WEP Concepts and Vulnerabilities

By
Advait Kothare

Introduction

- Wireless Networks in wide spread use
- Based on the IEEE 802.11 standard
- Confidentiality and Integrity issues
  - Different issues from wired networks
- Eavesdropping a major issue
- Attacks could be launched from the car park

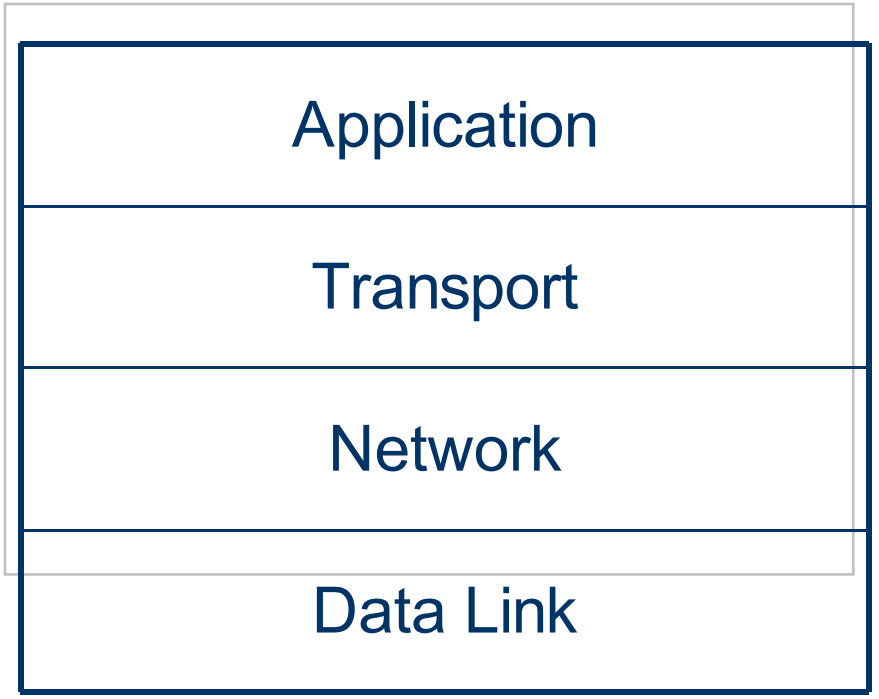
WEP

- Wired Equivalent Privacy
- Optional protocol as part of the 802.11 standard
- Intended to prevent unauthorized access by a casual eaves dropping
- Intention to provide privacy equivalent to a wired network

WEP Design goals

- Confidentiality
  - Prevent casual eavesdropping
- Access control
  - Prevent unauthorized access to network resources
- Data Integrity
  - Prevent tampering of data frames
- Self-synchronizing, Efficient, Exportable

WEP in the Protocol Stack

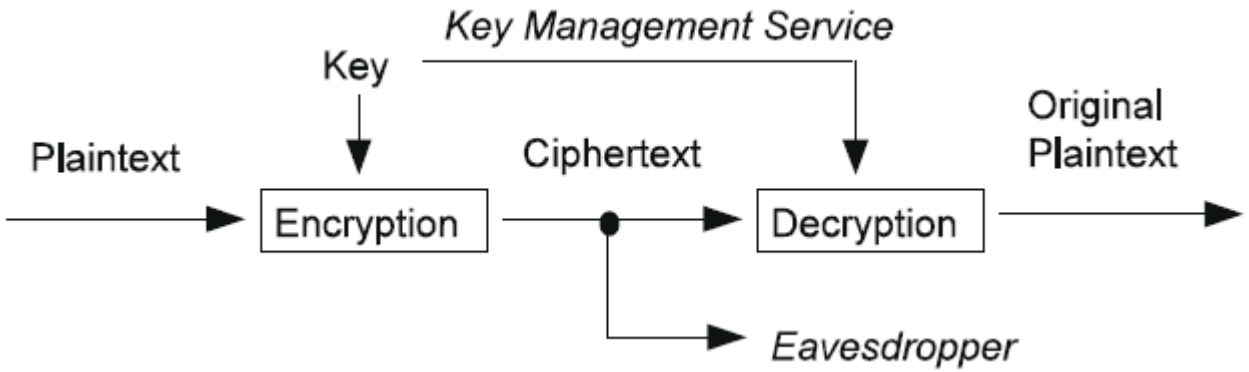


TCP/IP Protocol stack

WEP and Protocol Stack

- Implemented in the Link layer
  - Also called Medium Access Control layer
- Link layer includes the device driver in the operating system and the radio interface card

