Unit 13: Wireless Networks Security

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss the need for security
- Explain the concept of security threats
- Describe traffic monitoring
- Explain unauthorized access
- Explain middle attacks
- Describe denial of service
- Discuss various types of protective actions

Notes

Introduction

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WEP is an old IEEE 802.11 standard from 1999 which was outdated in 2003 by WPA or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device which encrypts the network with a 256 bit key; the longer key length improves security over WEP.

Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking is prone to some security issues. Crackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into wired networks. As a result, it's very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources. Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.

The risks to users of wireless technology have increased as the service has become more popular. There were relatively few dangers when wireless technology was first introduced. Crackers had not yet had time to latch on to the new technology and wireless was not commonly found in the work place. However, there are a great number of security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level. Cracking methods have become much more sophisticated and innovative with wireless. Cracking has also become much easier and more accessible with easy-to-use Windows or Linux-based tools being made available on the web at no charge.

Some organizations that have no wireless access points installed do not feel that they need to address wireless security concerns. In-Stat MDR and META Group have estimated that 95% of all corporate laptop computers that were planned to be purchased in 2005 were equipped with wireless. Issues can arise in a supposedly non-wireless organization when a wireless laptop is plugged into the corporate network. A cracker could sit out in the parking lot and gather info from it through laptops and/or other devices as handhelds, or even break in through this wireless card-equipped laptop and gain access to the wired network.

13.1 Need of Security

Wireless networking is inherently risky because you are transmitting information via radio waves. Data from your wireless network can be intercepted just like signals from your cellular or cordless phones. Whenever you use a wireless connection, you might want to ensure that your communications and files are private and protected. If your transmissions are not secure, it may be possible for others to intercept your e-mails, examine your files and records, and use your network and Internet connection to distribute their own messages and communications.

How secure you want your network to be depends on how you use it. If you're just surfing to do research or watch movies, you may not care if anyone picks up part of the transmission, but that's up to you. Even if you're shopping and purchasing items over the net, those financial transactions are usually protected by Secure Socket Layer (SSL). However, if your data is confidential or if you want additional security, there are several different technologies you can install. Keep in mind that security is a personal decision, but it's almost essential to use at least some level of security as a deterrent to intrusion and interception.

Notes

Did u know? In a home wireless network, you can use a variety of simple security procedures to protect your Wi-Fi connection. These include enabling Wi-Fi Protected Access, changing your password or network name (SSID) and closing your network. However, you can also employ additional, more sophisticated technologies and techniques to further secure your business network.

13.2 Security Threats

All computer systems and communications channels face security threats that can compromise systems, the services provided by the systems, and/or the data stored on or transmitted between systems. The most common threats are:

- Denial-Of-Service (DOS) occurs when an adversary causes a system or a network to become unavailable to legitimate users or causes services to be interrupted or delayed. Consequences can range from a measurable reduction in performance to the complete failure of the system. A wireless example would be using an external signal to jam the wireless channel. There is little that can be done to keep a serious adversary from mounting a denial of service attack.
- Interception has more than one meaning. A user's identity can be intercepted leading to a later instance of masquerading as a legitimate user or a data stream can be intercepted and decrypted for the purpose of disclosing otherwise private information. In either case, the adversary is attacking the confidentiality or privacy of the information that is intercepted.
- For example: eavesdropping and capturing the wireless interchanges between a wireless device and the network access point.
- Since wireless systems use the radio band for transmission, all transmissions can be readily intercepted. Therefore, some form of strong authentication and encryption is necessary in order to keep the contents of intercepted signals from being disclosed.
- Manipulation means that data has been inserted, deleted, or otherwise modified on a system or during transmission. This is an attack on the integrity of either the data transmission or on the data stored on a system. An example would be the insertion of a Trojan program or virus on a user device or into the network. Protection of access to the network and its attached systems is one means of avoiding manipulation.
- Masquerading refers to the act of an adversary posing as a legitimate user in order to gain access to a wireless network or a system served by the network.
- For example, a user with inappropriate access to a valid network authenticator could access the network and perform unacceptable functions (e.g., break into a server and plant malicious code, etc.). Strong authentication is required to avoid masquerade attacks.
- Repudiation is when a user denies having performed an action on the network. Users might deny having sent a particular message or deny accessing the network and performing some action. Strong authentication of users, integrity assurance methods, and digital signatures can minimize the possibility of repudiation.

