

SECURE WIRELESS LAN DEPLOYMENT

N.Sharmili¹, J.P.Praveen², CH. Yamini Sankar²

¹Associate Professor, ² M.Tech., (4th Semester)

GVP College of Engineering, Visakhapatnam, India

logintosharmi@gmail.com, jppraveen81@gmail.com, chysankar@rediffmail.com

ABSTRACT

Over the past few years, the world has become increasingly mobile, the most ubiquitous example of this being the widespread use of cell phones. This trend is being reflected in businesses too with the traditional ways of networking have proven inadequate to meet the challenges posed by the growing demands on efficiency and productivity. Many organizations have therefore started to complement their traditional wired networks with Wireless LANs.

Wireless LANs, with their low cost, combined with strong performance and ease of deployment holds the key to maximizing productivity and minimizing cost for business organizations. However, it is still pestered with security concerns, which makes businesses wary of its widespread usage. This paper is about model a configuration and deployment strategy of a wireless LAN that is both cost effective and secure to be implemented.

Keywords: Authentication, Encryption, Networks, Protocol, Security, Wireless

1 INTRODUCTION

With the advent of the Internet the face of how businesses processing is carried out changed. We are on the cusp of an equally profound change in computer networking.

The benefits of WLAN technology fall into two main categories: core business benefits and operational benefits. The core business benefits of WLANs arise from the increase in flexibility and mobility of your workforce. They include improved employee productivity, quicker and more efficient business processes, and greater potential for creating entirely new business functions. Operational benefits include lower costs of management and lower capital expenditure.

Wireless Networks, like any other network are composed of different components, each contributing an essential service to the overall working. But it remains that there are a number of ways that a wireless LAN can be implemented.

There is no right or wrong choice but is a product of the level of security, strength, capability and scalability desired by the target organization.

Following were the parameters that were kept in mind which contributed to formulation of the implementation:

1. Security

- a. Robust authentication and authorization of wireless clients
 - b. Robust access control to permit network access to authorized clients and to deny it to unauthorized clients
 - c. High strength encryption of wireless network traffic
 - d. Secure management of encryption keys
 - e. Resilience to DoS attacks
2. *Business Value*
 - a. The design should be cost effective, with reuse of existing infrastructure where ever possible.
 3. *Scalability*
 - a. Basic design that can scales upward and downward.

Based on these key parameters, after analyzing various wireless standards and different deployment strategies that mitigate WLANs security vulnerabilities, a design based on **IEEE 802.1X** and Extensible Authentication Protocol-Transport Layer Security (**EAP-TLS**) over Internet Authentication Service (**IAS**) which is Microsoft's Remote Authentication Dial-In Sever (**RADIUS**) implementation along with Microsoft's **Active Directory** support and a Public Key Infrastructure (**PKI**) provided by Microsoft's **Certificate Services** has been selected as the authentication method. For data encryption, **dynamic** Wired Equivalent

Protection (WEP) via Temporal Key Integrity Protocol (TKIP) has been selected.

In addition to these, following are the further specifications of the WLAN:

A. IEEE 802.11 Standard

MAC	CSMA/CA			
PHY	802.11 2 Mbps	802.11b 11 Mbps	802.11a 54 Mbps	802.11g 54 Mbps

Fig. 1. IEEE 802.11 Standards

IEEE 802.11 is an industry standard for a shared, wireless LAN that defines the physical (PHY) layer and Media Access Control (MAC) sub-layer for wireless communications. At the MAC sub-layer, all the IEEE 802.11 standards use the carrier sense multiple access with collision avoidance (CSMA/CA) MAC protocol. At the physical (PHY) layer, IEEE 802.11 defines a series of encoding and transmission schemes for wireless communications.

Weighing all the pros and cons the 802.11g has been selected as the preferred standard. It supports bandwidth up to 54 Mbps, and it uses the 2.4 GHz frequency for greater range. Apart from being faster than 802.11b and at times 802.11a, it is backward compatible with the 802.11b standard. It also supports more simultaneous users and is not easily obstructed.

