The State of Wi-Fi® Security

Wi-Fi CERTIFIED™ WPA2® Delivers Advanced Security to Homes, Enterprises and Mobile Devices

Wi-Fi Alliance®
September 2009

Executive Summary

Wi-Fi is one of the most widely used and trusted technologies in the world, with a strong, globally recognized brand. Users value its reliable performance, simplicity, and wide availability. Wi-Fi is everywhere—at work, at home, in public hotspots. Users access Wi-Fi networks with laptops, mobile phones, cameras, game consoles, and an increasing number of other consumer electronic devices.

The Wi-Fi Alliance promotes adoption and technological innovation of Wireless Local Area Network (WLAN) equipment, and interoperability through its Wi-Fi CERTIFIED™ program. Wi-Fi CERTIFIED equipment brings out-of-the-box multivendor interoperability, and great performance.

Enterprise, home, and mobile users know that Wi-Fi also provides state-of-the-art, standards-based, advanced security. Wi-Fi CERTIFIED equipment meets the security requirements of essential corporate networks and applications, and allows residential users to protect their networks.

Security has been at the core of the Wi-Fi Alliance efforts since the program launch in 2000. Wired Equivalent Privacy (WEP) was the first-generation solution. The Wi-Fi Alliance introduced Wi-Fi Protected Access® (WPA) in 2003 as an interim security solution to address market demand for more robust security mechanisms while the Institute of Electrical and Electronics Engineers (IEEE) 802.11i amendment was being developed. WPA addressed WEP vulnerabilities by providing mutual authentication and stronger encryption.

Wi-Fi security timeline
Wi-Fi Alliance certification program started in 2000 and included support for WEP
WPA certification was introduced in 2003 as an interim solution in anticipation of the ratification of the IEEE 802.11i amendment
WPA2 with AES encryption and EAP support was introduced in 2004, and became mandatory in 2006
Wi-Fi Protected Setup™ was introduced in 2007 as an optional certification program to simplify setup and expansion of security-protected home and small office networks
In 2009 the Wi-Fi Alliance expanded the list of supported Extensible Authentication Protocol (EAP) types to seven, with the addition of EAP-Authentication and Key Agreement (EAP-AKA) and EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)

WPA2 is today's generation of Wi-Fi security. It is founded on two key protocols: (1) Advanced Encryption Standard (AES), the encryption protocol used by the United States and other governments to protect confidential and classified information, and by the enterprise to secure WLANs, and (2) IEEE 802.1X, a standard widely used in corporate networks to provide robust authentication and sophisticated network access control features. WPA2 is based on IEEE 802.11i and provides 128-bit AES-based encryption. It also provides mutual authentication with Pre-Shared Key (PSK; in Personal mode) and with IEEE 802.1X / EAP (in Enterprise mode). In 2004 the Wi-Fi Alliance introduced WPA2 certification. In 2006 WPA2 certification became mandatory for all Wi-Fi CERTIFIED equipment submitted for certification. In addition, in 2007 the Wi-Fi Alliance introduced the Wi-Fi Protected Setup program to simplify and encourage the activation of WPA2 in residential networks.

With WPA2, Wi-Fi technology has reached a mature state that allows it to provide excellent, state-of-the-art security to all Wi-Fi users, across different device form factors, vendors, and geographical regions. The Wi-Fi Alliance is committed to expanding existing certification programs and creating new ones to promote adoption of new security solutions that benefit users.

Introduction

Wi-Fi is everywhere. About one-third of US households with broadband Internet access have a Wi-Fi network[1]. Two billion Wi-Fi chipsets are forecasted to be shipped by the end 2009; this number is forecast to reach 7 billion by 2013[2], with one of the highest growth rates in mobile and consumer electronic devices.

Since the introduction of its certification program in March 2000, the Wi-Fi Alliance has led efforts to foster the adoption, interoperability, and advancement of the technology. With more than 300 members and thousands of certified products, the Wi-Fi Alliance has been a driving force for the entire Wi-Fi ecosystem, including service providers, chipset and device vendors, and software developers.

Wi-Fi CERTIFIED products are subject to rigorous tests to help ensure interoperability and a great user experience. Consumer and enterprise users trust the Wi-Fi CERTIFIED brand and know that it consistently delivers out-of-the box interoperability, reliable performance, and the best user experience for a wide range of devices, including laptops, phones, and other mobile and consumer electronic devices.

