Wi-Fi

security threats

Contents

INTRODUCTION ABOUT WI-FI

Things You have to know about Wi-Fi

- Wi-Fi describes the embedded technology of wireless local area networks (WLAN) based on the IEEE 802.11 specifications
- It uses radio instead of wires to transmit data back and forth between computers
- Wi-Fi networks use radio technologies called IEEE 802.11a, 802.11b or 802.11g to provide secure, reliable, fast wireless connectivity

Comparison of WLAN Standards [1]

Protocol	Release Date	Op. Frequency	Data Rate (Typ)	Data Rate (Max)	Range (Indoor)	Range (Outdoor)
Legacy	1997	2.4-2.5 GHz	1 Mb/s	2 Mb/s	?	?
802.11a	1999	5.15-5.35/5.47-5.725/5.725-5.875 GHz	25 Mb/s	54 Mb/s	~25 meters	~75 meters
802.11b	1999	2.4-2.5 GHz	5.5 Mb/s	11 Mb/s	~35 meters	~100 meters
802.11g	2003	2.4-2.5 GHz	25 Mb/s	54 Mb/s	~25 meters	~75 meters
802.11n	2007 (unapproved draft)	2.4 GHz or 5 GHz bands	200 Mb/s	540 Mb/s	~50 meters	~126 meters

http://en.wikipedia.org/wiki/802.11

Comparison of WLAN Standards [2]

Characteristic	Bluetooth	802.11	802.11b	802.11a	HiperLAN/1	HiperLAN/2
Connections	PTMP	PTP*	PTP*	PTP*	PTMP	PTMP
Frequency Selection	FHSS	FHSS DSSS	DSSS	OFDM	OFDM	48 subcarrier OFDM
Authentication	Yes	No	No	No	Address	Address
Fixed Networks	Any	Ethernet	Ethernet	Ethernet	Ethernet, ATM, FireWire	Ethernet, ATM, FireWire, UMTS
Encryption	40-bit RC4	40-bit RC4	40-bit RC4	40-bit RC4	DES	DES, 3DES

* - up to 3 channels of audio supported

http://www.btdesigner.com/pdfs/KenNoblittComparison.pdf

Comparison of WLAN Standards [3]

	802.11b	802.11a	802.11g
Pros	lowest cost	fastest maximum speed	fastest maximum speed
	signal range is best and is not easily obstructed	supports more simulatenous users	supports more simulatenous users
		regulated frequencies prevent signal interference from other devices	signal range is best and is not easily obstructed
Cons	slowest maximum speed	highest cost	costs more than 802.11b
	supports fewer simultaneous users	shorter range signal that is more easily obstructed	appliances may interfere on the unregulated signal frequency
	appliances may interfere on the unregulated frequency band		

ADVANTAGES AND DISADVANTAGES OF WI-FI

Use of wi-fi [1]

Wi-Fi at home:

- Via a broadband Internet connection into a single router which can serve both wired and wireless clients
- Ad-hoc mode for client to client connections
- Built into non-computer devices to enable wireless connectivity to other devices or the Internet

Use of wi-fi [2]

Wi-Fi in Gaming:

- Gaming consoles and handhelds make use of Wi-Fi technology to enhance the gaming experience. Examples include:
  - The Nintendo DS
  - The PlayStation Portable
  - The Xbox 360 can be made Wi-Fi compatible if the user purchases a separate wireless adapter
  - The Wii

Use of wi-fi [3]

Wi-Fi in business:

- Widespread Coverage: allows an employee to take a laptop from an office to the conference room without losing network connectivity
- Offsite Access: Employees who are traveling to meet with clients can have access to company resources and email wherever they are
- Increased efficiency: Improved data communications lead to faster transfer of information within businesses and between partners and customers

Use of wi-fi [4]

Wi-Fi in business:

- Increasing number of Wi-Fi Access Points, in order to provide redundancy and smaller cells
- Wireless voice applications (VoWLAN or WVOIP)
- Moving toward 'thin' Access Points, with all of the intelligence housed in a centralized network appliance
- Outdoor applications utilizing true mesh topologies
- A proactive, self-managed network that functions as a security gateway, firewall, DHCP server, intrusion detection system

Use of wi-fi [5]

Wi-Fi at Hotspots:

- The most publically visible use of Wi-Fi is at hotspots. These trends include:
  - Free Wi-Fi at venues
  - Paid Wi-Fi at venues

Advantages of wi-fi [1]

- Allows LANs to be deployed without cabling
- Reduces the costs of network deployment and expansion
- Spaces where cables cannot be run, such as outdoor areas and historical buildings, can host wireless LANs

Advantages of wi-fi [2]

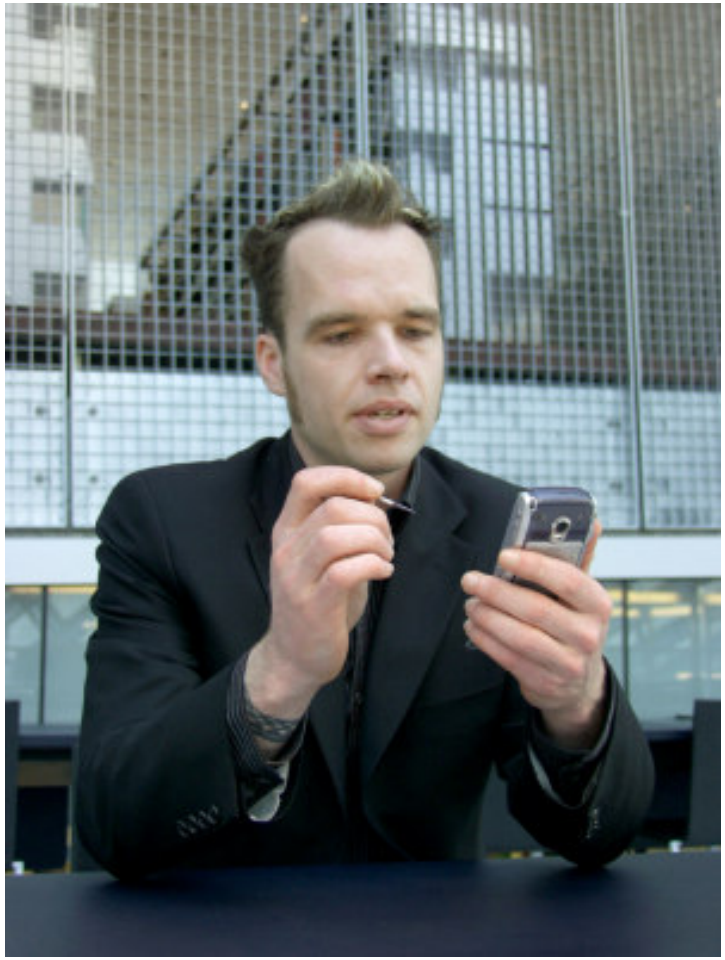
- Built into most modern laptops, budget laptops usually the exception
- Wi-Fi chipset pricing continues to come down, making Wi-Fi a very economical networking option and driving inclusion of Wi-Fi in an ever-widening array of devices

Advantages of wi-fi [3]

- Wi-Fi products are widely available in the market
- Different brands of access points and client network interfaces are interoperable at a basic level of service
- Products designated as Wi-Fi CERTIFIED by the Wi-Fi Alliance are interoperable and include WPA2 security

Advantages of wi-fi [4]

- Wi-Fi is a global set of standards. Unlike cellular carriers, the same Wi-Fi client works in different countries around the world
- Widely available in more than 250,000 public hot spots and millions of homes and corporate and university campuses worldwide



Advantages of wi-fi [5]

- As of 2006, WPA and WPA2 encryption are not easily crackable if strong passwords are used
- New protocols for Quality of Service (WMM) and power saving mechanisms (WMM Power Save) make Wi-Fi even more suitable for latency-sensitive applications (such as voice and video) and small form-factor

Advantages of wi-fi [6]

- Share a high-speed Internet connection between multiple PCs and to tap into that connection from various rooms using their laptop(s)
- Share a high-speed Internet connection with printer, scanner and other peripherals
- Send files between multiple computers

Wi-Fi Disadvantages [1]

Security:

- This is the most important potential problem with a wireless network
- Before installing a wireless network you must have a security plan in place. An unsecured network is an open door to your confidential business information

Wi-Fi Disadvantages [2]

Security:

- The most common wireless encryption standard, Wired Equivalent Privacy or WEP, has been shown to be breakable even when correctly configured
- Wi-Fi Protected Access (WPA and WPA2) which began shipping in 2003 aims to solve this problem and is now generally available

Wi-Fi Disadvantages [3]

Range:

- The wireless signal extends several hundred feet from the base station, but this range is greatly curtailed by obstructions and interference
- In an office environment, interior walls will likely limit the range to less than 100 feet, and an exterior wall may block the signal completely
- In a large office, this will require multiple base stations laid out to cover the entire office

Wi-Fi Disadvantages [4]

Interference:

- Some electronic equipment can interfere with radio waves and disrupt your Wi-Fi network
- The biggest problems come from microwaves and cell phones

VULNERABILITIES AND ATTACK METHODS

Security [1]

- Security takes three forms:
  - Physical
  - Virtual
  - Data

- For the wireless domain, we don't think of physical security, we consider the next form, virtual security

Security [2]

- Virtual security is the ability to keep data secure when access is possible without physical access
- Data security is protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure

Security threats

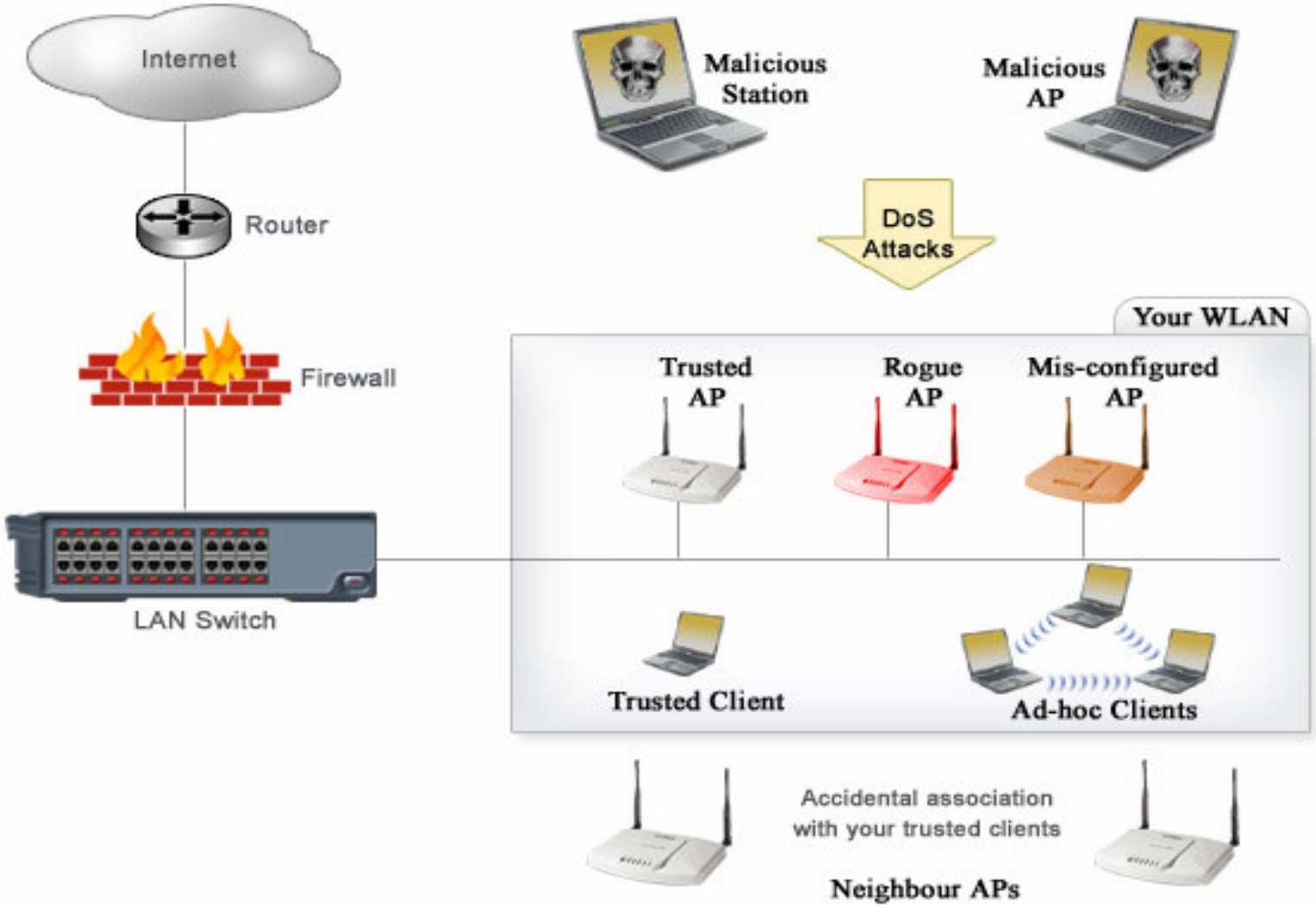
- Wireless networks add an extra level of security complexity compared to wired networks
- Whereas wired networks send electrical signals or pulses of light through cable, wireless radio signals propagate through the air and are naturally easier to intercept

Wi-fi dangers [1]

- Anyone can try to break into a network broadcasting a signal
- Many networks offer WEP - Wired Equivalent Privacy - security systems which have been found to be vulnerable to intrusion
- Though WEP does block some intruders, the security problems have caused some businesses to stick with wired networks until security can be improved

Rogue Access Points

- A rogue access point is any untrusted or unknown access point running in your WLAN



Employee Installed Rogue Access Points

- Some employees plug cheap Small Office Home Office (SOHO) grade access points to corporate LAN
- Visitors inside your building and hackers outside your building can connect to such unauthorized APs
  - steal bandwidth
  - send objectionable content to others
  - retrieve confidential data
  - attack company assets
  - use your network to attack others

Mis-Configured Rogue Access Points

- Sometimes an authorized access point could suddenly turn into a rogue device due to a minor configuration flaw
- If an AP doesn’t validate the client properly due to a configuration flaw, an attacker can:
  - send lot of such authentication requests
  - overflow the AP’s client-association-table
  - make it reject access to other clients including the legitimate ones

Rogue Access Points From Neighbor WLANs

- 802.11 clients automatically choose the best available AP nearby and connect with them
- Due to this behavior, authorized clients of one organization can connect to Access points from the neighbouring organization, so exposing sensitive data

Rogue Access Point That Dont Adher To Corporate Policies

- Enterprises can set polices on what constitutes an authorized AP (MAC addressed based filtering)
- Whenever a new access point is discovered in the network that falls outside the pre configured authorized LIST, it can be assumed to be a rogue AP

Rogue Access Points Operated By Attackers

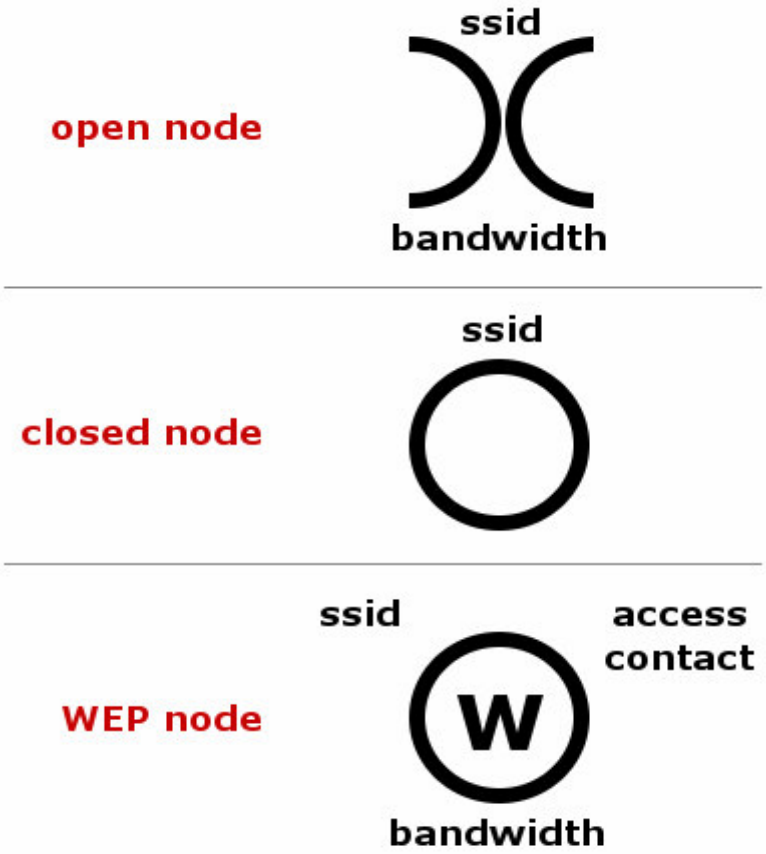
- Freely available open-source attack tools ease the job of attackers
- Clients receiving stronger signal from the attacker operated AP would then attract legitimate clients to associate with it

