MTU
Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

Computer Security Principles

Lecture 13: Wireless Security

www.mtu.ie

Introduction

- In recent years, wireless networking has become more available, affordable, and easy to use.
- Home users are adopting wireless technology in great numbers.
- On-the-go laptop users often find free wireless connections in places like coffee shops and airports.
- If you're using wireless technology, you should know about the security threats you may encounter.
- With wireless, you connect to the Internet through the air over a radio signal to your computers.

Wireless Security

A wireless-enabled device can make you more productive outside your office or home, but it can also expose you to a number of security threats.

MTU
Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

Home Wireless Threats

Home Wireless Threats

Piggybacking

- If you fail to secure your wireless network, anyone with a wireless-enabled computer within range of your wireless access point can hop a free ride on the Internet over your wireless connection.
- The typical indoor broadcast range of an access point is 150 – 300 feet.
- Outdoors, this range may extend as far as 1,000 feet.
- So, if you live in an estate, or if you live in an apartment, failure to secure your wireless network could potentially open your internet connection to quite a lot of users.

Home Wireless Threats

Piggybacking invites a number of problems:

- Service violations: You may exceed the number of connections permitted by your internet service provider.
- Bandwidth shortages: Users piggybacking on your internet connection might use up your bandwidth and slow your connection.
- Abuse by malicious users: Users piggybacking on your internet connection might engage in illegal activity that will be traced to you.
- Monitoring of your activity: Malicious users may be able to monitor your internet activity and steal information.
- Direct attack on your computer: Malicious users may be able to access files on your computer, install malicious programs, or take control of your computer.

War Driving and War Chalking

Home Wireless Threats

Wardriving

- Wardriving is a specific kind of piggybacking.
- Equipped with a wireless-equipped computer—sometimes with a powerful antenna, it is possible to search for unsecured wireless networks. This practice is nicknamed “wardriving.”
- Wardrivers often note the location of unsecured wireless networks and publish this information on web sites.
- Malicious individuals wardrive to find a connection they can use to perpetrate illegal online activity using your connection to mask their identities.

Home Wireless Threats

Unauthorized Computer Access

- An unsecured wireless network combined with unsecured file sharing can spell disaster. Under these conditions, a malicious user could access any directories and files you have allowed for sharing.

Initialization Vector Attack

- An initialization vector attack is an attack on wireless networks.
- This attack is aimed at network that uses the same key to encrypt and decrypt a series of data (WEP).
- In such networks, once the bad guy learns of the single key, s/he can read all the data passing through the network.
- The initialization vector is added as an extra security to scramble the key for each data stream to look different and thereby block off the bad guy.
- The end system know how to remove the initialization vector and be able to decrypt the data using the same key.

Initialization Vector Attacks

Network modifies the IV of an encrypted wireless packet during transmission.

Attacker learns the plaintext of one packet → compute the RC4 key stream generated by the IV → decrypt all other packets that use the same IV → build a decryption table to decrypt every packet sent over that wireless connection.

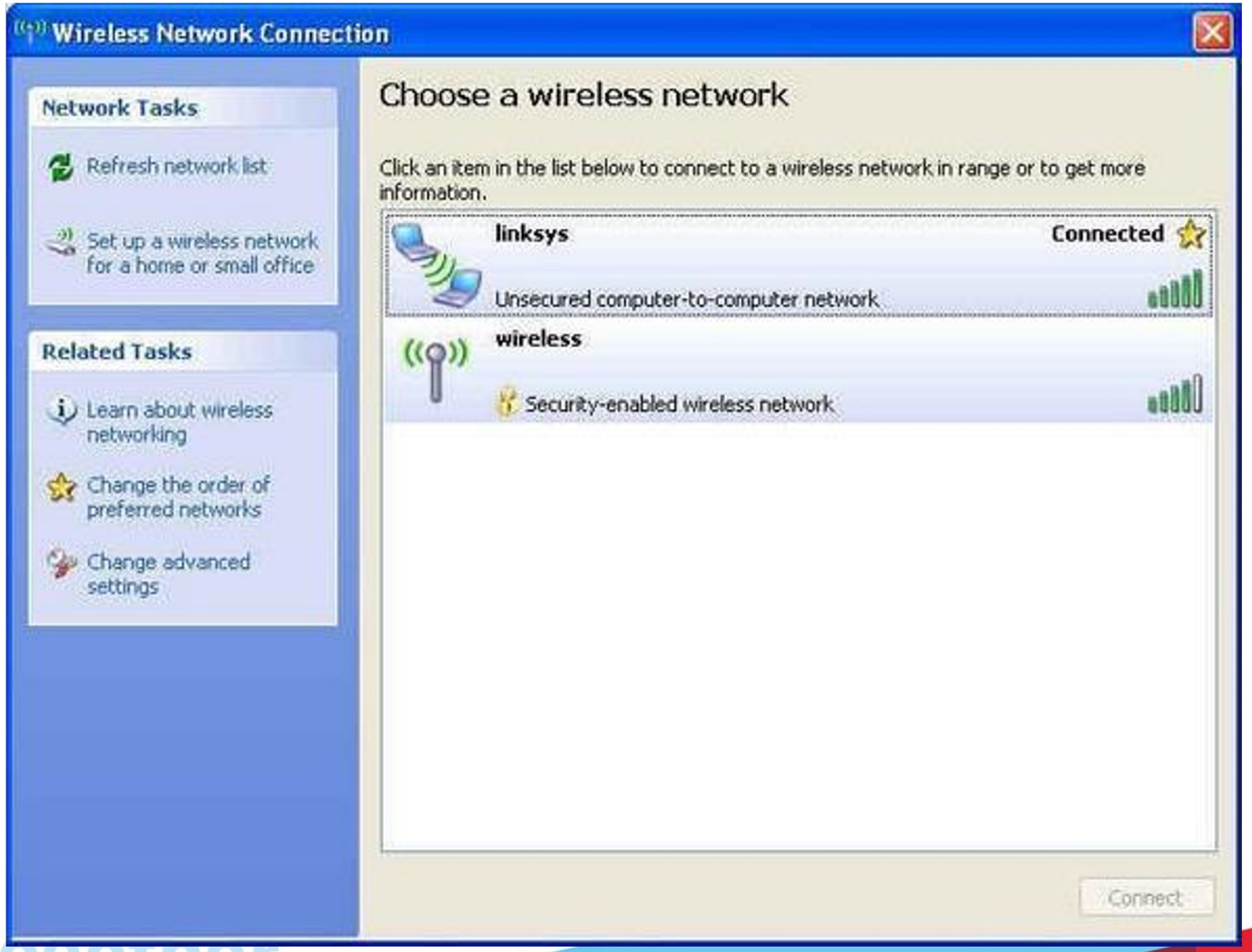
MTU
Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

