*International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*
*Volume 3 Issue 8, August 2014*

# Comparative Study of Attacks on Security Protocols

**Prof. Lakshmi Kurup** **Ms. Vidhi Shah** **Mr. Dhaval Shah**

Department of Computer Engineering,
University of Mumbai, India

*Abstract* - **During the last decade, wireless networks have become increasingly popular. Wireless networks are cheap and the main advantage is mobility and lack of cables. However, they are prone to a variety of threats like denial of service, chop-chop attack, replay attacks, man-in-the-middle and data modification. With growing popularity the threats to wireless networks have also increased significantly in the last few years. WLAN security has evolved in the last decade and this evolution occurred in three main phases. This paper gives a general idea of these three security schemes designed to protect wireless networks from such threats. We then present the vulnerabilities of each of these three schemes. We have studied the threats and attacks against each of these mechanisms in great detail. Along with their detailed description, we have also provided possible solutions and preventive measures. Using these preventive measures it is possible to get the best security out of these mechanisms.**

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

## I. Introduction

Wireless networks are rapidly gaining popularity in today's world because of their excellent usability. Two of the major advantages of wireless networks are: wireless networks are highly portable and no cables are required. Yet, relying on the radio waves to transmit critical data, such as credit card numbers, raises questions about the security aspect of wireless networks. How can users be guaranteed their data is safe and secure while being broadcast over the air?
As attacks on wireless LANs have become more widespread, security has evolved significantly from what was offered in the original IEEE 802.11 protocol to the IEEE 802.11i protocol which is being widely used today. The transformation occurred in three main phases: WEP, atransitionalphase with Wi-Fi Protected Access (WPA) and the third phase i.e. the WPA2 protocol.

The paper provides a brief introduction about each of these schemes along with their vulnerabilities. We then discuss various attacks possible on these security schemes in great detail.

## II. Wireless Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) was one of the first security mechanisms for Wireless LAN. It was introduced in September 1999 as part of IEEE 802.11 security standard.

The main aim was to provide security that is equivalent to that of wired networks. Two agents or parties participate in this mechanism: the initiator (any network client) and the responder (an access point). Authentication verifies the origin

of the messages received over wireless links. It is the process of determining whether the user is actually the same as he claims to be or not, before he can get access to the network resources. It is like confirming whether the person has the ticket before he is allowed to enter into the cinema hall. Two types of authentication are available with WEP: the open system and the shared key system. The open system always authenticates the client and permits all clients to enter the network. Hence, it provides no authentication security. The shared key process requires the initiator to know some shared secret or the shared key. The authentication process confirms that the initiator knows this secret. This secret is known as WEP encryption key.
WEP uses the RC4 symmetric stream cipher algorithm to perform encryption. The initial length of the WEP key was 40 bits, due to US Government restrictions on the export of cryptographic technology at the time the protocol was drafted [5]. This key length was too short and as a result, brute force attacks could be performed easily. However, all major manufacturers eventually implemented an extended 128-bit WEP protocol with the 104-bit key size.

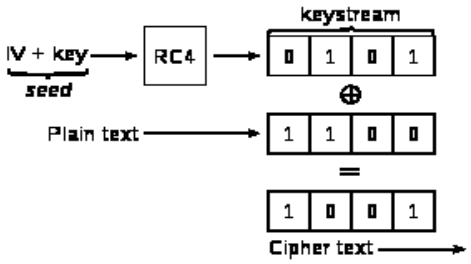


Figure 1: WEP Encryption Process

We'll be explaining different attacks possible on WEP in great detail in the next section.

### A. WEP Vulnerabilities

Critical security loopholes were detected in WEP. 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]. Various tools and software are available which enable data decryption within few minutes. WEP lacks key management and as a result, same keys are used for longer duration and tend to be of poor quality. Also, the standard specified for WEP provides support for 40 bit key only, thus it is prone to brute force attacks.
WEP also does not provide protection against replay attacks. An attacker can record and replay packets and they will be accepted as genuine. There are also few authentication issues in WEP. The AP confirms the identity of the mobile client. However, the mobile client has no way of confirming 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 [3]. In packet forgery the WEP does not provide any protection measures against packet forgery and in flooding an attacker can send large number of messages to access point (AP) and thus, preventing the AP from processing the traffic.

