

# Network Security

Sumeet Priyadarshee Dash

September 11, 2009

## Wired Equivalency Protocol (WEP)

WEP is a protocol to secure 802.11 based wireless networks.

The security goals of WEP are as follows.

1. Data Privacy
2. Data Integrity
3. Access Control

## Encryption Mechanism

WEP employs an encryption mechanism based on a 104 - bit key and a 24 - bit initialization vector (IV).

K : 104 bits

IV : 24 bits

---

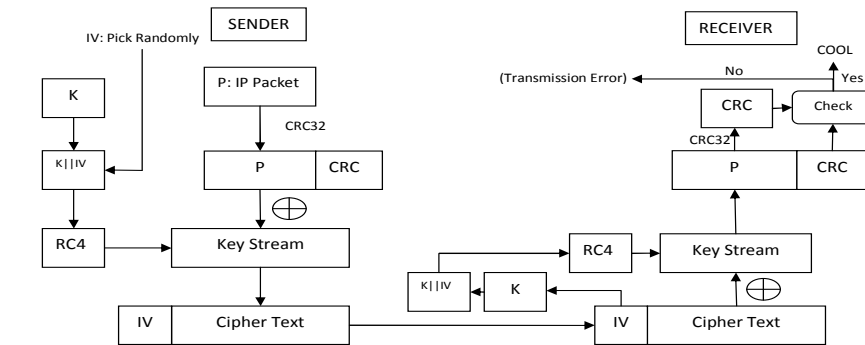
128 bits

## Salient Features

1. A key of length 104 bits is shared between the sender and receiver.
2. In order to avoid having the same encryption for two identical packets using the same key, an IV of 24 bits is appended to the key to form a new 128 bit key.
3. An IV is generated for each packet using a random number generator. The packet gets encrypted with the newly formed 128 bit key (Original key + IV).
4. The 128 bit key is then fed to a pseudo random number generator module (RC4) to generate a key stream to encrypt the entire packet.

5. The IV is transmitted along with the packet. The receiver upon receiving the packet separates the IV and appends it to its secret key to form the 128 bit encryption key.
6. An CRC is normally computed over the packet before encryption to detect transmission errors.

## Pictorial Depiction



## IV Choice and Reuse

An IV is a 24-bit number; which means that it can assume  $2^{24}$  different values. The idea is to have the IV as random as possible while selecting one. Probability of a single value appearing off the set =  $2^{-24}$ .

Expected number of collisions per  $l$  packets =  $\binom{l}{2} 2^{-24} \approx \frac{l^2}{2^{25}}$

Considering  $l$  to be around  $2^{20}$ ; expected number of collisions per  $2^{20}$  packets =  $2^{15} = 32,768$  (approx.)

Say the value of IV gets repeated for two packet  $P_1$  and  $P_2$ .  
Now,

$$\begin{aligned} C_1 &= (P_1 || CRC_1) \oplus KS \\ C_2 &= (P_2 || CRC_2) \oplus KS \end{aligned}$$

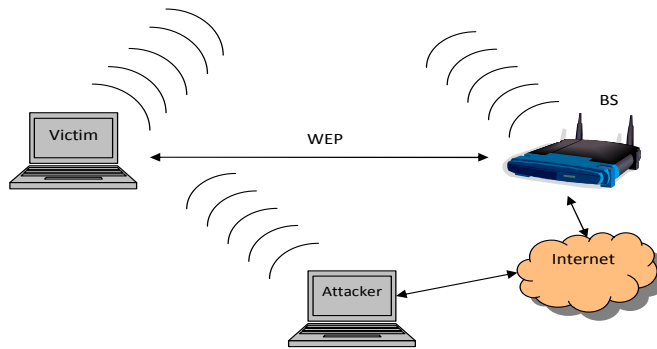
---


$$C_1 \oplus C_2 = P_1 \oplus P_2 || CRC_1 \oplus CRC_2$$

Both the keystreams cancel out each other. Nothing much is revealed about the key.

## Vulnerabilities

A WEP system has a number of inherent flaws. The encryption is easily broken using what is called a Chosen Plaintext attack. One such scheme is described below.



1. The attacker sends a packet, (say  $P_1$ ), to the victim's wireless network. The BS encrypts the packet as  $IV || P_1 \oplus KS_1$ .
2. The attacker keeps on sending the same packet to the victim's network until the value of IV gets repeated. If he notices the same ciphertext as obtained earlier ( $P_1 \oplus KS_1$ ), then he confirms that the cipher text is the right encryption for his test packet. The math then is simple. Let's consider a case where  $IV = 0$ .

$$\begin{aligned}
 DataTransmitted &= IV || P_1 \oplus KS_0 [IV = 0] \\
 &\Rightarrow C_1 = P_1 \oplus KS_0 \\
 &\Rightarrow KS_0 = C_1 \oplus P_1
 \end{aligned}$$

3. After a series of iterations the attacker would be able to establish the following table.

IV	KS
0	$KS_0$
1	$KS_3$
2	$KS_2$
...	
...	

4. The security is now compromised. The attacker has a table which contains the keystream for every possible value of IV. Using this table he can decrypt any future communication. In consequence WEP is totally broken. Due to its flaws the protocol has been deprecated and no longer is use.