05 - WLAN Encryption and Data Integrity Protocols

WIRELESS LAN SECURITY

Introduction

- 802.11i adds new encryption and data integrity methods.
- includes encryption algorithms to protect the data, cryptographic integrity checks to prevent message modification and replay, and dynamic key management algorithms
- describes the new security association concept associated with 802.11i.

IEEE 802.11i

- enhances 802.11 with several new security mechanisms to ensure message confidentiality and integrity.

- also incorporates the 802.1x port authentication algorithm to provide a framework for strong mutual authentication and key management.

Features

- Two new network types, called Transition Security Network (TSN) and Robust Security Network (RSN)
- New data encryption and data integrity methods: Temporal Key Integrity Protocol (TKIP) and Counter mode/CBC-MAC Protocol (CCMP)
- New authentication mechanisms using the Extensible Authentication Protocol (EAP)
- Key management via security handshake protocols conducted over 802.1x

TKIP

- a cipher suite
- includes a key mixing algorithm and a packet counter to protect cryptographic keys
- includes Michael, a Message Integrity Check (MIC) algorithm that, along with the packet counter, prevents packet replay and modification

CCMP

- based on AES that accomplishes encryption and data integrity
- provides stronger encryption and message integrity than TKIP
- not compatible with the older WEP-oriented hardware

RSN

- RSN allows only machines using TKIP/Michael and CCMP.
- A TSN is one that supports both RSN and pre-RSN (WEP) machines to operate.
- RSN is definitely preferred, and getting all networks to use CCMP exclusively would be ideal.

Encryption Protocols

- Three encryption protocols: WEP, TKIP, and CCMP.
- They primarily are used for confidentiality but also include message integrity.
- TKIP and CCMP also include replay protection.
- WEP does not provide robust message integrity or replay protection.

Wired Equivalent Privacy

Three main design goals:

- To prevent disclosure of packets in transit
- To prevent modification of packets in transit
- To provide access control for use of the network

Preventing Disclosure of Packets

- uses the RC4 algorithm
- RC4 is a stream cipher and is not supposed to be reused with the same key
- Therefore, the designers added the initialization vector (IV), which allows a fresh RC4 key to be used for every packet.
- Failure to prevent repeats of IV means that an attacker can replay packets, or attack on the RC4 keystream.

Preventing Modification of Packets

- uses the integrity check vector (ICV)
- The ICV is a four-octet linear checksum calculated over the packet's plaintext payload and included in the encrypted payload.
- It uses the 32-bit cyclic redundancy check (CRC-32) algorithm.

Achieving Access Control

- chooses a challenge-response mechanism based on knowledge of the WEP key, called shared-key authentication
- The idea was that a station needed to prove its knowledge of the WEP key to gain access to the network.
- This method not only is flawed, but it also compromises bits of the keystream.

