

Securing WLAN: From WEP to WPA

Demian Machta

Computer Security CS574

Instructor : T.Perrine

Word count: 3270
San Diego State University, Fall 2003
dmachta@eresmas.com

Index

I.	Introduction.....	3
II.	Wired Equivalent Privacy: WEP.....	5
III.	Wi-Fi Protected Access	
	III.1 Overview.....	8
	III.2 Temporary Key Integrity Protocol.....	9
	III.3 Authentication with 802.1X and EAP.....	12
IV.	Conclusions.....	15
V.	References and Citations.....	17
VI.	Bibliography.....	18

I. Introduction

Using high-frequency radio waves instead of wires to communicate between nodes, **Wireless Local Area Networks (WLAN)** are convenient and flexible, providing the user with mobility and ease of use. In the last few years we have seen an incredible growth in use and popularity of such networks. Today, the costs of equipment have dropped dramatically and “going wireless” is becoming a mainstream.

At the same time **security concerns** have raised. A large amount of information travels across the air in the form of radio waves, and there is a need for the information to be kept secret and confidential, preserving its integrity.

The two primary means of securing a network are **encryption** and **authentication**.

Encryption is a means of maintaining secure data in an insecure environment, such as the air. By a process of encoding the information transmitted over the physical medium, we intend to keep our data private, enforcing **confidentiality**, keeping intruders or interceptors from accessing it or modifying it, ensuring **integrity**.

It is also necessary that only **authorized users** access the resources provided by the network. Therefore there has to be authentication: a way to validate identity claims and clearance to the system of those who want to access the resources of the WLAN.

Wired Equivalent Privacy (WEP) is the original native security mechanism for WLANs since the release in 1997 of the 802.11 specification for WLAN by the **Institute of Electrical and Electronics Engineers (IEEE)**.

However WEP has been found to have several **flaws**, including cryptographic weaknesses. “A series of independent studies from various academic and commercial institutions had shown that an intruder equipped with the proper tools and a moderate amount of technical knowledge could gain unauthorized access to a WLAN even with WEP enabled” [WiFi2003].

Estimates indicate that by the end of 2003 more than 50% of the enterprises in this country will have a WLAN installation [Gart2002]. Concerned that a weak wireless security mechanism would slow down the adoption of Wi-Fi devices into the market, the **Wi-Fi Alliance** along with the IEEE initiated an effort to bring a strongly improved, standards-based, interoperable Wi-Fi security solution to the market. Those efforts have resulted in **Wi-Fi Protected Access (WPA)**, a security specification that addresses WEP flaws and vulnerabilities and that is intended to provide the confidentiality and integrity that companies were demanding to deploy WLAN.

In the present paper we will introduce the characteristics of WEP and identify its risks and vulnerabilities. Subsequently, we will discuss about WPA. Its history, main features and the way it has addressed the flaws encountered in WEP. We will focus with some emphasis in its encryption method, **TKIP**, as well as in the authentication that provides using **802.1X/EAP**. Finally we will conclude this paper summarizing the work done, evaluating the solutions provided by WPA, comparing them with WEP and foreseeing its future paper in 802.11i.

II. Wired Equivalent Privacy: WEP

WEP was the original native security mechanism for WLAN developed by IEEE members in order to provide security through a 802.11 network. "WEP was used to protect wireless communication from eavesdropping (confidentiality), prevent unauthorized access to a wireless network (access control) and prevent tampering with transmitted messages (data integrity)"[Wong2003]. It was intended to provide wireless users with the equivalent level of privacy inbuilt in wireless networks.

WEP appends a **32-bit CRC** checksum to each outgoing frame and then encrypts it using **RC4** stream cipher and 40 or 104-bit message keys and a 24-bit random initialization vector. The **Initialization Vector (IV)** and default key on the station and access point are used to create a **key stream** which is then used to convert the plain text message into the WEP encrypted frame.

WEP also decrypts each frame with the same message key and then validates the CRC checksum, being therefore a **symmetrical key** algorithm.

