Wi-Fi Security

Stewart S. Miller

McGraw-Hill
New York Chicago San Francisco Lisbon
London Madrid Mexico City Milan New Delhi
San Juan Seoul Singapore Sydney Toronto

CHAPTER 4

Issues in Wireless Security

This chapter presents an assessment of wireless security with focus on the effective response to the three primary issues noted below:

- Is the data adequately protected from compromise during transmission?
- Is access to the transmission and other information on the network controlled?
- Is there adequate protection from the range of DoS attacks?

The specific features of the RF transmission involved are also an issue since emanations are accessible to unintended recipients:

- What frequencies are available?
- How much transmitter power is required to ensure successful receipt?

We examine how security is applied in the wireless LAN and determine how these issues affect your environment. The idea is to see what pertains to your setup so that you can understand and effectively deal with these issues in your wireless security before they become a problem.

The State of Wireless LAN Security

In order to convince you that there are real issues to consider when implementing your WLAN, it is important to focus on the integrated security features present within 802.11b and their limitations.

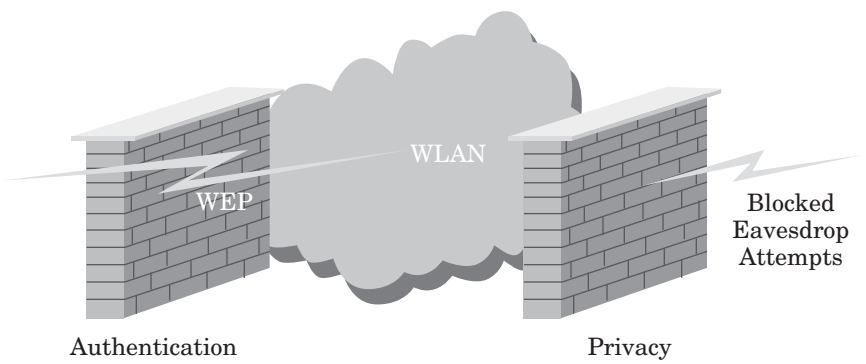
802.11b offers features and functionality that provide you with greater security in your wireless environment, however these security services are enabled for the most part through the wired equivalent privacy (WEP) mechanism to protect you at the link level during wireless transmissions that take place between the client and the access point. Note that WEP is not able to offer end-to-end security, but it does attempt to secure the actual radio transmission by encrypting the data channel.

Securing Your WLAN

The most important issue when dealing with wireless security is to consider the fundamental security mechanisms in your wireless network. There are two primary means of adding security to your environment (Figure 4.1):

1. **Authentication**—This mechanism has the objective of using WEP to enable your security to be verified by determining the actual information that defines each wireless workstation. It is necessary to yield access control to the network by restricting wireless workstation access to those clients who can properly authenticate themselves to the server.
2. **Privacy**—WEP maintains an effective level of privacy when dealing with security for the data communication channels in your wireless network. It attempts to stop information from being "hacked" by attackers trying to eavesdrop on your data transmissions. The objective is to make certain that messages are not altered while moving from the wireless workstation to the access point or server. Essentially, this is the means that enables you to trust your information so that you can be reasonably certain your information is secure and reliable.

Figure 4.1
Securing your WLAN.



Authenticating Data

When a wireless user attempts to acquire access to your wired network infrastructure, there are two ways in which access can be obtained:

1. **Open system**—Any user in range of the access point can roam onto the system (as long as the router is not set up to filter out the unique MAC address of wireless workstations that are not supposed to have access).
2. **Encrypted system**—All data is scrambled and access barriers are put into place so that a hacker cannot eavesdrop on your data (Figure 4.2).