Market success depends on more than user experience and interoperability. The rapidly growing numbers of home, enterprise, and mobile Wi-Fi adopters want more than interoperable, reliable, easy-to-use, and high-performing devices and access points. They need secure technology that protects their data and controls network access across their business, personal and mobile use. Peace of mind and trust are crucial ingredients of a great user experience.

All environments—residential, enterprise, and mobile—require high levels of protection. Wi-Fi is used to send confidential and personal information in a multitude of scenarios. Enterprise users use Wi-Fi to exchange highly sensitive information with colleagues, partners, and customers. Home and mobile users routinely use Wi-Fi to share private information with family and friends. Increasingly, customers in all environments are using voice over Wi-Fi in addition to data.

Protection of Wi-Fi devices and networks has been a pillar of the Wi-Fi CERTIFIED testing program from its inception. Support for WPA2 security has been mandatory for all Wi-Fi CERTIFIED equipment since early 2006. The Wi-Fi Alliance has taken a leading role in establishing WPA2 as a globally accepted, mature standard that is supported by all major vendors.

The Wi-Fi Alliance provides Wi-Fi users with the highest levels of security available using standards-based mechanisms, and with security interface tools that are easy to use and that promote adoption of security best practices. At the same time, the Wi-Fi Alliance recognizes that there is a need for multiple solutions to meet the security requirements of different use cases and devices. As a result, the Wi-Fi certification program has the flexibility to enable Wi-Fi CERTIFIED equipment to meet the requirements of different types of networks—ranging from a highly

---

[1] Source: Parks Associates
[2] Source: ABI Research

controlled corporate environment to a much more flexible home network—and to operate in different device form factors.

This paper presents an assessment of the state of Wi-Fi security, covering the evolution of the certification program to offer increasingly advanced and easy-to-use tools, and the key features supported by Wi-Fi CERTIFIED equipment. At the end of the paper, a case study on the University of Texas at Dallas illustrates how to secure a campus-wide Wi-Fi network with WPA2.

The Evolution of Wi-Fi Security

Wi-Fi technology has evolved quickly to adapt to changing market and technological conditions. Global adoption of WPA and WPA2 advanced security mechanisms has further strengthened trust and reliance on Wi-Fi CERTIFIED equipment worldwide (Table 1).

Date	Milestone
September 1997	IEEE 802.11 standard ratified, including WEP
April 2000	Wi-Fi CERTIFIED program launched, with support for WEP
May 2001	IEEE 802.11i task group created
April 2003	WPA introduced with: • IEEE 802.1X authentication • Temporal Key Integrity Protocol (TKIP) encryption • Support for EAP-Transport Layer Security (EAP-TLS)
September 2003	WPA mandatory for all Wi-Fi CERTIFIED equipment
June 2004	IEEE 802.11i amendment ratified
September 2004	WPA2 introduced with: • IEEE 802.1X authentication • AES encryption • Support for EAP-TLS
April 2005	Support for four additional EAP-types added: • EAP-Tunneled TLS Microsoft Challenge Handshake Authentication Protocol Version 2 (EAP-TTLS/MSCHAPv2) • Protected EAP Version 0 (PEAPv0)/EAP-MSCHAPv2 • Protected EAP Version 1 (PEAPv1)/EAP Generic Token Card (EAP-GTC) • EAP-Subscriber Identity Module (EAP-SIM)
March 2006	WPA2 mandatory for all Wi-Fi CERTIFIED equipment
January 2007	Wi-Fi Protected Setup program launched
November 2007	IEEE 802.11w task group created
May 2009	Support for EAP-AKA and EAP-FAST added

Table 1. Wi-Fi security timeline

The evolution of Wi-Fi security has been enabled by technological advances in access control and encryption, and the parallel standardization work—markedly within the IEEE 802.11i (Media Access Control [MAC] Layer Security Enhancements) and the IEEE 802.11w (Protected Management Frames) task groups.

New applications and usage scenarios that have become prominent with the growth of Wi-Fi adoption have led to the availability of new security mechanisms. Several years ago, the rapid spread of Wi-Fi in residential and enterprise networks increased the scrutiny of WEP, and its limitations were soon identified. Furthermore, the emergence of Wi-Fi as the primary access technology at home, the rising popularity of public hotspots, and the deployment of enterprise networks carrying sensitive and mission-critical data increased the security requirements for Wi-Fi.

