Security of Wireless Local Area Networks

Whitepaper for information security practitioners

Franjo Majstor

fmajstor@cisco.com

v1.1

February 2003

Index

1 Introduction and scope

Wireless communication represents a wide area of radio technologies, as well as protocols on a wide scope of transmission frequencies. Although initially used in venues where traditional, wired networks were previously unavailable, the flexibility of wireless communication together with the adoption of the 802.11 standard has driven wireless communication to rapidly move into the information technology environment in the form of the so called Wireless Local Area Networks (WLAN). The present document aims to give information security practitioners a quick overview of WLAN technology and an in depth view of the current security aspects of the same technology. Likewise, it will present possible solutions and directions for future developments.

2 WLAN technology overview

Wireless local area networking technology has existed for several years, providing connectivity to wired infrastructures where mobility was a requirement for specific working environments. Early networks were based on different radio technologies and were nonstandard implementations, with speeds ranging between 1 and 2 Mbps. Without any standards driving WLAN technologies, the early implementations of WLAN were relegated to vendor-specific implementation, with no provision for interoperability, inhibiting the growth of standards-based WLAN technologies. Even WLAN is not a single radio technology, but is represented by several different protocols and standards, which all fall under the 802.11 umbrella of the Institute of Electrical and Electronics Engineers (IEEE) standards.

Put simply, WLAN is, from the network connectivity perspective, similar to the wired Local Area Network (LAN) technology with a wireless Access Point (AP) acting as a hub for the connection stations equipped with WLAN networking cards. As to the absence of wires, there is a difference in communication speed amongst the stations and AP, depending on which particular WLAN technology or standard is used for building the wireless network.

2.1 802.11 Alphabet

WLAN technology gained its popularity after 1999 through the 802.11b standardization efforts of IEEE , but it is not the only standard in the 802.11 family. Others are 802.11a, 802.11g, 802.11i or 802.1x. For information security practitioners it is important to understand the differences between them as well as to know the ones that have relevant security implications on wireless data communications. What is interesting to mention before we demystify the 802.11 alphabet is that particular letters a,b,g etc. were assigned by the starting time of development of the particular standard. Some of them, however, were developed and accepted faster than the others, so they will be described in the order of importance and the scope of usage instead of alphabetical order.

2.1.1 802.11b

The 802.11b standard defines communication speeds of 1, 2, 5 and 11 Mbps at a frequency of 2.4 GHz and is the most widely accepted WLAN standard at present with a large number of vendors producing 802.11b devices. The interoperability of the devices from different vendors is ensured by an independent organization originally called the Wireless Ethernet Compatibility Alliance (WECA), which identifies products that are compliant to the 802.11b standard with "Wi-Fi" (Wireless Fidelity) brand. WECA has recently renamed itself to Wi-Fi Alliance. From the networking perspective, the 802.11b standard offers 11 (USA), 13 (Europe) or 14 (Japan) different channels, depending on the regional setup, while only 3 of those channels are non-overlapping channels. Each of the channels could be easily compared to an Ethernet collision domain on a wired network, since only stations, which transmit data on non-overlapping channels, do not cause mutual collisions, as is a very similar behavior to a wired Ethernet segment in a hub based LAN environment.

2.1.2 802.11a

In 1999 the IEEE also ratified another WLAN technology, known as 802.11a. 802.11a operates at a frequency of 5 GHz and has 8 non-overlapping channels, compared to 3 of 802.11b, which offers data speeds ranging from 6 Mbps up to 54 Mbps. In spite of its speed, at present, it is far from the level of acceptance of 802.11b due to several reasons. There are fewer vendor offers on the market and WECA interoperability testing has yet been done. 802.11a operates at different frequency than 802.11b and is not backwards compatible with it. Due to different frequency allocation and regulations in different parts of the world, 802.11a might be in the near future replaced by a 802.11g as a new compromised solution.

