**Security Issues in Wireless Systems**

**The Need for Wireless Network Security**

A wireless local area network is a flexible data communication system implemented as an extension to or as an alternative to the wired local area network. Wireless LANs transmit and receive the data over the air using the radio frequency technology, thus minimizing wired connections. Thus, wireless LANs combine data connectivity with user mobility. Wireless LANs have gained strong popularity in a number of vertical markets and these industries have profited from the productivity gains of using hand held terminals and notebook computers to transmit real-time information to centralized hosts for processing. Today, wireless LANs are becoming more widely recognized as a general-purpose connectivity alternative for a broad range of business customers. But one of the scariest revelations is that wireless LANs are insecure and the data sent over the them can be easily broken and compromised. The security issue in wireless networks is much more critical than in wired networks. Data sent on a wireless system is quite literally broadcast for the entire world to hear. Therefore, unless some serious countermeasures are taken, wireless systems should not be used in situations where critical data is sent over the airwaves. Any computer network, wireless or wireline, is subject

to substantial security risks. The major issues are [1–3]: (a) threats to the physical security of the network; (b) unauthorized access by unwanted parties; and (c) privacy.

A certain level of security is a must in almost all local area networks, regardless of whether they are wireless or wireline-based. There is no LAN owner who wants to risk having the LAN data exposed to unauthorized users or malicious attackers. If the data carried in the networks are sensitive, such as that found on the networks of financial institutions and banks, and e-commerce, e-government, and military networks, then extra measures must be taken to ensure confidentiality and privacy.

This chapter deals with various security issues related to wireless LANs including those that have been implemented in the IEEE 802.11 standard.

**Attacks on Wireless Networks**

The dependence of people on computer networks including wireless networks has increased tremendously in recent years and many corporations and businesses rely heavily on the effective, proper and secure operation of these networks. The total number of computer networks installed in most organizations has increased at a phenomenal rate. Corporations store sensitive and confidential information on marketing, credit records, income tax, trade secrets, national security data, and classified military data, among others.

Attacks on computer systems and networks can be divided into passive and active attacks . Active attacks involve altering data or creating fraudulent streams. These types of attacks can be divided into the following subclasses: (a) masquerade; (b) reply; (c) modifica-tion of messages; and (d) denial of service. A masquerade occurs when one entity pretends to be a different entity. For example, authentication can be collected and replayed after a valid authentication sequence has taken place. Reply involves the passive capture of a data unit and its subsequent retransmission to construct unwanted access. Modification of messages means that some portion of a genuine message is changed or that messages are delayed or recorded to produce an unauthorized result.

Passive attacks are inherently eavesdropping or snooping on transmission. The attacker tries to access information that is being transmitted. There are two subclasses: release of message contents, and traffic analysis. In the first type, the attacker reaches the e-mail messages or a file being transferred. In traffic analysis type of attack, the attacker could discover the location and identity of communicating hosts and could observe the frequency and length of encrypted messages being exchanged.

In general, passive attacks are difficult to detect, however, there are measures that can be used to avoid them. On the other hand, it is difficult to prevent active attacks.

The main categories of attack on wireless computer networks are :

* Interruption of service. Here, the resources of the system are destroyed or become unavail-able.
* Modification. This is an attack on the integrity of the system. In this case, the attacker not

only gains access to the network, but tampers with data such as changing the values in a database, altering a program so that it does different tasks.

