

# Tightening Security in Wireless Networks

Today's wireless networks can be the weakest link within the network infrastructure. However, by combining Dell™ TrueMobile™ wireless networking products with AirFortress® systems from Fortress Technologies, enterprises can help enable military-level security in a plug and play, user-friendly package. This article explains how AirFortress products can be used along with TrueMobile wireless devices to help provide an efficient and secure extension of the enterprise local area network.

BY BELSIS A. MELETIS AND JOHNNY DAHLBERG

Wireless networks are gaining acceptance in enterprises around the world, but these networks are not always secure. Installing firewalls or intrusion detection systems on the local area network (LAN) but keeping the wireless portion of the network insecure can leave flaws in the overall security architecture. For example, hackers using software packages such as NetStumbler or Kismet<sup>1</sup> to employ a process known as war driving can drive or walk by an enterprise's buildings to easily discover unprotected access points. By connecting their laptops to a Global Positioning System (GPS), war drivers can then use NetStumbler to produce a map of the area that displays the exact locations of unprotected access points. Some network administrators have even discovered their entire wireless architecture displayed on maps on the Internet at Web sites used by war drivers to exchange information.

To help protect corporate wireless networks, the IT community—in particular, the Wi-Fi® Alliance, a nonprofit organization devoted to improving wireless technology—

has worked to produce security protocols. Unfortunately, most of these protocols have security weaknesses that adversaries can easily exploit.

## Discovering the insecurity of wireless networks

The security protocol used today by most wireless vendors is the Wired Equivalent Privacy (WEP) protocol. It uses the RC4 algorithm, which encrypts data with either a 64-bit or a 128-bit key. However, the actual key lengths used by the protocol are only 40 bits or 104 bits long, and they are concatenated with a 24-bit Initial Vector (IV) to produce the actual encryption keys, which are 64 bits or 128 bits long. In a busy network, the possible key combinations that can be produced using the 24-bit IV are soon consumed and thus the system starts reusing the same encryption keys. Simply by capturing two data packets that have been encrypted with the same key, an adversary can perform statistical analysis to unearth the WEP key. Examples of programs that exploit these

<sup>1</sup>For more information about NetStumbler, visit <http://www.netstumbler.com>; for more information about Kismet, visit <http://www.kismetwireless.net>.

vulnerabilities include WEPCrack and AirSnort, which are designed to attack the WEP protocol and quickly discover a WEP key. In addition, WEP does not offer secure user authentication or key management. This makes WEP vulnerable to attacks when notebooks or personal digital assistants (PDAs) are stolen and used before administrators can manually change the WEP keys in every wireless terminal and access point.

To enhance the security of wireless networks, Wi-Fi Protected Access (WPA) was designed. The WPA protocol still uses the RC4 algorithm for encryption but provides some enhancements over WEP. These enhancements include 802.1x/Extensible Authentication Protocol (EAP) to provide user authentication; Temporal Key Integrity Protocol (TKIP) to allow automatic encryption key management; and a larger, 48-bit IV to reduce the potential for reusing the same encryption keys. WPA also uses a Message Integrity Check algorithm known as Michael to help protect the integrity of the transmitted data.<sup>2</sup> But WPA is still based on the RC4 encryption algorithm, which is outdated when compared with the advances in today's computing power, and industry experts expect that hackers will soon produce tools that use the distributed computing model to break the RC4 algorithm. In addition, the key renewal process requires significant computing resources, so the WPA protocol is not easily deployed on small devices like PDAs, barcode scanners, and IP phones. In fact, WPA was not intended to be a final protocol but rather a stopgap measure until the 802.11i protocol could be finalized.

### 802.11i: The next wireless security protocol

Because WEP and the RC4 algorithm have become outdated, the wireless community has begun developing the 802.11i protocol.<sup>3</sup> Currently in draft version 7.0, this protocol uses the 802.1x/EAP specification for user authentication along with the 128-bit, 192-bit, and 256-bit Advanced Encryption Standard (AES) and the Michael Message Integrity Check. To provide backward compatibility, 802.11i uses TKIP to interoperate with systems running WPA. Unfortunately, providing backward compatibility with WPA can introduce security flaws into a system because the entire wireless infrastructure will be forced to operate using the RC4 encryption algorithm, which is not considered secure for today's requirements. The 802.11i protocol bases its AES use on special processors installed on the wireless equipment. Users of newer wireless products that support WPA, such as the Dell TrueMobile 1170 Wireless Access Point, can simply update their hardware's firmware, but users of older wireless products that do

not support WPA must replace their wireless hardware. However, the 802.11i protocol has just completed the development stage and has not yet been implemented and tested by wireless vendors—which means it will be some time yet before 802.11i-based devices will be thoroughly available and accepted for use by enterprises.