2.1.3 802.11g

802.11g is the late entrant to the WLAN standardization efforts, which tries to achieve greater communication speeds at the same unlicensed frequency as 802.11b, i.e. 2.4 GHz, and also be backwards compatible with it. However 802.11g is at present not yet a ratified standard and there are no products offered by any of the vendors on the market. Due to practical reasons and the lateness of 802.11g standardizations efforts, vendors are also offering dual-band devices that are operating at both 2.4 GHz and 5 GHz, thus offering a flexible future migration path for connecting stations.

As was already mentioned above, there are multiple other "letters" in the alphabet of 802.11. 802.11d defines world mode and additional regulatory domains, 802.11e defines quality of service mechanisms, 802.11f is used as inter-access point protocol and 802.11h defines dynamic frequency selection and power control mechanisms, but they are all beyond the scope and level of this document. Others, like 802.11i and 802.1x, however, are very important from the security perspective and will be discussed in more detail in the sections on the security aspects of wireless LANs and on future developments.

3 WLAN security aspects

Considering that it doesn't stop at the physical boundaries or perimeters of a wired network, wireless communication has significant implications on security aspects of modern networking environment. WLAN technology has, precisely for that reason, built in the following mechanisms, which are meant to enhance the level of security for wireless communication:

- Service Set Identifier (SSID)
- Device authentication mechanisms
- Media Access Control (MAC) address filtering
- Wired Equivalent Privacy (WEP) encryption

3.1 Service Set Identifier

The Service Set Identifier (SSID) is a mechanism similar to a wired world Virtual Local Area Network (VLAN) ID that allows the logical separation of wireless LANs. In general, a client must be configured with the appropriate SSID to gain access to the wireless LAN. The SSID does not provide any data-privacy functions, nor does it really authenticate the client to the access point. SSID is advertised in plain text in the access point beacon messages. Although beacon messages are transparent to users, an eavesdropper can easily determine the SSID with the use of an 802.11 wireless LAN packet analyzer or by using a WLAN client that displays all available broadcasted SSIDs. Some access-point vendors offer the option to disable SSID broadcasts in the beacon messages, but the SSID can still be determined by sniffing the probe response frames from an access point. Hence it is important to understand that the SSID is not designed, nor intended for use, as a security mechanism. In addition, disabling SSID broadcasts might have adverse effects on Wi-Fi interoperability for mixed-client deployments.

3.2 Device authentication

The 802.11 specification provides two modes of authentication: open authentication and shared key authentication. Open authentication is a null authentication algorithm. It involves sending a challenge, but the AP will grant any request for authentication. It is simple and easy mainly due to 802.11-compliancy with hand-held devices that do not have the CPU capabilities required for complex authentication algorithms. A shared key authentication is the second mode of authentication specified in the 802.11 standard. Shared key authentication requires that the client configure a static WEP shared key and involves sending a challenge and then receiving an encrypted version of the challenge. Most experts believe that using shared key authentication is worse than using an open one and recommend turning it off. However, shared key authentication could help deter a denial of service (DoS) attack if the attacker doesn't know the correct WEP key. Unfortunately, there are other DoS attacks available.

It is important to note that both authentication mechanisms in the 802.11 specifications authenticate only wireless nodes and do not provide any mechanism for user authentication.

3.3 Media Access Control (MAC) address authentication

MAC address authentication is not specified in the 802.11 standard, but many vendors support it. MAC address authentication verifies the client's MAC address against a locally configured list of allowed addresses or against an external authentication server. MAC authentication is used to augment the open and shared key authentications provided by 802.11, further reducing the likelihood of unauthorized devices accessing the network.

However, as required by 802.11 specification MAC addresses are sent in the clear during the communication. A consequence for wireless LANs that rely only on MAC address authentication is that a network attacker might be able to bypass the MAC authentication process by "spoofing" a valid MAC address.

