White Paper

Wireless LAN Security

1 Introduction

As wireless LANs become widely deployed, and the business benefits become clear, concern has grown over their security. This white paper details these concerns and discusses advanced technologies that resolve the issues to produce robust security solutions. The key topics of encryption and authentication are defined in some depth. Recommendations are made on deploying enterprise class wireless LANs that are standards-compliant, scalable, manageable and extensible to encompass new technologies as they emerge.

2 Why is security so important?

Why is there so much apprehension over security of wireless LAN technology? It all stems from the open nature of the wireless media. To connect to a wired LAN you need physical access, you have to connect a PC into a live network port. With wireless you only need to be in the coverage area of an aerial (i.e. within range of an Access Point). Control for wired networks is simpler: traditional physical access control into buildings can be used and unused network ports can be disabled by management application. Wireless LANs use radio waves which pass through many modern building materials and thus coverage is not limited to the inside of a building. The radio waves appear in the street where transmissions from Wireless LANs can be monitored by an eavesdropper with suitable equipment. Access to a corporate network can be achieved from outside a building using readily available technology. Figure 1 shows how an eavesdropper can gain access to a wireless LAN from outside of an office building.

The solution is to implement a robust security network. For example use encryption to prevent an eavesdropper from understanding any intercepted transmissions and use strong authentication schemes to prevent unauthorised network access.

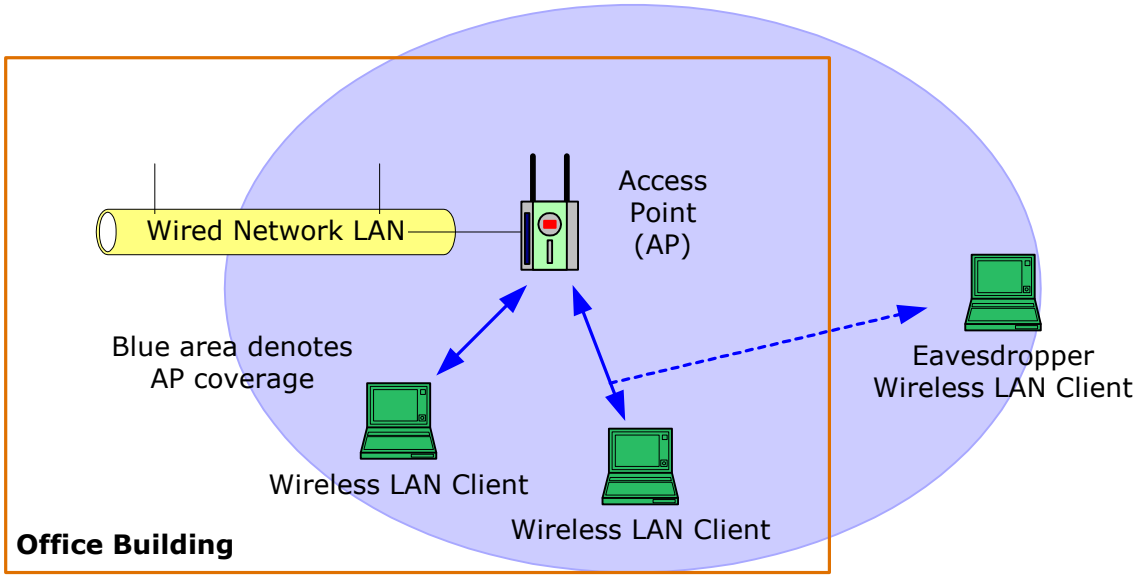

Figure 1: Eavesdropping example

3 Weaknesses in 802.11 security

The IEEE 802.11 standard defines Wired Equivalent Privacy (WEP) to protect wireless transmissions. WEP employs the RC4 symmetric stream cipher using an encryption key that is shared by all participants in the wireless network. 802.11 defines 64-bit WEP keys but most suppliers also support 128-bit keys. 802.11 does not define how keys are distributed. A WEP key consists of two parts: a 24-bit Initialisation Vector (IV) and a secret key. The IV is transmitted in plain text in the headers of 802.11 packets and can therefore be easily intercepted. Armed with the IV there are well-documented techniques available to "crack" WEP encrypted transmissions given sufficient sample data. The solution is to use dynamic WEP keys that change frequently.

