THE IMPLEMENTATION OF MULTISTAGE HACKING DEFENSE SYSTEM FOR WIRELESS LANS

Muayad K. Murtadha
Computer Center, University of Baghdad. Baghdad- Iraq.

Abstract

The security of wireless LANs has been a source of concern for businesses and individuals, who are aware of its advantages due to its flexibility, ease of development and reconfiguration. With the increase in the use of wireless LANs for enterprises and homes, where information resources are shared continually, security is of the essence. Wireless security and hacking defense systems becomes an alarming concern as everything being transmitted is available in the air. Encryption and Authentication are seen as major tools in the line of defense of wireless LANs. This paper discusses the various security protocols used in wireless LANs and how effective they are in keeping wireless LANs secure. The risks of using these protocols are outlined, and recommended suggestions for practical multistage hacking defense implementations with modern technologies are detailed. Also, the results of testing experiments for some protocols are presented.

بناء نظام دفاع متعدد المراحل ضد القرصنة المعلوماتية للشبكات اللاسلكية المحلية

مؤيد خليل مرتضى

مركز الحاسبة الألكترونية، جامعة بغداد. بغداد – العراق.

الخلاصة

أمن الشبكات اللاسلكية المحلية اصبح مصدر اهتمام للاعمال العامة و الفردية التي تتطلع الى فوائدها بسبب مرونتها و سهولة تطويرها و كذلك اعادة تركيبها و برمجتها. مع ازدياد استخدام الشبكات اللاسلكية في الشبكات الكبيرة و المنزلية، حيث مصادر المعلومات يتم مشاركتها بأستمرار، أمن الشبكات اللاسلكية يعتبر جوهر الموضوع. أمن الشبكات اللاسلكية و انظمة الدفاع من القرصنة المعلوماتية اصبحت محور اهتمام شديد لأن جميع المعلومات المرسلة تكون متوفرة على الهواء. التشفير و الموثوقية ظهرت كأدوات رئيسية في خط الحماية في الشبكات اللاسلكية. هذا البحث يناقش مختلف بوتوكولات الحماية المستخدمة في الشبكات اللاسلكية و كيفية تأثيرها و فعاليتها في الحفاظ على أمن الشبكات اللاسلكية. المخاطر الخاصة بهذه البروتوكولات اوجزت، و كذلك توصية لمقترحات عملية لبناء دفاع متعدد المراحل ضد القرصنة المعلوماتية مع التقنيات الحديثة تم تفصيلها. كذلك نتائج بعض تجارب الاختبارات لبعض هذه البروتوكولات تم عرضها.

Introduction

Wireless networking increases the flexibility in the home, work place and community to connect to the internet without being tied to a single location. With the benefits of Wireless Local Area Network (WLAN) or Wireless Fidelity (Wi-Fi) there are also some risks which users should be aware of, where, without any security implemented, unauthorized users may

steal data or load malicious code onto the network [1].
Unlike wired networks, the radio signal produced by wireless networks can penetrate walls, ceilings, floors and are therefore not confined to a building. Hackers can effortlessly pick up these signals from the outside of the building using easily available wireless detection tools. While a typical user would normally not transmit sensitive data, the increasing growth of the use of e-government services and e-commerce has meant that more sensitive data is being transmitted by citizens to local and national government. Therefore, the radio signal can easily be detected externally or in a neighboring building. This means that the attacker does not need to infiltrate the building to hack the network. Wireless detection devices work in two modes, passive and active. The passive mode listens for the access points broadcast, which may or may not contain the Service Set Identifier (SSID). Whereas active mode uses the probe request and response to detect access points, which involves the access point responding to the probe request [2].
Attacks on WLANs can be categorized as passive attacks, active attacks, Denial-of-Service attacks (DoS) and Man-in-the-middle attacks [3][4].

A. Passive Attacks - Accidental users

Occasionally, when trying to connect to an Access Point (AP) the computer may automatically connect to a different network and the user may "accidentally" use that connection without realizing it belongs to a third party. This may occur in the work place when users are unfamiliar with the company's SSID of access point and pick up a neighboring company's unsecured network.

B. Active Attacks - Brute force attack

A brute force attack is the systematic testing of different letters, numbers and symbols until the correct password or key is guessed. There are a number of software programmes available on the Internet that can be used to recover encryption keys on wireless LANs.

C. Denial-of-Service Attacks

A DoS can cause a network to slow down or become unusable. A DoS attack may occur if the attacker generates a lot of traffic on the network, which may block the server for hours or by attacking the resource itself. Another form of DoS attack is the use of a strong radio signal. This denies legitimate users from accessing a resource.

D. Man-in-the-Middle Attack - Evil Twin

A Man-in-the-middle attack occurs when an attacker is able to read and modify communications between two parties without them being aware of the attacker's presence.
To explain the proposed system, first we need to describe the wireless security protocols. Because of that, the paper is organized as follows:
Section 2 illustrates the most widely used wireless security protocols and techniques, while section 3 will describe the practical implementation of the multistage wireless networks security system, finally section 4 will explain the experiments and the test results.

Security Protocols in Wireless Network Devices

Many wireless devices such as access points and wireless routers have security features which can be configured to prevent attacks on wireless networks. Over time, the level of security has increased with the realization that the original security settings were flawed [3][5].