3.4 Wired Equivalent Privacy encryption

All of the previous mechanisms addressed the access control, while none of them so far has addressed the confidentiality or integrity of the wireless communication. Wired Equivalent Privacy (WEP), the encryption scheme adopted by the IEEE 802.11 committee, defines for that purpose the use of a symmetric key stream cipher RC4 that was invented by Ron Rivest of RSA Data Security, Inc. (RSADSI). A symmetric cipher uses the same key and algorithm for both encryption and decryption. The key is the one piece of information that must be shared by both the encrypting and decrypting endpoints. RC4 allows the key length to be variable, up to 256 bytes, as opposed to requiring the key to be fixed at a certain length. IEEE specifies that 802.11 devices must support 40-bit keys with the option to use longer key lengths. Several vendors support 128-bit WEP encryption with their wireless LAN solutions. WEP has security goals of confidentiality and integrity but could be used also as an access control mechanism. A node that lacks the correct WEP key cannot send data to nor receive data from an access point and also should not be able to decrypt the data nor change its integrity. The previous statement is fully correct in a sense that the node that does not have the key cannot access the WLAN network nor see or change the data. However several cryptography analysis listed in references, have explained the possibility that, given sufficient time and data, it is possible to derive the WEP key due to flaws in the way the WEP encryption scheme uses RC4 algorithm.

3.4.1 WEP vulnerabilities

Since WEP is a stream cipher, it requires a mechanism that will ensure that the same plaintext will not generate the same ciphertext. This is the role of an initialization vector, or IV, which is concatenated with the key bytes before generating the stream cipher. The IV is a 24-bit value that the IEEE suggests, although does not mandate, to be changed per each frame. Since the sender generates the IV with no standard scheme or schedule, it must be sent unencrypted with the data frame to the receiver. The receiver can concatenate the received IV with the WEP key it has stored locally to decrypt the data frame.

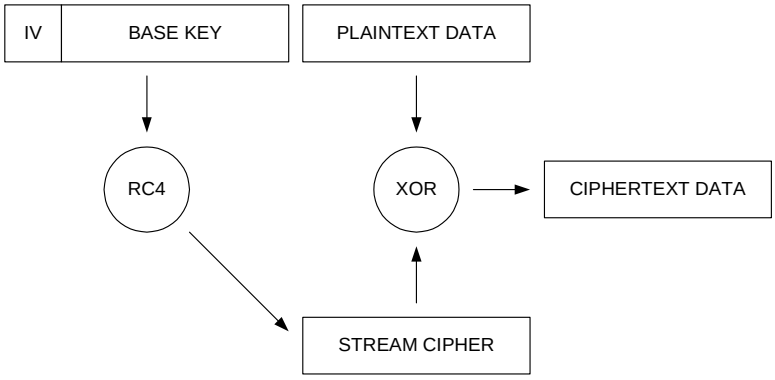

Exhibit 1: The WEP encryption process

The IV is the source of most problems with WEP. Since the IV is transmitted as plaintext and placed in the 802.11 header, anyone sniffing a WLAN can see it. At 24 bits long, the IV provides a range of 16,777,216 possible values. Analysts at University of California at Berkeley found that when the same IV is used with the same key on an encrypted packet (known as an IV collision), a person with malicious intentions could capture the data frames and derive information about the WEP key. Furthermore, cryptanalysts Fluhrer, Mantin, and Shamir (FMS) have also discovered inherent shortcomings in the RC4 key-scheduling algorithm. FMS have explained shortcomings that have practical applications in decrypting 802.11 frames using WEP by using a large class of weak IVs that can be generated by RC4, and have highlighted methods to break the WEP key using certain patterns in the IVs. Although the problem explained by FMS is pragmatic, the most worrying fact is that the attack is completely passive and that it has also been practically implemented by the AT&T Labs and Rice University and some tools publicly available on the Internet like Airsnort.

Further details about WEP weaknesses are explained in detail in references, but for information security practitioners it is important to understand that the 802.11 standard, together with its current WEP implementation, has security weaknesses which have to be taken care of when deploying WLAN networks.