The 802.11 standard defines very basic wireless client authentication that also uses the WEP key. The industry has adopted the 802.1x authentication framework (see section 7 entitled "*Wireless Authentication*") to overcome the deficiencies of the 802.11 standard. Recently the University of Maryland has documented potential security risks with the 802.1x protocol. Today's solution is to use mutual authentication to prevent "man in the middle" attacks and dynamic WEP keys that are distributed over secure, encrypted channels. Both these techniques are supported by the Transport Layer Security (TLS) protocol. Further enhancements include per-packet keying and message integrity checks – these are proposed enhancements to the 802.11i security standard.

4 Madge Wireless LAN architecture

The Madge wireless LAN architecture consists of three components: *Wireless Clients*, which communicate with *Access Points*, which in turn can communicate with and can be controlled by *Access Servers*. Wireless clients are typically laptop computers with a wireless Network Interface Card (NIC) installed to allow access to the wireless network. An Access Point (AP) provides radio coverage to a particular area (known as a cell) and connects to the wired network. Both 802.11b (11Mbps LANs at 2.4 GHz) and Bluetooth APs are supported. An Access Server (i.e. the Enterprise Access Server or EAS) provides control, management and advanced security features to the Enterprise wireless network.

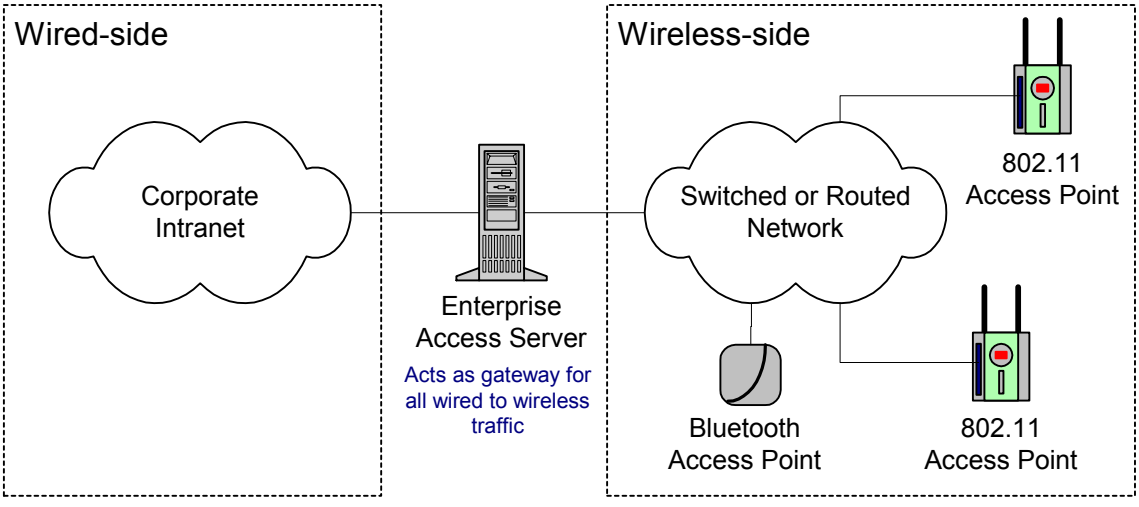

Figure 2: Enterprise Access Server in Gateway Mode

A Madge wireless infrastructure can be connected to existing wired networks in a number of ways. Common architectures include deploying the EAS in "*Gateway Mode*" or "*Controller Mode*". In Gateway Mode (see figure 2 above) the EAS is placed between the AP network and the rest of the enterprise network. The EAS therefore controls all traffic flow between the wired and wireless networks and acts as a firewall.