1. Wireless Equivalent Privacy (WEP)

In 1997, WEP was developed by the 802.11b task force with the introduction of wireless technology, and was the first encryption protocol to be deployed with wireless networks. WEP incorporates two types of protection, a secret key and encryption. The secret key, comprising of a 5- or 13-character simple password, is shared between a mobile device and a wireless access point. This key is used in the encryption process to scramble each packet of information with a unique password before transmission. The secret key is used to encrypt packets before they are transmitted. WEP also uses an Initialization Vector (IV) to augment the shared WEP key (secret key) to avoid encrypting two ciphertexts with the same key; this produces a different RC4 key for each packet. RC4 is a stream cipher that generates a pseudorandom stream of bits. Before a data packet is transmitted, an Integrity Check (IC) computes a checksum. Then WEP concatenates the data and IC with the key stream using the Exclusive-OR (XOR) function. WEP uses the RC4 algorithm for encryption and the same key

used to encrypt and decrypt the data. The purpose of the RC4 algorithm is to keep hackers from altering the data during the transmission. The RC4 algorithm then generates the key stream from the secret key and IV. By regenerating the RC4 key stream from the IV and the known key, the recipient can decrypt the data by running XOR [4].

It was soon discovered that the WEP security protocol was flawed and it was discovered that a passive attack could recover the RC4 key after eavesdropping on the network for a few hours. A hacker could use an XOR function to mathematically link two packets of a session that have been processed with the same IVs, i.e. identical RC4 keys, which can be used to recover the key [4][6]. Another fault with the WEP protocol was that the authentication only verifies the client machine, not the actual user accessing the machine [6].

2. Temporal Key Integrity Protocol (TKIP)

Temporal Key Integrity Protocol (TKIP) was the immediate replacement for WEP, which aimed to fix the problems, associated with WEP including small initialization vectors (IV) and short encryption keys. TKIP is a suite of algorithms that wrap around the WEP protocol to make it more secure. The reason why TKIP is an improvement on WEP is that it rotates the temporal keys; therefore, a different key is used for each packet. Each packet transmitted using TKIP has a unique 48-bit serial number that is incremented every time a new packet is transmitted [4].

Each time a wireless station associates with an access point, a new base key is created. The base key is built by hashing together a special session secret with some random numbers generated by the access point and the station as well as the Media Access Control (MAC) address of the access point and the station. This mixing operation is designed to put a minimum demand on the stations and access points, yet have enough cryptographic strength so that it cannot easily be broken. Putting a sequence number into the key ensures that the key is different for every packet [6]. TKIP also utilizes an integrity-checking feature called Message Integrity Check (MIC). This part of TKIP closes a hole that would allow a hacker to inject data into a packet, which allows the hacker to deduce the streaming key used to encrypt the data. MIC uses a cryptographically protected one way hash in the payload, which ensures packet tampering detection occurs immediately upon decryption. Compared to WEP, TKIP is a costly process and may degrade performance at many access points[6].

3. Wi-Fi Protected Access (WPA)

WPA was created by the Wi-Fi Alliance based on the WEP protocol, but utilizes the stronger encryption technology used in TKIP, which offers pre-packet key mixing and a message integrity check [3].

Although WPA is stronger than WEP, it is, however, vulnerable to DoS attacks. Initially designed as a safety feature, WPA shuts down the network if at least two packets using the wrong key are sent every second. A hacker could use this security feature to their advantage and can potentially bring down a WPA protected LAN. If this happens the access point assumes the hacker is trying to gain access to the network. The access point shuts off all connections for 1 minute to avoid the possible compromise of resources on the network. Thus, a continuous string of unauthorized data could keep the network from operating indefinitely. While this feature was designed to safeguard against breaches of security, it presents a prime opportunity for a hacker [4].

WPA comes in two modes, *enterprise mode* and *consumer mode*. Enterprise mode uses Remote Authentication Dial In User Service (RADIUS) for authentication. The RADIUS server checks that the information is correct using the authentication scheme Extensible Authentication Protocol (EAP) to process the information. If accepted, the server will then authorize access to the Internet Service Provider ISP system, select an IP address and Layer 2 Tunneling Protocol parameters [7]. A RADIUS server can be used for different internet connections other than dial-up. The *authentication server* is a certificate authenticator that only allows client stations to connect with the access point if it sees a valid certificate on the client, where the server is provided with database that contains all authenticated clients [8]. The consumer mode (or personal mode) of WPA uses a combination of pre-shared keys (PSK), TKIP and MIC. The consumer version is typically used in homes or small offices, which require each user to enter a common password. If consumer mode users select the typical 6-8 character passwords that corporate networks require for login purposes, the resulting system will still be insecure. WPA-

PSK (Wi-Fi Protected Access with Pre-Shared Key) is the better choice for Small Office and Home Office SOHO users, because of its simple setup and deployment across a multi-vendor environment. Although WPA-PSK was originally intended for home users, it has been adopted by small offices due to the cost and difficulty in setting up a RADIUS server [6].

4. Wi-Fi Protected Access 2 (WPA2)

The current standard for wireless security, Wi-Fi Protected Access 2 (WPA2), was introduced in September 2004. The IEEE 802.11i standard WPA2, addresses three main security areas: authentication, key management, and data transfer privacy. WPA2 uses the Advanced Encryption Standard (AES) for data encryption and is backward compatible with WPA. Like WPA, WPA2 is also available in Personal and Enterprise modes. WPA2 allows an easy transition from WPA mode by using WPA/WPA2 mixed mode, so networked computers can use either WPA or WPA2. However, although WPA2 implements the full standard, it will not work with some older network cards [6].

The encryption algorithm used in the 802.11i security protocol is AES-Counter Mode (Cipher Block Chaining- Message Authentication Code) CBC-MAC Protocol (AES-CCMP). It uses the AES block cipher, but restricts the key length to 128 bits [6][7].