Protecting Home Wireless Networks

Protecting Home Wireless

- While the security problems associated with wireless networking are serious, there are steps you can take to protect yourself.
- The following slides describe these steps:

Typical Screen for viewing available wireless networks



Protecting Home Wireless

MTU
Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

Make Your Wireless Network Invisible

- Wireless access points can announce their presence to wireless-enabled computers, known as “identifier broadcasting.”
- However, you’re the only one who needs to know you have a wireless network in your home.
- To make your network invisible to others, see your access point’s user manual for instructions on disabling identifier broadcasting.
- This “security through obscurity” is not foolproof but it is a starting point for securing your wireless network.

Protecting Home Wireless

Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

Rename Your Wireless Network

- Many wireless access point devices come with a default name.
- This name is referred to as the “service set identifier” (SSID) or “extended service set identifier” (ESSID).
- The default names used by various manufacturers are widely known and can be used to gain unauthorised access to your network.
- When you rename your network, you should choose a name that won’t be easily guessed by others.

Protecting Home Wireless

Encrypt Your Network Traffic

- Your wireless access point device should allow you to encrypt traffic passing between the device and your computers.
- By encrypting wireless traffic, you are converting it to a code that can only be understood by computers with the correct key to that code.
- If possible, you should use secure WPA2 (Wi-Fi Protected Access).

Protecting Home Wireless

WEP (Wired Equivalent Privacy)

- Is a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard.
- WEP was designed to provide the same level of security as that of a wired LAN.
- It turned out that WEP's privacy was not at all equivalent to that of a wired network.
- Therefore, it wasn't long before a new technology called WPA — Wi-Fi Protected Access — was created to address the many shortfall's of WEP.

Protecting Home Wireless

WPA2 (Wi-Fi Protected Access)

- Is a certification program created by the Wi-Fi Alliance to indicate compliance with the security protocol created by the Wi-Fi Alliance to secure wireless computer networks.
- The WPA protocol implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was being prepared.
- WPA2 then replaced WPA. WPA2 implements the mandatory elements of 802.11i.

Protecting Home Wireless – Enabling Encryption

Protecting Home Wireless

Change Your Administrator Password

- Your wireless access point device likely shipped with a default password. Default passwords for various manufacturers are widely known and can be used to gain unauthorized access to your network.
- Be sure to change your administrator password to one that is long, contains non-alphanumeric characters, and does not contain personal information.
- If your wireless access point does not have a default password, be sure to create one and use it to protect your device.

Protecting Home Wireless

MTU
Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

Use File Sharing with Caution

- If you don't need to share directories and files over your network, you should disable file sharing on your computers. You may want to consider creating a dedicated directory for file sharing, and move or copy files to that directory for sharing.
- In addition, you should password protect anything you share, and use a password that is long, contains non-alphanumeric characters, and does not contain personal information.
- Never open an entire hard drive for file sharing.

Protecting Home Wireless

Keep Your Access Point Software Patched and Up to Date

- From time to time, the manufacturer of your wireless access point will release updates to the device software or patches to repair bugs.
- Be sure to check the manufacturer's web site regularly for any updates or patches for your device's software.

Protecting Home Wireless

Check Your Internet Provider's Wireless Security Options

- Your internet service provider may provide information about securing your home wireless network.
- Check the customer support area of your provider's web site or contact your provider's customer support group.

