Security Methodologies for Wireless Networks

Michael Clonts
Computer Science 591
December 12, 2010
University of Colorado at Colorado Springs

I. INTRODUCTION

Wireless network technology is pervasive. Restaurants, schools, public buildings, and many residential homes support some level of internet accesses using 802.11 wireless protocols. As the ubiquity of wireless networking increases, users and providers make assumptions that their networks are secure, or they assume that the effects of unauthorized access to their networks would not be severe [1].

With this in mind, it becomes very important for wireless network users to understand the risk inherent in this activity and know how to protect themselves against them. This document attempts to create practical guidelines that wireless network users can follow to protect themselves and their data. Research will focus on two main areas:

1) *Home wireless networks:* How does one configure a home wireless LAN to ensure the highest level of security?

2) *Public wireless networks:* How can one conduct secure network transactions using a public wireless hotspot?

II. FUNDAMENTALS OF WIRELESS NETWORKING

The obvious, and key, difference between a conventional wired network and a wireless network exists at the physical layer. While cables provide some inherent protection of the information carried within, a wireless packet that is broadcast between two points is equally available to any other wireless device in the immediate area. In fact, studies reveal that through the use of high-gain antennas, wireless network data has been surreptitiously received over a mile from the source of the transmission [5]. While this is an extreme example, it underscores the importance of implementing robust security features in a wireless environment.

Wireless network transmissions generally adhere to the IEEE 802.11 set of standards, which define modulation types and other conventions for networking in frequency bands from 2.4 – 5 GHz [3]. Given the broadcasted nature of wireless traffic, encryption of data is naturally the most important feature of any wireless security policy. The encryption methods described in the 802.11 standards have evolved as new amendments are adopted. The earliest versions of the standard used WEP, Wired Equivalent Protection. As evident in its name, this encryption method intended to provide confidentiality equal to that of a wired network [2]. However, in practice, WEP has proved to be far less secure than a wired network.

A. WEP

The original 64-bit WEP utilizes an RC4 cipher key consisting of a 24-bit initialization vector concatenated with a 40-bit key. Later implementations of WEP increased the key size to 128 and 256 bits. However, regardless of the key size, one fundamental flaw of WEP is that the initialization vector is transmitted in clear text with every packet, so an eavesdropper will know 24 bits of every packet. This combined with the weak RC4 key schedule results in successful cryptanalytic attacks to break the encryption. Software programs are publically available that crack WEP encryption after capturing and analyzing a sufficient number of packets. Because of the weakness in RC4, this process sometimes take only a matter of minutes [3].

Other problems with WEP include its lack of a key management policy and a lack of cryptographic integrity protection. Regarding key management, because there is no automatic or frequent requirement for changing keys, the management is left as an exercise for the network administrators. As a result, keys are often left static for long periods of time and are shared between many users. This results in a large amount of cipher-text using the same key data available to any network eavesdroppers, increasing the risk that they may recover the key by analysis. Regarding integrity, the 802.11 MAC protocol uses the CRC-32 algorithm to create a four byte checksum for each packet. However, this checksum is not encrypted, which exposes the protocol to an active attack where a hacker modifies the

checksum, one byte at a time, and sends the packet to see when it will be correctly acknowledged. When an acknowledgement is returned, the correct checksum has been guessed, which gives the attacker some level of information about the cipher text [3].

In terms of authentication, WEP supports a shared key authentication sequence before allowing a client on the network. The sequence involves the access point sending a clear text challenge to the client, the client encrypting the text (using the same WEP key used for normal communication), and the access point validating this key was correctly encrypted. In theory, this authentication should better protect the network by ensuring only valid clients have the ability to send traffic to the network, which will limit the possibility of denial of service attacks by a flood of traffic with the wrong WEP key. However, practical examples have shown this authentication method actually *reduces* the security of a network because of both the clear and cipher text strings are transmitted during the authentication [3]. When an attacker has access to both clear and encrypted text, it is easier to recover the encryption key and gain access to the network.

Additionally, WEP provides no checksum validation of packet headers, which results in a lower integrity system than is otherwise possible. Likewise, this protocol does not maintain any sequence counters in packets; this leaves it susceptible to a replay attack of recorded legitimate messages.

B. WPA

Because of the limitations described above, WEP is not recommended as a security method for wireless operations, though most wireless network devices still allow its use. As a replacement for WEP, the IEEE introduced WPA, or WiFi Protected Access, as an intermediate security method that solves some of the vulnerabilities of WEP. WPA adds additional security measures while remaining backwards compatible with equipment running in a WEP environment.

WPA offers enhanced encryption over WEP by using the Temporal Key Integrity Protocol (TKIP). Most notably, TKIP performs a key mixing function that combines the secret key with the initialization vector before performing the RC4 encryption. This ensures that an eavesdropper can no longer view the initialization vector in clear text. Additionally, WPA adds a sequence counter to messages that ensure out of order packets are not accepted; this prevents attacks where legitimate messages are replayed at a later time. Finally, to overcome the integrity issues caused by a non-cryptographic CRC algorithm, WPA uses a method called Message Integrity Check (MIC). Because frames first have to match the correct TKIP sequence counter before entering the integrity check, it make the hacking practice of systematically changing and resending packets to gain information entirely impractical [2].

