An Overview of Wireless Networks and Security Issues For WiFi Networks

By Bo Li, Harold Lee, Narendra Kamat, Daniel Menchaca and Prof. Ted S. Rappaport

Wireless local area networks (WLANs) provide wireless connectivity between PCs, laptops and other equipment in corporate, public and home environments. Today, tens of millions of users rely on short-range wireless connectivity between computers or automation equipment using WLAN modem gear that complies with well-known standards such as IEEE 802.11, 802.11a, 802.11b and 802.11g. The first WLAN standard IEEE 802.11, initially contemplated in the late 1980's, was finalized in 1997 (10 years later!) and provided interoperability standards for equipment makers using 11 Mbps Direct Sequence-Spread Spectrum spreading and 2 Mbps user data rates in the 900 MHz and 2.4 GHz unlicensed bands.

In 1999, IEEE 802.11b and 802.11a standards were developed, and this created the foundation for the WiFi explosion we are witnessing today. IEEE 802.11b provided new user data rate capabilities of 11 Mbps and 5.5 Mbps in addition to the original 2 Mbps and 1 Mbps user rate of IEEE 802.11. Today, IEEE 802.11a offers high speed connectivity up to 54Mbps using OFDM in the 5 GHz frequency band, and IEEE 802.11g defines network connectivity in the 2.4 GHz band that is backward compatible with IEEE 802.11b and 802.11 standards.

Figure 1 illustrates the evolution of IEEE WLAN standards. An overview of the evolution of WiFi is...
given in [23].

The IEEE 802.11 specifications focus on the Medium Access Control (MAC) and PHY (physical layer) for Access Point (AP) based networks and ad hoc networks. The MAC layer provides reliable data delivery from the wireless physical (PHY) layer (e.g., the channel, where bits are formed in the radio channel) to the upper layers of the Open System Interconnection (OSI) network reference model. A controlled access method called Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) is used to pass data from the upper network layers to the wireless media.

Figure 2 shows different standards used for the PHY and MAC layers. The PHY layer functions as an interface to exchange data frames with the MAC layer for transmission and reception of data, and provides data modulation and demodulation. Figure 2 shows the structure of WLAN standards with reference to OSI model.

IEEE 802.11 Media Access Control (MAC) Physical Layer (PHY)

<table>
<thead>
<tr>
<th>FHSS interface</th>
<th>DSSS Interface</th>
<th>OFDM Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.11</td>
<td>IEEE 802.11a</td>
<td>IEEE 802.11g</td>
</tr>
</tbody>
</table>

IEEE 802.2 Logic Link Control (LLC)

OSI Data

MAC Link Layer

OSI Physical Layer

Some of the popularly known security risks to WLANs include: Insertion Attacks, Interception and Traffic Monitoring, Jamming and Client to Client Attacks [2]. Insertion attacks occur when unauthorized devices are placed on the wireless network without going through a security process. Interception and monitoring of wireless traffic involve wireless sniffers, session hijackings, broadcast monitoring, and cloning access points and intercepting traffic [2]. WLANs are particularly susceptible to denial-of-service attacks, in which legitimate traffic gets jammed due to illegal traffic that overwhelms the access point. Client to client attacks are a consequence of the fact that two wireless clients can talk directly to each other, thereby bypassing the access point.

WiFi is exploding, and coffee shops and restaurants are deploying WiFi equipment to provide ubiquitous portable Internet access. However, the perceived lack of security has been an impeding factor in the widespread acceptance of WLANs. Unofficial studies suggest that more than 70% of wireless access points are unencrypted, and underground snoopers and sniffers, as detailed in a publication called 2600, often publish lists of hundreds of corporate access points that can be used for instant access by strangers. Also, approximately 27% of the access points installed today use the hardware default value of the SSID (Service Set Identifier, a WLAN packet header field used in the authentication mechanism); this is akin to not changing the code on your garage door opener. Anybody with a wireless-enabled laptop can easily go near unprotected access points, sniff the traffic in the air and, at the very least, be able to see the data being transferred to and, from the access point and, at the very most, become a user of the WLAN network.

