Security Issues in Mobile Computing

Part 2

IEEE 802.11 security through WEP

- There are some built-in security features of 802.11.
  - It identifies several services to provide a secure operating environment.
- The security services are provided by the wired equivalent privacy (WEP) protocol .
  - to protect link-level data during wireless transmission between clients and APs.
  - WEP does not provide end-to-end security. Only the wireless portion of the connection is made secure.

WEP security features of 802.11 wireless LANS

- IEEE defines three basic security services for WLAN. They are:
  - Authentication
  - Confidentiality and
  - Integrity

Authentication

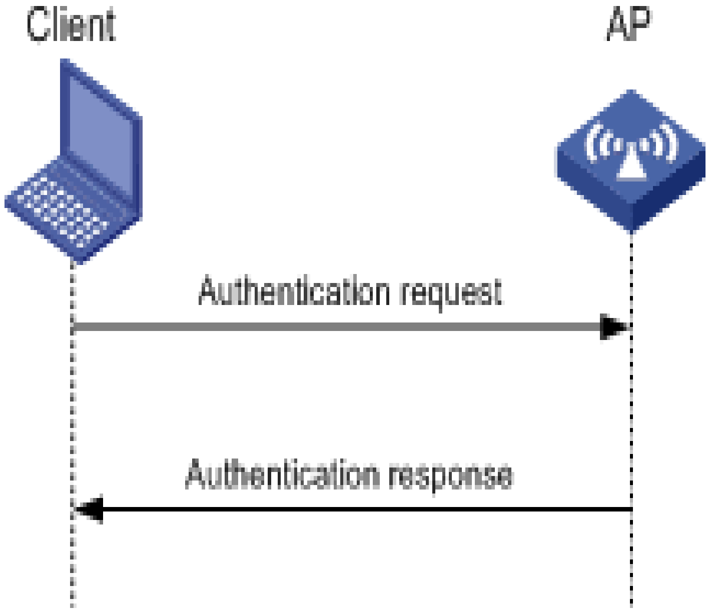
- Wireless users must get validation

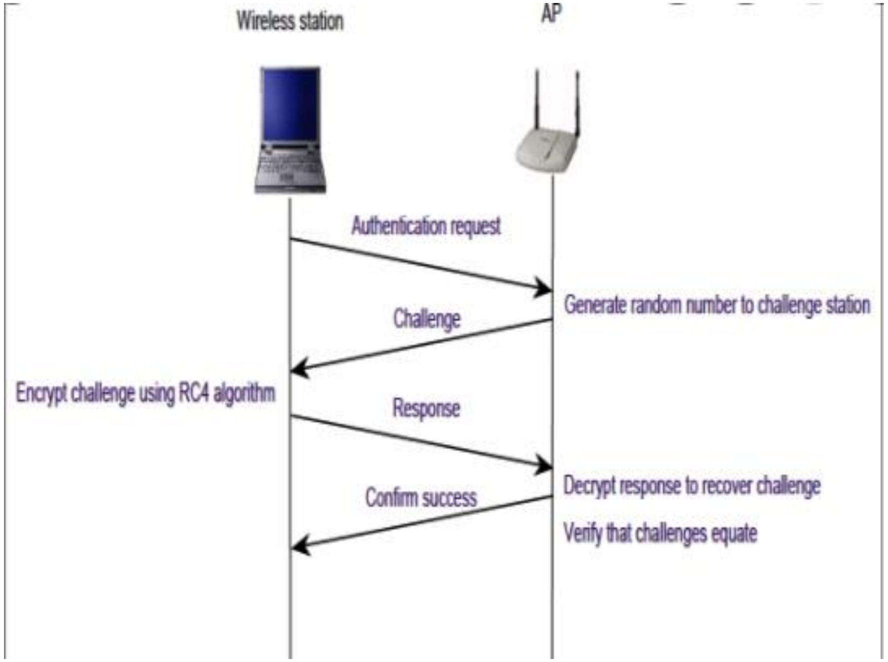
Authentication

- The IEEE 802.11 specification provides for two types of authentication :
    - open-system authentication
    - shared-key authentication

Authentication

Open System Authentication	Shared Key Authentication
Non Cryptographic.	Cryptographic.
1-Stage Challenge-Response.	2-Stage Challenge-Response.
No identity verification required for station to join network.	Station requires to prove shared WEP key to join network.




