WPA SECURITY
(Wi-Fi Protected Access)

Presentation

By

Douglas Cheathem
(csc 650.01 Spring 2007)

OUTLINE

- Introduction
- Security Risk
- Vulnerabilities
- Prevention
- Conclusion
- Live Demo
- Q & A

INTRODUCTION

- WPA is a standard security feature found on all Wi-Fi wireless devices which provides robust encryption and authentication techniques.
- Implementing network security is something that no one really likes to do. It's a chore that must be done if you want your data to be safe and secure from hackers.
- It takes time and effort, and can cost an organization more $$$ to implement later or correct if it is not considered during implementation.

WHY WIRELESS

- Mobility and Freedom (Work Anywhere)
- No restrictions of wires or fixed connection
- Quick, Effortless Installation
- No cables to buy $$$
- Save cabling time and hassle
- Easy to expand

WIRELESS COMMUNICATIONS

- The current proliferation of wireless technology has provided end users with a false since of security. And it is being widely adopted by many home users and small businesses.

- You might be wondering why? Well a large majority of businesses and individuals are using this technology for home networking. And they are connecting their home pc's to corporate networks. And many of them are unsecured, it was estimated at about 70% in 2006.

- (What? ☹ Yes, unsecured, which means their connection is the weakest link.) And your network is open for attack.

Wi-Fi Alliance

The WPA and WPA2 standards were created by the Wi-Fi Alliance industry group that promotes interoperability and security for the wireless LAN industry.

Wi-Fi was created in early 2003, to address the many flaws found in WEP, and to provide a greater amount of security for wireless network connections.

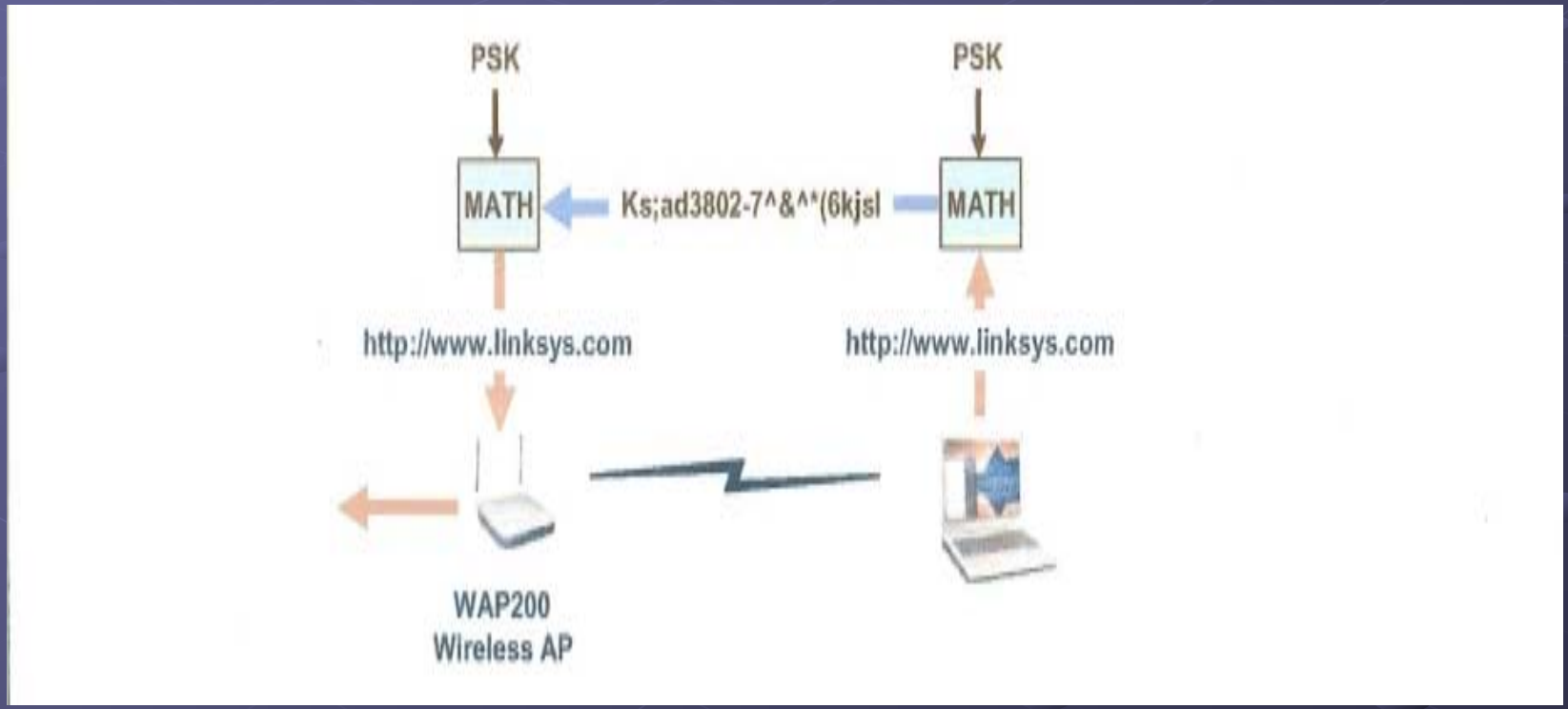
WHAT IS WPA ?
(CONT.)