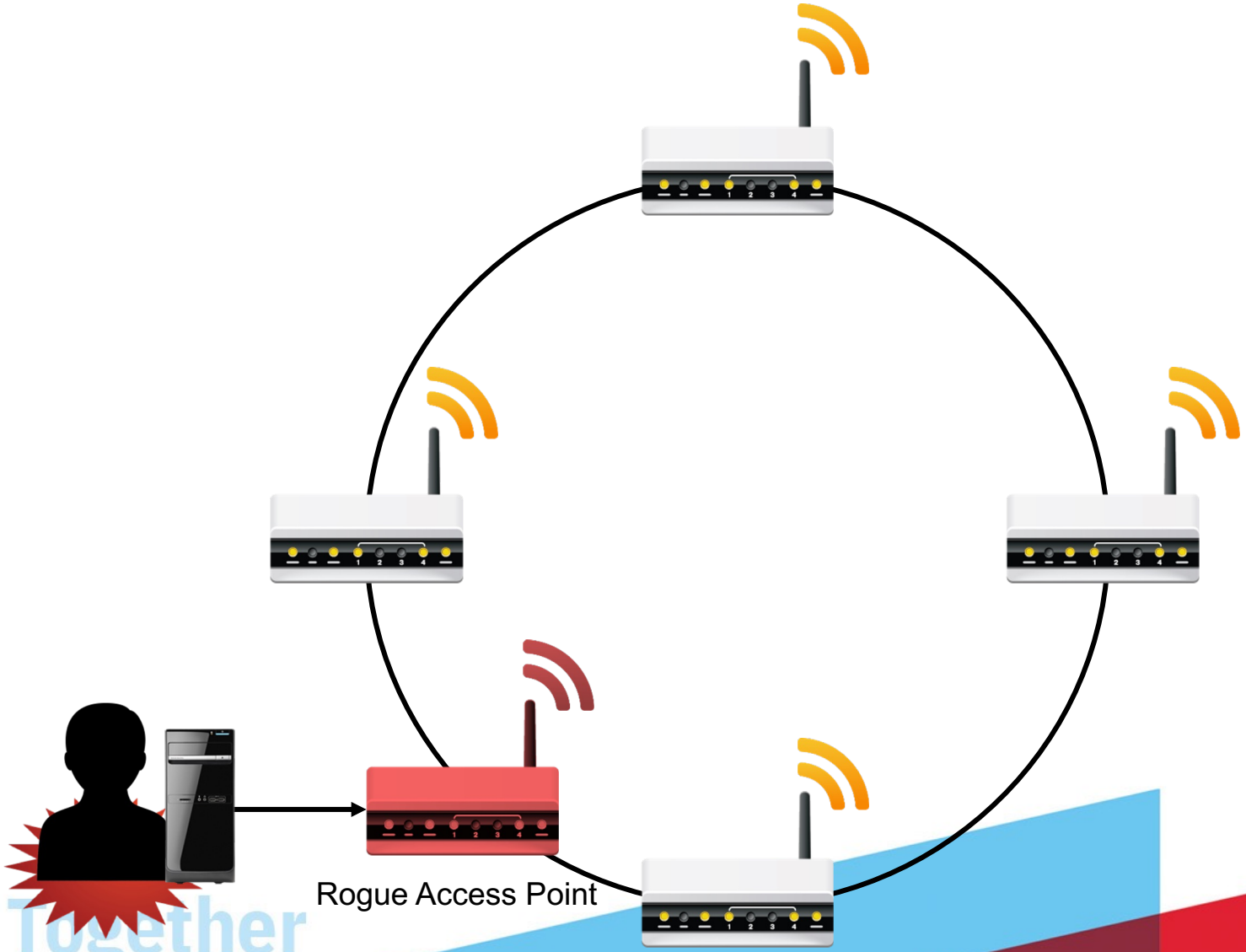
MTU
Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

Public Wireless Threats

Public Wireless Threats

- A wireless-enabled laptop can make you more productive outside your office or home, but it can also expose you to a number of security threats.
- The following slides describe some of the security threats you face when using a public access point.