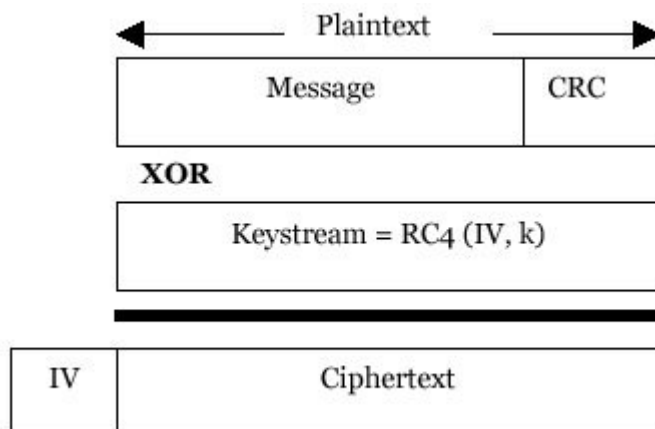


Figure 1 – Encrypted WEP Frame [LaRos2003]

RC4 and the message key are used to ensure privacy and access control whereas CRC checks for the integrity of the frame. However, "Use of RC4 for data privacy and CRC-32 for data integrity is due mainly to their speed and ease of implementation, but they do not provide cryptographically secure encryption and authentication"[Park2002]. If WEP remains useful for home users and small office/home office environments providing some protection, WEP alone **does not provide adequate security** for wide scale enterprise adaptation.

There have been many flaws and vulnerabilities identified in WEP. These include:

-**Weak keys:** It allows an attacker to discover the default key being used by the Access Point and client stations. This enables an attacker to decrypt all messages being sent over the encrypted channel.

-**Initialization vector reuse:** Being 24-bit long, there are 2^{24} different IVs. On a busy network, the IV will surely be reused, if the default key has not been changed, the original message can be retrieved relatively easily.

-**Known plaintext attacks:** Also exploit the reuse of IVs in WEP, making it possible to determine keystreams. This would enable an attacker to forge packets obtaining access to the WLAN.

-**Denial of Service Attacks:** Lacking strong authentication methods, DoS are trivial to implement. An attacker can record valid WEP packets and then retransmit them later (replay attack)

-**CRC is vulnerable:** WEP checksum is a linear unkeyed operation. An attacker could compromise data integrity arbitrarily modifying the messages without full knowledge of the original message.

-None/poor key management: There's no mechanisms to renew the stored WEP keys. In addition the message keys are shared between all members of the WLAN.

-No access point authentication: WEP only provides a method for Network Interface Cards (NIC) to authenticate Access Points (AP). An AP can not authenticate NICs. This enables the possibility for an attacker to re-route the data to access points through an alternate unauthorized path.

The combination of IV reuse and weak keys, can allow an attacker to retrieve the original message without even knowing the key. Statistical analysis of natural language have shown that some characters appear with more frequency than others. Having two messages share the same IV and with no change in the message key (most likely to happen), a message will have the same keystream. With today's technology it is then feasible to decrypt encoded messages.

Upon the discovery of all WEP's vulnerabilities, many companies have tried to use **custom security solutions** and other proprietary technologies to increase WLAN protection. Vendors have also come up with modifications to WEP to enhance its performance. Such custom solutions include:

- Enhanced WEP key
- Dynamic WEP
- Virtual Private Networks (VPNs)

III. Wi-Fi Protected Access (WPA)

III.1 Overview

Concerned that a weak wireless security mechanism like WEP would refrain enterprises from deploying WLANs, the Wi-Fi alliance along with the IEEE initiated an effort to bring a strongly improved, standards-based, interoperable Wi-Fi security solution to the market. In October 2002, WPA was born as a strong interoperable security specification for WLAN.

WPA very much increases the level of data protection and access control on existing and future WLANs, **addressing all the vulnerabilities** of its predecessor WEP. And it will fully replace WEP as the Wi-Fi security solution.

With the apparition of Wi-Fi Protected Access, companies that have been using add-on security mechanisms such as VPNs, will find that those are not longer needed to secure the wireless segments of the network. WPA allows to **secure all existing versions of 802.11 devices**: a, b, g, multi-band and multi-mode, since it has been designed to minimize the impact on network performance running as a **software upgrade** on the many Wi-Fi devices in today's market. Access Points, Network Interface Cards and possibly Operating systems will require a software upgrade in order to implement WPA. Enterprises will require an **authentication server** like RADIUS, but WPA accommodates home and small office/home office with a special mode of operation without them, using a shared password mechanism to activate WPA protection.

WPA provides a high level of assurance that the data will remain private and that only authorized users can access the network by addressing Wi-Fi security with a stronger encryption algorithm, as well as user authentication. A feature that was largely missing in WEP.

Using the Temporary Key Integrity Protocol (TKIP) for encryption, employing 802.1X authentication with Extensible Authentication Protocol (EAP), along with the Michael Message Integrity Check to enforce data integrity, WPA protects against the most targeted hacker attacks.