- WPA is a standard security feature found on all Wi-Fi wireless devices which provides robust encryption and authentication techniques.

- Encryption translates data into a secret code to insure data is secure.

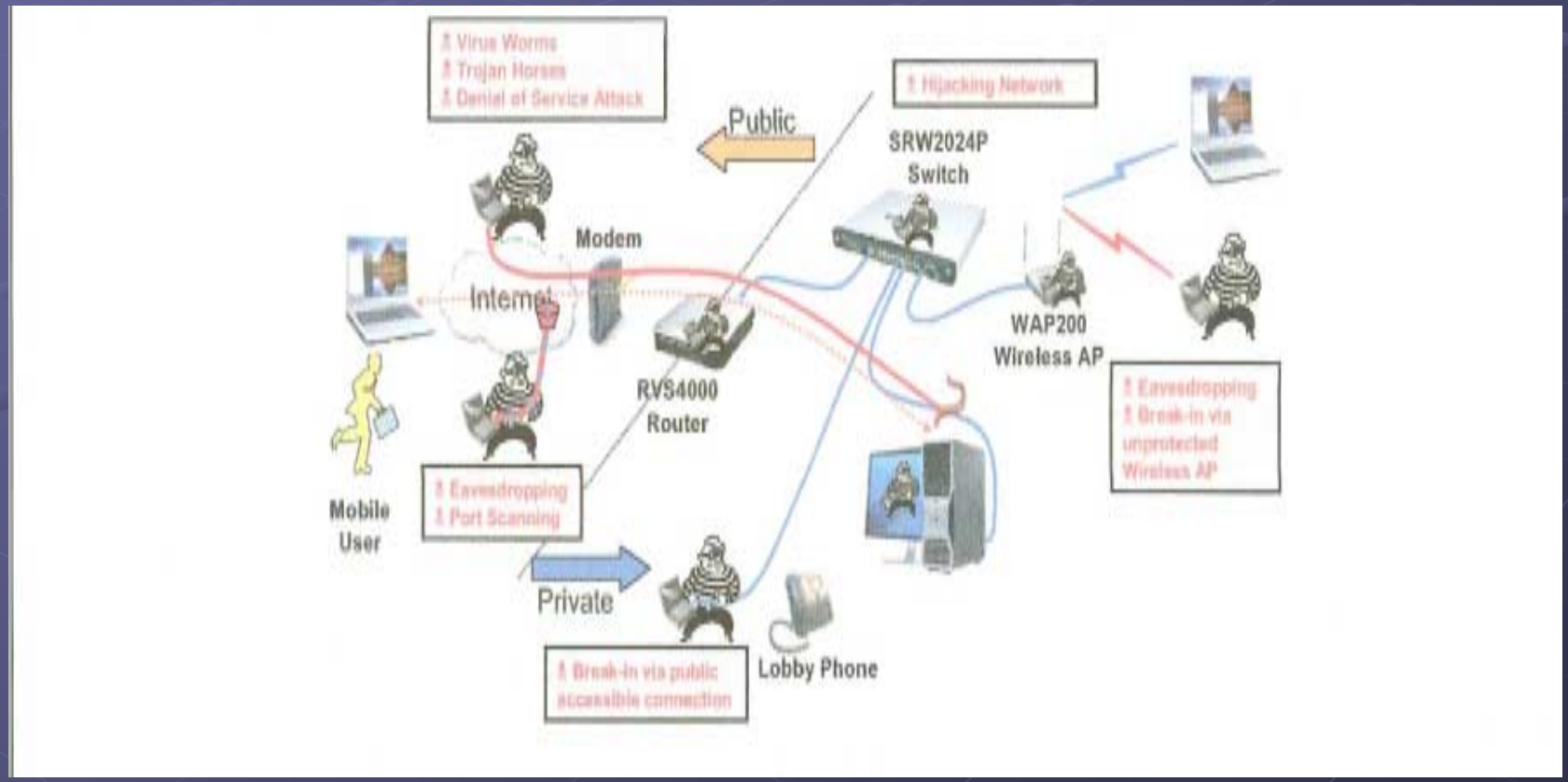
WHAT IS WPA ?
(Wi-Fi Protected Access)

