WLAN Security Update

Whitepaper for Information Security Professionals

by

Franjo Majstor
franjo@employees.org

April 2004
Version 1.1

Index of Content

Index of Exhibits

1 Introduction and Scope

For the past few years the explosion in deployment of Wireless Local Area Networks (WLANs) was delayed only due to concerns about their security exposures. Since introduction to the market in mid 1999, 802.11 WLAN technologies went through several revisions as 802.11b, 802.11a and 802.11g, while the main headache to all them was numerous vulnerabilities discovered in the 802.11 initial security mechanisms known as Wire Equivalent Privacy (WEP). The Wi-Fi Alliance industry consortium since then made several efforts to address the security issues as well as interoperability of the security solution and as result of that effort in mid 2003 the Wi-Fi Protected Access (WPA) specification was born to address major security issues within the WEP protocol. In spite of all the headaches with their security exposures WLAN technologies have anyway, due to flexibility and easiness in their deployment, already penetrated the IT world in most enterprises as well as public areas, hotels, cafes and airports. Hence, information security professionals have to be aware of the issues with the old and current WLAN technology as well as technical solutions that already exist or are in the development pipe to come soon to the market. The aim of this chapter is to give an overview of the 802.11 WLAN historical security facts and focus on a technical solution that lies ahead.

1.1 Demystifying the 802.11 alphabet

WLAN technology gained its popularity after 1999 through the 802.11***b*** standardization efforts of the IEEE and Wi-Fi Alliance, but 802.***11b*** is definitely not alone protocol within the 802.11 family. 802.11***a*** and ***g*** followed quickly as speed enhancements, while others like ***d,f,h,m,n,k*** or ***i*** are addressing other issues in the 802.11 based networks. For information security practitioners it is important to understand the differences between them as well as to know the ones that have relevant security implications on wireless data communications. Short descriptions and meanings of 802.11 protocols are outlined in Exhibit 1, while more detailed descriptions on most of them can be obtained from the previous version of Information Security Management Handbook as well as the IEEE web site under the 802.11 standards. It is also important to understand that although ***b***, ***a*** and ***g*** versions of 802.11 standard were developed in different times and describe different frequencies, number of channels, and speed of communication, they initially altogether suffered from the same security exposures.

802.11	Description
a	5 GHz, 54 Mbps
b	2.4 GHz, 11 Mbps
d	World mode and additional regulatory domains
e	Quality of Service (QoS)
f	Inter-Access Point Protocol (IAPP)
g	2.4 GHz, 54 Mbps standard backward compatible with 802.11b
h	Dynamic frequency selection and transmit power control mechanisms
i	Security
j	Japan 5 GHz Channels (4.9-5.1 GHz)
k	Measurement
m	Maintenance
n	High-Speed

Exhibit 1: 802.11 Standards

2 Security aspects of the 802.11 WLAN technologies

2.1 Failures of the Past and the Roadmap for the Future

Back in 1999 when the first of the 802.11 standards, 802.11b got ratified, the only security mechanism existing within it was Wired Equivalent Privacy (WEP). Not long after its development, WEP's cryptographic weaknesses began to be exposed. A series of independent studies from various academic and commercial institutions found that even with WEP enabled, third parties can breach WLAN security. A hacker with the proper equipment and tools can collect and analyze enough data to recover the shared encryption key. Although such security breaches might take days on a home or small business WLAN where traffic is light, it can be accomplished in a matter of hours on a busy corporate network. Despite its flaws, WEP provides some margin of security compared with no security at all and remains useful for the casual home user for purposes of deflecting would-be eavesdroppers. For large enterprise users WEP native security can be strengthened by deploying it in conjunction with other security technologies such as Virtual Private Networks or 802.1x authentications with dynamic WEP keys. These have appeared as proprietary vendor solutions already in late 2000. As Wi-Fi users demanded a strong, interoperable, and immediate security enhancement native to Wi-Fi, the Wi-Fi Alliance defined Wi-Fi Protected Access (WPA) as a precursor to the 802.11i standard. In today's terminology the first effort of the Wi-Fi Alliance got named as WPAv1 while the full IEEE 802.11i security standard specification is getting referred as WPAv2. The timeline of this historical evolution as well as the expected finalization of, from the current point in time, not yet finished work is illustrated in Exhibit 2.

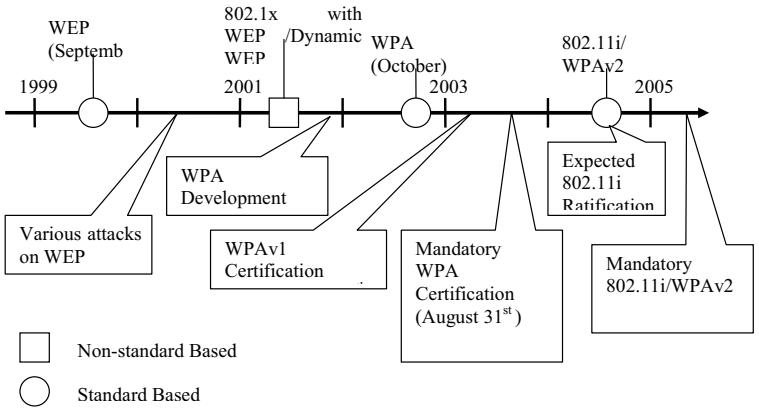


Exhibit 2: 802.11 WLAN Security Technology Evolution

2.2 WLAN Security Threats

It is well known to information security professionals that a security threats analysis of any technology, and the WLAN technology is no exception, is done from the three main aspects: confidentiality, integrity and availability of data. While the first two are addressed in detail, attacks on the WLAN availability in a sense of jamming the radio space or a DoS attack on the WLAN Access Point are serious threats, yet not easy to address by any of the security technologies or protocols that are discussed within this article.