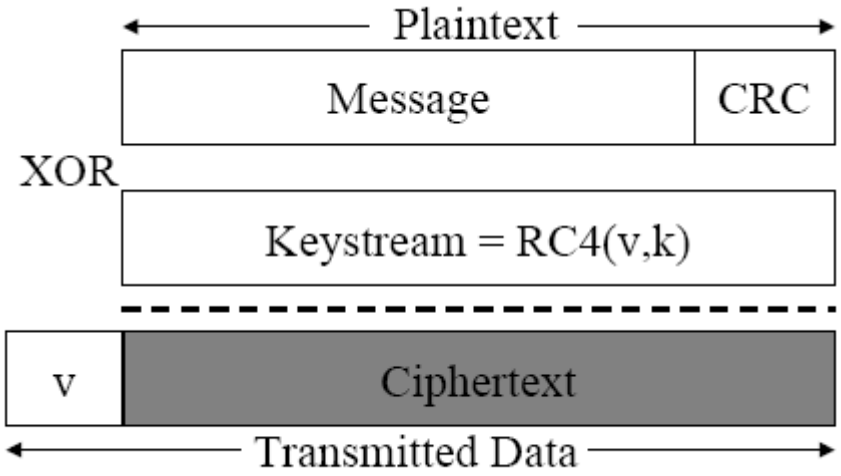
WEP Overview



WEP Overview

- Use RC4 encryption algorithm
  - Stream cipher
  - Shared symmetric key used to encrypt and decrypt
- RC4 takes the shared key and generates a key stream
- Key stream is bitwise XOR with the plain text to produce cipher text

WEP Operation



Data frame view

WEP Operation - Integrity

- Calculate the checksum value ICV
  - Uses CRC-32
  - Integrity protection
- Concatenate with data frame to get plain text
  - To get the MPDU

