

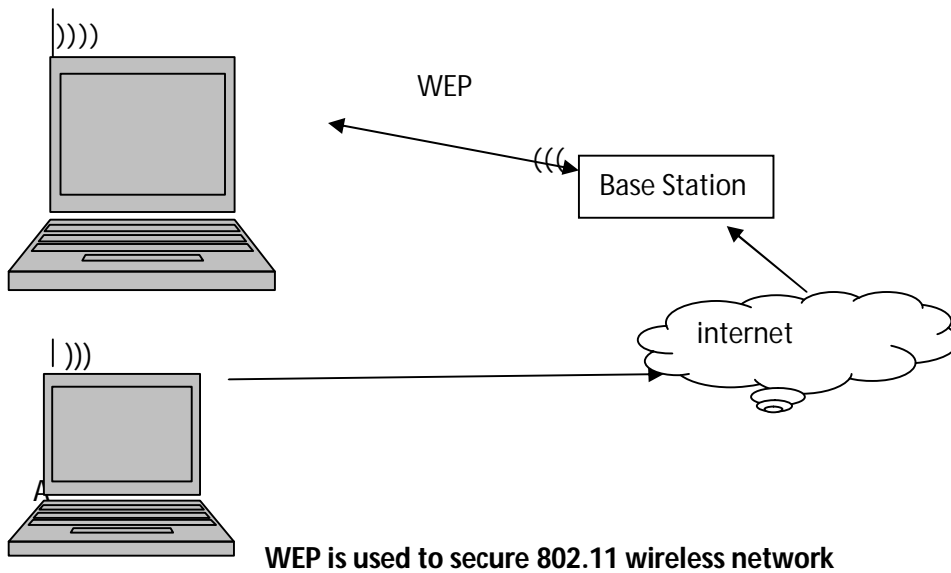
TOPICS COVERED

WEP Principle and Procedure

2 ways of choosing the IV

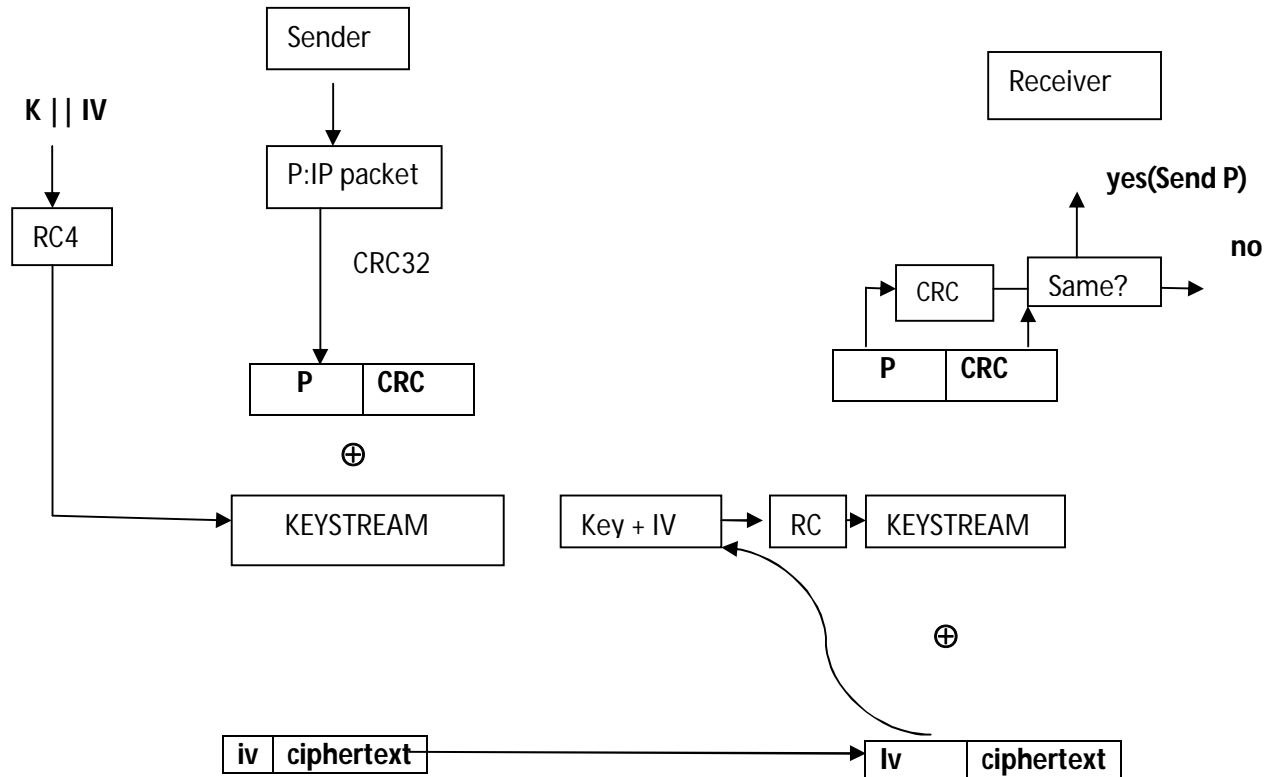
Chosen Plaintext attack

Integrity Attack



WEP PRINCIPLE AND PROCEDURE

- WEP uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity.
- 128 WEP key is entered by user as a string giving 104 bits, adding 24 bit IV gives the final 128 bit key
- The purpose of IV is to avoid repetition and it is transmitted in plain text.
- K: 104 bit IV: 24 bits
- Initialization vector is changed for every packet
- If we reinitialize RC4 by $K || IV$ output is random