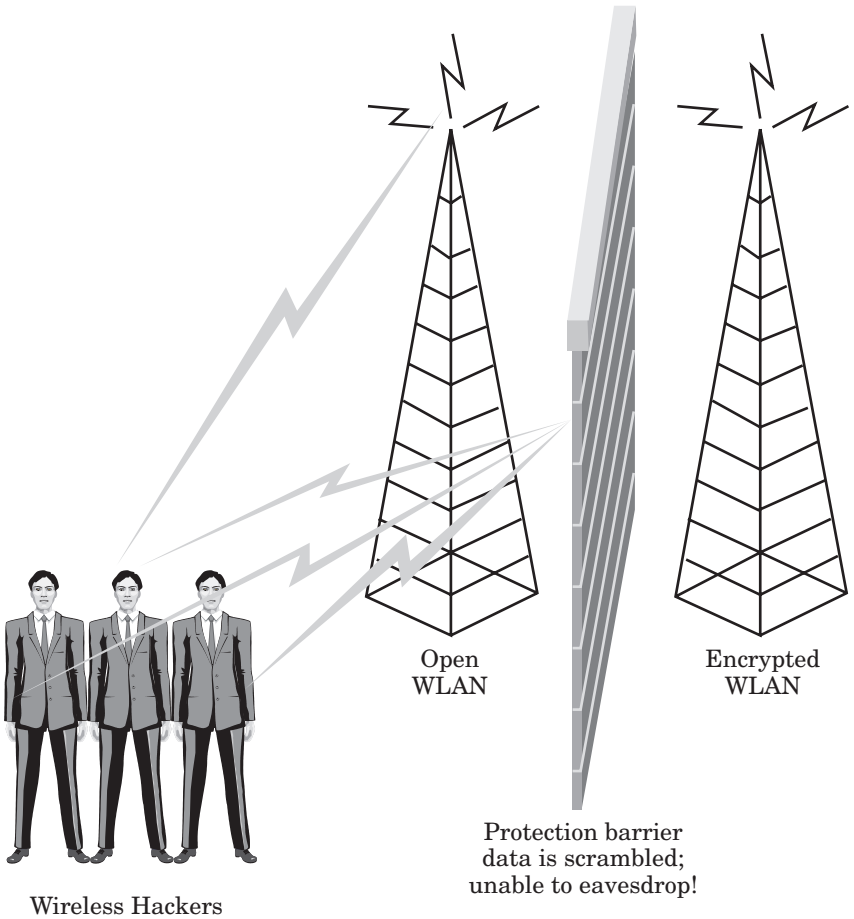


Figure 4.2
Protecting barrier safeguards network data.

In an open system without encryption, a wireless workstation can join your WLAN by using identity types of verification methods. The actual access request in an open environment occurs when the wireless server replies with the service set identifier (SSID) for the WLAN. This means there isn't any actual authentication taking place; the wireless workstation simply roams onto the network.

In contrast, you can see the differences spelled out between an open versus closed system:

	Open System	**Closed System**
Encryption	Nothing	RC4
Authentication	No SSID	SSID

Because of the unique SSID set for a company, many people believe that nobody could actually roam onto a network without knowing what unique identifier defined the network. In fact, it is possible for a wireless user to leave the SSID as "NULL" or blank; then when he is in range of the access point, the wireless workstation automatically finds and logs into the network. This means that basic systems of authentication are not sufficient to protect your network. This is why a combination of encryption and authentication is important in implementing your wireless security—but this still represents a small part of what needs to be done to provide a truly secure WLAN.

Client Authentication in a Closed System

In the previous section we saw that when a wireless workstation replies to the access point with a null or empty string in place of the actual SSID, it is automatically authenticated into the open system. However, when working in a closed authentication environment, the wireless workstation must reply with the exact SSID in order to log into the wireless network. The client is only granted access if it replies with the exact SSID string that identifies the client to the server.

Shared Key Authentication

The shared key authentication encryption mechanism uses the "challenge-response" mechanism. The idea is that each wireless client has an understanding of what is commonly referred to as a "shared secret."

The access point creates a random type of challenge that is transmitted to the wireless workstation. The wireless workstation then uses the encryption or WEP key it shares with the access point. The challenge is itself encrypted and then replies with the answer to the access point, which then deciphers that answer sent by the client. Based on the result, the client is granted access only if the deciphered answer is the same expected value as the random challenge.

RC4

Data is encrypted using the RC4 cipher. Note that the wireless workstation does not authenticate the access point, so that there is no verifiable

means to make certain that the client is effectively talking to an authorized access point on the WLAN.

The problem is that it is possible for attacks to occur when hackers attempt to "spoof" authorized access points in order to "trick" wireless workstations or mobile users into inadvertently connecting to the hacker's access point, thus compromising the wireless network and stealing important information.

Ensuring Privacy

In dealing with security and privacy so much in my career, I once learned the mantra that "A security solution *without* ensuring privacy is *not a solution at all*!"

As we concentrate on the issues pertinent in wireless security, it is imperative to deal with the issue of privacy. The 802.11 standard can deal with privacy issues through using cryptographic mechanisms in its wireless connectivity.