As a first-generation security solution, WEP was vulnerable due to limitations in key size (initially 40 bits, later extended to 104 bits) and its lack of replay detection. As a result, users had to complement WEP with Virtual Private Networks (VPNs), IEEE 802.1X, or proprietary solutions to meet their security needs.

By 2003, the Wi-Fi Alliance had already moved to WPA, which included a subset of the IEEE 802.11i amendment features. WPA was a second-generation interim solution designed to address WEP vulnerabilities in anticipation of the ratification of the IEEE 802.11i amendment, which was later incorporated into the IEEE 802.11-2007 standard and specified security mechanisms for Wi-Fi (Table 2). WPA uses TKIP for data encryption. WPA authentication is provided by IEEE 802.1X with EAP for enterprise users and by PSK for residential and consumer users.

Concurrently with the ratification of the IEEE 802.11i amendment in 2004, the Wi-Fi Alliance introduced WPA2. Initially it was an optional certification, but in 2006 it became a mandatory requirement for new equipment submitted for certification designed to supersede WPA. While building on the WPA features, WPA2 introduced stronger encryption with the adoption of the CCMP protocol with the AES block cipher. All Wi-Fi CERTIFIED equipment tested since 2006 supports WPA2 and gives Wi-Fi users access to the most advanced standards-based security mechanisms. WPA2 has quickly become the most widely used and trusted security framework for Wi-Fi equipment.

	WEP	WPA	WPA2
Encryption	Manual key assignment, shared keys using Rivest Cipher 4 (RC4) stream cipher	TKIP based on RC4 stream cipher	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) with 128-bit AES block cipher
Data integrity	Linear hash function	Cryptographic hash function	
Key management	No	Yes	
Replay detection	No	Yes	

Table 2. WEP, WPA, and WPA2 compared

Technology Overview of WPA2

Widespread acceptance and trust among vendors and users of WPA2 is due to four key factors:

- **Mutual authentication.** WPA2 uses IEEE 802.1X (WPA2-Enterprise) and PSK (WPA2-Personal) to provide mutual authentication. With one-way authentication, the client device sends its credentials and, if access is authorized, the client device is connected to the network. Mutual authentication requires the client device to verify the network credential before establishing the connection, to prevent the user from connecting to unauthorized access points.

- **Strong encryption.** AES is defined as a Federal Information Processing Standard (FIPS Publication 197) and is the first publicly available encryption mechanism that meets the requirements of the U.S. government for protecting sensitive and classified information[3]. To date, AES has proved to be extremely resilient in the face of the high number of published attacks triggered by AES's wide adoption. The data travelling across a WPA2 network is encrypted using the CCMP algorithm with AES, which together provide the most advanced standards-based data encryption method available. AES support is required by many protocols and applications used worldwide in enterprise networks.

- **Interoperability.** WPA2 is a standards-based solution, supported by all Wi-Fi CERTIFIED equipment that has undergone testing since 2006. WPA2 can be activated within any session in which the access point and the client device support WPA2, regardless of the equipment brands involved. This greatly expands the availability of WPA2 and gives confidence to network operators and users that their networks, devices, and data flows can be protected everywhere.

- **Ease of use.** WPA2 is not only a powerful tool to protect Wi-Fi users, it is also easy to activate. In 2007 the Wi-Fi Alliance introduced a separate certification program, Wi-Fi Protected Setup, to simplify the configuration of WPA2 and to accelerate its adoption in residential networks.

WPA2-Enterprise and WPA2-Personal

WPA2 operates in two modes, Enterprise and Personal, depending on the requirements of the network (Table 3). Support for WPA2-Personal is mandatory in all Wi-Fi CERTIFIED client devices and access points. Support for WPA2-Enterprise is optional, but recommended for devices working in large-scale networks. Specific security requirements dictate which mode is used within a network.

Residential and small office networks typically use WPA2-Personal, because it does not require any equipment beyond a Wi-Fi CERTIFIED access point and device. In WPA2-Personal the key is derived from the network Service Set Identifier (SSID) and a passphrase entered by the user. The selection of a strong passphrase is required in order to take full advantage of WPA2 protection. Long, complex, and random passphrases are crucial to good security, as are frequent passphrase changes.

Enterprise networks with IEEE 802.1X Authentication, Authorization, Accounting (AAA) servers can benefit from the more sophisticated functionality afforded by WPA2-Enterprise, which includes the ability to monitor and manage traffic, to define user-specific authentication levels, and to offer guest access. WPA2-Enterprise also allows wireless access to be integrated with the overall network access control by sharing existing user databases.