On the other hand, WEP has tackled only confidentiality of the WLAN communication, while it didn't manage to solve the integrity part. Major other missing parts of WEP were the lack of a key management protocol and no user-level authentication as well as cryptographic usage of RC-4 algorithm within WEP. Weaknesses of the WEP protocol and their influence on confidentiality, integrity and authentication are outlined in the Exhibit 3.

Authentication Problem	Confidentiality problem	Integrity problem
One-way authentication	No key management protocol	Bad choice of IV: CRC
No user-level authentication	Insufficient key length	Short IV space
Static and shared WEP key	Bad use of IV	

Exhibit 3: WEP Security Issues

WLAN communication is in particular exposed to unintended parties not necessarily physically located within the network physical boundaries and problems of WEP, even when it is deployed, have opened WLAN's to the possibility of passive eavesdropping that could be also augmented with active eavesdropping. Both, passive and active eavesdropping attacks are exposing the problem of confidentiality of the data sent over the WLAN network while the lack of a mutual authentication scheme is exposing WLAN traffic to a Man-in-the-Middle (MitM) attack. In the MitM attack, the attacker first breaks the connection between the target and the access point and then presents itself as an access point that allows the target to associate and authenticate with it. The target believes that it is interacting with the legitimate access point because the attacker has established a valid session with the destination access point. Once, when the MitM attack is successful and the target is communicating through the intermediary point, this attack can be used to bypass confidentiality and read the private data from a session or to modify the packets thus violating the integrity of a session.
To mitigate outlined threats, the Wi-Fi Alliance has defined the WPA specification which is addressing the weakness of WEP as it is illustrated in Exhibit 4.

3 Industry initiatives

802.11 WLAN technology has its elements developed in several different standardization organizations. IEEE is developing all of 802 standards, while IETF is developing all EAP methods. The Wi-Fi Compatibility Alliance as an industry consortium of the WLAN vendors is on the third side putting together specifications, such as Wi-Fi Protected Access, for interoperability and compatibility testing amongst all WLAN products on the market.

3.1 Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancements that strongly increase the level of data protection and access control for existing and future wireless LAN systems. Wi-Fi Protected Access has in its specification addressed several goals such as strong interoperable security as the replacement for WEP and software upgradeability of existing Wi-Fi certified products. Its targets both home and large enterprise users, and a requirement for its development was to be available immediately. As WPA is derived from IEEE 802.11i standardization efforts, it is also forward compatible with the upcoming standard. When properly installed, WPA provides wireless LAN

users with a high level of assurance that their data will remain protected and that only authorized network users can access the network. The Wi-Fi Alliance started interoperability certification testing on Wi-Fi Protected Access in February 2003 and mandates WPA certification from all vendors shipping WLAN products as of August 31st 2003.

<table>
<tr><th>Area</th><th>WEP's Weakness</th><th>Attack/Problem</th><th colspan="2">WPA</th></tr>
<tr><td rowspan="3">Authentication</td><td>One-way authentication</td><td>MitM Attack</td><td colspan="2" rowspan="4">802.1x/EAP</td></tr>
<tr><td>No user-level authentication</td><td>Theft of device</td></tr>
<tr><td>Bad authentication Algorithm</td><td>Key recovery attack</td></tr>
<tr><td>Key Management</td><td>No key management (static and overhead)</td><td>Management overhead</td></tr>
<tr><td rowspan="5">Encryption</td><td>RC4 Key Scheduling</td><td>Weak key attack</td><td>Per-packet key mixing function</td><td rowspan="5">TKIP</td></tr>
<tr><td>Insufficient Key length</td><td rowspan="2">Collision attack</td><td rowspan="2">Rapid re-keying</td></tr>
<tr><td>Bad use of IV</td></tr>
<tr><td rowspan="2">Bad choice of ICV:CRC</td><td>Replay attack</td><td rowspan="2">Extended IV with sequencing</td></tr>
<tr><td>Forgery attack</td><td>MIC called Michael</td></tr>
</table>

Exhibit 4: WPA vs. WEP

To address the WEP problems, as already illustrated in Exhibit 4, WPA has improved data encryption and user authentication together with a dynamic per user per session key exchange mechanism. Enhanced data encryption is achieved through Temporal Key Integrity Protocol (TKIP). TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, and an extended initialization vector (IV) of 48-bits together with sequencing rules. Through these enhancements, TKIP addresses all so far known WEP's encryption vulnerabilities. For the dynamic per user per session key exchange, WPA relies on Extensible Authentication Protocol (EAP) methods and depending on its use, WPA has several flavors: enterprise, home/SOHO, public, and mixed modes.