4 WLAN Security Solutions

Major security issues in WEP are that, firstly, it does not define the key exchange mechanism and, secondly, it has implementation flaws with the use of static keys. An additional missing security element from the current security 802.11 feature set is the lack of individual user authentication. Information security practitioners should be aware of this and look for solutions appropriate to their environment. A proposal jointly submitted to the IEEE by Cisco Systems, Microsoft, and other organizations introduced a solution for the above issues using 802.1X and the Extensible Authentication Protocol (EAP) to provide enhanced security functionality. Central to this proposal are two main elements:

- EAP allows wireless clients that may support different authentication types to communicate with different back-end servers such as Remote Access Dial-In User Service (RADIUS).

- IEEE 802.1X, a standard for port based network access control.

4.1 IEEE 802.1x Protocol

The 802.1x is a port-based security standard protocol developed by IEEE 802.1 working group for network access control for wired networks. Its major role is to block all the data traffic through any network port until the client user authentication process has been successfully completed. In essence it operates as a simple switch mechanism for data traffic as is illustrated in Exhibit 2.

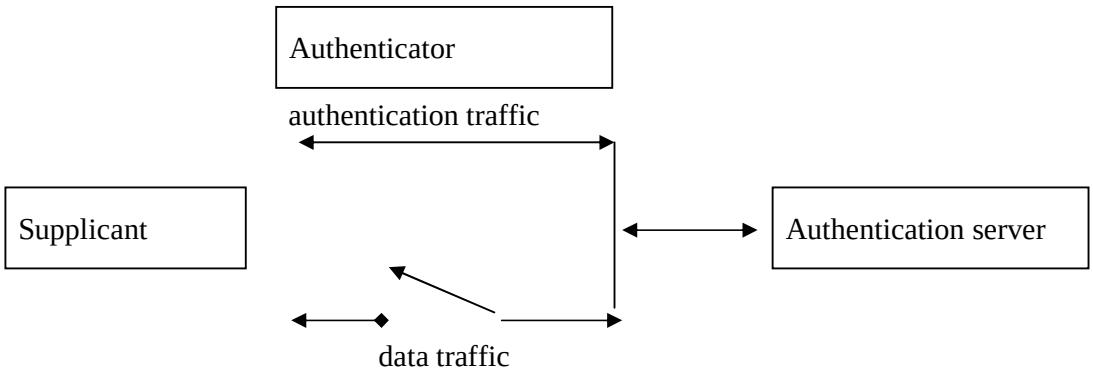

Exhibit 2: The 802.1x port access control mechanism

4.2 Extensible Authentication Protocol

Extensible Authentication Protocol (EAP) is a flexible authentication protocol specified in RFC 2284 that rides on top of another protocol such as 802.1X or RADIUS. It is an extension of the Point-to-Point Protocol (PPP) that enables the support of advanced authentication methods such as digital certificates, MD-5 hashed authentication or One Time Password (OTP) protocols. Layers of 802.1x and EAP methods are illustrated on Exhibit 3.

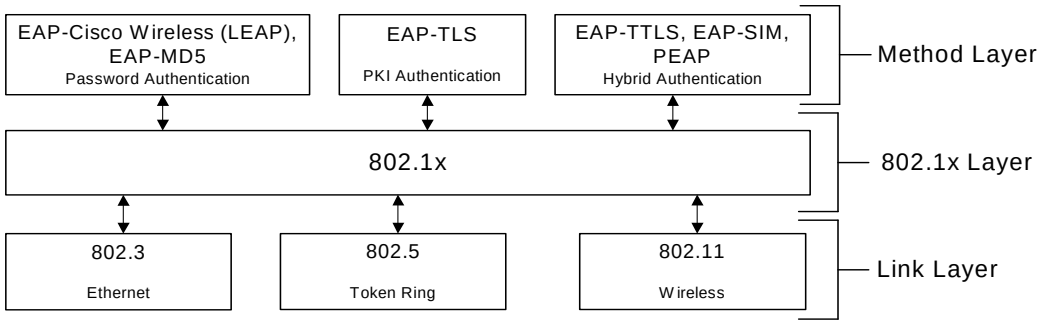

Exhibit 3: EAP and 802.1x layers

4.3 Dynamic key exchange mechanisms

Each of the mentioned EAP protocols, except EAP-MD5, provides a solution to WEP security problems by tying the dynamic key calculation process to an individual user authentication. With the EAP mechanism each individual user obtains its own unique dynamic WEP key that is changed every time the user connects to an access point. Alternatively, it could also be recalculated based on the timeout defined on the authentication server.

