity mechanisms through to WAP2 (IEEE 802.11i) which maintains the management and integrity mechanisms of WPA but introduces AES encryption as well as moving much of the security functionality to the hardware. This paper traces the evolution and development of this new WLAN security architecture.

KEY WORDS
Wireless LAN, IEEE802.11x, WEP (Wireless Equivalent Privacy), WPA (Wi-Fi Protected Access), TKIP (Temporal Key Integrity Protocol), AES (Advanced Encryption Standard)

1. Introduction

The use of wireless networking has grown rapidly, with organisations and home users extending their wired local area networks (LAN) to include wireless LANs (WLAN). The IEEE 802.11 (Wireless LAN) protocol has allowed for this seamless flow of data between the two types of LANs. WLAN users require the same level of security for their wireless data as they do for their wired LANs. However, wireless networks pose different security problems to wired networks. To gain access to a wired LAN, the attacker has to physically connect to the wired network. Wireless networks broadcast radio waves and an attacker with publicly available tools only has to be within range of the access point to initiate an attack.

As attacks on wireless LANs have become more widespread [1], security has evolved from that offered in the original IEEE 802.11 protocol to the IEEE 802.11i protocol which is starting to become widely used today. The evolution occurred in three main stages: the original IEEE 802.11b protocol, an intermediate stage with Wi-Fi Protected Access (WPA), and the third stage defining the IEEE 802.11i protocol. In 2000, after successful attacks were demonstrated on the IEEE 802.11 security standard — Wireless Equivalent Privacy (WEP) — the IEEE and Wi-Fi Alliance commenced the design of the IEEE 802.11i standard which was ratified in 2004 and came into use in 2006. To offer interim protection, the Wi-Fi Alliance created their own subset of the 802.11i protocol called the Wi-Fi Protected Access (WPA). This paper addresses each of the three stages involved in the evolution this WLAN security architecture.

2. Stage 1: IEEE 802.11b

In this stage, there were three main methods designed to implement security in the wireless network: MAC (Media Access Control) address filtering, Service Set Identifiers (SSID), and WEP (Wired Equivalent Privacy) [2].

2.1 Ethernet MAC Address Filtering

Although MAC Address Filtering is not part of the 802.11 standard, it is included here as it was widely deployed. At layer two, each network interface has a unique MAC address. This method of access control involves configuring the access points to only allow authorised MAC addresses to enter the network. A similar proprietary access control mechanism by Lucent is described in [3].

2.2 Service Set Identifiers (SSID)

The SSID acts as an identifier for a particular WLAN [2]. It is a 32-byte (or less) network name of a service set. There are two modes of operation: open and closed. In the open mode, the SSID of the AP (Access Point) is broadcast to the world, whereas in the closed mode it is not. Closed mode WLANs do not respond to messages unless they contain the correct SSID in the message headers. All devices connecting to a particular WLAN must be configured with the same SSID. The SSID is sent to the AP in the header of each message in clear text and confirmed by the AP before communication can progress.

2.3 WEP

Wired Equivalent Privacy (WEP) was established as a security standard when 802.11 was ratified, and aimed to provide an equivalent amount of privacy in the wireless network as in a wired network. Two agents or parties are

involved: the initiator (any network client) and the responder (an access point). It also recognised three main areas of relevant interest, namely authentication, encryption, and data integrity, and attempted to provide a security solution for each.

2.3.1 Authentication

Two types of authentication are available with WEP: the open system and the shared key system [4]. The open system always authenticates the client and permits all clients to enter the network, providing no authentication security. The shared key process requires the initiator to know some shared secret. The authentication process confirms that the initiator knows this secret, namely the WEP encryption key. The client sends an authentication request to the AP which then replies with a random number known as a challenge text. The client encrypts this challenge text with the WEP encryption key to produce the cipher text, which it sends to the AP for confirmation. The client is authenticated on a confirmation from the AP. Full protection against man-in-the-middle attacks can only be achieved with the use of digital certificates for authentication.

2.3.2 Encryption

WEP uses the RC4 symmetric stream cipher algorithm to perform encryption. The encryption key is shared amongst all stations that are connected to the AP. The steps in encrypting and creating a packet under WEP are shown in Figure 1. In the first step, the shared WEP key is added to a 24-bit initialisation vector (IV) to create a key for this packet. Due to export restrictions in place when the WEP was originally released, the initial length of the WEP key was 40 bits. This was later increased to 104 bits. The plain text data is XORed with the key to form the cipher text in the second step. For the receiver to decrypt the packet, the IV is added to the packet in plain text and sent to the receiver.