3.1.1 Wi-Fi Protected Access for the Enterprise

Wi-Fi Protected Access effectively addresses the WLAN security requirements for the enterprise and provides a strong encryption and authentication solution prior to the ratification of the IEEE 802.11i standard. In an enterprise scenario WPA should be used in conjunction with an authentication server such as RADIUS to provide centralized access control and user level authentication management. It includes enhanced data encryption through TKIP plus per session per user key generation and management protocol via EAP methods.

3.1.2 Wi-Fi Protected Access for Home/SOHO

In a home or Small Office/Home Office (SOHO) environment where there are no central authentication servers or EAP framework, Wi-Fi Protected Access runs in a special home mode. This mode, also called Pre-Shared Key (PSK), allows the use of manually-entered keys or passwords and is designed to be easy to set up for the home user. All the home user needs to do is enter a password (also called a master key) in their Access Point or home wireless gateway and in each PC that is on the Wi-Fi wireless network. WPA takes over automatically from that point. First, the password allows only devices with a matching password to join the network, which keeps out eavesdroppers and other unauthorized users. Second, the password automatically kicks off the TKIP encryption process which defeats known WEP encryption vulnerabilities. As for the WPA manual password security level, it is recommended to use a robust password or a passphrase greater than 8 characters with alpha, numeric and special characters, and no dictionary names.

3.1.3 Wi-Fi Protected Access for Public Access

The intrinsic encryption and authentication schemes defined in WPA may also prove useful for Wireless Internet Service Providers (WISPs) offering Wi-Fi public access in "hot spots" where secure transmission and authentication is particularly important to users unknown to each other. The authentication capability defined in the specification enables a secure access control mechanism for the service providers and for mobile users not utilizing VPN connections.

3.1.4 Wi-Fi Protected Access in "Mixed Mode" Deployment

In a large network with many clients, a likely scenario is that access points will be upgraded before all the Wi-Fi clients. Some access points may operate in a "mixed mode", which supports both clients running WPA and clients running original WEP security. While useful for transition, the net effect of supporting both types of client devices is that security will operate at the less secure level (WEP), common to all the devices. Therefore, benefit of this mode are limited and meant to be used only during the transition period.

3.1.5 Wi-Fi Protected Access and IEEE 802.11i/WPAv2 Comparison

WPAv1 will be forward compatible with the IEEE 802.11i security specification currently still under development by the IEEE. WPAv1 is a subset of the current 802.11i draft, taking certain pieces of the 802.11i draft that are ready to bring to market today, such as its implementation of 802.1x and TKIP. These features can also be enabled on most existing Wi-Fi certified products as a software upgrade. The main pieces of the 802.11i draft that are not included in WPAv1 are secure Independent Basic Service Set (IBSS), also known as ad-hoc mode, secure fast handoff, secure de-authentication and disassociation, as well as enhanced encryption protocols for confidentiality and integrity such as Advance Encryption Standard in the Counter with CBC MAC Protocol (AES-CCMP) mode . These features are either not yet ready or will require hardware upgrades to implement. The IEEE 802.11i specification is expected to be published by the end of 2004 and is already referred to as WPAv2. The comparison function table of WEP, WPAv1 and 802.11i/WPAv2 protocols is illustrated in the Exhibit 5.

Similar to WPAv1, the WPA2-will have several flavors like WPAv2-Enterprise and WPA2-Personal as well as mixed mode WPAv2. WPAv2-Enterprise will be similar to WPAv1 and cover the full requirements for WPA2, including support for 802.1x/EAP based authentication and Pre-Shared Key (PSK). WPA2-Personal will require only the PSK method and not 802.1x/EAP based authentication. In the mixed mode WPAv2 shall be backwards compatible with WPAv1 certified products which means that the WLAN Access Points should be able to be configured and to support WPAv1 and WPA2 clients simultaneously.

Protocol / Function	WEP	WPA	802.11i (WPAv2)
Cipher algorithm	RC4	RC4 with TKIP	AES (CCMP)
Encryption key size	40 bits 104 bits *	128 bits	128 bits
Authentication key size	-	64 bits	128 bits
IV size	24 bits	48 bits	48 bits
Per-packet key	Concatenated	Derived from mixing function	Not needed
Key uniqueness	Network	Packet, Session, User	Packet, Session
Data Integrity	CRC-32	Michael	CCMP
Header Integrity	-	Michael	CCMP
Replay protection	-	IV sequence	IV Sequence
Key Management	-	802.1x/EAP	802.1x/EAP

* Most of the WLAN vendors have implemented 104 bits as extensions to standard WEP

Exhibit 5: Comparison of WEP, WPA and 802.11i/WPAv2

4 802.1x and EAP authentication protocols update

4.1 The Role of 802.1x

IEEE 802.1x is a specification for port-based authentication for wired networks. It has been extended for use in wireless networks. It provides user-based authentication, access control and key transport. 802.1x uses three types of entities: the supplicant which is the client, the authenticator which is the access point or the switch, and the authentication server. The main role of the authenticator is to act as a logical gate to pass only authentication traffic through and block any data traffic until the authentication has successfully completed. Typically, authentication is done on the authentication server which is in most cases the Remote Authentication Dial-In User Service (RADIUS) server. 802.1x is designed to be flexible and

extensible so it relies on Extensible Authentication Protocol (EAP) for authentication, which was originally designed for Point-to-Point Protocol (PPP) but was reused in 802.1x

4.2 The Role of EAP

At the current point in time, there are several EAP protocols defined and implemented using the 802.1x framework available for deployment in both wired and wireless networks. The most commonly deployed EAP protocols are LEAP, PEAP, and EAP-TLS. In addition to these protocols, there are also some newer ones that are trying to address design shortcomings or the vulnerabilities present in the existing protocols.