Offline dictionary attack is a type of brute force attack where frequently used words for encryption are considered and the result is compared with captured traffic to reveal the secret passphrase. Reuse initialization vector is a flaw wherein the initialization vector is reused and thus, data can easily be decrypted without the knowledge of encryption key using various cryptanalytic methods. Since the IV is only 24 bits, it only provides 2^24 combinations and offers the possibility of having duplicate IV's in a relatively short time.

### B. Attacks On WEP

**Chopchop Attack:**

The attacker can decrypt the last n bytes of plaintext of encrypted packet by sending an average of n*128 packets on the network [3]. There is always an Integrity Check Value (ICV) appended with the plain text and chopchop attack exploits the weakness of this four byte checksum. This attack does not reveal the root key. Various access points can easily differentiate between correct and incorrect checksum of encrypted packets. The attacker uses this principle for packet decryption. The attacker initially chops one byte from end of captured packet and then he will guess the packet's last byte and modify the checksum accordingly. He then sends the packet to the access point. If the guess was right, the access point will accept the packet and the attacker now knows the last byte of plaintext. So, attacker proceeds to guess the second last byte. In case, the guess of last byte was wrong then, the access point will discard the packet and attacker will make a new guess for last byte. Using this principle, there has been a tremendous reduction in amount of time required to crack WEP keys.

**Fluhrer, Mantin and Shamir (FMS) Attack:**

One of the most serious attacks on WEP was discovered by Fluhrer, Mantin and Shamir. FMS attacks are due to use of weak initialization vectors(IV's) in RC4 algorithm. The encrypted packets along with initialization vectors for these packets can be recorded by an attacker who is passively listening to the network traffic. The attacker can then easily recover the first bytes of keystream, which were used for encrypting the packet. The first bytes of plaintext can be easily predicted by the attacker. The attacker can also easily find out the initialization vector (first three bytes of per packet key), which is transmitted with the packets in an unencrypted form. Rest of bytes per packet key are unknown to attacker but they are identical for all packets [6].

**Fragmentation Attack:**

After eavesdropping one data packet, the attacker recovers eight bytes of keystream due to the fact that the initial portion of 802.11 packets is virtually constant. Then the attacker generates a 64 bytes long plain text and uses 802.11 fragmentation feature to divide it to 8 byte fragments. Because the attacker knows 8 bytes of the keystream, he can encrypt the fragments, and send them to the address of the snooped packet. These fragments go through an access point, which reassembles them into a single packet, encrypts the packet and forwards it to its destination. By eavesdropping on this, the attacker gets the encrypted version of his own plain text, and can XOR the plain and cipher text to obtain the keystream. After this, snooped data packet can be decrypted to discover the local network IP addresses.

### C. Solutions

WEP protocol was extended to counteract the uncovered flaws. The first extension, WEP2, addressed the problem of short IV by expanding the IV key space to 128 bits. As a result, the repetition of IV was decreased, making the attacks exploiting the weak keys, slow down considerably. Yet, due to the fact that the reuse of IV was still permitted, WEP could still be compromised. The second extension, WEPPlus (or WEP+) provided the methods for hardware to avoid weak IVs. This made the attacks based on use of weak IVs practically impossible, but the fragmentation attack was still possible. The other disadvantage of this security scheme was that it had to be employed at both ends of the wireless connection, which was difficult to enforce. As a result, the need for a completely new and better security scheme continued to grow.

## III. Wi-Fi protected Access (WPA)

Wi-Fi Protected Access (WPA) was introduced in 2003 by the Wi-Fi (Wireless Fidelity) alliance to overcome the flaws of WEP [3]. WPA implements majority of the IEEE 802.11i standard. WPA was created by the Wi-Fi Alliance as a temporary solution to replace WEP before 802.11i standard was ready. WPA vastly improves encrypting process of WEP and adds a concrete user authentication mechanism to it. The encryption key must be manually entered on wireless access points and devices and it does not change. TKIP employs a per-packet key which means that it dynamically generates a new 128-bit key for each packet.

WPA operates in two modes, the Preshared Key (PSK) and Enterprise. The WPA-PSK offers a lesser security than the Enterprise version, as it requires a shared secret but it is easier to install.