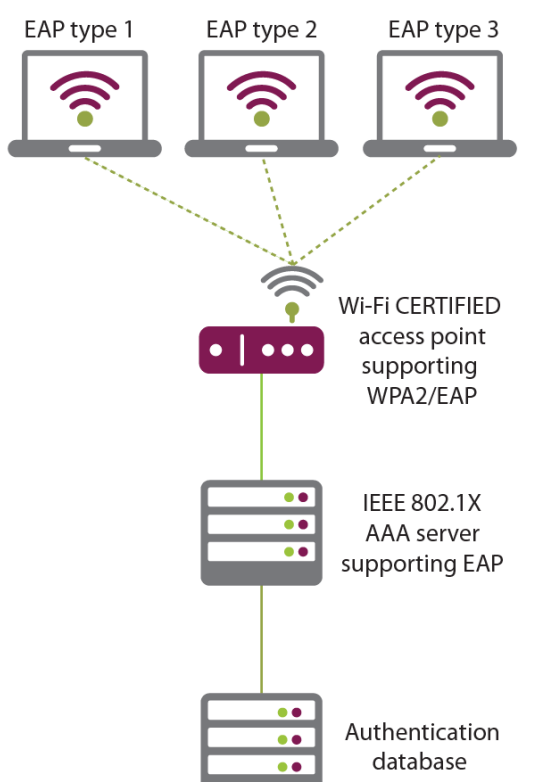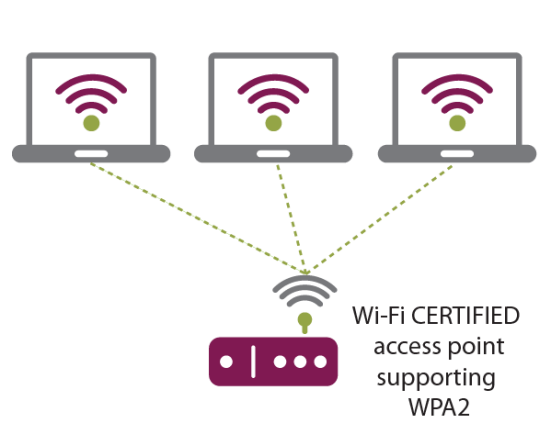[3] Confidential information can use 128-bit AES; classified information requires 192- or 256-bit AES.

WPA2-Enterprise	WPA2-Personal
Each user is assigned unique credentials	Unmanaged mode for authentication using PSK allows use of a manually entered passphrase, which typically is shared by users of that network
IEEE 802.1X AAA server with EAP support and authentication database required	No authentication server required
Data security keys are unique for each session	Data security keys are unique for each session
Wi-Fi CERTIFIED client devices with WPA2-Enterprise	Wi-Fi CERTIFIED client devices with WPA2-Personal

Table 3. WPA2-Enterprise and WPA2-Personal

Authentication with IEEE 802.1X / EAP

WPA2-Enterprise uses the IEEE 802.1X framework with EAP support for authentication (Table 4). Support for multiple EAP types allows the enterprise to select the most appropriate authentication technology for the environment in which it operates. On the network side, support for one or more EAP types has to be enabled within the access point, the IEEE 802.1X AAA server. Both the client device and the network (i.e., access point and servers) need to support the same EAP method to complete the authentication process.

WPA2-Enterprise supports multiple EAP methods that are used worldwide to provide secure authentication in enterprise environments. WPA2 has the flexibility to support new EAP types as

they become available. The Wi-Fi Alliance continues to add support for new EAP types as demand grows in the market to provide users the authentication technology that is best suited for their devices, applications, and networks.

The selection of EAP types to support within a Wi-Fi network depends on the device form factors, on the applications that the network hosts, on the operating system used, and on the specific security requirements of the network owner, including user name and passwords, tokens, certificates and PSKs.

The EAP methods currently supported by the Wi-Fi Alliance certification program are:

- **EAP-TLS**, an Internet Engineering Task Force (IETF) global standard protocol which uses digital certificates for authentication.

- **EAP-TTLS/MSCHAPv2**, which securely tunnels client password authentication within TLS records.

- **PEAPv0/EAP-MSCHAPv2**, which uses password-based authentication.