In Controller Mode (see figure 3) the EAS manages the APs and controls access to the wireless network but is not involved in the transfer of user data. In this mode the wireless network can be separated from the wired network with an additional firewall or fully integrated into the enterprise wired network.

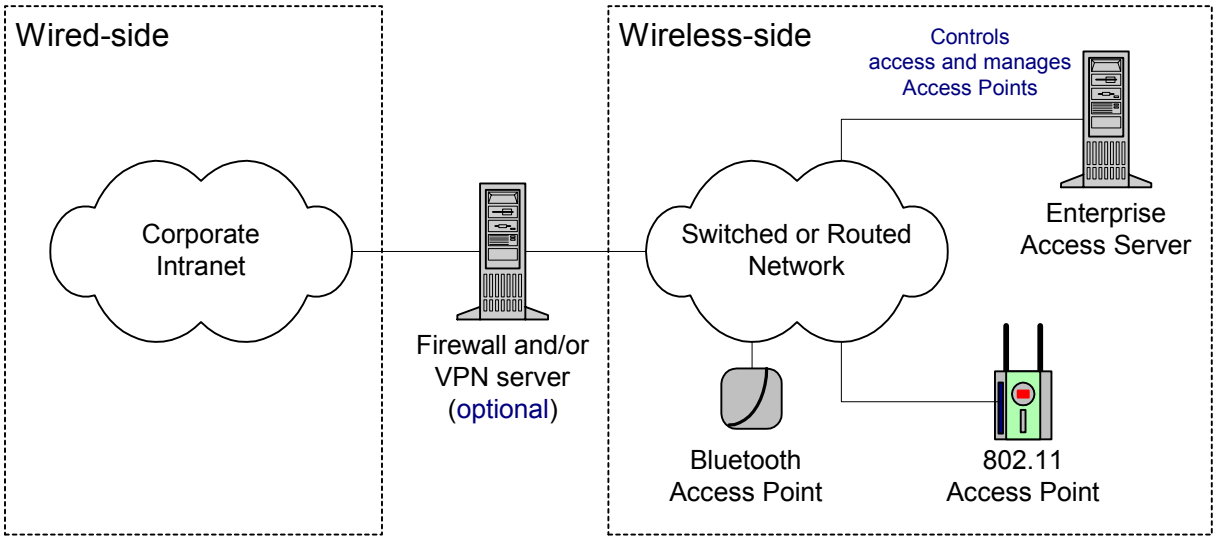

Figure 3: Enterprise Access Server in Controller Mode

5 Madge Wireless Security Model

The Madge wireless LAN architecture supports a comprehensive and extensible security model based on industry-standards as shown in figure 4. Each element within the model is configurable allowing network administrators to balance usability and security appropriate to their needs.

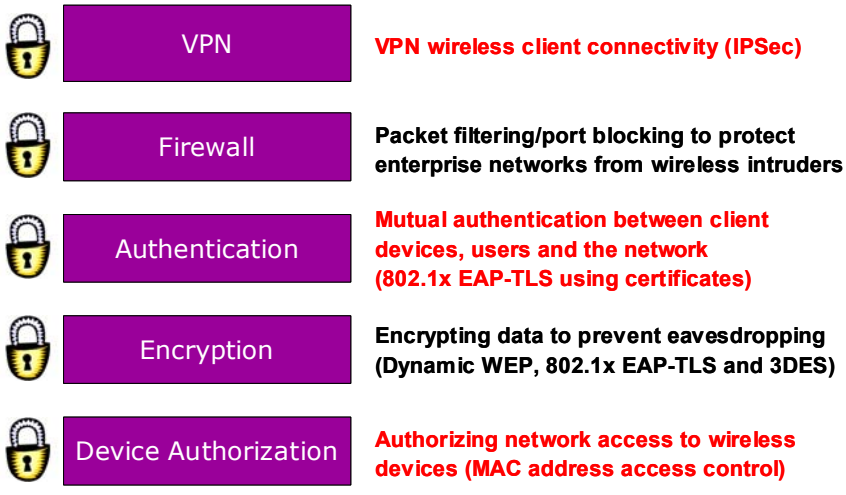

Figure 4: Wireless security model

Device Authorisation: wireless clients can be excluded from the network according to their hardware address (e.g. MAC address). The EAS maintains a database of authorised wireless clients and individual APs either pass or block traffic accordingly.