How to cope with rogue access points

- Network administrators must make sure to implement strict polices regarding the deployment of wireless hardware
- Audit their networks often with reliable tools to ensure that these rogue access points do not exist

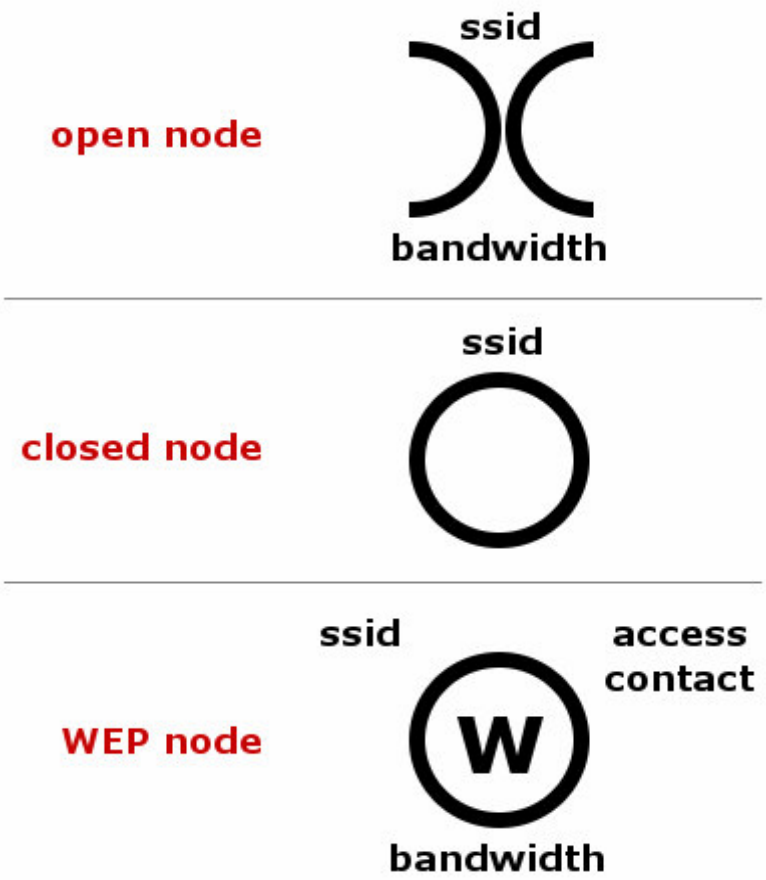
Warchalking [1]

- Using a fairly universal hobo sign language, individuals mark structures that have hotspots associated with them
- Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post.



Warchalking [2]

- Those offering Wi-Fi service might also draw such a symbol to advertise the availability of their Wi-Fi location, whether commercial or personal.
- The marks are designed to be recognized by those in the know

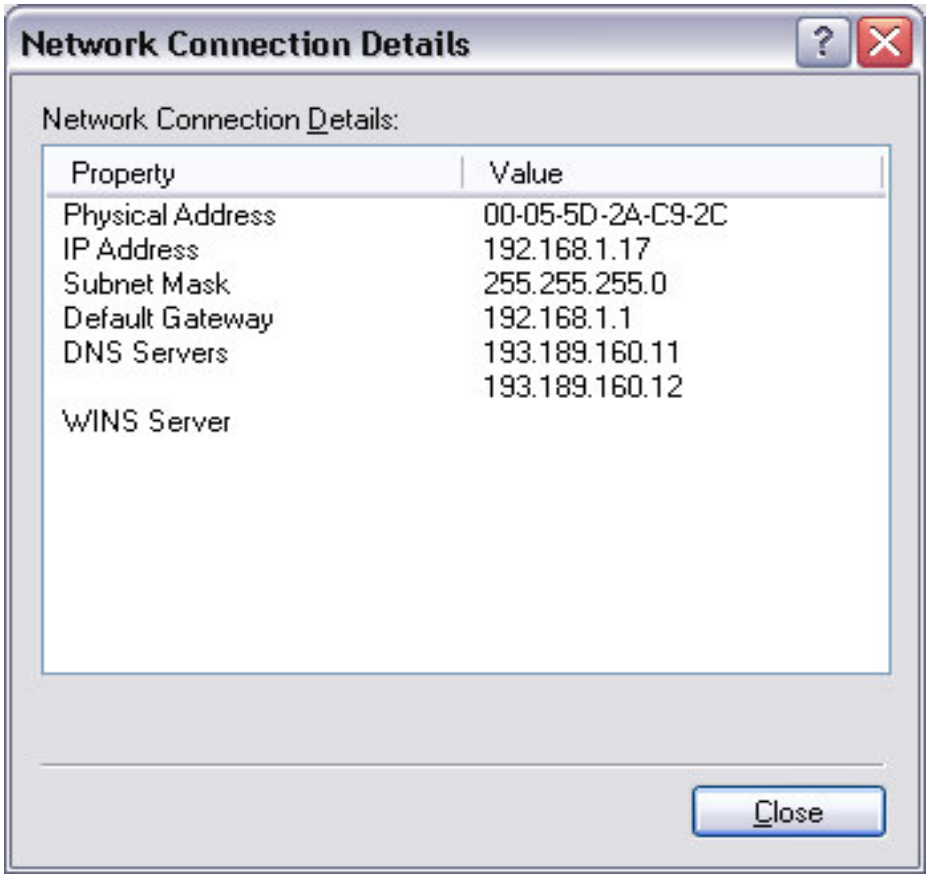


MAC filtering

- MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists
- There are methods to avoid this form of access control through address modification ("spoofing") or the physical exchange of network cards between hosts

MAC Address Spoofing [1]

- Existing encryption standards are not foolproof
- A hacker can:
  - pick off authorized MAC addresses and steal bandwidth
  - corrupt or download files
  - wreak havoc on an entire network



MAC Address Spoofing [2]

- Even if you are using encryption or virtual private networks (VPNs), MAC addresses are always in the air
- Hackers can change their MAC address to the valid user's MAC address using any number of spoofing or cloning utilities
- Then the hacker can connect to the wireless LAN and bypass any MAC address filtering

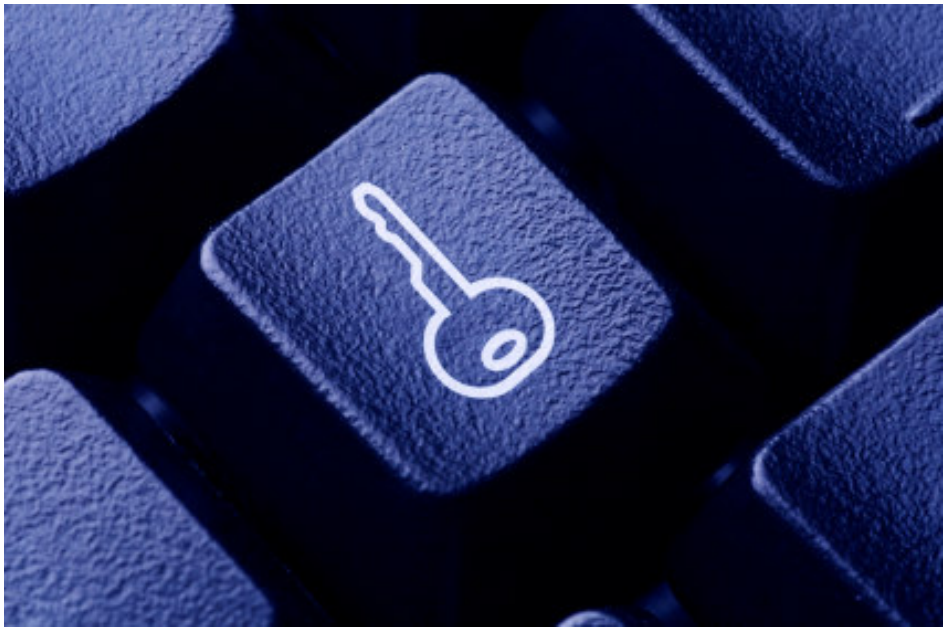
Noisy Neighbours

- Because we are dealing with radio waves passing through the air, unwanted radio signals can wander into our domain from outside sources:
  - cordless phones
  - microwave ovens
  - neighbouring business' 802.11 router
- This noise, or interference can have a drastic effect on network performance and reliability

ENCRYPTION

Encryption

- Encrypt your home wireless network
- Without encryption, anyone within range of your wireless router can use your network to go online
- If they know what they're doing, these freeloaders can tap into your computer, too



Wireless Encryption Protocol (WEP)

- WEP is a protocol that adds security to wireless local area networks (WLANs) based on the 802.11 Wi-Fi standard
- WEP was integrated into wireless devices to:
  - Prevent casual eavesdropping on a network
  - Prevent unauthorized access to wireless networks