IEEE WLANs operate in two modes: 1) a host-to-client mode, also known as an AP-based network where a fixed access point serves many co-channel clients, or users, and 2) in an ad hoc network mode where there is not a single known fixed access point, and all users are peer to one another (also known as Independent Basic Service Set (IBSS) or peer-to-peer mode). In the ad hoc mode, stations communicate directly with each other. Figure 3 depicts these two WLAN operation modes.
<table>
<thead>
<tr>
<th>Terminology</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA Server</td>
<td>Authentication, Authorization and Accounting server.</td>
</tr>
<tr>
<td>AES</td>
<td>AES is an advanced encryption standard used by the US Government and is defined by the National Institute of Standards and Technology. It employs a symmetric encryption algorithm and the Rijndael block cipher in order to protect user data.</td>
</tr>
<tr>
<td>Authentication Server</td>
<td>An entity that provides an authentication service to an authenticator. This service determines, from the credentials provided by the supplicant, whether the supplicant is authorized to access the services provided by the authenticator.</td>
</tr>
<tr>
<td>Authenticator</td>
<td>An entity at one of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link.</td>
</tr>
<tr>
<td>Encapsulate</td>
<td>To construct a protected packet from an unprotected packet.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Encryption is the conversion of data into a form, called a ciphertext, that can’t be easily understood by unauthorized people.</td>
</tr>
<tr>
<td>Group Transient Key</td>
<td>A value derived from the Pseudo-Random Function using the Group Nonces. It is split up into as many as three keys (a Temporal Encryption Key and two Temporal MIC Keys) for use by the rest of the system.</td>
</tr>
<tr>
<td>Key Management Service</td>
<td>A service to distribute and manage cryptographic keys within a Robust Security Network.</td>
</tr>
<tr>
<td>Kerberos</td>
<td>Kerberos is a distributed authentication service that allows a process (a client) running on behalf of a principal (a user) to prove its identity to a verifier (an application server, or just server) without sending data across the network that might allow an attacker or the verifier to subsequently impersonate the principal.</td>
</tr>
<tr>
<td>Network Access Port</td>
<td>A point of attachment of a system to a LAN. It can be a physical port (perhaps a single LNA MAC attached to a physical LAN segment) or a logical port (an IEEE 802.11 association between a station and an access point).</td>
</tr>
<tr>
<td>Pairwise Transient Key</td>
<td>A value that is derived from the PRF using the SNonce, split up into as many as five keys (Temporal Encryption Key, two Temporal MIC Keys, EAPOL-Key Encryption Key, EAPOL-Key MIC Key) for use by the rest of the system.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial In User Service, an example of software running on an authentication server.</td>
</tr>
<tr>
<td>Robust Security Network</td>
<td>An IEEE 802.11 LAN relying on IEEE 802.1X for its authentication and key management service, and CCMP, WRAP, or TKIP for data protection.</td>
</tr>
<tr>
<td>Session</td>
<td>A session is a series of interactions between two communication endpoints that occur during the span of a single connection. Typically, one end point requests a connection with another specified end point and if that end point replies agreeing to the connection, the end points take turns exchanging commands and data. The session begins when the connection is established at both ends, and it terminates when the connection is ended.</td>
</tr>
<tr>
<td>Supplicant</td>
<td>An entity at one end of a point-to-point LAN segment that is being authenticated by an authenticator attached to the other end of that link.</td>
</tr>
<tr>
<td>VPN</td>
<td>A virtual private network (VPN) is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organizations' networks.</td>
</tr>
</tbody>
</table>
and any security features contained therein.

