ISBN: 979-756-061-6

SECURITY ON 802.11 WIRELESS LAN A COMPREHENSIVE COMPARISON

Wawan Indarto
Cisco Networking Academy Program
Jurusan Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia
Kampus Terpadu UII, Jl Kaliurang Km 14.5 Yogyakarta.
E-mail: wawan@fti.uii.ac.id

Abstract

Since the ratification of the IEEE 802.11b standard in 1999, wireless LANs have become more prevalent. Today, wireless LANs are widely deployed in places such as corporate office conference rooms, industrial warehouses, Internet-ready classrooms, and even coffeehouses.These IEEE 802.11-based wireless LANs present new challenges for network administrators and information security administrators alike. Unlike the relative simplicity of wired Ethernet deployments, 802.11-based wireless LANs broadcast radio-frequency (RF) data for the client stations to hear.[2] This presents new and complex security issues that involve augmenting the 802.11 standard.

***Keyword**: IEEE 802.11, WLAN, Security*

1. Introduction

Security in the IEEE 802.11 specification—which applies to 802.11b, 802.11a, and 802.11g—has come under intense scrutiny. Researchers have exposed several vulnerabilities in the authentication, data-privacy, and message-integrity mechanisms defined in the specification

2. 802.11 Authentication and Its Weaknesse

Wireless LANs, because of their broadcast nature, require the addition of[1]:

a. User authentication to prevent unauthorized access to network resources
b. Data privacy to protect the integrity and privacy of transmitted data

The 802.11 specification stipulates two mechanisms for authenticating wireless LAN clients: open authentication and shared key authentication. Two other mechanisms—the Service Set Identifier (SSID) and authentication by client Media Access Control (MAC) address—are also commonly used. This section explains each approach and its weaknesses.

The use of Wired Equivalent Privacy (WEP) keys can function as a type of access control because a client that lacks the correct WEP key cannot send data to or receive data from an access point. WEP, the encryption scheme adopted by the IEEE 802.11 committee, provides encryption with 40 bits or 104 bits of key strength. A subsequent section of this paper discusses WEP and its weaknesses in greater detail.

2.1 Service Set Identifier

The SSID is a construct that allows logical separation of wireless LANs. In general, a client must be configured with the appropriate SSID to gain access to the wireless LAN. The SSID does not provide any data-privacy functions, nor does it truly authenticate the client to the access point.

2.2 802.11 Station Authentication

Authentication in the 802.11 specification is based on authenticating a wireless station or device instead of authenticating a user. The specification provides for two modes of authentication: open authentication and shared key authentication.

The 802.11 client authentication process consists of the following transactions (Figure 1):

1. Client broadcasts a probe request frame on every channel
2. Access points within range respond with a probe response frame
3. The client decides which access point (AP) is the best for access and sends an authentication request
4. The access point will send an authentication reply
5. Upon successful authentication, the client will send an association request frame to the access point
6. The access point will reply with an association response
7. The client is now able to pass traffic to the access point

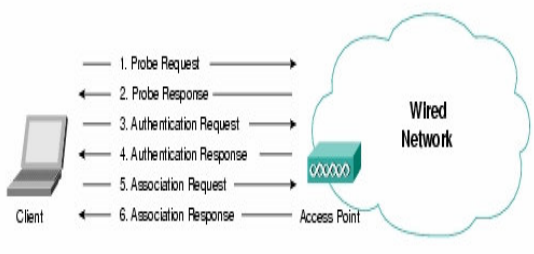

Figure 1. 802.11 Client Authentication Process

ISBN: 979-756-061-6

2.2.1 Probe Requests and Responses

Sinnce the client becomes active on the medium, it searches for access points in radio range using the 802.11 management frames known as probe request frames. The probe request frame is sent on every channel the client supports in an attempt to find all access points in range that match the SSID and client-requested data rates (Figure 2).

