

Understanding Wireless LAN Security

WEP (Wired Equivalent Privacy):

The WEP protocol is defined as an optional feature in the IEEE 802.11 specification and intended to provide a level of security comparable to wired networks by encrypting data transmitted over the air. The two available encryption levels, commonly referred to as WEP64 and WEP128, correspond to WEP key formats of 64 and 128 bit, respectively. In both cases, the encryption key is composed of a 24 bit initialization vector (randomly generated by the system and modified for every session) and a secret key (with key length 40 or 104 bit) set by the user. To allow the exchange of packets between wireless clients and access points, their secret keys must match each other. If the secret keys do not equal, this would indicate a security violation, and the packet would be discarded.

It should be noted that the original IEEE 802.11 standard does not specify key lengths greater than 64 bit; however, 128 bit encryption has quickly become a de-facto industry standard.

Network Name:

Another feature defined in the 802.11 specification is the SSID (Service Set Identifier), often called the network name, that uniquely identifies a wireless network and allows a wireless client to select the most appropriate access point to connect to. In order to establish a connection with the desired access point, the client must be configured to use the same network name. To protect the integrity of this access control mechanism, it is necessary to deactivate the „Broadcast SSID“ function of the access point (which is inconsistent with the 802.11 standard). That is, if the broadcast of SSIDs is suppressed, the client must respond with the correct network name to be authenticated by the access point. If „Broadcast SSID“ is enabled, the client will be granted access if it simply responds with an „any“ string for the network name, regardless of the network name configured for the access point, thereby bypassing the intended identification scheme.

ACL (Access Control List):

The ACL enables the IT manager to register a list of wireless client MAC addresses that may gain access to the network. Association requests by intruders with unauthorized MAC address will be denied by the access point. Although the ACL functionality is outside of the scope of the 802.11 specification, the wireless industry has embraced it as one of the most widely implemented security mechanisms, primarily due to its proven effectiveness in the wired world.

Security Vulnerabilities:

In principal, all of the above parameters (secret key, network name, and MAC address) can be recovered from intercepted data packets. The latter two parameters are transmitted in the clear, and could be easily compromised by an attacker listening in with a wireless sniffer or packet analyzer. If a large amount of traffic is available to an eavesdropper for analytic attacks, the secret key can be computed as well. Hence, all three security parameters are exposed to attackers that are able to gain physical access to the wireless coverage area.

Countermeasures:

These known deficiencies in the standard 802.11 security protocol can be addressed by enhancing the existing mechanisms with stronger encryption schemes and frequent key updates, which will eliminate or significantly mitigate the risk of passive attacks.