However, despite the improvements over WEP, there are still security limitations in WPA. Because TKIP still uses the RC4 stream cipher, it is susceptible to reverse encryption for short packets with mostly known contents, such as ARP requests. This attack does not lead to full key recovery, but it does allow the attacker to send a small amount of data to the access point which will appear to be legitimate traffic [6].

Additionally, the 802.11i standard mentions that because the WPA key is generated from user-selected passphrase, using a weak phrase – such as a dictionary word less than 20 characters – is possible to be compromised by a brute force attack [6].

C. WPA2 (or RSN)

Beginning with the 802.11i standard, the IEEE describes a more robust security methodology called Robust Security Network (RSN), which is commonly called WPA2. Unlike WEP and WPA, which use fixed encryption methods, WPA2 supports dynamic negotiation of authentication and encryption methods between an access point and a wireless client. This ensures the protocol is extensible into the future as new security methodologies are developed [3]. For encryption, WPA2 implements the Advanced Encryption Standard (AES), a standard block cipher widely used in modern security applications. The 128-bit key used by AES provides much stronger security than the 40-bit key in the original version of WEP.

The following table compares the strengths and weaknesses of the security protocols. Overall, WPA2 provides the strongest protection and should be used when available.

TABLE I
COMARISON OF WIRELESS ENCRYPTION TECHNOLOGIES [3]

Feature	WEP	WPA	RSN
Encryption Cipher	RC4	RC4/TKIP	AES
Encryption Key Length	40 bits	128 bits	128 bits
Encryption Key Per Packet	Concatenated	Mixed	Not Needed
Key Management	None	802.1x	802.1x
Key Change Frequency	None	Each Packet	Not Needed
Initialization Vector Length	24 bits	48 bits	48 bits
Authentication	Weak	802.1x-EAP	802.1x-EAP
Data Integrity	CRC-32	MIC	CCM
Header Integrity	None	MIC	CCM
Reply Attack Prevention	None	IV Sequence Counter	IV Sequence Counter

III. HOME WIRELESS NETWORKS

Many modern home owners install their very own wireless network for convenience, mobility, and flexibility. In 2008, Cisco Linksys reports that around 50% of homes with internet access also had wireless networks installed [7]. However, empirical evidence suggests that many home wireless networks are not following security guidelines recommended by the router manufacturers. In fact, a significant percentage of home networks use the "out of the box" default settings shipped on the equipment. Table II, included at the end of this paper, summarizes a study by Eric Geier of security features in home and business networks [8]. (Image used with permission)

The following list describes practices that enhance security on home wireless networks. While none of the items guarantee a totally secure network, when use in conjunction they create the highest level of network security available in current technology.

As a representative example of the procedures mentioned here, screenshots of configuration on a Linksys router are included. While every hardware vendor provides a different interface into their equipment, these images provide some indication about how such a configuration change can be made. Because of the large image sizes, they are included at the end of this document instead of here in the dual column format.

a) Change router administrator passwords and user names

Most vendors use standard, well-documented user names and passwords for initial log in to the equipment. As this information is publicly available on the internet, any intruder can use these to compromise the access point unless they are changed. With access to the router administration, an intruder could reconfigure it such that only his/her equipment has access to the network. An example of changing the administrator user name and password is shown in Figure I.

b) Use encryption, preferably WPA or WPA2

Arguably, this is one of the most important settings to enhance wireless security. Without encryption, network packets are broadcast in plain text, meaning passwords and other sensitive information could be retrieved any anyone capturing the wireless traffic. As discussed earlier in the paper, WEP encryption is easily broken by publicly-available software tools given enough time listening to network traffic, so stronger methodologies such as WPA or WPA2 should be used with available. An example of enabling encryption on a router is shown in Figure III.

c) Disable SSID broadcast

The Security Set Identifier (SSID) is the unique name of a network that is displayed by network monitor tools on a client system. Routers have a feature to broadcast the name of the SSID so that any clients in the area can detect its presence. However, this also broadcasts the availability of the network to network intruders. By disabling the SSID broadcast, the network is essentially "hidden". Clients that know the name of the SSID may connect, but other clients will not detect it is present. Sophisticated attackers can use tools to determine even non-broadcasting SSIDs, but this provides an added inconvenience that

may deter attacks [9]. An example of modifying SSID settings is shown in Figure II.

d) Change default SSID name

Most routers are shipped with a default SSID name, such as "linksys." Even if the SSID is not broadcast, unauthorized users can try to connect to these default SSIDs, so changing this name prevents this kind of access. An example of modifying SSID settings is shown in Figure II.

e) Enable MAC address filtering

Many wireless routers support MAC address filtering, which allows the administrator to specify the specific Media Access Control (MAC) addresses of the equipment allowed to connect to the access point. The MAC address uniquely identifies the hardware that connects to the network. While a sophisticated intruder can manually change his or her MAC address to match allowed systems, this setting provides another level of protection against less sophisticated attacks. Examples of modifying MAC address filtering settings are showing in Figures IV and V.