5. Extensible Authentication Protocol

WPA and WPA2 enterprise modes both utilize the Extensible Authentication Protocol (EAP) as an authentication framework. EAP is an 802.1X standard that allows developers to pass security authentication data between the RADIUS server, the access point and wireless client [6]. EAP has a number of variants, including EAP MD5, EAP-Tunneled TLS (EAP-TTLS), Lightweight EAP (LEAP), and Protected EAP (PEAP). EAP resides in the access point and keeps the network port disconnected until authentication is completed. Depending on the results, either the port is made available to the user, or the user is denied access to the network [7][8].

6. Robust Secure Network (RSN)

Robust Secure Network (RSN) is a protocol used for establishing secure communications over an 802.11 wireless network, and is an element of the 802.11i standard. RSN dynamically negotiates the authentication and encryption algorithms to be used for communications between wireless access point and wireless clients. This means that as new threats are discovered, new algorithms can be added. Transitional Security Network (TSN) is a specification that is designed to allow RSN and WEP to coexist on the same wireless LAN [6].

Implementation of Multistage Wireless Network Security

The hackers and intruders can easily connect to the campus network through the wireless connection, as WLAN with no security enhancement enabled is just like throwing the hub ports outside the campus to allow anyone to connect for free. Wireless detection tools can determine the level of security and an unsecured network is an easy target even for novice hackers [9].

In order to secure a wireless network users should follow a number of procedures to prevent the network from being penetrated. From the outset, some devices have the security settings disabled as the default option; therefore it is important to switch on the security settings when setting up the device [10][11] .

Although WPA and WPA2 are securer encryption protocols than WEP, and WEP is well renowned for its weaknesses, if the access point only supports WEP it is worthwhile enabling it. This will prevent neighboring Wi-Fi users without the knowledge or intention to hack from sharing bandwidth. It is also important to change the password regularly, as an attack may occur over a long period of time if the intruder is determined to gain the information [12][13].

Seeing how vulnerable is the wireless network compared to the wired network, it is important to implement a multistage security recommendations, as shown in figure 1, by using all the available security protocols provided with most wireless network devices, which summarized below.

A. Change Default SSID, IP Address and Login Details

Tougher SSID, which is the name of AP can be set rather than using the default SSID of the access point. Broadcast of SSID can also be disabled to prevent the detection of the wireless access point through the usage of war driving software. The default/fixed IP address (like in some AP's) should be changed. Linksys AP uses

login/password for accessing AP's management console and some other APs use no specific initial passwords. The network administrator only has the authority to change the password and the IP address of the access point. These details need to be changed immediately.

Figure 2(a) shows the password screen to enter the access point and then configuring it, while figure 2(b) shows the password screen management window that allows the network administrator can change the password of the access point.

Figure 3 shows the basic setup screen that allows the network administrator to change the default name of the access point (SSID) and IP configuration (IP address, subnet mask, and gateway).

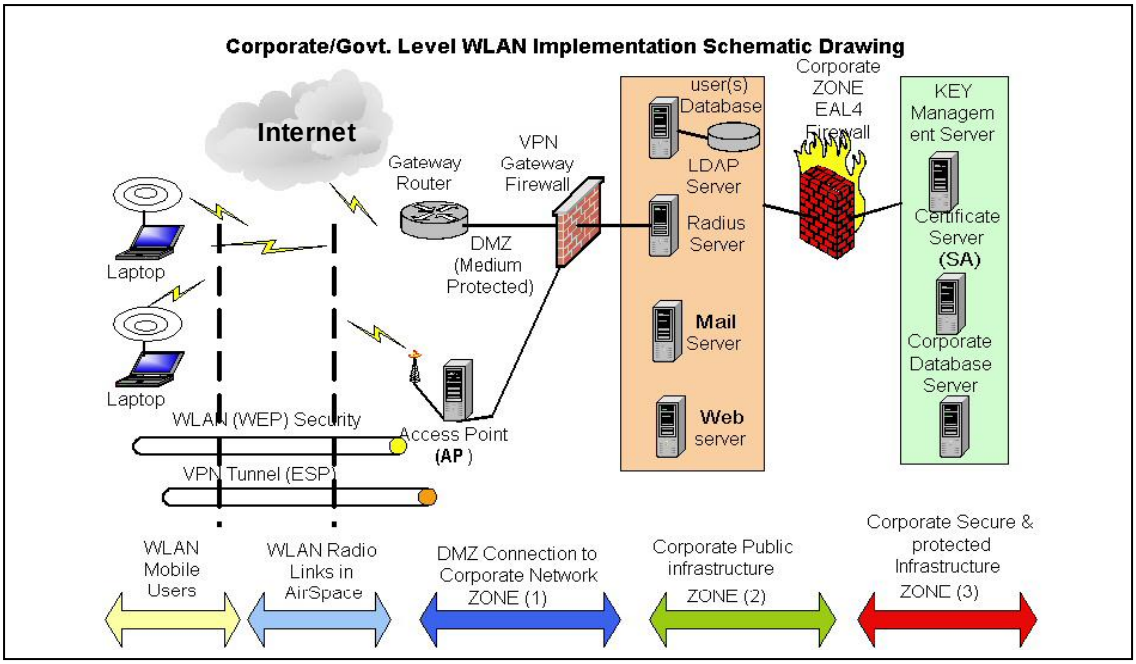
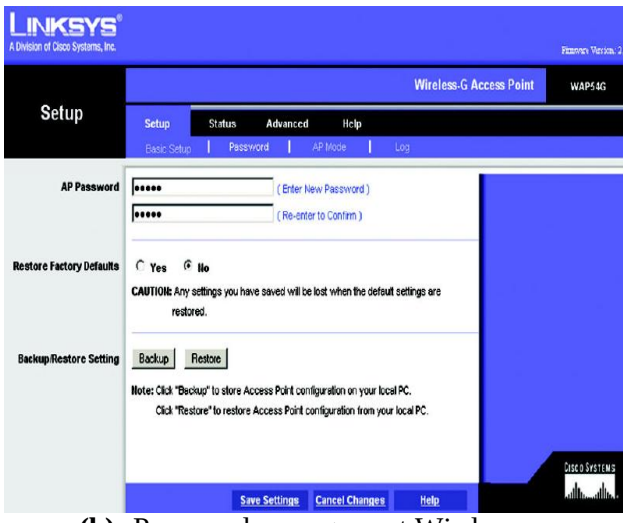