All access points that are in range and match the probe request criteria will respond with a probe response frame containing synchronization information and access point load. The client can determine which access point to associate to by weighing the supported data rates and access point load. Once the client determines the optimal access point to connect to, it moves to the authentication phase of 802.11 network access.

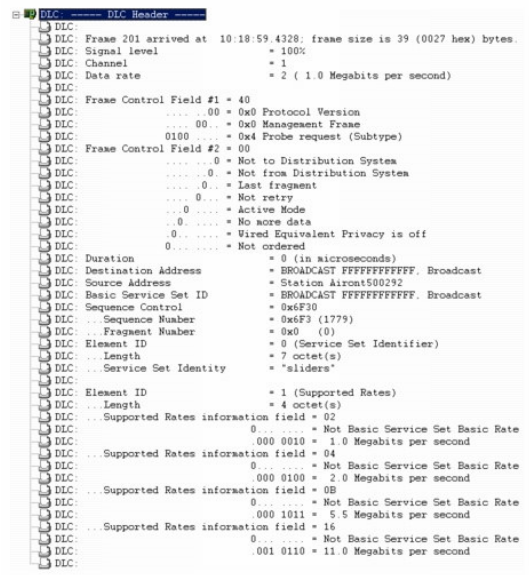

Figure 2. Probe Request Frame

Open authentication allows any device network access. If no encryption is enabled on the network, any device that knows the SSID of the access point can gain access to the network. With WEP encryption enabled on an access point, the WEP key itself becomes a means of access control. If a device does not have the correct WEP key, even though authentication is successful, the device will be unable to transmit data through the access point. Neither can it decrypt data sent from the access point (Figure 3).

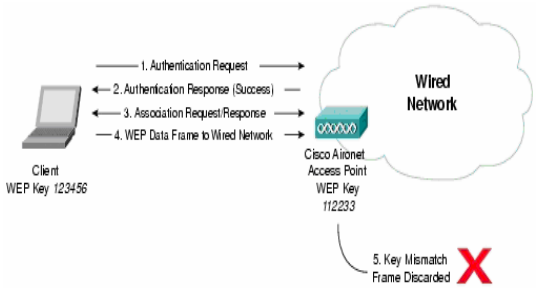

Figure 3. Open Authentication with Differing WEP Keys

2.2.3 Shared Key Authentication

Shared key authentication is the second mode of authentication specified in the 802.11 standard. Shared key authentication requires that the client configure a static WEP key. Figure 46 describes the shared key authentication process.

1. The client sends an authentication request to the access point requesting shared key authentication
2. The access point responds with an authentication response containing challenge text
3. The client uses its locally configured WEP key to encrypt the challenge text and reply with a subsequent authentication request
4. If the access point can decrypt the authentication request and retrieve the original challenge text, then it responds with an authentication response that grants the client access

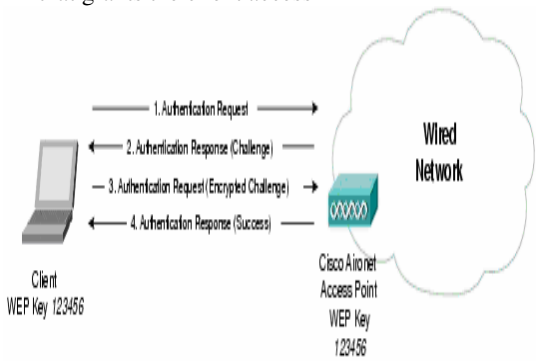

Figure 4. Shared Key Authentication Process

2.2.4 MAC Address Authentication

The SSID is advertised in plain-text in the access point beacon messages (Figure 8). Although beacon messages are transparent to users, an eavesdropper can easily determine the SSID with the use of an 802.11 wireless LAN packet analyzer, like Sniffer Pro. Some access-point vendors, including Cisco, offer the option to disable SSID broadcasts in the beacon messages. The SSID can still be determined by sniffing the probe response frames from an access point (Figure 9).