4.3.1 EAP-MD5

EAP-MD5 (Message Digest 5) is the easiest of EAP authentication schemes, which provides only user authentication. The user authentication scheme employed is a simple username/password method that incorporates MD5 hashing for more secure authentication. It does not provide a mutual authentication nor the method for dynamic WEP key calculation, hence it still requires manual WEP key configuration on both sides, client side as well as on the wireless Access Point (AP) side.

4.3.2 EAP-Cisco Wireless or Lightweight Extensible Authentication Protocol (LEAP)

EAP-Cisco Wireless, also known as LEAP (Lightweight Extensible Authentication Protocol), is an EAP method developed by Cisco Systems. Based on the 802.1x authentication framework, EAP-Cisco Wireless mitigates several of the weaknesses by utilizing dynamic WEP key management. It supports mutual authentication between the client and an Authentication Server (AS) and its advantage is that it uses a simple username/password mechanism for providing dynamic per-user, per-session WEP key derivation. A wireless client can only transmit EAP traffic after it is successfully authenticated. During the user login, mutual authentication between the client and the AS occurs. A dynamic WEP key is then derived during this mutual authentication between the client and the AS, and the AS sends the dynamic WEP key to the Access Point (AP). After the AP receives the key, regular network traffic forwarding is enabled at the AP for the authenticated client. The credentials used for authentication, such as a log-on password, are never transmitted in the clear, or

without encryption, over the wireless medium. Upon client logoff, the client association entry in the AP returns to the non-authenticated mode. EAP-Cisco Wireless mechanism also supports dynamic re-keying based on the predefined timeout pre-configured on the AS. The disadvantage of EAP-Cisco Wireless method is that, although it is based on an open standard, it is still proprietary and its authentication mechanism is limited to a static user name and password, thus eliminating the possible use of One Time Password (OTP) user authentication mechanism.

4.3.3 EAP-TLS

The EAP Transport Layer Security (TLS) as defined in RFC2716 is a Microsoft-supported EAP authentication method based on the TLS protocol defined in RFC2246. TLS is the IETF version of Secure Socket Layer (SSL) used in most web browsers for secure web application transactions. TLS has proved to be a secure authentication scheme and is also available as an 802.1x EAP authentication type. TLS utilizes mutual authentication based on X.509 certificates. Since it requires the usage of digital certificates on both the client and on the authentications server side, it is the most secure method for user authentication and dynamic per-user, per-session WEP key derivation that also supports OTP servers. EAP-TLS security superiority over any of the other EAP methods is, at the same time, its weakness, since it is overkill to require the establishment of a Public Key Infrastructure (PKI) with a certificate authority to distribute, revoke, and otherwise manage user certificates just to be able to use layer two WLAN connectivity. This is the main reason why TLS has resulted in the development of a hybrid, compromised solutions such as EAP-TTLS and PEAP.

4.3.4 EAP-TTLS

EAP-TTLS or EAP Tunneled TLS protocol is an 802.1X EAP authentication method that was jointly authored by Funk Software and Certicom, and is currently an IETF draft RFC. It uses server-side TLS and supports a variety of authentication methods, including passwords and OTPs.

With the EAP-TTLS method, the user's identity and password-based credentials are tunneled during authentication negotiation, and are therefore not observable in the communications channel. This prevents dictionary attacks, man-in-the-middle attacks, and hijacked connections by wireless eavesdroppers. In addition, dynamic per-session keys are generated to encrypt the wireless connection and protect data privacy. The authentication server can be configured to re-authenticate and thus re-key at any interval, a technique that thwarts known attacks against the encryption method used in WEP.