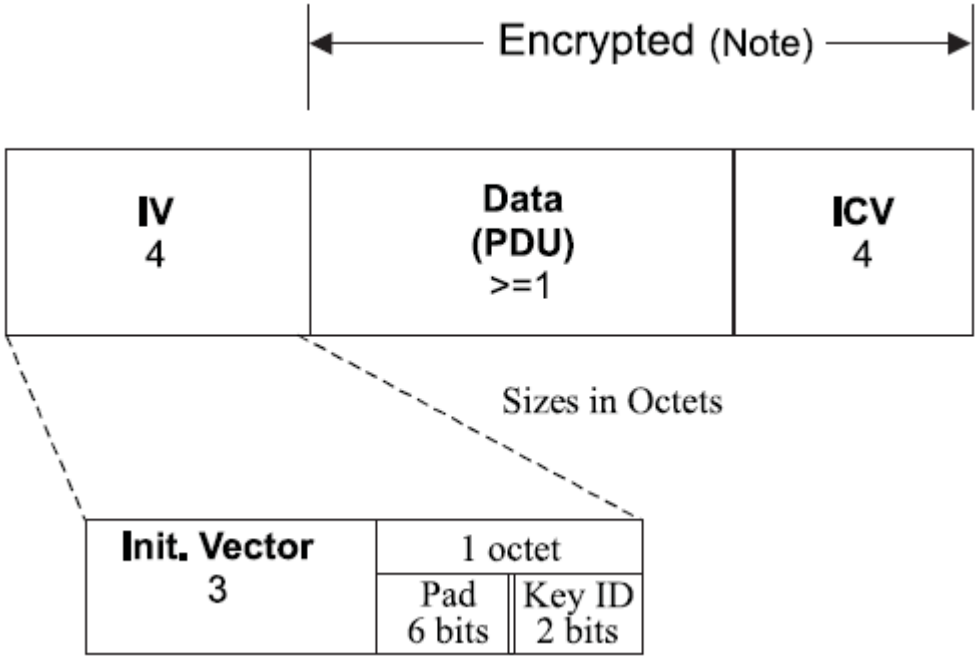
WEP Operation - Confidentiality

- The shared key is concatenated with a Initialization Vector
- Seed value to the WEP Pseudo Random Number Generator (PRNG)
- PRNG pseudo random octet stream equal in length to the number of octets in the MPDU

WEP Operation – All together

- Key stream is bit wise XORed with the MPDU to get the Cipher text
- IV consists of an initialization vector
- Concatenate IV with Cipher text to produce the data frame ready for transmission over the radio link

Extended MPDU



Extended MPDU

- The Integrity Check Value is also encrypted
- Key Id selects 1 of 4 shared secret key values
- The Initialization vector is limited to 24 bits in size

Weakness

- Shared keys limited to 40 bits by US government export restrictions
  - Practical to launch a brute force attack on the key of this size
  - Manufacturers added extensions to lengthen the key length

Weakness – Stream ciphers

- Vulnerable when the IV and key are reused

$$C1 = P1 \oplus RC4(v, k)$$

$$C2 = P2 \oplus RC4(v, k)$$

giving us:

$$C2 \oplus C1 = P1 \oplus P2$$

RC4 = RC4 key stream generator function

v = initialization vector, k = shared key

Weakness – Stream Ciphers

- IV values are limited by IV length (24 bits)
  - Also by implementation faults
  - Such as during interface card initialization initial value is set to a standard value
- This weakness is irrespective of the key length
  - Increasing the key size doesn’t solve this problem

Weakness – Key Distribution

- RC4 uses a shared symmetric key.
- Changing the key requires manually reconfiguring each individual Access Point and radio interface card
- Time consuming and expensive process
- Does not scale well in the enterprise size network

Weakness – Message Integrity

- WEP checksum value is a linear function of the message
- Checksum operation distributes across the encryption operation

$$c(x \oplus y) = c(x) \oplus c(y)$$

which results in:

$$c(M) \oplus c(d) = c(M \oplus d)$$

- Cipher text C could be modified to a value C', which would then be deciphered to plain text P $\oplus$ d.

Weakness – Message Integrity

- Intruder to change parts of a message without disrupting the checksum.
- Controlled modification can be made to an encrypted message without fear of detection.

Next Generation Standards

- IEEE 802.1x authentication mechanism
  - Designed for wired networks
  - Provide authentication only
  - Encryption by SSL, IPSec or SSH
- IEEE 802.11i
  - Uses AES 128 for encryption, which is yet to be broken
  - Defines a Key Distribution Framework for scalability to large networks

Summary

- WEP is insecure, but still can secure networks if certain best practices are followed
  - Maintain access control lists
  - Use vendor specific key distribution schemes
  - Physically Secure Access Points
  - Change keys periodically
  - Shutdown AP when not in use
- WEP can deter casual eavesdroppers

Refernces

- LAN MAN Standards Committee of the IEEE Computer Society. *Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*. IEEE Standard 802.11, 1999 Edition, 1999.
- W. Richards Stevens. *TCP/IP Illustrated, Volume 1. The Protocols*.
- R. L. Rivest. *The RC4 Encryption Algorithm*. RSA Data Security, Inc, March 12, 1992.
- Gast, Matthew. *Wireless LAN Security: A Short History*, 19 April 2002. URL: http://www.oreillynet.com/pub/a/wireless/2002/04/19/security.html (14 Jan 2003).
- N. Borisov, I. Goldberg, and D. Wagner, *Intercepting Mobile Communications: The Insecurity of 802.11*, In Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking, July, 2001.
- S. Fluhrer, I. Mantin, and A. Shamir, *Weaknesses in the Scheduling Algorithm of RC4*, In Eight Annual Workshop on Selected Areas in Cryptography, August, 2001.

Thanks