The SSID is not designed, nor intended for use, as a security mechanism. In addition, disabling SSID broadcasts might have adverse effects on Wi-Fi interoperability for mixed-client deployments.

ISBN: 979-756-061-6

Therefore, Cisco does not recommend using the SSID as a mode of security [3].

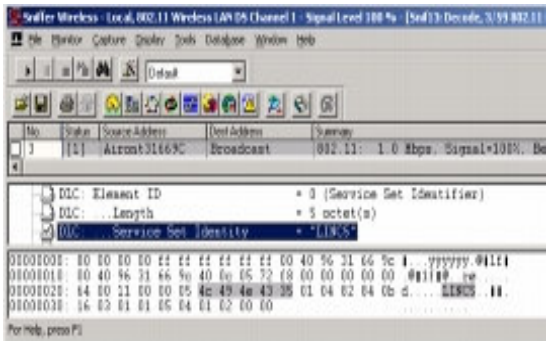

Figure 5. SSID in an Access Point Beacon Frame

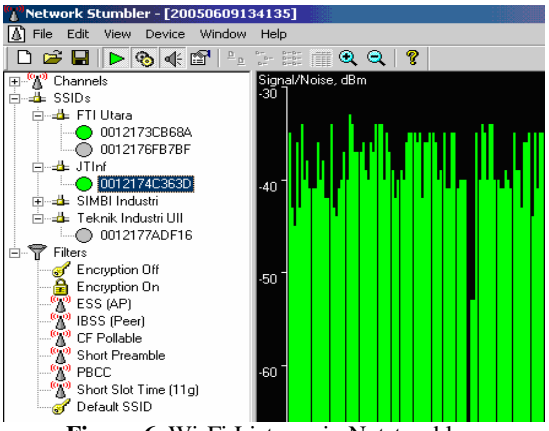

Figure 6. Wi-Fi Listener in Netstumbler

2.3.2 Open Authentication Vulnerabilities

Open authentication provides no way for the access point to determine whether a client is valid. This is a major security vulnerability if WEP encryption is not implemented in a wireless LAN. Cisco does not recommend deploying wireless LANs without WEP encryption. In scenarios in which WEP encryption is not needed or is not feasible to deploy, such as public wireless LAN deployments strong, higher-layer authentication can be provided by implementing a Service Selection Gateway (SSG).

2.3.3 Shared Key Authentication Vulnerablitis

Shared key authentication requires the client use a preshared WEP key to encrypt challenge text sent from the access point. The access point authenticates the client by decrypting the shared key response and validating that the challenge text is the same.

The process of exchanging the challenge text occurs over the wireless link and is vulnerable to a man-in-the-middle attack. An eavesdropper can capture both the plain-text challenge text and the cipher-text response. WEP encryption is done by performing an exclusive OR (XOR) function on the plain-text with the key stream to produce the cipher-text. It is important to note that if the XOR function is performed on the plain-text and cipher-text are XORed, the result is the key stream. Therefore, an eavesdropper can easily derive the key stream just by sniffing the shared key authentication process with a protocol analyzer (Figure 7).

2.3.4 MAC Address Authentication Vulnerabilities

MAC addresses are sent in the clear as required by the 802.11 specification. As a result, in wireless LANs that use MAC authentication, a network attacker might be able to subvert the MAC authentication process by "spoofing" a valid MAC address.

MAC address spoofing is possible in 802.11 network interface cards (NICs) that allow the universally administered address (UAA) to be overwritten with a locally administered address (LAA). A network attacker can use a protocol analyzer to determine a valid MAC address in the business support system (BSS) and an LAA-compliant NIC with which to spoof the valid MAC address.