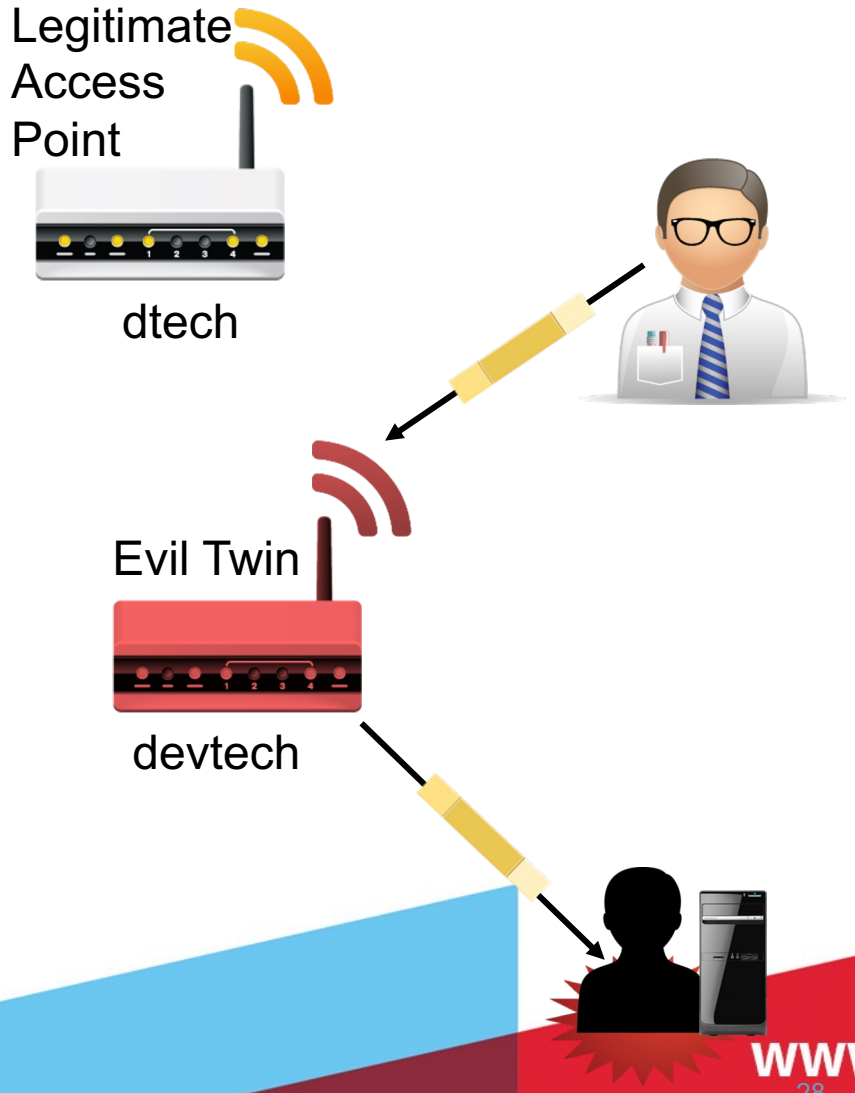
Rogue Access Points



Evil Twins

The attacker will use a broadcast signal stronger than the one generated by the real access point.

Unsuspecting users will connect using the stronger, bogus signal. Because the victim is connecting to the internet through the attacker's system, it's easy for the attacker to use specialized tools to read any data the victim sends over the internet.



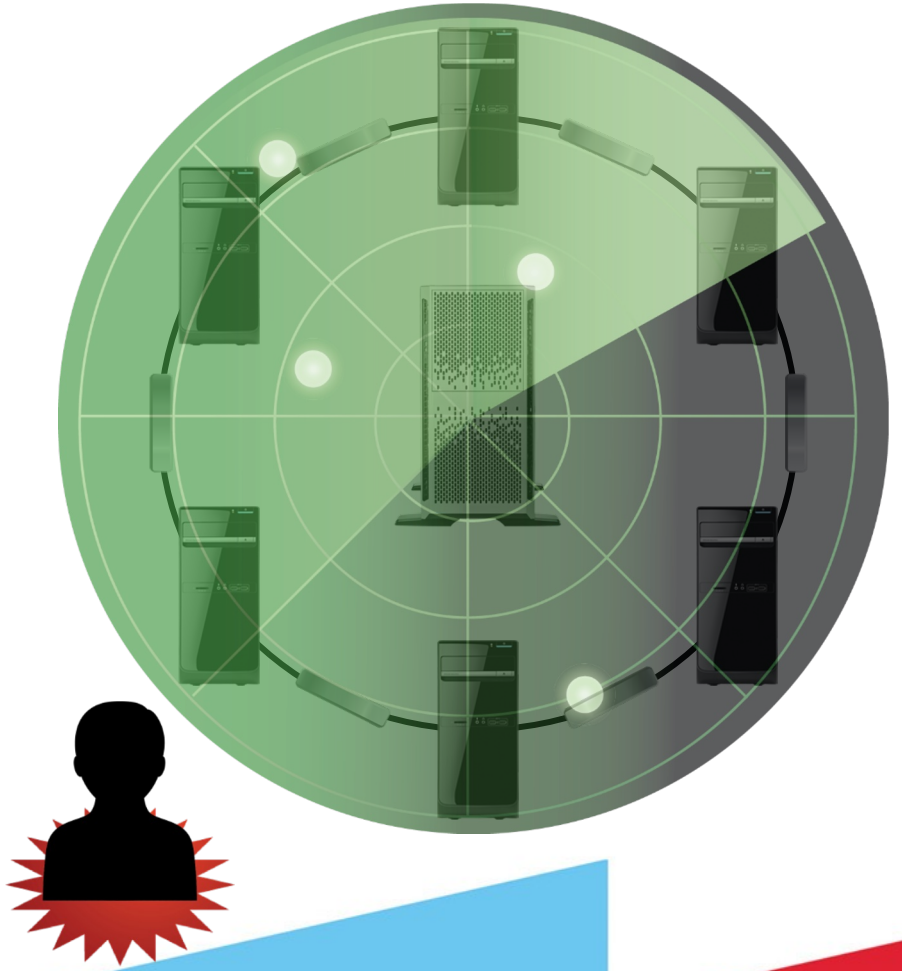
Jamming

The deliberate blocking, interference or jamming of wireless signal, this can be achieved by a dedicated hardware (see hak5 Pineapple) or using the any WiFi transmitter

Public Wireless Threats

Wireless Sniffing

- Many public access points are not secured, and the traffic they carry is not encrypted.
- This can put your sensitive communications or transactions at risk.
- Because your connection is being transmitted “in the clear,” malicious users can use “sniffing” tools to obtain sensitive information such as passwords, bank account numbers, and credit card numbers.