* Fabrication. This is an attack on the authenticity of the network. Here the attacker inserts counterfeit objects such as inserting a record in a file.
* Interception. This is an attack on the confidentiality of the network such as wiretapping or eavesdropping to capture data in a network. Eavesdropping is easy in a wireless network environment since when one sends a message over a radio path, everyone equipped with the proper transceiver equipment in the range of transmission can eavesdrop the data. These kinds of devices are usually inexpensive. The sender or intended receiver may not be able to find out whether their messages have been eavesdropped or not. Moreover, if there is no special electromagnetic shielding, the traffic of a wireless network can be eavesdropped from outside the building where the network is operating. In most wireless networks, there is a kind of link level ciphering done by the MAC entities.
* Jamming. Interruption of service attacks is also easily applied to wireless networks. In such a case, the legitimate traffic cannot reach clients or access points due to the fact that illegitimate traffic overwhelms the frequencies. An attacker can use special equipment to flood the 2.4 GHz frequency band. Such a denial of service can originate from outside the service area of the access point, or from other wireless devices installed in other work areas that degrade the overall strength of the signal.
* Client-to-client attacks. Wireless network users need to defend clients not just against an external threat, but also against each other. Wireless clients that run TCP/IP protocols such as file sharing are vulnerable to the same misconfigurations as wired networks. Also, duplication of IP or MAC addresses whether its intentional or accidental, may cause disruption of service.
* Attacks against encryption. The IEEE 802.11b standard uses an encryption scheme called Wired Equivalent Privacy (WEP) which has proven to have some weaknesses. Sophisti-cated attacker can break the WEP scheme.
* Misconfiguration. In order to have ease and rapid deployment, the majority of access points have an unsecured configuration. This means that unless the network administrator configures each access point properly, these access points remain at high risk of being accessed by unauthorized parties or hackers.
* Brute force attacks against passwords of access points. The majority of access points use a single password or key, which is shared by all connecting wireless clients. Attackers can attempt to compromise this password or key by trying all possibilities. Once the attacker guesses the key or the password, he/she can gain access to the access point and compro-mise the security of the system. Moreover, not changing the passwords or keys on a regular basis may put the network system at great risk especially if employees leave the company. On the other hand, managing a large number of access points and clients complicates the security system.

Any network security system should maintain the following characteristics :

* Integrity. This requirement means that operations such as substitution, insertion or dele-tion of data can only be performed by authorized users using authorized methods. Three aspects of integrity are commonly recognized: authorized actions, protection of resources, and error detection and correction.
* Confidentiality. This means that the network system can only be accessed by authorized users. The type of access can be read-only access. Another is privileged access where viewing, printing, or even knowing the existence of an object is permitted.
* Denial of service. This term is also known by its opposite, availability. An authorized individual should not be prevented or denied access to objects to which he has legitimate access. This access applies to both service and data. Denning [6] states that the effective-ness of access control is based on two ideas: (a) user identification and (b) protecting the access right of users.

Computer networks, in general, have security problems due to:

* Sharing. Since network resources are shared, more users have the potential to access networked systems rather than just a single computer node.
* Complexity. Due to the complexity of computer networks of all types, reliable and secure operation is a challenge. Moreover, computer networks may have dissimilar nodes with different operating systems, which makes security more challenging.
* Anonymity. A hacker or intruder can attack a network system from hundreds of miles away and thus never have to touch the network or even come into contact with any of its users or administrators.
* Multiple point of attack. When a file exists physically on a remote host, it may pass many nodes in the network before reaching the user.
* Unknown path. In computer networks, routes taken to route a packet are seldom known ahead of time by the network user. Also these users have no control of the routes taken by their own packets. Routes taken depend on many factors such as traffic patterns, load condition, and cost.

**Security Services**

Security services can be classified as follows

* Confidentiality. This service means the protection of data being carried by the network from passive attacks. The broadcast service should protect data sent by users. Other forms of this service include the protection of a single message or a specific field of a message. Another aspect of confidentiality is the protection of traffic from a hacker who attempts to analyze it. In other words, there must be some measures that deny the hackers from observing the frequency and length of use, as well as other traffic characteristics in the network.