The three basic security concepts concerning information on any network are confidentiality, integrity and availability. The requirement that information is read or copied only by authorized persons or intended recipients is known as confidentiality. It is a prime requirement in corporate and defense communication applications. The requirement that the message received by the recipient is identical to the message sent by the receiver is known as integrity. It is of primary importance in legal and financial communications. Making information or network service inaccessible to bona fide users violates the requirement of availability, which is most important for service-oriented businesses. Violation of this requirement is known as a denial of service.

To users of information carried by the network, the most important concepts are authentication, authorization, and non-repudiation. Authentication is the process of verifying that a user is, in fact, who he or she claims to be. The proof of identity may involve something the user knows (e.g., a password), something the user has (e.g., a "smart card") or something about the user that proves a unique identity (e.g., a fingerprint). Authorization is the process of determining whether a particular user (or computer system) has the right to carry out a certain activity, such as reading a file or running a program. Authentication and authorization go hand in hand. Users must be authenticated before carrying out the activity they are authorized to perform. Non-repudiation is the requirement that if a user sends a message or performs an activity after authentication, there should be no way for him or her to deny that fact later — essentially, an electronic paper trail.

When these ideas are applied to WLANs, it must be realized that the wireless medium is unlike the wired network, in that the airwaves are shared. Wired networks afford a sense of physical security, but in WLANs, any adversary has physical access to the medium over the air. This warrants more careful deployment of security techniques at the application layer. Also, most users of WLANs are mobile, using portable computing devices (e.g., laptops). These users obtain network connectivity through access points. These access points have to run at very high speeds, switching packets to and from users at a very high data rate (several megabits per second). Therefore, introducing secure communications at the wrong point potentially can have a deleterious effect on high-speed performance, creating delays, timing jitter or outages due to synchronization problems.

Thus, WLANs require a mechanism that allows fulfillment of security requirements without impacting data rates. For example, by letting access points manage sessions and provide packet switching, and providing a dedicated server that handles authentication/authorization, WLANs can be made to run more efficiently. Finally, strong security techniques in WLANs are inextricably linked to user awareness and cooperation. The most powerful encryption technique would be quite useless if the user has it turned off. Table 1 lists network security terminologies used by the IEEE [3, 4] and their definitions, as a requisite part of our further discussion.

A good wireless network should provide a range of different user-authentication and data-encryption options, so that users can be given the appropriate level of security for their particular applications.

Confidentiality, integrity and mutual authentication are some of the issues common to all network security discussions. When the first WLAN standard 802.11 was developed, there was an attempt to address these issues by the security mechanism known as Wired Equivalent Privacy (WEP). Although it is better than no encryption at all, WEP had some serious vulnerabilities [6, 7]. After WEP, the security standard 802.1X has been gaining popularity. However, 802.1X is not a complete security standard, but just an authentication model. The IEEE 802.1X is a standard for port-based network access control. The standard can be applied to both wired and wireless networks and provides a framework for user authentication and encryption key distribution.

However, even this new protocol is not free from some initial design flaws [8]. Currently, the industry is eagerly awaiting the security standard proposed by IEEE 802.11 Task Group I, known as 802.11i. It is hoped that the experience with the previous security approaches will lead to 802.11i having properly dealt with all known vulnerabilities of WEP and 802.1X. 802.11i uses two-way authenticated 802.1X as part of its mechanism, and it is expected that encryption will be carried out using the relatively new Advanced Encryption Standard (AES) that uses two AES-based protocols: Wireless Robust Authenticated Protocol (WRAP) and Counter-Mode Cipher Block Chaining-Message Authentication and Control Protocol (CCMP).

Another way to provide security is to use an application-based login screen and a network-layer authentication technique, such as a VPN. VPNs also
WLAN Security Solution

- From wired network to wireless network: WEP and WEP2

To provide the basic security features of confidentiality, authentication and integrity to the stations using a WLAN, the IEEE standard 802.11 proposed a protocol known as Wired Equivalent Privacy (WEP) [9]. This section takes a look at how WEP works, the security features it provides, the vulnerabilities inherent in WEP, and suggestions to address some of these vulnerabilities.

Figure 5. The WEP encryption engine.