B. Operating Mode

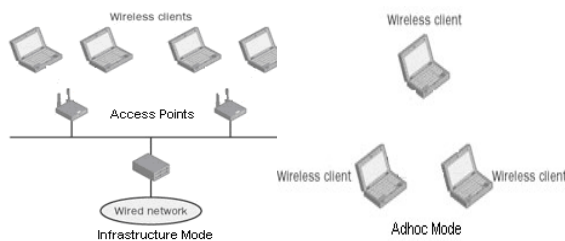


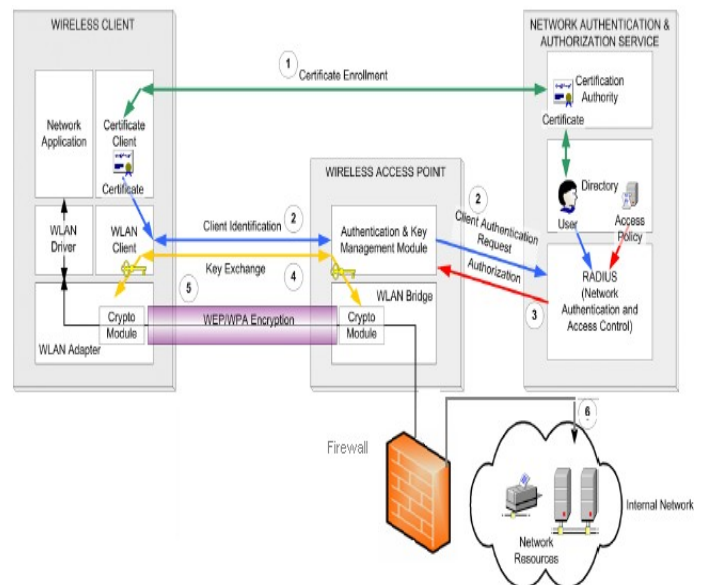
Fig. 2. Operating Mode

In *ad hoc mode*, wireless clients communicate directly with each other without the use of a wireless Access Point. This makes it harder to authenticate clients joining in the network and monitor their activities. Hence, infrastructure mode has been selected in which there is at least one wireless Access Point and one wireless client. The wireless client uses the wireless AP to access the resources of a traditional wired network.

2 CONCEPTUAL DESIGN

- **Wireless Client** – this is a computer or laptop or any other device with a wireless network interface card. It has the capability of securely exchanging credentials like certificates, passwords etc and also of encrypting its network traffic.
- **Wireless AP** – it is a Layer 2 device that contains 802.11 PHY and RF radio connectivity and provides access control functions to allow or deny access to the wired network and provides the capability of encrypting wireless traffic. It secures network traffic by having the ability to securely exchange encryption keys with the wireless client. Finally, it can query an authentication and authorization service for authorization decisions.
- **Network Authentication and Authorization Service (NAAS)** – this is the storehouse of the valid clients credential based on whose verification it makes authentication and authorization decisions.
- **Internal Network** – this is a secure and trusted area of networked services. Typically, the wireless client runs applications which need to gain access to these services. The two networks are separated by a firewall as the wireless network is not trusted.

Fig. 3. Conceptual Design



The above diagram depicts four main components:

The basic network access process is described in the following steps as numbered in the above diagram: [5]

1. The wireless client must at some point establish credentials with a central authority before wireless network access is established. This is done

by the client by connecting to the wired network and gaining a certificate from the *Enterprise Certification Authority* by means of *auto-enrollment*.

2. When the client requires wireless access it passes its certificate to the wireless AP which in turn passes it to the NAAS, in our case the RADIUS server to check authentication.

3. The RADIUS server based on the validation of the certificate and its access policy either grants or denies the authorization request.