Encryption: the Madge WLAN family of products support the WEP, 3DES and TLS standards that use encryption to prevent eavesdropping. WEP keys can be generated on a per-user, per session basis.

Authentication: the Madge WLAN family of products support mutual authentication (using 802.1x EAP-TLS) to ensure only authorised wireless clients are permitted to access the wireless network. The EAS uses an internal RADIUS server for authentication using digital certificates. Digital certificates can be obtained from the internal Certificate Authority (CA) or imported from an external CA. This maximises security and minimises administrative overhead.

Firewall: the EAS incorporates a customisable packet filtering and port blocking firewall based on Linux IPchains. Built-in preset configurations allow common traffic types to be enabled or disabled.

VPN: the EAS contains an IPSec VPN server that allows wireless clients to establish secure VPN sessions over the wireless network to the EAS.

6 Encryption

Encryption is about transforming data so that only authorised parties can decode it. The encryption process combines some plaintext with a key to produce Ciphertext. Decryption reverses the process by taking the Ciphertext and combining it with a key to reproduce the original plaintext as shown in figure 5. The process of defining and distributing the keys is known as key management.

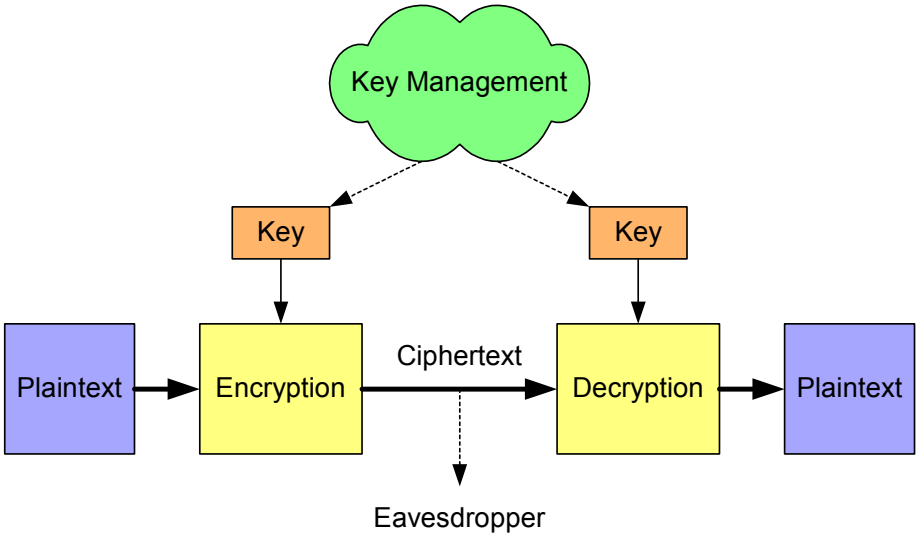

Figure 5: Encryption

If the same key is used for both encryption and decryption then the keys are known as "symmetric". If different keys are used then they are known as "asymmetric". Asymmetric keys are typically used in Public Key Infrastructures (PKIs) where one key is "public" and the other is "private".

There are two main encryption methods: block ciphers and stream ciphers. Block ciphers operate on plaintext in groups of bits, called blocks that are typically 64 or 128 bits long. Examples of block ciphers are: DES, triple DES (3DES), AES and Blowfish. Stream ciphers convert a key into a random "keystream" (a stream of small keys of typically 8 bits each) that is then combined with the plaintext to encode it. Stream ciphers are generally much more efficient than block ciphers. Examples of stream ciphers are: RC4 (used in 802.11 wireless LANs), SEAL and SOBER.