Wireless station
AP
Authentication request
Generate random number to challenge station
Challenge
Encrypt challenge using RC4 algorithm
Response
Decrypt response to recover challenge
Confirm success
Verify that challenges equate

Authentication

open-system authentication

- A client station exchanges messages with an access point.

- The AP sends a query as a ‘challenge’ to the station.

- If the station sends the correct response, i.e., the correct MAC address fields, it is considered authenticated.
  - There is no cryptographic validation here.
    - highly vulnerable to unauthorized access and attack.
  - The 802.11 specification only requires this type of authentication.
  - cannot be really called authentication.

Authentication

shared-key authentication

- The challenge-response technique used is based on cryptography.
- A random challenge generated by the AP and sent to the wireless client.
- The client uses a cryptographic key that is shared with the AP to encrypt the challenge and returns the result to the AP.
- The AP decrypts this challenge and if the decrypted value is the same in the random challenge it had sent, it allows access.
    - shared key authentication is optional in the IEEE 802.11 specification

Authentication

- **Limitations:**

1. don’t provide mutual authentication.
   - i.e., the AP authenticates the wireless client, but the client does not authenticate the AP. The mobile station must trust that it is communicating with a legitimate AP.

2. the simple challenge-response schemes used in these techniques are known to be weak.
   - suffer from attacks like the man-in-the-middle' attack

Confidentiality

- aim of confidentiality/privacy- to prevent information being eavesdropped during transfer(as is done in a wired network.)
  - Eavesdropping is a purely passive attack which must be avoided.
- The 802.11 standard for WEP also uses the RC4 symmetric key, stream cipher algorithm.