13.3 Traffic Monitoring

13.3.1 Monitoring Requirements

To plan for wireless traffic monitoring, there are few thing to consider. It's not hard and you just need to prepare something software and hardware.

Notes

- Determine why and where to capture wireless traffic. To get quality wireless signal, try your best to get close to the object that you want to monitor wireless traffic from.
- Install wireless monitoring software on your pc or laptop. You can find lots of wireless traffic sniffer tools on the web. And lots of them are freeware.
- Prepare a wireless adapter. Some wireless monitor tools require specific wireless adapter or specific driver. So you may need to get one wireless adapter for your wireless traffic monitor software.
- Get wireless security key for the wireless network if it uses encryption. It's often that wireless networks implement encryption for security purposes. So you need the key for the wireless traffic monitor software to decode the wireless data.

13.3.2 Additional Equipment

Because wireless traffic transmits in air, it's helpful if you have better equipment to perform wireless traffic monitoring. Equipment that may be useful for wireless traffic monitoring includes:

- a wireless network card supports 802.11a, b, g, n
- an omni-directional antenna
- a high-gain yagi directional antenna
- pigtail cables for the yagi and omni-directional antenns
- a USB GPS adapter

13.4 Unauthorized Access

The modes of unauthorised access to links, to functions and to data is as variable as the respective entities make use of program code. There does not exist a full scope model of such threat. To some extent the prevention relies on known modes and methods of attack and relevant methods for suppression of the applied methods. However, each new mode of operation will create new options of threatening. Hence prevention requires a steady drive for improvement. The described modes of attack are just a snapshot of typical methods and scenarios where to apply.

- ***Non-traditional networks:*** Non-traditional networks such as personal network Bluetooth devices are not safe from cracking and should be regarded as a security risk. Even barcode readers, handheld PDAs, and wireless printers and copiers should be secured. These non-traditional networks can be easily overlooked by IT personnel who have narrowly focused on laptops and access points.
- ***Identity theft (MAC spoofing):*** Identity theft (or MAC spoofing) occurs when a cracker is able to listen in on network traffic and identify the MAC address of a computer with network privileges. Most wireless systems allow some kind of MAC filtering to allow only authorized computers with specific MAC IDs to gain access and utilize the network. However, programs exist that have network "sniffing" capabilities. Combine these programs with other software that allow a computer to pretend it has any MAC address that the cracker desires, and the cracker can easily get around that hurdle.

  MAC filtering is effective only for small residential (SOHO) networks, since it provides protection only when the wireless device is "off the air". Any 802.11 device "on the air" freely transmits its unencrypted MAC address in its 802.11 headers, and it requires no special equipment or software to detect it. Anyone with an 802.11 receiver (laptop and wireless adapter) and a freeware wireless packet analyzer can obtain the MAC address of any transmitting 802.11 within range. In an organizational environment, where most wireless

Notes

devices are "on the air" throughout the active working shift, MAC filtering provides only a false sense of security since it prevents only "casual" or unintended connections to the organizational infrastructure and does nothing to prevent a directed attack.

- ***Network injection:*** In a network injection attack, a cracker can make use of access points that are exposed to non-filtered network traffic, specifically broadcasting network traffic such as "Spanning Tree" (802.1D), OSPF, RIP, and HSRP. The cracker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs. A whole network can be brought down in this manner and require rebooting or even reprogramming of all intelligent networking devices.
- ***Caffe Latte attack:*** The Caffe Latte attack is another way to defeat WEP. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client. By sending a flood of encrypted ARP requests, the assailant takes advantage of the shared key authentication and the message modification flaws in 802.11 WEP. The attacker uses the ARP responses to obtain the WEP key in less than 6 minutes.

Self-Assessment

Fill in the blanks:

1. ..... is an attack on the integrity of either the data transmission or on the data stored on a system.
2. ..... is when a user denies having performed an action on the network
3. Non-traditional networks such as personal network Bluetooth devices are not safe from cracking and should be regarded as a ..... risk.
4. Identity theft (or MAC spoofing) occurs when a .....is able to listen in on network traffic and identify the MAC address of a computer with network privileges.
5. ..... is effective only for small residential (SOHO) networks, since it provides protection only when the wireless device is "off the air".
6. In a network .....attack, a cracker can make use of access points that are exposed to non-filtered network traffic.