2.3.3 Data Integrity

To ensure that data is not changed en-route, a cyclic redundancy check (CRC-32) is created on the original packet and a 4-byte integrity check value (ICV) is calculated. The ICV is then encrypted and added to the original packet and sent to the receiver. The receiver also calculates the ICV value using the same algorithm, checks for similarity between the ICV values, and confirms data integrity. If even one bit is different, the packet is discarded.

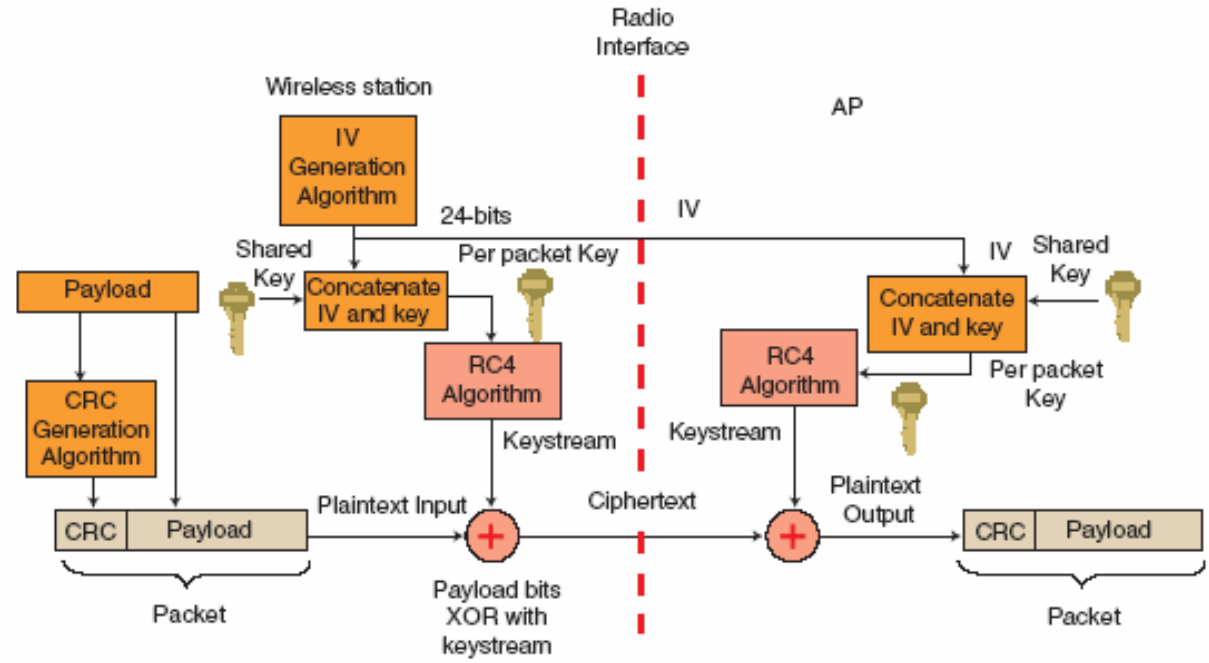

Figure 1: Overview of how Ciphertext is Constructed and Transmitted using WEP [5]

2.4 Vulnerabilities in IEEE 802.11

2.4.1 Problems with MAC address filtering

Two issues resulted in inadequate security for MAC filtering. First, the release of software such as Kismet[1], a network-sniffing tool, which captures large amounts of network traffic including MAC addresses of authorised computers, and SMAC[2], a tool used to change MAC addresses on a network interface card (NIC) created mechanisms for spoofing attacks. Second, the logistics of keeping continually updated lists of authorised MAC addresses, then updating the AP's with these lists — particularly in large networks — often created security

[1] http://www.kismetwireless.net

[2] http://www.klcconsulting.net/smac

holes when either these lists were not correctly updated, or an AP contained an out-of-date list.

2.4.2 Problems with SSID

Broadcasting the SSID in an open system creates its own vulnerability. A client may also send a *probe* request frame to find an AP with a particular SSID. Network beacon sniffers such as NetStumbler[3] can be used to find such networks. On closed networks, active beacon sniffers make too much noise and are easy to detect. However, passive sniffers with their network cards set to operate in monitor mode, passively capturing all traffic on a particular frequency band, can detect the SSID of a network [6].