7 Wireless Authentication

Authentication is about proving or disproving someone's or something's claimed identity. Traditionally authentication is a one-way process, e.g. a user logs onto a computer and proves their identity with a username and password. In wireless networking mutual authentication should be employed where the network authenticates the client *and* the client authenticates the network. This prevents rogue devices from masquerading as network equipment to gain access to sensitive data on the wireless client (e.g. usernames and passwords).

The original 802.11 wireless LAN standards did not include comprehensive authentication, so the industry has adopted the 802.1x protocol for its authentication framework. 802.1x defines port-based network access control that uses the Extensible Authentication Protocol (EAP) and a RADIUS server. 802.1x doesn't define the actual authentication protocol but specifies EAP that in turn supports a number of authentication protocols such as CHAP-MD5, Transport Layer Security (TLS) and Kerberos. EAP is extensible so that new authentication protocols can be supported as they are developed. EAP was originally specified to operate over the Point-to-Point Protocol (PPP); in order to make it compatible with other data link layer protocols (such as 802.5 Token Ring or 802.11 Wireless LANs) EAP Over LANs (EAPOL) was developed. The resulting Authentication model is shown in figure 6.

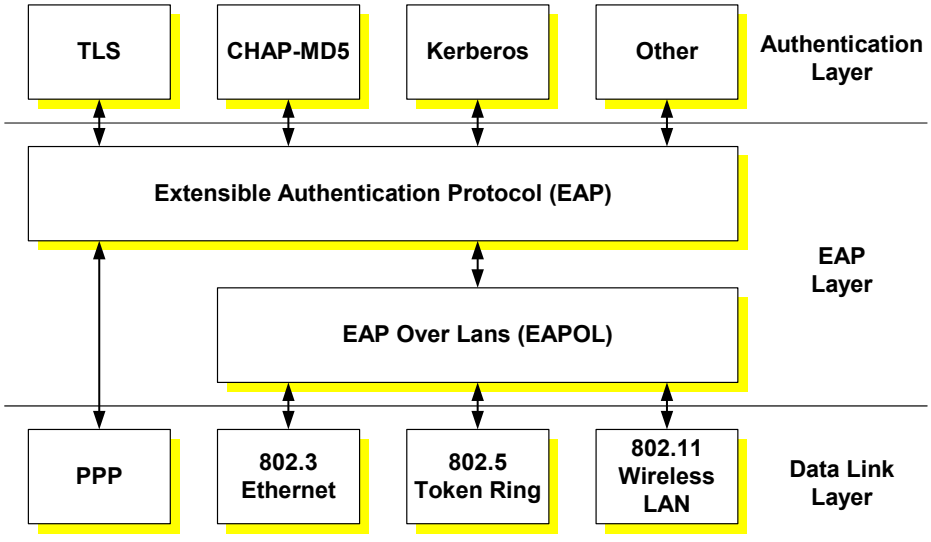

Figure 6: Authentication model

802.1x EAP-TLS is used in certificate-based environments and is highly secure. The EAP-TLS exchange of messages provides mutual authentication, negotiation of the encryption method and secured key exchange between a wireless client and the network. EAP-TLS is the mechanism that provides per-user, per-session dynamic encryption keys. This significantly improves security and overcomes many of the weaknesses in wireless networks.

Figure 7 shows the sequence of events that occur when a wireless client is authenticated using 802.1x EAP-TLS. Two digital certificates are required: one on the RADIUS server (e.g. the EAS) and one on the wireless client. Note that network access is denied until authentication has succeeded and dynamic WEP keys have been established.