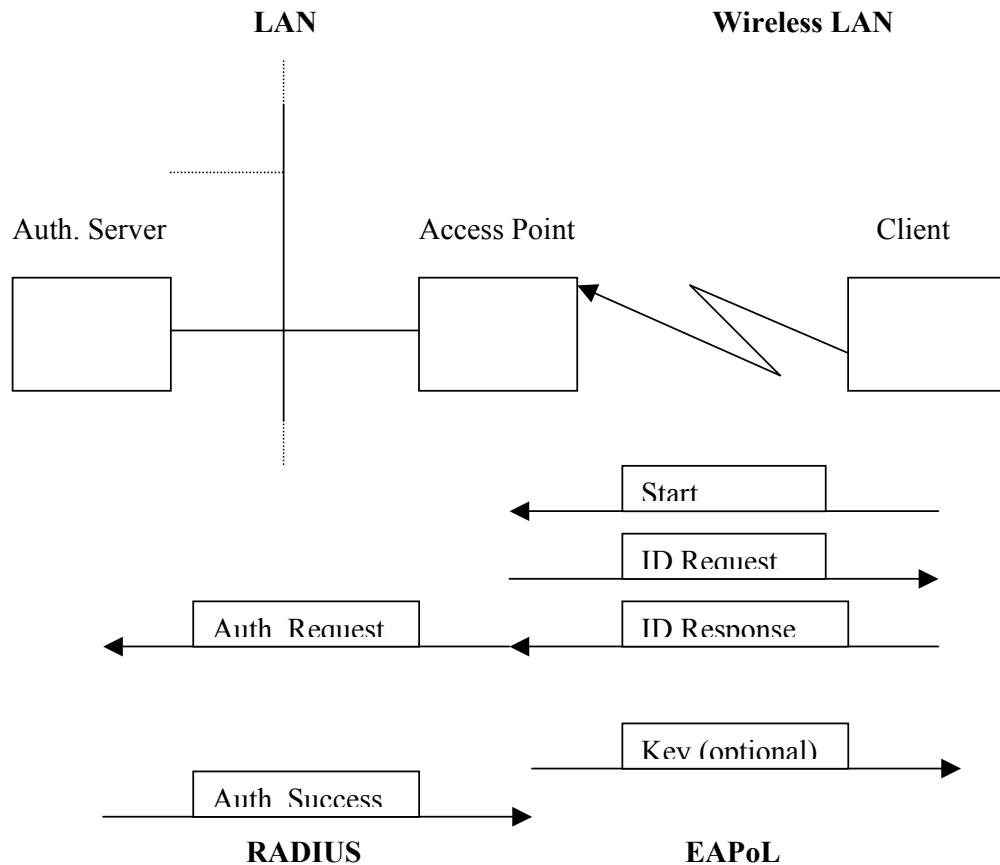
Furthermore, upper-layer authentication mechanisms can be integrated into the wireless LAN to provide reliable verification that wireless clients and access points are legitimate.

IEEE 802.1x/EAP:

The IEEE 802.1x standard defines a generic framework for port-based access control and key distribution that can be applied to both wired and wireless networks. With this model, an access point authenticates a wireless client requesting access to the network by consulting an authentication server (such as RADIUS, Kerberos, or proprietary solutions). The access point enforces the authentication process by blocking all data traffic until the client has been successfully identified by the authentication server. As part of the authentication process, unique encryption keys are generated and distributed to the wireless client and the access point.

In 802.1x terminology, the client is referred to as the „supplicant“ and the access point as the „authenticator“. The supplicant communicates with the authenticator using the EAPoL protocol (Extensible Authentication Protocol over LAN). The message protocol used between the authenticator and the authentication server is RADIUS (to be precise, EAP over RADIUS). In both cases, the EAP encapsulation ensures the secure exchange of credentials and delivery of the actual encryption keys. The following steps occur:

1. The wireless client (supplicant) submits an 802.11 conformant association request to the access point (authenticator). Upon receipt of the association request, the access point initiates the authentication sequence.
2. The access point issues an identification challenge to the wireless client.
3. The wireless client sends its identity (e.g., username and password or digital certificate) to the access point, which forwards it to a trusted authentication server.
4. Upon validating the identity of the wireless client, the authentication server transmits an „authentication success“ message to the access point.
5. Now the access point can transmit an encryption key to the wireless client. Depending upon the configuration, this key can either be based on a pre-shared key in the access point, or dynamically generated by the authentication server.
6. The access point allows communication through its controlled 802.1x port as the wireless client now possesses a valid key.
7. If necessary and desired, the encryption key is frequently updated (dynamic re-keying) and supplied by the access point.



To take advantage of this authentication procedure, both the client operating system and the authentication server must support the EAP method defined by 802.1x. Currently, Windows XP is the only operating system with built-in 802.1x/EAP protocol support, but third-party supplicant software packages are available for other platforms.

The most commonly used EAP methods are EAP-MD5, a one-way authentication scheme based on the client's username and password, and EAP-TLS, which uses digital certificates for mutual authentication. In addition, there are two proprietary derivatives of TLS dubbed TTLS (Tunneled TLS) and PEAP (Protected EAP).