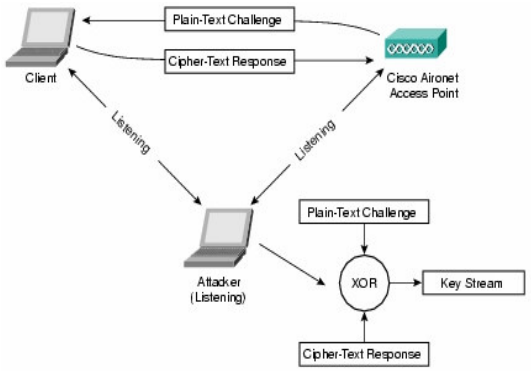

Figure 7. Vulnerability of Shared Key Authentication

3. WEP Encryption and Its Weaknesses

frWEP is based on the RC4 algorithm, which is a symmetric key stream cipher. As noted previously, the encryption keys must match on both the client and the access point for frame exchanges to succeed. The following section will examine stream ciphers and provide some perspective on how they work and how they compare to block ciphers.

3.1 Stream Ciphers and Block Ciphers

A stream cipher encrypts data by generating a key stream from the key and performing the XOR function on the key stream with the plain-text data. The key stream can be any size necessary to match the size of the plain-text frame to encrypt (Figure 8).

ISBN: 979-756-061-6

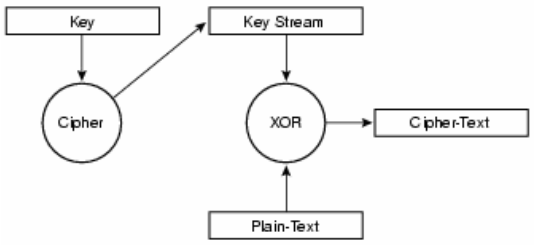

Figure 8. Stream Cipher Operation

Block ciphers deal with data in defined blocks, rather than frames of varying sizes. The block cipher fragments the frame into blocks of predetermined size and performs the XOR function on each block. Each block must be the predetermined size, and leftover frame fragments are padded to the appropriate block size (Figure 9). For example, if a block cipher fragments frames into 16 byte blocks, and a 38-byte frame is to be encrypted, the block cipher fragments the frame into two 16-byte blocks and one six-byte block. The six-byte block is padded with 10 bytes of padding to meet the 16-byte block size.

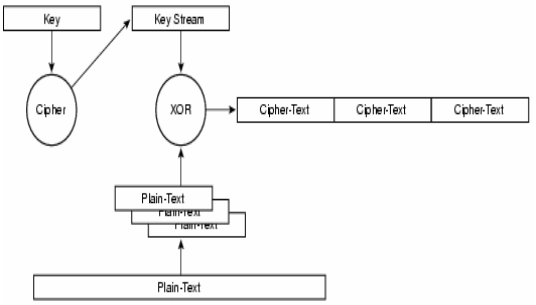

Figure 9. Block Cipher Operation

The process of encryption described above for stream ciphers and block ciphers is known as Electronic Code Book (ECB) mode encryption. With ECB mode encryption, the same plain-text input always generates the same cipher-text output. As Figure 10 illustrates, the input text of "FOO" always produces the same cipher-text. This is a potential security threat because eavesdroppers can see patterns in the cipher-text and start making educated guesses about what the original plain-text is.

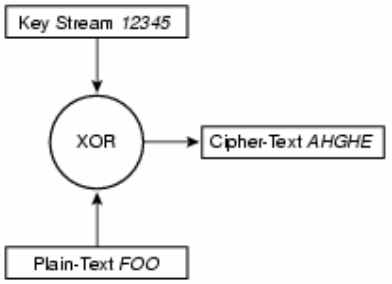

Figure 10. Electronic Code Book Encryption

There are two encryption techniques to overcome this issue: Initialization vectors and Feedback modes

3.1.1 Initialization Vectors

An initialization vector (IV) is used to alter the key stream. The IV is a numeric value that is concatenated to the base key before the key stream is generated. Every time the IV changes, so does the key stream. Figure 11 shows the same plain-text "FOO" with the XOR function performed with the IV augmented key stream to generate different cipher-text. The 802.11 standard recommends that the IV change on a per-frame basis. This way, if the same packet is transmitted twice, the resulting cipher-text will be different for each transmission

The IV is a 24-bit value (Figure 11) that augments a 40-bit WEP key to 64 bits and a 104-bit WEP key to 128 bits. The IV is sent in the clear in the frame header so the receiving station knows the IV value and is able to decrypt the frame (Figure 12). Although 40-bit and 104-bit WEP keys are often referred to as 64-bit and 128-bit WEP keys, the effective key strength is only 40 bits and 104 bits, respectively, because the IV is sent unencrypted.