	WEP	WPA
Encryption	Flawed, cracked by scientists and hackers	Fixes all WEP flaws
	40-bit keys	128-bit keys
	Static – 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

Figure 2 – Comparing WEP and WPA features [Wifi2003]

III.2 Temporal Key Integrity Protocol (TKIP)

As we discussed earlier, WEP encryption algorithm is compromised and has many flaws that can permit an attacker to access the information compromising the WLAN. At the same time WPA is intended to be interoperable with all existing Wi-Fi devices already in the market and that were shipped in millions implementing this flawed and poorly designed IEEE native security mechanism.

TKIP is a **wrapper around WEP** that intends to enhance its security features. To comply with this constraint, TKIP uses the **same stream cipher** used by WEP: RC4. This way only a software upgrade is needed to implement TKIP. “In general, most security experts believe that TKIP is a stronger encryption than WEP. However, they also agree that TKIP should be an interim solution because of its use of RC4 algorithm.” [Wong2003]

The primary advantage of TKIP over WEP is the **key rotation**. TKIP changes the keys used for RC4 often (every 10,000 packets), and the way Initialization Vectors (IVs) are created is different.

In fact, TKIP is composed of **four algorithms** wrapping WEP to achieve the best security possible given the problem design constraints, these are:

- Cryptographic Message Integrity Code (MIC)
- New IV sequencing discipline
- Per packet key mixing function
- Re-keying mechanism

Message Integrity Code (MIC)

Intended to detect forgeries, it has three components. A **secret 64-bit authentication key** K, shared only between the sender and the receiver. A **tagging function** takes the key K and a message M as an input and creates a **message integrity code** T as an output. This tag T is sent along with the message M. To detect a forgery, the receiver inputs K, T and M into the **verification predicate** and creates his own tag code T' with M and K. If both tag codes match the message is presumed authentic.

IV sequencing discipline

In WEP an attacker could create forgeries by recording valid WEP packets and the re-transmitting them later (replay attack). To defeat this, TKIP employs **packet sequencing numbers** and synchronization between sender and receiver. Proper IV sequencing of arriving packets determines if there has been a replay and if so, discard the packet. Both sender and receiver reset their counters whenever new keys are set.

Per-Packet Key Mixing Function

Keys in TKIP have a **fixed lifetime** and are replaced frequently. The mixing function in WEP operates in **two phases** and “substitutes a temporal key for the WEP base key and constructs the WEP per-packet key”[Walker 2002]. Each phase compensates for a particular design flaw in WEP.

In phase one, an **intermediate key** is created combining the use of S-boxes and the client's MAC address. This eliminates the same key from use by all links, like in WEP. In phase two, the **packet sequence number is encrypted** with a small cipher using the intermediate key. This way it de-correlates the public IV from known per-packet key.

Re-keying Mechanism

TKIP re-key architecture is hierarchical, with **three key types**: temporal keys, key encryption keys, and master keys.

We discussed earlier the problem of re-using IVs in WEP. To solve this problem, and in conjunction with the key-mixing mechanism, TKIP uses a key update mechanism using special re-key messages that distribute keying material deriving the next set of **temporal keys** between the station and the access point. There are two kinds of temporal keys, 128-bit keys are used for encryption and 64-bit keys for data integrity.

The re-key messages are secured with the **key encryption keys**, that protect temporal keys. The station and Access Point have to communicate and establish a fresh set of keys on association or re-association.

To accomplish all these transactions, TKIP uses 802.1X authentication servers to push a common set of key encryption keys to the station and AP. The **master key** is used to secure their distribution, and it's closely tied to the authentication process and the authentication server. A new and un-related master key is used for each session.

