

**Wireless Security - The New 'Keeping the
Bad Guys Out of Your 802.11 Wireless
Network'
2004 Edition**



Wireless Security - The New 'Keeping the Bad Guys Out of Your 802.11 Wireless Network'

May 2004 Update

When this paper was last updated, in September of 2002, we reported that “Concerns over the security of standard 802.11 networks have grown to near hysteric proportions...”. The situation has much improved since that time. We are not exactly out of the woods yet, but at least the path is becoming clear.

WPA

The biggest advance in wireless security over the past year and a half has been the release and growing market acceptance of the Wi-Fi Protected Access (WPA) security specification. The WPA standard was created by the Wi-Fi Alliance in early 2003. The Wi-Fi Alliance began testing WPA compatibility in June 2003, and recently made WPA mandatory for obtaining the Wi-Fi label.

The Wi-Fi Alliance based WPA on the work being done in the IEEE 802.11i task group – specifically on 802.11i Draft 3.0. The Wi-Fi Alliance selected portions of the 802.11i work that were well defined and certain to survive unchanged through the final adoption of the 802.11i standard.

WPA specifies user *authentication* based on 802.1x, enhanced *data encryption* using Temporal Key Integrity Protocol (TKIP) and *data validation* using Message Integrity Check (MIC).

WPA Authentication

802.1x provides a flexible protocol for secure mutual authentication of users and networks. 802.1x is based on the Extensible Authentication Protocol (EAP). Several EAP methods have been developed specifically for wireless applications. These include Transport Layer Security (TLS), Tunneled Transport Layer Security (TTLS), Protected Extensible Authentication Protocol (PEAP) and Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST). A secure mutual authentication method not only prevents unauthorized users from accessing the network, it also prevents rogue access points and man-in-the-middle attacks.

802.1x authentication requires three network components – a supplicant, an authenticator and an authentication server. The supplicant is software on the client device that implements one or more of the 802.1x protocols. The authenticator acts as the gatekeeper for the network and relays 802.1x messages from the supplicant to the authentication server. In an 802.11 network, the access points typically act as the authenticators. The authentication server is responsible to validate that the client has permission to join the network. 802.1x authentication servers are typically RADIUS servers.

WPA also provides an alternate authentication method called Pre-Shared Key (PSK). PSK is provided for residential or small office applications where a secure authentication method is not as critical. PSK authentication does not require the use of an authentication server. PSK requires only two network components – the client supplicant and the authenticator. In this model the access point must implement PSK and is solely responsible for allowing the client onto the network.

WPA Data Encryption

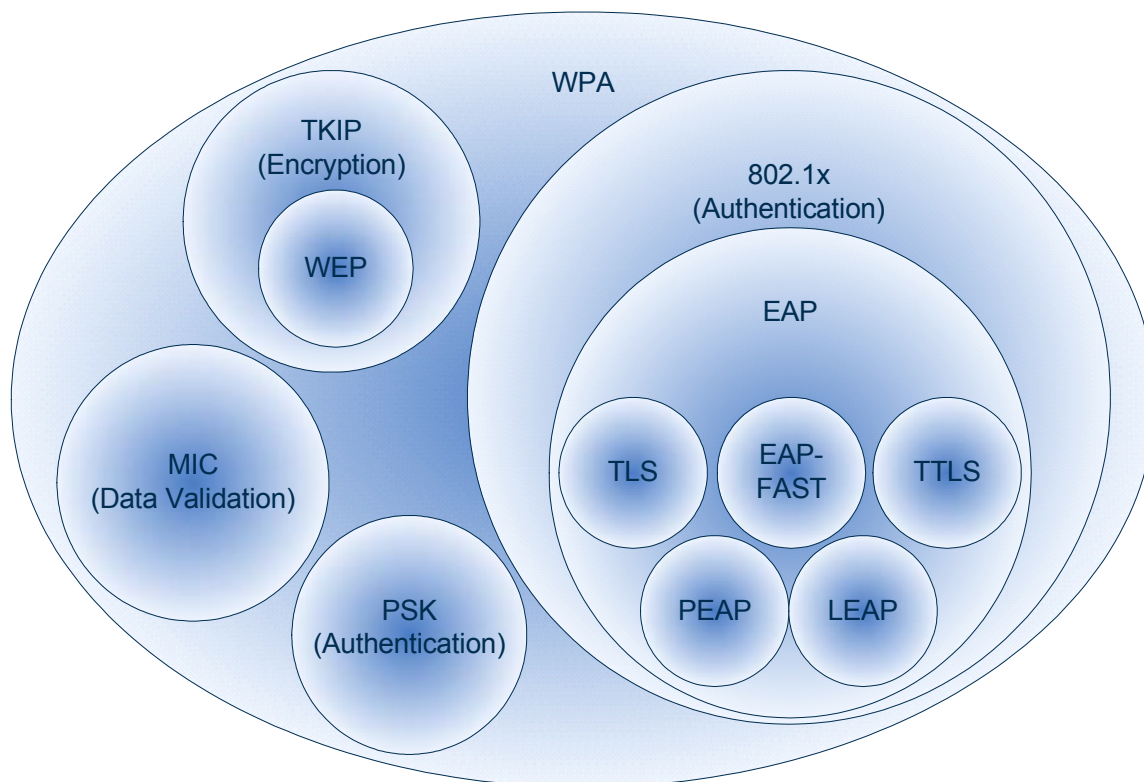
TKIP enhances the Wired Equivalent Privacy (WEP) protocol found in the original 802.11 standard by providing a mechanism to securely alter the WEP key with every data packet. Data encryption in general prevents eavesdropping. TKIP is designed specifically to prevent WEP key attacks such as the one implemented by AirSnort and WEPCrack from working.