13.5 Middle Attacks

A man-in-the-middle attacker entices computers to log into a computer which is set up as a soft AP (Access Point). Once this is done, the hacker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent hacking computer to the real network. The hacker can then sniff the traffic. One type of man-in-the-middle attack relies on security faults in challenge and handshake protocols to execute a "de-authentication attack". This attack forces AP-connected computers to drop their connections and reconnect with the cracker's soft AP (disconnects the user from the modem so they have to connect again using their password which you can extract from the recording of the event). Man-in-the-middle attacks are enhanced by software such as LANjack and AirJack which automate multiple steps of the process, meaning what once required some skill can now be done by script kiddies. Hotspots are particularly vulnerable to any attack since there is little to no security on these networks.

13.5.1 Address Resolution Protocol (ARP) Poisoning

Address Resolution Protocol (ARP) poisoning is a type of attack where the Media Access Control (MAC) address is changed by the attacker. Also, called an ARP spoofing attacks, it is effective

Notes

against both wired and wireless local networks. Some of the things an attacker could perform from ARP poisoning attacks include stealing data from the compromised computers, eavesdrop using man-in-the middle methods, and prevent legitimate access to services, such as Internet service.

A MAC address is a unique identifier for network nodes, such as computers, printers, and other devices on a LAN. MAC addresses are associated to network adapter that connects devices to networks. The MAC address is critical to locating networked hardware devices because it ensures that data packets go to the correct place. ARP tables, or cache, are used to correlate network devices' IP addresses to their MAC addresses.

In for a device to be able to communicate with another device with a known IP Address but an unknown MAC address the sender sends out an ARP packet to all computers on the network. The ARP packet requests the MAC address from the intended recipient with the known IP address. When the sender receives the correct MAC address then is able to send data to the correct location and the IP address and corresponding MAC address are store in the ARP table for later use.

ARP poisoning is when an attacker is able to compromise the ARP table and changes the MAC address so that the IP address points to another machine. If the attacker makes the compromised device's IP address point to his own MAC address then he would be able to steal the information, or simply eavesdrop and forward on communications meant for the victim. Additionally, if the attacker changed the MAC address of the device that is used to connect the network to Internet then he could effectively disable access to the web and other external networks.

13.6 Denial of Service (DoS) Attack

A Denial-of-Service attack (DoS) occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These cause legitimate users to not be able to get on the network and may even cause the network to crash. These attacks rely on the abuse of protocols such as the Extensible Authentication Protocol (EAP).

The DoS attack in itself does little to expose organizational data to a malicious attacker, since the interruption of the network prevents the flow of data and actually indirectly protects data by preventing it from being transmitted. The usual reason for performing a DoS attack is to observe the recovery of the wireless network, during which all of the initial handshake codes are re-transmitted by all devices, providing an opportunity for the malicious attacker to record these codes and use various "cracking" tools to analyze security weaknesses and exploit them to gain unauthorized access to the system. This works best on weakly encrypted systems such as WEP, where there are a number of tools available which can launch a dictionary style attack of "possibly accepted" security keys based on the "model" security key captured during the network recovery.

13.6.1 Types of Denial of Service (DoS) Attacks

The most common type of Denial of Service attack involves flooding the target resource with external communication requests. This overload prevents the resource from responding to legitimate traffic, or slows its response so significantly that it is rendered effectively unavailable.

Resources targeted in a DoS attack can be a specific computer, a port or service on the targeted system, an entire network, a component of a given network any system component. DoS attacks may also target human-system communications (e.g. disabling an alarm or printer), or human-response systems (e.g. disabling an important technician's phone or laptop).

Notes

DoS attacks can also target tangible system resources, such as computational resources (bandwidth, disk space, processor time); configuration information (routing information, etc.); state information (for example, unsolicited TCP session resetting). Moreover, a DoS attack can be designed to: execute malware that maxes out the processor, preventing usage; trigger errors in machine microcode or sequencing of instructions, forcing the computer into an unstable state; exploit operating system vulnerabilities to sap system resources; crash the operating system altogether.