2.4.3 Problems with WEP

WEP was shown to have critical security flaws in [7] and [8]. Some say that the vulnerabilities are not due to the weakness of each component but the incorrect use of the RC4 stream cipher and poor choice of CRC-32 to validate data integrity [4, 6]. The main problems responsible for the vulnerabilities are listed below.

In 802.11, the use of WEP is optional has to be manually configured. War driving experiments have found that a high percentage of wireless networks have no security implemented. With WEP, the AP confirms the identity of the mobile client. However, the mobile client does not confirm the identity of the AP. An attacker could use this one-way authentication process to their advantage by masquerading as the AP, authenticating clients, and redirecting traffic destined for the AP.

The WEP security system does not have a procedure for creating and managing the shared key or the initialisation vectors. How the secret key is shared between the stations is left up to the administrator and was never part of the 802.11 standard. As this can be laborious and time consuming, the keys are usually not changed frequently [9]. This allows for a patient attacker to collect a large amount of data relating to the same key, making decryption easier.

As the WEP key is shared, the addition of an IV to give a different initialisation state was also added. However since the IV is only 24 bits, it only provides 2^{24} combinations [10] and offers the possibility of having duplicate IV's in a relatively short time. The IV is also sent in plain text which allows an attacker to create a WEP key combination database or dictionary that can then be used to either inject or decode packets.

Three properties of the CRC checksum make it vulnerable to attack. First, the WEP checksum is a linear function of the message which introduces decryption vulnerabilities and can result in controlled modifications to the cipher text without disrupting the checksum. Second, the WEP checksum is an un-keyed function of the message which implies that an attacker can compute the checksum. Third, it is possible to reuse the IV without triggering alarms at the receiver. A detailed account of key stream reuse can be found in [8].

Fluhrer et al [8] found that certain keys when XORed with data did not have a significant effect, if any, on the output. These keys are termed *weak* keys. A patient attacker using a product like Airsnort[4] could exploit this fact to decipher the secret key [6]. The ICV is the encrypted value derived from the cyclic redundancy check. If the attacker has successfully gained the secret key, a new ICV can be calculated by running the CRC on the data before injecting the packet. As the ICV satisfies the check on the new data, the receiver would accept the packet as being legitimate.

3. Stage 2: WPA (Wi-Fi Protected Access)

To correct the flaws in WEP, the IEEE 802.11 Task Group I (TGi) introduced the Wi-Fi Protected Access (WPA) security structure containing the Temporal Key Integrity Protocol (TKIP). WPA operates in two modes: Preshared Key (PSK) and Enterprise [11]. The WPA-PSK offers less security than the Enterprise version, as it requires a shared secret; however, it is easier to install. The TKIP is a WEP patch, designed to run on current hardware, wrapping the WEP protocol with three new elements: a message integrity code (MIC) named *Michael*, a packet sequencing procedure, and a per packet key mixing function (Figure 2). Encryption is still carried out using the RC4 Stream Cipher.

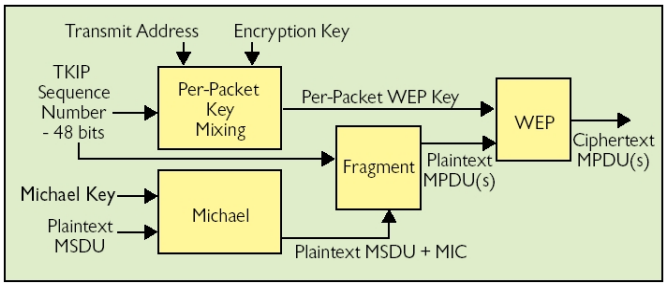

Figure 2: Flow of TKIP Processing [10]

3.1 Michael

The MIC algorithm checks for forgeries and ensures data integrity. A tag value is calculated at the sender's end, using the data and a predefined algorithm and sent with the key. The receiver makes a similar calculation, and verifies data integrity based on similarity of the tags. Different MIC algorithms such as HMAC-SHA1 can be used and are therefore superior to the CRC method used with WEP. However, as conventional algorithms are expensive, the TGi adopted a new algorithm called Michael. Michael uses a 64-bit key and requires a fresh key after an MIC validation error, or once per minute.

3.2 Packet Sequencing

To avoid replay attacks, TKIP uses a 48-bit sequence

[3] http://www.netstumbler.com

[4] http://airsnort.shmoo.com

number. This sequence is changed whenever a MIC key is replaced. The sequence number is mixed in with the encryption key and encrypts the MIC and WEP ICV. The AP discards any packets that have an out-of-sequence sequence number.