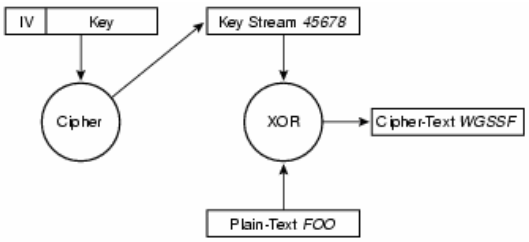

Figure 11. Encryption with an Initialization Vector

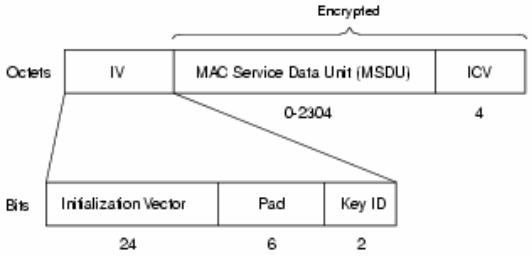

Figure 12. Initialization Vector in a WEP-Encrypted Frame

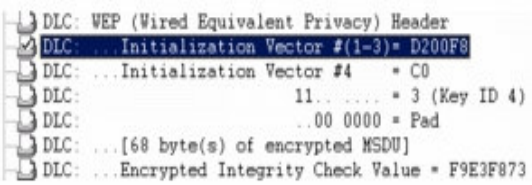

Figure 12. Initialization Vector in an 802.11 Protocol Decode

 ISBN: 979-756-061-6

3.1.2 Feedback Modes

Feedback modes are modifications to the encryption process to prevent a plain-text message from generating the same cipher-text during encryption. Feedback modes are generally used with block ciphers, and the most common feedback mode is known as cipher block chaining (CBC) mode.

The premise behind CBC mode is that a plain-text block has the XOR function performed with the previous block of cipher-text. Because the first block has no preceding cipher-text block, an IV is used to change the key stream.

3.2 Statistical Key Derivation—Passive Network Attacks

An August 2001, cryptanalysts Fluhrer, Mantin, and Shamir determined that a WEP key could be derived by passively collecting particular frames from a wireless LAN. The vulnerability is how WEP has implemented the key scheduling algorithm (KSA) from the RC4 stream cipher. Several IVs (referred to as weak IVs) can reveal key bytes after statistical analysis. Researchers at AT&T/Rice University as well as the developers of the AirSnort application implemented this vulnerability and verified that WEP keys of either 40- or 128-bit key length can be derived after as few as 4 million frames. For high-usage wireless LANs, this translates to roughly four hours until a 128-bit WEP key is derived.

This vulnerability renders WEP ineffective. Using dynamic WEP keys can mitigate this vulnerability, but reactive efforts only mitigate known issues. To eliminate this vulnerability, a mechanism that strengthens the WEP key is required.

3.3 Inductive Key Derivation—Active Network Attacks

Inductive key derivation is the process of deriving a key by coercing information from the wireless LAN and is also referred to as an active network attack. As mentioned in the section on stream ciphers, encryption is accomplished by performing the XOR function with the stream cipher to produce the cipher-text. Inductive network attacks work on this premise.Man-in-the-middle attacks, a form of inductive key derivation attack, are effective in 802.11 networks because of the lack of effective message integrity. The receiver of a frame cannot verify that the frame was not tampered with during its transmission. In addition, the Integrity Check Value (ICV) used to provide message integrity is based on the 32-bit cyclic redundancy check (CRC32) checksum function. The CRC32 value is vulnerable to bit-flipping attacks, which render it ineffective. With no effective mechanism to verify message integrity, wireless LANs are vulnerable to man-in-the-middle attacks, which include bit-flipping attacks and IV replay attacks.[8]