* Nonrepudiation. This service prevents the sending or receiving party from denying the sent or received message. This means that when a message is received, the sender can confirm that the message was in fact received by the assumed receiver.
* Authentication. The authentication service is to ensure that the message is from an authen-tic source. In other words, it ensures that each communicating party is the entity that it claims to be. Also, this service must ensure that the connection is not interfered with in a way that a third party impersonates one of the authorized parties.
* Access control. This service must be accurate and intelligent enough so that only author-ized parties can use the system. Also, this accuracy should not deny authorized parties from using the network system.
* Integrity. In this context, we differentiate between connection-oriented and connection-based integrity services. The connection-oriented integrity service deals with a stream of messages, and ensures that the messages are sent properly without duplication, modifica-tion, reordering or reply. Moreover, the denial of service aspect is covered under the connection-oriented service. The connectionless integrity service deals only with the protection against message modification. A hybrid type of integrity service was proposed to deal with the applications that require protection against replay and reordering, but do need strict sequencing [2–4]. A good security system should be able to detect any integrity problem and if a violation of integrity is reported, then the service should report this problem. A software mechanism or human intervention should resolve this problem. The software approach is supposed to resolve the problem automatically without human intervention.
* Availability. Some attacks may result in loss or reduction of availability of the system. Automated schemes can resolve some of these problems while others require some type of physical procedures.

**Wired Equivalent Privacy (WEP) Protocol**

The name, wired equivalent privacy (WEP), implies that the goal of WEP is to provide the level of privacy that is equivalent to that of a wired LAN. This was designed to provide confidentiality for network traffic using wireless protocols. WEP was intended to provide a similar level of privacy over wireless networks that one may get from a wired network. The WEP algorithm is used to protect wireless networks from eavesdropping. It is also meant to prevent unauthorized access to wireless networks. The scheme relies on a secret key that is shared between a wireless node and an access point. The secret key is used to encrypt data packets before sending them. The IEEE 802.11 standard does not specify how the standard key is established and most implementations use a single key that is shared between all mobiles and access points.

WEP relies on a default set of keys, which are shared between wireless LAN adapters and access points .

The IEEE 802.11 committee has established standards for wireless LANs and several companies have designed wireless LAN products that are compatible with these universal standards. Wireless networks users are primarily concerned that an intruder should not be able to: (a) access the network by using similar wireless LAN equipment; and (b) capture wireless LAN traffic by eavesdropping or other methods for further analysis .

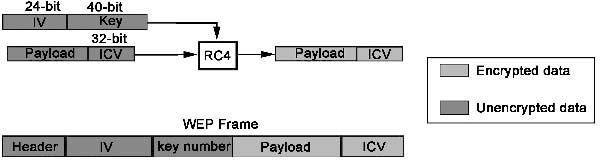


Figure: An authenticated frame

In IEEE 802.11 networks, access to network resources is denied for any user who does not prove knowledge of the current key. Eavesdropping is prevented by using the WEP scheme whereby a pseudorandom number generator is initialized by a shared secret key. Based on the Rivest–Shamir–Adelman (RSA) RC4 algorithm, this simple WEP algorithm has the follow-ing properties: (a) reasonably strong – a brute force attack on this algorithm is difficult because every frame is sent with an initialization vector, which restarts the PseudoRandom Number Generator (PRNG) for each frame; (b) self-synchronizing – since just like in any LAN, the wireless LAN stations work in a connectionless environment where packets may get lost, the WEP algorithm resynchronizes at each message [13–23]. Figure shows an authenticated frame.

The WEP algorithm uses the RC4 encryption scheme which is often called the stream cipher. RC4 is a stream cipher similar to the encryption scheme used in the Secure Socket Layer (SSL) to secure access to web sites. It works fine when used with SSL. This is because each transaction is assigned a unique 128-bit key. The WEP algorithm is part of the IEEE 802.11 standard and it defines how encryption must support the authentication, integrity, and confidentiality of packets sent using wireless systems. The standard committee selected RC4, a proven encryption scheme, to be used for wireless security and all wireless system manu-facturers support IEEE 802.11. Designing systems that use cryptographic tools is a challen-ging task.

The open system authentication is the default authentication for the 802.11 standard. This scheme authenticates everyone that requests authentication. It relies on the default set of keys that are shared between the wireless devices and the wireless access points. Only a client with the correct key can communicate with any access point on the network. If a client without the correct key requests connection, then the request is rejected. The data is encrypted before transmitting, and an integrity check is performed to make sure that the packets are not modified in transit. Only a client with the correct key can decrypt the transmitted data preventing unauthenticated users from accessing the information.