When WPA is activated, each user on your network will be assigned a unique secret key which is used to translate the encrypted data.



SECURITY RISK

- Hackers, Worms, Dos, and Trojan Attacks



WIRELESS PIT FALLS

- Users have encryption turned off
- SSID - Broadcasted by Router
- Users choose WEP 64/128 for encryption
- Phase-key Length not unique / too short

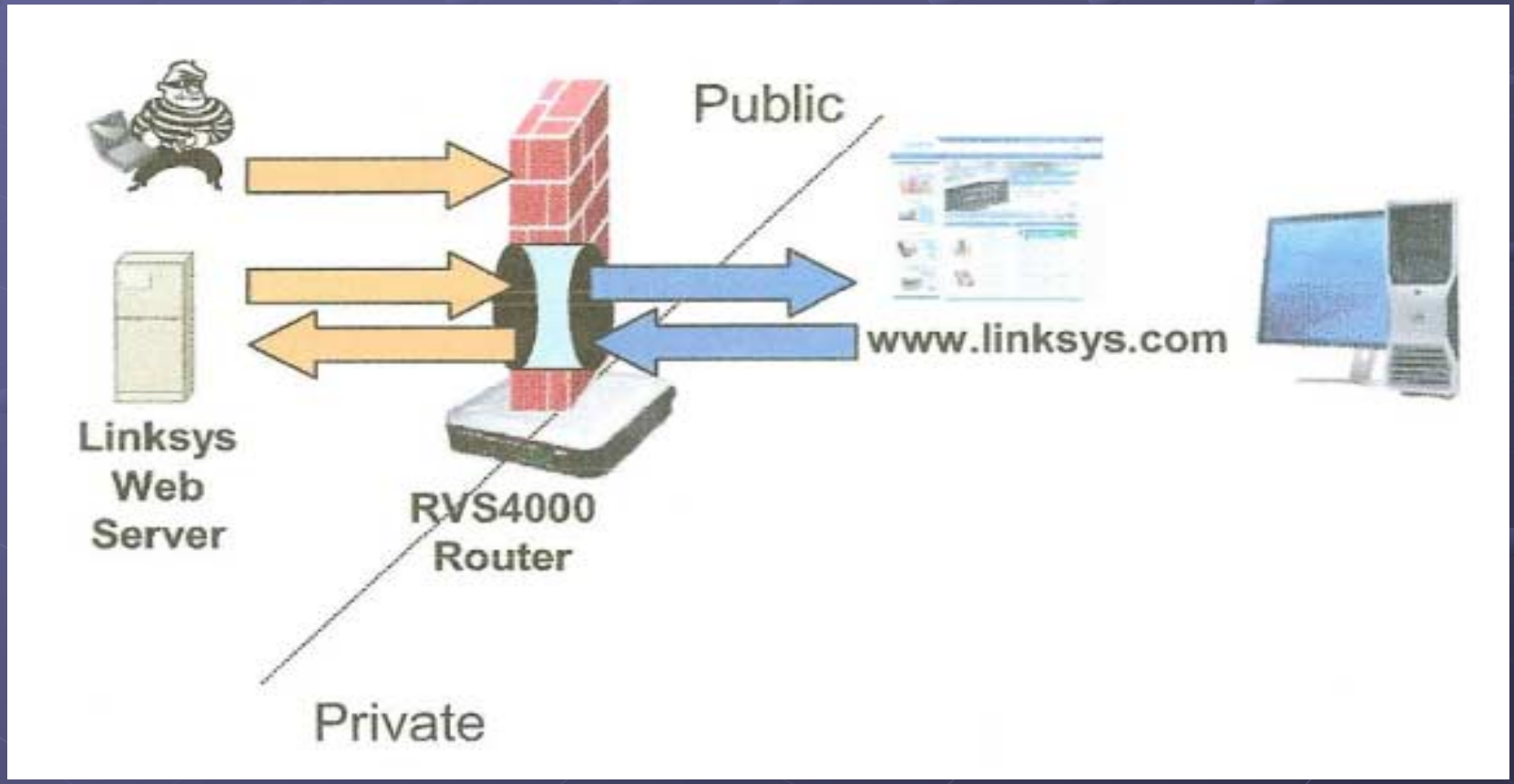
HOME SECURITY

- No Encryption (system open to attack)
- WEP 64/128 (wired equivalent privacy)
  (Crackable)
- WPA (Wi-Fi protect access) (Secure Using)
  - TKIP (Temporal Key Integrity Protocol)
  - AES (Advanced Encryption Standard)
  - EAP (Extensible Authentication Protocol)
- VPN (virtual private network) (Secure)

SECURITY THREATS

- Hackers
- Worms
- Dos Attacks
- Trojans
- AirSnort
- WepCrack
- WepAttack
- Brute Force

THREAT PREVENTION



SECURITY USING WPA

Since WPA uses dynamic key encryption, the key is constantly changing, making intrusion into your wireless network nearly impossible.

WPA is considered one of the highest levels of wireless security for your network, and is significantly more secure than WEP.

Within WPA, there are four types of encryption methodologies each utilizing different processes for authentication:

- WEP (Basic Encryption)
- WPA (Personal)
- WPA2 (Enterprise)
- EAP (RADIUS)

WPA ENCRYPTION

Used by Primarily by Home Uses:
AND USES TWO TYPES OF ENCRYPTION

- WEP

Encrypts the data on your network so that only the intended recipient is able to access it. 64-bit and 128-bit encryptions are two levels of WEP security. WEP encodes your data using an encryption "key" before sending it out into the air. The longer the key is, the stronger the encryption will be.

Any receiving device must know the same key to decrypt the data. Keys are entered as strings of 10 or 26 hexadecimal digits. To simplify creating and entering the keys, most products include a "Passphrase" feature. An easy-to-remember word or phrase is entered, and an algorithm generates the hexadecimal digit keys for you.

Since the security key that WEP uses is static, or does not change, it is still possible for a motivated intruder to break into your network with enough time and effort. Thus, it is a good idea to frequently change the WEP key. At most, WEP will prevent accidental unauthorized use.