TKIP Design

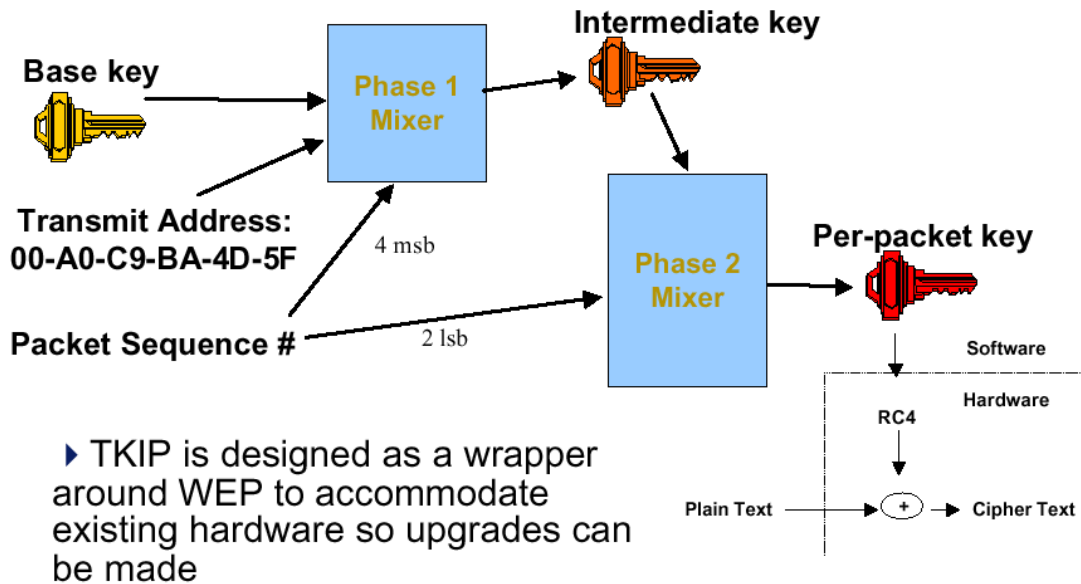


Figure 3 – TKIP design [Mill2002]

III.3 Authentication with 802.1X and EAP

WPA uses port-based network access control, 802.1X with the Extensible Authentication Protocol (EAP) to provide authentication and access control to the WLAN. Adopted by IEEE in August 2001 as a standard, 802.1X makes use of an **authentication server** to grant or deny access to the network. IEEE specifies in his standard that a **Remote Dial-In User Authentication Server** (RADIUS) should be used for this purpose.

There are several components that take part in the authentication process:

- Supplicant:** Is the client/devices requesting WLAN services
- Authenticator:** Is the network Access Point that has 802.1X enabled
- Authentication Server:** Is the server that carries out the authentication process.
- EAP:** Is the protocol employed between the station and the authenticator
- Port Access Entry (PAE):** Is the 802.1X ‘logical’ component of the client and authenticator that exchange EAP messages.

Before any traffic is allowed to travel the network, a successful authentication process shall be completed. In a WLAN environment, the clients are not physically connected to the network. An association with the Access Point (AP) needs to be formed. When this occurs, the AP learns the client's MAC address creating a '**logical port**', PAE.

Once the association has been established, the 'logical port' has to be authorized. To do so the PAE, is set to '**uncontrolled mode**', meaning that at this point, the client can only send EAP requests to the authenticator. This **EAP messages** present the client credentials, identifying his self in one of many different forms. It can be through certificates, user name/password, smart cards, etc.

Upon receipt of the EAP messages, the authenticator will forward the request to the authentication server, which in turn, will authenticate the identity of the supplicant, granting or denying access to the network. If the supplicant has been successfully authenticated, an **ACCEPT message** is sent to the authenticator. The 'logical ports' of supplicant and authenticator are then set to '**controlled mode**', and the master TKIP key is sent to both the client and the Access Point. "802.1X and EAP also ensure that new encryption keys are generated and distributed frequently. This frequent distribution is known as "dynamic key" distribution, an essential element in a good security solution." [Wifi2003]

802.1X is only a **perimeter security technology**, that means that once a supplicant is successfully authenticated, the system will not control his network traffic.

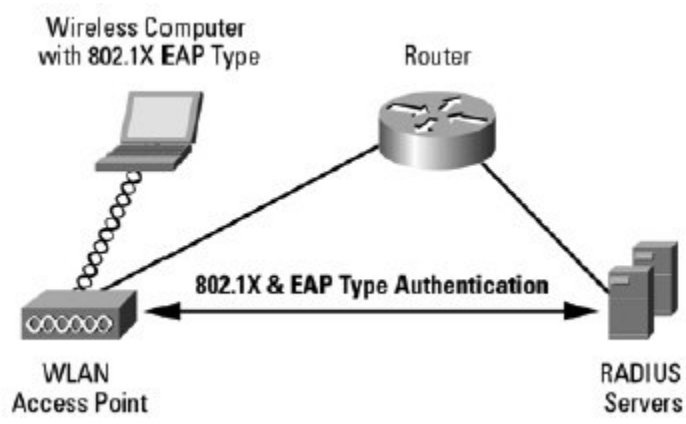


Figure 4 – Authentication with 802.1X and EAP [Wifi2003]

For the small home/home office environment (SOHO) in which an authentication server is not present, the authentication methods include 802.1X and **Pre-shared Key (PSK)**. Pre-shared key uses a statically configured pass phrase on both the stations and the access point. “The difference is that here, a password is manually entered on client devices and on the AP or wireless gateway and used for authentication.” [Wifi2003].

