Wireless Networks Security

Prepared for
Dr. Wibowo
IFMG 250

Submitted by
Joshua Muscatello
Joshua Martin

April 20, 2005

I. Introduction
II. Major Networking Hardware Components
    a. Network Interface Cards
    b. Modems
    c. Routers
    d. Hubs
    e. Switches
    f. Access Points
    g. Print Server
II. Wired Networks
    a. Definition
    b. Types
    c. Range
    d. Benefit
III. Wireless Networks
    a. Definition
    b. Types
    c. Transmission Standards
    d. Range
    e. Benefit
IV. Wired Networks vs. Wireless Networks
    a. Mobility
    b. Cost
    c. Range
    d. Speed
    e. Security
V. Wireless Network Security
    a. What is at Risk?
        i. Confidentiality
        ii. Integrity
        iii. Availability
    b. Intrusion Methods
        i. Trojan Horse
        ii. Denial of Service (DOS)
        iii. Email Spoofing
        iv. Email-Borne Viruses
        v. Packet Sniffing
    c. Preventative Methods
        i. Firewalls
        ii. Encryption
        iii. Anti-virus Applications
        iv. Anti Spy ware applications
VI. Conclusion

Abstract

As technology advances in society the need for wired and wireless networking has become essential. Each of these types of networking has their advantages and disadvantages according to security. Wired networking has different hardware requirements and the range and benefits are different. Wireless networking takes into consideration the range, mobility, and the several types of hardware components needed to establish a wireless network. As you read on you will understand different types of configurations of networks and the security measures that need to be taken to ensure a secure network.

Introduction

Organizations rely heavily on the ability to share information throughout the organization in an efficient and productive manner. Computer networks have allowed for this technology and are now apart of almost every business. An organization has two options when it comes to setting up a network. They can use a completely wired network, which uses networking cable to connect computers, or they can use a wireless network, which uses radio frequencies to connect computer. Wireless networks have allowed organizations to become more mobile; therefore, organizations are now using a combination of both wired and wireless networks.

They basic hardware layout for the two types of networks are fairly similar but for an organization to go wireless it requires a few more hardware components. Although networks provide convenience they do open the organization up to security and privacy risks. If a company is faced with a security they are ways that they can fix and prevent future security risks. As you read on, you will learn how the network has become an essential part of today's organizations.

Hardware Components

Before one can begin to setup a network they must first be sure they have a network interface card, commonly referred to as a NIC. A NIC is a device that connects a computer or other device to a network. For computers, the NIC is usually installed in an expansion slot and has a chip that handles the physical and data-link layers of network communications. (Cert.org/Tech)

To establish your network you will need a few key components. If you plan to access the internet you will start your network off with a cable modem. This type of modem is designed to operate using your existing cable lines. Cable internet has a high bandwidth and can support most, if not, all applications you will be using. The second component is a router. A router is a device that routes data from one network to another network. A router is connected to at least two networks, commonly two networks or a network and its ISP's network. A router allows for everyone on the network to access the internet.(Webopedia.com)

The next component that you will need to setup a network is a hub or sometimes a switch. A hub is a device that connects the cables from computers and other devices such as printers in a network. Traditionally, hubs are used for star topology networks, but they are often used with other configurations to make it easy to add and remove computers without bringing down the network. (Webopedia.com) A hub can be either active or passive; simply forwarding messages or amplifying or refreshing the data. A switch is a device similar to a hub that enables the connection of multiple computers, access points, and other network enabled devices. The difference between a hub and a switch is that a switch filters the data that passes through it and a hub does not.

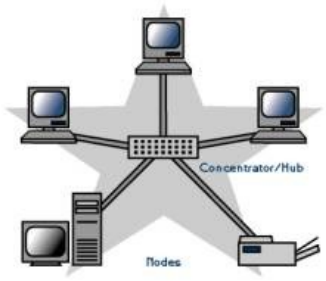
These components have all been modified and are capable of establishing wireless networks. A router can be purchased with wireless capability but a more efficient way of adding wireless to your network is to simply add wired access points. An access point will bride a wired network with a wireless network and can be hard wired in to your

existing system. (Wi-Fiplanet.com) This option allows for the mobility of a wireless network.

Another key component is a print server. A print server is used to connect printers to a network to allow for network printing. The server will act as a buffer; storing the messaging and printing them in order of the queue. This device can drastically reduce the cost of networking because now everyone can use the same printer without having a printer attached to every computer.