The overriding similarity in these examples is that, as a result of the successful Denial of Service attack, the system in question does not respond as before, and service is either denied or severly limited.

13.6.2 Distributed Denial of Service (DDoS) Attacks

A DDOS attack (better known as a Distributed Denial of Service attack) is a type of web attack that seeks to disrupt the normal function of the targeted computer network. This is any type of attack that attempts to make this computer resource unavailable to its users. While this type of attack typically follows the same sorts of patterns, the definition of the term Distributed Denial of Service does not make any specific indications of how this type of attack is to be pulled off. What makes this type of attack "distributed" is the concerted efforts between a large number of disruptors all for the common goal of preventing web servers (and therefore websites) from functioning effectively at all. These users may be willing participants, or in some cases be tricked into downloading software that will use their terminal to aid in the offensive. All in all, regardless of the means, a DDOS attack is simply a combined effort to prevent computer systems from working as well as they should, typically from a remote location over the internet.

The most common method of attack is to send a mass saturation of incessant requests for external communication to the target. These systems are flooded with requests for information from non-users, and often non-visitors to the website. The goal of this attack is to create a large enough presence of false traffic such that legitimate web traffic intended for actual web users is slowed down and delayed. If this type of service becomes too slow, time sensitive information such as live video footage may be rendered entirely useless to legitimate end users.

For a DDOS to work effectively, the process has to be heavily automated on the attacker's end. Customized software is designed to flood these services with false traffic, and is run on as many computers as possible. There are a few instances in which this type of software was set up like a virus, infecting computers and taking control of their communication functions. These users unwillingly are aiding in a DDOS attack, sometimes without being the slightest bit aware of it. If there seems to be large delays in normal internet service, there may be outbound requests being made consuming your internet connections given throughput, and can sometimes be an indication of foul play. Users seeking to limit this risk should keep anti-virus software up to date, and scan frequently for these types of programs.

While there are few court cases on the books of Distributed Denial of Service perpetrators being held accountable for their actions, as well as the potential lost income for commercial websites, this type of activity almost always violates the terms of service and acceptable use policies of internet service providers, as well as often violating individual communication law within the nation. These types of attacks have become more and more prevalent as time goes on, and in many nation legislation is in the works, with hopes of criminal penalties for those involved with this sort of attack.

All in all, a DDOS attack is a very real threat to businesses and organizations across the world, and it's important that they be prepared in case some group of people decides to cause trouble for your organization. Being prepared to identify these types of threats is an important part of proper internet use, and should be a part of your daily life online.

Notes

13.7 Protective Actions

The various protective actions are as ollows:

13.7.1 Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standard ratified in September 1999, its intention was to provide data confidentiality comparable to that of a traditional wired network. WEP, recognizable by the key of 10 or 26 hexadecimal digits, is widely in use and is often the first security choice presented to users by router configuration tools.

Although its name implies that it is as secure as a wired connection, WEP has been demonstrated to have numerous flaws and has been deprecated in favour of newer standards such as WPA2. In 2003 the Wi-Fi Alliance announced that WEP had been superseded by Wi-Fi Protected Access (WPA). In 2004, with the ratification of the full 802.11i standard (i.e. WPA2), the IEEE declared that both WEP-40 and WEP-104 "have been deprecated as they fail to meet their security goals

WEP was included as the privacy component of the original IEEE 802.11 standard ratified in September 1999.[citation needed]WEP uses the stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity. It was deprecated in 2004 and is documented in the current standard.

Standard 64-bit WEP uses a 40 bit key (also known as WEP-40), which is concatenated with a 24-bit initialization vector (IV) to form the RC4 key. At the time that the original WEP standard was drafted, the U.S. Government's export restrictions on cryptographic technology limited the key size. Once the restrictions were lifted, manufacturers of access points implemented an extended 128-bit WEP protocol using a 104-bit key size (WEP-104).