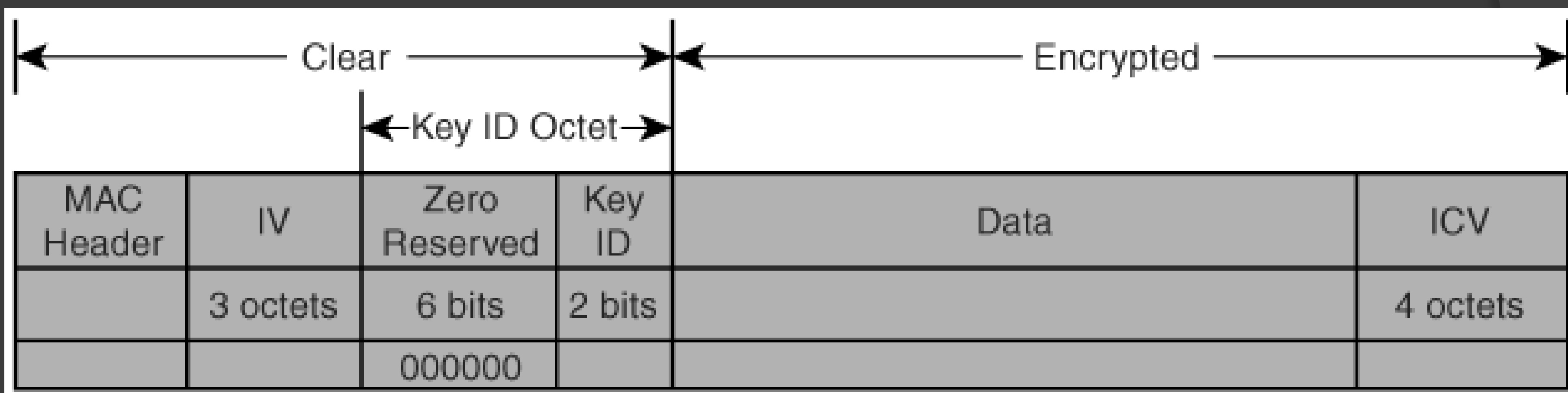
RC4

- RC4 is the basic encryption algorithm that WEP employs.
- RC4 is a symmetric stream cipher, so it produces a keystream of the same length as the data.
- In WEP, this keystream is combined with the data using the exclusive OR (XOR) operation to produce the ciphertext.

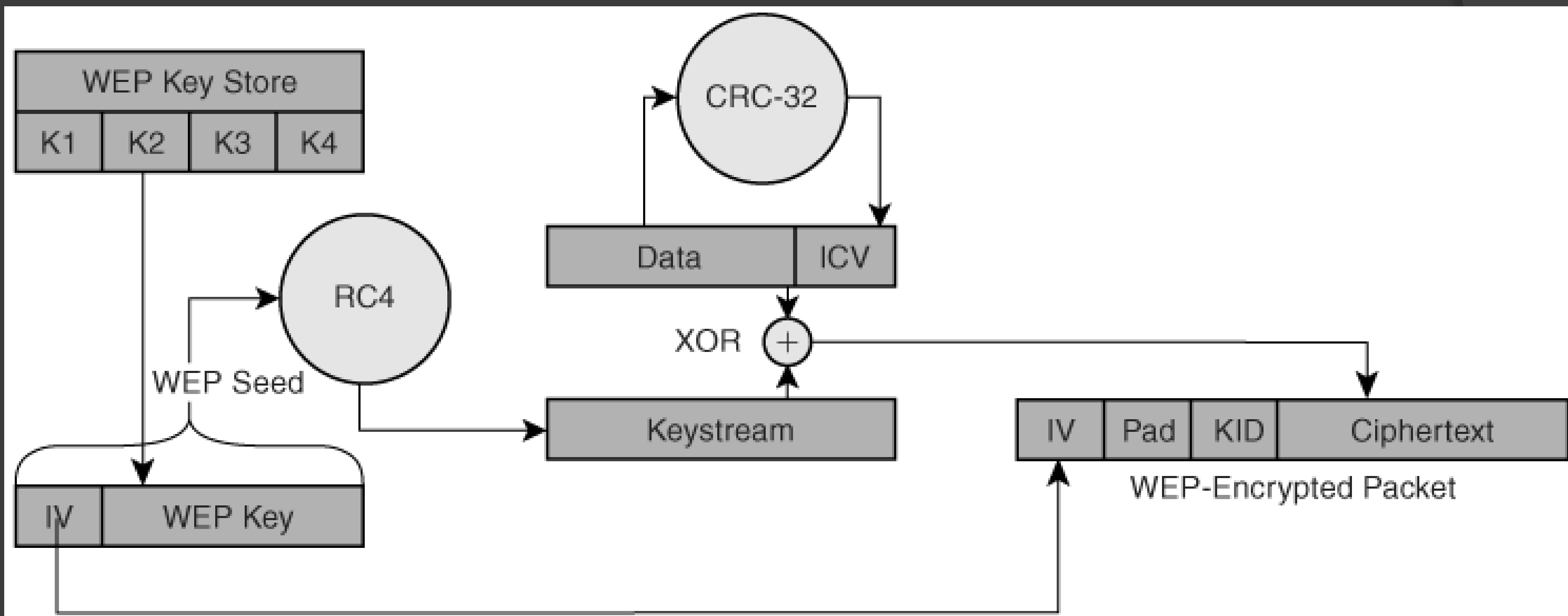
WEP Encapsulation

- involves encryption, integrity check calculation, possible fragmentation, and attachment of headers.
- Decapsulation is the opposite, involving processes such as removing headers, decryption, reassembling packets, and verifying integrity checks.

WEP Packet Format



The Process of Encapsulation of the WEP Packet



WEP Decapsulation