Meanwhile, the 802.1x/EAP protocol is extensively used in hard-wired network configurations, and numerous 802.1x/EAP implementations have been proposed and used in wireless environments. Examples of such wireless implementations include EAP-Transport Layer Security (EAP-TLS) from Microsoft, which offers strong encryption but needs a fully operational Public Key Infrastructure (PKI) environment to be deployed; EAP-Protected EAP (EAP-PEAP) from Cisco and Microsoft, which can be vulnerable to replay, or *man-in-the-middle*, attacks;<sup>4</sup> and EAP-Message Digest 5 (EAP-MD5), which is a lightweight implementation of EAP that can be used in small mobile devices with low processing capability. EAP-MD5 offers no key management and provides only one-way authentication. Cisco proposed its own implementation of EAP called Lightweight EAP (LEAP), but hackers have developed numerous ways to attack LEAP, including a software package called Asleep. These attacks can be successful because LEAP uses the Microsoft® Challenge Handshake Authentication Protocol (CHAP), which can be vulnerable to dictionary attacks.<sup>5</sup>

### The role of VPNs

To protect their wireless infrastructures, enterprises usually implement virtual private networks (VPNs) on wireless gateways, such as the Dell TrueMobile 2300 Wireless Broadband Router. VPNs are designed to offer strong encryption using AES, and when combined with a Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System Plus (TACACS+) server, VPNs can provide strong user authentication.

Although VPNs are relatively secure, they can introduce several problems for administrators. For example, installing a full VPN architecture just for the wireless portion of the network infrastructure can greatly increase management costs of the overall architecture. In addition, the strong encryption that VPNs are designed to offer can significantly reduce overall wireless throughput. Also, providing the ability to roam in a VPN can be difficult because the Layer 3 connection (the network layer of the ISO/OSI model) that VPNs create can be lost when moving from one access point to another, and thus users need to authenticate again before they can access the network resources. In addition to the management

<sup>2</sup>For more information about the Michael Message Integrity Check algorithm, visit <http://corky.net/2600/wireless-networks/mic-message-integrity-check.shtml>.

<sup>3</sup>For more information about the 802.11i protocol, visit [http://csrc.nist.gov/wireless/S10\\_802.11i%20Overview-jw1.pdf](http://csrc.nist.gov/wireless/S10_802.11i%20Overview-jw1.pdf).

<sup>4</sup>In a man-in-the-middle attack, hackers use packet sniffing to intercept data on a private network. The hackers then modify the data and insert it back into the network. Neither end point on the intercepted link is aware that the hacker can read and change the data traveling on the link.

<sup>5</sup>In a dictionary attack, hackers use common words from a dictionary to determine a user password or an encryption key.

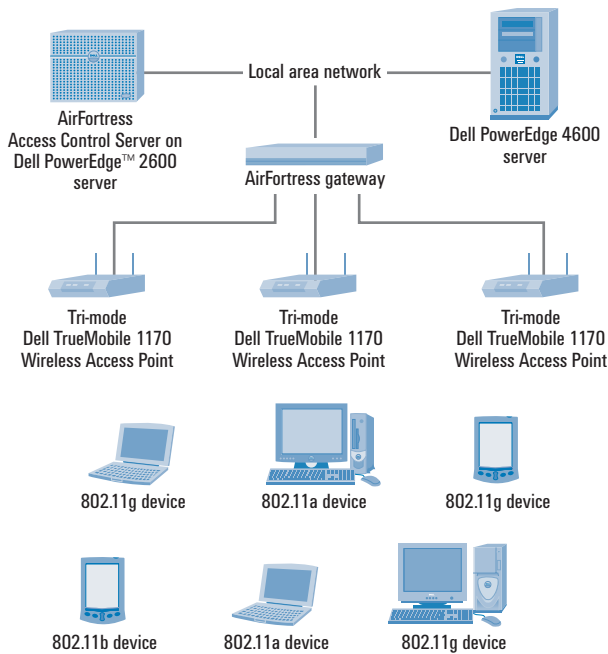


Figure 1. AirFortress security devices within a Dell wireless architecture

issues previously discussed, most wireless VPN deployments operate at Layer 3, which allows hackers to sniff Layer 2–related (data link) information such as packet headers. This information can be used in numerous future attacks. An example of such an attack is the MAC spoofing attack, in which fake Media Access Control (MAC) addresses are used to gain entry into a network.

