

# CSE 508 – Network Security

Date : 09/11/2009

Topics: WEP, Chosen Plaintext Attack

## 1. WEP (Wired Equivalency Privacy)

WEP is an encryption algorithm used in IEEE 802.11 standard

### 1.1. Security Goals of WEP

- Secrecy
- Integrity
- Access control

## 2. Wireless setup

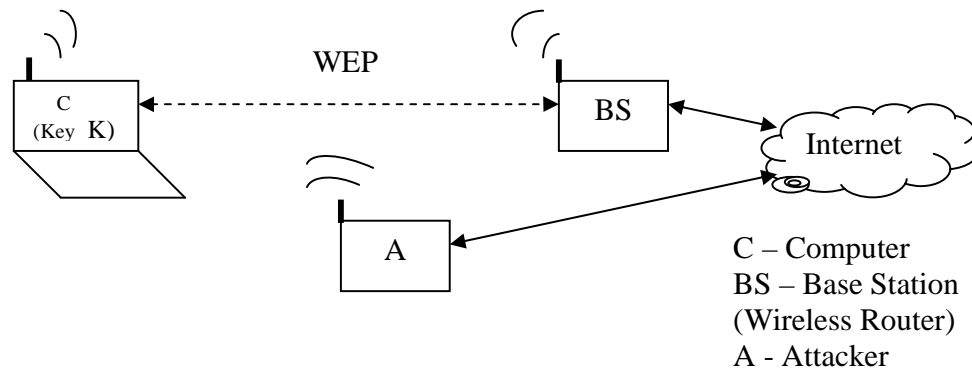


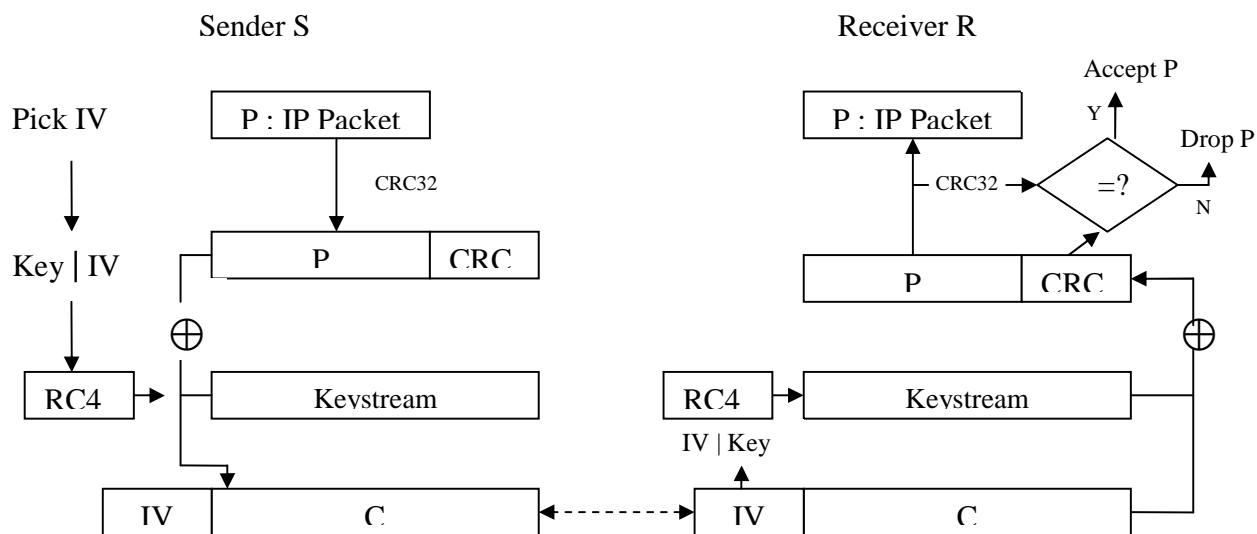
Fig 1: WEP Block Diagram

- WEP operates between C and BS
- Key K is shared between C and BS
- The attacker A is connected to Internet
- The attacker is able to capture the packets transferred in the wireless link between the BS and Client C

## 3. WEP Procedure

Figure 2 explains the WEP Procedure

- C and BS can act as Sender S as well as Receiver R
- RC4 is the Expansion Function
- Key K is of 104 bits shared between S and R
- Initialization Vector IV is of 24 bits generated for each packet and appended to the packet itself as a plaintext (meaning it is not secret)



**Fig 2. WEP Procedure**

#### **4. Choice of IV**

One of the obvious ways to choose IV is to pick it randomly. In that case,

$$\text{After } l \text{ packets, expected number of collisions} = \binom{l}{2} 2^{-24} \approx l^2 / 2^{25}$$

So when  $l \approx 2^{12.5} \approx 6000$ , there would be a collision. If  $l$  is  $2^{20}$  there will be  $2^{15}$  collisions, which is huge.

If IV is generated in sequence (say  $IV = 0, 1, 2, \dots$ ) then it takes  $2^{24}$  packets before repetition and it's very likely to occur in a few days on a busy network. Further in many systems IV starts back from 0 when the system reset. In that case the collision is expected to occur sooner.

