# CSC574 Project 1
# Wireless LAN Security
# Fall 2015

## Wired Equivalent privacy (WEP)

**Submitted By:**

**Purna Mani Kumar G - 200066404**
**&**
**Rashmi Sandilya - 200084902**

## Objective:

The goal of the project is 1) To understand and review different methods to crack the wireless security protocol (WEP), 2) To give comprehensive survey exploiting WEP security vulnerabilities, and (B) explaining how these were resolved in WPA and 3) To program a method to break WEP.

## WEP Introduction:

Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks. With the technological advancement, the need for people to share data increased. The popularity of laptops and portable computing devices has caused an increase in the range of places people perform computing. As a result wireless network have gained tremendous popularity. A wireless network broadcasts messages using radio signals. When the transmissions are broadcast over radio, it is particularly susceptible to eavesdropping and interception. WEP was designed to provide comparable confidentiality to a traditional wired network. However, WEP fell short of accomplishing the security goals and suffered from serious weaknesses as identified by cryptographers. WEP was superseded by Wi-Fi Protected Access (WPA) in 2003.

## WEP Goals

The main security goal of the WEP as per the research papers are as follows:

- **Confidentiality:** Protecting the communication between two hosts from casual eavesdropping.
- **Data Integrity**: Protect access to a wireless network infrastructure.
- **Authentication or Access Control**: Prevention against any kind of modification or tempering of the transmitted messages.

## Working of WEP

WEP uses the stream cipher RC4 with 40-bits or 104-bits shared key size for confidentiality. A 24-bits Initialization Vector (IV) is used to augment the shared key and produce a different RC4 key for each packet. The IV value is transmitted in the clear. WEP also uses the CRC-32 checksum for integrity.

### WEP Encryption

Encryption of a WEP frame is done in two stages:

**Checksum**: An integrity checksum is calculate on Message original message say **M** and concatenated with message M to get obtain Plain text Message **P**.

$$\mathbf{P = <M, c(M)>}$$

**Encryption:** RC4 algorithm is used to generate keystream which is a function of Initialization vector v and secret key k. The cipher text is obtained by XOR of plaintext message obtained in part 1 and keystream.

$$\mathbf{C = P \oplus RC4(v, k)}$$

The transmitted message from host **A** to host **B** consists of Initialization vector **v** sent in clear and the cipher text **C**.

$$\mathbf{A \text{ -> } B: \quad v, P \oplus RC4(v, k)}$$

## WEP Decryption:

WEP decryption follows the reverse algorithm of encryption process. The receiving hosts first generates the pseudorandom keystream using the Initialization vector v (received as part of received message) and shared key (with previous knowledge). The Plaintext P is then obtained by XOR of the received cipher text and the generated keystream as follows:

$$\begin{aligned} \mathbf{P'} &\mathbf{= C \oplus RC4(v, k)} \\ &\mathbf{= P \oplus RC4(v, k) \oplus RC4(v, k)} \\ &\mathbf{= P} \end{aligned}$$

## WEP flaws:

WEP flaws are due to the certain weakness in the features used in the algorithm. All the WEP attacks uses wither of these flaws to mount the attack. The attacks of WEP can be broadly classified in two types:

1. Attacks based on exploiting the weakness of RC4 mainly keystream reuse
2. Attacks based on checksum and authentication weaknesses

## WEP Attacks

## 1. Attacks based on exploiting the weakness of RC4 mainly keystream reuse

### Keystream Reuse Attack:

WEP provides data confidentiality using a stream cipher called RC4. A well-known pitfall of stream ciphers is encrypting two messages under same Initialization vector and key can reveal information about both the messages as:

$$\mathbf{C1 = P1 \oplus RC4(v, k)}$$

$$\mathbf{C2 = P2 \oplus RC4(v, k)}$$

$$\mathbf{C1 \oplus C2 = P1 \oplus RC4(v, k) \oplus P2 \oplus RC4(v, k)}$$

$$\mathbf{= P1 \oplus P2}$$

There are various ways to get the individual message from the XOR of plaintexts. As per the research paper one such method can be having the knowledge of one of the plaintext message can be used to derive the other message. Second method can be the use of predictable field of IP header. Since protocols use well defined structures in messages, contents of messages are predictable. Another method can be to send known plaintext IP traffic to a mobile host from an internet's host under attacker's control. Yet another method can be to an educated guess about the structure of plaintext.

**Dictionary attack or table based attack**

This type of attack uses the keystream reuse for the initial phase. Once the plain text is obtained either through the colliding IV's or any means, attacker also learns the keystream used to encrypt the message. Over time, the attacker can build up a table of IVs and corresponding key streams. The amount of work required to build such a table is tremendous but once such a table is built, it becomes easy to decrypt the subsequent cipher text with very little effort.

**Partial key exposure attack of Fluhrer, Mantin and Shamir**

FMS attack is a popular attacks which was developed by Fluhrer, Mantin, and Shamir. In this attack an adversary is able to recover a full key by passively collecting particular frames from a wireless LAN. This attack takes advantage of the weakness in the RC4 Key Scheduling Algorithm (KSA) to reconstruct the key from encrypted messages. This attack is based on the fact that since first bytes of the plaintext of most packets are easily predictable, the attacker is able to recover the first bytes of the keystreams used to encrypt these packets.

To mount the attack, we search for IVs that place the key setup algorithm into a state which leaks information about the key. Using the terminology of Fluhrer et al., we refer to these key leaking cases as resolved.