- **PEAPv1/EAP-GTC**, which uses a changing token value for authentication.

- **EAP-FAST**, which securely tunnels any credential form for authentication (such as a password or a token) using TLS.

- **EAP-SIM,** which is based on the SIM installed in mobile phones and other devices that use Global System for Mobile Communications (GSM) networks.

- **EAP-AKA**, which uses the Universal Mobile Telecommunications System (UMTS) Subscriber Identity Module (USIM) for authentication.

How does WPA2 work?	
WPA2-Enterprise	**WPA2-Personal**
1. The client device associates with the access point and sends its identity to the authentication server 2. The authentication server accepts the client identity and sends its credentials to the client device 3. The client device identifies the server as an authorized one and submits user credentials for validation 4. A Pairwise Master Key (PMK) and Pairwise Transient Keys (PTKs) are generated at the client device and at the authentication server 5. Authentication is completed between the client device and the access point with a four-way handshake 6. AES encryption keys are derived from the PTKs to encrypt data exchanged between client device and access point	1. The client device associates with the access point. Both the client and the access point verify that they are in possession of the same PSK 2. Authentication is completed between the client device and the access point with a four-way handshake 3. In the four-way handshake, the PSK is used to generate the PTK at both the client device and the access point 4. AES encryption keys are derived from the PTKs to encrypt data exchanged between client device and access point

Table 4. WPA2-Enterprise and WPA2-Personal

CCMP Encryption with AES

IEEE 802.11i and WPA2 mandate the use of CCMP, an encryption protocol in which the same key is used for both encryption and integrity protection using AES. AES is a block cipher that operates with multiple key lengths and block sizes. IEEE 802.11i and WPA2 mandate the use of AES with 128-bit keys and 128-bit blocks. The AES encryption keys are derived from the PTK using the four-way handshake defined by the IEEE 802.11i key management protocol.

The inclusion of AES within WPA2 gives Wi-Fi users access to one of the most widely tested and widely used encryption standards. Today, AES is used across multiple data transport technologies and has withstood extensive scrutiny by cryptographers.

Wi-Fi Protected Setup

Wi-Fi Protected Setup was introduced in 2007 as an optional certification program to simplify the configuration and activation of WPA2 in home and small office networks (Figure 1). To date, more than 700 products had been certified for Wi-Fi Protected Setup. While all Wi-Fi CERTIFIED equipment tested since 2006 supports WPA2, WPA2 must be configured and activated in order for the equipment's users to benefit from it. Wi-Fi Protected Setup allows residential and small business users to skip detailed WPA2 configuration steps if desired. Users no longer need to know about PSKs and SSIDs, nor do they have to manually enter PSKs, to secure their networks with WPA2.

Figure 1. The Wi-Fi Protected Setup logo helps users identify equipment that supports it

With Wi-Fi Protected Setup, users have multiple options to set up WPA2:

- **Personal Identification Number (PIN),** with the user entering a numeric code. Mandatory for access points and client devices.

- **Push Button Configuration (PBC)**, with the user pushing a button on both the access point and the enrolling client device. Mandatory for access points, optional for client devices.

- **Near Field Communication (NFC) token**, by using a NFC token, or by putting in contact the access point with the client. Optional.

The Wi-Fi Alliance plans to extend Wi-Fi Protected Setup certification testing in 2010 to include the ad-hoc mode.

Wi-Fi CERTIFIED Makes It Wi-Fi

The Advantages of Choosing Wi-Fi CERTIFIED

Since 2000, Wi-Fi Alliance certification programs have played a proactive, leading role in establishing interoperability among WLAN equipment, enabling a great user experience, expanding Wi-Fi functionality, and improving Wi-Fi performance.

These efforts have been instrumental in widening the adoption of Wi-Fi and in ensuring that Wi-Fi CERTIFIED products have become a globally known and trusted brand. When choosing a new device or access point, users look for the Wi-Fi CERTIFIED logo, because it gives them confidence that the product they buy will work out of the box with Wi-Fi CERTIFIED equipment from any other vendor. Wi-Fi vendors worldwide send their products to be certified in one of the Wi-Fi Alliance Authorized Test Laboratories (ATLs).

To date, more than 6,000 product certifications have been completed, with more than half supporting WPA2. The draft IEEE 802.11n certification program has been very successful, with more than 600 products supporting this next-generation standard. The fastest growth is in mobile phones, with more than 375 Wi-Fi CERTIFIED models.