CHOOSING THE IV

1) If IV is chosen randomly

Chances of collision for every pair = 2^{-24}

After L packets, Expected no. of collision is $(L * L - 1/2) * 2^{-24} = L^2 / 2^{25}$

Hence 1st Collision will take place after $2^{12.5}$ packets

Hence there is 50 % chance of IV reuse if IV is chosen randomly

2)if IV is started from 0 and increased incrementally for each packet

It takes 2^{24} packets before repetition occurs, which often takes days on a busy network.

IV reuse

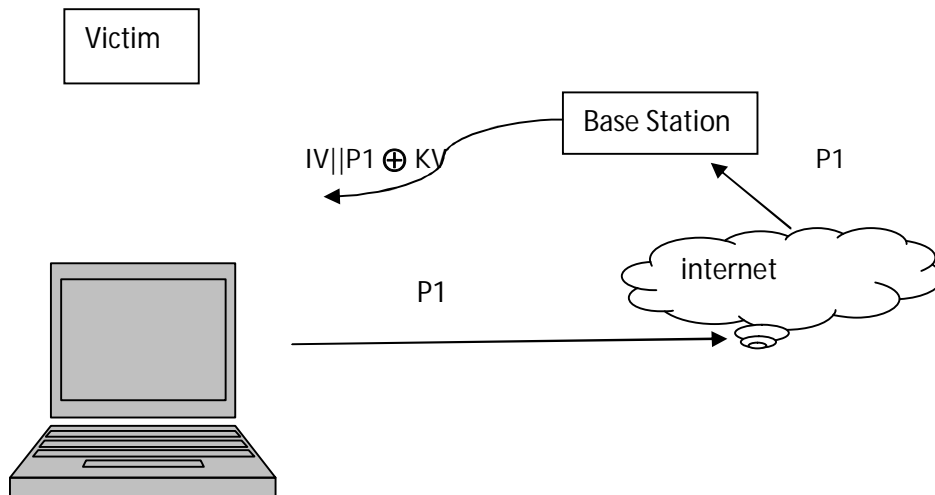
$$P1 || CRC \oplus KS$$

$$\oplus P2 || CRC \oplus KS$$

$$P1 \oplus P2 || CRC1 \oplus CRC2$$

CHOSEN PLAINTEXT ATTACK

We can send an email to a victim on internet and then observe packets to create a table of Keystreams for corresponding Ivs



If the victim is on the Internet, the attacker can simply send an e-mail message. If the attacker is able to send the victim packets and observe and analyze those encrypted packets, he can deduce the cipher stream.

$$C = (P1 || CRC1) \oplus KS$$

$$KS = C \oplus (P1 || CRC1)$$

CREATE A TABLE FOR DECRYPTION

IV	KS
0	KS0
1	KS1
2	KS2
.	.
.	.

$$C = (P1 || CRC1) \oplus KS$$

$$KS = C \oplus (P1 \parallel CRC1)$$

SO We totally broke

Secrecy

Access Control

Integrity

INTEGRITY ATTACK

Assuming it to be IP Network

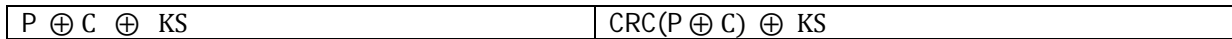
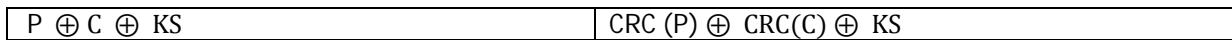
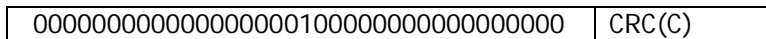
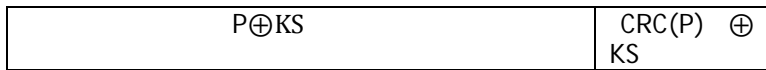
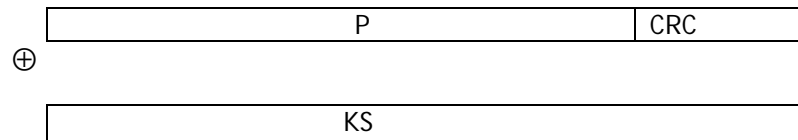
1st 4 bytes of Keystream is known to attacker

4	5	0	Deductible by sub crc & iv from total length	
Version	Header Length	Type of service(8 bits)	Total length(16bits)	

FACT $CRC(X \oplus Y) = CRC(X) \oplus CRC(Y)$

Using this fact , **we can easily alter packets**

Suppose if we know that there is amount in particular position, we can manipulate a bit in most significant position



CSE 508 NETWORK SECURITY- Sept, 11,2009
WIRED EQUIVALENCY PROTOCOL

Hence we have been able to produce correct CRC after manipulating the desired bit position using the above fact

The weakness of WEP is because of RC4 , as there is correlation between keystream produced and the key.