4.3 xy-EAP: LEAP, MD5, TLS, TTLS, PEAP, …

This section is, after a quick introduction, focusing only on the delta from the article which can be found in the previous version of the Information Security Management Handbook. Details of all EAP methods can be also found on the IETF web site.
The pallet of EAP protocols started with the development of the proprietary mechanisms like LEAP in parallel with standard defined EAP methods like EAP-MD5 and EAP-TLS. By RFC 2284 the only mandatory EAP method is EAP-MD5 and even though this is the easiest one to deploy it is security wise, the least useful one. EAP-MD5 does not provide mutual authentication or dynamic key derivation. The EAP-TLS method is, from a security perspective, the most secure one as it does mutual authentication as well as dynamic key derivation via using public key cryptography with digital certificates for each communicating party. This is making it the most expensive one for deployment.
As a compromise between security and simplicity of deployment, several tunneling EAP methods like EAP-TTLS and EAP-PEAP were developed. They all try to simplify the deployment by using a digital certificate for server authentication while using a password for the user side authentication, and protecting the user credentials exchange via a secure tunnel protected by the public key of the server.
Although at first sight tunneling EAP protocols seemed to be a viable solution for the secure WLAN communication, analysis of the first generation of them gave the result that they are all vulnerable to a Man-in-the-Middle (MitM) attack.

4.4 Known “new” vulnerabilities

4.4.1 Attack on the Tunneled Authentication Protocols

The two main problems of current tunneled authentication methods such as EAP-PEAP and EAP-TTLS amongst the others are that tunneling doesn’t perform mutual authentication and that there is no evidence that tunnel endpoints and authentication endpoints are the same. This makes them vulnerable to a MitM attacks that are possible when one-way authenticated tunnels are used to protect communications of one or a sequence of authentication methods. Since the attacker has access to the keys derived from the tunnel, it can gain access to the network. The MitM attack is enabled whenever compound authentication techniques are used, allowing clients and servers to authenticate each other with one or more methods encapsulated within an independently authenticated tunnel. The simplest MitM attack occurs when the tunnel is authenticated only from the server to the client, and where tunneled authentication techniques are permitted both inside and outside a tunnel using the same credentials. The tunnel client, having not proved its identity, can act as a Man-in-the-Middle, luring unsuspecting clients to authenticate to it, using any authentication method suitable for use inside the tunnel. For the purposes of the MitM attack, it makes no difference whether the authentication method used inside the tunnel supports mutual authentication or not. The vulnerability exists as long as both sides of the tunnel are not required to

demonstrate participation in the previous "tunnel authentication" as well as subsequent authentications, and as long as keys derived during the exchange are not dependent on material from all of the authentications.

Thus, it is the lack of client authentication within the initial security association, combined with key derivation based on a one-way tunnel authentication, and lack of "cryptographic binding" between the security association and the tunneled inner authentication method that enables the MitM vulnerability.

4.4.2 Attack on the LEAP

Let us now look at the one of the first EAP methods which made a compromise between the deployment and security: Lightweight Extensible Authentication Protocol, LEAP is a proprietary protocol developed by Cisco Systems. LEAP has addressed mutual authentication and dynamic key generation with simplicity of deployment at once. It uses a simple user name password mechanism for mutual authentication and, hence, is very simple to deploy. Based on the mutual challenges and responses, it generates a per user per session unique key as is illustrated in Exhibit 6.

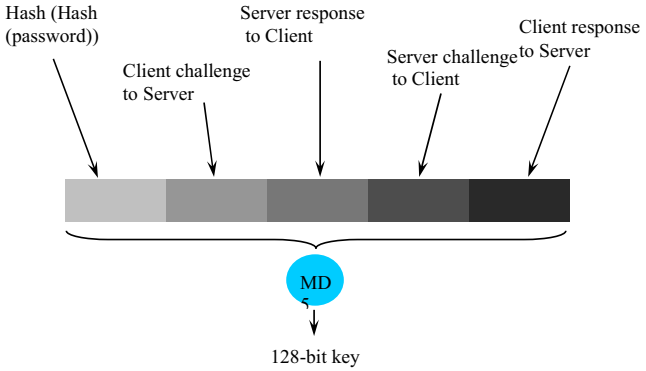


Exhibit 6: LEAP Key Generation

Compromise in simplicity of course has its price. Almost any password based protection could be exposed to a dictionary attack. Considering that LEAP due to its design cannot provide support to OTP (One Time Password) technology and considering that an average user typically doesn't invent, remember or maintain strong passwords, it seems to be logical to think of a LEAP key generation as vulnerable to a dictionary attack. With users using weak passwords and a knowledge of the LEAP key generation scheme, it is not that difficult to mount a dictionary attack on it. This was recognized at the very beginning yet it became a serious threat once tools such as ASLEAP were publicly released on the Internet. The ASLEAP tool simply reads in an ASCII file of dictionary words and associated hashes of those words and does brute-force LEAP challenge and response exchanges. Sample screen output from the tool is illustrated in Exhibit 7.