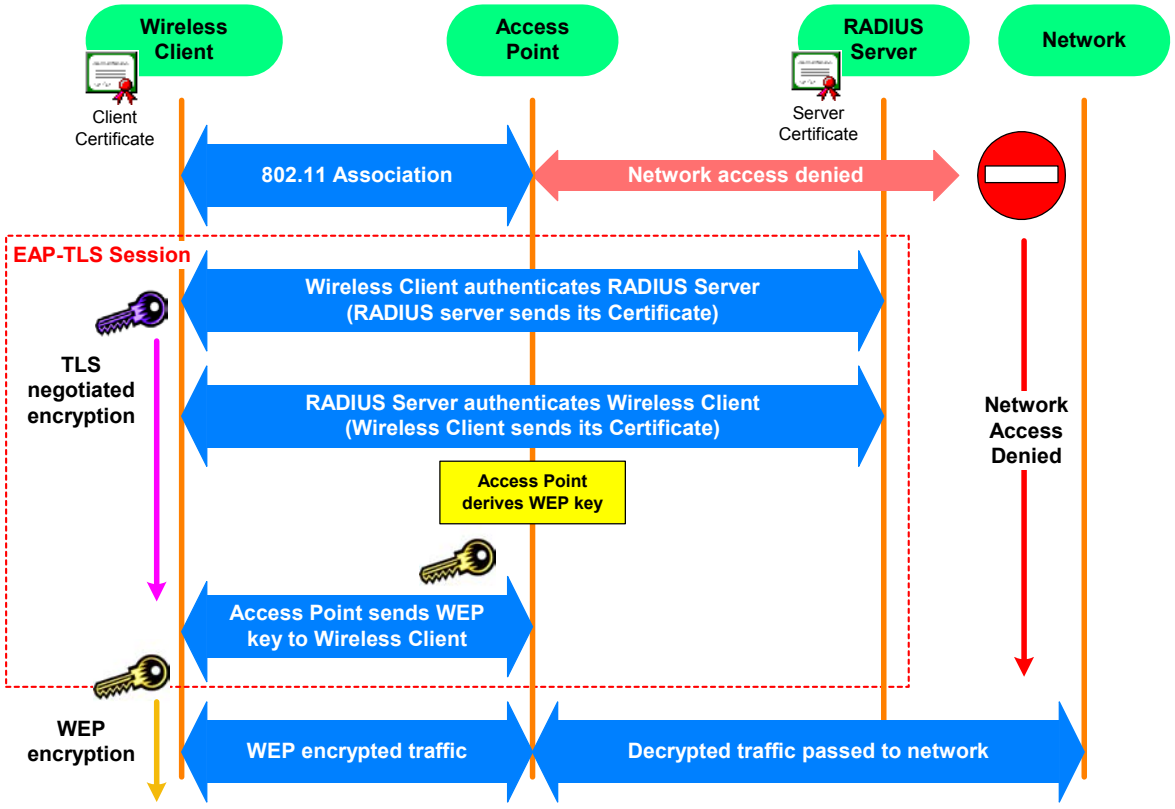

Figure 7: 802.1x EAP-TLS authentication

802.1x EAP-TLS operation with the EAS in Controller Mode is shown in figure 8. The wireless client has its digital certificate pre-installed, as does the EAS. The wireless client communicates with the EAS via the AP. All three components (wireless client, AP and EAS) support the 802.1x EAP-TLS process. The wireless client can use Windows XP (which has built-in support for 802.1x EAP-TLS) or Windows 98/Me/2000 by using the Madge Wireless LAN Utility (WLU). Once authenticated the user's data is routed directly to the corporate intranet without passing through the SWAS. 802.1x EAP-TLS can also be used with the EAS configured in Gateway Mode.