3.3.1 Initialization Vector Replay Attacks

The initialization vector (IV) replay attack is a network attack that has been practically implemented, not just theorized. Although various forms of the network attack exist, the one that clearly illustrates its inductive nature is described below and illustrated in Figure 14:

1. A known plain-text message is sent to an observable wireless LAN client (an e-mail message)
2. The network attacker will sniff the wireless LAN looking for the predicted cipher-text
3. The network attacker will find the known frame and derive the key stream
4. The network attacker can "grow" the key stream using the same IV/WEP key pair as the observed frame

This attack is based on the knowledge that the IV and base WEP key can be reused or replayed repeatedly to generate a key stream large enough to subvert the network.

Once a key stream has been derived for a given frame size, it can be "grown" to any size required. This process is described below and illustrated in Figure 15:

1. The network attacker can build a frame one byte larger than the known key stream size; an Internet Control Message Protocol (ICMP) echo frame is ideal because the access point solicits a response
2. The network attacker then augments the key stream by one byte
3. The additional byte is guessed because only 256 possible values are possible
4. When the network attacker guesses the correct value, the expected response is received: in this example, the ICMP echo reply message
5. The process is repeated until the desired key stream length is obtained.

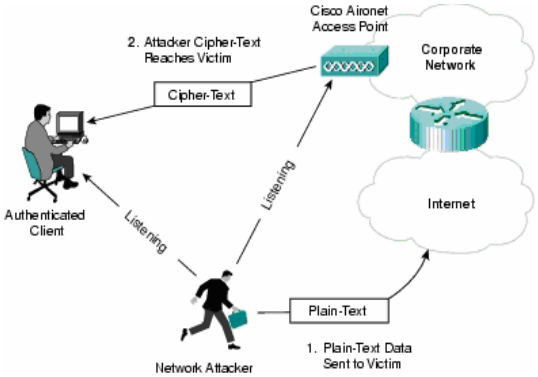

Figure 14. Initialization Vector Reuse Vulnerability

ISBN: 979-756-061-6

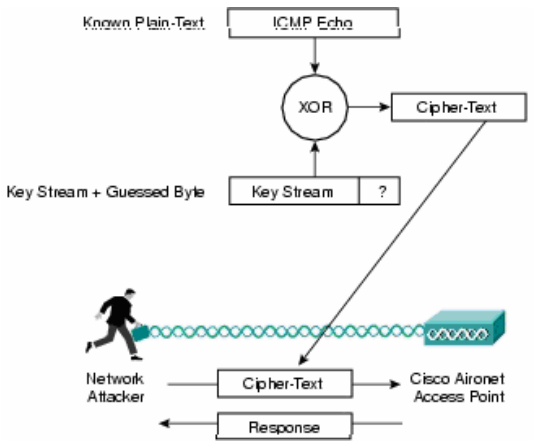

Figure 15. "Growing" a Key Stream

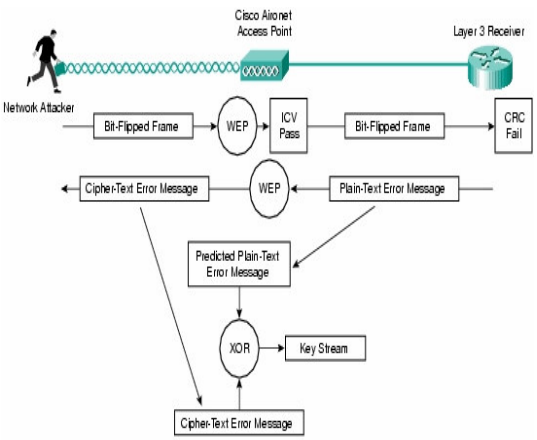

Figure 17. Bit-Flipping Attack

3.3.2 Bit-Flipping Attacks

Bit-flipping attacks have the same goal as IV replay attacks, but they rely on the weakness of the ICV. Although the data payload size may vary, many elements remain constant and in the same bit position. The attacker will tamper with the payload portion of the frame to modify the higher layer packet. The process for a bit-flipping attack is listed below and in Figure16:

