

# Network Security, Lecture Notes, Class 3

September 11, 2009

## 1 WEP: Wired Equivalency Protocol

- IEEE 802.11a standardized the Wireless Equivalence Protocol (WEP)
- In the early days of IEEE 802.11a, security was the main concern of wireless networks.

### 1.1 Security Goals of WEP:

- Secrecy
- Integrity: Intruder should not meddle with the message.
- Access Control

### 1.2 Features of WEP

- Both the base Station (BS) and the client will have a key.
- The key will be: 104 - bit and the Initialization Vector will be: 24 - bit. So a total of 128-bits is used as a keystream in WEP.
- When we encrypt the same packet twice, the ciphertexts should not be the same. For this reason, IV is used.

Sender side:

- RC4 is used in WEP, WPA, Microsoft PPP, Encrypted pdfs and so on. Basically, RC4 is an expansion function. The key (104-bit) is concatenated with the IV (24-bit) to get the RC4 key.
- The RC4 keystream with the packet to obtain the ciphertext.

Receiver Side:

- IV is XORed with the 104-bit key to obtain the RC4 key ( $K \parallel IV$ ). This is used to decrypt the ciphertext, which results in the Packet along with the CRC.
- The CRC of the packet is calculated separately and compared with the CRC obtained from the receiver side.

- If the CRC matches, then the packet is said to be genuine. Otherwise, the packet is dropped.

Initialisation Vector (IV) Choice:

- Pick an IV randomly. Total number of possible IVs will be  $2^{24}$ .
- After 'l' packets, expected number of collisions =  $\binom{l}{2} * 24 \approx l^2/2^{25}$ .  $l \approx 2^{12.5}$ ;  $l \approx 6000$ .
- If there is an IV reuse, then,

$$P_1 || CRC_1 \oplus keystream$$

$$P_2 || CRC_2 \oplus keystream$$

If we XOR these 2 equations, we get,  $P_1 \oplus P_2 || CRC_1 \oplus CRC_2$ .

- If we know some information about the packet in prior, then it is very easy to break it.
- Now, assume that the intruder knows the packet  $P_1$ . By building a table of all possible IV vs Keystream and then matching the current one with the one in the table, he/she can easily break it.
- In an IP packet, by knowing the header and IV, we can easily break the packet.
- It is possible to distinguish between an RC4 stream from a totally random stream. Hence it is not secure.