

## **Networking and Security**

### Team

Matthew Drowser

Phil Mulcahy

Rich Mock

### Instructor

Michael Manojlovich

May 07, 2008

## **Introduction**

The current worldwide community relies more on an e-commerce culture dominated by electronic devices and communications. Computer networks continue to grow at an explosive rate. Not that long ago few people had access to a network. Today, networking, network security and privacy are terms people are becoming more and more familiar with in regards to their wide range of usage of Information Technology solutions – from social networking, downloading your favorite music, buying consumer products on-line to balancing your check book or scheduling your car for service at a local dealership. This paper will discuss some important concepts associated with networking and security associated with information technology solutions.

## **Information Technology**

Before we get started, it is important to understand what information technology is. Information technology (IT) as defined by the Information Technology Association of America (ITAA), is "the study, design, development, implementation, support or management of computer-based information systems, particularly software applications and computer hardware". IT deals with the use of computers and computer software to convert, store, to protect, process, transmit, and securely retrieve information.

IT professionals perform a variety of duties that range from installing applications to designing complex computer networks and information databases. A few of the duties, that IT professionals perform, may include data management, networking, engineering computer hardware, database and software design, as well as the management and administration of entire systems. IT is a general term that describes any technology that helps people network effectively during communication activities that may involve IT. That is, IT supports producing, manipulating, storing, communicating, and/or disseminating information within an organization or around the world.

## **Networking**

When talking about IT solutions, an important concept to be very familiar with is networking. Networking is a general term used to describe any interconnected group or system. Therefore, a computer network is an interconnected group of computers. Typically a network is any method of sharing information between two or more distinct systems (human or mechanical).

The term network may involve:

- Human networks – social
- Media networks – radio, television
- Technology networks – electronic, computer, pipeline
- Science, mathematics and engineering networks – neural, genetic
- Other networks - transportation – the moving of people and/or goods

Networking is used in every aspect of business – i.e., advertising, production, shipping, planning, billing and accounting. Schools at all levels use computer networks to obtain information from libraries around the world instantaneously. Federal, state and local governments and military organizations use networks. Global internet is one of the most interesting and exciting phenomena ever (Comer, 2004). The growth associated with computer networks has had and continues to have a large impact on our political, economic and social infrastructures. With the current global information technology culture the limit of distance has been traversed and conquered allowing for people throughout the world to engage in e-commerce and other global ventures and experiences.

## **Computer Networks**

Computer networking is a complex subject. Several technologies exist and organizations generate networks in many variations that may or may not be compatible with one another. Many combinations are possible when it comes to

computer networks (Comer, 2004). Also, networks may be private or public. Private networks are typically owned by a single company or individual. Public networks are operated by common carriers or service providers. Any subscriber can use a public network for communication.

It is important to understand the major concepts when learning about networking and not get hung up on the details. For example, it is important to understand the different types of wiring schemes and the associated advantages and disadvantages of each (Comer, 2004). In the following paragraphs this paper will address some important topics from a high level in regards to networks. Additional information may be obtained from researching computer networks on the internet.

### **Network Communication**

Network architectures are designed for sharing information. Networks transfer data from one point to the other without understanding what the data is – i.e., the network does not process the data in any way; networks just move the data. Data may be processed by application programs located anywhere within the network. Applications use networks to send and receive data. This is typically referred to as client-server computing or pair programming. Client-server computing enables applications contained or connected via a network to communicate effectively. In other words, client-server computing allows applications to find each other, while sending and receiving data across a network. The server waits for contact and the client initiates the contact. The computer and application become the unique address used to help the client and server find one another. Most internet applications also use this arrangement.

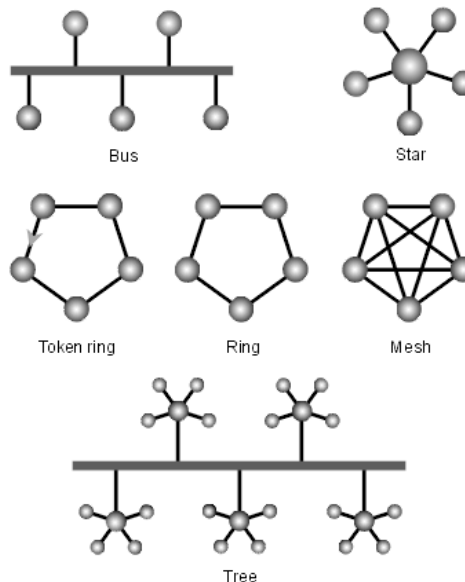
Application program interfaces (APIs) are high level, sometimes complex, programming operations used by networking administrators to help networks communicate. Programmers are able to create networks that operate across the global internet using API. Thus, making our world a smaller place; business

transactions via organizational networks or IT solutions that run on networks can be performed readily in minutes versus days, weeks or months.