WEP key [1]

- WEP keys allow a group of devices on a local network (such as a home network) to exchange encoded messages with each other while hiding the contents of the messages from easy viewing by outsiders

WEP key [2]

- The length of a WEP key depends on the type of WEP security (called "encryption") utilized:
  - 40- / 64-bit WEP: 10 digit key
  - 104- / 128-bit WEP: 26 digit key
  - 256-bit WEP: 58 digit key

Methods of attacking WEP

Brute force attacks

- Simply break down WEP's functionality forcing errors within the protocol and eventually causing it to open a door on its own

Dictionary attack

- Uses dictionary of keys stored over time to try guessing a different key until one works

IV (Initialization Vector) vulnerability

- Simply break down defenses by causing confusion within the WEP transmissions

Advantages of WEP

- WEP does a fine job at keeping novice hackers from spying on your valuable data
- WEP is a good method for preventing attackers from capturing your network traffic
- Not only is WEP a good way to ward off many would-be attackers, it is strengthened when used with other security techniques

MAC Address Blocking

- You can specify which computers should be able access to your wireless access points
- Telling the access points which hardware MAC addresses can join the network does this

WPA [1]

- WPA (Wi-Fi Protected Access) is a security technology for wireless networks, which improves on the authentication and encryption features of WEP
- WPA is used for WiFi networks to correct deficiencies in the older WEP standard

WPA [2]

- WPA provides more security to wireless networks than a WEP security set up
- The use of firewalls will help with security breaches which can help to fix security problems in some wireless networks that are more vulnerable

Key components of WPA [1]

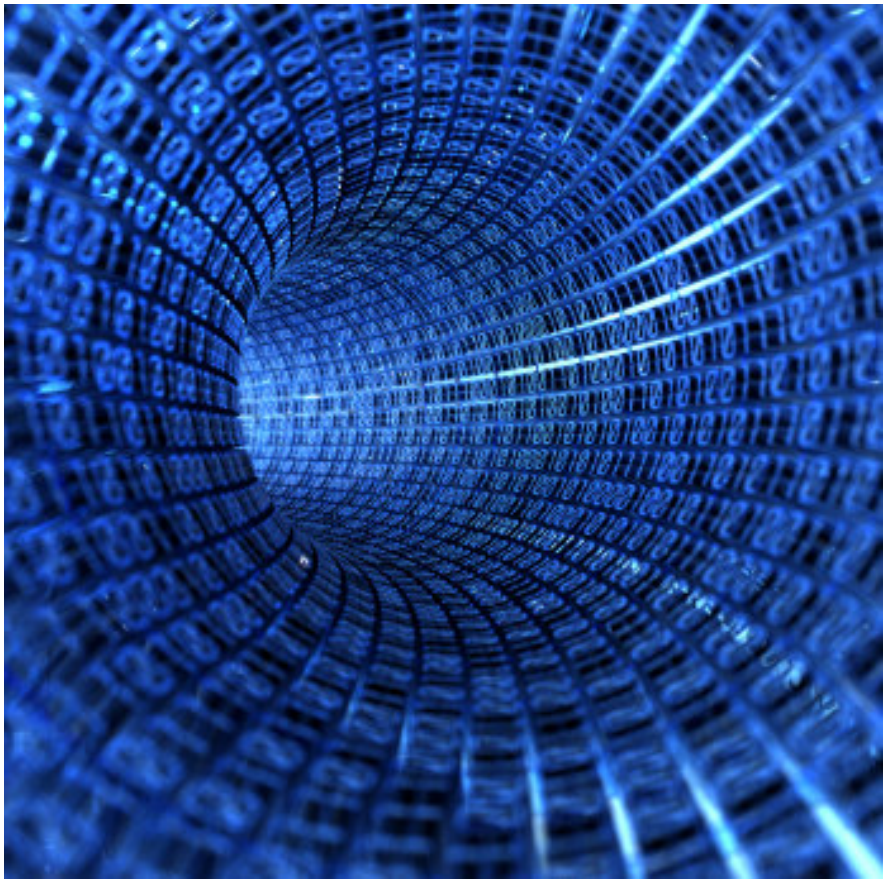
Temporal Key Integrity Protocol (TKIP)

- TKIP was designed to replace WEP without replacing legacy hardware
- TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP

Key components of WPA [2]

Built-in authentication

- Provides roughly comparable security to VPN tunneling with WEP, with the benefit of easier administration and use



SOLUTIONS

Network Auditing [1]

- Network administrators should equip themselves with the proper tools for auditing and troubleshooting their wireless networks
- Two leading technologies that are gaining momentum in enterprise and small business LANs alike, are Intrusion Prevention Systems (IPS), and Intrusion Detection Systems (IDS)

Network Auditing [2]

- Intrusion Prevention Systems try to take a proactive measure in network security, so as to stop the attack before it starts
- Intrusion Detection Systems are more passive in their methodology, monitoring and informing network administrators of any intrusive presence.

Virtual Private Networks [1]

- VPN facilitate security over public connections through encryption techniques and other various security methods
- A VPN works by sending data through a "tunnel" which cannot be penetrated by paths outside of the tunnel
- This is done through the use of tunneling protocols such as Layer Two Tunneling Protocol, which encrypts the data at the sending end, and decrypts it at the receiving end

Virtual Private Networks [2]

- In order for a VPN to function properly, network users must install a small client application on their computers, which is used to decipher and help facilitate the encoded communication

VNP use [1]

- To connect to the firm’s computer network, a wireless device requires a wireless network adapter
- If a user does not change the default name to a secure code—and most don’t—it can be easy for an intruder to crack the default code and intercept the user’s communications

VNP use [2]

- Many firms recognize this problem and insist that users change their default settings
- But if just one person fails to do so, the entire system may be wide open
- For this reason, some organizations have installed wireless virtual private network (VPN) access points

STATISTICS

Wardriving [1]

It is driving around a city searching for the existence of Wireless LAN (802.11) Networks.

- In June of 2004, WorldWide Wardrive 4 reported that an alarming 61.6 percent of all submitted wireless access points were broadcasting data with no encryption enabled

Wardriving [2]

- 31.4 percent of the logged access points were using default SSIDs
- 27.5 percent were using no encryption with default SSIDs
- The amount of access points using no encryption decreased by 6.04 percent from the previous year's endeavor

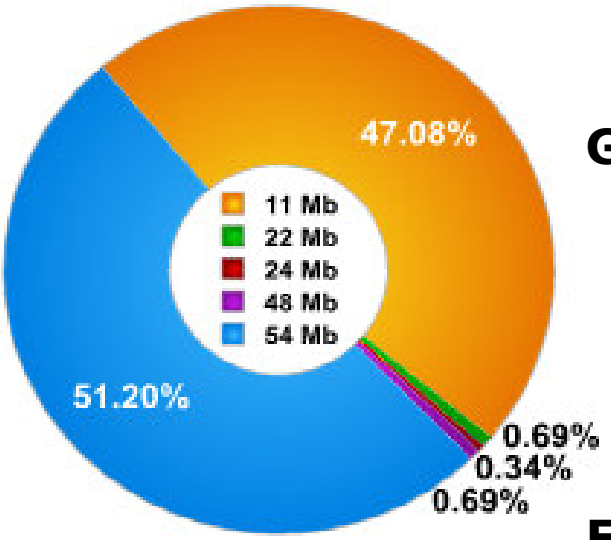
Wardriving [3]

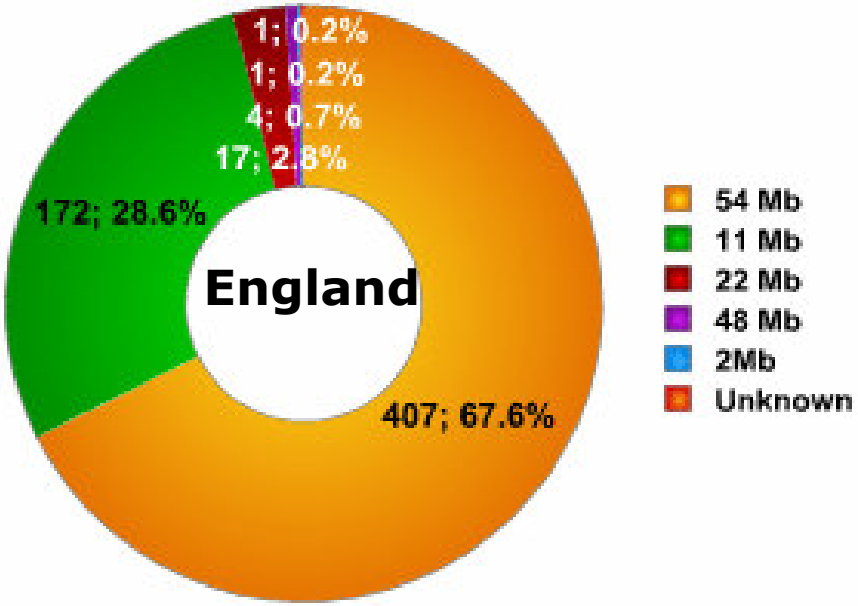
- The number of wireless networks broadcasting default SSIDs and which used no encryption and default SSIDs actually increased by 3.57 percent and 2.54 percent, respectively