4.3.5 Protected EAP (PEAP)

Protected EAP (PEAP) is another IETF draft developed by RSA Security, Cisco Systems and Microsoft. It is an EAP authentication method that is, similar to EAP-TTLS, designed to allow hybrid authentication. It uses digital certificate authentication for server-side only, while for the client-side authentication, PEAP can use any other EAP authentication type. PEAP first establishes a secure tunnel via server-side authentication, and secondly it can use

any other EAP type for client-side authentication, like one-time passwords (OTP) or EAP-MD5 for static password based authentication. PEAP is by using only server-side EAP-TLS addressing the manageability and scalability shortcomings of EAP-TLS for user authentication. It avoids the issues associated with installing digital certificates on every client machine as required by EAP-TLS so the clients can select the method that best suits them.

4.3.6 EAP-SIM

The EAP subscriber identity module (SIM) authentication method is an IEEE draft protocol designed to provide per-user/per-session mutual authentication between a WLAN client and an AS like all of the previous methods. It also defines a method for generating the master key used by the client and AS for the derivation of WEP keys. The difference between EAP-SIM authentication and other EAP methods is that it is based on the authentication and encryption algorithms stored on the Global System for Mobile Communications (GSM) subscriber identity module (SIM) card, which is a Smartcard designed according to the specific requirements detailed in the GSM standards. GSM authentication is based on a challenge-response mechanism and employs a shared secret key, which is stored on the SIM and otherwise known only to the GSM operator's Authentication Center. When a GSM SIM is given a 128-bit random number as a challenge, it calculates a 32-bit response and a 64-bit encryption key using an operator-specific algorithm. In GSM systems, the same key is used to encrypt mobile phone conversations over the air interface.

4.4 EAP methods compared

It is obvious that a variety of EAP methods try to solve the WLAN security problems. All of them, with the exception of the EAP-SIM method specifics to GSM networks and EAP-MD5, introduce solutions for user authentication and dynamic key derivation by using different mechanisms of protection for the initial user credentials exchange and different legacy user authentications methods. The feature of EAP method comparison is shown in table form on Exhibit 4.

	EAP-MD5	EAP-TLS	EAP-Cisco Wireless	EAP-TTLS	PEAP
Dynamic WEP Key	**No**	**Yes**	**Yes**	**Yes**	**Yes**
Mutual Authentication	**No**	**Yes**	**Yes**	**Yes**	**Yes**
Client Certificate	**No**	**Yes**	**No**	**No**	**No**
Server Certificate	**No**	**Yes**	**No**	**Yes**	**Yes**
Static Password	**Yes**	**No**	**Yes**	**Yes**	**Yes**
OTP Support	**No**	**Yes**	**No**	**No**	**Yes**

Exhibit 4: EAP Methods Compared

5 VPN and WLAN

5.1 Combining IPsec based VPN and WLAN

Since WLAN media can carry IP protocol over it without any problems, it comes easily as an idea for solving all security problems of WEP to simply run IP Security Protocol or IPsec over WLAN. While fairly standardized and security robust IPsec based solution could certainly help to improve the security of communication over WLAN media, it also has its own limitations to the overall problem. WLAN media can carry any type of IP traffic, including broadcast and multicast, while IPsec is limited to unicast traffic only. Hence if it is necessary to support mutlicast application over WLAN, IPsec does not represent a viable solution. While it is possible to run IPsec encryption algorithms like DES or 3DES in hardware, it is very seldom the case that the client personal computers are equipped with the additional IPsec hardware accelerators. That means that IPsec encryption is done only in the software, limited with a speed of the personal computer CPU that certainly represents a bottleneck and thus reduces the overall speed of communication over WLAN media in particular on low CPU handheld devices. IPsec authentication mechanisms support pre-shared key, RSA digital-signatures and digital certificates, which are all flexible options, but only digital certificates are the most scalable and robust secure option, which requires establishment of PKI services. If PKI services are already established, the same security level could be also achieved with EAP-TLS. The EAP-TLS method avoids all the limitations of IPsec with regard to the overall solution. Last but not least, running IPsec on user personal computers most of the time requires, depending on the operating systems, additional software installation plus loss of user transparent connectivity and it keeps the device protected only while the IPsec tunnels is established. Overall, IPsec protected WLAN communication could possibly solve WLAN security problems, but it is not always applicable and requires an examination of its benefits and disadvantages before being deployed.