WPA also includes a message integrity check which is designed to prevent an attacker from capturing, altering and/or re-sending data packets. This replaces the cyclic redundancy check (CRC) algorithm used by earlier standards of WEP.

TKIP enhances the integrity of the packets by adding a Message Integrity Check (MIC) field. The MIC algorithm is used to check for forgeries and to ensure data integrity. The MIC value is computed with a cryptographic algorithm called Michael. Michael uses a 64-bit key and divides the packets into 32-bit blocks. It then uses shift, exclusive Ors, and additions for the processing of each 32-bit block into two 32-bit registers. As an additional feature, Michael detects any attempt to break TKIP and thus blocks communication with the attacker.

### A. WPA Vulnerabilities

WPA uses the old cryptography algorithm RC4 in place of the superior Advanced Encryption Standard (AES).

WPA is vulnerable to brute force attacks if there is a weak passphrase for pre shared key mode.

Due to use of hash functions for TKIP key mixing it is prone to threats during Hash collisions. WPA is also vulnerable to availability attacks like the Denial of Service.

A very complex setup is required for WPA-enterprise.

  

### B. Attacks On WPA

**WPA-PSK Attack:**

The Authentication mechanisms of WPA-PSK is prone to offline dictionary attack because the information has to be broadcasted verified for the session key [2]. Therefore to generate the PMK, the passphrase, the Service Set Identifier (SSID) and SSID length have to be fed into the hashing algorithm. The SSID can be easily recovered so in order to identify PMK only the passphrase needs to be guessed. The security per character in passphrase is approximately 2.5 bits. Therefore, n bytes passphrase gives a key with 2.5n+12 bits of security strength. Thus it is vulnerable to dictionary attack in case of short passphrase which is less than 20 characters. The he can gain access to the network if PMK is determined by attacker. The tools which can be used for attack are Aircrack and coWPAtty.

**Beck-Tews Attack:**

This attack is an extension of the chopchop attack on WEP. TKIP implements MIC, and so if two MIC failures are observed within 60 seconds then both client and access point are shut down and then the TKIP session key is rekeyed. Thus the attacker waits for 60 seconds to avoid countermeasures in case of a failure. Packet can be decoded at a rate of one byte per minute with the help of this attack. After the plaintext has been retrieved by attacker, he has access to MIC and keystream of packet. This can be used to construct and transmit a new packet on network which enables the attacker to execute Denial of service and ARP poisoning attacks. This attack can be executed only against TKIP and not against WPA implementing AES.

**Ohigashi-Morii Attack:**

This attack uses a mechanism which is similar to Beck-Tews attack. It also executes a man in the middle attack. This is efficient for all WPA modes and does not require Quality of Service to be enabled on access point unlike the Beck-Tews Attack. The time to inject a fake packet is reduced to approximately 15 minutes to 1 minute at the best. For this attack, the MITM is superposed on the Beck-Tews attack, with tips to reduce the execution time of the attack.

## IV. Wi-Fi Protected Access 2 (WPA2)

WPA2 was introduced in September 2004 by Wi-Fi alliance. WPA2 completely implements IEEE 802.11i standard and is an improvement over WPA. In addition to TKIP, MIC and Michael algorithm, it introduces CCMP(Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). CCMP is a new encryption mode based on Advanced Encryption Standard(AES) with strong security. WPA2 has replaced WPA.

There are two purposes of CCMP:

1. The Counter mode is used for providing data protection from unauthorized access.
2. The CBC-MAC is used to provide the message integrity to the network.

The IEEE 802.11i improved the three basic areas in order to provide the security to IEEE 802.11b for which WEP is unable to provide the security.

WPA2 uses AES-CMP for encryption. CCM is used to calculate the MIC value as to provide integrity and authentication. The 802.1x key generation protocols are used to help generate matching Pairwise Master Keys (PMK). To add randomness, and associate the keys to the pairs of devices that created them, random nonce and both the device MAC addresses are added to the key. Finally, the access point also has to prove its identity with the authentication server.