Wired Networks

Wired networks, also called Ethernet networks, are the most common type of local area network (LAN) technology. A wired network is simply a collection of two or more computers, printers, and other devices linked by Ethernet cables. Ethernet is the fastest wired network protocol, with connection speeds of 10 megabits per second (Mbps) to 100 Mbps or higher.

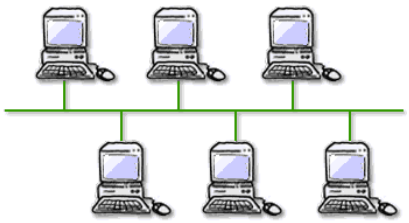


Wired networks can also be used as part of other wired and wireless networks. To connect a computer to a network with an Ethernet cable, the computer must have an Ethernet adapter (sometimes called a network interface card, or NIC). Ethernet adapters can be internal (installed in a computer) or external (housed in a separate case). Some computers include a built-in Ethernet adapter port, which eliminates the need for a separate adapter (Microsoft). There are three basic network topologies that are most commonly used today. (Homenthelp.com)

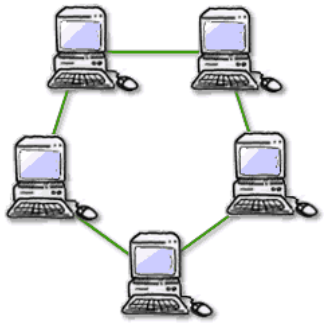
The star network, a general more simplistic type of topology, has one central hub that connects to three or more computers and the ability to network printers. This type can be used for small businesses and even home networks. The star network is very useful for applications where some processing must be centralized and some must be performed locally. The major disadvantage is the star network is its vulnerability. All

data must pass through one central host computer and if that host fails the entire network will fail.

On the other hand the bus network has no central computer and all computers are linked on a single circuit. This type broadcasts signals in all directions and it uses special software to identify which computer gets what signal. One disadvantage with this type of network is that only one signal can be sent at one time, if two signals are sent at the same time they will collide and the signal will fail to reach its destination. One advantage is that there is no central computer so if one computer goes down others will not be affected and will be able to send messages to one another. (Laudon)



The third type of network is the ring network. Similar to the bus network, the ring network does not rely on a central host computer either. Each computer in the network can communicate directly with any other computer, and each processes its own applications independently. A ring network forms a closed loop and data is sent in one direction only and if a computer in the network fails the data is still able to be transmitted.



Typically the range of a wired network is within a 2,000-foot-radius. The disadvantage of this is that data transmission over this distance may be slow or nonexistent. The benefit of a wired network is that bandwidth is very high and that interference is very limited through direct connections. Wired networks are more secure and can be used in many situations; corporate LANs, school networks and hospitals. The biggest drawback to this type of network is that it must be rewired every time it is moved. (Laudon)

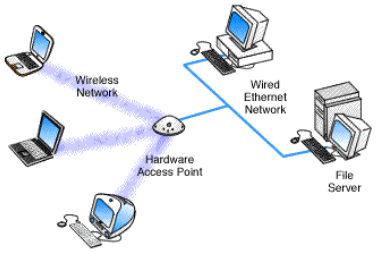
Wireless Networks

A wireless network, which uses high-frequency radio waves rather than wires to communicate between nodes, is another option for home or business networking. Individuals and organizations can use this option to expand their existing wired network or to go completely wireless. Wireless allows for devices to be shared without networking cable which increases mobility but decreases range. There are two main types of wireless networking; peer to peer or ad-hoc and infrastructure. (Wi-fi.com)

An ad-hoc or peer-to-peer wireless network consists of a number of computers

each equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless enabled computers. They can share files and printers this way, but may not be able to access wired LAN resources, unless one of the computers acts as a bridge to the wired LAN using special software.

An infrastructure wireless network consists of an access point or a base station. In this type of network the access point acts like a hub, providing connectivity for the wireless computers. It can connect or bridge the wireless LAN to a wired LAN, allowing wireless computer access to LAN resources, such as file servers or existing Internet Connectivity. (compnetworking.about.com)



There are four basic types of transmissions standards for wireless networking. These types are produced by the Institute of Electrical and Electronic Engineers (IEEE). These standards define all aspects of radio frequency wireless networking. They have established four transmission standards; 802.11, 802.11a, 802.11b, 802.11g.