The access control list can provide a minimal level of security. In order that vendors can provide security, they often use this mechanism by using the access control list, which is based on the Ethernet MAC addresses of the clients. This list consists of the MAC addresses of all of its clients and only the clients whose MAC addresses are listed can access the network. If the address is not listed, access is not granted. Figure 1depicts WEP based security with the access control list .

The IEEE 802.11 standard specifies two methods for using the WEP. The first method provides a window of four keys. A station or an access point can decrypt packets enciphered

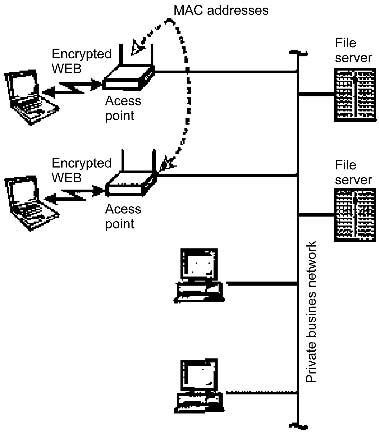


Figure : Security with access control list

with any of the four keys. The transmission is limited to any one of the four manually entered keys, which is known as the default key. The second method is called the key-mapping table where each unique MAC address can have separate keys. The use of a separate key for each client mitigates the cryptographic attacks found by others. The disadvantage is that all of these keys should be configured manually on each device or access point.

In the shared key authentication method, the station wishing to authenticate (initiator) sends an authentication request management frame indicating that it wishes to use the shared key authentication. The responder responds by sending the challenge text, which is the authentication management frame to the initiator. The PRNG with the shared secret and the random initialization vector generates this challenge text. After the initiator receives the challenge management frame from the responder, it copies the contents of the challenge text into the new management frame body. The new management frame body is then encrypted using the shared secret along with the new Initiating Vector (IV) selected by the initiator. This frame is then sent to the responder. The latter decrypts the received frame and verifies that the Cyclic Redundancy Code (CRC) Integrity Check Value (ICV) is valid, and that the challenge text matches the one that is sent in the first message. If they do, then the authentication is successful and the initiator and the responder switch roles and repeat the process to ensure mutual authentication.

Figure shows what the authentication management frame looks like. The value is set to zero if successful and is set to an error value if unsuccessful. The element identifier

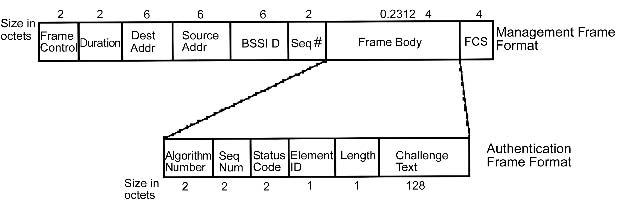


Figure: Authentication management frame

identifies if the challenge text is included. The length field identifies the length of the challenge text, which includes a random challenge string .

**Mobile IP**

Mobile IP was developed in response to the increasing use of mobile computers in order to enable computers to maintain Internet connection during their movement from one Internet access point to another. It is important to note that the term mobile implies that the user is connected to one or more application across the Internet and the access point changes dynamically. Clearly, this is different from when a traveler uses his ISP account to access the Internet from different locations during his trip .

Mobile IP is the modification to the standard IP so that it allows the client to send and receive datagrams no matter where it is attached to the network. The only security problem using this mechanism is redirection attacks. A redirection attack occurs when a malicious client gives false information to the home agent in the mobile IP network. The home agent is informed that the client has a new care of address. So all IP datagrams addressed to the actual client are redirected to the malicious client.

Mobile IP is designed to resist two kinds of attacks: (a) a malicious agent that may reply to old registration messages and cut the node from its network, and (b) a node that may pretend to be a foreign agent and send a registration request to a home agent in order to divert traffic that is intended for a mobile node to itself. Message authentication and proper use of the identification field of the registration request and reply messages are often used to protect mobile IPs from these kinds of attack. In order to protect against such attacks, the use of message authentication and proper use of the identification field of the registration request and reply messages is supposed to be effective. Each registration request and reply contains an authentication extension that has the following fields:

* Type. This is an 8 bit field that designates the type of authentication extension.
* Length. This is an 8 bit field that identifies the number of bytes in the authenticator.
* Security Parameter Index. This field has 4 bytes and is used to identify the security context between a pair of nodes. The configuration of the security context is made so that the two nodes share the same secret key and parameters relevant to the authentication scheme.
* Authenticator. This field has a code that is inserted by the sender into the message using a

shared secret key. The receiver uses the same code to make sure that the message has not been modified. The default authentication scheme is the keyed-MD5 (Message Digest 5) which produces a 128-bit message digest. MD5 was developed in 1994 as a one-way hash algorithm which takes any length of data and produces a 128-bit ‘fingerprint’ or ‘message digest.’ It is computationally not feasible to determine the original message based on the fingerprint.

Weaknesses in the WEP Scheme

The weakness of the WEP protocol involves the RC4 encryption algorithm and the Initializa-tion Vector (IV). The RC4 takes an encryption key and generates a pseudorandom stream of bytes called the keystream . The latter is pseudorandom as every key is guaranteed to produce a different keystream. Many researchers have found a number of flaws in WEP that seriously undermine the security of the system. WEP is weak against the following attacks:

1. active attacks that inject new traffic from unauthorized mobile stations; (b) active attacks to decrypt traffic based on fooling the access point; (c) passive attacks to decrypt traffic based on statistical analysis; and (d) dictionary-building attacks which allow real-time automated decryption of traffic after some analysis .

Active attack to inject traffic is due to the situation where an attacker knows the exact plain text for one encrypted message. By using this knowledge, the attacker can construct correct encrypted packets. This involves constructing a new message, calculating the CRC-32, and performing bit flips on the original encrypted message. This packet can now be sent to the access point or to a mobile node and accepted as a valid packet.

In the passive attack that is based on traffic decryption, an eavesdropper can intercept all wireless traffic until an IV collision occurs. The attacker can obtain the XOR of two plain text messages by XORing two packets which use the same Initialization Vector (IV). This result can be used to interpret data about the two messages. IP traffic is often predictable and has redundancy that can be used to eliminate many possibilities for the content of messages. Advanced guesses about the content of one or both of the messages can be obtained by using statistical analysis techniques to determine the exact content. Once it is possible to detect the entire plain text for one message, it is possible to detect the plain texts of all other messages with the same IV. Another scenario of this attack occurs when the attacker uses a host on the Internet to send traffic from outside to a host on the wireless system facilities. The attacker will be able to know the content of such traffic, hence, the plain text will be known. If the attacker intercepts the encrypted version of the message sent over an IEEE 802.11 system, he will be able to decrypt packets that use the same IV.

**Virtual Private Network (VPN)**

A Virtual Private Network (VPN) connects the components and resources of one network over another network. VPNs accomplish this by allowing the user to tunnel through the wireless network or other public network in such a way that the tunnel participants enjoy at least the same level of confidentiality and features as when they are attached to a private wired network. A VPN is a group of two or more computer systems connected to a private network, which is built and maintained by the organization for its own use with limited public network access. A VPN solution for wireless access is currently the most suitable alternative to WEP. It is already widely deployed to provide remote workers with secure access to the networks via the Internet. In the remote user application, a VPN provides a secure, dedicated path called a tunnel over an untrusted network. A comprehensive VPN requires three main technology components: security, traffic control, and enterprise management.

VPNs provide the following main advantages :

* Security. By using advanced encryption and authentication schemes, VPNs can secure data from being accessed by hackers and unauthorized users.
* Scalability. They enable organizations to use the Internet infrastructure within ISPs and devices in an easy and cost-effective manner. This will enable organizations to add large amounts of capacity without the need to add new significant infrastructure.
* Compatibility with broadband technology. VPN technology allows mobile users and telecommuters to benefit from the high-speed access techniques such as DSL and cable modem, to get access to their organization networks. This provides users with significant flexibility and efficiency. Moreover, such high-speed broadband connections provide a cost-effective solution for connecting remote offices.
* They are currently deployed on many enterprise networks
* They have low administration requirements.
* The traffic to the internal network is isolated until VPN authentication is performed.
* WEP key and MAC address list management become optional since the security measures are created by the VPN channel itself.