- WEP architecture

As can be seen from Figure 5, WEP depends on a secret key shared between the communicating parties (client station and access point) to protect the payload of a transmitted frame in each direction. The basic encryption is carried out using the digital logic X-OR operation, where the plain-text message (with its attendant checksum) is X-OREd with a keystream. To help ensure that the keystream is not repeated, WEP uses a pseudo-random number generator using RC4. This takes as input a secret key k (one of a few possible keys, known to both parties initially) and a 24-bit Initialization Vector (IV).

Because, ideally, each message is X-OREd with a new keystream, the system provides an unbreakable encryption. But this "security" strongly depends on the fact that two keystreams should not be the same. This is somewhat hampered by the very infrequent change to the secret key, and the very small (24-bit) IV, leading to rapid reuse of the IV and, hence, the keystream. Reuse of the keystream seriously threatens the security of this encryption, although the concept of RC4 is accepted to be secure.

- WEP intentions

The following points discuss how WEP intended to address the security requirements for WLANs.

Integrity: WEP computes the Integrity Check Vector (ICV) by performing a 32-bit cyclical redundancy check (CRC-32) of the frame and appends the vector to the original frame, resulting in the plaintext. Thus the ICV is piggybacked with the data in the encrypted frame. The inclusion of the ICV is meant to provide integrity. On receiving and decrypting the frame, the receiver recalculates the ICV using the CRC computation. The idea is that if any modification is made to a packet en-route, then the CRC checksum that is also transmitted with the packet will not match the CRC calculated at the receiver. The receiver will thus identify the packet as damaged or corrupted and discard it.

Authentication: There are two kinds of Authentication provided by WEP:

1. Open System Authentication: There is no authentication required and any station is allowed to join the Basic Service Set if the WEP
configuration has been set to Open System.

2. Shared Key Authentication: The client station requests authentication from the Access Point and indicates that it wishes to use Shared Key Authentication. The Access Point generates a random 40-bit (or 128-bit) challenge and sends it in the plain text to the client station. The client station encrypts the challenge using the shared key and sends it back to the Access Point. The access point decrypts the challenge and uses the CRC to verify its integrity. If the decrypted frame matches the original challenge, the station is considered authentic.

Confidentiality: The confidentiality of WEP depends on the use of a secret-key symmetric algorithm, which is used to encrypt the body of a transmitted frame of data. The message plus ICV is encrypted via the RC4 pseudo-random number generator algorithm using a long sequence key stream. Finally, it is the cipher text that is sent over the radio link. Only an intended recipient will have the secret key that is needed to generate the keystream to decrypt the frame. Because (ideally) each packet will be encrypted by a different keystream, it was thought that it will not be easy to attack the encryption unless a brute-force mechanism to obtain the key is used.

- **WEP logistic issues and vulnerabilities**

If the Shared Key Authentication is enabled (imposing access control), then the access points and the stations must have the secret key. The secret key is presumed to have been delivered to participating stations via a secure channel independent of the 802.11 specification. To prevent the sending of the secret key in the clear, each station has a small set of possible keys to be used, in the form of an array of secret keys. The station sends only the array index of the key it is using in its encryption algorithm.

Two stations may have a predetermined key (between the two). If the frame is to be sent to a station with which this prior arrangement has been worked out, the frame will be encrypted using a different secret key. The access point has a mapping of the secret keys of these stations to their MAC addresses, known as an Access Control List. By looking up the appropriate key, the receiver is able to decrypt the frame. This shows the system is not limited to using a single secret key for all stations.

A robust and secure key distribution mechanism is not defined in the 802.11 standard and, therefore, the implementation is left to the equipment vendors and the users. The disadvantage is that physical (safe) distribution of keys can’t be carried out often; the secret key will not be changed often enough or will be easy to guess.

There are widely known fundamental security problems with WEP. In [6, 7], the authors have pointed out possible attacks on WEP, which can violate all the requirements of privacy, access control, and integrity.