f) Assign static IP addresses to devices instead of using DHCP

While the DHCP feature of wireless routers is a great convenience when machines are often added and removed from a network, it is normally unnecessary in a fixed home network environment. DHCP automatically assigns an IP address to new systems on the network, meaning intruders will also be granted an IP address. Some routers support features to disable DHCP for address assignment and accept a list of valid static IP addresses that are authorized on the network. This requires setting the IP of the client systems statically to match the router settings.

g) Position router to minimize the signal strength outside of the building

An often overlooked aspect of wireless security is the position of the router within the building. When positioned near a wall of the structure, the signal can remain at usable levels far outside of the home. Good practice for home networks is to position the device near the center of the building. If this is not practical based on the configuration of the home, the router should be as far away from the street as possible to limit the possibility of "war driving" intruders, who drive through neighborhoods in vehicles searching for wireless signals.

h) Review router logs

Wireless routers normally hold a non-volatile system log that includes information about what clients have connected or attempted to connect. Periodically reviewing these logs give the network administer insight about possible attacks against the network. For example, if there were a flurry of packets rejected because they had the wrong CRC, it might indicate an attacker is systematically modifying the CRC of a packet to determine when it will be acknowledged by the router instead of being rejected.

i) Install upgrades from manufacturer

Websites of all major wireless router vendors will provide firmware upgrades periodically. These upgrades often contain patches for security-related vulnerabilities. Exploits for equipment are often documented online, which gives intruders valuable information about how to break into an un-patched system. Downloading fixes from the vendor is a critical step to ensure these vulnerabilities do not exist on any protected systems. An example of upgrading router firmware is shown in Figure VI.

j) Enable firewalls on routers and devices

More advanced wireless routers support built in firewalls that can be configured by the router administrator. Such a firewall can provide an effective first line of defense to stop suspicious traffic coming into a home network. Additionally, as is good practice on any type of network, enabling local firewall on the client system can further protect against malicious access.

k) Periodically change passphrases used to generate encryption keys

When using encryption protocols such as WEP and WPA, router administrators are prompted to enter a passphrase used to generate the private keys for encryption. Often these are set once and never changes. Like any password, it is good security

practice to periodically change these strings. Strong password rules - such as using upper case, lower case, numbers, and symbols - help protect against brute force attacks. Because of the relative ease with which WEP systems can be compromised, passphrase string longer than 20 characters are recommended [10].

l) Disable during extended periods of non-use

Most home wireless networks are left constantly enabled. When the users are away from the home for an extended period of time – such as for vacation or business trips – disabling the wireless router guarantees there can be no unauthorized access through wireless protocols.

IV. PUBLIC WIRELESS NETWORKS

It is common for businesses like restaurants and coffee shops to provide free wireless access to their patrons. These "hotspots" encourage customers to frequent the establishment by offering this service free of charge. As a matter of convenience, free hotspots are predominantly open access networks, meaning there is no data encryption or authentication of users. This prevents the need for each user to obtain a key or password from the business. While convenient, this dictates that network packets are transmitted unencrypted. Because malicious users have access to these networks and public areas too, unencrypted sensitive data may be collected by them if they choose to capture it. Furthermore, these networks can serve as a bridge between malicious user computers and target computers; data can be extracted from victims' computers if appropriate security measures are not enabled [5].

The list below describes best practices for security when connecting to an unsecured public wireless network. While none of these things entirely remove the risk inherent to networking, they can provide a high-level of confidence that confidentiality, integrity, and availability are maintained.

a) Disable auto-connection to open networks

Some operating systems have features to automatically connect when an open wireless network is detected. While this may serve a convenience for the user, it also exposes the system to a risk from connecting to rogue networks with the strongest signal in the area. Hackers may place their own hotspots in public places and spoof the name of a legitimate access point, such as "Starbucks" or "Hotel Wireless" with the intent of luring unsuspecting users onto their network and capturing passwords or other sensitive data. By disabling the auto-connection feature requires the user to choose and verify that they are connecting to the network they expect.

b) Enable a local firewall

Firewall software, often built into the operating system, can effectively block incoming access from undesirable sources or to unnecessary network ports. Enabling a firewall ensures some level of filtering of incoming traffic to the system, and protects everything on the system from being openly access to networked computers. It is important to check the firewall rules to ensure they provide the highest level of protection. For example, ports may be left open when on corporate networks, but at a public hotspot, all unnecessary ports should be closed. An example of enabling the firewall on Windows is shown in Figure VII.

c) Disable file sharing

File sharing services built into operating systems allow for easy sharing of data with other users on a network. While a convenient feature in a home or workplace, this feature is dangerous in public hotspots, as it could allow malicious users access to files on your system, and therefore should be disabled on open wireless networks. In Microsoft Windows, file sharing can be disabled quickly through the firewall configuration. By default, the Windows Firewall allows an exception for file sharing, so before connecting to a public hotspot, this firewall exception should be disabled. An example of how file sharing can be disabled in Windows is shown in Figure VIII.

d) Use only trusted and encrypted connections when exchanging sensitive data

While open networks do not encrypt transmissions at the link layer, there are other methods available that encrypt transmissions at higher layers. HTTPS –

which is HTTP using TLS or SSL - is an example of an application layer solution to transporting sensitive data. Any reputable bank or financial institution website will support HTTPS to protect transmitted data. HTTPS performs two functions important in this environment, authentication and encryption. Authenticating the source of the website using a legitimate Certificate Authority ensures the site has not been subverted by an illegitimate site. Encrypting the data is the most important feature on an unsecured wireless network, as it ensures sensitive data is not transmitted in clear text when it is sent to and from the website.