A 64-bit WEP key is usually entered as a string of 10 hexadecimal(base 16) characters (0-9 and A-F). Each character represents four bits, 10 digits of four bits each gives 40 bits; adding the 24-bit IV produces the complete 64-bit WEP key. Most devices also allow the user to enter the key as five ASCII characters, each of which is turned into eight bits using the character's byte value in ASCII; however, this restricts each byte to be a printable ASCII character, which is only a small fraction of possible byte values, greatly reducing the space of possible keys.

A 128-bit WEP key is usually entered as a string of 26 hexadecimal characters. Twenty-six digits of four bits each gives 104 bits; adding the 24-bit IV produces the complete 128-bit WEP key. Most devices also allow the user to enter it as 13 ASCII characters.

A 256-bit WEP system is available from some vendors. As with the other WEP-variants 24 bits of that is for the IV, leaving 232 bits for actual protection. These 232 bits are typically entered as 58 hexadecimal characters. ((58 × 4 bits =) 232 bits) + 24 IV bits = 256-bit WEP key.

13.7.2 Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, WEP (Wired Equivalent Privacy).

WPA (sometimes referred to as the draft IEEE 802.11i standard) became available in 2003. The Wi-Fi Alliance intended it as an intermediate measure in anticipation of the availability of the more secure and complex WPA2. WPA2 became available in 2004 and is a common shorthand for the full IEEE 802.11i (or IEEE 802.11i-2004) standard.

Notes

Notes A flaw in a feature added to Wi-Fi, called Wi-Fi Protected Setup, allows WPA and WPA2 security to be bypassed and effectively broken in many situations. WPA and WPA2 security implemented without using the Wi-Fi Protected Setup feature are unaffected by the security vulnerability.

A flaw in a feature added to Wi-Fi, called Wi-Fi Protected Setup, allows WPA and WPA2 security to be bypassed and effectively broken in many situations. WPA and WPA2 security implemented without using the Wi-Fi Protected Setup feature are unaffected by the security vulnerability.

WPA and WPA 2

The Wi-Fi Alliance intended WPA as an intermediate measure to take the place of WEP pending the availability of the full IEEE 802.11i standard. WPA could be implemented through firmware upgrades on wireless network interface cards designed for WEP that began shipping as far back as 1999. However, since the changes required in the wireless access points (APs) were more extensive than those needed on the network cards, most pre-2003 APs could not be upgraded to support WPA.

The WPA protocol implements much of the IEEE 802.11i standard. Specifically, the Temporal Key Integrity Protocol (TKIP), was adopted for WPA. WEP used a 40-bit or 104-bit encryption key that must be manually entered on wireless access points and devices and does not change. TKIP employs a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP.

WPA also includes a message integrity check. This is designed to prevent an attacker from capturing, altering and/or resending data packets. This replaces the cyclic redundancy check (CRC) that was used by the WEP standard. CRC's main flaw was that it did not provide a sufficiently strong data integrity guarantee for the packets it handled. Well tested message authentication codes existed to solve these problems, but they required too much computation to be used on old network cards. WPA uses a message integrity check algorithm called Michael to verify the integrity of the packets. Michael is much stronger than a CRC, but not as strong as the algorithm used in WPA2. Researchers have since discovered a flaw in WPA that relied on older weaknesses in WEP and the limitations of Michael to retrieve the keystream from short packets to use for re-injection and spoofing.

WPA2 has replaced WPA. WPA2, which requires testing and certification by the Wi-Fi Alliance, implements the mandatory elements of IEEE 802.11i. In particular, it introduces CCMP, a new AES-based encryption mode with strong security. Certification began in September, 2004; from March 13, 2006, WPA2 certification is mandatory for all new devices to bear the Wi-Fi trademark

13.7.3 Virtual Private Network (VPN)

A virtual private network (VPN) extends a private networkacross a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

A VPN connection across the Internet is similar to a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from the private network.

Notes

VPNs allow employees to securely access their company's intranet while traveling outside the office. Similarly, VPNs securely and cost effectively connect geographically disparate offices of an organization creating one cohesive virtual network. VPN technology is also used by ordinary Internet to connect toproxy servers for the purpose of protecting one's identity.

Caution To prevent disclosure of private information, VPNs typically allow only authenticated remote access and make use of encryption techniques.