4. If the client gets authorized, access is allowed, and the client securely exchanges encryption keys with the wireless AP. These keys are generated by the RADIUS server and transmitted to the wireless AP over a secure channel. No further communication takes place if access is denied.

5. Using the encryption keys, the client and wireless AP establish a secured connection over the wireless link, and connectivity is established between the client and the internal network.

6. The client begins communicating with devices on the internal network.

- No key distribution method defined. Hence the shared key is not changed over long periods of time.
- Because of the short length of the IV vector, after a while the encryption key starts getting repeated.
- Data Integrity not maintained due to the linearity of the CRC algorithm.

WEP uses the RC4 encryption algorithm, a stream cipher. Both the sender and receiver use the stream cipher to create identical pseudorandom strings from a known shared key. The process entails the sender to logically XOR the plaintext transmission with the stream cipher to produce the cipher text. The receiver takes the shared key and identical stream and reverses the process to gain the plaintext transmission.

Following are the attacks to which static WEP is susceptible to:

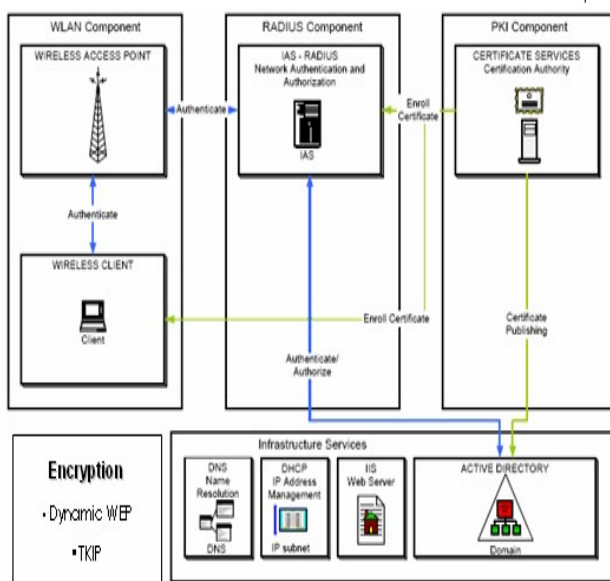
- Passive attacks to decrypt traffic based on statistical analysis.
- Active attack to inject new traffic from unauthorized mobile stations, based on known plaintext.
- Active attacks to decrypt traffic, based on tricking the access point.
- Dictionary-building attack that, after analysis of about a day's worth of traffic, allows real-time automated decryption of all traffic.

• Dynamic WEP & TKIP

Dynamic Wired Equivalent Privacy allows for the creation of keying material that, unlike static WEP, changes automatically on a periodic basis without the need for the network administrator to visit each wireless device. Dynamic WEP can be established on a per-user, per frame basis adding a great deal of variation into the encryption frame circumventing the previously stated attacks.

TKIP (Temporal Key Integrity Protocol) is a suite of algorithms that works as a "wrapper" to WEP, which allows users of legacy WLAN equipment to upgrade to TKIP without replacing hardware. TKIP uses RC4 to perform the encryption, which is the same as WEP. A major difference from WEP, however, is that TKIP changes temporal keys every 10,000 packets. The TKIP process begins with a 128-bit "temporal key" shared among clients and access points. TKIP combines the temporal key with the client's MAC address and then adds a relatively large 16-octet initialization vector to produce the key that will encrypt the data. This procedure ensures that each station uses different key streams to encrypt the data. [6]

Some of the essential characteristics of the TKIP algorithm are highlighted in the following list: [3]



3 LOGICAL DESIGN

Fig. 4. Logical Design

1 Encryption

• WEP

Wired Equivalent Privacy is a security protocol for wireless local area networks. WEP is designed to provide the same level of security as that of a wired LAN. But it fails to do so, both because of the inherent vulnerability of the medium and due to fundamental design flaws in the protocol itself which are: [1]

- Per-user, per-frame keying – key mixing is used to create a strong WEP seed which is used to generate cipher text with the RC4 algorithm.
- Per-frame sequence counter – sequences each frame to help mitigate replay attacks against the WLAN.
- Larger Initialization Vector – the larger 48-bit IV (281 trillion possible IVs), coupled with a limited temporal key lifetime makes it virtually impossible to exhaust the IV space.
- Michael Integrity Check (MIC) – a more robust integrity checking process that identifies unauthorized changes to the WLAN frames and is supported by additional countermeasures.