Likewise, SSL technologies have been incorporated into other protocols. For instance, SSH is an encrypted replacement for Telnet console connections, and SFTP encrypts file transfer data. Before sending sensitive data on an open network, the user should verify that one of these tools is being used at a higher layer.

e) Connect to a secure Virtual Private Network

VPNs provide a level of authentication and confidentiality on even unsafe networks by tunneling into a secure network and encrypting all transmissions between the two locations. When a user is connected to a VPN, even unsecure services such as HTTP are protected through the encapsulation provided by the VPN. If the endpoint of the VPN is a safe and secure network, the user can be confident that essentially the same level of protection is provided for the services run on this remote network.

f) Only connect to access points from a known provider

Because hackers may install their own access points and with names that seem legitimate, it is important to double check with an establishment before connecting to their network. For example, if a client system detects two networks, one called "Coffee Shop" and one called "Coffee Cafe", it is important to check with the establishment to determine which network is legitimate.

g) Encrypt sensitive files

Operating systems, and publicly-available software, provide methods for encrypting file system directories or files. Manually encrypting sensitive files adds a layer of protection in the event that an intruder gains access to them. Even if files are removed from a system, the illegitimate user will be unable to open them if appropriate levels of encryption are used to protect them.

h) Remove sensitive files from you system altogether

For highly sensitive data, the only guaranteed method to prevent it from being accessed is removing it from the computer altogether. Most companies provide corporate network data storage for such files, and they can be saved in this location before a laptop connects to a public, and potentially dangerous, network.

V. CONCLUSION

Wireless networking is inherently risky. However, in the modern era of laptops, 802.11-enabled phones, and PDAs, wireless networks are a technological staple. Security measures do exist to provide secure wireless communications. In home environments, this requires configuring the wireless router to enable a strong set of security features. In public network environments, this requires enabling local security measures on client machines and encrypting transmissions using higher-layer technologies. With the proper safeguards in place, users can maintain a reasonable level of confidence in their security on wireless networks.

VI. REFERENCES

[1] I. Woon, G. Tan, and R. Low, "A Protection Motivation Theory Approach to Home Wireless Security," *Proceedings of the International Conference on Information Systems*, ICIS, 2005.

[2] B. Bulbul, I Batmaz, and M. Ozel, "Wireless Network Security: Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) Security Protocols," *Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop*, ICST, Brussels, Belgium, Belgium, 2008.

[3] T. Karygiannis and L. Owens, "Wireless Network Security: 802.11, Bluetooth and Handheld Devices," *Special Publication 800-48*, National Institute of Standards and Technology, 2002.

[4] A. Loo. “The Myths and Truths of Wireless Security,” *Communications of the ACM 51*, 2 (Feb. 2008), 66-71.

[5] B. Potter, “Wireless Hotspots: Petri Dish of Wireless Security,” *Communications of the ACM 49*, 6 (June 2006), 50-56.

[6] M. Beck, and E. Tews, “Practical Attacks against WEP and WPA,” *http://dl.aircrack-ng.org/breakingwepandwpa.pdf*, 2008.

[7] B. Reese “Cisco Linksys’ revenue challenged by slow shift to 802.11n,” *http://www.networkworld.com/community/node/24788*, 2008.

[8] E. Geier. “A War Driving Experience – Part 1: The Results,” *http://www.egeier.com/publications/A_War_Driving_Experience_Part_I_The_Results.htm*, 2002.

[9] K. Karagiannis, “Ten Steps to a Secure Wireless Network,” *www.pcmag.com/article2/0,2817,842886,00.asp*, 2003.

[10] Z. Yang, A. Champion, B. Gu, X. Bai, and D. Xuan, “Link-Layer Protection in 802.11i WLANs with Dummy Authentication,” *WiSec ‘09*, ACM, 2009, pp 131-138.