With respect to the encryption key length, the 802.1x/EAP framework is completely agnostic. That means, both 802.11 conformant key types (WEP64) and stronger keys (e.g., WEP128, AES) are possible.

Weak Key Avoidance:

Certain values of the 24-bit initialization vector defined by the 802.11 standard result in so-called „weak keys“ which, when used, make the encrypted data particularly vulnerable to attacks. To eliminate initialization vector values that generate weak keys, IT managers should therefore employ the „Weak Key Avoidance“ algorithm (also known as „WEPplus“).

TKIP (Temporal Key Integrity Protocol):

TKIP has been defined by the IEEE 802.11 TG1 committee (the task group working on the 802.11i specification) and is intended to enhance the security of the WEP protocol. TKIP doubles the length of the initialization vector to 48 bit, and introduces a key mixing function for rapid renewal of the temporal encryption key. To maintain backward compatibility with legacy equipment, TKIP has been designed to rely on the same RC4 stream cipher algorithm

that is used by WEP. A new message integrity check function prevents a data packet from being manipulated by an attacker by constructing a message integrity code that covers both the source and destination MAC addresses, and the data (recognition of forgery attacks).

SSN (Simple Security Network):

The SSN initiative was spearheaded by Microsoft with the objective of overcoming the deficiencies of the WEP algorithm. It describes enhanced authentication and encryption mechanisms based on IEEE 802.1x and TKIP. SSN will be superseded by the functionally equivalent WPA specification, as described below, and have no more meaning in this form.

IEEE 802.1i:

The 802.11i standard will address all the vulnerabilities identified with WEP and offer a comprehensive, long-term security solution for wireless networks. It is currently under development by IEEE 802.11 TGi, and not expected to be ratified before the end of 2003. That means, 802.11i compliant products are unlikely to reach the market before 2004. One of the cornerstones of the draft 802.11i specification, the highly secure AES (Advanced Encryption Standard) encryption algorithm will replace RC4. Because of the computational complexity of AES, it cannot be implemented on the current-generation hardware.

WPA (Wi-Fi Protected Access):

To deliver a strongly enhanced, interoperable security solution to the market prior to the ratification of the 802.11i standard, the Wi-Fi Alliance (formerly known as WECA) has derived a subset of the current 802.11i draft that is market-ready and designed to run on existing hardware. The result of this effort is WPA. WPA is essentially based on the IEEE 802.1x, EAP-TLS, and TKIP protocols for upper-layer authentication and enhanced privacy. In addition to the WPA enterprise mode that assumes an authentication server, WPA defines a SOHO/home mode which specifies the use of pre-shared keys as the means of authenticating a wireless device. This mode allows the access point to become the authentication and key management authority in environments where no authentication server is present.

Conclusion:

WPA represents a significant near-term enhancement to 802.11 security. It integrates seamlessly into the existing wireless infrastructure and allows operation on legacy hardware. That is, changes to firmware and software drivers only will be required to upgrade to WPA. WPA is useful for both large business deployments, but also for more casual home use. In larger environments, an authentication server (RADIUS) and sophisticated protocols are utilized to cover all security measures and administrative tasks (authentication and key management), in many cases eliminating the need to deploy proprietary VPN-based (Virtual Private Networks) solutions. For home and SOHO users who don't have access to an authentication server, WPA features a special mode designed to be easy to set up, yet providing adequate security. In this mode, the user manually enters the starting password (master key) to activate the TKIP sequence. In contrast to WEP, which is based on static encryption keys, TKIP takes the master key only as a starting point and derives the actual encryption key from it, so that the same key is never used twice.

The WPA certification awarded by the Wi-Fi Alliance (formerly WECA) will assure that products from different vendors work together, facilitating widespread acceptance by promoting interoperability. Lastly, since WPA is forward-compatible to 802.11i, it is a future-proof solution that can grow to meet all your future wireless networking needs.