3.3 Per Packet Key Mixing

Instead of concatenating the IV with the key (as in WEP), a mixing function takes the key, the transmitter's MAC address, and packet sequence number and outputs a new WEP key [10].

3.4 Keys and authentication

TKIP requires two keys: a 128-bit key used by the mixing function described above to obtain a per packet key, and a 64-bit key used by Michael. TKIP uses the IEEE 802.1x protocol to authenticate users and provide a key management scheme by supplying fresh keys.

3.5 IEEE 802.1x

IEEE 802.1x [12] is an IEEE standard used in both wired and wireless networks to provide a means for authenticating clients onto a network. As PPP evolved from being used purely for dial-up Internet access, the requirement for a variety of more secure (and sometimes proprietary) authentication systems increased. To accommodate this need, a new protocol, the Extensible Authentication Protocol (EAP) [13] was created to form the framework within PPP upon which other authentication methods could operate. EAP standardised authentication, allowing remote servers to pass authentication methods onto the authenticating servers (e.g. RADIUS or DIAMETER) without having to decipher each protocol. This method of authentication was then adopted for use over LANs, using Ethernet instead of PPP. A protocol called EAP Encapsulation over LANs (EAPOL) [14] was created, and defined within the 802.1x IEEE standard.

IEEE 802.1x defines three participating entities in the authentication process: the supplicant, the authenticator, and the authentication server (Figure 3). The supplicant is the client that requires authentication onto the network; the authenticator is a mediating device between the client and the network that provides network access e.g. a network accesses server (NAS); the authentication server (AS) identifies the supplicant, checks its credentials, and defines privileges and restrictions, and allows or denies it access to the network and services. In the case of wireless networks, the supplicant could be any mobile node (MN) or device that requires connection to the network; the authenticator could be an access point (AP); the authentication server could be a RADIUS, DIAMETER, or any other device or server used for authentication. In some instances the authenticator and authentication server could be components of a single device.

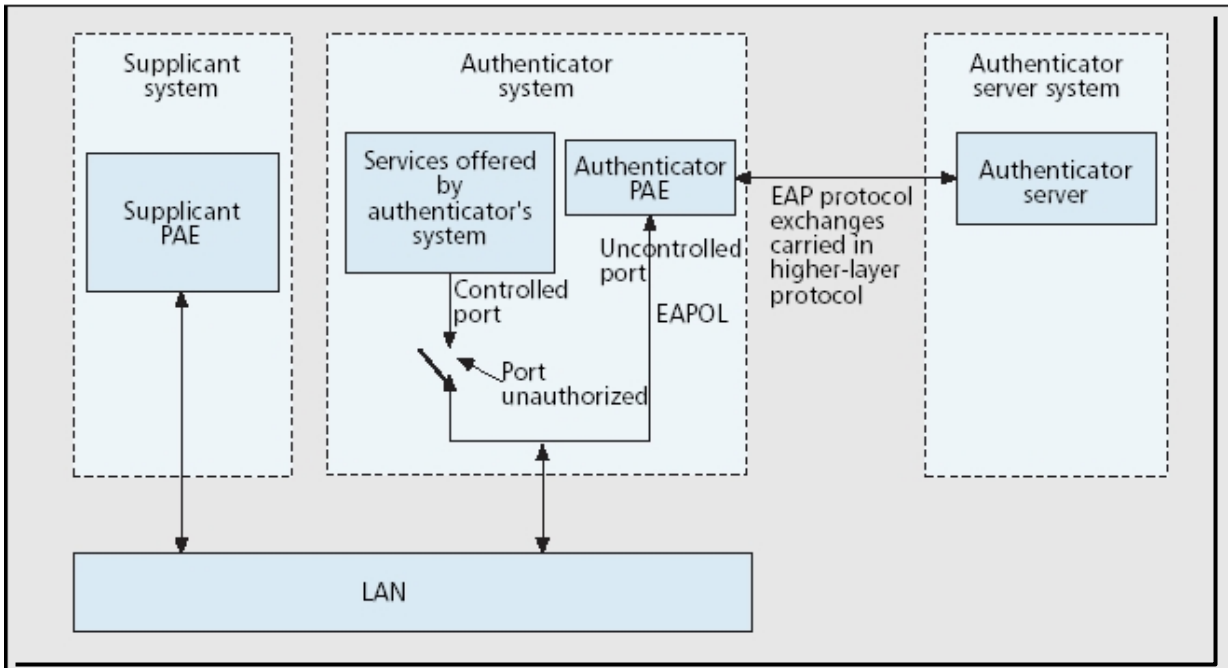

Figure 3: The IEEE 802.1x Framework [15]

The IEEE 802.1x standard allows for the authenticator to be relatively 'dumb', i.e. the authenticator does not have to have large processing and memory capabilities, as most of the processing is carried out at the authenticating server and client ends. This makes it an ideal protocol for WLANs, as most access points have relatively small processing and memory capabilities.