6 Future directions

The IEEE has formed a task group i (TGi) working on 802.11i protocol specification to solve the security problems of WEP protocol and provide a standardized way of doing it. The solution will most probably come in multiple phases with a first initial help for already known problems up to the replacement of the encryption scheme in WEP protocol.

6.1 Temporal Key Integrity Protocol

Temporal Key Integrity Protocol (TKIP), aims to fix the WEP integrity problem and is intended to work with existing and legacy hardware. It uses a mechanism called fast-packet re-keying, which changes the encryption keys frequently and provides two major enhancements to WEP:

- A message integrity check (MIC) function on all WEP-encrypted data frames.
- Per-packet keying on all WEP-encrypted data frames.

The MIC augments the ineffective integrity check function (ICV) of the 802.11 standard and is designed to solve the following major vulnerabilities of IV reuse and bit flipping. For Initialization Vector/base key reuse - the MIC adds a sequence number field to the wireless

frame so that the AP can drop frames received out of order. For frame tampering/bit flipping problem - the MIC feature adds a MIC field to the wireless frame, which provides a frame integrity check not vulnerable to the same mathematical shortcomings as the ICV.

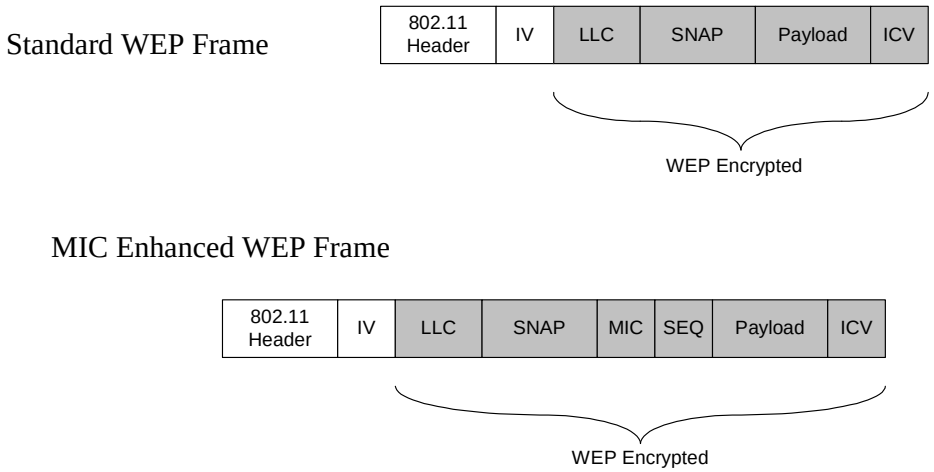

Exhibit 5: Message Integrity Check - MIC

TKIP is using advanced hashing techniques, understood by both the client and the access point, so that the WEP key is changed on a packet-by-packet basis. The per-packet key is a function of the dynamic, base WEP key. TKIP is not yet required for Wi-Fi certification, but WECA hopes to add it to its certification testing later in the year.