- **Integrity** The CRC can be easily modified. The IC field is implemented as a CRC-32 checksum - a common error detection scheme. The problem with this scheme is that it is linear; thus, it is possible to compute the bit difference of the two CRCs based on the bit difference of the data packets. This allows the attacker to be able to determine which bits of the CRC-32 code to correct when flipping arbitrary bits in the packets so that the resulting packet seems valid.

- **Confidentiality and Authentication** There are several issues with the encryption used by WEP.

  1. The WEP algorithm uses encryption provided by X-Oring, the plain text block with a keystream sequence generated by the RC4 stream-cipher pseudo-random number generator. The inputs to the RC4 algorithm are a secret key $k$ (which is comparatively short) and an initialization vector. If the same keystream is used for different plain texts, then we have the following situation:

      \[
      C_1 = P_1 \oplus RC4(IV,k) \\
      C_2 = P_2 \oplus RC4(IV,k)
      \]

      If $RC4(IV,k)$ gets repeated, then the eavesdropper could perform

      \[
      C_1 \oplus C_2 = P_1 \oplus RC4(IV,k) \oplus P_2 \oplus RC4(IV,k) = P_1 \oplus P_2
      \]

      With some knowledge about the type of data (plain text) there is a good chance the attacker will be able to arrive at both $P_1$ and $P_2$, given the redundancy in real-world data. To prevent this, it is required that $RC4(IV,k)$ does not recur. This is implemented by changing the IV on a per-packet basis. Because the receiver also needs to know IV used for any packet, it also is transmitted as the unencrypted part for this packet (this makes the IV available to the attacker as well). WEP uses only 24-bit IV, so any high-volume access point, even if using totally-random IVs, will run out of IVs in about half a day and be forced to reuse an IV. This is termed an IV collision. An attacker can detect that an IV collision has occurred, because the IV is transmitted unencrypted in the packet. An IV collision results in the same keystream generated by
RC4, and the above attack can then be carried out. Even with a longer keylength for IV, such as that used in WPE2 (128 bits secret key), the fundamental problem is not solved.

In addition to the plain text, the successful attack also provides the attacker with the keystream corresponding to that IV. With sufficient effort, the attacker then can build a table of keystreams for each IV, which provides a direct decryption dictionary.

In addition, the secret key is one of a small set of values (four) that the two participants have. This is to help ensure the secret key need not be transmitted over the medium. Because the key is not changed frequently, the threat posed by IV collision is even more serious.

2. When an IV and its corresponding keystream are known, it can be used to construct a new message and inject it into the network. The access point will have no reason to suspect this packet as a spurious one, because it has a valid IV, and it is encrypted with the correct keystream.

3. In the challenge/response sequence while performing Shared Key Authentication, the challenge (plain text), the response (cipher text) and the IV used to encrypt the challenge are all visible to the eavesdropper. Thus, the authentication sequence provides the attacker with a keystream corresponding to that IV. If that IV is reused, (and the shared key is not changed), then the attacker has direct ability to decrypt the frame.

The above analysis shows that only WEP cannot be relied upon as a complete security solution. While difficult to intercept by most users, the deficiencies make WEP easy to attack. The lack of transparency in the design process led to some obvious errors being overlooked. Although RC4 is in itself a secure stream cipher (without any known vulnerabilities), its application in early WLANs led to a specification that has major vulnerabilities.

- **WEP2 improvements and its inherent setbacks**

WEP2 was developed to acknowledge problems with the initial 802.11 security protocol WEP. It was created to be backwards compatible with WEP. Compared with WEP, WEP2 uses 128-bit secret keys. Some of the attacks on the WEP secret key can’t be mounted easily if WEP2 is in use, because the attacker needs to monitor a much larger stream of traffic before being able to decode and decipher. However, because WEP2 still runs on linear scaling, it is not a significant improvement. WEP2 has the same inherent vulnerabilities that exist in WEP: static secret key, IV key reuse, and known plain text attacks [5].