### Network Topology

Network topology may refer to the physical and/or logical schematic description of the network architecture including nodes and connecting lines. There are two ways of defining network geometry: the physical topology and the logical (or signal) topology.

Physical topologies describe the arrangement of workstations within a network. Several physical topology arrangements are possible depending on the needs of the organization establishing the networks – e.g., several workstations may need to share a single printer. It is up to the organization’s IT department to select the best network topology. **Figure 1** depicts some common network topologies – i.e., bus, star, token ring, ring, mesh and tree.



**Figure 1**

The physical network perspective involves geographic locations. In figure one each circle represents a node, a workstation, printer or some other device that

may process data. The nodes are connected via copper wires (cables), glass fibers, modems, routers, bridges and other hardware or they may involve wireless technology.

Logical networks are sometimes referred to as signal topologies or subnets which define how a signal flows from node to node. Typically, logical topologies are the same as physical topologies, but you may have variations using both types of topologies within the same network. Each topology has its advantages and disadvantages and it is up to the organization's IT department to select the topology that best fits its needs. Commonly used topology configurations or network types include:

- Local Area Networks (LAN) are in common use throughout major companies and organizations to allow users to share data and facilities such as printers and Internet links.
- Wide Area Network (WAN) is a network that spans a large geographical area, the most common example being the Internet.
- Metropolitan Area Network (MAN) is a larger type of network interconnecting different LANs. Most organizations do not use the term MAN and tend to call them a small WAN instead.
- Extranets bridge between different parts of the same organization by communicating through the Internet.
- Intranets connect private networks via the Internet or leased lines but with extra security.
- Virtual private networks (VPN) connect private networks via the Internet or leased lines but with extra security.
- Wireless LAN or WAN (WLAN or WWAN, respectfully) is basically the same as a LAN or a WAN but there are no wires between hosts and servers. The data is transferred over sets of radio transceivers. These types of networks are beneficial when it is too costly or inconvenient to run the necessary cables.

The Internet is made up of many users, organizations, and content providers that are interconnected by Internet Service Providers (ISP). Basically, the Internet is the set of subnets, and aggregates of subnets, which share a registered IP address space and exchange information about those IP addresses using the Border Gateway Protocol. The human-readable names of servers are translated to IP addresses, transparently to users, via the directory function of the Domain Name System (DNS).

### **LAN Wiring, Physical Topology and Interface Hardware**

Networks are designed for a combination of speed, distance and cost. Network interface card (NIC) or network adapter installed in computers and other data processing devices accommodate various wiring schemes supporting computer networks. The type of connection between the NIC and a network depends on the network technology (Comer, 2004).

### **Network Cabling Materials – Transmission Media**

All computer communications involve encoding data in a form of energy. This energy is sent across a transmission medium – i.e., wire or cable. It is important to understand some basic information about network cabling materials to understand how the different transmission media types may affect data transmission. Each transmission media has its advantages and disadvantages.

Networks may employ one or more of the following types of transmission media:

- Copper wires – a primary medium to connect computers. A relatively inexpensive and easy to use medium that transports an electrical signal across a network. Three basic types of copper wire are typically used: (1)

unshielded twisted pair (UTP), (2) coaxial cable and (3) shielded twisted pair (STP).

- Glass fiber – also known as optical fiber. Optical fiber uses light to transport data in lieu of electrical energy. Optical fibers have four main advantages over copper wire: (1) light that is transmitted causes no electrical interference, (2) light signals can be carried further than signals carried via copper wire, (3) light can encode more information than electrical signals, and (4) light can travel from one computer to another over a single fiber; unlike copper wires, where two wires are required.
- Radio – radio frequency transmissions do not require direct physical connection between computers. An antenna connected to a computer or network is used to transmit and receive radio frequencies.
- Satellites – radio frequencies do not travel around the earth's surface without the combination of satellite use. Satellites are used to extend the distances of radio frequencies around the globe.
- Geosynchronous satellites – is one type of satellite positioned in orbit at a location which is synchronized with the earth's rotation.
- Low earth orbit satellites – are typically placed somewhere between 200 to 400 miles above the earth's crust.
- Microwave – electromagnetic radiation may also be used to transport information. Basically, this technology is a higher frequency version of radio waves aimed in a single direction.
- Infrared – similar to wireless remote controls; data may be transmitted via infrared transmissions for short distances.