The basic differences between these four types are connection speed and radio frequency. 802.11 and 802.11b are the slowest at 1 or 2 Mbps and 5.5 and 11Mbps respectively. They both operate off of the 2.4 GHz radio frequency. 802.11a operates off of a 5 GHz frequency and can transmit up to 54 Mbps and the 802.11g operates off of the 2.4 GHz frequency and can transmit up to 54 Mbps. Actual transmission speeds vary

depending on such factors as the number and size of the physical barriers within the network and any interference in the radio transmissions. (Wi-fi.com)

Wireless networks are reliable, but when interfered with it can reduce the range and the quality of the signal. Interference can be caused by other devices operating on the same radio frequency and it is very hard to control the addition of new devices on the same frequency. Usually if your wireless range is compromised considerably, more than likely, interference is to blame. (Laudon)

A major cause of interference with any radio signals are the materials in your surroundings, especially metallic substances, which have a tendency to reflect radio signals. Needless to say, the potential sources of metal around a home are numerous--things like metal studs, nails, building insulation with a foil backing and even lead paint can all possibly reduce the quality of the wireless radio signal. Materials with a high density, like concrete, tend to be harder for radio signals to penetrate, absorbing more of the energy. Other devices utilizing the same frequency can also result in interference with your wireless. For example, the 2.4GHz frequency used by 802.11b-based wireless products to communicate with each other. Wireless devices don't have this frequency all to themselves. In a business environment, other devices that use the 2.4GHz band include microwave ovens and certain cordless phones. (Laundon)

On the other hand, many wireless networks can increase the range of the signal by using many different types of hardware devices. A wireless extender can be used to relay the radio frequency from one point to another without losing signal strength. Even though this device extends the range of a wireless signal it has some drawbacks. One drawback is that it extends the signal, but the transmission speed will be slowed.

There are many benefits to a wireless network. The most important one is the option to expand your current wired network to other areas of your organization where it would otherwise not be cost effective or practical to do so. An organization can also install a wireless network without physically disrupting the current workplace or wired

network. (Wi-Fi.org) Wireless networks are far easier to move than a wired network and adding users to an existing wireless network is easy. Organizations opt for a wireless network in conference rooms, lobbies and offices where adding to the existing wired network may be too expensive to do so.

Wired vs. Wireless Networking

The biggest difference between these two types of networks is one uses network cables and one uses radio frequencies. A wired network allows for a faster and more secure connection and can only be used for distances shorter than 2,000 feet. A wireless network is a lot less secure and transmission speeds can suffer from outside interference. Although wireless networking is a lot more mobile than wired networking the range of the network is usually 150-300 indoors and up to 1000 feet outdoors depending on the terrain. (Homelanextream.com)

The cost for wired networking has become rather inexpensive. Ethernet cables, hubs and switches are very inexpensive. Some connection sharing software packages, like ICS, are free; some cost a nominal fee. Broadband routers cost more, but these are optional components of a wired network, and their higher cost is offset by the benefit of easier installation and built-in security features.

Wireless gear costs somewhat more than the equivalent wired Ethernet products. At full retail prices, wireless adapters and access points may cost three or four times as much as Ethernet cable adapters and hubs/switches, respectively. 802.11b products have dropped in price considerably with the release of 802.11g. (Homelanextream.com)

Wired LANs offer superior performance. A traditional Ethernet connection offers only 10 Mbps bandwidth, but 100 Mbps Fast Ethernet technology costs a little more and is readily available. Fast Ethernet should be sufficient for file sharing, gaming, and high-speed Internet access for many years into the future. (Wi-Fi.org) Wired LANs utilizing hubs can suffer performance slowdown if computers heavily utilize the network

simultaneously. Use Ethernet switches instead of hubs to avoid this problem; a switch costs little more than a hub.

Wireless networks using 802.11b support a maximum bandwidth of 11 Mbps, roughly the same as that of old, traditional Ethernet. 802.11a and 802.11g LANs support 54 Mbps, that is approximately one-half the bandwidth of Fast Ethernet. Furthermore, wireless networking performance is distance sensitive, meaning that maximum performance will degrade on computers farther away from the access point or other communication endpoint. As more wireless devices utilize the 802.11 LAN more heavily, performance degrades even further. (Wi-Fi.org)

The greater mobility of wireless LANs helps offset the performance disadvantage. Mobile computers do not need to be tied to an Ethernet cable and can roam freely within the wireless network range. However, many computers are larger desktop models, and even mobile computers must sometimes be tied to an electrical cord and outlet for power. This undermines the mobility advantage of wireless networks in many organizations and homes.