The WEP mechanism ensures privacy through its use of the RC4 symmetric-key cipher algorithm to create a pseudorandom data sequence. WEP makes it possible for data to be protected from interception (or really understood) between transmission points along the wireless network (Figure 4.3). WEP is useful for all data in the WLAN, to protect and make your data channel private. The idea is to protect data when flowing through:

- Transmission control protocol/Internet protocol (TCP/IP)
- Internet packet exchange (IPX)
- Hyper text transfer protocol (HTTP)

WEP is designed to permit privacy by supporting cryptographic keys ranging in size from 40 to 104 bits. The idea is that by increasing the size of the key, you proportionally increase your level of security. For example, a secure setup includes a 104-bit WEP key using 128-bit RC4.

In practice, when you employ a key size in excess of 80 bits, it makes brute force hacker attacks very lengthy, time consuming, and generally unrealistic as a form of breaking into a network without being detected. In fact, with 80-bit keys, the number of possible keys is so great that even the most powerful computers produced today would not be powerful enough to break the code.

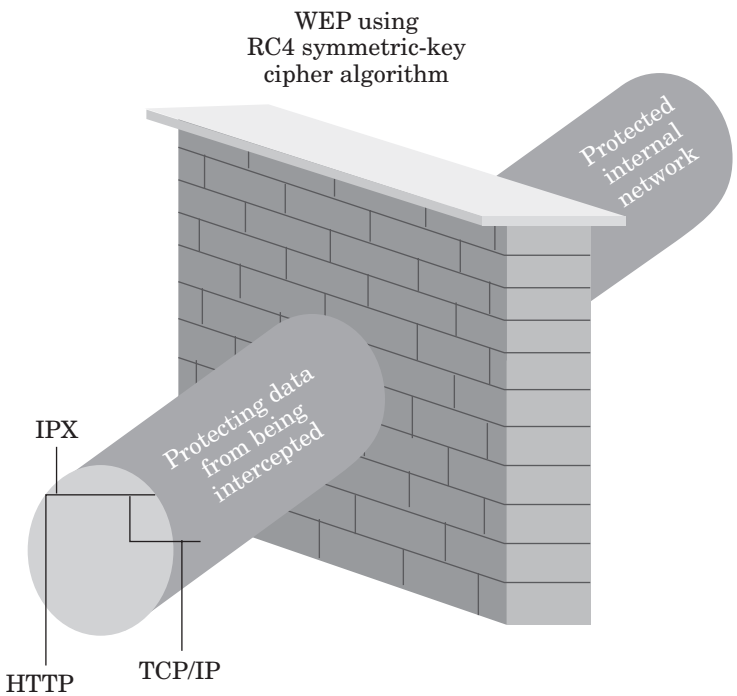


Figure 4.3
Protected network data in transit.

Unfortunately, in my experience, most companies don't use these keys for even the simplest form of protection on their network. Most WLAN implementations use only 40-bit keys. Most hacker attacks are successful on implementations that use 40-bit WEP keys; the majority of WLANs are at serious risk of being compromised.

Keeping Data Intact

One of the advantages of 802.11b is that it ensures that your data transmission remains intact as it follows the wireless path between the wireless workstation and the access point. The idea of this level of security is to reject any message transmission that may have been modified or intentionally altered during its path from point to point.

To maintain privacy, the 802.11 standard was designed specifically to reject any message altered in transit, either by accident or by design. To ensure that data privacy has been maintained, the cyclic redundancy check (CRC) technique is used as a form of encryption. This setup requires that each encrypted packet is "sealed" in a bubble using the

RC4 key encryption to scramble the transmission. Only when the packets are received are they decrypted; a CRC check is computed to ensure that it matches the CRC value before it was sent. Should the CRC value not match, then you have a receive error that defines an integrity violation and the packet is thrown away as corrupt.

Managing Keys

One of the problems with the 802.11 standard is that it has no good way of managing keys (Figure 4.4). The administrators who take care of your wireless network are responsible for several methods of managing keys with respect to:

- Creating keys
- Distributing keys among wireless users
- Archiving/storing keys so that they don't fall into the hands of a hacker
- Auditing who has what cryptographic keys
- Terminating keys that have become compromised

What happens if nobody takes care of these key management issues? Your wireless network is highly vulnerable to a hacker attack. These insecurities include:

- WEP keys are not unique and can be compromised
- Factory default passwords are prominently posted on hacker sites. This means that no matter which access point you are using, you are *vulnerable* if you have left your default administrative password unchanged since deploying your WLAN.
- Bad keys. Never make a key all zeros or all ones for the sake of convenience. Those types of keys are the first detected by a hacker looking to see how easy it will be to gain access to your wireless network.
- Factory defaults must always be changed as they are the easiest and simplest ways for a hacker to gain access.