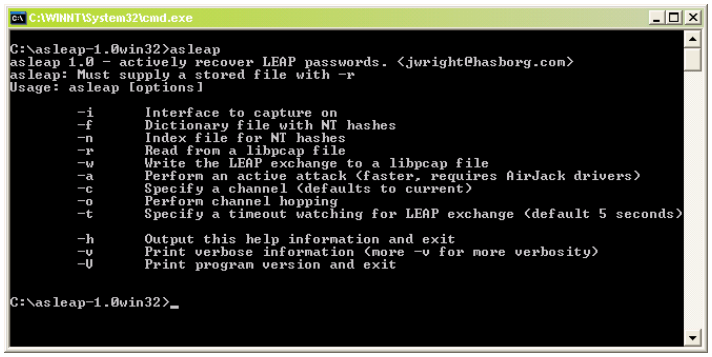


Exhibit 7: ASLEAP Tool Screen Sample

There are two follow up protocols that are standing in front to solve the problems with MitM and dictionary attacks on current EAP methods yet keep the promise of easiness of their deployment. These are the next generation of PEAP, PEAPv2 and EAP-FAST.

4.5 PEAPv2

The Protected EAP (PEAP) protocol is an EAP authentication method that uses digital certificate authentication for the server-side only, while for the client-side authentication PEAP can use any other authentication mechanisms like certificates or simple user name and password where username password exchange is done via a protected tunnel. Like multiple other first generation tunneled authentication protocols which do not provide cryptographic binding between a tunnel authentication and other EAP methods, the PEAPv1 is also vulnerable to MitM attacks. This has been fixed in PEAPv2. PEAPv2, same as original PEAPv1, uses TLS to protect against rogue authenticators and against various attacks on the confidentiality and integrity of the inner EAP method exchange as well as providing EAP peer identity privacy. Other benefits of PEAPv2 include dictionary attack resistance and header protection via protected negotiation. PEAPv2 also provides fragmentation and reassembly, key establishment and a sequencing of multiple EAP methods.

Since all sequence negotiations and exchanges are protected by the TLS channel, they are immune to snooping and MitM attacks with the use of cryptographic binding. To make sure that the same parties are involved in establishing the tunnel and EAP inner method, before engaging the next method to send more sensitive information, both peer and server must use the cryptographic binding between methods to check the tunnel integrity. PEAPv2 prevents a MitM attack by using the keys generated by the inner EAP method in the cryptographic binding exchange in a protected termination section. MitM attack is not prevented if the inner EAP method does not generate keys (e.g., case of EAP-MD5) or if the keys generated by the inner EAP method can be compromised.

Even though PEAPv2 addresses MitM attacks and multiple other security issues, it still requires usage of the public key cryptography at least for the server authentication as well as for the tunnel protection.

While public key cryptography does its function for protection, it also causes a slower exchange and requires a higher performing CPU capability at the end node devices.

4.6 EAP-FAST

A protocol which avoids the use of public key cryptography can be easier deployed on small, mobile and skinny devices with low CPU power. Avoiding public key cryptography also makes roaming faster. Fast Authentication via Secure Tunneling (FAST) is the new IETF EAP method proposed to protect wireless LAN users from hacker dictionary or MitM attacks. EAP-FAST enables 802.11 users to run a secure network without the need for a strong password policy or certificates on either end of the client/server point connection. A simple feature and performance comparison of other tunneled authentication EAP protocols with EAP-FAST is illustrated in Exhibit 8.

EAP Method / Requirements	EAP-TTLS	EAP-PEAP	EAP-FAST
PKI infrastructure required	Yes	Yes	No
Suitable for Skinny Devices	No	No	Yes

Exhibit 8: Basic Comparison of EAP-TTLS, EAP-PEAP and EAP-FAST

The EAP-FAST protocol is a client-server security architecture that encrypts EAP transactions within a TLS tunnel. While similar to PEAP in this respect, it differs significantly in the fact that EAP-FAST tunnel establishment is based upon strong shared secrets that are unique to users. These secrets are called Protected Access Credentials (PACs). Because handshakes based upon shared secrets are intrinsically faster than handshakes based upon a PKI infrastructure, EAP-FAST is significantly faster than solutions which provide protected EAP transactions based on PKI. EAP-FAST is also easy to deploy and allows smooth migration from LEAP due to the fact that it does not require digital certificates on the clients or on the server side.