LAN transmission media typically involves copper wires or radio frequencies. Most WANs use leased digital circuits to provide long-distance communication. Several organizations use T1 or T3 digital circuits. T1 circuits have data rates of 1.544 Mbps (mega bits per second) and T3 circuits have a data

rate of 44,736 Mbps. Higher capacities are available – e.g., optical fiber. Optical signals are governed by Optical carrier standards designated as OC. OC-3 circuits operate at approximately 155,520 Mbps. Most individuals use digital subscriber line (DSL) or cable modems for home or small business use.

### **Network Standards or Protocols**

Depending on the type of network technology, a network administrator must be equipped with a good working knowledge on how to build and/or maintain a basic network or a large complex physical network.

Communication protocol software is used to interact with the data transmitted over a network. Protocol software processes information into a language that can be interpreted by computers or computer applications. Protocol rules govern how data is interpreted when communicating across a network. Network designers must plan for, design or trouble shoot protocols to accommodate their given network environment. Some common types of protocol software are:

- Transmission Control Protocol/ Internet Protocol (TCP/IP) - is a widely used protocol for internetworking. The U.S. military funded much of the research costs with developing TCP/IP through Advanced Research Projects Agency (ARPA). Five layers make up the TCP/IP – Physical, Network Interface, Internet, Transport, and Application. The IP provides a uniform addressing to be used by applications connected to an internetworking environment.
- User Datagram Protocol (UDP) – provides an end-to-end service that allows an application program to send and receive messages, each traveling in a separate datagram. An application can select to restrict communication to one other another program or communicate with multiple applications.
- Asynchronous Transfer Mode (ATM) – originated in the telecommunications industry. ATM handles voice, video, and data

transmission. ATM uses a connection-oriented paradigm by creating a virtual channel to communicate. Once completed the virtual channel is terminated. Due its complexity and cost this protocol is not prevalent.

- File Transfer Protocol (FTP) – is the most widely used internet file transfer service. FTP is a general purpose protocol that can be used to copy files from one computer to another.
- Hypertext Transfer Protocol (HTTP) – allows a web browser to display files from a web server.

### **Security**

Security is the condition of being protected against danger, destruction or loss. Information technology security is very important to individuals, organizations, nations and the world. Appropriate measures must be taken to store and protect the wealth of important data and information. Types of security associated with information technology solutions typically involve:

- Application
- Host
- Network
- Physical
- Social

### **Application**

Application security typically involves databases or dynamic systems – i.e., banking systems, Amazon, school applications, etc. Data integrity, availability, confidentiality and privacy all must be carefully considered during the design and implementation of an application.

Typical encoding schemes help to protect information within a network. Encryption or cryptographic hashing mechanisms use secret keys known only to the sender and receiver of specific data during transmissions.

Access control mechanisms use an individual's identification to establish access controls for a specific application. Typically, a user must provide a password prior to being able to access a certain application or information. An individual using a computer for protection against security attacks wants to ensure that the latest service packs are installed on their operating system.

### **Host**

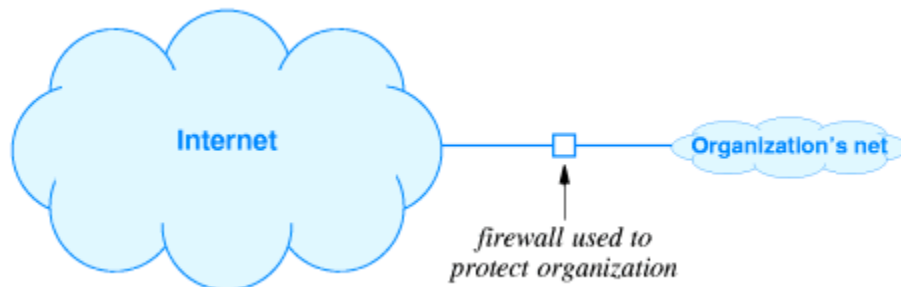
Host security involves working with the host computers or server operating systems that transmit data back to client requests – e.g., web pages; surfing the web to ensure they are secure. Authorization must be established and controlled. Things like who is responsible for the location of information and who has access to information.

### **Network**

As we mentioned previously, networks are the interconnection of systems or applications. Networks must remain intact or unbroken and secure. “Devising a network security policy can be complex, because a rational policy requires an organization to relate network and computer security to human behavior and to assess the value of information” (Comer, 2004).

Network attacks may come in the form of various malicious programs aimed to cause networks or components on networks to fail or to work in an inefficient manner. Several things can be performed to reduce attacks against a network.