The greatest difficulty is that the problem with managing keys grows in proportion with the size of your organization and the number of keys you will need to keep track of your wireless workforce.

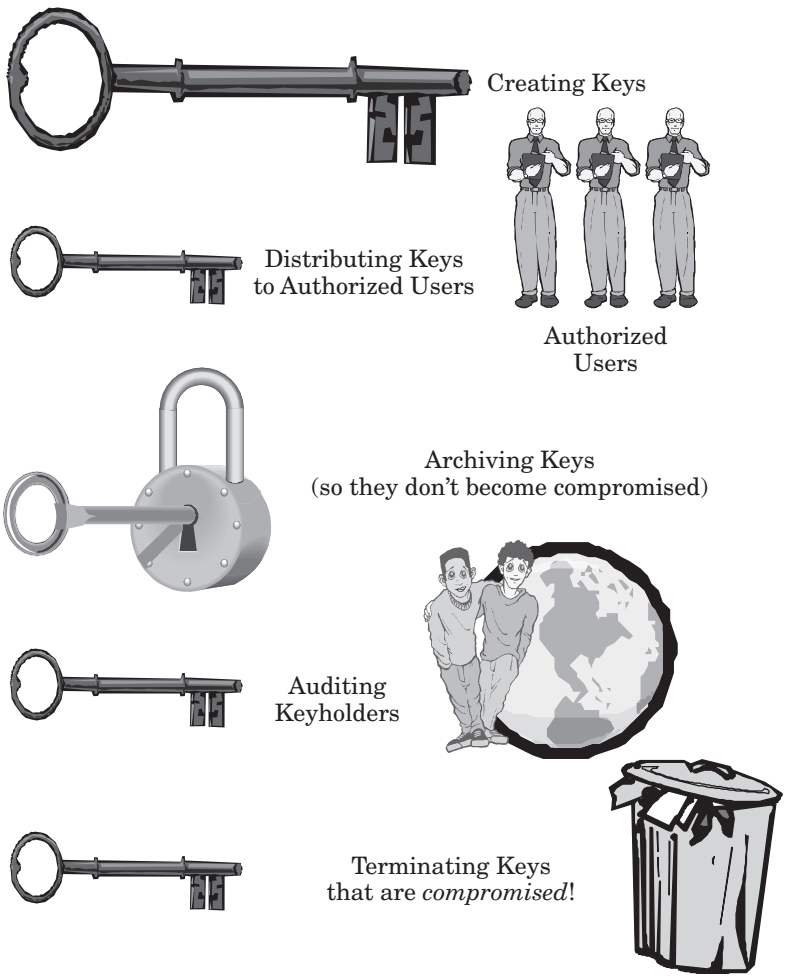


Figure 4.4
Key management.

To indicate how extensive the task of managing keys actually is, consider that it is very difficult to scale your organization to change keys often enough to randomize them sufficiently to protect you against a hacker attack. In a large environment, you could be dealing with tens of thousands of keys.

In essence, vigilance and time are required, besides the fact that you must know how to protect your WLAN through the effective management of your encryption keys.

WLAN Vulnerabilities

There are a number of security vulnerabilities in 802.11 that have unfortunately been discovered by malicious hacker exploits. These vulnerabilities constitute passive types of attacks that are designed to decrypt traffic with respect to algorithms based on statistical analysis and active attacks designed to decipher network traffic. An active attack is basically accomplished by confusing the access point to give up to the attacker information it should not. This is the reason why default passwords and settings should always be changed as soon as you deploy your WLAN.

The most significant problem rests with WEP, which was itself designed to make a wireless network nearly as secure as the wired Ethernet. The biggest problems result from using the same WEP key over and over again. The more you use the same keys, the greater the chance an attacker will learn this piece of information so that he might ultimately use it against you for the purpose of accessing your WLAN. The vulnerability here rests in the fact that the same key is used for extended time periods, and nobody really thinks to change it. When you think of a WEP key, you should remember to change the key as often as you might change your logon password.

The *initialization vector* (IV) constitutes the 24-bit field transmitted in clear text as part of WEP. This 24-bit information initializes the RC4 algorithm key string. The IV is basically a short field used for encryption.

