

(802.11)Wireless

saraninejad@gmail.com

mahdi10_2004@yahoo.com

(airborne) . security :

WLAN .

pringle

WLAN WEP SSID (wireless) :

1

WLAN

2005 Gartner

2000 2010

[2]

wireless

Wireless .

LAN-2

LAN

1980

LAN

1990

WLAN . WLAN.

WLAN .

LAN WLAN

laptop (AP)

300 () LAN

[2]

IEEE802.11b . 802.11b WLAN

2.4GHZ

LAN -1 2

LAN

LAN :

LAN (1

AP

:() Mobility (2

AP

:

(3

WLAN : Application agnostic (4

TCP/IP

WLAN : (5

3

: [1]

(1

(2

(3

DOS (4

(5

(6

(7

) (8

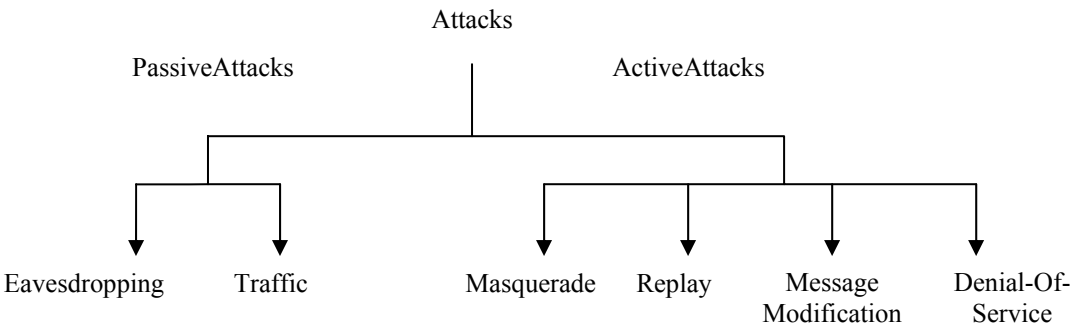
(

(9

4

IEEE 802.11X

:[1]



1 4

1 1 4

()

2 1 4

2 4

1 2 4

2 2 4

3 2 4

(DoS) Denial-of-Service

4 2 4

Wired Equivalent

WEP.
(WAP)

Wired Privacy Equivalent

Wireless Encryption Protocol Protocol

Service Set Identifier(SSID)-1-5

Beacon

SSID

SSID

SSID upfront

SSID .

SSID

SSID

SSID .[2]

<http://www.cirt.net>

SSID

Wired Equivalent Privacy(WEP) 2 5

WEP .

WEP

WEP .

WEP

WEP .

WEP

WEP

$$:[1]$$

WEP.

(1

40

(2

148

(3

WEP

WAP

WEP

WEP

WEP

"passphrase"

WAP

II

Wired Equivalent WEP
WEP .

The diagram illustrates the WEP (Wired Equivalent Privacy) encryption process, divided into two main parts: Key Derivation and Packet Structure.

Key Derivation Process

- Input:** A 40-bit RC4 key and a 128-bit Initialization Vector (IV).
- Process:** The 40-bit RC4 key and the 128-bit IV are combined to form a 168-bit WEP key.
- Output:** The 168-bit WEP key is used to encrypt the data.

Packet Structure

The diagram shows the structure of a WEP packet, which consists of the following fields:

- Header:** Contains the 24-bit IV and the 104-bit WEP key.
- Body:** Contains the encrypted data (128 bits).
- Footer:** Contains the 40-bit pass phrase.

The diagram also shows the process of cracking the WEP key, which involves analyzing the packet structure and the key derivation process.

¹EAP (7

session (8

(9

(10

7

8

9

[1]. NIST Special Publication 800-48, "Wireless Network Security".

.82 116 108

".[2]

.1382

. [3]

¹ Extensible Autentication Protocol(EAP)