TABLE II
RESULTS OF WIRELESS SECURITY STUDY BY ERIC GEIER [8]

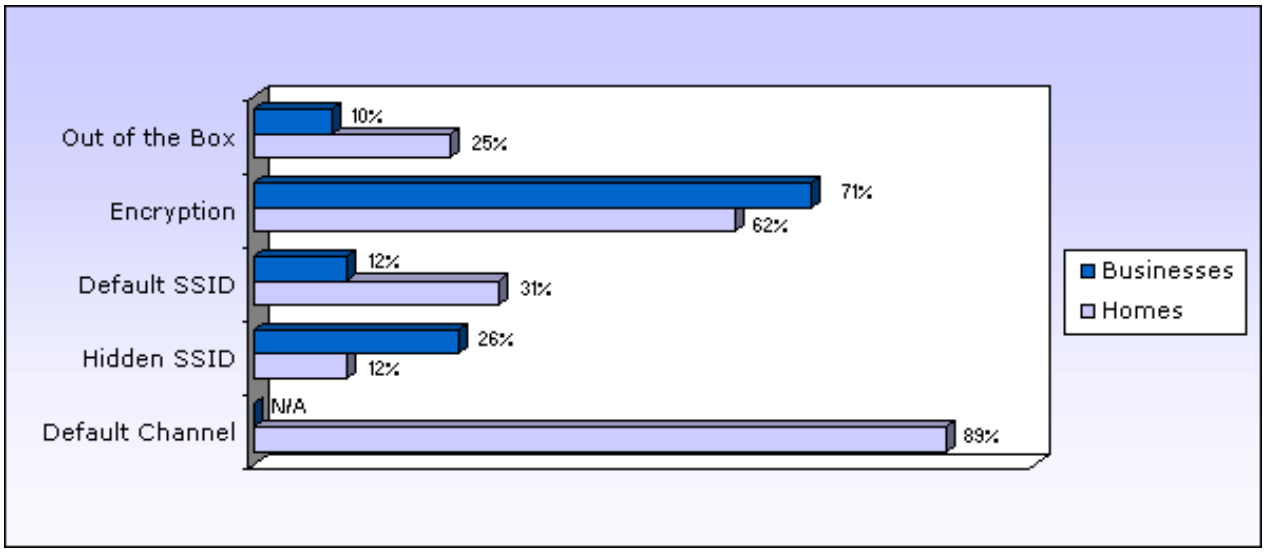

FIGURE I
LINKSYS ROUTER – MODIFY ADMINISTRATIVE PERMISSIONS

