

Network Security

Prof. Rob Johnson - Class Notes – 11 Sep 2009

Wired Equivalency Protocol (IEEE 802.11a) :-

Security goals:

1. Secrecy
2. Integrity
3. Access Control

S



Wireless Network Setup 1

Above is a normal wireless IP network setup using WEP.

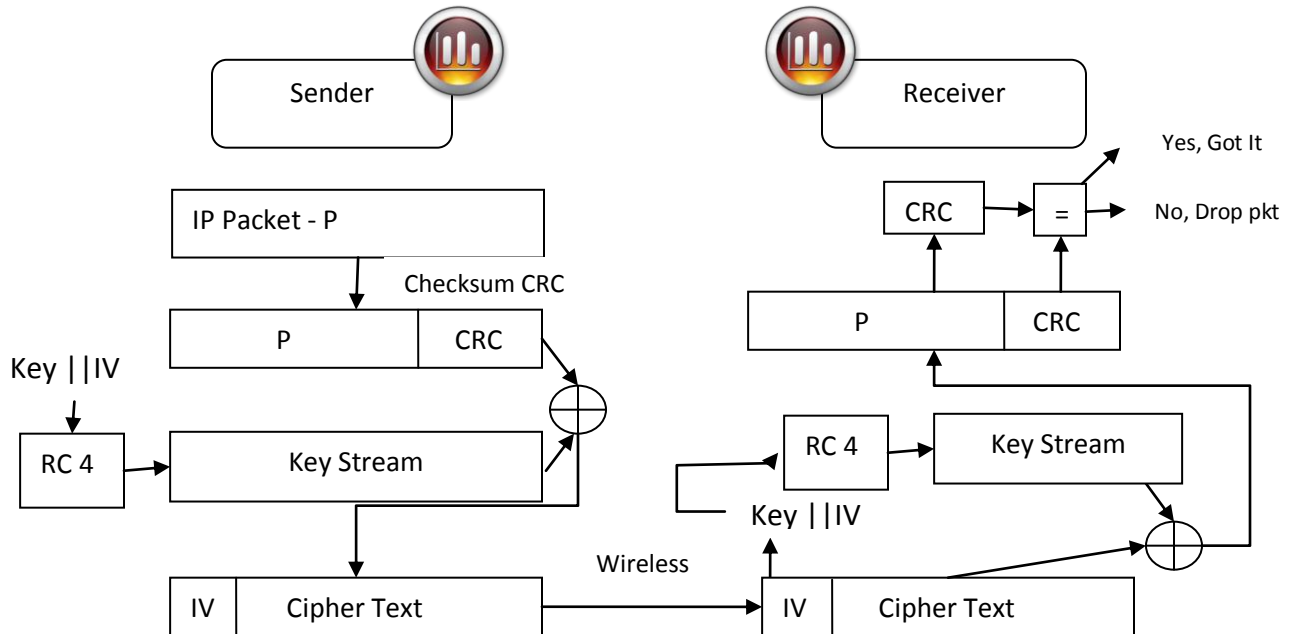
The wireless user has setup this network to connect to the internet, here the attacker can either try directly eavesdrop the data being transmitted and try to break the encryption code. The attacker here is also connected directly to the internet through a private wired network.

WEP Key – 128 Bit (Actual key 104 bit + Initialization Vector [IV] 24 bit)

Significance of IV->

1. IV differs for every packet transmission.
2. This random IV is concatenated with actual shared Key so as to generate a different cipher text even if the same message is encrypted more than once to avoid attacks.

Encryption Process in WEP ->



IV Choice ->

1. Pick IV Randomly.
 - a. Max values possible 2^{24}
 - b. Probability of IV repeating 2^{-24}
 - c. Expected No. of collisions $l_c 2 \times 2^{-24} = l^2 / 2^{25}$
 - d. l approx = $2^{12.5} = 6000$
 - e. if $l=2^{20}$ then 2^{15} collisions
2. IV = 0,1,2,3,.....
 - a. Total 2^{24} packets transmitted before IV pattern repeats.
 - b. Problem if system or wireless card is reset, which will make the sequence start again from 0.
 - c. An alternative to this is to start from a random number in the beginning.

Attacks on WEP ->

1. Problem on reuse of IV

$$P_1 \oplus CRC_1 \oplus K_s$$

$$\oplus P_2 \oplus CRC_2 \oplus K_s$$

$$P_1 \oplus P_2 \oplus CRC_1 \oplus CRC_2$$

Easy to decrypt if the content of plain text is familiar (eg known to contain English characters).

- Injecting a packet P1 in the wireless network via the attackers private internet connection if IP of the wireless user in the network is known(Determining IP is easy – For ex. Send an email to the user which contains an embedded image, if the email client of the user is not much secure it will send a GET request for the image and the image web server can get all the details of the user such as IP, OS used, Browser settings etc from HTTP headers).

This packet P1 is broadcasted by the Base Station as $IV \oplus P_1 \oplus K_s$.

The attacker can now listen to the network and intercept this packet and easily form a table as below.

| IV | Key Stream |
|-----|------------|
| 0 | Ks0 |
| 1 | Ks1 |
| ... | ... |

Since the IV and P1 contents are known to the attacker, it is very easy to get the Key Steam. Just the matter that all possible key steams and IV combination would require around 16GB of space which is easily manageable these days.

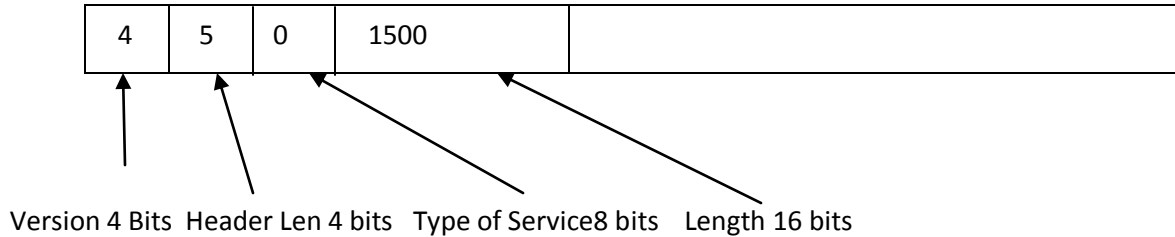
Note- To be sure that the Base Station is forwarding the packet P1 injected by the attacker, the attacker has to do this during an idle time when no other transmission is in progress(eg at night).

Once this table is retrieved the WEP encryption is totally broken, No secrecy, No integrity and No access control.

- Sending Fake packets becomes very easy if the attacker is just able to get one pair of IV and Keystream as above.

4. Key can also be found without even needing to find all possible pairs of IV and Ks as above if the network protocol being used is known. For eg IP.

Assume IP protocol is being used in the network.



The attacker can trim the IV and the CRC part of an encrypted packet transmitted on the WEP network and get the IP packet as above.

Now 1st 4 bytes of IP header are standard values as above, the attacker can easily guess the keystream and break the encryption.

5. FACT – $CRC(x \text{ Ex-OR } y) = CRC(x) \text{ Ex-OR } CRC(y)$

As CRC is linear it can be adjusted after flipping some of the bits of the encrypted message so that the changed message appears to be a valid one. This may be used to either corrupt the original packet data or can be manipulate transactions (Eg. - bank transaction by flipping any of the Most Significant Bits to increase the amount being transacted)