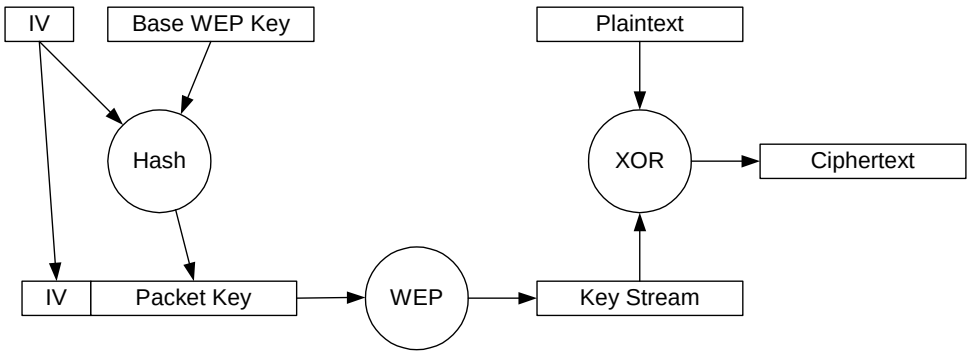

Exhibit 6: The TKIP encryption process

Wi-Fi Alliance has accepted TKIP as an easy, software based upgrade, intermediate solution for WEP security issues and has established a new certification program under the name of Wi-Fi Protected Access or WPA. On a side of TKIP for WEP encryption improvement, WPA also covers user authentication mechanisms relaying on 802.1x and EAP.

6.2 Advanced Encryption Standard

In essence, all of the mentioned proposals do not really fix the WEP vulnerabilities, but when combined with packet re-keying significantly reduce the probability that an FMS or Berkely attack will be effective. Flaws with RC4 implementation still exist but are harder to compromise since there is less traffic with identical keys. Standards bodies are investigating the use of the Advanced Encryption Standard (AES) as a possible alternative to RC4 in future versions of 802.11 security solutions. AES is a replacement for DES (Data Encryption Standard) and uses the Rijndael algorithm, which was selected by the US Government to protect sensitive information. However, the standardization of AES to solve encryption problems is currently still under discussion without any commercially available products on the market today. As standards continue to develop, many security experts recommend using Internet Protocol Security or IPSec standard that has been deployed in global networks for over five years as an alternative available today.

7 Summary

WLAN technology based on 802.11 standards plays an important role in today's modern networking and although it has its advantages in rapid and very flexible deployment, information security practitioners should be aware of its security weaknesses. Multiple proposals are on the scene to address major flaws in the WEP security protocol with different mechanisms for cryptographic integrity checks, dynamic key exchange and individual user authentication. It is important to understand what security functionalities they offer or miss. While IPsec VPN technology deployed over WLAN is an optional solution too, it requires additional hardware and, hence, creates additional costs besides its limitations. Out of multiple EAP proposals for per-user/per-session dynamic WEP key derivation, it is expected that EAP-TTLS or PEAP will be the predominant solutions in the near future, assuming either solution gets ratified. As the short-term solution for 802.11 security problems, an alliance of multiple vendors has decided to adopt the TKIP solution as a sufficient fix for existing WEP vulnerabilities under the name of Safe Secure Networks (SSN) even before its final approval by the IEEE 802.11i standards body and Wi-Fi Alliance has also adopted the similar scheme for its vendor interoperability testing under the name of Wi-Fi Protected Access (WPA) which all together gives the bright future for the safer WLAN networks deployment.

8 References

[1] Aboba, B., Simon, D., PPP EAP TLS Authentication Protocol, RFC 2716, October 1999.

[2] Andersson, H., Josefsson, S., Zorn, G., Simon, D., Palekar, A., Protected EAP Protocol (PEAP), IETF Internet Draft, < draft-josefsson-pppext-eap-tls-eap-05.txt>, September 2002.

[3] AT&T Labs and Rice University paper, Using the Fluhrer, Mantin, and Shamir Attack to Break WEP, <www.cs.rice.edu/~astubble/wep/wep_attack.pdf>, August 21st 2001.

[4] Blunk, L.,Vollbrecht, J., EAP PPP Extensible Authentication Protocol (EAP), RFC 2284, March 1998.

[5] Greem, Brian C., Wi-Fi Protected Access, <www.wi-fi.net/opensection/pdf/wi-fi_protected_access_overview.pdf>, October 2002.

[6] Fluhrer, S., Mantin, I., Shamir, A., Weaknesses in the Key Scheduling Algorithm of RC4, <www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps>

[7] Funk, P., Blake-Wilson, S., EAP Tunneled TLS Authentication Protocol (EAP_TTLS), IETF Internet Draft, <draft-ietf-pppext-eap-ttls-01.txt >, February 2002.

[8] SAFE: Wireless LAN Security in Depth, white paper from Cisco Systems, Inc.,<Cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm>