03 - WLAN Basic Authentication and Privacy Methods

WIRELESS LAN SECURITY

Contents

- Basic authentication services:
  - the open authentication
  - shared-key authentication

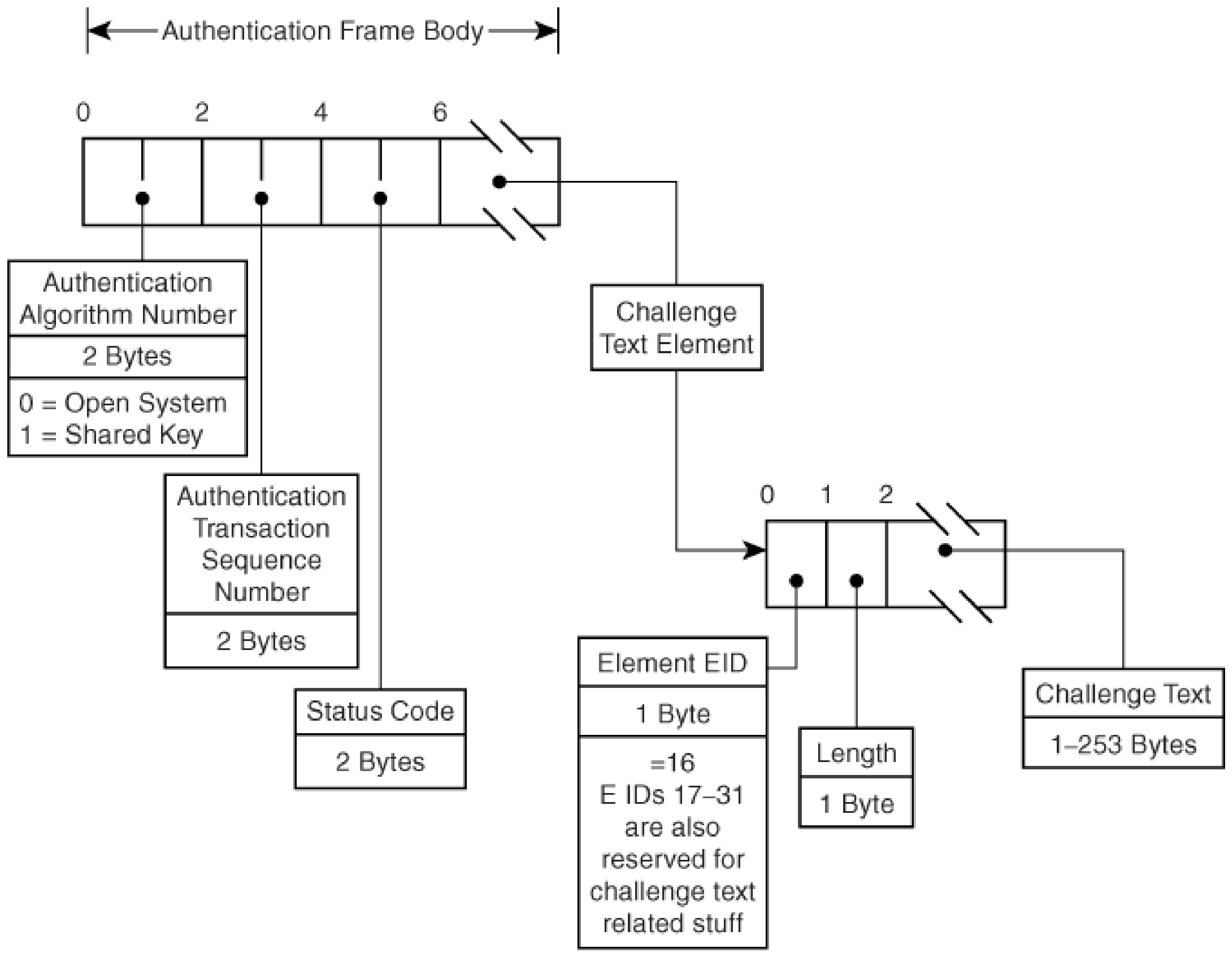
- Wired Equivalent Privacy (WEP) mechanisms

Note

- Only point-to-point authentication is supported; no multicast authentication is allowed.

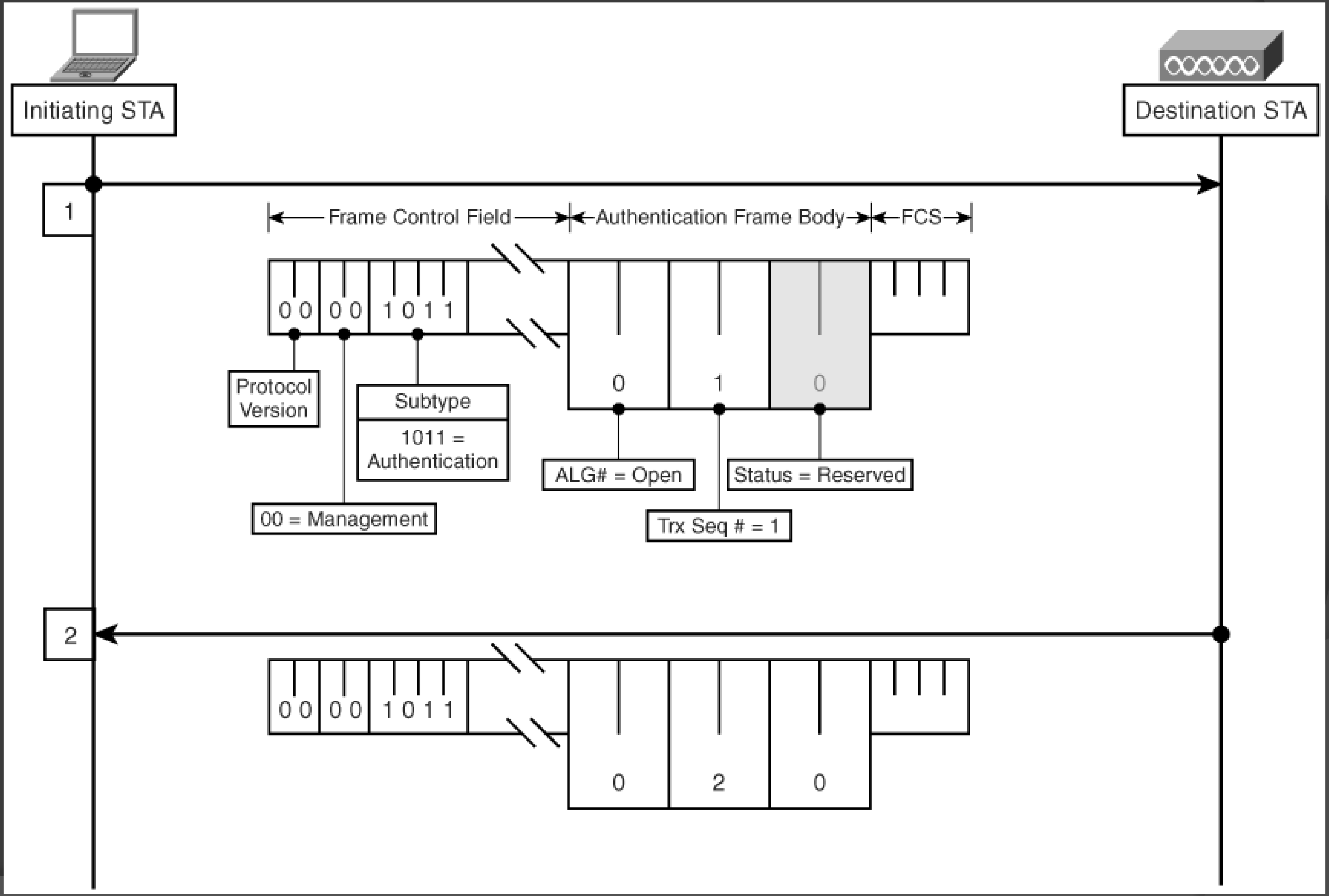
- The authentication is session, user, or device authentication; it is not message authentication.

Authentication Frame Body



Authentication Frame Body
0
2
4
6
Authentication Algorithm Number
2 Bytes
0 = Open System
1 = Shared Key
Authentication Transaction Sequence Number
2 Bytes
Status Code
2 Bytes
Challenge Text Element
0
1
2
Element EID
1 Byte
=16
E IDs 17–31 are also reserved for challenge text related stuff
Length
1 Byte
Challenge Text
1–253 Bytes

Open Authentication



Trust Model and Assumptions

- provides no security
- trusts all STAs that ask to be connected
- The only security aspect is that the STAs should know the Service Set Identifier (SSID) of the AP
- The AP's policy could base its access on the client's MAC address

Applications

- The advantage is the simplicity and ease, precisely because no setup is required.

- suitable for public WLANs, including the ones available in hotels, coffee shops, airport lounges, and conference halls.

Vulnerabilities

- should use a hardware or software firewall
- your computer is not fully secure against threats from the Internet
- use a VPN solution, the VPNs usually filter out and disable local connections

MAC-Based Authentication

- The AP has an internal table of MAC addresses from which it allows access to the network.

- MAC-based authentication can be achieved when using either open authentication or shared-key authentication.

Trust Model and Assumptions

- trust the registered MAC addresses and assumes their integrity—that is, it assumes that the MAC addresses belong to the devices.

- presumes that the receiver trusts the message because the message is not integrity protected.