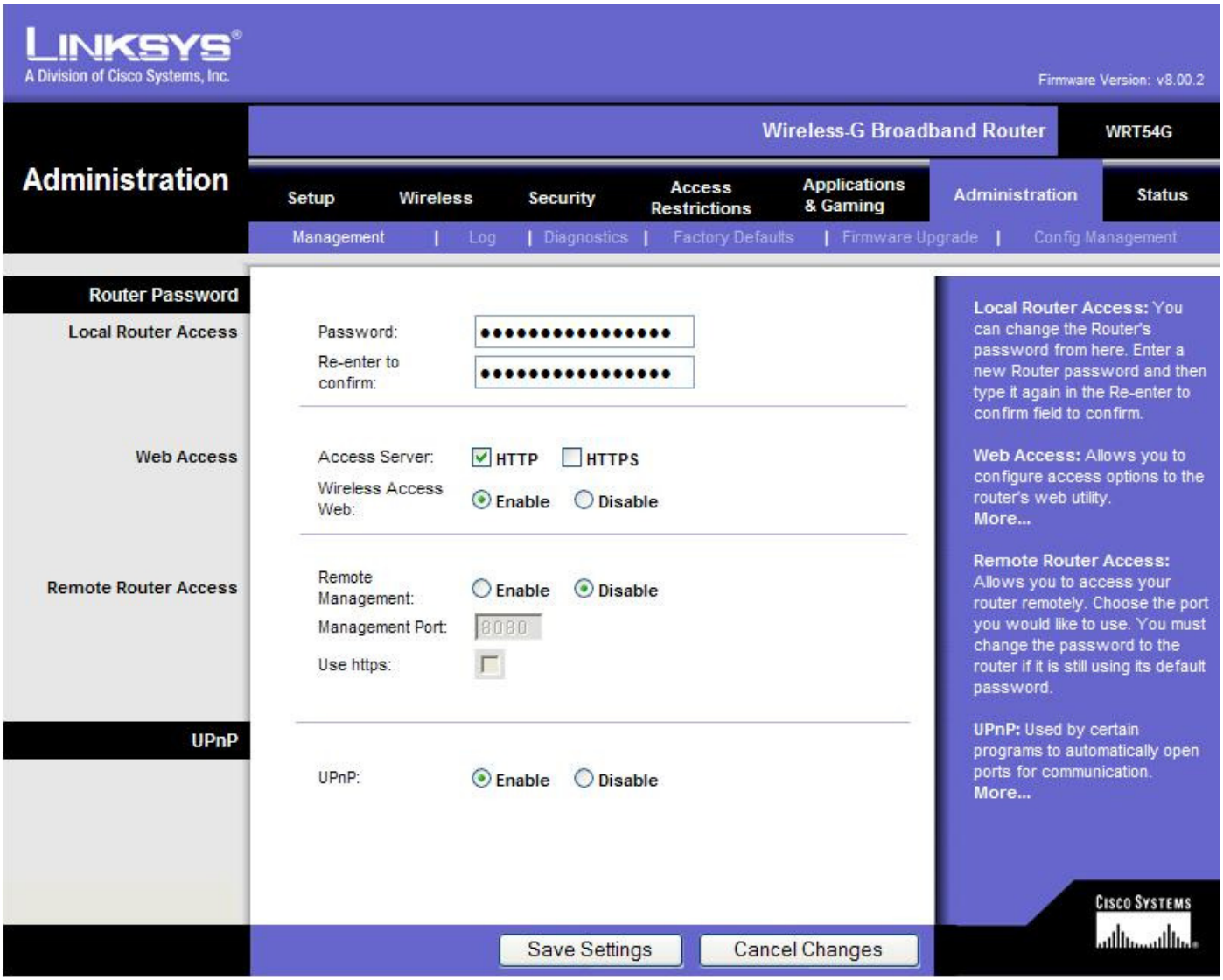

FIGURE II
LINKSYS ROUTER – SSID FEATURES

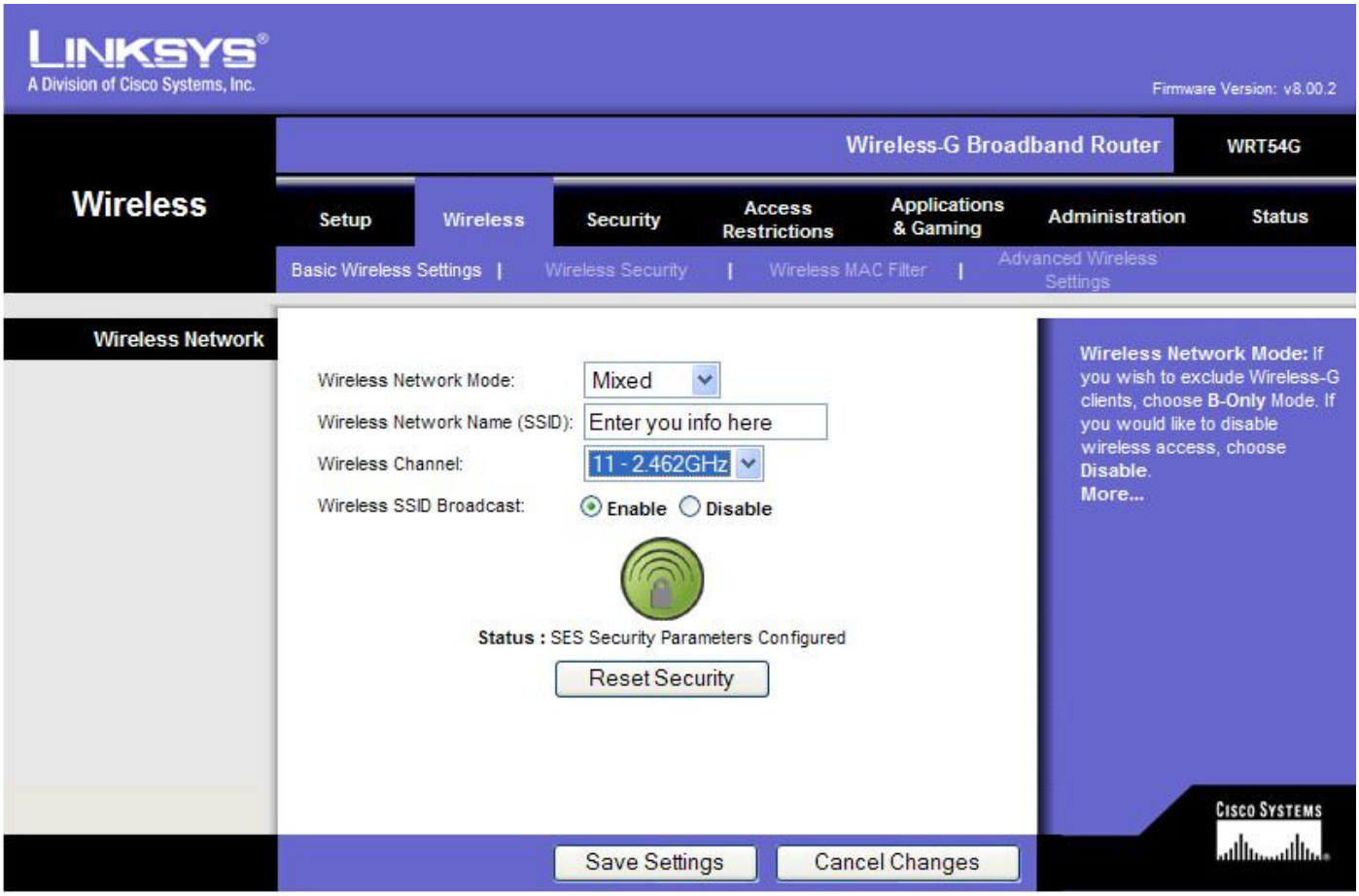

FIGURE III
LINKSYS ROUTER – ENABLE ENCRYPTION

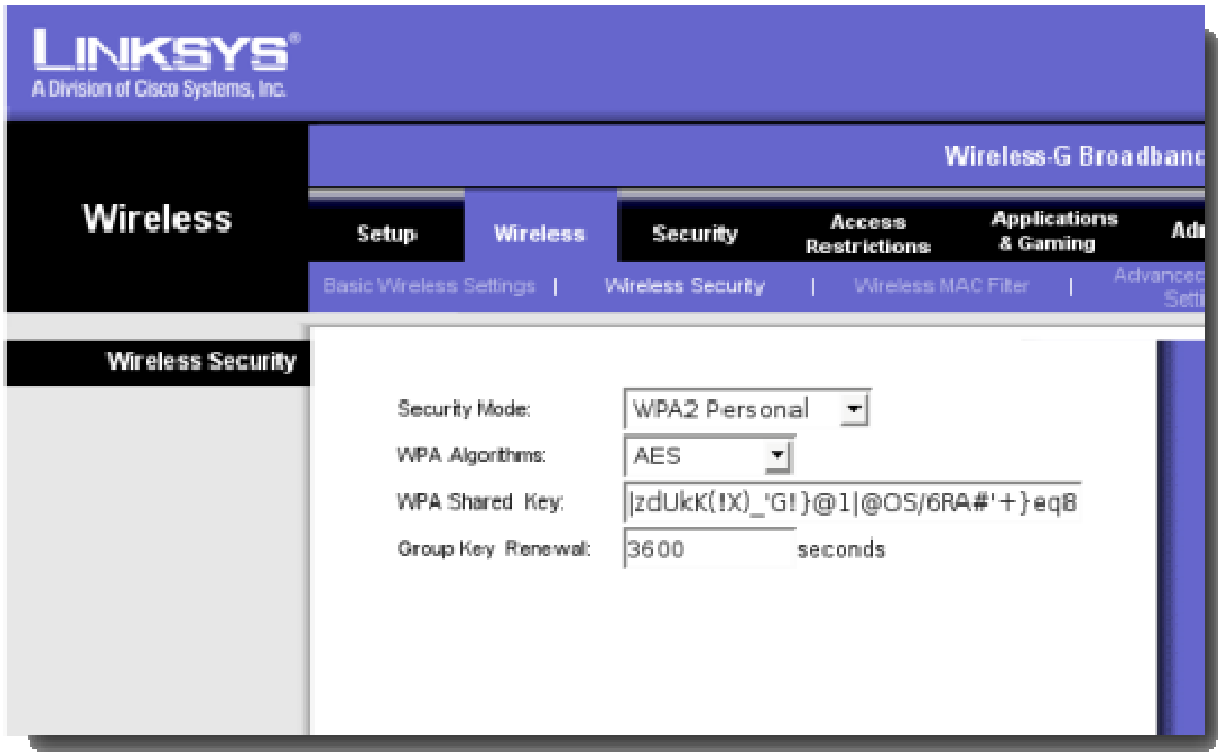