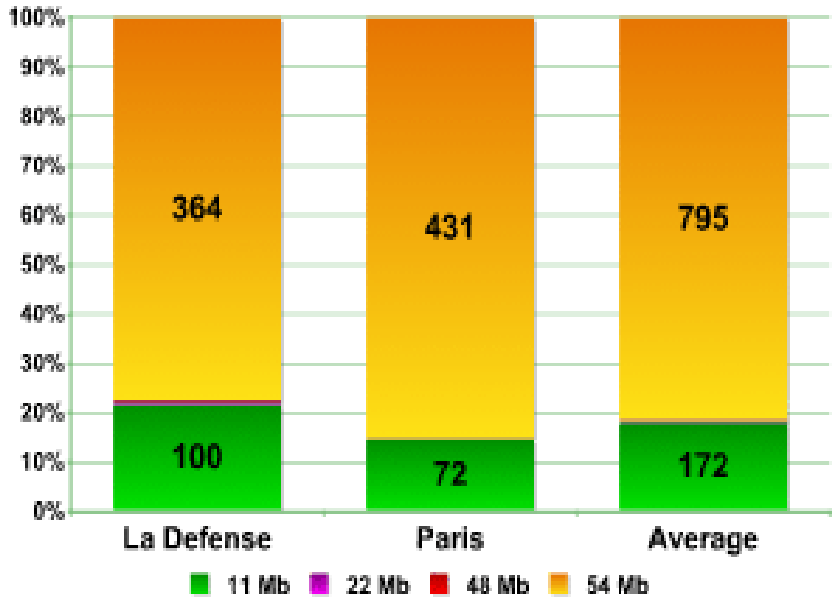
Wardriving statistics

- Wardriving in Germany, Mar 15 2006
- Wardriving in England, London, May 23 2006
- Wardriving in France, Paris, Dec 20 2006
- Wardriving in Poland, Warsaw, Apr 06 2007