Public Wireless Threats

Peer-to-Peer Connections

- Many laptop computers, particularly those equipped with 802.11-type WiFi wireless networking cards, can create ad hoc networks if they are within range of one another.
- These networks enable computer-to-computer connections, a situation that creates security concerns you should be aware of.
- An attacker with a network card configured for ad hoc mode and using the same settings as your computer may gain unauthorised access to your sensitive files.
- You should note that many PCs ship from the same manufacturer could have wireless cards set to ad hoc mode by default.

Public Wireless Threats

Unauthorized Computer Access

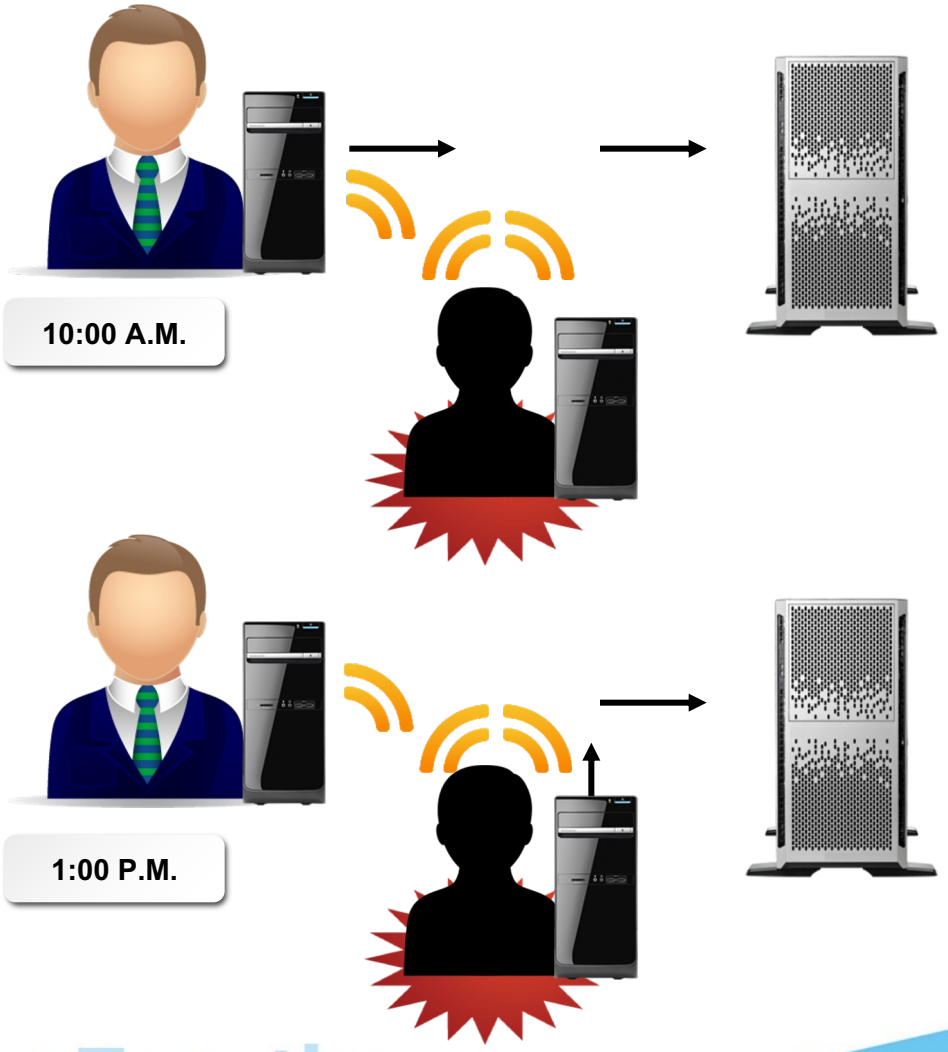
- As is the case with unsecured home wireless networks, an unsecured public wireless network combined with unsecured file sharing can spell disaster.
- Under these conditions, a malicious user could access any directories and files you have allowed for sharing.

Public Wireless Threats

Shoulder Surfing

- In public wireless areas, the bad guys don't even need a computer to steal your sensitive information.
- The fact that you may be conducting personal business in a public space is opportunity enough for them.
- If close enough, they can simply glance over your shoulder as you type.
- By simply watching you, they can steal all kinds of sensitive, personal information.