FIGURE IV
LINKSYS ROUTER – ENABLING MAC ADDRESS FILTERING

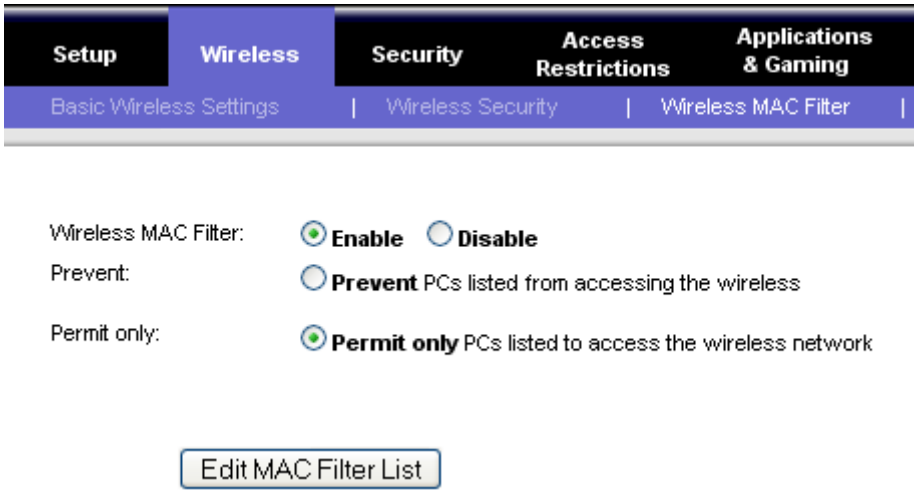

FIGURE V
LINKSYS ROUTER – MAC ADDRESS FILTERING

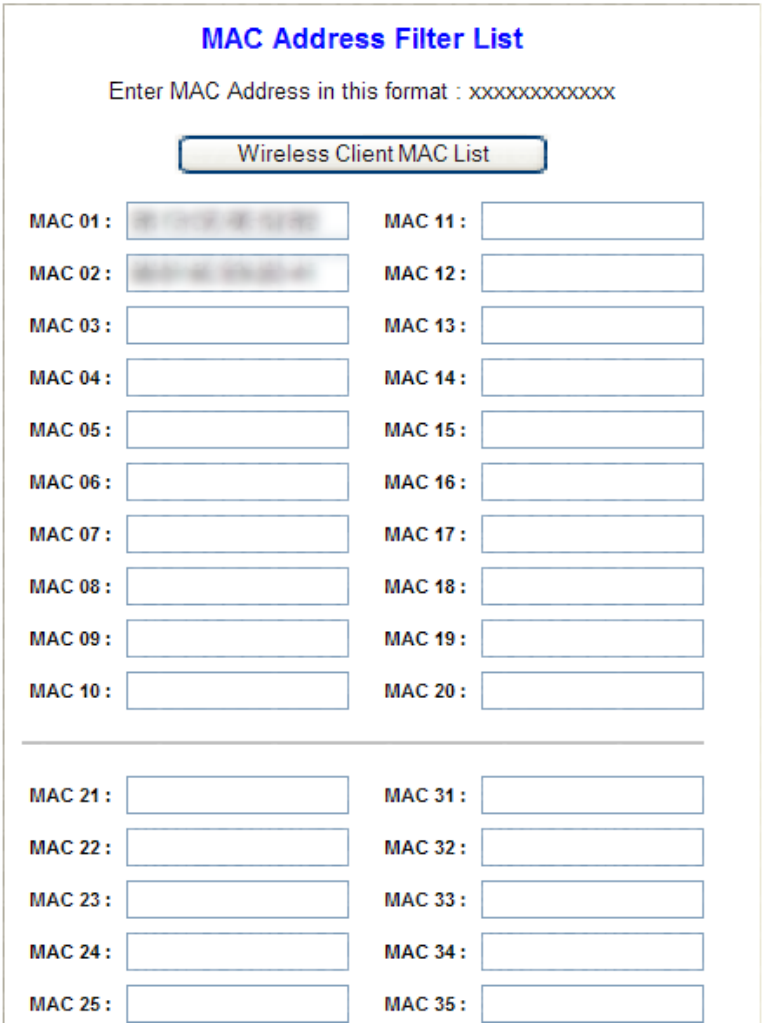