Data Validity

MIC replaces the cyclic redundancy check (CRC) algorithm of 802.11 to provide data validity checking. The CRC algorithm used by 802.11 is very easy to circumvent. MIC is much more robust. Data validation procedures guard against both malicious and accidental changes to the data during transit.

WPA, TKIP, MIC, 802.1x, EAP – All These Acronyms!

Security professionals certainly like their acronyms. (But who wants to go around saying “Temporal Key Integrity Protocol”?) It is certainly difficult to keep all these terms straight – particularly because they are all related to each other under the WPA umbrella. The diagram below provides a simplified representation of the relationship of all these protocols.



Note that WPA requires the three components – Encryption, Authentication and Data Validation. TKIP and MIC are required, but for authentication, a choice between 802.1x and Pre-Shared Key is allowed.

WPA for ADC

While the general market acceptance of WPA is the good news, the bad news for the ADC market is that there are currently very few data collection devices that have obtained the WPA certification. Some of the current crop of WPA certified access points are certainly suitable for industrial applications, but the vast majority of the client devices certified at this point are intended for office or consumer applications.

In practical terms, the situation is not as bad as the lack of WPA certification implies. We expect that all ADC hardware vendors are moving toward getting devices certified. In the meantime, it is possible to obtain the functionality of WPA on devices that have not yet passed through the Wi-Fi certification process. This includes devices that can deploy any of several 802.1x authentication protocols, including PEAP, TLS, TTLS and LEAP. These devices can also implement TKIP and MIC.

The security capabilities available for any particular device depend largely upon the operating system installed. There are a very large number of data collection devices still in use that run the DOS operating system. Standards-based 802.1x protocols have proven to be too computationally difficult to deploy on DOS-based platforms. The best security

available for a DOS-based mobile computer today is still Cisco's LEAP protocol, along with Cisco's pre-standard implementation of TKIP (sometimes referred to as CKIP). Of course, this security is available only if a Cisco wireless network is deployed.

As we move to more modern operating systems, the story begins to improve. Starting with Pocket PC 2002 and later versions of Windows CE, security supplicant software is available that implements all of the standards-track 802.1x protocols, along with standard TKIP and MIC. This same also applies to computers running desktop Windows 2000 and Windows XP. Devices equipped with these operating systems can run on any wireless backbone that implements 802.1x, TKIP and MIC – including any of the WPA certified access points listed on the Wi-Fi Alliance web site.

	DOS	WinCE 3.0	PocketPC 2002	WinCE .NET 4.2	Pocket PC 2003	Windows 2000	Windows XP
128-bit WEP	●	●	●	●	●	●	●
Cisco LEAP	●	●	●	●	●	●	●
WPA			●	●	●	●	●
VPN		●	●	●	●	●	●
3 rd Party Security Overlay*		●	●	●	●	●	●

Evaluating Wireless Data Security Options

Up to this point, we have talked a lot about WPA. While WPA security is probably a reasonable goal for most organizations, many companies will find it difficult to implement because they still deploy a large number of older data collection computers that cannot implement WPA.