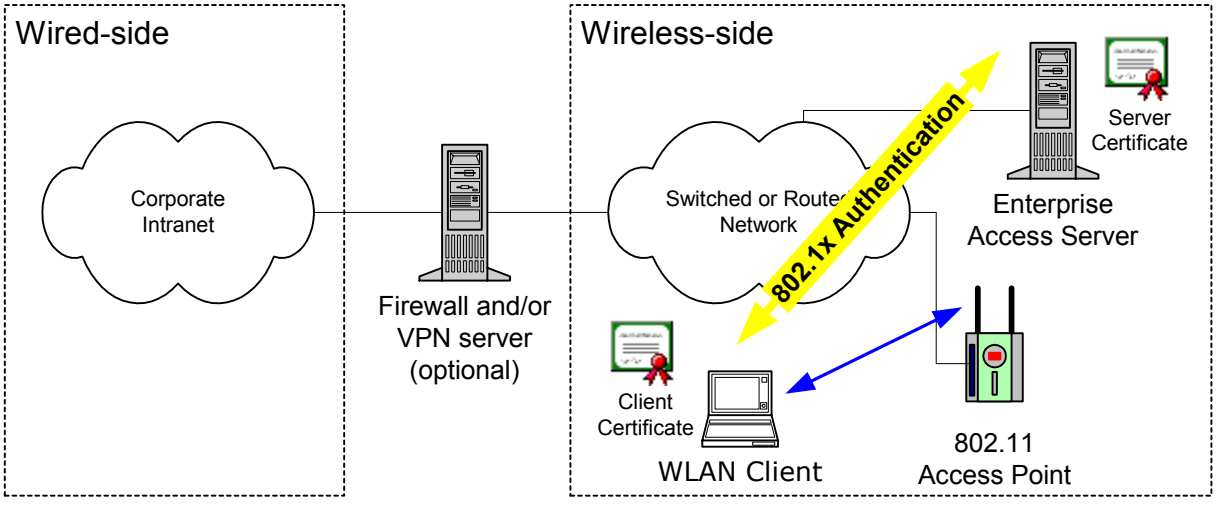

Figure 8: 802.1x EAP-TLS operation in Controller Mode

8 New Technologies and Future directions

The IEEE 802.11i Task Group is working on enhancements to both encryption and authentication in wireless LANs. 802.1x will be incorporated into the 802.11i specifications. Enhancements to WEP include the Temporal Key Integrity Protocol (TKIP). TKIP provides three security improvements: fast-packet keying (key-hashing per packet), real message integrity checking (to prevent forgery) and dynamic key management (re-keying). The Advanced Encryption Standard (AES) is also in the draft 801.11i specifications. AES is a symmetric block cipher operating on blocks of 128 bits using three possible key sizes: 128, 192 and 256 bits. There is an "advanced subset" of 802.11i, known as WiFi Protected Access (WPA), which is compatible with existing hardware; it includes both 802.1x and TKIP.

The Internet Engineering Task Force (IETF) has produced an Internet-Draft document defining a new authentication protocol based on EAP called Protected EAP (PEAP). It works by wrapping the EAP protocol within TLS thus protecting the EAP message exchanges. Any EAP authentication method running within PEAP is provided with protected key exchange and session resumption (which allows fast re-authentication when a wireless client roams from one AP to another).

Madge is committed to tracking emerging standards and extending its product family to support these when appropriate. With its extensible, field-upgradeable, software architecture Madge can incorporate new security technologies as they develop.

9 Recommendations

Madge recommends deploying robust wireless LAN security solutions:

- Deploy an extensible networking and security architecture that can evolve as new standards-based wireless LAN technologies emerge (e.g. PEAP and 802.11i).
- Implement a robust security network that incorporates 802.1x EAP-TLS using digital certificates and dynamic per-user, per-session WEP keys.
- Where 802.1x EAP-TLS isn't practical consider using IPSec VPNs to secure wireless traffic. When deploying VPNs ensure that the network design accommodates the increased performance requirements of the encryption technology (e.g. 3DES).
- Centralise security management by using enhanced security products such as the Madge Enterprise Access Server (EAS).
- Separate a wireless network from a wired network by deploying firewalls.
- Always use WEP encryption, never implement an "open system". Use 128-bit WEP keys for maximum security.
- Change WEP keys frequently when not using dynamic keys. Deploy security management products that simplify this process.
- Use device authorisation (e.g. MAC access control) to exclude unwanted wireless clients.
- Change default passwords, network names (e.g. SSIDs) and SNMP community strings that are pre-configured in the factory.
- Change passwords regularly. Use "difficult to crack" passwords that are not susceptible to "dictionary attacks". Enable "BIOS" passwords and screen saver passwords to prevent unauthorised people accessing wireless LAN configuration parameters such as static WEP keys (if used).