### Integrating AirFortress security devices into Dell wireless architectures

AirFortress gateways, developed by Fortress Technologies, are designed to offer a plug and play security solution that can be easily integrated with Dell TrueMobile wireless network architectures (see Figure 1). The AirFortress AF2100 and AF7500 gateways have been tested and certified by the U.S. government (Certification No. 231) to comply with Federal Information Processing Standard No. 140 (FIPS-140) and have been extensively deployed and used by U.S. government departments, including the U.S. Army, the U.S. Department of Veteran Affairs, and the U.S. Defense Commissary Agency. An example government project for which AirFortress was selected to provide strong security is the Combat Service Support Automated Information System Interface (CAISI) developed by the U.S. Army.

The AirFortress AF2100 and AF7500 gateways are designed to offer real-time encryption using several known encryption algorithms, such as AES and Triple Data Encryption Standard (3DES), as well as strong authentication. The authentication can comprise up to three steps, depending on the security policy that administrators set:

- **Network authentication:** Users must have the correct access ID for the specific network. This access ID is different from the known Service Set ID (SSID), and it is not transmitted in a clear-text form. The access ID helps prevent unauthorized clients and intruders from performing a key exchange by providing a mechanism to segment communication and control network access.
- **Device authentication:** The system is not based on the classic model of MAC filtering, which is vulnerable to MAC spoofing attacks. Instead, it uses a static Diffie-Hellman public key to authenticate the mobile device—not the wireless card.
- **Username authentication:** The user must provide a username and password before accessing any resources. The gateway alone offers connectivity to the corporate RADIUS server. The AirFortress Access Control Server (ACS) is designed to allow authentication to the Lightweight Directory Access Protocol (LDAP), RADIUS, NT domain, and Microsoft Active Directory® servers.

Because AirFortress gateway devices work on Layer 2 of the ISO/OSI model, they are designed to be integrated with wireless infrastructures such as 900 MHz, 2.4 MHz, 5 MHz, or any hybrid architecture that includes multiple wireless technologies (such as 802.11a/b/g). For example, the Dell TrueMobile 1170 Wireless Access Point is designed to support such a hybrid wireless infrastructure. In addition, the AirFortress gateways are designed to support encrypted traffic over wireless networks implemented under 802.16 broadband protocols. Because the AirFortress driver compresses data, it can enable increased bandwidth and shorter transmit times.

### The components of an AirFortress security architecture

The AirFortress security architecture comprises three major components:

- **AirFortress gateway:** This component enables authentication and separation of wired and wireless LANs.
- **AirFortress client:** This component is a lightweight software application that runs on wireless client devices. Currently, numerous client applications support a broad range of operating systems such as Microsoft Windows® XP, DOS, Windows CE, and Linux® platforms.
- **AirFortress ACS:** This component stores information about user accounts that can access network resources. The ACS can be used to locally store a user database or to allow accessibility of known directory databases like Active Directory and LDAP.

Administrators can manage both the AirFortress gateways and the ACS through simple but secure Web-based interfaces, using