VPNs provide security by the use of tunneling protocols and through security procedures such as encryption. The VPN security model provides:

- confidentiality such that even if the network traffic is sniffed at the packet level (see network sniffer and Deep packet inspection), an attacker would only see encrypted data
- sender authentication to prevent unauthorized users from accessing the VPN.
- message integrity to detect any instances of tampering with transmitted messages

Secure VPN protocols include the following:

- Internet Protocol Security (IPsec) as initially developed by the Internet Engineering Task Force (IETF) for IPv6, which was required in all standards-compliant implementations of IPv6 before RFC 6434 made it only a recommendation. This standards-based security protocol is also widely used with IPv4 and the Layer 2 Tunneling Protocol. Its design meets most security goals: authentication, integrity, and confidentiality. IPsec uses encryption, encapsulating an IP packet inside an IPsec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.
- Transport Layer Security (SSL/TLS) can tunnel an entire network's traffic (as it does in the OpenVPN project) or secure an individual connection. A number of vendors provide remote-access VPN capabilities through SSL. An SSL VPN can connect from locations where IPsec runs into trouble with Network Address Translation and firewall rules.
- Datagram Transport Layer Security (DTLS) - used in Cisco Any Connect VPN and in OpenConnect VPN[9] to solve the issues SSL/TLS has with tunneling over UDP.
- Microsoft Point-to-Point Encryption (MPPE) works with the Point-to-Point Tunneling Protocol and in several compatible implementations on other platforms.
- Microsoft Secure Socket Tunneling Protocol (SSTP) tunnels Point-to-Point Protocol (PPP) or Layer 2 Tunneling Protocol traffic through an SSL 3.0 channel.
- Multi Path Virtual Private Network (MPVPN). Ragula Systems Development Company owns the registered trademark "MPVPN".

Secure Shell (SSH) VPN – Open SSH offers VPN tunneling (distinct from port forwarding) to secure remote connections to a network or to inter-network links. Open SSH server provides a limited number of concurrent tunnels. The VPN feature itself does not support personal authentication.

Self-Assessment

Fill in the blanks:

7. A ..... attacker entices computers to log into a computer which is set up as a soft AP
8. ..... poisoning is a type of attack where the Media Access Control (MAC) address is changed by the attacker.

Notes

9. A ..... is a type of web attack that seeks to disrupt the normal function of the targeted computer network.

10. Wired Equivalent Privacy (WEP) is a security algorithm for ..... wireless networks.

11. Twenty-six digits of four bits each gives 104 bits; adding the 24-bit IV produces the complete ..... WEP key.

12. ..... allow employees to securely access their company's intranet while traveling outside the office.

Case Study **Wireless Network Security**

With the explosion in "WiFi" wireless networks, a new and very real threat to companies has emerged, against which most are as yet unprotected. Many organisations are introducing this new and very useful technology to their networks without fully understanding the security implications.

What are the dangers?

Recent intruder activities such as "warchalking" and "wardriving" have captured the media's attention and increased awareness of wireless network security risks. These risks are basically:

1. Unauthorised use of your internet connection

   Alongside the enormous growth in WiFi, there is a broadband revolution going on. This means that fast internet connections could be used by intruders, causing excess traffic and overloading of your service.

2. Unauthorised access to your internal servers and confidential data

   Given enough time, an intruder could work out your computer passwords and gain access to your data.

3. An intruder reading the network traffic as it flows across the network

By using a WiFi listening tool, an intruder can listen in on network traffic. When a document is viewed from across the network, the intruder can see that information. This requires sophisticated software and some expertise on the part of the intruder, but is still a real danger.

Making your wireless network more secure

The designers of WiFi have incorporated measures to prevent intruders from gaining access to your wireless network. Depending on your specific requirements, you can use some or all of them. The main measures are as follows:

1. Introducing access lists

   Each WiFi card has a unique identification number. Most WiFi networks have a list of allowed cards. Adding only your cards will stop an intruder's card from accessing your WiFi network.

2. Using encryption

   A basic encryption is available in WiFi. Using this will stop an intruder from accessing your wireless network in the short term. It will also stop a casual intruder from seeing data on your network.

Contd...

Notes

3. Hiding your network

   Most access points broadcast their WiFi name. This name is used to access a wireless network. Turning this feature off stops the WiFi network from drawing attention to itself. There are some further precautions you might consider taking, such as:

4. Monitoring WiFi traffic

   Software is now available to allow a WiFi network owner to monitor cards that have access to the network. This can alert the network owner if an intruder gains access.