### A. WPA2 Vulnerabilities

WPA2 has limited drawbacks available in comparison to initial security solution WEP and substitute security solution WPA. WPA 2 technique is very much costly for the already deployed networks due to the new encryption CCMP and AES needs to change the overall hardware for the network. WPA 2 requires more hardware due to the two-way authentication between user and AP. It is prone to availability attacks like Jamming and Flooding since it cannot prevent physical layer attack. Also, the Group Temporal Key(GTK) is shared amongst all authorized clients of the network. A malicious authenticated client may insert spoofed GTK packets in the network. Thus, an authorized user can listen to and decrypt data of other authorized users. He may also install malware and compromise the safety of other users. This is known as Hole196 vulnerability.

### B. Attacks on WPA2

**Hole 196:**

Hole196 attack is one attack to WPA2 from its insiders. Central to this vulnerability is the group temporal key (GTK) that is shared among all authorized clients in a WPA2 network. Nothing in the standard of WPA2 stops a malicious authorized client from inserting spoofed GTK-encrypted packets! Exploiting this loophole, an insider who is an authorized user can listen to and decrypt data from other authorized users as well and scan their Wi-Fi devices for vulnerabilities. He can then install malware and possibly compromise the security of those devices. As a result of this attack, inter-user data privacy among authorized users is inherently lost over the air in a WPA2-secured network.

**Denial Of Service:**

Another attack on WPA2 is the DOS attack. In computing, a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users [3]. People with slower internet connections, such as dial-up, are affected more by these attacks.

The attacker will continuously send connection requests to the Access Point. Thus, the system gets too much internet traffic. The traffic uses bandwidth and the internet servers slow down and eventually stop.One common method of attack involves saturating the target machine with external communications requests. In such a scenario it cannot respond to legitimate traffic, or responds so slowly as to be considered essentially unavailable. Such attacks usually creates a huge overload on the server. In general terms, there are two ways to implement these attacks: one way is to force the targeted computer(s) to reset or consume its resources so that it can no longer provide its projected service and the other way is by obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

## V. Proposed Solutions

After reading in depth about these attacks on WPA2, we have come up with a possible solution to each of these attacks. To mitigate the attacks of DOS, it generally makes sense to have more bandwidth available to your web server than you ever think you are likely to need. Even if you overprovision by

  

100 or 500 percent, it likely won't stop a DDoS attack. But it might give you some time to act before your resources are overwhelmed. You can also add filters to tell your router to drop packets from obvious sources of attack. Another measure which is quite simple to adopt, is to set lower SYN, ICMP and UDP flood drop thresholds. You can even timeout half-out connections more aggressively and drop spoofed or malformed packages to partially mitigate the effects of a DDoS attack.

We further researched about another major flaw of WPA2 – Hole 196. "Hole196" is vulnerability in the WPA2 security protocol exposing WPA2-secured Wi-Fi networks to insider attacks.

Turning on Client Isolation is the most effective strategy that can be employed. Turning ON the Client isolation (or PSPF) feature on an AP or WLAN controller can prevent two Wi-Fi clients associated with an AP from communicating with each other via the AP. This means that while a malicious insider can continue to send spoofed GTK encrypted packets directly to other clients in the network, the data traffic from the victim clients will not be forwarded by the AP to the attacker's Wi-Fi device.

Note also that, as this is an attack that only a trusted insider can pull off, it might be a good idea to think about the background-checking process used to screen new hires, and to do updates on a random sampling from time to time. AP vendors can implement a patch to their AP software to assign a unique, randomly generated GTK to each client instead of sharing the same GTK among all clients. Using unique GTKs will neutralize the Hole196 vulnerability.

**References**

[1] Moffat Matthews, Evolution of WLAN Security Architecture, Canterbury University, 2009

[2] TimoHassinen, Overview of WLAN Security, Helsinki University of Technology, 2006

[3] Shilpa Gupta, Wireless Network Security Protocols-A Comparative Study, IJETAE, 2012

[4] Seth Fogie. *Cracking Wi-Fi Protected Access (WPA), Part 2*, 2005.

[5] NIST Computer Security Division. Advanced Encryption Standard, 2001.

[6] Bernard Aboba. IEEE 802.1X Pre- Authentication. Presentation to 802.11 WGi, July 2002.

[7] Tim Moore. Validating Disassociate Deauth Messages. Presentation to 802.11 WGi, September 2002.

[8] Mike Lynn and Robert Baird. Advanced 802.11 Attack. Black Hat Briefings, July 2002.

  