Supporting AAA Infrastructure

- No AAA mechanisms are used
- Out-of-band registration of client MAC addresses
- The STAs' MAC addresses are manually entered into the APs.
- If only a couple of MAC addresses are registered, this might be worth the effort.

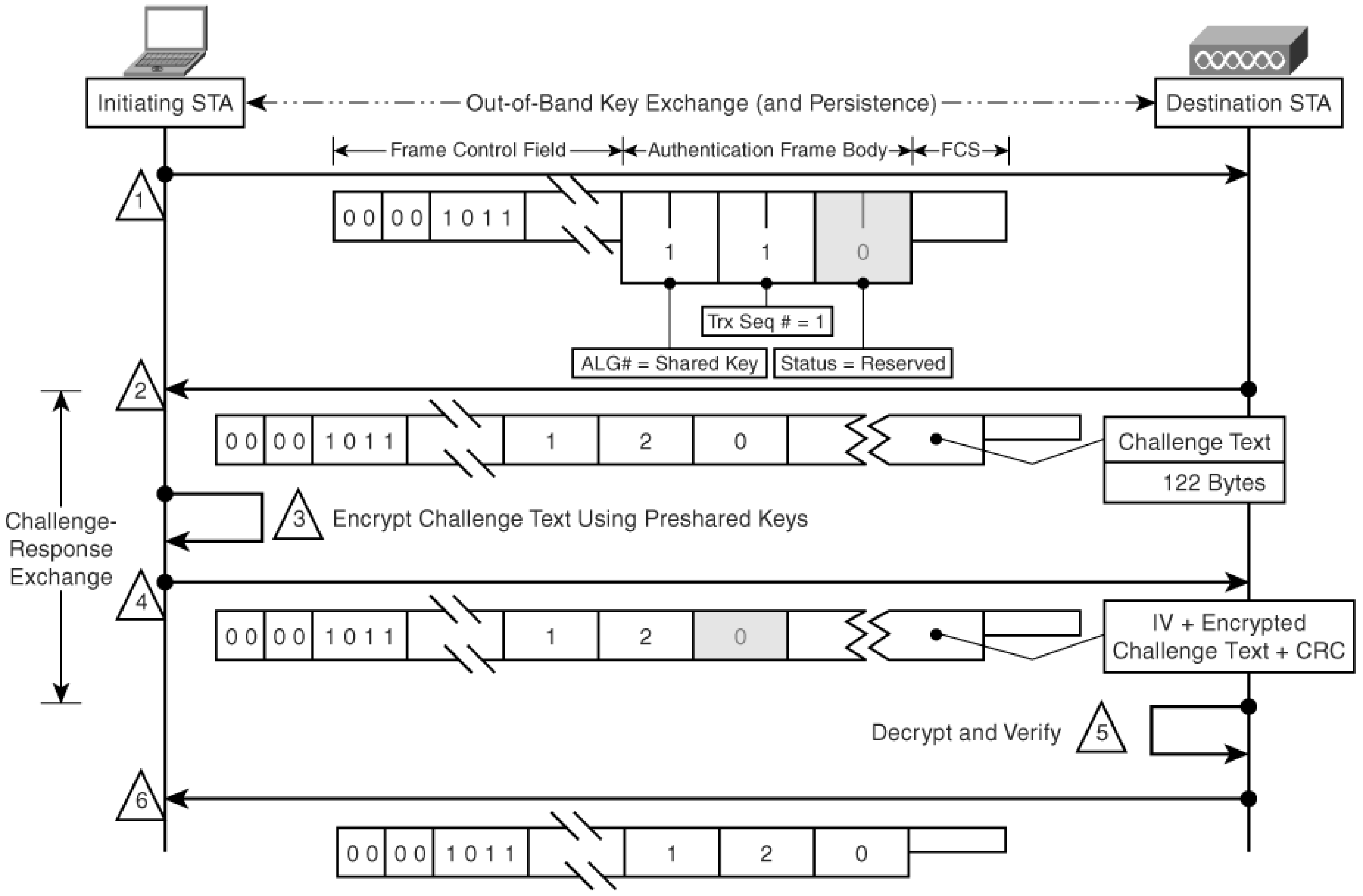
Applications and Vulnerabilities

- suitable for home LANs and for small offices where the number of computers is small.
- A hacker can hide the device's built-in MAC address and spoof other MAC addresses using a firmware overlay.
- use VPN for a secure connection and, if someone is surfing the Internet, use a firewall.

Shared-Key Authentication

- based on a challenge-response protocol
- requires WEP mechanisms
- establishes proof that both parties share the same secret
- does not prove or authenticate each party's identity

Protocol Choreography



Trust Model and Assumptions

- based on WEP primitives
- hinges on the key distribution (such as the ability to distribute to and keep the keys in only the intended devices)
- the strength of WEP algorithms
- Both of these have been under attack

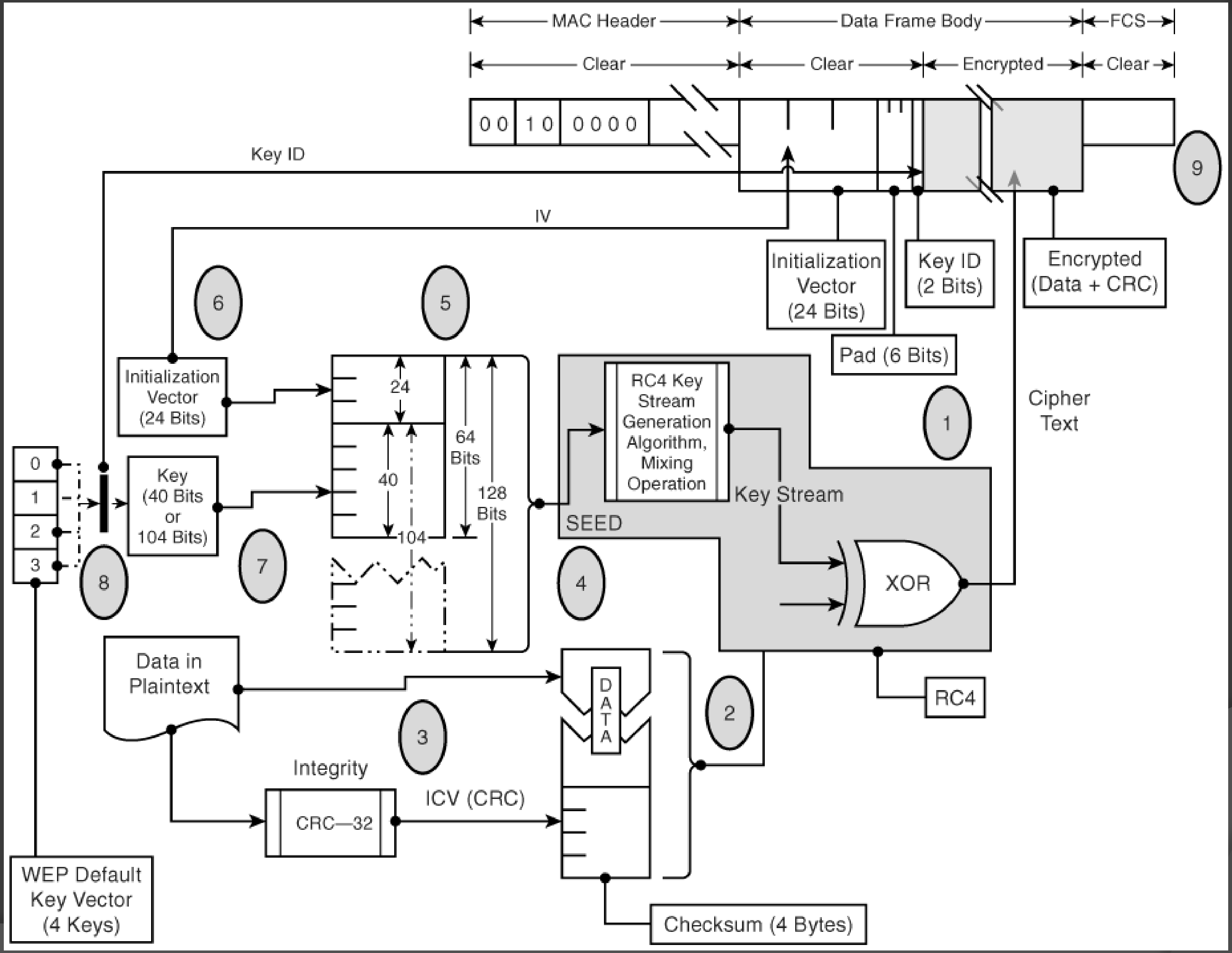
Vulnerabilities

- The out-of-band, manual authentication key distribution to all STAs.
- Keys tend to be common across multiple APs and clients.
- The authentication process leaks information about the key stream.

WEP Privacy Mechanics

- The encryption exchanges and mechanics, RC4.
- How an initialization vector (IV) is generated and handled
- How keys are generated and distributed.

WEP Processing Model



RC4 Algorithm

- a symmetric algorithm and a stream cipher.
- 2 phases:
  - key stream generation: a set of state machine and mixing operations that result in a pseudorandom stream of bits. The key setup takes a seed.
  - encryption: an XOR of the plaintext with the generated key stream.

Key Generation and Selection

- uses static pre-shared keys
- defines a key vector that can hold four keys, distributed out of band
- The key can be 40 bits or 104 bits in length
- lacks key management mechanisms

Vulnerabilities

- The choice of IV
- The transmission of the IV
- The ICV mechanisms
- Weak Ivs
- RC4 weak keys
- The non-scalability of key distribution