5. Implementing secure VPN for wireless users

For near impenetrability, a WiFi owner can introduce another level of security between the wireless network and the standard wired network. This is a costly exercise really only implemented on networks that contain particularly confidential and sensitive data.

Risks versus benefits of wireless

Wireless is a very flexible, cheap, highly useful and desirable new technology. There are very good reasons to implement it on your network. However, because it can offer intruders an entry point, you need to understand and guard against the dangers. Bridge Partners can help you weigh the benefits of wireless against the risks, and to manage these risks in line with your own security needs. By implementing some of the measures described here, you can greatly reduce the risk of a security breach and still enjoy the many benefits of WiFi.

Questions:

1. Study and analyse the case.
2. Write down the case facts.
3. What do you infer from it?

Source: http://www.bridgepartners.co.uk/wireless-network-security

13.8 Summary

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).

The risks to users of wireless technology have increased as the service has become more popular.

Wireless networking is inherently risky because you are transmitting information via radio waves. Data from your wireless network can be intercepted just like signals from your cellular or cordless phones.

The modes of unauthorised access to links, to functions and to data is as variable as the respective entities make use of program code.

Non-traditional networks such as personal network Bluetooth devices are not safe from cracking and should be regarded as a security risk.

Address Resolution Protocol (ARP) poisoning is a type of attack where the Media Access Control (MAC) address is changed by the attacker. Also, called an ARP spoofing attacks, it is effective against both wired and wireless local networks.

Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11wireless networks.

Notes

Although its name implies that it is as secure as a wired connection, WEP has been demonstrated to have numerous flaws and has been deprecated in favor of newer standards such as WPA2.

A virtual private network (VPN) extends a private network across a public network, such as the Internet.

VPNs allow employees to securely access their company's intranet while traveling outside the office.

VPNs provide security by the use of tunneling protocols and through security procedures such as encryption.

13.9 Keywords

Address Resolution Protocol (ARP): poisoning is a type of attack where the Media Access Control (MAC) address is changed by the attacker.

Denial-Of-Service (DOS): occurs when an adversary causes a system or a network to become unavailable to legitimate users or causes services to be interrupted or delayed.

Distributed Denial of Service attack): is a type of web attack that seeks to disrupt the normal function of the targeted computer network.

Identity theft: (or MAC spoofing) occurs when a cracker is able to listen in on network traffic and identify the MAC address of a computer with network privileges.

Manipulation: means that data has been inserted, deleted, or otherwise modified on a system or during transmission.

Masquerading: refers to the act of an adversary posing as a legitimate user in order to gain access to a wireless network or a system served by the network.

Repudiation: is when a user denies having performed an action on the network.

Virtual private network (VPN): extends a private networkacross a public network, such as the Internet.

Wired Equivalent Privacy (WEP): is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standard ratified in September 1999, its intention was to provide data confidentiality comparable to that of a traditional wired network.

Wireless security: is the prevention of unauthorized access or damage to computers using wireless networks

13.10 Review Questions

13. Describe denial of service.
14. Describe the concept of security threats
15. Explain the need for wireless security
16. Explain the procedure of traffic monitoring
17. What are the various types of protective actions?
18. What do you mean by unauthorized access
19. What is middle attacks?

Notes

Answers: Self-Assessment

1. Manipulation
2. Repudiation
3. Security
4. Cracker
5. MAC filtering
6. Injection
7. man-in-the-middle
8. Address Resolution Protocol (ARP)
9. Distributed Denial of Service attack
10. IEEE 802.11
11. 128-bit
12. VPNs

13.11 Further Readings

Books

802.11 Wireless Networks: The Definitive Guide, Second Edition, Matthew Gast

Introduction to wireless networks, John Ross

Wireless Communications & Networking, Vijay Garg

Wireless Communications: Principles and Practice, Theodore S. Rappaport

Online links

http://whatismyipaddress.com/ddos-attack

http://www.incapsula.com/ddos/ddos-attacks/denial-of-service

http://www.computer-network-security-training.com/what-is-arp-poisoning/