The IV is meant to protect your information, but a short IV ultimately gets repeated many times over the network when there is a great deal of traffic. The problem is that an attacker may easily use this information to intercept your wireless data channel, find your key stream, and then use this information to decipher the encrypted data on your WLAN.

Since the IV is actually an element from the RC4 encryption key, once the hacker has intercepted this bit of information and can intercept every packet key. Since the RC4 key is weak in and of itself, this could indicate the precursor of a significant attack. In fact, this attack could easily be run a script kiddie because once the secret key is recovered, it is possible to analyze only a small portion of the wireless network traffic and be able to have full access to the WLAN.

There isn't any protection for the actual composition of the encryption that WEP has to offer except that the MAC portion of the 802.11 standard uses the CRC element described earlier as a form of privacy protection.

Subtle Attacks

Another problem possible on your 802.11 WLAN is a WEP attack where a hacker initiates an active attack while simultaneously deciphering data channel packets by altering their information and CRC and then transmitting these altered bits of information back to the access point.

There is a great deal of risk associated with the creation of encryption protocols that do not possess a cryptographic privacy protection mechanism due to the communication necessary with several other protocol levels that can leak information about your encrypted data.

Common Security Pitfalls

Knowing the most common problems with WLAN security as it relates to the 802.11 standard can help you find and solve the problems with your implementation before they become vulnerabilities that hackers can exploit to your disadvantage.

Poor Security, Better than No Security at All!

The most common problem is that the security controls in your wireless equipment are turned off by default out of the box. Although these security features and functions are not all-encompassing to stop hackers, leaving them disabled just puts you at unjustified risk. Better that you should have minimal security measures as opposed to having no security enabled.

Short Keys

Most cipher keys are very short; most implementations use only 40-bit encryption keys, which can make the key stream repeat. There is no reason why you should not at least use larger key sizes when employing encryption techniques. To that end, a key size should be at least 80 bits long. When using longer keys, the likelihood of having them compromised by a hacker is far less. Hackers use “brute force” attacks that basically try all possible combinations of usernames and passwords to

"force" their way into your WLAN. When you make the hacker's job much longer and more difficult, there is a greater likelihood you will catch the intrusion attempt and resolve your network vulnerability.

Initialization Vectors

Repetition is bad because it makes it easier for hackers to decipher the data channel for the average LAN. Initialization vectors make the cipher stream repeat, and it is that very repetition that creates vulnerability in your WLAN.

Shared Keys

One of the methods meant for protecting your WLAN is the element that can be most easily compromised. "Shared" cipher keys by their very definition constitute a vulnerability because they can be "shared" with hackers as well as legitimate employees. The entire basis of maintaining security is highly dependent on keeping these keys secret and in the possession of authorized users only.

In the previous section we saw that hackers often try every possible username and password combination in order to try and "force" access privileges into your WLAN. Your encryption keys must be changed often, otherwise you have very little means to protect yourself against a hacker attack.

WEP uses the RC4 keys, but their deployment is poor at best due to the fact that a hacker can sometimes intercept the key just by examining the first few packets. (There are a number of other programs that do not have the same RC4 vulnerabilities; they do not leak the key schedule in each packet transmission.) Although this type of interception is often used by more advanced hackers, in fact there a number of automated means that have made this type of attack much more accessible to almost anyone interested in a simple point-and-click interface to run scripts to intercept information pertaining to your wireless network.

Checks and Balances for Packets

It is essential to maintain the privacy and substance of each packet during wireless transmission handled by cyclic redundancy checks. However,

CRC is not always sufficient to maintain the substance of the encrypted packets because it is quite possible for someone to intercept and modify the data channel. This means that these types of protection mechanisms are not sufficient to protect your WLAN from a hacker attack.

Using encryption enables you to protect yourself so that you do not become an easy target for a hacker attack. If you use protocols that do not employ encryption, you are leaving yourself open to a cryptographic attack on your WLAN.

Authentication

Accessing the network need not necessarily depend on trying to crack the access codes; it could be done by something as simple and easy as stealing the actual wireless network interface card already configured with its unique MAC address to access the wireless network.

In the vast majority of WLANs, no authentication is actually taking place. At a minimal level, only verification that the wireless device is set to use the proper SSID occurs. Systems that screen out devices based on identity are highly vulnerable because it is a simple and easy matter to "spoof" or fake the identity of your wireless device based on the SSID. Sometimes you only require just that piece of information to log into the wireless network. How secure is that?