Authentication

- **IEEE 802.1X Standard & EAP**

The IEEE 802.1X standard defines port-based, network access control used to provide authenticated network access for Ethernet networks. This port-based network access control uses the physical characteristics of the switched LAN infrastructure to authenticate devices attached to a LAN port. Access to the port can be denied if the authentication process fails. Although this standard was designed for wired Ethernet networks, it has been adapted for use on 802.11 wireless LANs.

Because multiple wireless clients contend for access to the same channel and send data using the same channel, an extension to the basic IEEE 802.1X protocol is required to allow a wireless AP to identify the secured traffic of a particular wireless client. The wireless client and wireless AP do this through the mutual determination of a per-client unicast session key. Only authenticated wireless clients have knowledge of their per-client unicast session key. Without a valid unicast session key tied to a successful authentication, a wireless AP discards the traffic sent from the wireless client.

To provide a standard authentication mechanism for IEEE 802.1X, the Extensible Authentication Protocol (EAP) was chosen. EAP is a Point-to-Point Protocol (PPP)- based authentication mechanism that was adapted for use on point-to-point LAN segments. EAP messages are normally sent as the payload of PPP frames. To adapt EAP messages to be sent over Ethernet or wireless LAN segments, the IEEE 802.1X standard defines EAP over LAN (EAPOL), a standard encapsulation method for EAP messages

With EAP, the specific authentication mechanism is not chosen during the link establishment phase of the PPP connection; instead, each PPP peer negotiates to perform EAP during the connection authentication phase. When the connection authentication phase is reached, the peers negotiate

the use of a specific EAP authentication scheme known as an *EAP type*.

- **EAP – TLS**

Extended Authentication Protocol - Transport Layer Security (EAP-TLS) is an EAP type that is used in certificate- based security environments and provides the strongest authentication method. The EAP-TLS exchange of messages provides mutual authentication, integrity-protected cipher suite negotiation, and encryption key determination.

EAP-TLS uses both user and computer certificates. Its advantages are the following:

- EAP-TLS does not require any dependencies on the user account's password.
- EAP-TLS authentication occurs automatically, usually with no intervention by the user.
- EAP-TLS uses certificates, which provide a relatively strong authentication scheme.
- EAP-TLS exchange is protected with public key cryptography and is not susceptible to offline dictionary attacks.
- EAP-TLS authentication results in mutually determined keying material for data encryption and signing.

- **PKI & CA**

A public key infrastructure (PKI) is a system of digital certificates and CA (Certification Authority) - an entity that users of the certificate can trust that verifies and authenticates the validity of each entity that is participating in secure communications through the use of public key cryptography^[9].

Public-key cryptography introduced the concept of having keys work in pairs, an encryption key (public key) and a decryption key (private key), and having them created in such a way that generating one key from the other is infeasible. The encryption key is then made public to anyone wishing to encrypt a message to the holder of the secret decryption key. Because identifying or creating the decryption key from the encryption key is infeasible, anyone who happens to have the encrypted message and the encryption key will be unable to decrypt the message or determine the decryption key needed to decrypt the message.

To secure the integrity of the public key, the public key is published as part of a certificate. A *certificate*, also known as a *digital certificate* or *public key certificate*, is a data structure that contains a digital signature of a certification authority (CA). A certificate is a digitally signed statement that binds the value of a public key to the identity of the person, device, or service that holds the corresponding private key.