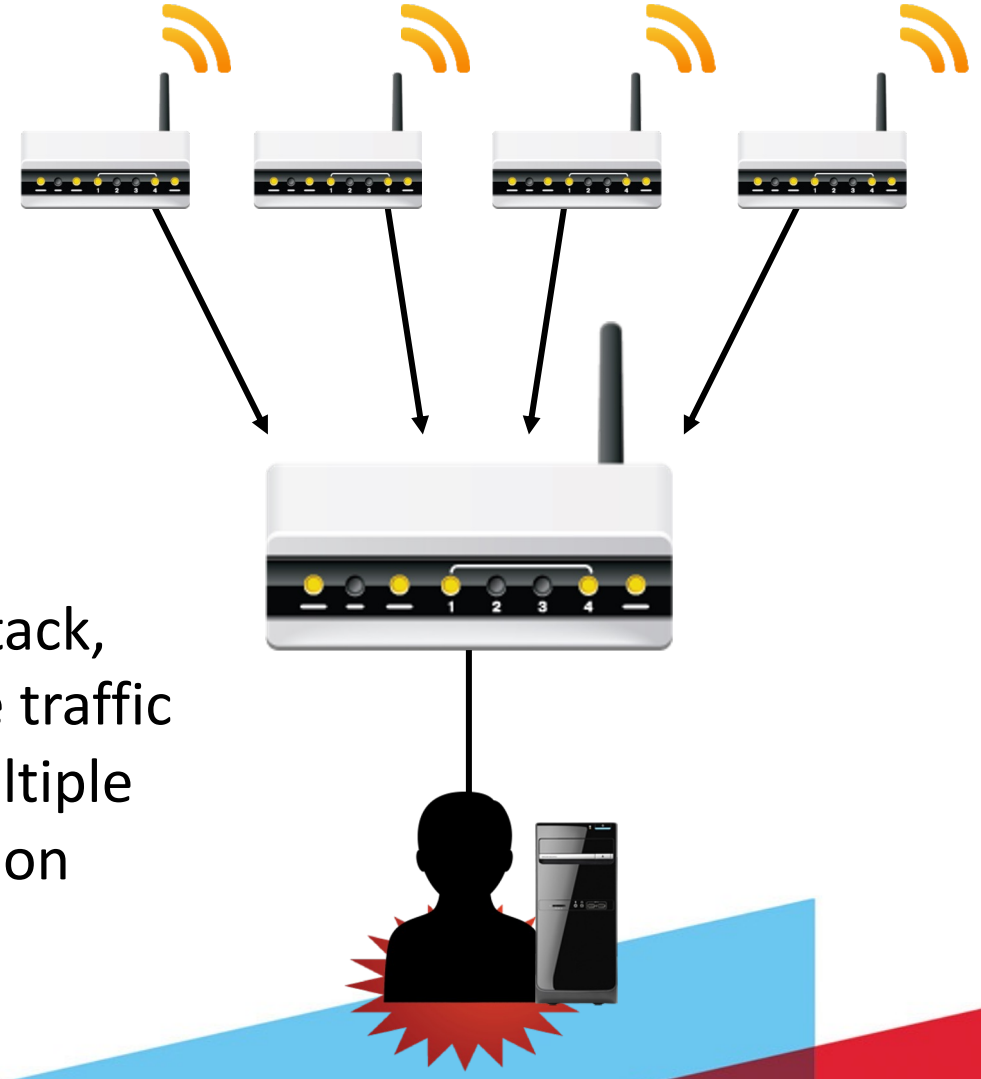
Wireless Replay Attacks



In these attacks valid data transmission is maliciously or fraudulently repeated or delayed

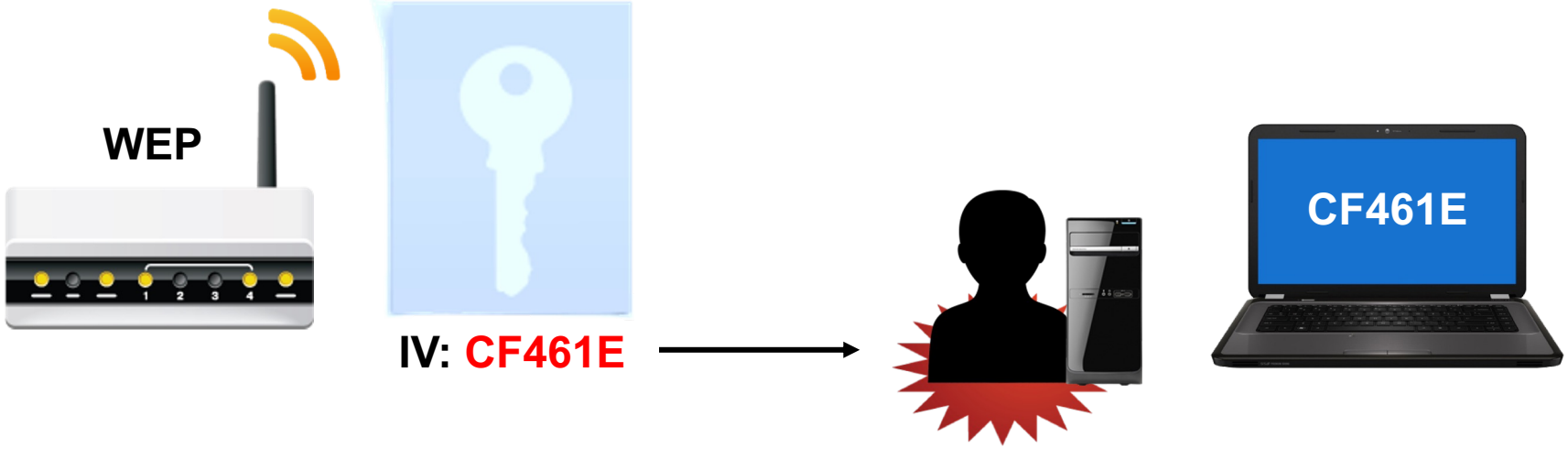
It can be used to impersonate and gain access to a system.