Figure 1: Multistage Security Model for Wireless Networks

(a): Password Screen Login



(b): Password management Window

Figure 2: Password Screen Windows

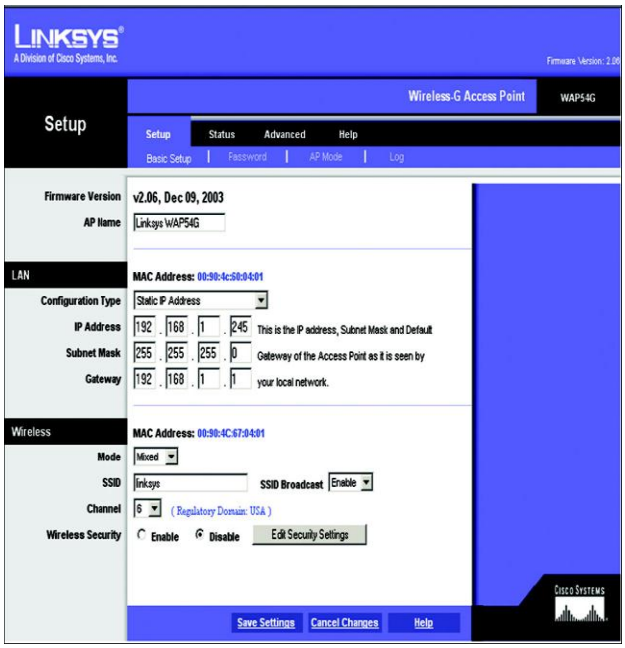


Figure 3: Basic Setup Screen to Change SSID and Default IP

B. Enable Encryption Schemes

As for WEP encryption, 128-bit WEP key should be used instead of 64-bit WEP key since it is harder to crack as shown in figure 4. The WEP key shall be a very random alphanumeric combination. In order to overcome the weakness in the WEP, use Temporal Key Integrity protocol (TKIP) that helps to minimize cryptographic attacks against WEP key, brute force attack and the weakness of static key. TKIP also help to prevent undetected modification to the WEP key by providing an 8-byte message integrity code (MIC). Furthermore, Counter mode Cipher Block Chaining with message authentication codes (counter mode CBC-MAC or CCMP) which will be the long term security solution introduced by 802.11i standard uses Advanced Encryption Standard (AES) which encrypts data in 128-bit chunks using cipher block chaining (CBC) mode and provides data integrity checks via Medium Access Control (MAC). It is best to use WPA or WPA2 for encryption with RADIUS authentication server as shown in figure 5, where this protocol is available in most modern network devices.

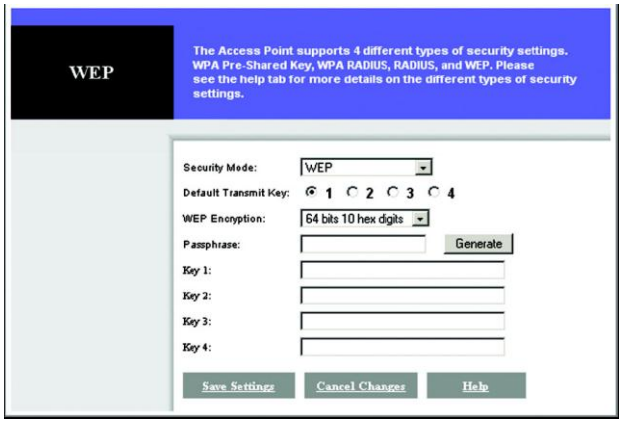


Figure 4: WEP Setting in Linksys AP

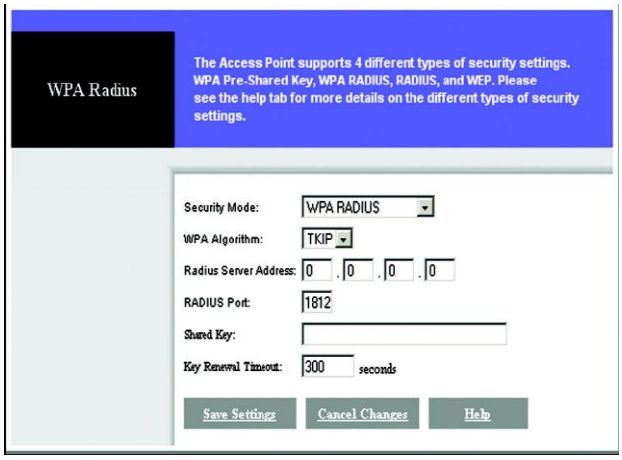


Figure 5: WPA Setting in Linksys AP

C. Use MAC Filtering

At the AP end and/or on RADIUS server, MAC filtering can be used to provide MAC address based authentication. Though MAC address can be spoofed, it can certainly help along with other security guards. MAC address filtering was enabled on the access point and the MAC addresses of the wireless network interfaces were entered as shown in figure 6 so that the wireless access point does not allow any computer except the ones that are connecting with the given MAC addresses.