##### **4.1. Issues with IV reuse**

Let's assume the same Keystream  $KS$  is used in two packets. In that case,

$$C_1 = P_1 | CRC_1 \oplus KS$$

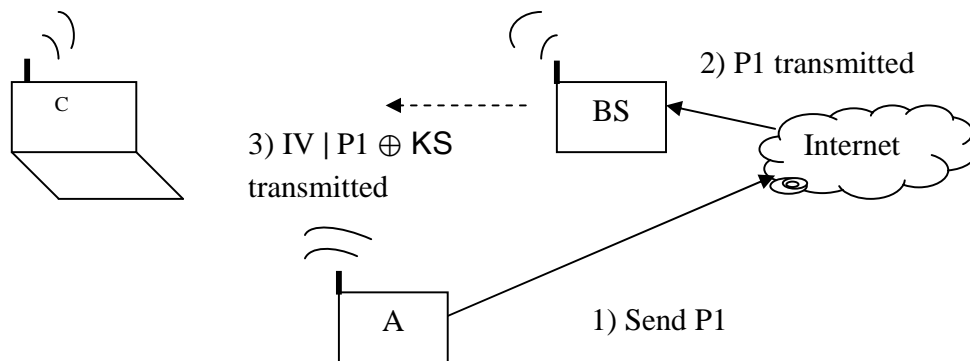
$$C_2 = P_2 | CRC_2 \oplus KS$$

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

$CRC_1 \oplus CRC_2$  can be segregated from the plaintext and ignored by the attacker. Now the attacker can infer information from  $P_1 \oplus P_2$ . This is similar to the case when we reuse key in One-Time Pad.

### 5. Chosen Plaintext Attack

The attacker can decrypt a cipher if he knows the KS. Below figure describes an attack called 'Chosen Plaintext Attack' where the attacker builds a table of KS.



**Fig 3:** Chosen Plaintext Attack

- A sends some Plaintext P1 destined to the wireless network of BS via Internet
- BS encrypts P1 and sends the encrypted message in the wireless network
- A listens to the encrypted message and builds a table similar to **Table 1**
- Here BS acts as Encryption Oracle for the attacker

IV	KS
0	KS <sub>0</sub>
1	KS <sub>1</sub>
2	KS <sub>2</sub>
⋮	⋮
⋮	⋮

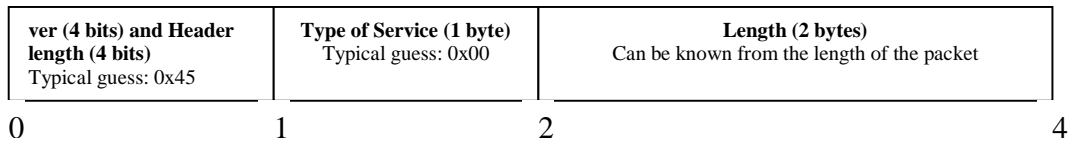
**Table 1:** IV and KS pairs

What it takes from A to send (encrypt) packets within the wireless network? Just one valid pair of IV and KS

What it takes from A to receive (decrypt) packets within the wireless network? Table 1 has to be built completely

### 5.1. Knowledge of Plaintext

In most of the cases the attacker has some knowledge of the Plaintext. For ex. in IP network the attacker can easily predict the first four bytes of an IP header. This knowledge helps the attacker to break the system quicker.

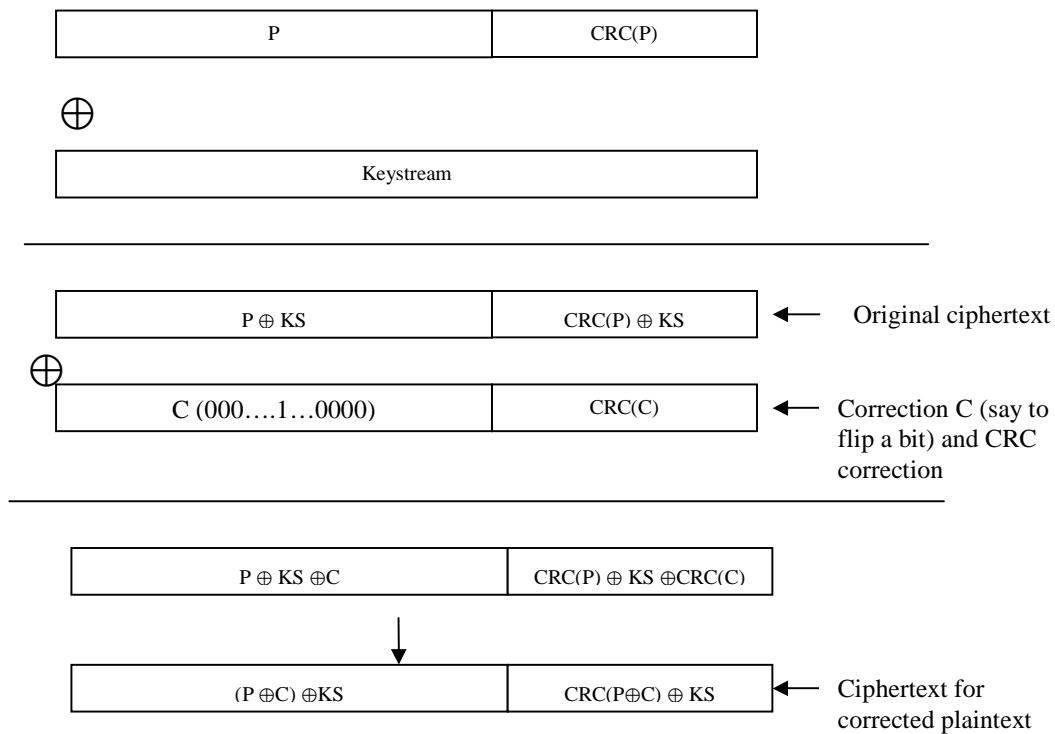


**Fig 4: IP Header**

### 6. Integrity attack

The attacker A can fiddle with the integrity of the message as well. Fig 5 explains how the attacker can flip a bit of a message.

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



**Fig 5: Flipping a bit of a message**

**The Chosen Plaintext attack and Integrity attack shows that RC4 fails to be a good expansion function**