4.6.1 How EAP-FAST Works

EAP-FAST is a 2-phase mutual authentication tunneling protocol. Phase 1 uses a pre-shared secret named Protected Access Credential (PAC) to mutually authenticate client and server and also create the secure tunnel between them. PAC is associated with a specific Initiator ID (client) as well as with an Authority ID (server) and is used only during Phase 1 of the EAP-FAST authentication. As the Phase 2 exchange is protected by the Phase 1 mutually authenticated tunnel, it is sufficient for the inner EAP method to use a simple username and password authentication scheme. By deploying the tunnel endpoints mutual authentication and a cryptographically binding it to the following inner EAP method, the EAP-FAST has successfully addressed the MiTM attack, while secure tunnel protects the EAP exchange from a dictionary attack. Simplicity of deployment with EAP-FAST is achieved with both simple user authentication and a PAC. PAC, even though it looks like a certificate with fields like Initiator ID and Authority ID, version and expiration, completely removes the need for a PKI infrastructure and digital

certificates. The PAC is the shared security credential generated by the server for the client and consists of the following three parts:

1. PAC-Key: a 32-byte key used by the client to establish the EAP-FAST Phase 1 tunnel. This key maps as the TLS pre-master-secret and is randomly generated by the server to produce a strong entropy key.
2. PAC-Opaque: a variable length field that is sent to the server during the EAP-FAST Phase 1 tunnel establishment. The PAC-Opaque can only be interpreted by the server to recover the required information for the server to validate the client's identity.
3. PAC-Info: a variable length field used to provide the identity of an authority or PAC issuer and optionally the PAC-Key lifetime.

Details of the PAC are illustrated in Exhibit 9.

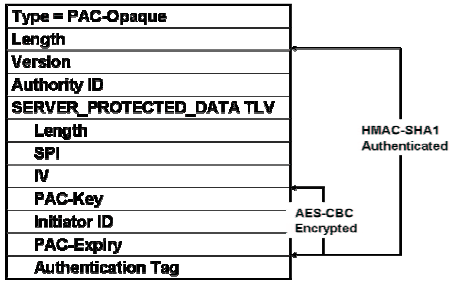


Exhibit 9: Protected Access Credential (PAC) Details

On the other hand, the PAC also needs to be provisioned. PAC provisioning to the client can be done manually out-of-band through some external application tool, or dynamically via the in-band PAC-Auto-Provisioning mechanism defined in the EAP-FAST protocol specification. Overall, the two major differences between EAP-FAST and any other PKI based tunneled EAP method is that EAP-FAST has only one step provisioning of security credentials, and lower power consumption due to the fact that it does not require use of the PKI based authentication which makes it very attractive for deployment on low end devices as already illustrated on Exhibit 8.

4.7 EAP Methods Functionality Comparison

With invention of new EAP methods as well as their scrutiny against new and old security vulnerabilities, the job of information security professionals with regards of WLAN technology and its security aspects did not get much easier. The choice of which EAP method to deploy is most of the time not based on its security but rather on the risk acceptance and most of all on functionality that can be achieved with it. Last but certainly not the least decision point is the availability of the specific products on the market that implement a certain EAP method. While availability of the products on the market will change during the

time, the information security professional should be aware of the security function brought by each of the EAP methods. A summarized view that compares features, security vulnerabilities as well as deployment complexity of the latest EAP methods is given in Exhibit 10.

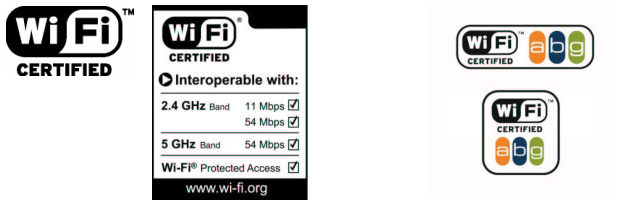
EAP Method / Feature/ Vulnerability	Cisco LEAP	EAP-FAST	Microsoft PEAP (MS-CHAPv2)	Cisco PEAP (EAP-GTC)	EAP-TLS
Single Sign-On (MS AD)	Yes	Yes	Yes	No	Yes
Login Scripts (MS AD)	Yes	Yes	Yes	Yes	Yes
Password Change (MS AD)	No	Yes	Yes	Yes	N/A
LDAP DB support	No	Yes	No	Yes	Yes
OTP Authentication Support	No	Yes*	No	Yes	No
Server Certificate Required	No	No	Yes	Yes	Yes
Client Certificate Required	No	No	No	No	Yes
Dictionary Attacks	Yes	No	No	No	No
Susceptible to MITM Attacks	No	No	Yes	Yes	No
Deployment Complexity	Low	Low	Medium	Medium	High

*EAP-FAST protocol has capability to support OTP while Cisco Systems initial implementation does not support it.

Exhibit 10: Detailed Comparison of EAP Modes

5 Interoperability

The main task of standards is to drive interoperability. However interpretation of the standard specifications or, in particular, parts which are mandatory to implement versus optional ones are arguments why there is a need for interoperability testing and accreditation. Wi-Fi Alliance has achieved significant results on the market with Wi-Fi technology interoperability testing and has successfully launched the Wi-Fi logos which are illustrated in Exhibit 11.