Wi-Fi certification programs meet the varying requirements of different device form factors, vendor choices, and market demand (

Figure 2. The Wi-Fi CERTIFIED logo can be found on the packaging of Wi-Fi equipment to facilitate the user's selection

Figure 3. The Wi-Fi Interoperability Certificate lists the features that each device or access point supports

Figure 4. The Wi-Fi CERTIFIED product database at www.wi-fi.org

Figure 3). Some Wi-Fi programs are mandatory, because they cover essential Wi-Fi features; others are optional.

Currently active Wi-Fi certification programs

(asterisks indicate optional programs) include:

- Interoperability and standard compliance: **IEEE 802.11a, IEEE 802.11b, IEEE 802.11g**, and **IEEE 802.11n***

- Security: **WPA2-Personal, WPA2-Enterprise* with EAP support, Wi-Fi Protected Setup***

- Voice over Wi-Fi: **Voice Personal***

- Application support through Quality of Service (QoS): **Wi-Fi Multimedia^{TM}*** (**WMM®**)

- Power conservation for mobile devices: **WMM Power Save***

- Wi-Fi and cellular convergence: **Converged Wireless Group Radio Frequency (CWG-RF) Profile*.**

The Current State of Wi-Fi Security

With WPA2, Wi-Fi CERTIFIED equipment offers advanced security tools to enterprise, home, and mobile users worldwide, across a wide and ever expanding range of devices. WPA2 functionality is supported in all new Wi-Fi CERTIFIED devices and access points and it is activated and used on a daily basis by a growing number of Wi-Fi users.

In many enterprises, Wi-Fi is the default access technology. The use of WPA2 is mandated by internal IT policy because it is recognized as a technology that can protect the network and the confidential information transmitted over the Wi-Fi link. As Wi-Fi has become pervasive in more applications and more types of devices, Wi-Fi network security is an integrated component in the overall enterprise security strategy. The adoption of solutions that are used in multiple access technologies, such as IEEE 802.1X or AES, makes it possible to integrate Wi-Fi more deeply within the IT corporate infrastructure. The case study on the University of Texas at Dallas in this paper illustrates how WPA2 secures the WLAN without adding additional complexity to the network and fitting within the existing infrastructure.

In home networks, Wi-Fi Protected Setup helps users set up a network, add devices to an existing network, and activate WPA2. Increasingly, Wi-Fi users realize the paramount importance of security when using any networking technology, and they value the ability to have access to robust data protection without the support of corporate IT staff or spending hours learning about security mechanisms. Enabling WPA2 in a home network typically takes a few minutes, and requires only that the user enter a strong passphrase. WPA2 is becoming a commonly used, essential security measure, like setting up a firewall, using a VPN, or installing antivirus software to protect user data while the user is connected at home or in public hotspots.

The Wi-Fi Alliance continues to promote technological advances in Wi-Fi security and is committed to incorporating future advances into the Wi-Fi CERTIFIED program. The current generation of Wi-Fi technology has reached a comfortable level of maturity that enables it to benefit from the most advanced security technology with WPA2. WPA2 is mandatory in all Wi-Fi CERTIFIED equipment tested since 2006, with more than 3,000 products tested. WPA2 is a pervasive, global standard widely adopted in enterprise and residential networks alike. WPA2 helps protect residential, enterprise, and hotspot networks against hacker threats such as man-in-the-middle attacks, authentication forging, reply, key collision, weak keys, packet forging, and brute-force/dictionary attacks. WPA2 makes robust security available to all Wi-Fi CERTIFIED users, raising the Wi-Fi experience to a high level of reliability, trust, and safety.

UTD

Case study: The University of Texas at Dallas

Securing a campus-wide Wi-Fi network with WPA2

The University of Texas (UT) at Dallas has approximately 15,000 students and 2,500 faculty and staff members spread across 29 buildings on three campuses. UT Dallas has a distinctive heritage and owes its existence to the founders of Texas Instruments, who in the early 1960s identified a lack of scientific and engineering expertise in the region and so established a research center to attract some of the best scientific talent in the nation. This early think tank eventually became a university in 1969 and part of the UT system. Today the university has seven degree-granting schools and more than 125 academic programs. The Wi-Fi network is critical to both the university's research mission and its quality of student life.