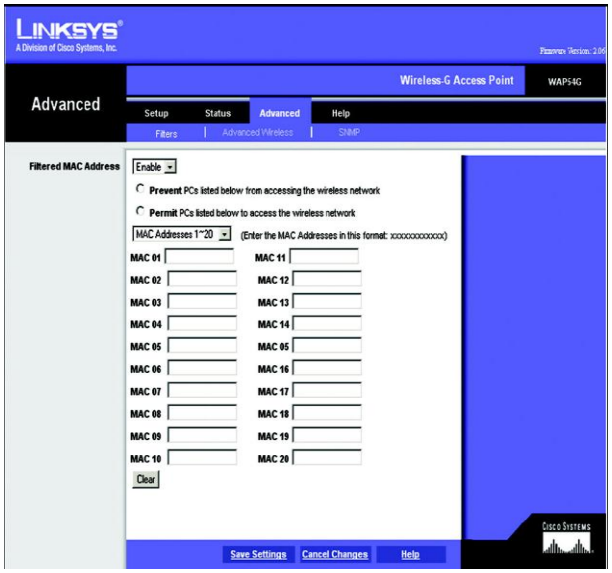


Figure 6: MAC Filtering in Linksys AP

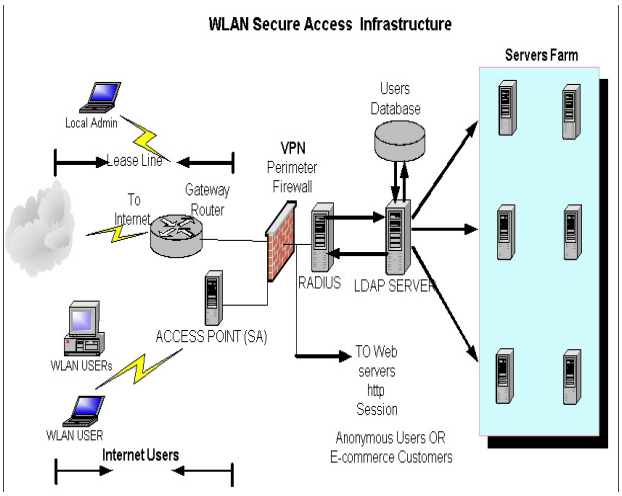


Figure 7: Extensible Authentication Protocol Implementation with RADIUS Server [8]

D. Implement EAP Authentication with RADIUS server

Its very important to improve over all network security by implementing EAP authentication on a RADIUS server as shown in figure 7, which would act as a backend process to verify user or station credentials, such as when WLAN user is accessed. It also ensures mutual authentication (client to AP and AP to client authentication). So only users having a RADIUS server account can access the WLAN. When Supplicant (Client) becomes active status on Client device and connects to AP. Authenticator detects the client's connection request and then passes only 802.1X traffic from the supplicant as shown in figure 8. The supplicant sends an "EAP-Start" message to the authenticator, and then authenticator replies an "EAP Request Identity" message for getting the client ID. The supplicant's "EAP Response" packet which includes the client ID is pass on to authentication server, then the authentication server authenticates the client using AES algorithm. Traffic allowance depends on a "Radius-ACCEPT" packet or a "Radius-REJECT" packet which is passed from the Radius server to the AP. 802.1X provides methods of identifying certificates that the wireless client can communicate with the authentication server. Microsoft Windows Server 2003 come with its own RADIUS server and certificate authority CA offering as shown in figures 9 & 10.

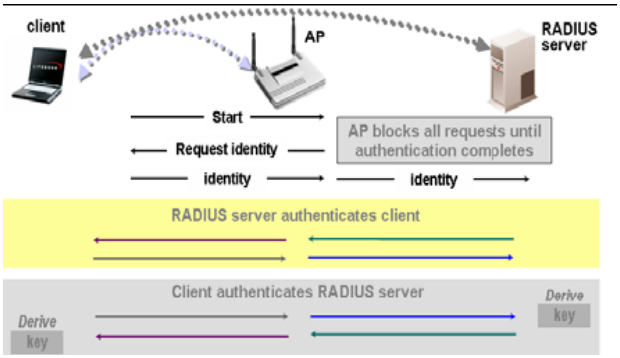


Figure 8: 802.1X Authentication Process [8]