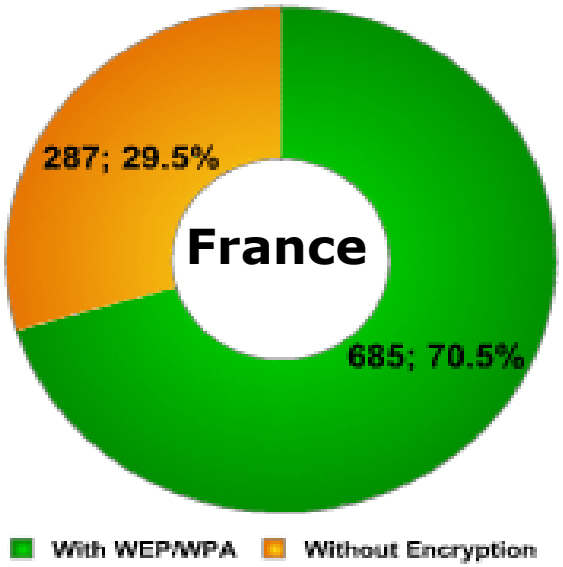
Data transmission speed

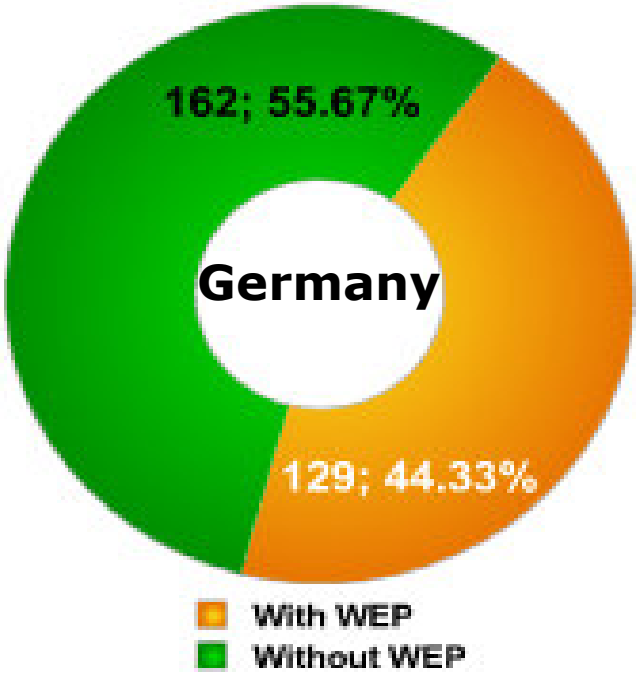


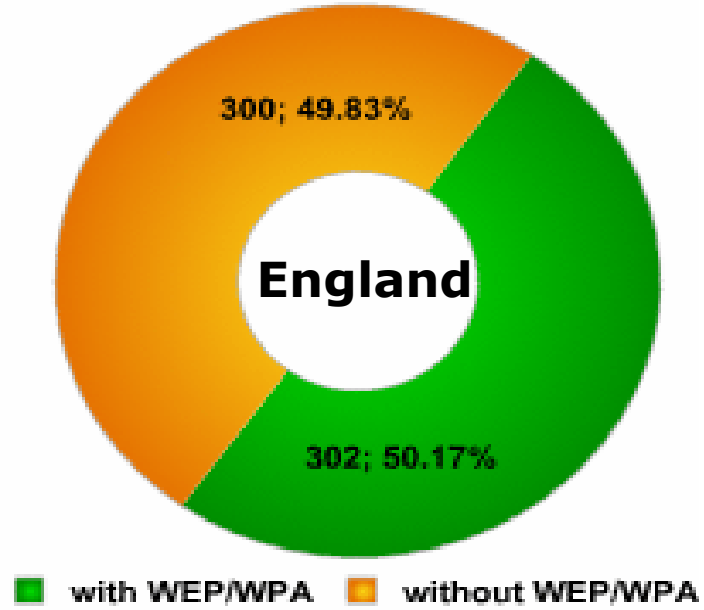




Data encryption

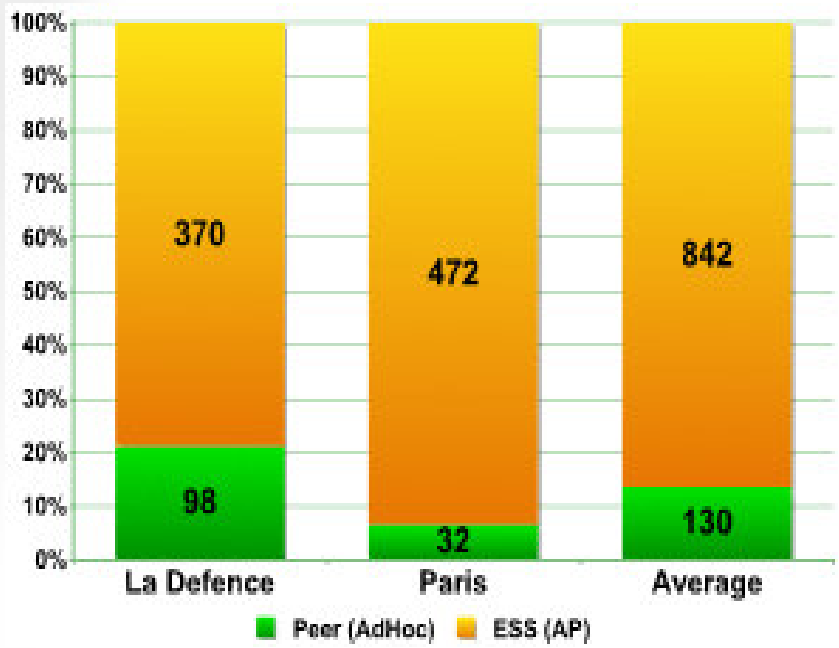




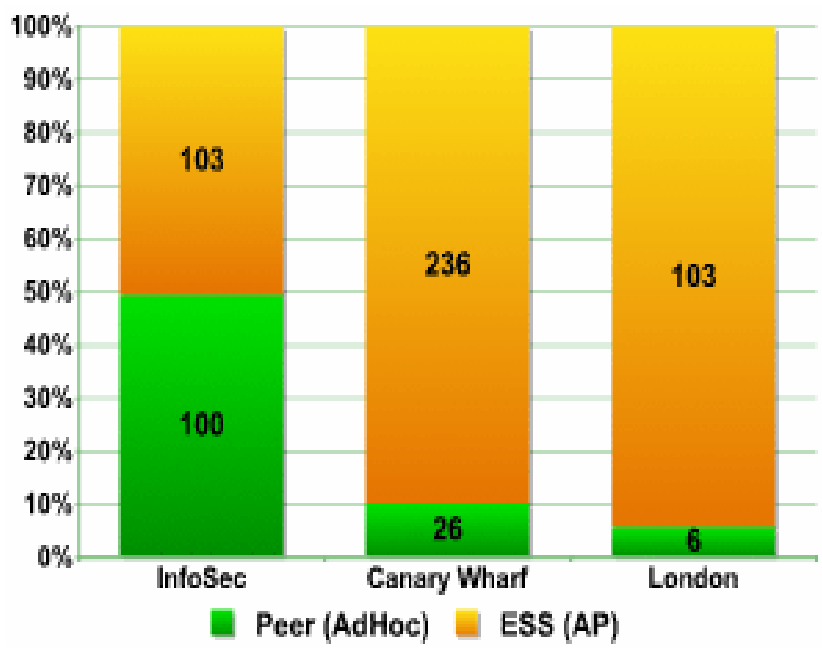


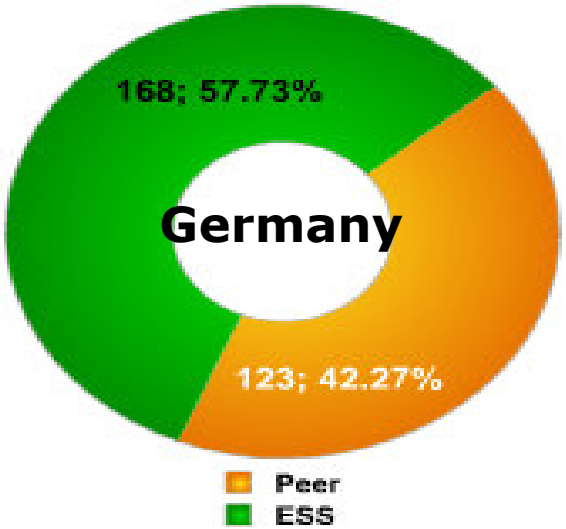
Types of network access

France



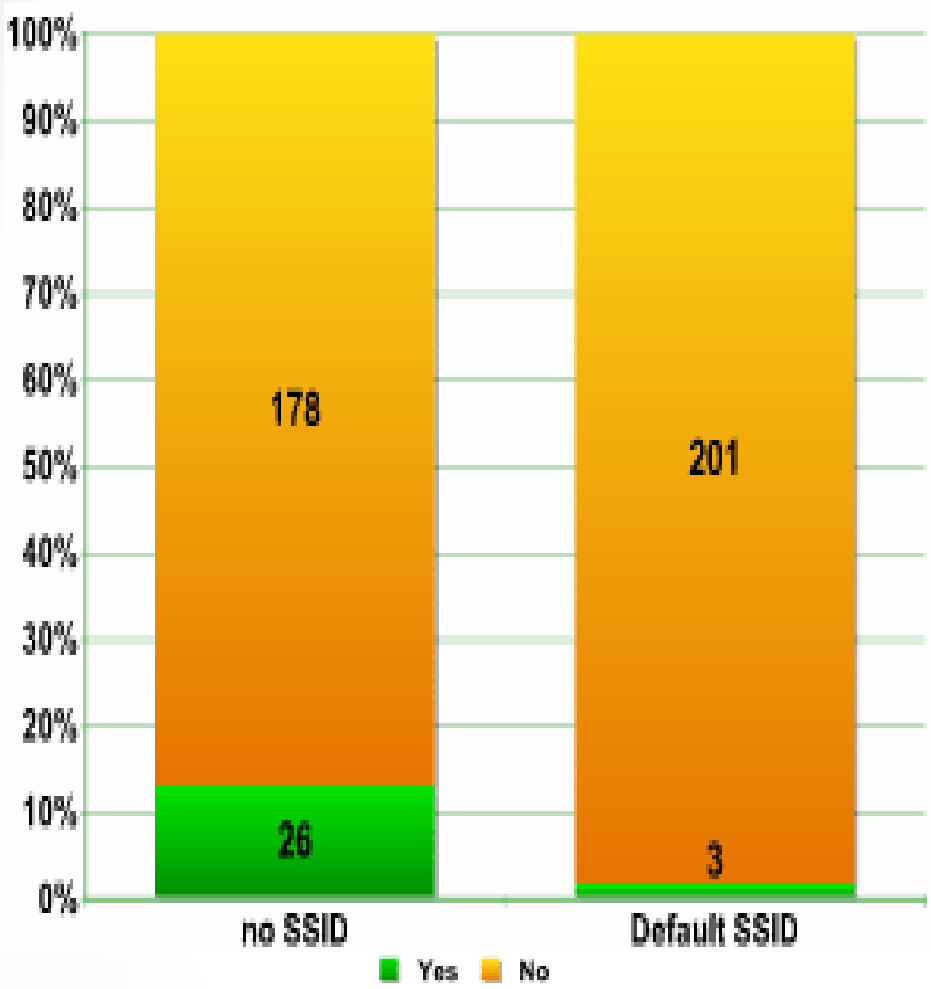
England

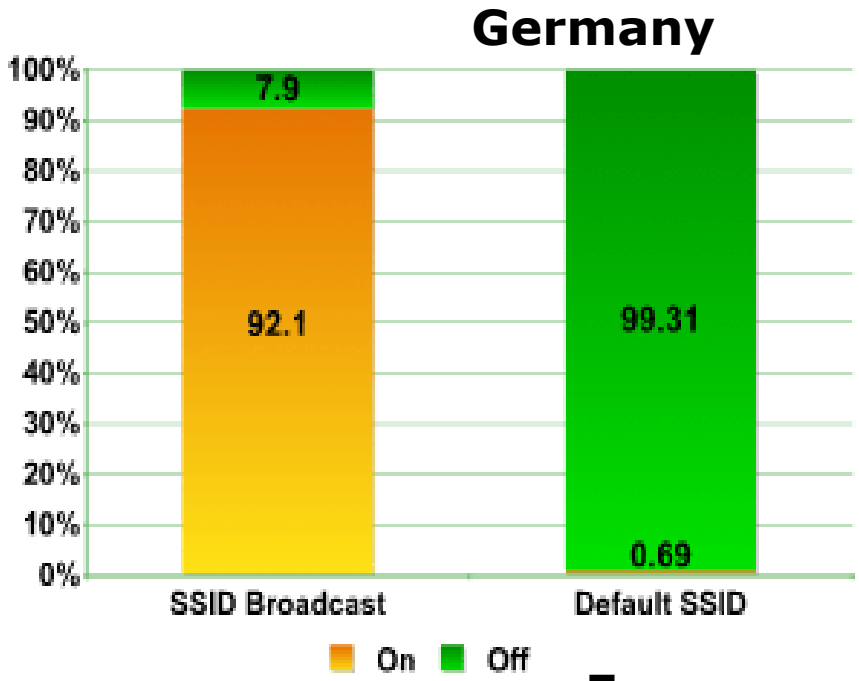


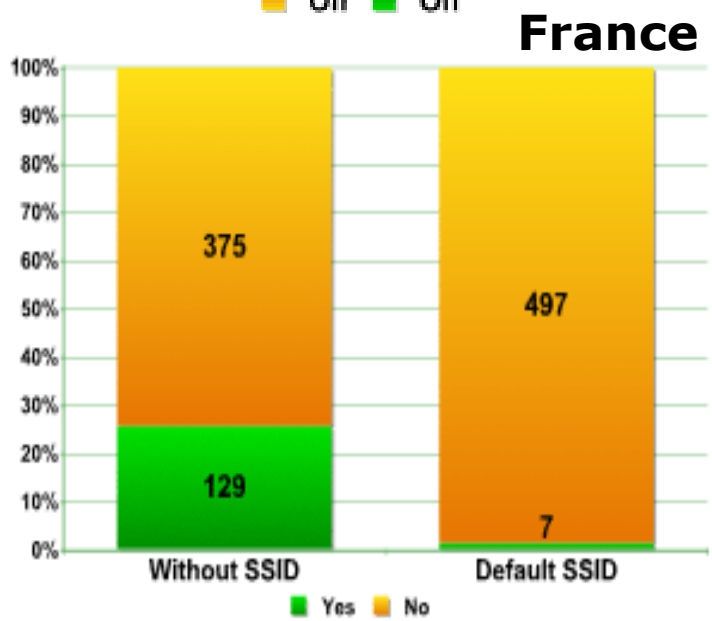


InfoSecurityLab

Default configuration



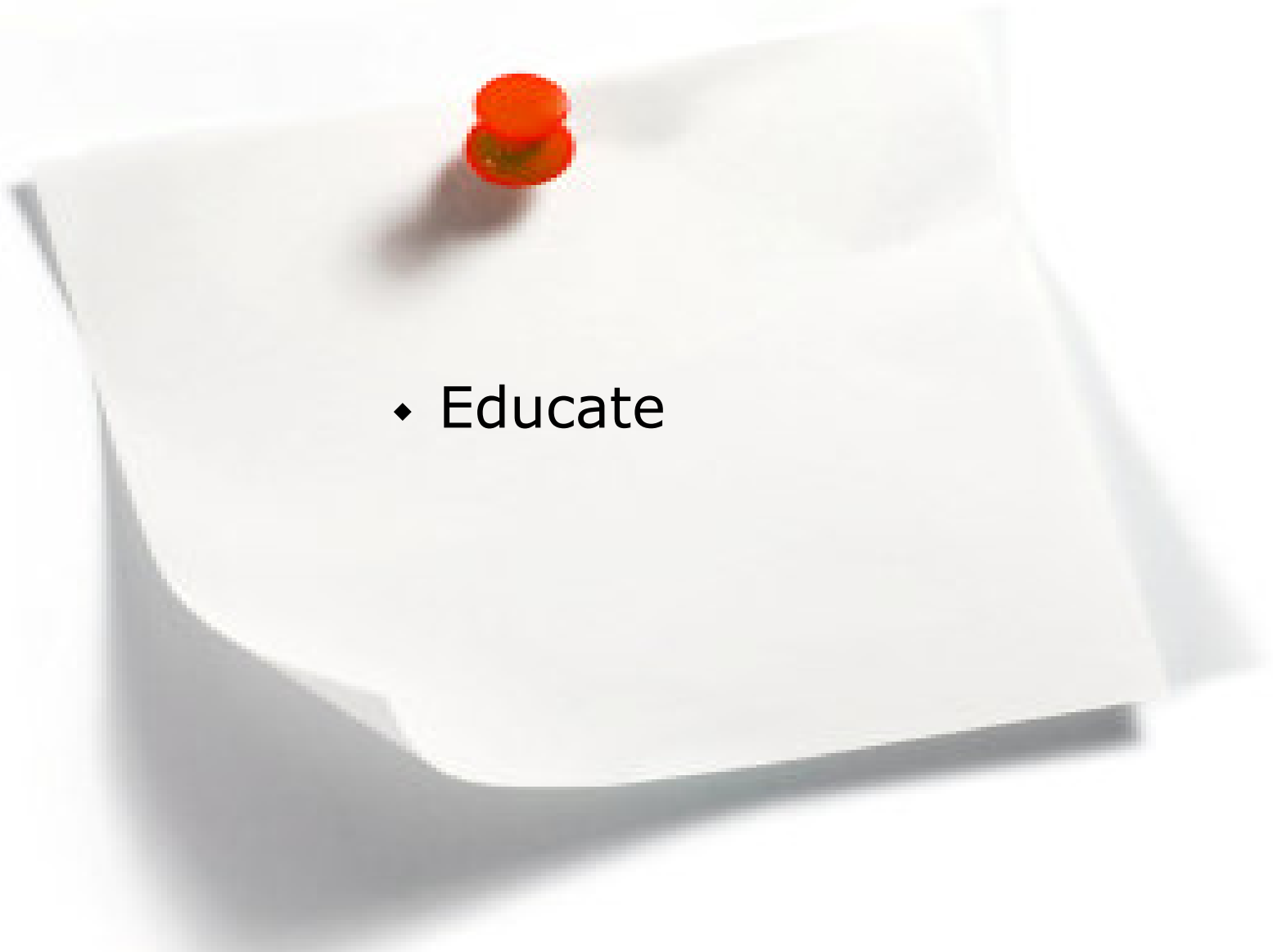




http://www.viruslist.com

InfoSecurityLab

HOW TO SECURE YOUR WI-FI NETWORK

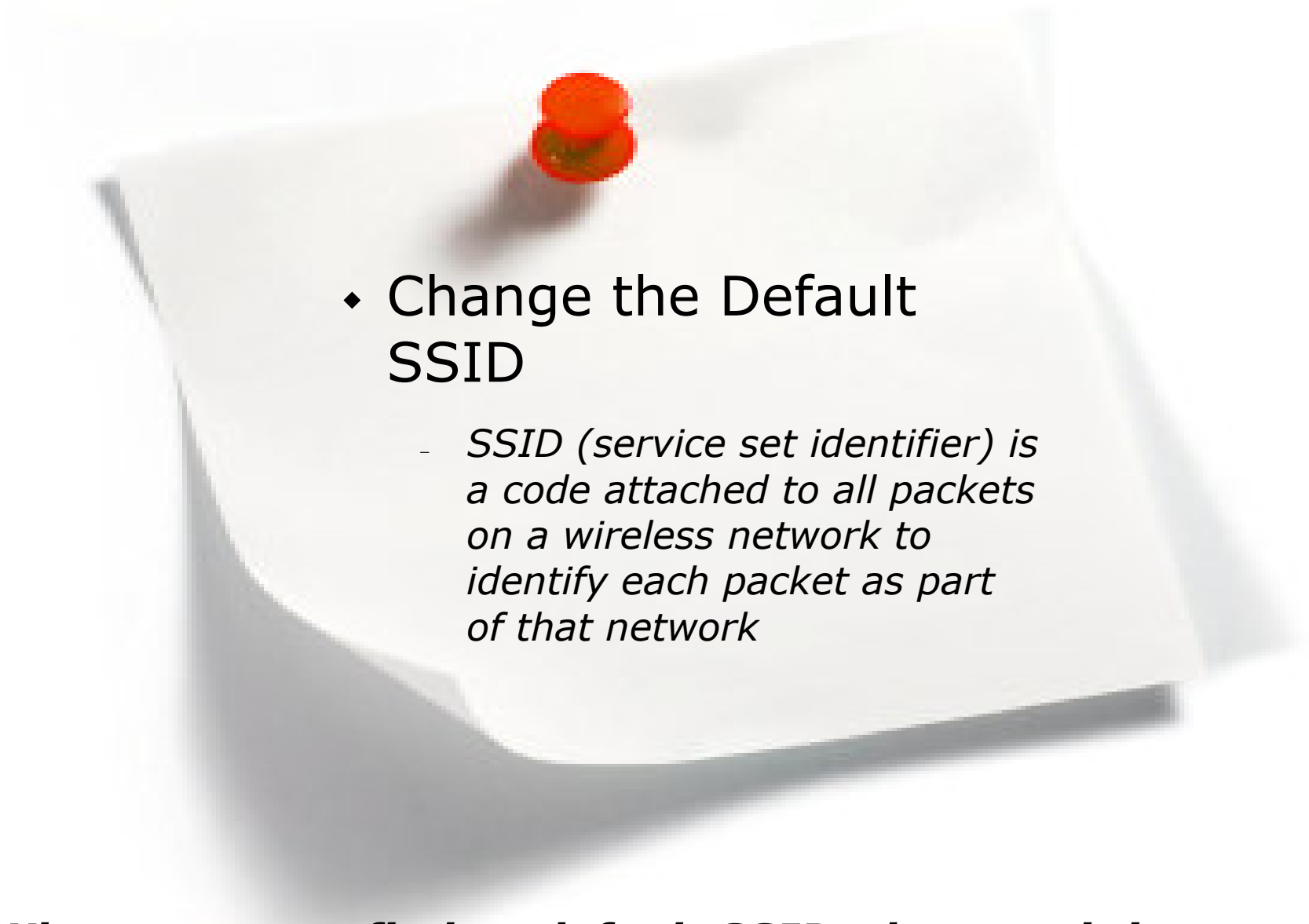


The biggest threats to computer security are often an organization's own employees. It is critical to teach employees how to use wireless computers safely

The logins provided are simple and very well-known to hackers on the Internet

Encryption technology scrambles messages sent over wireless networks so that they cannot be easily read by humans

WPA2/802.11i strongly preferred. Use decent keys



- Change the Default SSID
  - *SSID (service set identifier) is a code attached to all packets on a wireless network to identify each packet as part of that network*

When someone finds a default SSID, they see it is a poorly configured network and are much more likely to attack it

Restrict the network to only allow connections. Hacker software programs can fake MAC addresses easily