Logo and label are valid until 31 Dec **New logo valid from 1 March**

Exhibit 11: Wi-Fi Alliance Logos

It is now repeating the success with new WLAN security specifications by defining and mandating the WPAv1 and soon WPAv2 as the integral part of the same accreditation. Important is however to understand that interoperability testing could not possible test every single combination of features but is rather limited to a subset of the existing ones. An example of that is the WPAv1 which mandates the use of TKIP and Michael MIC, while it leaves open which EAP methods to be used, so the interoperability testing is done only with the most pervasive methods such as EAP-TLS for enterprise mode or PSK for home use. The WPAv2 specification will include on top of that minimum the new AES crypto suite interoperability testing as well as backward compatibility modes. Some countries on the other hand, due to economical or political reasons, decided to take their own path in addressing the WLAN security issues. On May 12 2003, China issued two WLAN security standards which became compulsory on Dec 1, 2003. The information security portion of these standards specifies the WLAN Authentication and Privacy Infrastructure (WAPI) which appears to differ significantly and is incompatible with WPA or 802.11i. Many details required for implementation of the standard are not fully defined, including encryption, authentication, protocol interfaces and cryptographic module APIs. Up to the current point of time, the Wi-Fi Alliance efforts to obtain the details of the WAPI specification were not successful which makes WAPI specification based products unfortunately completely out of the interoperability scope of the Wi-Fi Alliance.

6 Future directions

6.1 WLAN Mobility and Roaming

Although one could think of the WLAN technology as mobile, actually it is not. A particular WLAN client associated to a particular WLAN Access Point (AP) is mobile only within the range of this particular AP. If it would require moving and associating to an AP from another vendor or different service provider, this will be not possible as the 802.11 specification does not stipulate any particular mechanism for roaming. Therefore, it is up to each vendor to define an algorithm for its WLAN clients of how to make roaming decisions. The basic act of roaming is making a decision to roam, followed by the act of locating a new AP to roam to. This scenario can involve reinitiating a search for an AP, in the same manner the client would when it is initialized, or another means, such as referencing a table built during the previous association. The timing of WLAN roams also varies according to vendor, but in most cases is less than 1 second, and in the best cases, less than 200 msec.

6.2 Fast and secure roaming

The two main goals for roaming are to be fast and to be secure. While the speed of roaming is important for delay sensitive applications such as voice over IP, security aspects of the roaming are even more important. Speed and a security are also most of the time technically opposite requirements. While we have seen that security solutions for the 802.11 WLAN technologies are rapidly progressing, combining them with roaming presents another challenge of a centralized key management structure, like it is illustrated in Exhibit 12.

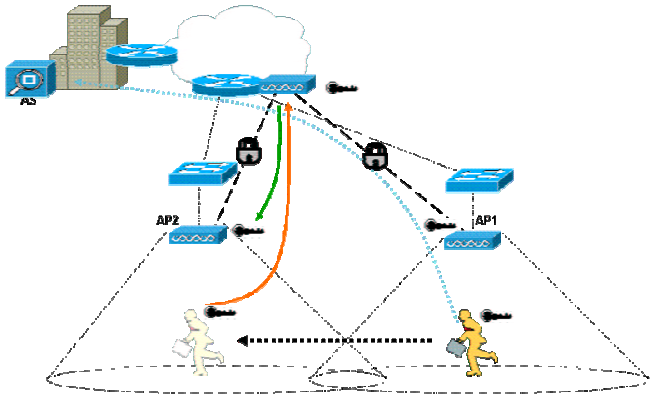


Exhibit 12: Security and Roaming

The roaming mobile device, which has already associated and finished its secure association with AP1, moving to an AP2 would need to re-start all the security session negotiations, which is both a time and CPU expensive task. This would not be necessary if there is a third party keeping all the necessary security information about the existing session of a particular mobile device with AP1.
Both topics, the roaming and the security of the roaming are so far only future standardization topics that are depending only on the particular vendor implementations. Fast Secure Roaming is an example of the proprietary solution coming from Cisco Systems which follows the model of centralized key management. With Fast Secure Roaming, authenticated client devices can roam securely at layer two from one access point to another without any perceptible delay during re-association because the central Wireless Domain Services (WDS) device acts as the centralized key management server that keeps and distributes necessary security session information to all the AP's involved in the roaming process. That releases the client from running the CPU expensive security portion of the re-association process and saves the time necessary to gain on the speed of the overall secure roaming process.

7 Securing WLAN with IPsec or SSL VPN

With all the security issues surrounding the WLAN technology, relying on another technology such as VPN, to help in solving security issues seems to be at first sight a viable solution. Especially in the case of a growing interest in Web VPN based technology that promises ease of use and no additional client installation. It is important though to understand that even VPN technology has its own limitations. In case of an IPsec for example, it is not possible to transport multicast IP traffic, while in case of a Web VPN there is a limitation of the number and type of supported applications. It is also important to understand that the integrity, authentication and confidentiality functions in both VPN scenarios most of the time are done in software which could be either a bottleneck or even not supported on low CPU handheld devices. Last but not least, while roaming with a Web based VPN doesn't seem to be an issue,

roaming with an IPsec based VPN opens a can of worms with security issues and a special Mobile IP client stack underlying the IPsec client that requires the IP Home and Foreign Agent capable IP gateway devices. These are just some of the issues which have to be considered before doing an offload of the security role from WLAN technology to VPN technologies.