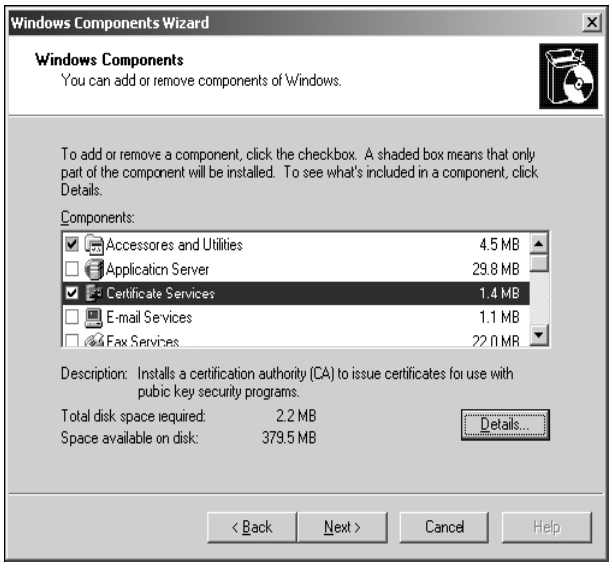


Figure 9: Certificate Services, installed from the Windows Components Wizard

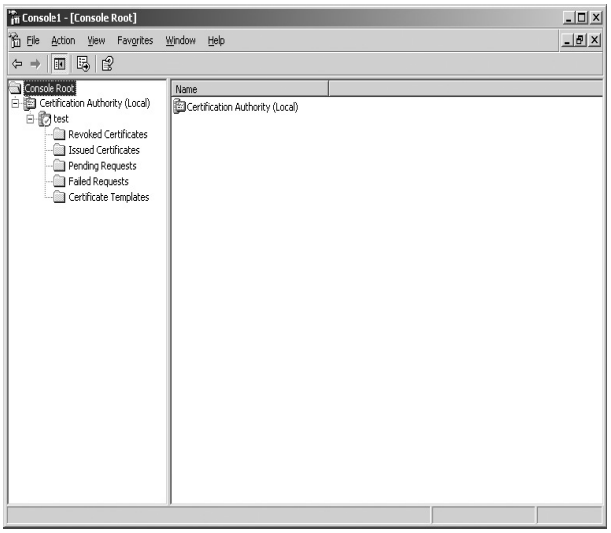


Figure 10: Management of Certification Authority in MS Windows 2003

E. Centralized Management of Access Points

The security management of the Access Points can be made better, especially when the WLAN deployment is large with many APs installation a cross a campus. In such a situation, security configuration and other policies need to be done on individual APs and that can be a hassle when the numbers of APs increase. To make the AP's less intelligent from what it is now, putting an intelligent central switch to control a limited set of AP's configuration, policy and security settings, like in any client-server environment as shown in figure 11. Hence the management of AP security settings can be done centrally.

One drawback of this technique happen when the central switch becomes idle, this leads to shutoffs the entire network until maintaining the central switch or changes it with new one.

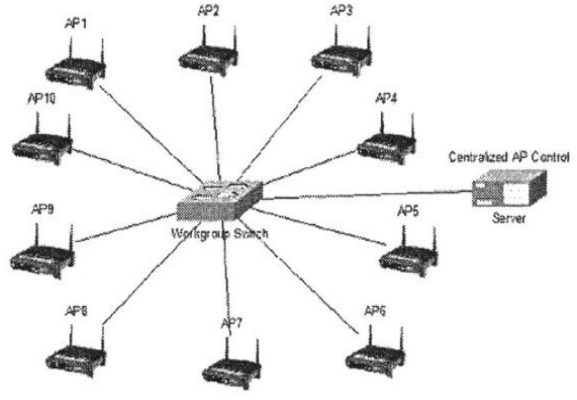


Figure 11: Centralized AP Control Switch to Reduce the Work of Configuration and Management of Each AP Separately [12]

F. Usage of Monitoring Software

It would be suggestive to use monitoring tools to police the activities on WLAN like intrusion and rogue access points [14]. One such example is to use network monitor, where Network Monitor is a very basic IP traffic monitoring tool included with Windows Server 2003, as shown in figure 12. It can only be used to monitor traffic to and from the server. Network Monitor can be used to capture data, filter data, identify other Network Monitor users on the local segment, and view packet data. In any case, an intelligent WLAN monitoring tool or Intrusion detection software can help to locate suspicious activities

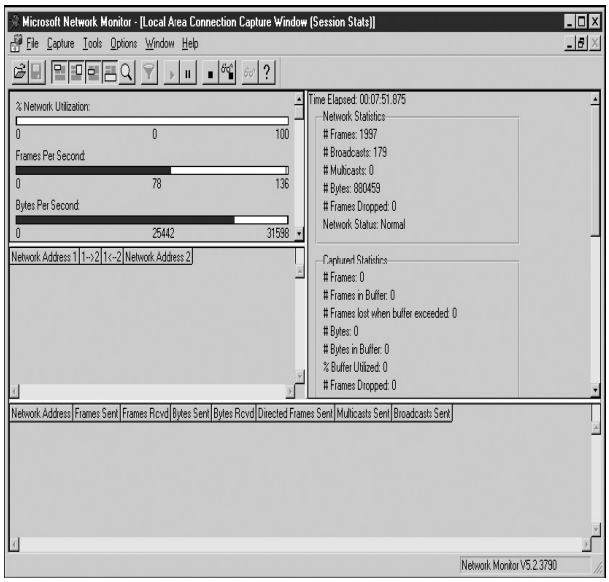


Figure 12: Network Monitor Included in Windows Server 2003

G. Antenna Positioning and Shielding

Antenna positioning can help the radio waves to be more directed and antenna shielding with radio transmission power adjustment can confine it to a more restricted environment. Also shielding the AP with aluminum foil can be carried out.

H. Implementation of Firewall

Implementation of firewall as shown in figure 13 between AP and the wired LAN can help to increase the security, as the firewall can be set to prevent unauthorized access. Specific IP addresses or address blocks, MAC addresses, Ports, Protocols etc. can thus controlled. Firewall services available in many wireless access points, and also firewalls comes with many operating systems such as Windows

server 2003 with many features and capabilities as shown in figure 14.

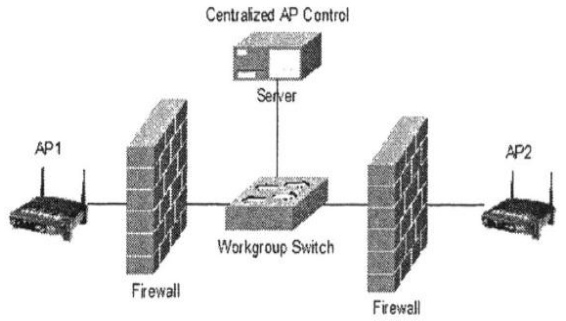


Figure 13: Firewall Implementation Between The AP and Wired LAN Switch To Block Unauthorized Access From Intruders

Figure 14: Firewall Implementation in MS Windows server 2003

I. Implementation of VPN

Implementation of Virtual Private Network (VPN) can secure WLAN traffic. Here tunneling protocols like Point To Point Tunneling Protocol (PPTP), Layer Two Tunneling Protocol (L2TP) and IPSec can be used that encrypts the traffic. By using VPN, only authorized users can log in to the wireless network that will also require the user's username and password. The VPN server provides secure ways for user to connect to campus and Internet resources. IPSec which is a set of protocols developed to support secure exchange of packets at IP layer has been deployed widely to implement VPN. Figure 15 shows the main window to implement VPN server by using VPN services available in windows server 2003.