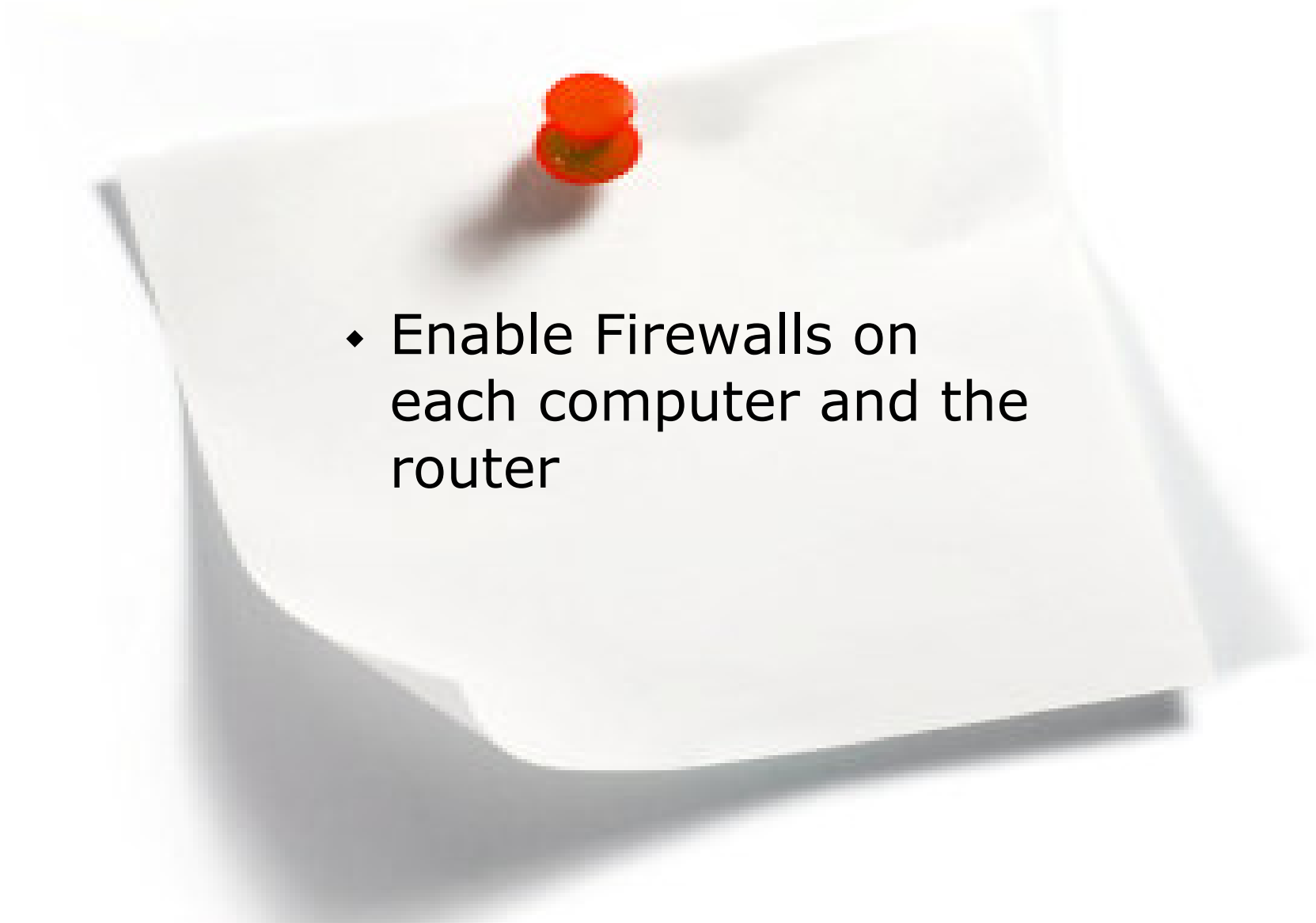
If enabled, it increases the possibility an unwelcome neighbour or hacker will try to log in to your network

- Do Not Auto-Connect to Open Wi-Fi Networks

It exposes your computer to security risks. This setting should not be enabled except in temporary situations

- Assign Static IP Addresses to Devices

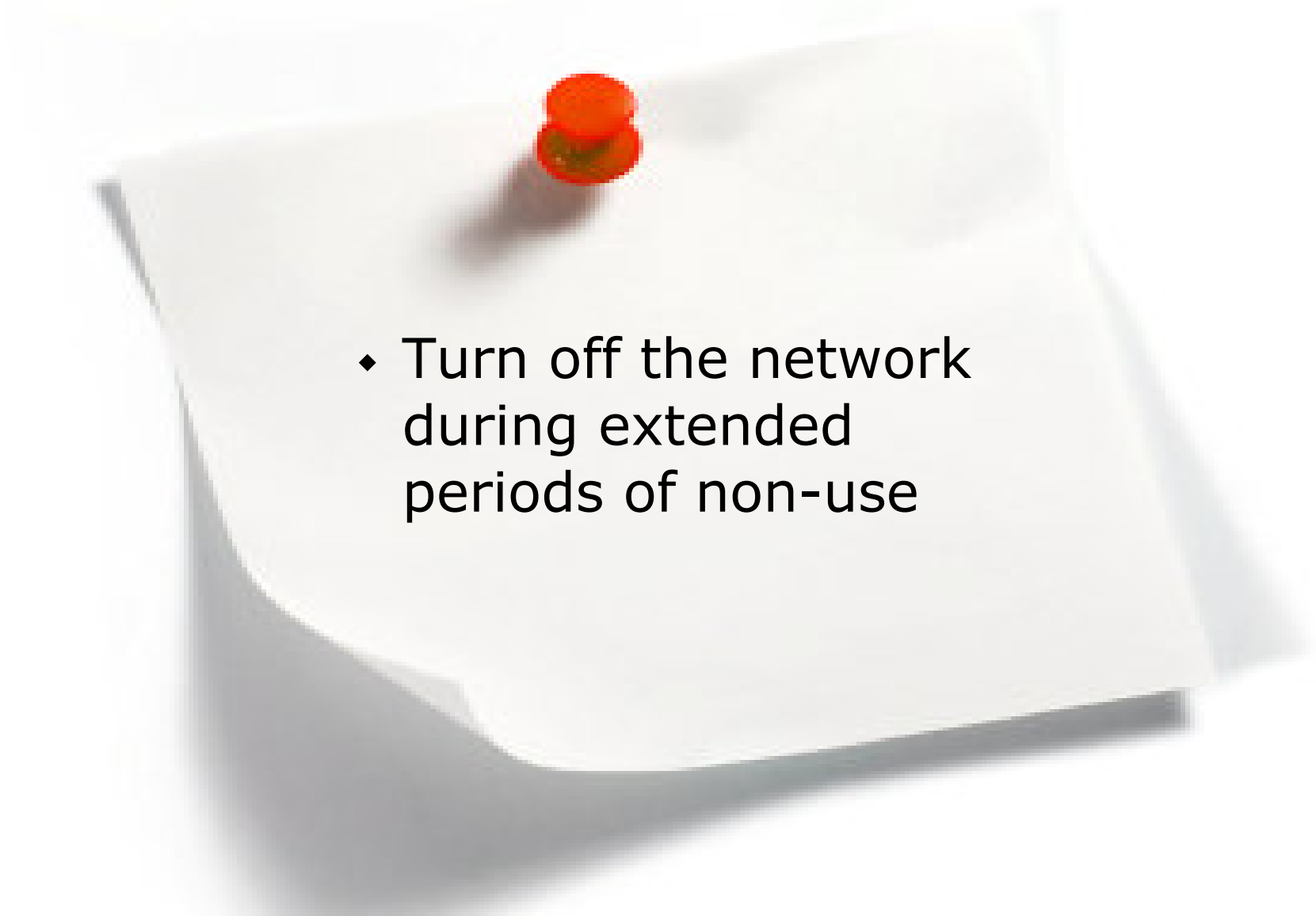
1. ***Turn off DHCP on the router or access point***
2. ***Set a fixed IP address range***
3. ***Set each connected device to match***
4. ***Use a private IP range (like 10.0.0.x) to prevent computers from being directly reached from the Internet***



Consider installing and running personal firewall software on each computer connected to the router for extra protection

- Position the router or Access point safely

Try to position these devices near the centre of the home rather than near windows to minimize leakage



Shutting down the network will most certainly prevent outside hackers from breaking in

- Update the firmware and drivers on your access point and wireless cards

Manufacturers commonly fix known issues, security holes, and enable new features with these updates

If you're sending or receiving email while using a Wi-Fi network, make sure you log-in to your web-based email using SSL

Conclusion

- In this presentation we learned, how to secure your wireless network, and also we saw that many people leave default settings, thus let hackers easily to break in their networks

Keep secure!