WPA ENCRYPTION

Used Primarily By Home Users:
AND USES TWO TYPES OF ALGORITHMS

- TKIP

Temporal Key Integrity Protocol (TKIP) is a type of mechanism used to create dynamic key encryption and mutual authentication.

TKIP provides the security features that fix the limitations of WEP. Since the keys are always changing, it provides a very high level of security for your network.

- AES 128

AES stand for **A**dvanced **E**ncryption **S**tandard. **128** means 128-bit encryption key. AES is a very popular encryption algorithm. It is fast and secure. 128-bit key means that there are 2128 key combinations. i.e. 3.4 x 1038 combinations. It is a very powerful encryption algorithm.

EPA ENCRYPTION

- **EAP / RADIUS (Used Primarily by Business/Enterprise)**

  Extensible Authentication Protocol (EAP) is used for message exchange during the authentication process.

  It utilizes 802.1x Server Technology to authenticate users via a RADIUS server (Remote Authentication Dial-In User Service).

  This provides industrial strength security for your network, but requires a RADIUS server.

VPN ENCRYPTION

- VPN

  VPN's are used to secure the actual transmission of information from one specific place to another specific place over the Internet. The idea is to secure the data when it is in a public place (the Internet) where hackers or anyone else could access it, but is generally left unencrypted while it is in a private network under your control (the corporate network at your office).

  With the proper login and VPN software installed, only authorized users can access the corporate network through the Internet and any data that is exchanged cannot be intercepted.