For any wired network connected to the Internet, firewalls are the primary security consideration. Wired Ethernet hubs and switches do not support firewalls. However, firewall software products like Zone Alarm can be installed on the computers themselves. Broadband routers offer equivalent firewall capability built into the device, configurable through its own software.

In theory, wireless LANs are less secure than wired LANs, because wireless communication signals travel through the air and can easily be intercepted. The weaknesses of wireless security are more theoretical than practical. (Wi-Fi.org) Wireless networks protect their data through the Wired Equivalent Privacy (WEP) encryption standard that makes wireless communications reasonably as safe as wired ones.

No computer network is completely secure. Important security considerations for organizations tend to not be related to whether the network is wired or wireless but rather

ensuring that the firewall is properly configured, employees are aware of the dangers of spoof emails, they are away of spy ware and how to avoid and that anyone outside the organization does not have unauthorized access to the network.

Wireless Network Security

Network security is a big concern for individuals and organizations because vital information is stored on the network and most critical process of the business are done through the network. If a network is to fail or security is compromised an organization could be completely crippled. For example, if Wal-Mart was to lose their cash register network than they would suffer a huge loss of business and would take, depending on the severity of the breach, several hours to days to fix.

Also at risk is employee and client privacy. If an organization's network is hacked into they would have access to client databases as well as employee databases. The most important thing to keep in mind when it comes to wireless network security is keeping unauthorized users from accessing your network. The first step is to know your wireless network's range and to use specific software to grant access only to authorized users.

Trojan Horse

Intruders use several different ways of gaining access to your network. Some of the most common ones are Trojan horses, denial of service, e-mail spoofing, e-mail borne viruses and packet sniffing. A Trojan horse is a program that appears legitimate, but performs some illicit activity when it is run. It may be used to locate password information or make the system more vulnerable to future entry or simply destroy programs or data on the hard disk. A Trojan horse is similar to a virus, except that it does not replicate itself. It stays in the computer doing its damage or allowing somebody from

a remote site to take control of the computer. Trojans often sneak in attached to a free game or other utility.

Denial of Service (DoS)

Another common method of intrusion is denial of service (DoS). A DoS is a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Denial of Service attacks is termed one of the worst attacks and is next to impossible to track. Some things that can be done to reduce the risk of being stung by a denial of service attack include: (windowsecurity.com)

- Not running your servers at a level too close to capacity.
- Using packet filtering.
- Keeping up-to-date on security-related patches.

E-mail Borne Viruses

Email-borne viruses are another attempt people will use to gain entry or cripple your network. Email-borne viruses are viruses and malicious code that is sent as an attachment to an e-mail. The most important thing to remember is not to open any attachments without knowing the source. Most times even knowing the source isn't as safe. For example, the Melissa Virus was spread by sending to people in your own address book. It spread quickly because people were getting emails from people they knew and trusted. (BlackBox.com) Ways to avoid e-mail borne viruses is to:

- Never run a program unless you know it to be authored by a person or company your trust.

- Don’t send programs to your friends simply because they are amusing – they may contain e-mail borne viruses or malicious code.

Packet Sniffing

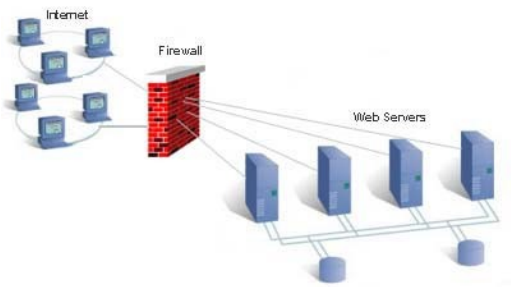
A packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names and passwords that travel over the network in clear text. With perhaps hundreds or thousands of passwords captured by the packet sniffer, intruders can launch widespread attacks on systems. Installing a packet sniffer does not necessarily require administrator-level access. (windowssecurity.com)

Cable modem users have a higher risk of exposure to packet sniffers since entire neighborhoods of cable modem users are effectively part of the same network. A packet sniffer installed on any cable modem user's computer in a neighborhood may be able to capture data transmitted by any other cable modem in the same neighborhood. This same concept applies to anyone who is attempting to access your wireless network without permission. If they have these types of files installed on their computer it is most likely going to affect your network.