FIGURE VI
LINKSYS ROUTER – UPGRADING FIRMWARE

FIGURE VII
WINDOWS - ENABLING FIREWALL

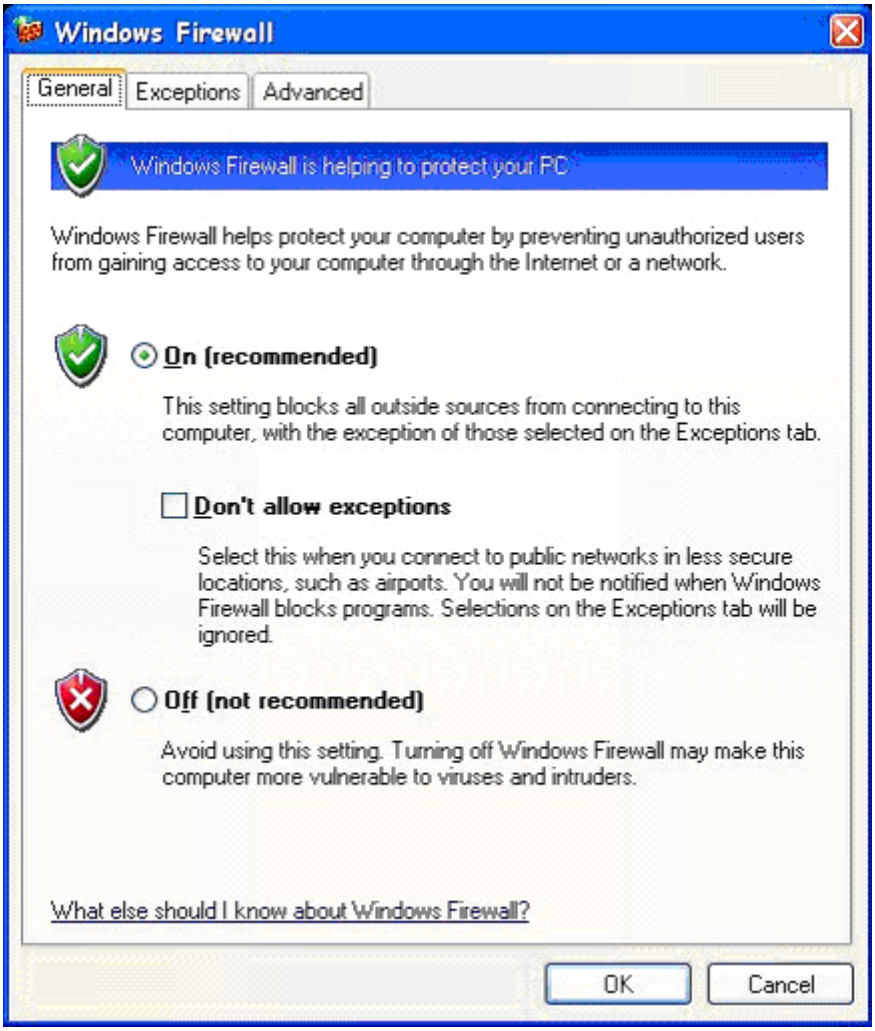

FIGURE VIII
WINDOWS – DISABLING FILE SHARING