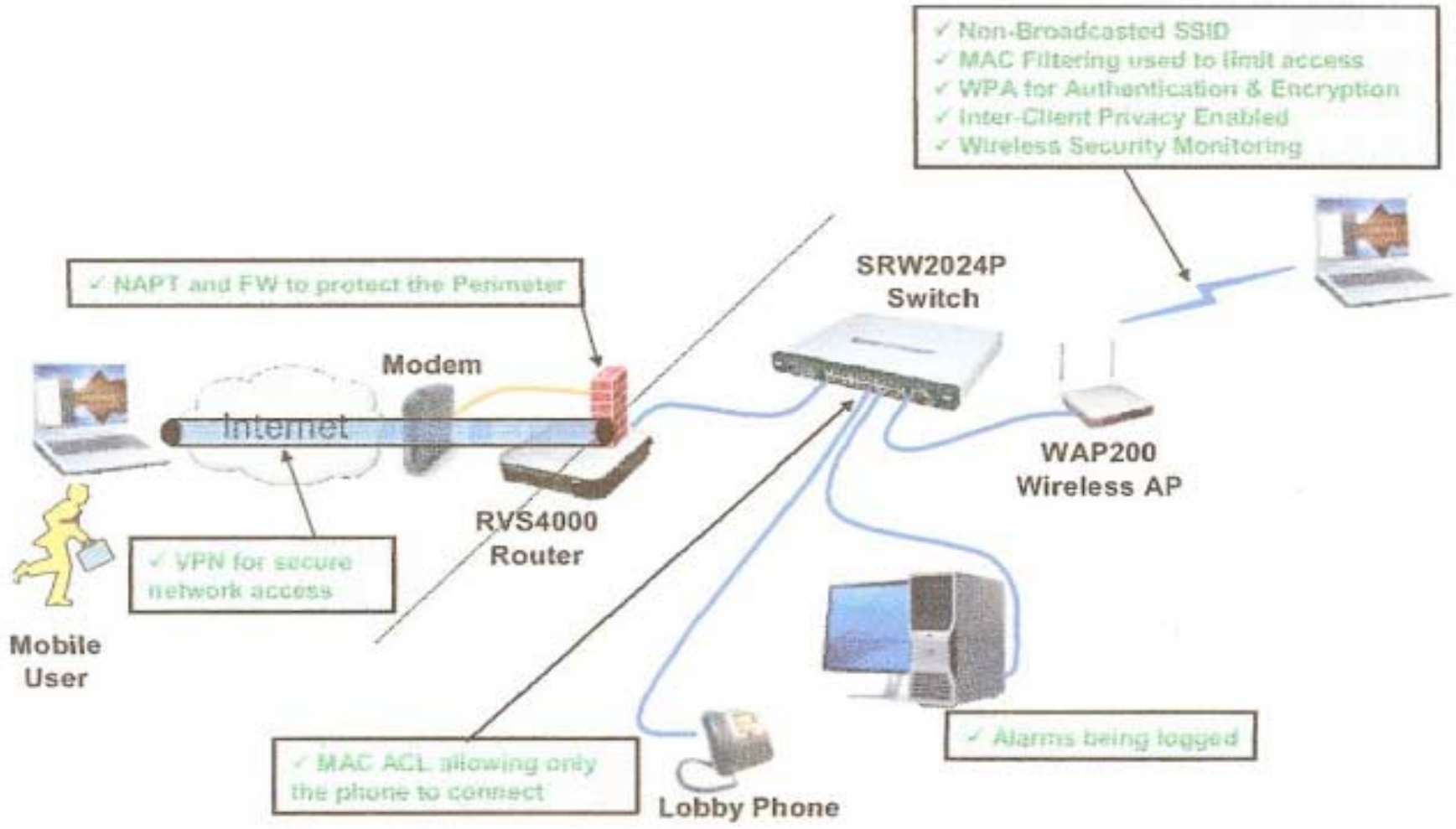
MAC ADDRESS FILTERING

- Mac Address Filter

  The MAC address is a unique series of numbers and letters assigned to every networking device. With MAC address filtering enabled, wireless network access is provided solely for wireless devices with specific MAC addresses.

  For example, you can specify only the computers in your house to access your wireless network. It would be very difficult for a hacker to access your network using a random MAC address.

CONCLUSION


✓ Non-Broadcasted SSID
✓ MAC Filtering used to limit access
✓ WPA for Authentication & Encryption
✓ Inter-Client Privacy Enabled
✓ Wireless Security Monitoring
✓ NAPT and FW to protect the Perimeter
SRW2024P
Switch
Modem
Internet
RVS4000
Router
WAP200
Wireless AP
✓ VPN for secure network access
Mobile
User
✓ MAC ACL allowing only the phone to connect
Lobby Phone
✓ Alarms being logged

WHY IS WPA SECURITY IMPORTANT ?

- ✓ Network security is extremely important, especially for applications or programs that keep your valuable information. If not configured on your wireless network, you are leaving yourself wide open to the interception of emails and examination of your private files.
- ✓ You are allowing unknown intruders to use your network and Internet connection to distribute their own communications.
- ✓ The enhanced security you receive with WPA increases your level of data protection and assists in the avoidance of viral invasions and unauthorized access or destruction of your personal information.
- ✓ It is strongly recommended that you use the highest level of security on your networking device, which is either WPA or WPA2.

WIRELESS PROTOCOLS DEFINITIONS

- 802.11a - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps and an operating frequency of 5GHz.
- 802.11b - An IEEE wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.
- 802.11g - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.
- 802.11n - The next generation of high-speed wireless networking, capable of delivering the range and capacity to support today's most bandwidth-hungry applications like streaming high definition video, voice, and music. Wireless N is based on MIMO (Multiple Input, Multiple Output) technology, which uses multiple radios to transmit multiple streams of data over multiple channels.

REFERENCES

- Wi-Fi Alliance - Site: http://www.wi-fi.com
- Linksys - Site: http://www.linksys.com
- Linksys - White Papers: EDCS-580528 V1.0
- Wi-Foo - Book: Secrets of Wireless Hacking by:
  Andrew A. Vladimirov
  Konstantin V. Gavrilenko
  Andrei A. Mikhailovsky

LIVE DEMO

Q & A