- **RADIUS**

Remote Authentication Dial in User Service (RADIUS) is a widely deployed protocol enabling centralized authentication, authorization, and accounting for network access. IAS in Windows 2000 Server is the Microsoft implementation of a RADIUS server.

The RADIUS servers are used to manage credentials, provide profiles for what different roles can perform and track resources. [6] There are three components to it:

- Authentication – allows an entity to provide credentials and assert its identity.
- Authorization – delineates what functions the entity is permitted to perform.
- Accounting – provides a way of logging and recording usage information.

When accessing the network, the user enters authentication information and passed by the Access Point to a RADIUS server, which verifies the information is correct and present in its database. It may use an internal database of users or may optionally point to an external database such as Microsoft Windows Active Directory as is in our case.

To provide security for RADIUS messages, the RADIUS client and the RADIUS server are configured with a common shared secret. The shared secret is used to authenticate RADIUS messages (by using the Authenticator field in the RADIUS header of RADIUS response messages) and to encrypt sensitive RADIUS attributes. The shared secret is commonly configured as a text string on both the RADIUS client and server.

Using RADIUS servers provides the following advantages:

- 3 Authentication is not based on hardware, which reduces costs and administration overhead when upgrades occur or authentication data is changed.
- 4 Stolen wireless hardware such as 802.11 cards does not necessarily mean that security will be compromised because user authorization is required.
- 5 Both RADIUS and Active Directory are already in use in the TCS organization, making adoption for the wireless segment easier.
- 6 Accounting and auditing are available, allowing enterprises to audit usage and create alarms for intrusion.

4 IMPLEMENTATION

Based on the above conceptual design and logical design and along with the hardware and infrastructure constraints the following configuration

was implemented.

The infrastructure for the wireless test lab network consists of four computers, two switches, one wireless access point and one wireless client performing the following roles:

- A computer running Microsoft Windows Server 2003 with Service Pack (SP1), Enterprise Edition, named DC that is acting as a domain controller, Domain Name System (DNS) server and a Certification Authority (CA).
- A computer running Microsoft Windows Server 2003 with SP1, Standard Edition, named IAS that is acting as a Remote Authentication Dial-In User Service (RADIUS) server.
- A computer running Windows Server 2003 with SP1, Standard Edition, named IIS1 that is acting as a web and file server.
- A computer running LINUX Fedora named as FIRWAL that is acting as a packet filter and a Dynamic Host Configuration Protocol (DHCP) server.
- A DELL laptop running Windows XP Professional with SP2 named CLIENT that is acting as a wireless client.
- A Cisco Aironet 1100 access point.

The computers on the opposite side of the firewall belong to different subnets. DC, IAS and IIS are configured to subnet 10.25.25.0/24. The Access Point is configured to subnet 192.168.0.0/24. On the FIRWAL the Ethernet ports eth0 and eth1 are given IP addresses 192.168.0.1 and 10.25.25.1 respectively.

On the Cisco AP following the settings which are configured:

- Broadcast SSID off
- IP Address of the RADIUS server 10.25.25.2 with ports 1812 and 1813.
- Authentication selected 802.1X
- EAP-Type
- Encryption Dynamic WEP/TKIP.

The IP Tables software installed in the FIRWAL machine is used for filtering packets according to the rules defined by the network administrator. It also performs network address translation as packets travel from one subnet to another. The link doing NAT remembers how it mangled a packet, and when a reply packet passes through the other way, it will do the reverse mangling on that reply packet. The main advantage of using this filter is that it occupies only 64MB space unlike Microsoft's Internet Service Accelerator firewall which requires 4GB. Also it is free and open source and not proprietary software.