8 Summary

This article went through the brief historical overview of the 802.11 WLAN security issues with the sole purpose of helping the information security professional to understand the current and future development of security solutions within the 802.11 WLAN technology space. Even though the WLAN technology had a few security hiccups at the beginning it is, in spite of those, rapidly spreading around and is already present in almost every modern network environment. Security solutions, such as WPAv1, are finding the ground, new ease of deployment protocols such as EAP-FAST are already appearing on the horizon, and the future security specification WPAv2 is coming soon out as well. In that entire matrix it is not trivial to look for a proper solution without understanding the building blocks of the WLAN security technology and the threats on the WLAN protocols that don't address them properly. TKIP is on one side through WPAv1 addressing all known WEP vulnerabilities, while 802.1x and EAP methods are delivering promised user level authentication together with a key exchange mechanism. Some of the EAP methods like LEAP, were already exposed to publicly available hacking tolls. Others, like PEAP that is vulnerable to the Man-in-the-Middle attack, got fixes with cryptographic binding of the tunnel and inner EAP authentication method on time and before the exploits were available. It is now on the shoulders of the information security professional to recognize the method, protocol or solution as they are being implemented in particular vendor solution and do a proper risk analysis of the exposures versus ease of use before letting them be deployed in any modern network environment.

9 List of Acronyms

AES - Advanced Encryption Standard
CBC - Cipher Block Chaining
CCMP - Counter with CBC MAC Protocol
CRC - Cyclic Redundancy Check
CSMA/CD - Carrier Sense Multiple Access Collision Detect
EAP - Extensible Authentication Protocol
EAP-FAST - Extensible Authentication - Fast Authentication via Secure Tunneling
GTC - Generic Token Card
IBSS - Independent Basic Service Set
IV - Initialization Vector
LEAP - Lightweight Extensible Authentication Protocol
MAC - Message Authentication Code
MD5 - Message Digest 5
MIC - Message Integrity Check
MitM - Man-in-the-Middle attack
MS-CHAPv2 - Microsoft Challenge Handshake Authentication Protocol version 2
OTP - One Time Password
PAC - Protected Access Credential
PEAP - Protected Extensible Authentication Protocol
PKI - Public Key Infrastructure
PPP - Point-to-Point Protocol
PSK - Pre-Shared Key
RADIUS - Remote Authentication Dial-In User Service
SSID - Service Set Identifier
SSL - Secure Socket Layer
TLS - Transport Layer Security
TLV - Type Length Value
TTLS - Tunneled Transport Layer Security
VPN - Virtual Private Network
WAPI - WLAN Authentication and Privacy Infrastructure, Chinese specification
WEP - Wire Equivalent Privacy
WISP - Wireless Internet Service Provider
WLAN - Wireless Local Area Network
WPA - Wi-Fi Protected Access

10 References

[1] Aboba, B., Simon, D., PPP EAP TLS Authentication Protocol, RFC 2716, October 1999.

[2] Andersson, H., Josefsson, S., Zorn, G., Simon, D., Palekar, A., Protected EAP Protocol (PEAP), IETF Internet Draft, < draft-josefsson-pppext-eap-tls-eap-05.txt>, September 2002.

[3] AT&T Labs and Rice University paper, Using the Fluhrer, Mantin, and Shamir Attack to Break WEP, <www.cs.rice.edu/~astubble/wep/wep_attack.pdf>, August 21st 2001.

[4] Blunk, L.,Vollbrecht, J., EAP PPP Extensible Authentication Protocol (EAP), RFC 2284, March 1998.

[5] Cam-Winget, N. et al EAP Flexible Authentication via Secure Tunneling (EAP-FAST), IETF Internet Draft, <draft-cam-winget-eap-fast-00.txt>, February 2004.

[6] Cisco Response to Dictionary Attacks on Cisco LEAP, Product Bulletin No. 2331 <www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a00801cc901.html>

[7] Fluhrer, S., Mantin, I., Shamir, A., Weaknesses in the Key Scheduling Algorithm of RC4, <www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps>

[8] Funk, P., Blake-Wilson, S., EAP Tunneled TLS Authentication Protocol (EAP_TTLS), IETF Internet Draft, <draft-ietf-pppext-eap-ttls-01.txt >, February 2002.

[9] Greem, Brian C., Wi-Fi Protected Access, <www.wi-fi.net/opensection/pdf/wi-fi_protected_access_overview.pdf>, October 2002.

[10] IEEE TGi meetings update site <grouper.ieee.org/groups/802/11/Reports/tgi_update.htm>

[11] Palekar, A. at al, Protected EAP Protocol (PEAP) Version 2, IETF Internet Draft, <draft-josefsson-pppext-eap-tls-eap-07.txt>, October 2003.

[12] Puthenkulam, J. at al, The Compound Authentication Binding Problem, IETF Internet Draft, <draft-puthenkulam-eap-binding-04.txt>, October 2003.

[13] SAFE: Wireless LAN Security in Depth, white paper from Cisco Systems, Inc.,<Cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm>

[14] Tipton F. H., Krause M., Information Security Management Handbook, Fifth Edition, Auerbach Publications, 2004

[15] Wi-Fi Alliance WPA specification, <www.wi-fi.com/OpenSection/protected_access.asp>

[16] Wright, J. As in "asleap behind the wheel" <asleap.sourceforge.net>