- **IEEE 802.1X**

Solutions based on the WEP standard alone do not offer system administrators effective methods to update the keys. On larger networks, the job of renewing keys can be a huge task. As a result, companies either do not use WEP at all, or they maintain the same keys for months and even years. Both cases significantly heighten the wireless LAN’s vulnerability to eavesdroppers.

The use of IEEE 802.1X offers an effective framework for authenticating and controlling user traffic to a protected network as well as dynamically varying encryption keys. 802.1X ties a protocol called EAP (Extensible Authentication Protocol) to both the wired and wireless LAN media, and it supports multiple authentication methods, including RADIUS, Kerberos, one-time passwords, certificates and public key authentication.

- **EAP essentials**

EAP was designed to de-couple the mechanisms of data transfer, encryption and authentication. EAP is the Internet Engineering Task Force (IETF) standard for extensible authentication in network access. It is standardized for use within PPP (Point-to-Point Protocol, RFC 2284), wired IEEE 802 networks.
Developed as a generalized framework for several different authentication methods, EAP is supposed to avoid proprietary authentication systems. It can facilitate different authentication techniques, from passwords to challenge-response tokens and public key infrastructure certificates.

With a standardized EAP, interoperability and compatibility of authentication methods becomes simpler. For example, when one dials up a remote-access server and uses EAP as part of the PPP connection, the Remote Access Server (RAS) does not need to know any of the details about the authentication system. By supporting EAP authentication, an access point gets out of the business of acting as middle man, and it just packages and repackages EAP packets to hand off to a RADIUS (or equivalent) server that will do the actual authentication.

The three entities involved in authentication, using the EAP framework are as follows:

1. Supplicant: the entity that desires to use a network service. This service is offered by a port on the authenticator.

2. Authenticator (Access Point): Provides ports for a network service, (the supplicant authenticates via authenticator to authentication server). All sessions go through the access point.

3. Authentication Server: Dedicated server running any authentication protocol such as CHAP, PAP, Kerberos, etc. It receives and responds to authentication requests from clients (sent via the uncontrolled port of the access point). It directs the authenticator to provide service after successful authentication.

EAP is flexible in the sense that any authentication mechanism can be encapsulated within EAP request/response messages. It gains flexibility by operating at the network layer rather than the link layer. Because each network port is not required to make authentication decisions, this is a key performance benefit.

**IEEE 802.1X Architecture**

802.1X provides an architecture for authentication methods by using simple transport for EAP messages, running over all 802 LANs. 802.1X inherits the EAP (Extensible Authentication Protocol) architecture and provides port based network access control with dynamic key management. A network port is defined as an association between a client station and an access point.

In the context of an 802.11 wireless network, 802.1X is used to securely establish an authenticated association between the client and the access point. An 802.11 Robust Security Network (RSN) uses 802.1X to provide security: authentication, access control and key management. It provides mechanisms to restrict network connectivity at MAC layer to authorized entities. The network connectivity is through network port.

IEEE 802.1X authentication is a client-server architecture delivered with EAPOL (EAP over LAN). Figure 6 shows the IEEE 802.1X authentication architecture. The authentication server (mostly RADIUS) authenticates each client connected to an Access Point (Supplicant) before accessing any services offered by the WLAN. Typically, the RADIUS protocol is used for the communication between authentication server and authenticator. It encapsulates EAP messages as a RADIUS attribute. It provides mechanism for per-packet authentication and for integrity verification between access point and RADIUS server. Sometimes, an Authenticator and an Authentication Server can be co-located within the same system such as an AP, allowing it to perform the authentication function without the need for communication with an external server.

Before the authentication succeeds, the access point must allow EAP traffic. However, this traffic would originate from an (as yet) unauthenticated client. To sidestep this issue, a dual-port model is used; the access point is considered to have two logical ports. One is the uncontrolled port, on which information pertaining to those users who have not yet been authenticated can be safely sent. This port connects only to the authentication server. The other is the controlled port, which allows access to other (useful) network services. It is not possible for an unauthenticated user to use the controlled port. The job of the access point is thus simplified.