Confidentiality

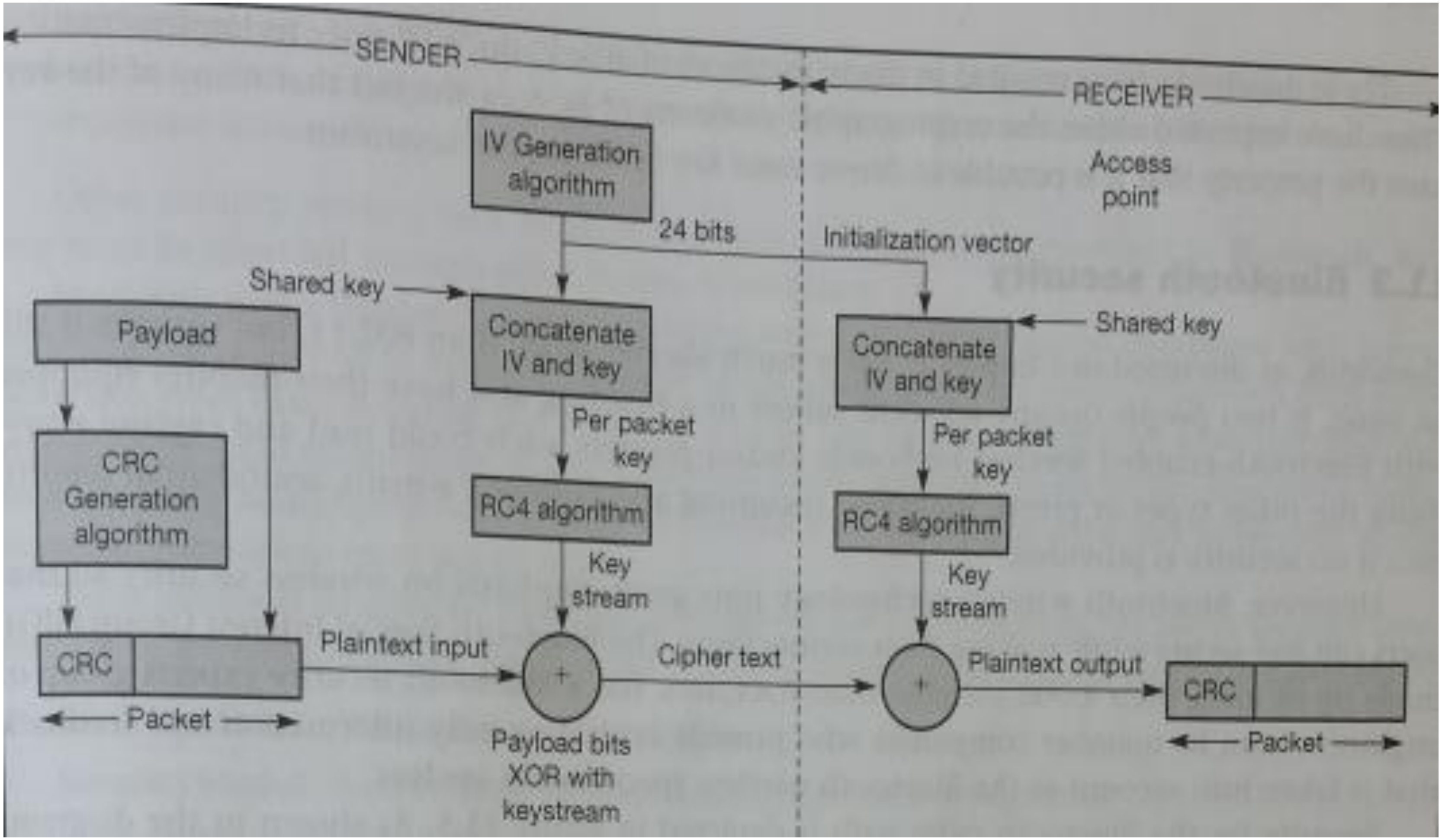


Fig: WEP privacy and integrity using RC4 algorithm

Confidentiality

At the wireless station side:

- A pseudo-random data sequence, called a keystream, is obtained
  - by concatenating a 24-bit Initialization Vector (IV) to a shared 40 bit key and
  - passing the same through the RC4 algorithm.
- Then the payload, which consists of
  - the plain text (transmission data) together with
  - the CRC generated by the CRC generating algorithm
- The Payload and the keystream is XORed with the keystream to generate the cipher text.

- At the AP side, the procedure is performed in reverse to get back the plaintext.

Confidentiality

- In this way, data can be protected from eavesdropping during transmission over the wireless link using WEP.

- WEP is applied to all data above the 802.11 WLAN layers to protect Transmission Control Protocol/Internet Protocol (TCP/IP), Internet Packet Exchange (IPX) and Hyper Text Transfer Protocol (HTTP) traffic.

- The 802.11 standard WEP supports only a 40-bit cryptographic keys size for the shared key, but nonstandard extensions of WEP that support key lengths up-to 104 bits are also prevalent.

- It may be noted that increasing the kay size increases the security of a cryptographic technique.

Integrity

- Ensures that data/message between the wireless clients and the AP are not modified in transit in an active attack (the integrity is not compromised).
- The IEEE 802.11 specification provides such a data integrity service so that an active adversary ‘in the middle’ can be thwarted.

Integrity

- The same procedure that is used for providing confidentiality, is used at the wireless client side, to provide such data integrity.
- At the receiving AP :
  - decryption is performed and the CRC is recomputed on the received message.
  - This is compared with the one computed with the original message.
- If the CRCs do not match, this indicates an integrity violation and the packet is discarded.

- The simple CRC is not as cryptographically secure as a hash or message authentication code.

Drawbacks of WEP

- The IEEE 802.11 specification does not provide for key management mechanisms like generating, distributing, storing, loading etc. of keys.
  - Keys must either be preloaded by the manufacturer or
  - exchanged in advance over a wired backbone network.
- The base station or the mobile station could also choose a random key and send over the air, encrypted with the other's public key. Such keys generally remain stable for months or years.

- The main drawback of the WEP algorithm is that the same key is shared by all wireless clients so there is no way to distinguish one tom another. Also all users can read each other’s' data.