Sinkhole Attacks



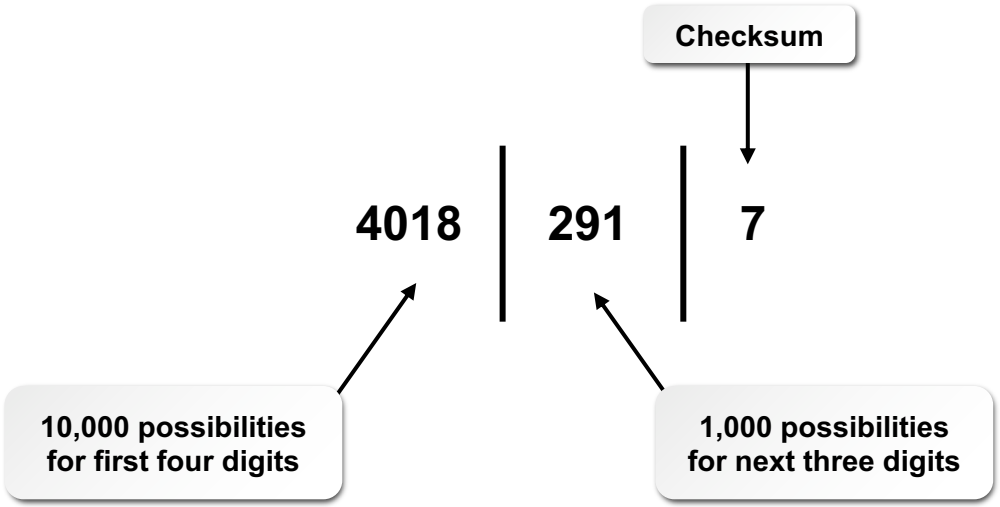
Very complex form of attack, the sinkhole takes all the traffic it can, this attack has multiple uses but the most common is eavesdropping

WEP and WPA Attacks



WiFi Protected Setup (WPS) Attacks

WPS PIN



11,000 possibilities, not 100,000,000

Bluejacking

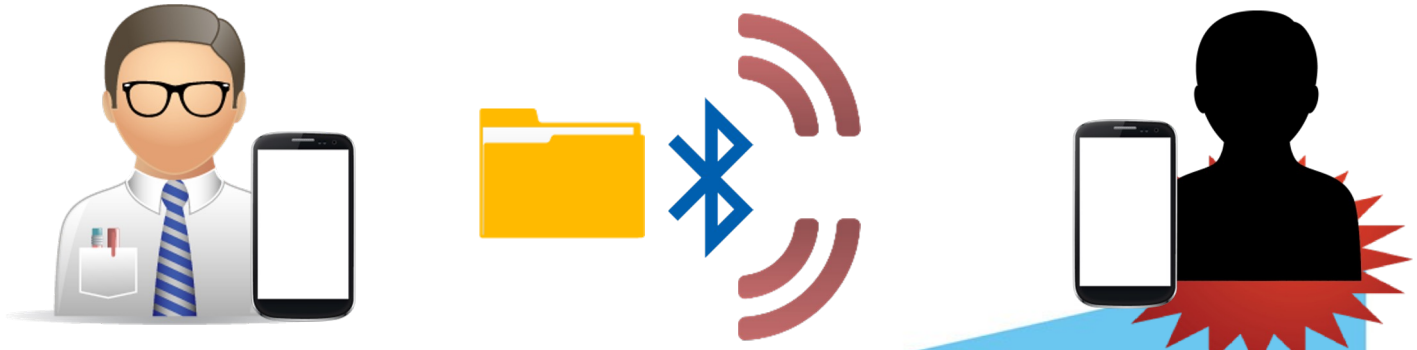
- As the name suggests, this is hijacking Bluetooth communications by sending unsolicited communications to Bluetooth enabled devices.

- In Bluejacking, packets are sent to the Bluetooth device from the attacker

Bluesnarfing

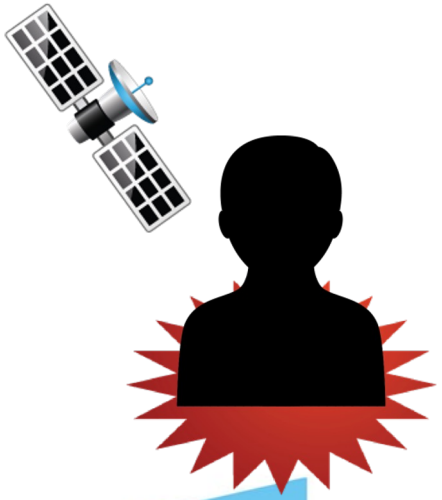
- This is the unauthorised access of information from a bluetooth enabled device through Bluetooth communications.

- While Bluejacking is often harmless, Bluesnarfing involves the theft of information (contacts, emails, texts etc.)



Near Field Communication

NFC is used for communications between smartcards and POS terminals, exploit kits are emerging/available to target this and allow attackers to steal information.



This can be mitigated by using EM shielding around NFC enabled systems when not in use

MTU
Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

Safe Public Wireless Access

Safe Wireless Networking in Public Spaces

- Accessing the internet via a public wireless access point involves serious security threats you should guard against.
- These threats are compounded by your inability to control the security setup of the wireless network.
- You are often in range of numerous wireless-enabled computers operated by people you don't know.
- The following slides describe steps you can take to protect yourself.