Network security is always a balance between technical vulnerabilities, the abilities of attackers to exploit those vulnerabilities, the value of the data and resources being exposed, and the costs of increased security. For data collection applications, the cost of increased security may include the cost to upgrade their client computers. In these environments, it may be determined that upgrading to WPA security is not cost effective.

In our September 2002 paper, we described some of the wireless data vulnerabilities and security issues encountered in warehouse and port environments. In this paper, we will assume that our goal is to deploy WPA security if possible, and to provide the 'best reasonable security' if WPA is not possible.

Do Client Computers Support WPA?

- Do all the client computers run Windows 2000/XP, or do they run Windows CE (Pocket PC 2002 or later)?
- Are there radio drivers available for all client computers that support WPA? (Most client radios require updated drivers to support WPA. In some cases, these drivers are not yet available.)
- Most client computers will require third party supplicant software. Does the perceived security risk justify the financial commitment?

If the answers to all the above questions is 'Yes', then it is reasonable to standardize on WPA security and to require all client devices to implement it. Even so, there are still more choices you have to make:

WPA-802.1x or WPA-PSK?

- 802.1x provides better security than Pre-Shared Key, but also requires a RADIUS authentication server. Do you already implement RADIUS? Does your RADIUS server support 802.1x?
- If you do not have RADIUS, do your security concerns justify adding RADIUS to your network?

If you answered 'Yes' to these questions, you will want to implement 802.1x authentication. If not, you should consider Pre-Shared Key authentication. Note, however, that Pre-Shared Key authentication may pose more of an administrative burden than 802.1x, since 802.1x can automatically handle key provisioning.

Which 802.1x Protocol?

Once you have decided to deploy 802.1x authentication, you still will need to choose the 802.1x protocol to run. (You can choose more than one. They are not mutually exclusive, and most RADIUS servers and client supplicants can handle multiple protocols.)

- **EAP-TLS:** This is probably the most secure of the 802.1x protocols in common use. But this security comes at a price. EAP-TLS requires PKI certificates on both the authentication server and on the client computers. It requires more administrative attention than other 802.1x protocols.
- **PEAP:** PEAP is similar to EAP-TLS in that it is based on Transport Layer Security. PEAP, however, does not require certificates on the client computers. PEAP establishes a protected tunnel to pass user credentials back to the authentication server.

There are two versions of PEAP available. One version uses MS-CHAP v2 to authenticate user names and passwords. The second version uses credentials obtained from a Generic Token Card (GTC) to validate the user. Both versions

are commonly supported. However, it is our opinion that the MS-CHAP version is better suited to data collection applications.

- **EAP-TTLS:** EAP-TTLS is very similar to PEAP. EAP-TTLS uses user names and passwords for user authentication. EAP-TTLS is typically available only using third-party supplicant software.
- **EAP-FAST:** EAP-FAST differs from the above protocols in that it does not require any PKI. EAP-FAST designed to place as little burden as possible on the network administrator while still maintaining secure authentication.

We believe that EAP-FAST will become most commonly deployed 802.1x method in data applications. However, this is also the newest protocol, and is not widely implemented at this point.

- **LEAP:** LEAP is an 802.1x implementation proprietary to Cisco. LEAP is very 'lightweight' in terms of administrative or user requirements. It authenticates users based on user names and passwords. LEAP does not require a PKI.

LEAP is the oldest of the wireless oriented 802.1x protocols, and the most widely deployed. Recently published tools to exploit password vulnerabilities in the LEAP protocol have made it less attractive. LEAP should be deployed only if no other 802.1x protocol is supported.

There are other 802.1x protocols available, and probably more will be developed. The above are most commonly found in local area wireless data networks today.

What If Not All Client Computers Support WPA?

It is very common to find that, in today's data collection networks, only a few of the newest products will support WPA. In this case, the decisions become more difficult. Trade-offs will have to be made with respect to upgrading devices to provide WPA and accepting a lesser security implementation.

Can non-WPA Client Computers be Upgraded to Support WPA?