The main drawbacks of the current VPNs as applied to WLANs are :

* Lack of support for multicasting and roaming between the wireless networks.
* They are not completely transparent since users receive a login dialog when roaming between VPN servers on the network or when a client system resumes from standby mode.

Various tunneling protocols, which are discussed below, are used to ensure security .

**Point-to-Point Tunneling Protocol (PPTP)**

This protocol is built on the Internet communications protocol called Point to Point Protocol

1. and the TCP/IP protocol. PPP offers authentication as well as methods of privacy and compression of data. PPTP allows the PPP session to be tunneled through an existing IP connection. The existing connection can be treated as if it were a telephone line. Therefore, a private network can run over a public network. Tunneling is achieved because PPTP provides encapsulation by wrapping packets of information within IP packets for transmission through the Internet. Upon reception, the external IP packets are stripped away, exposing the original packets for delivery. Encapsulation allows the transport of packets that will not otherwise conform to Internet address standards.

Layer-2 Transport Protocol (L2TP)

Similar to PPTP, L2TP is basically a tunneling protocol and does not include any encryption or authentication mechanism. The main difference between PPTP and L2TP is that L2TP combines the data and control channels and runs over the User Datagram Protocol (UDP). The latter is faster for sending packets that are commonly used in real-time Internet commu-nication because it does not retransmit lost packets. On the other hand, PPTP separates the control stream, which runs over TCP, and the data stream, which runs over GRE. Combining these two channels and using high performance UDP makes L2TP more firewall friendly than the PPTP. This is the main advantage as most firewalls do not support GRE.

In PPP, a connection is tunneled using IP. An L2TP access concentrator is the client end of

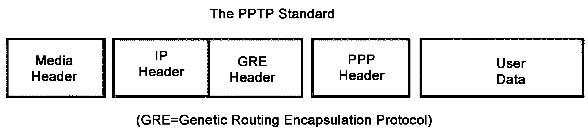


Figure: The Point-to-Point Tunneling Protocol (PPTP) standard

the connection while an L2TP network server is the server side. The PPP packets are encap-sulated in an L2TP header that is encapsulated in IP. These IP packets can traverse the network just like ordinary IP datagrams.

Data transmission in an L2TP can be implemented as a UDP-based IP protocol. The packet is first generated at the client computer. This IP packet is sourced from the client computer and destined for the remote network. The packet is encapsulated in PPP. This packet is then encapsulated in L2TP. UDP header is added to this L2TP packet and is encapsulated in an IP datagram. This IP packet is destined for the Internet Service Provider (ISP) network. The IP packets will again be encapsulated at PPP and terminate at the ISP’s network authentication server. This final heavily encapsulated packet will be sent over the circuit switched layer 2 network.

Internet Protocol Security (IPSec)

IPSec is an open standard that is based on network layer 3 security protocol. The latter protects IP datagrams by defining a method of specifying how the traffic is protected and to whom it is sent. In order to protect IP datagrams, the IPSec protocol uses either the Encapsulation Security Payload (ESP) or Authentication Header (AH) protocols [3,21].

The data origin authentication ensures that the received data is the same as that sent and the recipient knows who sent the data (see Figure 12.5). Data integrity ensures data transmission without alteration while relay protection offers partial sequence integrity. Data confidentiality ensures that no one can read the transmitted data which can be possible by using encryption algorithms.

Integrating L2TP with IPSec offers the ability to use L2TP as a tunneling protocol; however, securing the data is achieved using an IPSec scheme. Using L2TP as the tunneling protocol gives the added advantage of increased manageability for end-to-end communica-tions. Moreover, L2TP is a widely available standard; therefore the interoperability between vendors is far better than just IPSec alone.

The same VPN technology can be used to secure wireless systems. The Access Points (APs) are configured for open access with no WEP encryption, but wireless access is isolated from the enterprise network by a VPN server and a VLAN between the APs and VPN servers. Authentication and full encryption over the wireless network is provided using the VPN servers which also act as gateways to the private network. Clearly, a VPN-based solution has the advantage of being scalable for a very large number of users.