4. Stage 3: IEEE 802.11i (WPA2)

In 2004, the IEEE 802.11i standard was ratified and is also referred to by the Wi-Fi Alliance name —WPA2. The 802.11i standard implements the 128-bit Advanced

Encryption Standard (AES) block cipher algorithm for encryption and authentication. Uncontrolled ports are used for requests prior to authorisation. Authenticated clients are then granted access to network resources on controlled ports. Additionally 802.11i can use application layer authentication (Section 4.1).

4.1 Upper Layer Authentication

The 802.11i standard provides a secure network infrastructure, whilst still being flexible enough to leave the actual authentication choice to the enterprise. While the Wi-Fi Alliance recommends the use of EAP-TLS for authentication, the IEEE refrains from any recommendations, leaving the choice of authentication schemes such as Kerberos, EAP-LEAP, EAP-MDS, EAP-PEAP, EAP-TLS, EAP-TTLS, and EAP-SIM to the enterprise. The only requirement is that the authentication scheme chosen must operate with 802.1x.

4.2 Key Management

Whilst WPA uses TKIP, 802.11i uses AES-CCMP (Counter mode with CBC-MAC) for encryption. CCM (CBC-MAC) is used to calculate the MIC value so as to provide integrity and authentication. This replaces the old CRC-32 checksum method used with WEP.

Two types of key management systems exist: the use of an authentication server to generate and manage keys, or the use of pre-shared keys. Although complete implementation of the 802.11i protocol does not normally allow for pre-shared keys, this option is available to make implementation easier for home and small business users.

Key generation is hierarchical in nature. The 802.1x key generation protocols are used to help generate matching Pairwise Master Keys (PMK) at both the authentication server and supplicant ends. Four 128-bit temporal keys, together called the Pairwise Transient Key (PTK), are created each time a device associates with an AP: a data encryption key, a data integrity key, EAPOL-key encryption, and EAPOL-key integrity key. To add randomness, and associate the keys to the pairs of devices that created them, a random nonce and both the device MAC addresses are added to the key. Finally, the AP also has to prove its identity with the authentication server. A four way exchange occurs facilitating the process. The four way exchange (or handshake) consists of: a pair of nonces created by the supplicant and authenticator, temporal keys are generated, the supplicant proves it has knowledge of the PMK, the authenticator proves it has knowledge of the PMK, and both devices have encryption turned on for unicast packets. Details about the four way handshake can be found in [16].

80211i supports broadcast messages. To do this efficiently, a process facilitates the creation of a Group Master Key (GMK), which in turn is used to create the Group Encryption Key and the Group Integrity Key. These are transmitted securely to all the clients involved.

The main differences between the protocols discussed are shown in Figure 4. Being a relatively new protocol, further analysis of the claims of 802.11i security are still being undertaken. Another factor affecting the implementation of the 802.11i standard is that it requires a hardware upgrade.

Security Method → Property ↓	**WEP**	**WPA**	**802.11i (WPA2)**
Cipher	RC4	RC4	AES
Key Size	40/104 bits	128 bits (encryption) 64 bits (authentication)	128 bits
Key Life	24-bit IV Concatenate IV to base key	48/128-bit IV TKIP mixing function	48/128-bit IV TKIP mixing function
Packet Key	Concatenated	Mixing function	Not needed
Data Integrity	CRC-32	MIC (Michael)	CCM
Replay Detection	None	Enforce IV sequencing	Enforce IV sequencing
Header Integrity	None	MIC (Michael)	CCM
Key Management	None	EAP-based (802.1X)	EAP-based (802.1X)

Figure 4: Comparison of Security Protocol Feature

5. Conclusions

The IEEE 802.11 standard gave users the ability to seamlessly integrate their WLANs with their wired LANs, using the Ethernet protocol. This standard provided an optional security feature — WEP which was intended to provide the same level of security as a wired LAN. Other optional security measures such as access control lists (MAC address filtering) and SSID were also used. It soon was apparent that these methods were inadequate to provide security against a range of common attacks. Attacks carried out using publicly available tools, inexpensive equipment, and a bit of patience soon demonstrated the flaws in WEP and its associated infrastructure.