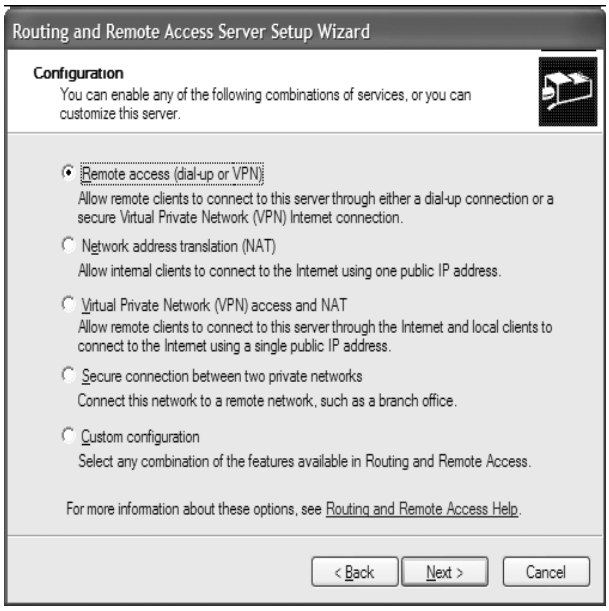


Figure 15: VPN in Windows server 2003

4. Experiments and Results

The system has been tested in a simple lab related to a company specialized in Information Technology solutions, which have many experienced teams, engineers and technicians in the field of networks security and they use different tools for hacking wireless network.

The simple lab consisted of a centralized switch connect to the company networks, which have many access points distributed in three floors, and server computer supported with Microsoft windows server 2003 to implement RADIUS and to monitoring network traffics also.

Any hacking or improper wireless connectivity to wireless network means that the intruder is deeply in the network. This person is able to gain unlimited access to the company's resources as if he insider.

The WLAN security checked by putting WLAN under survey to several types of attacks related to different layers before deploying the multistage hacking defense system, where several WLAN hacking and cracking utilities had started their attacks while the WLAN has been tested and monitored. These attacks included: passive attacks (accidental users), active attacks (brute force attack), denial-of-service attacks, man-in-the-middle attack, session hijacking, broadcast monitoring, base station clone intercept traffic, plug-in unauthorized users and plug-in unauthorized devices.

Since the main wireless security protocols summarized in encryption and authentication processes, therefore the experiments details user

authentication attacks, transmission attacks and insertion attacks (when unauthorized devices are placed on the wireless network without going through a security process).

Some of the experiments were carried out while the access point uses WEP encryption protocol as shown in figure 16, and figure 17 that explains the experiments when using MAC filter firewall. While figure 18 shows the results of experiments when using WPA with RADIUS server (encryption and authentication solution).

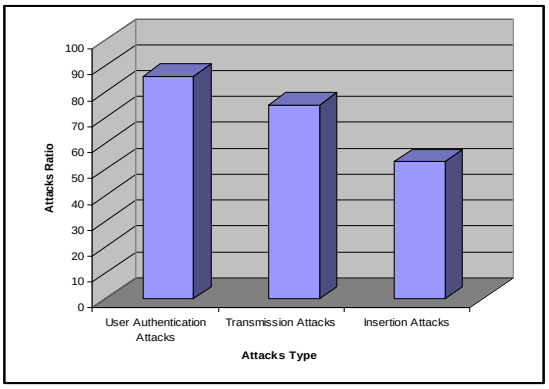


Figure 16: Attacks Ratio When Using WEP

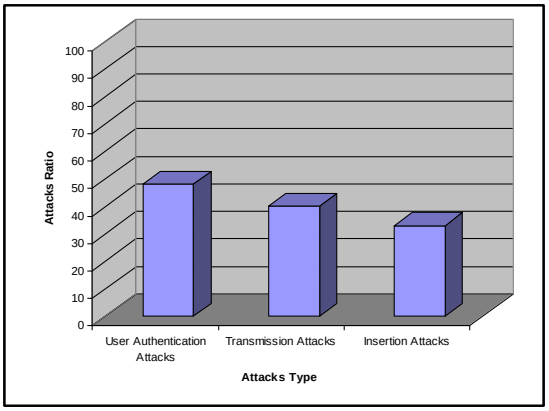


Figure 17: Attacks Ratio When Using MAC Filter Firewall

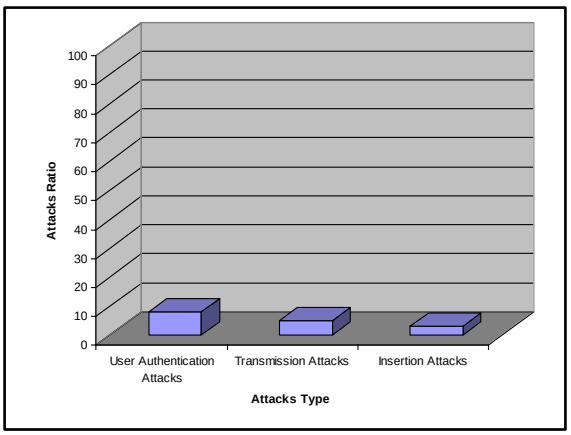


Figure 18: Attacks Ratio When Using WPA with RADIUS Server

In these figures, the x-axis used to represent different attacks types, while the y-axis used to represent the attacks ratio which is the percentage of all users using the network to the number of attackers that can hack the network.