Safe Wireless Networking in Public Spaces

Watch What You Do Online

- Because you're likely to have an unsecured, unencrypted network connection when you use a public wireless access point, be careful about what you do online—there's always the chance that another user on the network could be monitoring your activity.
- If you can't connect securely using a VPN, then consider avoiding
  - online banking
  - online shopping
  - sending email
  - typing passwords or credit card numbers

Safe Wireless Networking in Public Spaces

MTU
Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

Connect Using a VPN

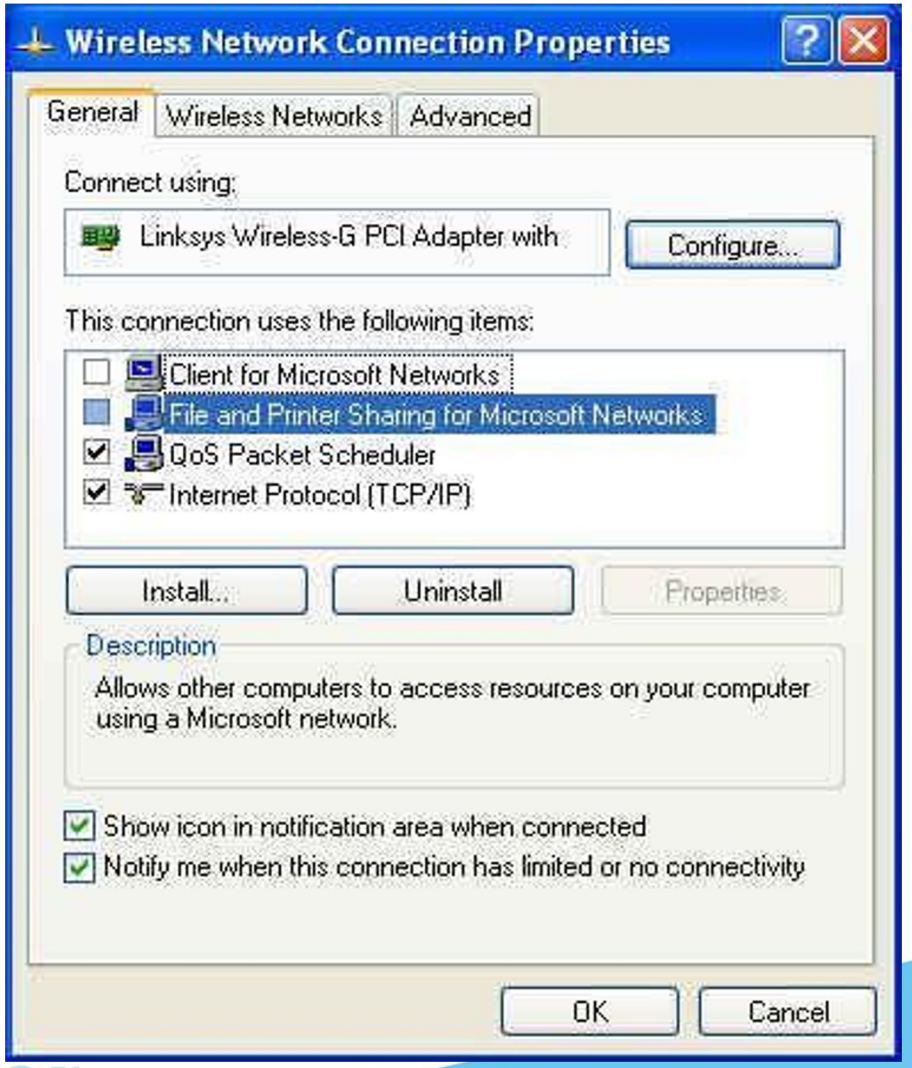
- Many companies and organizations have a virtual private network (VPN).
- VPNs allow employees to connect securely to their network when away from the office.
- VPNs encrypt connections at the sending and receiving ends, and keep out traffic that is not properly encrypted.
- If a VPN is available to you, make sure you log onto it any time you need to use a public wireless access point.

Safe Wireless Networking in Public Spaces

Disable File Sharing

- File sharing in public wireless spaces is even more dangerous than it is on your home wireless network.
- This is because you and your wireless-enabled laptop are likely to be even closer to other wireless computers operated by people you don't know.
- Also, many public wireless networks feature peer-to-peer networking in which other computers will attempt to connect directly to yours.
- To prevent attackers from gaining access to your sensitive files, you should disable file sharing when connecting to a public wireless access point.

Safe Wireless Networking in Public Spaces



Safe Wireless Networking in Public Spaces

MTU
Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

Do not auto-connect to open Wi-Fi networks

- Connecting to an open Wi-Fi network such as a free wireless hotspot exposes your computer to security risks.
- Although not normally enabled, most computers have a setting available allowing these connections to happen automatically without notifying you (the user).
- This setting should not be enabled except in temporary situations.

Safe Wireless Networking in Public Spaces

MTU
Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

Be Aware of Your Surroundings

- When using a public wireless access point, you should be aware of what's going on around you.
  - Are others using their computers in close proximity to you?
  - Can others view your screen?
- If any of these conditions exist, your sensitive data might be at risk.
- Consider whether it is essential to connect to the internet.
- If an internet connection is not essential, disable wireless networking altogether.
- If you do need to connect, use caution and follow the steps noted previously.

MTU
Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

Thank You!