WEP's simple authentication procedures were easy to break. The encryption key used was shared amongst all clients thus increasing security risks. The case of using weak keys when the initialisation vector was added, posed a further vulnerability. Various attacks showed that the encryption could be cracked with available software tools in a relatively short time. With the failure of encryption, data integrity was also compromised, as WEP's data integrity check relied heavily upon encryption.

The IEEE standards committee decided on a new security protocol — IEEE 802.11i. In the meantime, an interim solution was implemented. This solution, called WPA, implemented the TKIP protocol. This was essentially a WEP patch, designed to run on current hardware, as a temporary fix to WEP's flaws. It used IEEE 802.1x for authentication and key management. It also implemented a message integrity code algorithm, a packet sequencing procedure, and a per packet key mixing sequence, designed to combat the attacks made on WEP.

In 2004, the IEEE 802.11i standard was ratified and WPA2-compliant products came onto the market in 2006. This standard used the 802.1x protocol for authentication and key generation. Instead of TKIP, it uses CCMP as its key integrity protocol. It also uses the AES encryption algorithm, requiring a hardware upgrade to AP's and NICs. The increase in key sizes, the use of temporal keys during the four way handshake to authenticate both the client and the AP, and the key mixing are designed to provide full data confidentiality, two-way authentication, and maintaince of data integrity.

As wireless networks become more prolific and complex, security vulnerabilities and issues will have to be met with well thought-out solutions to maintain the security required on the various networks. These security solutions have to become part of the initial design and not merely patches or upgrades if they are to deliver the claims they make.

6. References

[1] Stubblefield, A., Ioannidis, J., Rubin, A.. A key recovery attack on the 802.11b wired equivalent privacy protocol. *ACM Trans. Inf. Syst. Secur.*, 2004. 7(2): p.319.

[2] Yasir, Z. and Yang. T., Wireless LAN security and laboratory designs. *J. Comput. Small Coll.*, 2004. 19(3): p. 44-60.

[3] Arbaugh, W., Shankar, N. and Wan, Y., Your 802.11 Wireless Network has No Clothes. 2001, University of Maryland: Maryland. p. 1-13.

[4] Housley, R.. and Arbaugh, W., Security problems in 802.11-based networks. *Com. ACM, 2003*. 46(5): p. 31-34.

[5] Brown, B., 802.11: The Security Difference Between b and i. 2003, *IEEE Potentials*, Vol 22 No 4 p. 23-27, November 2003

[6] Berghel, H. and Uecker, J., Wireless infidelity II: airjacking. *Com. ACM, 2004*. 47(12): p. 15-20.

[7] Borisov, N., Goldberg, I., Wagner, D., Intercepting Mobile Communications: The Insecurity of 802.11, *Proc. 7th Annual Conf. on Mobile Computing and Networking, Rome, Italy*, p. 180-189, ACM SIGMOBILE, 2001.

[8] Fluhrer, S., Mantin, I. and Shamir,A., Weaknesses in the Key Scheduling Algorithm of RC4. *Proc. 8th Workshop on Selected Areas in Cryptography, Lecture Notes in Computer Science 2259*, Springer-Verlag, 2001

[9] Borisov, N., Goldberg, I., Wagner, D., Security of the WEP Algorithm. Available from: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.

[10] Cam-Winget, N., Housley, R., Wagner, D., Walker, J. Security flaws in 802.11 data link protocols. *Com. ACM*, 2003. 46(5): p. 35-39.

[11] Robinson, F., Examining 802.11i and WPA: The New Standards - Up Close. *Network Computing*, Ap. 2004.

[12] IEEE, IEEE Standard for Local and Metropolitan Area Networks: Port Based Network Access Control. 2004, IEEE. p. 1-179.

[13] Aboba, B., et al. RFC 3748: Extensible Authentication Protocol (EAP). 2004; http://www.ietf.org/rfc/rfc3748.txt.

[14] Stanley, D., Walker, J., Aboba, B., RFC 4017: Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs. 2005. http://www.ietf.org/rfc/rfc4017.txt

[15] Chen, J., Jiang, M., Liu, Y., Wireless LAN security and IEEE 802.11i. *Wireless Communications, IEEE*, 2005. 12(1): p. 27-36.

[16] He, C., Mitchell, J. Analysis of the 802.11i 4-way handshake, in *Proceedings of the 2004 ACM workshop on Wireless security*. 2004, ACM Press: Phil., PA, US.