1. The attacker sniffs a frame on the wireless LAN
2. The attacker captures the frame and flips random bits in the data payload of the frame
3. The attacker modifies the ICV (detailed later)
4. The attacker transmits the modified frame
5. The receiver (either a client or the access point) receives the frame and calculates the ICV based on the frame contents
6. The receiver compares the calculated ICV with the value in the ICV field of the frame
7. The receiver accepts the modified frame
8. The receiver de-encapsulates the frame and processes the Layer 3 packet
9. Because bits are flipped in the layer packet, the Layer 3 checksum fails
10. The receiver IP stack generates a predictable error
11. The attacker sniffs the wireless LAN looking for the encrypted error message
12. Upon receiving the error message, the attacker derives the key stream as with the IV replay attack.

The basis for this attack is the failure of the ICV. The ICV is in the WEP-encrypted portion of the frame, so how is the attacker able to modify it to match the bit-flipped changes to the frame? The process of flipping bits is:

1. A given frame (F1 in Figure 18) has an ICV (C1)
2. A new frame is generated (F2) the same length as F1 with bits set
3. Frame F3 is created by performing the XOR function F1 and F2
4. The ICV for F3 is calculated (C2)
5. ICV C3 is generated by performing the XOR function C1 and C2.

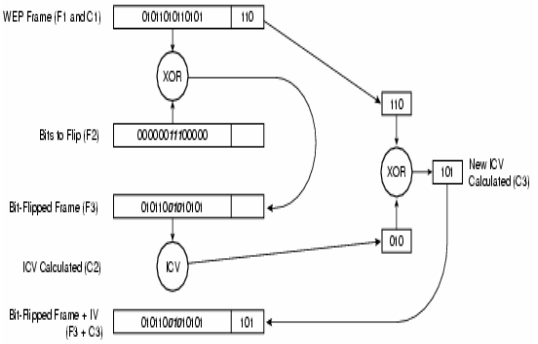

Figure 18. Bit flipping attack resolve

3.4 Static WEP Key Management Issues

The 802.11 standard does not specify key management mechanisms. WEP is defined to support only static, preshared keys. Because 802.11 authentication authenticates a device and not the user of the device, the loss or theft of a wireless adapter becomes a security issue for the network. The loss of an adapter and the compromising of the existing key presents network administrators with the tedious task of manually rekeying all wireless devices in the network.

This task might be acceptable for small deployments but is not realistic in midsize and large deployments in which the number of wireless users

ISBN: 979-756-061-6

can reach into the thousands. Without a mechanism to distribute or generate keys, administrators must watch wireless NICs closely.

References

[1] Indarto, Wawan, *Lecture Handout: Computer Security System*, Informatic Department, Islamic University of Indonesia, 2003.
[2] Indarto, Wawan, *Lecture Handout: Computer Network*, Informatic Department, Islamic University of Indonesia, 2005.
[3] Indarto, Wawan, *Computer Network–Outdoor Practical Lab. Handout: CAN Antenna and Home Made Antenna for 2.4 Ghz*, Informatic Department, Islamic University of Indonesia, 2005.
[4] Steven, W. Richard, *TCP/IP Illustrated*, Addison Wesley 1994
[5] Chapman, D. Brent, Elizabeth DZ., *Building Internet Firewalls*, O'Reilly 1995
[6] Stallings, William, *Cryptography and Network Security*, Pearson Education 2004.
[7] Nelson, Mark, *The Data Compression Book*, M&T Books 1996
[8] Cisco, Inc, *Cisco Security Suite*, Cisco 2005.
[9] http://cisco.netacad.net