IV. Conclusions

The growth in use and popularity of WLAN is already a fact. Thanks to their flexibility and ease of use, today millions of people worldwide enjoy of its convenience. However, as plenty of data flows through the air in the form of radio waves, confidentiality and integrity of such data may be compromised.

Due to a weak design and probably poor/incomplete peer reviews, the original native security method for wireless networks, **WEP**, introduced several vulnerabilities that could compromise the information being transmitted.

In the last few years companies had to adopt custom solutions to enhance the security of such networks. Add-on proprietary technologies such as VPN were used to increase protection.

The Wi-Fi Alliance along with the IEEE, concerned that a weak security system could slow down the rapid adoption of Wi-Fi in the market, worked in a new standard specification to secure WLAN. However millions of devices had already been shipped and were in use implementing the flawed technology. This issue defined a design constraint for the new specification to come.

In October 2001, **Wi-Fi Protected Access (WPA)** was born with the idea of being an interoperable standard based security specification, enabling existing devices to be 'patched' through software upgrades to implement the new features.

As we have seen, one of WEP's greater weaknesses was the lack of strong authentication. With the use of **802.1X authentication using the EAP protocol**, WPA provides an effective method to grant/deny a client with authorization to the network. Whether in a big company, using authentication servers as **RADIUS**, or in a small office/home office user, using **Pre Shared Key** methods, a client can be proven to be legitimated to access the resources provided by the WLAN.

In this paper we have also presented how WPA addresses the vulnerabilities of the encryption algorithm used in WEP by wrapping it up with **TKIP**. We have discussed the four new algorithms that are implemented to enhance encryption efficiency and make it more difficult to break. However, and because the design constraints that required WPA to be interoperable with the existing Wi-Fi devices, TKIP is, as WEP, **RC4** based. Therefore having also the same weaknesses.

IEEE forthcoming standard **802.11i**, that will be approved tentatively by the end of 2003, will be using many of the features provided by WPA. It will provide the same authentication approaches, 802.1X with EAP, but will upgrade the 802.11 encryption algorithm from TKIP/WEP to the **Advanced Encryption Standard (AES)**.

In conclusion we have seen that the implantation of a new technology in the market always raises security risks. A careful design of the security implementation is necessary in order to minimize those vulnerabilities and make the technology safe and secure to use.

V. References and Citations

- [Wifi2003] → **Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks**, Wi-Fi Alliance, 2003 www.weca.net
- [Wong2003] → **The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards** Stanley Wong GSEC Practical v1.4b, 2003
- [Walk2002] → **-802.11 Security Series Part II: The Temporal Key Integrity Protocol (TKIP)**, Jesse Walker, Intel Corporation, 2002
- [Park2002] → **- Enhanced Wired Equivalent Privacy for IEEE 802.11 Wireless LANs**, Taejoon Park, Haining Wang, Min-gyu Cho, and Kang G. Shin, Real-Time Computing Laboratory, The University of Michigan, 2002
- [LaRos2003] → **- WPA: A Key Step Forward in Enterpriser-class Wireless LAN (WLAN) Security**, Jon A. LaRosa, MeetingHouse data communications, 2003

VI. Bibliography

- 802.11 Security Series Part II: The Temporal Key Integrity Protocol (TKIP)**, Jesse Walker, Intel Corporation, 2002
- Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks**, Wi-Fi Alliance, 2003 www.weca.net
- The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards**, Stanley Wong GSEC Practical v1.4b, 2003
- **Enhanced Wired Equivalent Privacy for IEEE 802.11 Wireless LANs**, Taejoon Park, Haining Wang, Min-gyu Cho, and Kang G. Shin, Real-Time Computing Laboratory, The University of Michigan, 2002

-- **WPA: A Key Step Forward in Enterpriser-class Wireless LAN (WLAN) Security**,
Jon A. LaRosa, MeetingHouse data communications, 2003

-**Using IEEE 802.1x to Enhance Network Security**, Anthon James, 2002, Foundry
Networks

-**Introduction to 802.1X for Wireless Local Area Networks**, 2002, Interlink Networks
www.interlinknetworks.com

-**Issues in Wireless Security (WEP, WPA & 802.11i)** Presented to the 18 th Annual
Computer Security Applications Conference 11 December 2002 Brian R. Miller, Booz
Allen Hamilton