We have already considered the case where client computers can be upgraded to meet the WPA standard through new software. The assumption is that this upgrade would be undertaken. But in many cases, a software upgrade will not suffice. In these cases, the cost/benefit trade-offs become more difficult.

- Can the 802.11 radio be changed to a radio that does support WPA? For some computers, this may be a fairly simple operation that can be performed in the field. For other computers, this may require the device be returned to the manufacturer.
- Can the client computer itself be replaced by a product that supports WPA? For DOS-based data collection computers, this is the only option that meets a WPA security requirement. This is also true for computers running Windows CE 3.0 (but not Pocket PC 2002). Radio and software upgrades are not sufficient to make these products WPA compatible.

Both of the above options can lead to a significant expense. It may be decided that it is best to accept a lesser level of security – at least on certain parts of the network.

Can the Network be Segmented?

If it is possible to segment the network, you can still provide WPA protection on the newest devices while isolating other devices onto restricted network segments. The most efficient way to do this is to implement access-point based VLANs.

- Do the access points support multiple SSID-based VLANs? Most 802.11b access points will support at least 2 VLANs. Many support more. Some older products may require a software upgrade.
- Does the Ethernet infrastructure support VLAN switching? Most Ethernet products today do support VLAN switching. Some very old products may not.

If the answer to these two questions is 'Yes', then create a separate VLAN for devices that do not meet the WPA security standard. This VLAN can be restricted to allow those protocols needed to administer and run the data collection application, and can be restricted to a limited number of host IP addresses.

Even on this isolated VLAN, the best possible security policies should be put in place.

Protecting the non-WPA Clients

If the decision is made that some devices that do not support WPA must remain on the network, the question then becomes one of providing the best possible protection for those devices.

LEAP or WEP?

LEAP has been compromised, but it is still the best security solution available for many products – if you can enforce a strong password policy.

- Do your client devices use Cisco client radios, or CCX v1 client radios?
- Do you use Cisco access points on your wireless network?
- Do you, or can you, deploy an 802.1x compatible RADIUS server?
- Can you enforce strong passwords?

If you answer 'Yes' to these questions, LEAP is a better solution than WEP. The strong password policy should include requiring the longest possible password (8 characters should be the minimum, 10 are better), and should enforce periodic password changes. If possible, passwords should include a mixture of letters, numbers and special characters. (But take into consideration the limitations of the keyboards being deployed. Many data collection devices have only limited keyboards.)

If the answer to any of the above questions is 'No', then you are probably better off running WEP. WEP has also been compromised, but WEP can still provide value in protecting your wireless network. In fact, most vendors have updated their WEP algorithms to thwart the published WEP attacks. It is likely that these WEP attacks could

eventually succeed against the updated algorithms, but it would take many times longer than the figures originally cited.

The biggest problem with WEP is that it has gotten a very bad reputation due to all the negative publicity surrounding the original discovery of the vulnerabilities. Today's WEP algorithms can add a significant level of security to your wireless network.

Proposing WEP as an alternative to LEAP is a bit inappropriate, since LEAP is primarily an authentication service, whereas WEP is primarily intended for data encryption. However, WEP does act as a de facto authentication service. A client can associate to an access point without the WEP key (assuming 802.11 open authentication), but will not be able to transmit any data.

Using TKIP

In some cases, TKIP can be used to enhance WEP data encryption even if WPA is not possible.

- Do your client devices use Cisco client radios, or CCX v1 client radios?
- Do you use Cisco access points on your wireless network?

If you can answer 'Yes' to both of these questions, you can implement Cisco's pre-standard implementation of TKIP. In this case, your best option is to enable WEP along with TKIP. This configuration avoids the dictionary attack vulnerability of LEAP, and also greatly mitigates the WEP key attacks. TKIP effectively changes the WEP encryption key on every packet. WEP hacking tools such as AirSnort have virtually no chance of succeeding when TKIP is active.

Conclusion

The security options for wireless data networks are showing definite signs of improvement. Products conforming to the WPA standard are expected to alleviate the security concerns of most enterprises. These products are now becoming available for Windows laptop applications, but are just starting to appear in products designed for data collection applications.

Over the next year, most new data collection products will include WPA capabilities. In the meantime, enterprises will have to understand their current product mix to design the best available security standards.