Any wireless network is vulnerable to attacks, as they do not even implement the basic WEP key encryption protocol. However enabling the WEP protocol is not enough as different software tools can be used to capture the packets and then to crack the WEP key, that's clear by experiments results obtained as shown in figure16. Also, MAC filtering firewall may be used that gives better performance than WEP key protocol as shown by the experiments in figure 17, because there are many and many cracking tools on the Internet designed for WEP protocol, but it is still not enough because there are many tools to change devices MAC address and then putting them inside the network. So WPA with TKIP/AES encryption and EAP authentication with RADIUS server is the best enterprise solution that tested successfully by the experiments on the wireless network as shown in figure 18.

Conclusion

WLANs offer new services that traditional wired LANs cannot provide, but they also introduce new security concerns. As wireless local area networks become integral parts of any enterprise networks, it has become important that the wireless components of the network be as secure as the wired network. Although the early versions of WLANs were not designed for security, standards and methods are emerging for securing WLANs. With 802.1X and 802.11i protocols, there is now a good choices for encryption and authentication. Therefore all wireless security protocols used by wireless devices are described such as WEP, TKIP, WPA, and WPA with RADIUS server…etc.

These emerging security features must be implemented in order to assure the security of information on the wireless networks. To enhance WLAN security and to improve hacking defense system, many stages of security techniques are explained, so multistage hacking defense system can be easily implemented with simple and dynamic features such that it can be upgraded to add more security products. With careful planning and good configuration for wireless devices, a wireless network can be as secure as a wired network. Human factors are as

important as technical factors in ensuring wireless security management.

Some of the security stages are tested in a simple lab connected to enterprise WLAN network. Experiments were carried out under situations where the results are taken when several hacking and cracking utilities had started their attacks while the WLAN has been tested.

These results are based on practical experiments. No system is 100% secure because the security here depends on commercial products, which have their own vulnerabilities. We have to conduct another set of experiments using much more attacking and cracking tools and different security products rather than those used here, and then get an average. Those results may vary slightly depending on the type of security products deployed. This is because the performance of the system is tightly related to the performance of each individual security product's behavior. The multistage system only directs the operations of these security products and gathers its results then translates them into policies and recommended actions. Thus, the weaknesses of individual stage may cancel when using multistage hacking defense system.

Beside this, we can mention that the multistage security technique has two drawbacks:

1. It has high delay time compared to individual security stages because it summarize the time delay of all stages implemented and this leads to performance degradation.
2. The cost of multistage security is high because it requires using RADIUS server (hardware and software) with assisted modern wireless devices that have WPA capability.

References

1. Stewart S. Miller, **2003.** *Wi-Fi Security* , Published by McGraw-Hill.
2. Omar Santos, **2008**. *End-to-End Network Security Defense-in-Depth*", Cisco Press,.
3. Kevin Beaver, Peter T. Davis, **2005**. *Hacking Wireless Networks For Dummies* , Wiley Publishing, Inc, Pages: 65-80.
4. Carsten Maple, Helen Jacobs and Matthew Reeve, **2006.** Choosing The Right Wireless LAN Security Protocol for The Home and Business User, Proceedings of the First International Conference on Availability, Reliability and Security, Pages: 8.
5. Randall K. Nichols and Panos C. Lekkas, **2003.** *Wireless Security: Models, Threats, and Solutions*, Published by McGraw-Hill, Pages: 330-345.
6. Jiang Li and Moses Garuba, **2008.** *Encryption as an Effective Tool in Reducing Wireless LAN Vulnerabilities*, Fifth International Conference on Information Technology, Las Vegas. Pages: 557-562.
7. Tae-Sub Kim, Yi-Kang Kim, Byung-Bog Lee, Seung-Wan Ryu and Choong-Ho Cho, **2008.** *Designs of a Secure Wireless LAN Access Technique and an Intrusion Detection System for Home Network*, Forth International Conference on Network Computing and advanced Management, Volume 1, Pages: 318-324.
8. Mohammad R. Ahmadi and Muhammad M. Satti, **2007.** *A Security Solution for Wireless Local Area Network (WLAN)* , International Symposium on High Capacity Optical Network and Enabling Technology, Pages: 1-6.
9. Chris Brenton and Cameron Hunt, **2003.** *Mastering Network Security*", Published by SYBEX Inc, Pages: 430-438.
10. Fareeha Waheed, Sadia Muhiuddin and Saqib MIlyas, **2005**, Multi level Security For Wireless LAN, The Student Conference on Engineering Sciences and Technology, Pages:1-9.
11. Hassan M. Faheem, **2005.** Multiagent Based Security for The Wireless LAN, *IEEE Potentials*, **24(**2):19-22.
12. Chan, F.K.L.; Ang Hee Hoon and Issac, B., **2005**, Analysis of IEEE 802.11b Wireless Security for University Wireless LAN Design, IEEE 7th Malaysia International Conference on Communication, Volume 2, Pages: 16-18.
13. Samad S. Kolahi, Shaneel Narayan, Du D. T. Nguyen, Yonathan Sunarto and Paul Mani**, 2008.** The Impact of Wireless LAN Security on Performance of Different Windows Operating Systems, IEEE Symposium on Computers and Communications, Pages: 260-264
14. Lapiotis, G.; Byungsuk Kim; Das, S. and Anjum,F., **2005**, A policy-based approach to wireless LAN security management, Security and Privacy for Emerging Areas in Communication Networks, Workshop of the 1st International Conference, NewJersy, Pages:181 – 189.