The rules implemented on the FIRWAL are the following:

- Before the authentication and authorization of the client is done, only TCP/UDP packets with destination address that of the IAS server 10.25.25.2 and port number 1824 and 1823 are allowed.
- Post authentication and authorization the allowed services are:
 - Dynamic Host Configuration Protocol on Port 546, 547/TCP, UDP with destination IP address 192.168.0.1 of Ethernet port eth0 of the FIRWAL machine.
 - File Transfer Protocol on Port 20, 21/TCP with destination IP address that of the Web and File server 10.25.25.4.

The authentication process for the wireless client is as follows:

1. Association and request for identity.

If the wireless AP (IP address 192.168.0.2) observes a new wireless client associating with it, the wireless AP transmits an EAP-Request/Identity message to the wireless client. Alternately, when a wireless client associates with a new wireless AP, it transmits an EAP-Start message. If the IEEE 802.1X process on the wireless AP receives an EAP-Start message from a wireless client, it transmits an EAP-Request/Identity message to the wireless client.

2. EAP-Response/Identity response.

If there is no user logged on to the wireless client, it transmits an EAP-Response/Identity containing the computer name CLIENT to the AP. If the user is logged on it sends the username TEST.

The wireless AP forwards the EAP-Response/Identity message to Ethernet port eth0 of FIRWAL with port 1812.

The wireless AP forwards the EAP-Response/Identity message to RADIUS server (IP 10.25.25.2) in the form of a RADIUS Access-Request message.

This message passes through the FIRWAL which according to the rules either allows the packet to pass or drops it. If it allows access it performs a NAT giving the source an IP address from the 10.25.25.0/24 subnet on its eth1 port.

3. EAP-Request from RADIUS server (Start TLS).

The RADIUS server sends a RADIUS Access-Challenge message containing an EAP-Request message with the EAP-Type set to EAP-TLS, requesting a start to the TLS authentication process.

The destination IP address of this packet is the same as the source IP address assigned by the FIRWAL when it performed NAT. After address

translation the packet is forwarded to the wireless AP which in turn forwards the EAP message to the wireless client.

4. EAP-Response from the wireless client (TLS Client Hello).

The wireless client sends an EAP-Response message with the EAP-Type set to EAP-TLS, indicating the TLS client hello. The wireless AP via the FIRWAL in accordance with the rules and by performing NAT forwards the EAP message to the RADIUS server in the form of a RADIUS Access-Request message.

5. EAP Request from RADIUS server (RADIUS Server's Certificate).

The RADIUS server sends a RADIUS Access-Challenge message containing an EAP-Request message with the EAP-Type set to EAP-TLS and includes the RADIUS server's certificate chain. The wireless AP on receiving the packet via the firewall forwards the EAP message to the wireless client.

6. EAP-Response from the wireless client (Wireless Client's Certificate).

The wireless client sends an EAP-Response message with the EAP-Type set to EAP-TLS and includes the wireless client's certificate chain. The wireless AP via the firewall forwards the EAP message to the RADIUS server in the form of a RADIUS Access-Request message.

7. EAP-Request from RADIUS server (Cipher suite, TLS complete).

The RADIUS server sends a RADIUS Access-Challenge message containing an EAP-Request message with the EAP-Type set to EAP-TLS, which includes the cipher suite and an indication that TLS authentication message exchanges are complete. The wireless AP on receiving the packet via the firewall forwards the EAP message to the wireless client.

8. EAP-Response from the wireless client.

The wireless client sends an EAP-Response message with the EAP-Type set to EAP-TLS. The wireless AP forwards the EAP message to the RADIUS server via the firewall in the form of a RADIUS Access-Request message.

9. EAP-Success from RADIUS server.

The RADIUS server derives the per-client unicast session key and the signing key from the keying material that is a result of the EAP-TLS authentication process. Next, the RADIUS server via the firewall sends a RADIUS Access-Accept message containing an EAP-Success message and the Send-Key and Receive-Key to the wireless AP.