A long-time user of WLANs, the university initially deployed a network of proprietary, pre-Wi-Fi access points before upgrading to 802.11b, and then to 802.11a/g. Its most recent upgrade brought in a network of 450 dual-radio access points, with both access points and clients managed by five network controllers. Students treat the network as a utility, using it for Internet access, online tests, and Voice over Internet Protocol (VoIP). Beyond WLAN, the network is multi-homed with one connection to the academic networking consortium Internet2 through North Texas Gigapop, a cooperative association of research institutions, and another commodity connection through the UT System Office of Telecommunications. Average throughput on the wireless network alone is more than 50 Mbps.

Wireless networks have more security requirements than wired Ethernet networks, so UT Dallas needed a system that could offer strong encryption without an additional management burden. "We were looking for a complete and secure network that could be managed by our current staff. We have no dedicated people to manage wireless security, so we needed a system that could reuse as much of the existing wired infrastructure as possible—in particular, authentication," says Bruce Nunn, Software Systems Specialist IV, University of Texas at Dallas.

The Meru system that UT Dallas chose meets the university's targets through its support of WPA2-Enterprise. WPA2 is interoperable with Remote Authentication Dial In User Service (RADIUS) authentication systems, making it easy to link the wireless network to the university's Lightweight Directory Access Protocol (LDAP) database. Users authenticate using IEEE 802.1X and automatically receive a strong AES encryption key. Encryption is completely transparent to the user and the IT department, while authentication uses the same client- and server-side software the wired network uses.

One of the many new applications enabled by the University's wireless network is guest access, which poses specific security issues. Guests are not internal users who can authenticate against a RADIUS database, yet the network still has to be secured. "With WPA2, we were able to provide secure guest access using a separate SSID that redirects users to a captive portal," says Nunn. "Guests do not have to provide IEEE 802.1X credentials, but must accept network usage policies at the captive portal and are only permitted to access the Internet."

Acronyms

3G	Third Generation	MAC	Media Access Control [Layer]
AAA	Authentication, Authorization, Accounting	MSCHAPv2	Microsoft Challenge Handshake Authentication Protocol version 2
AES	Advanced Encryption Standard	NFC	Near Field Communication
ATL	Authorized Test Laboratory	PBC	Push Button Configuration
CCMP	Cipher Block Chaining Message Authentication Code Protocol	PEAP	Protected EAP
		PIN	Personal Identification Number
CWG-RF	Converged Wireless Group Radio Frequency	PMK	Pairwise Master Key
EAP	Extensible Authentication Protocol	PSK	Pre-Shared Key
		PTK	Pairwise Transient Key
EAP-AKA	EAP–Authentication and Key Agreement	RADIUS	Remote Authentication Dial In User Service
EAP-FAST	EAP–Flexible Authentication via Secure Tunneling	RC4	Rivest Cipher 4
		SIM	Subscriber Identity Module
EAP-GTC	EAP–Generic Token Card	SSID	Service Set Identifier
EAP-SIM	EAP–Subscriber Identity Module	TKIP	Temporal Key Integrity Protocol
EAP-TLS	EAP–Transport Layer Security	UMTS	Universal Mobile Telecommunications System
EAP-TTLS	EAP–Tunneled TLS	VoIP	Voice over Internet Protocol
FIPS	Federal Information Processing Standard	VPN	Virtual Private Network
GSM	Global System for Mobile Communications	WLAN	Wireless Local Area Network
IEEE	Institute of Electrical and Electronics Engineers	WMM®	Wi-Fi Multimedia™
IETF	Internet Engineering Task Force	WPA®	Wi-Fi Protected Access®
		WPA2®	Wi-Fi Protected Access 2®
LDAP	Lightweight Directory Access Protocol		

About the Wi-Fi Alliance

The Wi-Fi Alliance is a global non-profit industry association of hundreds of leading companies devoted to the proliferation of Wi-Fi technology across devices and market segments. With technology development, market building, and regulatory programs, the Wi-Fi Alliance has enabled widespread adoption of Wi-Fi worldwide.

The Wi-Fi CERTIFIED™ program was launched in March 2000. It provides a widely-recognized designation of interoperability and quality, and it helps to ensure that Wi-Fi enabled products deliver the best user experience. The Wi-Fi Alliance has completed more than 6,000 product certifications to date, encouraging the expanded use of Wi-Fi products and services in new and established markets.

Further information on Wi-Fi Security and on the Wi-Fi Alliance certification program, including downloadable white papers, is available at www.wi-fi.org

15 of 15