The goals of 802.1X are to provide access control and authentication, flexibility and scalability. The use of EAP fits in admirably with the latter two goals. However, as will be seen in the next subsection, the initial design of 802.1X was not free from some vulnerabilities.

**802.1X Vulnerabilities**

In spite of careful design, there were some serious vulnerabilities with 802.1X as a security standard for WLANs. Here it should be noted that part of the problem was that 802.1X is not meant for the wireless environment as such, but rather it is a general...
specificatiqn for any 802 network. Its applicability to the wireless environment was not well thought out, initially. While some of the weaknesses reported in [6] have now been fixed by various organizations, the major vulnerabilities include:

- **Man-in-the-middle attack (MITM):** One of the main design issues with 802.1X was that it didn’t specify that the authentication needed to be mutual. The authentication was only one-way. The access point could verify the identity of the client, but there was no way for the client to verify the identity of the access point. This permitted some interesting exploits, based on the adversary’s placing a rogue access point in the vicinity of the client. The rogue access point would act as an access point to the client, and also as a client to the real access point (authenticator). Thus, the attacker could get all the network traffic of that particular client to pass through it.

- **Session Hijacking:** This weakness is due to a lack of coherence between the old RSN state machine and the 802.1X state machine. After a supplicant has authenticated itself, the attacker sends a 802.11 MAC disassociate management frame to the supplicant. It uses the authenticator’s MAC address to do this. Upon receiving this frame, the RSN state machine of the supplicant goes into the “unassociated” state, while the 802.1X state machine stays in the “authenticated” state. In this situation, the attacker gains network access using the MAC address of the victim supplicant, because it was still in the authenticated state.

- **Denial of Service:** 802.1X enables per-user session keys. However, there is no keyed message integrity check specified in 802.1X, which allows the possibility of denial of service attack by a malicious party. These vulnerabilities can be mitigated to a large extent by the following. Firstly, the management frames of EAP have to be authenticated and their integrity should be guarded. This should be ensured not just between the authenticator and the RADIUS server, but also between the authenticator and the supplicant. Secondly, two-way (or peer-to-peer) authentication is required to prevent the problem of rogue access points. Again, this should be enforced not just between the authenticator and the RADIUS server, but also between the authenticator and the supplicant. Most implementations of 802.1X today have dealt with these well-known problems.

It must be understood that 802.1X is just an authentication model. It is not a complete security solution because it does not provide any mechanism for encryption, which is needed for confidentiality. In other words, an attacker can passively sniff all network traffic of authenticated clients. Many vendors continue to use WEP as the encryption mechanism along with 802.1X for authentication, which causes network implementers who are most concerned about security to use a VPN for their WLAN networks (this will be detailed in the Spring 2004 Proceedings).

802.1X also supports dynamic key exchange. The keys are managed at the transport layer by using what is known as EAP-TLS. TLS stands for Transport Layer Security. The use of EAP-TLS is similar to the mechanism to secure web transactions on the Internet (Secure Sockets Layer protocol). The variants to this have been the use of WTLS (TLS optimized for WLANs, keeping in mind the low bandwidth, low processing power requirements of this approach) and TTLS (which requires only the authentication server to possess the digital certificate, rather than each user).
To conclude, IEEE 802.1X is an improvement over WEP with authentication, dynamic key management and MAC access control. 802.1X does not make any encryption specification; thus, vendors may keep WEP as the encryption standard. However, addition of per-packet and peer-to-peer authentication, combined with the adoption of stronger encryption algorithms, would take WLANs closer to a complete security solution.

REFERENCES:
[1]. Table for wireless standards, URL: http://www.cs.umd.edu/waa/1x.pdf
[3]. IEEE Std 802.1X-2001
[4]. IEEE Std 802.11i/D3.0, November 2002