

# NETWORK SECURITY

SEPTEMBER 11, 2009

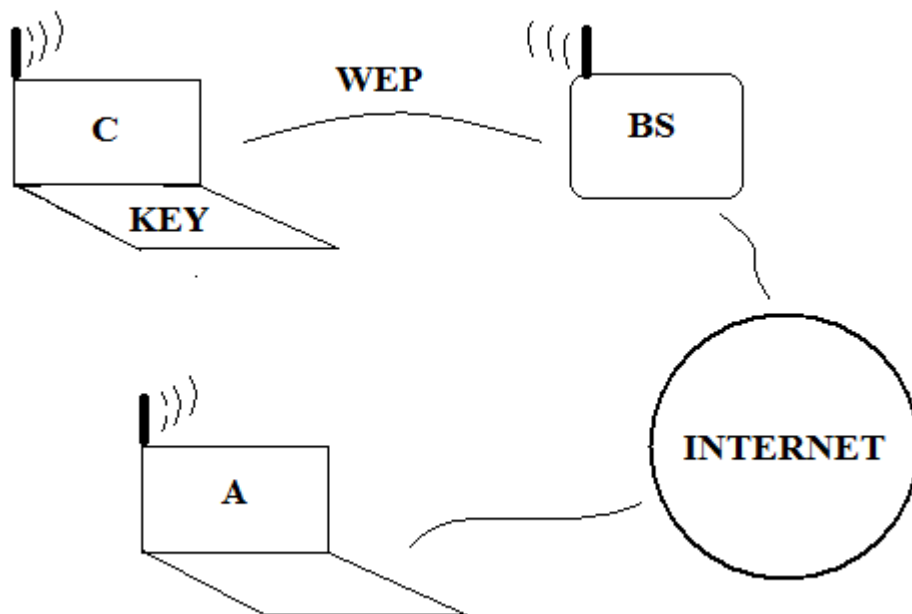
## WEP: WIRELESS EQUIVALENT PRIVACY

This is the IEEE 802.11 standard for wireless networks. It is designed to provide security and confidentiality to the wireless networks which are more susceptible to eavesdropping.

## SECURITY GOALS OF WEP

- Secrecy
- Integrity
- Access Control

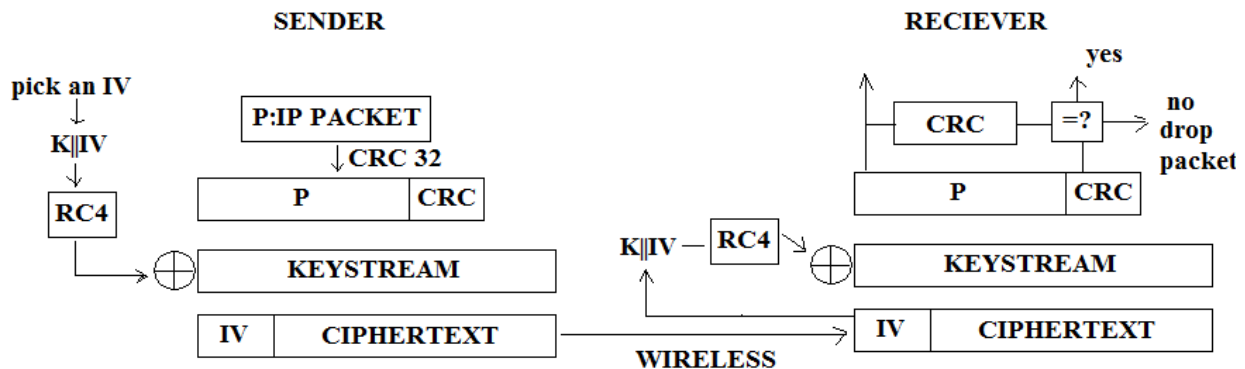
Consider the following scenario:



Here while the Client C is normally communicating with the base station BS over the Internet using WEP, there might be an attacker A somewhere intending to interpret the network packets being exchanged in the communication. To secure such a communication WEP makes use of encryption of data using a key and an integrity check to ensure that the packets are not modified in transit.

The key to be used for encryption and decryption is usually 128-bits long. Out of the 128-bits, 24-bits constitute the Initialization vector. Initialization vector changes per packet, thus, ensuring that the key stream is different per packet. Thus, the intention is to make sure that if we send the same message twice, the attacker will not be able to determine the same.

WEP makes use of RC4 encryption algorithm which is the most widely used stream cipher. The process takes place as follows:



To ensure the integrity, a CRC checksum is appended to the IP packet. The sender XORs the keystream with the plaintext to produce the ciphertext and also attaches the IV along with it. The receiver, who has the copy of the same key, retrieves the IV and produces the key stream which is then XORed with the ciphertext to produce the plaintext. The receiver can calculate the CRC checksum for the received plaintext and compare it with the appended one to ensure the integrity of the message.

### METHODS FOR CHOOSING IP

1. Pick IV randomly:

After L packets, there will be  $2^{-24}$  chances of collision for every pair.

$$\text{Expected \# of collisions: } \binom{L}{2} 2^{-24} = \frac{L^2}{2^{24}}$$

Therefore,  $L \approx 2^{12.5}$

$$L \approx 6000$$

2. Choose serially:

IV = 0, 1, 2, ...

This approach can send  $2^{24}$  packets before repetition. But it takes only a few days on a busy network.

Problem: What will happen if the system resets?

It resets the IV every time which in turn results in the repetition of first few IVs in the series.

**IV REUSE**

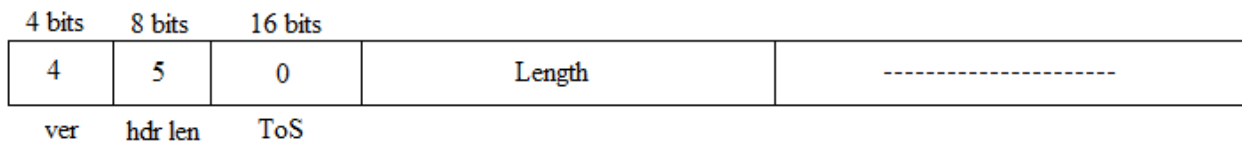
By XORing two packets that use the same IV, the attacker can obtain the XOR of the two plaintext messages.

This is shown by the following equation:

$$\begin{array}{r}
 P_1 \parallel CRC_1 \oplus KS \\
 \oplus P_2 \parallel CRC_2 \oplus KS \\
 \hline
 P_1 \oplus P_2 \parallel CRC_1 \oplus CRC_2
 \end{array}$$

The attacker can keep sending packets to the base station and thus create a table of IV and the corresponding key streams KS. With the help of this table, he can determine the IVs and the key streams of the other packets being transmitted on the network. Thus, the attacker can totally break the secrecy, access control and integrity of the message.

The structure of an IP packet is:



Thus the first 4 bytes of the key stream are already known to the attacker.

**Fact:**  $CRC(X \oplus Y) = CRC(X) \oplus CRC(Y)$

Using the above fact, an attacker can modify the original message by flipping some bits. The attacker can XOR the encrypted message with a stream of zeroes containing 1 in the position where the bit has to be flipped. The encrypted CRC can be successfully adjusted to produce the correct version of the encrypted message. This packet when sent to the base station will now be accepted as a valid packet!