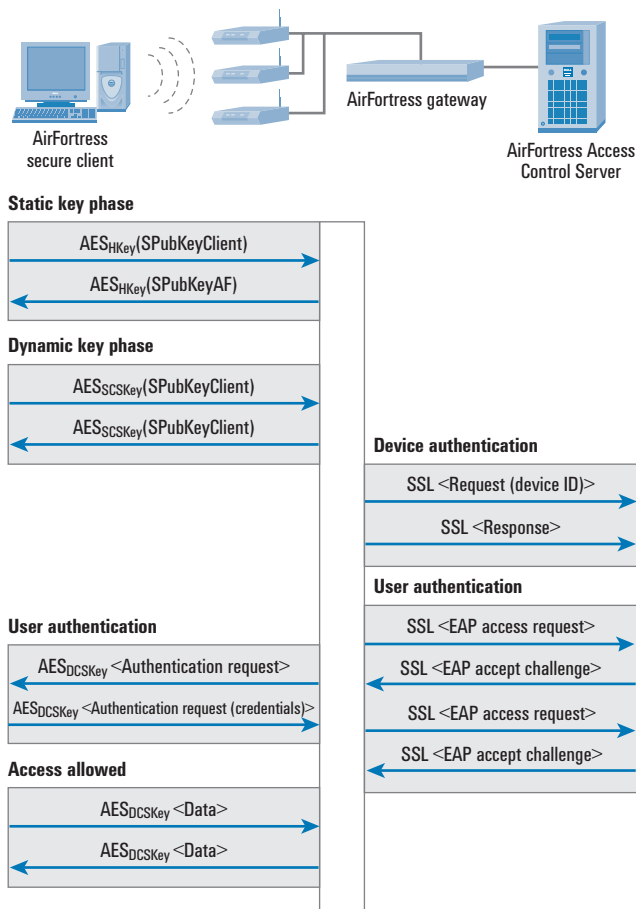


Figure 2. The key negotiation process employed by AirFortress security devices

security provided through Secure Sockets Layer (SSL). In addition, AirFortress gateways are designed to offer both a Secure Shell (SSH) connection and a terminal connection to help perform more advanced and offline management.

To exchange encryption keys, AirFortress devices use only two steps and two transmissions in each direction. Figure 2 depicts the AirFortress key negotiation process.

To protect transmission of keys during the authentication process, AirFortress devices are designed to provide dynamic per-session keys that are generated by a dual Diffie-Hellman exchange, which helps to prevent man-in-the-middle attacks and spoofing. Further, to protect the integrity of the keys, the AirFortress gateways do not transmit the actual session key used to encrypt the data; this key is used only for internal calculations within the end points. These private keys never leave the AirFortress gateway and are newly generated each time the AirFortress device initiates a session. The Diffie-Hellman public key exchange protocol is designed to provide secure distribution of a common secret key between two nodes of a network—that is, secure from passive attacks such

as eavesdropping. However, unlike the generic Diffie-Hellman key agreement method—which can be vulnerable to man-in-the-middle attacks that intercept, modify, or inject messages—the AirFortress devices can perform a secondary Diffie-Hellman key exchange using dynamically generated public keys. To protect the system from Address Resolution Protocol (ARP)–poisoning attacks, the AirFortress device encrypts all ARP-related packets. The Layer 2 encryption renders information unreadable during transport while critical internal addressing information is protected. *Replay protection* guards against data being captured and then re-inserted into the network after it has been compromised.

### Strengthening the security of wireless networks

Wireless networks can be the weakest link in the enterprise IT infrastructure. Combining Dell TrueMobile products with AirFortress devices from Fortress Technologies can help enhance the efficiency and security of today’s business-critical networks by allowing enterprises to take advantage of the capabilities that Wi-Fi technology is designed to offer without sacrificing security. Leveraging the stability and efficiency that Dell wireless products can provide with the security that AirFortress devices are designed to offer can help enable the use of secure wireless technology throughout the enterprise.

**Belsis A. Meletis** is an IT security consultant at Technoplus in Athens and a Fortress engineer. Belsis has a Masters of Philosophy in Information Security, a Masters of Research in Information Technology, and a B.S. in Computer Science from the University of Coventry in the U.K. He is a Certified Wireless Security Professional (CWSP), as certified by Planet3. Belsis is also a research associate of the Biomedical Computing Research Group (BIOCORE) in the U.K.

**Johnny Dahlberg** is an enterprise systems consultant and the head of enterprise at Dell in Athens, Greece. He recommends business solutions by considering customer needs and identifying how Dell can help solve specific market challenges in targeted industries. As head of enterprise, Johnny helps ensure that Dell increases its enterprise market share and helps promote new products as they are developed and introduced to market. Johnny joined Dell in Sweden in 1992.

### FOR MORE INFORMATION

- Dell:**  
<http://www.dell.com>
- Fortress Technologies:**  
<http://www.fortresstech.com>
- NetStumbler:**  
<http://www.netstumbler.com>
- Kismet:**  
<http://www.kismetwireless.net>