Each resolved packet leaks information about only one key byte, and we must correctly guess each key byte before any packet gives us information about a later key byte.With WEP, when we are in a resolved state, the value of the next key byte is(with high probability) given by the equation:

$$\mathbf{K[B] = S^{-1}_{B+2}[Out] - j_{B+2} - S_{B+2}[B + 3]}$$

Where **B** is the byte current being guessed, **Out** is the first output from the pseudo random number generator, and $\mathbf{S^{-1}}$ is the position in **S** where its argument occurs.

To obtain values of S and S $^{-1}$, the attacker must simulate the key setup algorithm. He is able to do this perfectly for the first B iterations, as he already knows the key bytes used.

**KoreK Attack**

This attack can be split into three different groups. The first group just uses K[0] to K[l − 1] and the first word of output of the RC4PRGA denoted by Z[0] to determine the first key byte K[l]. The original FMS attack is one of the attacks in this group. The second group additionally uses Z[1] and the third group is called inverse attacks. Instead of trying to determine the next key byte, these attacks can help to exclude certain values from being K[l].

## 2. Attacks based on checksum and authentication weaknesses

**Message modification:**

This type of attack uses linear property of WEP checksum. The cipher text is modified without disrupting the checksum and original transmission is replaced with the modified cipher text. This attack is an active attack. This type of attack fails WEP to achieve its security goal of data integrity.

**Message Injection:**

This type of attack violates the WEP security goal of access control and is active attack in nature. This attack is based on the property the WEP checksum is an unkeyed function of the message. If an attacker gets hold of entire plain text corresponding to a transmitted frame, he will be able to inject arbitrary traffic into the network.

**Authentication Spoofing:**

In this type of attack, an attacker intercepts a single authentication sequence. An attacker learns both the plain text challenge send by access point and encrypted version sent from host and derives the keystream. After intercepting a single authentication, attacker can authenticate himself with that key infinitely**.**

**IP redirection Attack:**

This can be used when the WEP access point acts as an IP router with Internet connectivity. In this case. The idea is to sniff an encrypted packet off the air, and use the message modification technique described above to modify it so that it has a new destination address controlled by the attacker. The access point will then decrypt the packet, and send the packet off to its (new) destination, where the attacker can read the packet, now in the clear.

**Reaction attack:**

This attack can be mounted only against TCP traffic. The attack relies on the fact that TCP packet is accepted only when the checksum is correct and acknowledgment packet is sent in response. The cipher text is intercepted with unknown decryption. In the cipher text few bits are flipped and adjust the encrypted CRC with the valid WEP checksum. The response from receiver is tracked by the attacker and tells whether the modified text passed the TCP checksum and accepted by the receiver.

## Ways to counter WEP attacks:

The counter measures to WEP attack can be bigger size of Initialization Vector (IV), use of Hash functions for message Integrity, frequent change of secret key, use of hashed value of IV for transmission rather than sending in clear and better key management.

## Improved protocol standard for Wireless Security

### WPA (Wireless Protected Access)

WPA is based on the 802.11i wireless security standard, which was finalized in 2003. This protocol was released primarily to counter the vulnerabilities of WEP standard. The most distinguishing feature of the WPA are WPA- PSK (Pre shared key) which is 256 bit shared key as opposed to 64 bit key or 128 key in WEP. The longer keys ensures more security.

To improve data encryption, Wi-Fi Protected Access utilizes the Temporal Key Integrity Protocol (TKIP). TKIP provides important data encryption enhancements including

- A per-packet key mixing function
- A message integrity check (MIC) named Michael
- Extended initialization vector (IV) with sequencing rules
- Re-keying mechanism.

Through these enhancements, TKIP addresses all WEP's known vulnerabilities.

### Why WPA provided better immunity against attacks?

WPA is more immune to active attacks, i.e., capturing or altering packets passed between the access point and client. Another major improvement is TKIP (Temporal Key Integrity Protocol) which employs a per packet key system that is security wise superior to WEP. But as TKIP was designed with backward compatibility in mind, it is susceptible to certain attacks. Also, attackers took advantage of a weaknesses in the supplementary system that was rolled out with WPA, WiFi Protected Setup (WPS) which was designed to make it easy to link devices to modern access points.

### WPA2 vs WPA

WPA2 came with the mandatory use of AES algorithm and the introduction of CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code protocol). CCMP is the standard encryption protocol and is much more secure than WEP protocol and TKIP protocol of WPA.

## Conclusion

The report talks about the weakness of WEP that leads to several types of attacks. The different type of WEP attacks are described and visited in length. The report also talks about some of the counter measures to minimize the WEP attack and finally an overview of improved wireless security standard like WPA is given. The report also gives the key benefits of WPA over WEP and how WPA features circumvents the attacks possible in WEP standard. It is established that WEP is no longer secure and reliable and should not be used, rather one should consider moving to better protocols like WPA2.

## References

1. Adam Stubblefield, John Ioannidis, Aviel D. Rubin, " A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP) ". TISSEC Vol. 7, No.2, May 2004, pp 319-332.
2. Scott R. Fluhrer, Itsik Mantin, Adi Shamir, " Weaknesses in the Key Scheduling Algorithm of RC4". Selected Areas in Cryptography 2001: pp1–24.
3. Nikita Borisov, Ian Goldberg, David Wagner, " Intercepting mobile communications: the insecurity of 802.11 ". MOBICOM 2001, pp180–189.
4. Martin Beck, TU-Dresden, Germany, Erik Tews, TU-Darmstadt, Germany “Practical attacks against WEP and WPA”
5. Matthieu Caneill, Jean – Loup Gills “Attack against the Wifi protocols WEP and WPA”
6. Web Resources- Security Flaws in WEP: http://users.ece.cmu.edu/~adrian/630-f04/readings/wagner-walker-80211.pdf
7. WEP Protocol Weaknesses and Vulnerabilities – UCSB – University of California, Santa Barbara