The wireless AP uses the key encrypted in the Send-Key attribute as the per-client unicast session key for data transmissions to the wireless client. The wireless AP uses the key encrypted in the Received-Key attribute as a signing key for data transmissions to the wireless clients that require signing.

The wireless client derives the per-client unicast session key (the same value as the decrypted Send-Key attribute in the RADIUS message sent to the wireless AP) and the signing key (the same value as the decrypted Received-Key attribute in the RADIUS message sent to the wireless AP) from the keying material that is a result of the EAP-TLS authentication process. Therefore, the wireless AP and the wireless client are using the same keys for both the encryption and signing of unicast data.

After receiving the RADIUS server message, the wireless AP forwards the EAP-Success message to the wireless client. The EAP-Success message does not contain the per-station unicast session or signing keys.

10. Multicast/global encryption key to the wireless client.

The wireless AP sends an EAP over LAN (EAPOL)-Key message to the wireless client containing the multicast/global key that is encrypted using the per-client unicast session key.

11. Client IP address configuration.

Next, the wireless LAN network adapter driver indicates the per-client unicast session key, the per-client unicast signing key, and the multicast/global key to the wireless LAN network adapter. After the keys are indicated, the wireless client begins the protocol configuration by sending a request to the FIRWAL machine through the AP which is also configured as a Dynamic Host Configuration Protocol (DHCP) to obtain an IP address configuration.

The FIRWAL assigns it an IP address in the 192.168.0.0/24 subnet barring 192.168.0.1 and 192.168.0.2.

The CLIENT is now connected to the WLAN and has an IP address using which it can use the file transfer facility provided.

Following are some of the major problems which were encountered during the implementation:

- In the RADIUS Server the authentication was not happening. This was as there was a problem in the Remote Access Policy that was created. Two options were getting generated with an AND connector between them. One of them had to be deleted for the system to work.
- In the RADIUS server trying to access the log files using Microsoft's Event Viewer. However,

in IAS in the Event Viewer log files do not get generated.

- In the Access point the RADIUS IP address was specified but the type of EAP was not specified.

Benefits:

- **Mutual Authentication:** Both the client and the wireless AP get authenticated. Therefore minimizing the treat of Rogue Access Points.

- **Stronger encryption:** Per-Client per-session unicast key. Also, encryption Key derived after authentication therefore no need to manually manage keys.

- **Transparent:** It provides transparent authentication and connection to the WLAN.

- **User and computer authentication:** It allows separate authentication of user and computer. Separate authentication of computer allows the computer to be managed even when no user is logged on.

- **Standardization & Low cost:** 802.1X based technology is standard which means that hardware from many different vendors is likely to support the authentication process. Low cost of network hardware and reuse of existing software solution in some cases.

- **High performance:** Because encryption is performed in WLAN hardware and not by client computer CPU, WLAN encryption has no impact on the performance level of the client computer.

References:

- [1] About Internet Security Systems, Wireless LAN Security *802.11b and Corporate Networks*, 2001
- [2] Airwave Wireless Inc, Wireless Industry Standards & WLAN Management: What You Need to Know, 2006-7
- [3] Certified Wireless Security Professional Official Study Guide, TATA McGraw Hill, 2007
- [4] Cisco, Secure Wireless Integrity of Information on the Move, 2007
- [5] Joseph Davies, Deploying Secure 802.11 Wireless Networks with Microsoft Windows, Microsoft Press, 2004
- [6] Matthew Gast, 802.11 Wireless Networks: The Definitive Guide, O'Reilly, April 2002
- [7] Microsoft Corporation, Secure Wireless Access in a Test Lab, April 2005
- [8] Microsoft Corporation, Secure Wireless Access Point Configuration, August 2006
- [9] Microsoft Corporation, Securing Wireless LANs with PEAP and Passwords, 2004

- [10] Microsoft Corporation, Securing Wireless LANs with Certificate Services, 2004
- [11] www.wikipedia.com