Preventative Methods

Individuals and organizations can take preventative methods to avoid intrusions. Organizations first step is to protect their valuable information. Their first line of defense is a firewall. A firewall is a number of security schemes that prevents unauthorized users from gaining access to a computer network or a firewall could be used to monitor transfers of information to and from a network.

Firewalls come in a wide variety of forms. Routers come complete with a built-in firewall and can be used for home networking. Several companies make more powerful,



external firewalls which can be used with corporate networks. Firewalls are very effective at preventing attacks and the cost for a firewall is definitely offset by the benefit and security it provides.

Encryption

Organizations can use encryption to transform data into a hard to interpret form. This allows businesses to transmit data over their networks in a secure way and even if a person were to intercept the data they wouldn't be able to interpret anyway. Companies will use encryption to protect confidentiality, integrity and authenticity. One business that uses encryption is H&R Block. There are times when a customer's income tax return must be saved to a diskette for transfer or edit purposes. These files are encrypted and can only be interpreted by H&R Block software. (foundstone.com)

Anti-virus Software

An anti-virus program is a utility that searches a hard disk for viruses and removes any that are found. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. Examples of this type of software are Norton Anti-virus, McAfee Anti-virus and AVG virus protection. (windowssecurity.com)

Anti-virus software is an essential utility for organizations to have to prevent viruses from infecting their network. Current anti-virus programs have on-demand file scanning which means that every time you access a file it is scanned for a virus. I have tested many anti-virus utilities and have found the AVG anti-virus is the most efficient at getting the job done. This utility is free for individuals and a reasonable cost for organizations.

Anti-Spyware Applications

To understand spyware applications you must first understand what spyware is. Spyware consists of computer software that gathers and reports information about a computer user without the user's knowledge or consent. A network can be infiltrated with spyware when an employee visits a website using the network's internet connection. Spyware can go undetected or can be very bothersome to the user. Most often times their will be pop-up ads, unwanted programs and most importantly the network will suffer a huge decrease in performance. (Interhack.net)

Spyware has become very popular and many applications have been created to prevent such computer abuse. One example is Lavasoft's AdAware. This program scans your computer's hard drive for spyware and deletes them from the system. This is a very effective program along with Spybot Search & Destroy. This program is very similar but offers a real time protection utility that can find and delete spyware on demand. (Interhack.com)

Conclusion

Wired and Wireless networks are very common in the workplace as well as in the home. Technology has been created to store, transmit and receive data through networks at very high rates of speed. Networks have become essential to completing daily business tasks and most business, those who rely heavily on information technologies, would be crippled without their networks.

Advances in networking storage have allowed for organizations to use their networks not only for the sharing of resources but to store large pools of data to be used for data analysis. Companies can now store detailed profile information for customers at a very low cost. In the future, the speed of networks will increase as they have in past years. The cost of networks will continue to decline and using a network will be essential for every organization. As computing technology increases in power, and decreases in size, the price of creating a high-powered full featured network will decrease rapidly.

Works Cited

http://www.homelanxtreme.com/wired-vs-wireless.htm

http://www.vicomsoft.com/knowledge/reference/wireless1.html#6

http://www.cert.org/tech_tips/home_networks.html#introduction

http://www.pcstats.com/articleview.cfm?articleID=1489

http://compnetworking.about.com/od/wirelesssecurity/

http://www.microsoft.com/hardware/broadbandnetworking/10_concept_what_is_wireless.mspx

http://www.infotel-systems.com/wireless%20networking%20outline.htm

http://www.homenethelp.com/web/diagram/index.asp

http://www.windowsecurity.com/articles/Wireless-Networks-Surpassed-Security-Wired-Networks.html

http://whatis.techtarget.com/definitionsCategory/0,289915,sid9_tax1681,00.html

http://www.wi-fi.org/OpenSection/wireless_vs_wired.asp?TID=2

http://www.wi-fiplanet.com/tutorials/article.php/1494241

http://www.blackbox.com/tech_docs/tech_overviews/wiredwireless.html

http://www.designshare.com/Research/Wired/Wired2.htm