Authenticating the device often relies on the simplest form of "shared key challenge response" mechanism. The attack most common in this type of authentication is the hacker who is between the wireless workstation and the access point using challenge response authentication mechanisms that proceed in one direction only. However, an added level of protection is possible when authentication occurs on both sides in order to verify that both the users and network are authorized to use the network resources.

Location! Location! Location!

The 802.11 standard has become enormously popular in a diverse number of implementations including hospitals, airports, retail outlets, and businesses.

The attacks, however, are growing significantly, so that having a wireless network is almost a guarantee that your private information

will leak out to the hacker world. The significant risks in wireless security include:

- Privacy attacks
- Data substance and integrity
- Wireless network availability

Attack Patterns

Wireless attacks are either active or passive, as shown in Figure 4.5.

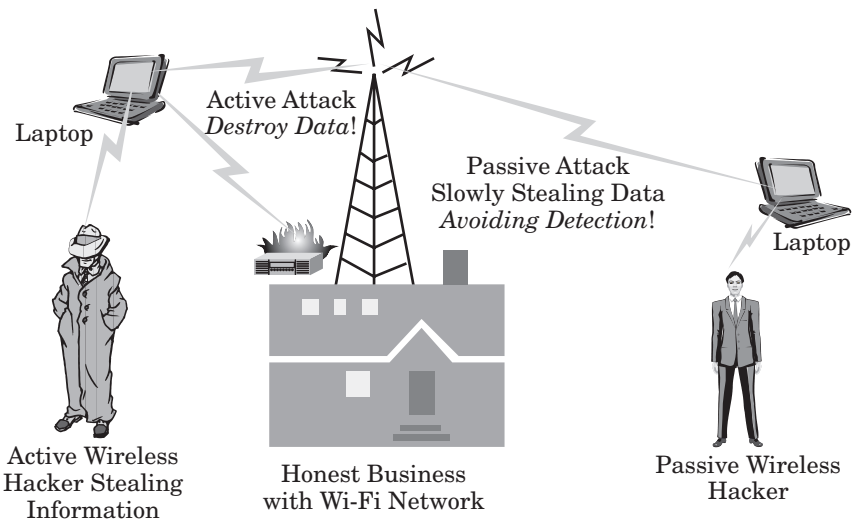


Figure 4.5
Active versus passive attack patterns.

Active Attack Patterns

An active attack constitutes a pattern where a hacker attempts to modify your data channel, messages, or files. With constant vigilance you will be able to catch this type of attack; however it is difficult to prevent this type of attack without actually pulling the plug of your WLAN.

Active attacks include: denial of service (DoS) and message alteration.

Denial of service attacks A DoS or distributed denial of service (DDoS) is an active attack pattern that prevents legitimate users from using their wireless network. There are a number of risks because these

attacks prevent local and remote users from using your network resources. Besides the problems with destroying your network connectivity, you also lose business opportunities, revenue, and good public opinion.

Message alteration In this type of attack, the hacker alters the real message by either adding, erasing, or changing the sequence of the message. This removes the trust factor of your message and makes all your traffic unusable.

Passive Attacks

In these attacks, an unauthorized user acquires access to your network data sources. There is no alteration of message content, but it is possible to eavesdrop on the transmission. Passive attacks are meant not to disrupt, but to acquire information flowing across your wireless network.

Replay In this type of passive attack, the hacker intercepts or eavesdrops on your data channel. The hacker does not do anything to compromise your systems at first, but can resend altered messages to an authorized user pretending to be the system host.

Eavesdropping This is a passive attack in which the hacker listens to all your network transmissions in an effort to acquire information flowing from one wireless workstation to the access point.

Traffic analysis The hacker analyzes your traffic pattern through this type of passive attack to determine what network patterns exist. He can then use all the information acquired to gain information about the traffic from each user on your wireless network.

Conclusion

It is understandable that the nature of the wireless LAN makes it fraught with a number of wireless security risks.

Most WLAN devices come out of the box having no actual means of security to protect them against hackers. It is the responsibility of every user to ensure (as much as humanly possible) that the best possible safety precautions have been taken so that your systems are shored up

against the most common problems, such as changing default values and passwords.

If you are mindful of your environment and wireless transmissions, you can effectively protect your systems against attack and ensure your WLAN is as secure as it possibly can be in the face of new hacker attacks.