Internet firewalls help to protect an organization's computers and networks from unwanted Internet activity. The firewall is typically placed between an organization or individual's network and the internet (see Figure 2). Any traffic or data transmissions entering and leaving the organization pass through the firewall and filtering of data takes place to reduce potential threats. The firewall is immune to security attacks.



**Figure 2**

Examples of other types of security technologies are:

Intrusion Detection System (IDS), Pretty Good Privacy (PGP), Secure Shell (ssh), Secure Socket Layer (SSL), IP security (IPsec), Remote Authentication Dial-In User Service (RADIUS), and Wired Equivalent Privacy (WEP) part of the Wi-Fi wireless LAN standard.

Organizations and individuals may demand secure networks; however, it is not possible to provide a single definition or answer that covers all needs. Each organization or individual must define its own security policy, that specifically outlines sensitive information to be protected.

### **Physical**

Any good organization should include physical safeguards to protect its network against unauthorized access, detects attempted or actual unauthorized access. These measures are what are referred to as physical security. Physical security is required to help control access information or data assets. Physical security involves, locking the door to the room where PC or key network components may be located. The physical security requirements vary among organizations depending on the type of data and physical layout of the facility – i.e., each facility is unique.

Organization may have to implement physical security measures such as restricted security zones, locked doors, access control systems, intrusion alarm systems, approved security containers, destruction equipment and other applicable measures. Administrative security requirements such as establishing company security guidelines and/or security awareness programs may also be considered (INFOSYSSEC, 2007).

### **Social**

People use social networks to

- Socialize
- Stay in-touch with family
- Publicize information – myspace; e.g., hot new band
- Club or activity based communication

While participating in social networking environments – i.e., emailing, chatting, blogging you need to ensure you know who you are communicating with at all times. Several ingenious attempts to threaten your privacy are continuously engineered by people with nothing better to do. Social attacks may involve bullying, cyber stalking or innocent users whom unknowingly divulge confidential information by way of trickery.

Pre-texting is the act of contacting people to gain private information about an individual or company. Other social attacks involve what is called phishing. During phishing attempts, people try to gain sensitive, personal information – i.e., usernames, passwords, and credit card numbers by pretending to be a trustworthy entity. Phishing usually takes the form of emails and instant messaging. Know who you are talking to.

Keystroke logging is another form of a social security attack. During keystroke logging a user can determine a user's key stroke activity. Passwords and personal information have been given out when using this method.

There are many other types of security threats that are distributed via emails or downloaded via executable files. In all cases when emailing, instant messaging or downloading files you should always know the source.

### **Protecting Yourself**

Always keep your anti-virus software updated. Anti-virus software helps to keep your computer protected against unwanted attacks. If maintaining a personal network, ensure to include a firewall to keep your network safe from unwanted traffic.

If socializing over the Internet, know who you are socializing with. Always keep your user name and profile generic and anonymous. Avoid posting personal photos online; always keep your personal information private. Once you post something online, even for a short time, it will be saved somewhere where it could be later accessed, keep some control over the information you share with others by restricting access to your page. Trust your gut if you're suspicious! Remember, if you parents would not approve of it, it's probably not a good idea! It's already a huge business for people to try and trick you into giving away personal information. Don't make it any easier by offering it on a site. When creating social networking accounts look for https, unbroken keys, or a padlock for secure sites. For additional information on personal security visit: <http://ftc.isafe.org/idtheft.html>.

### **Employment Opportunities**

Network managers are people, that are responsible for monitoring, controlling and securing the hardware and software systems that comprise a network or internetwork. This task can be challenging due to the various configurations and software components manufactured by multiple companies. Also, networks are large and often reside in remote locations. Detecting problems in remote locations can be tedious.

### **Important Security Web Sites**



<http://www.cert.org/>

One of the most well known centers for computer security research is found right in Pittsburgh / Oakland. CERT is based at the Software Engineering Institute at Carnegie-Mellon University.

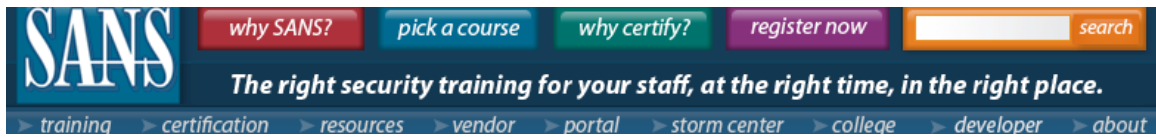
---



<http://www.us-cert.gov/index.html>

The United States Computer Emergency Readiness Team (US-CERT) is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation.

---



<http://www.sans.org/>

SANS is the most trusted and by far the largest source for information security training and certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - Internet Storm Center.

---



<http://isc.sans.org/>

The Internet Storm Center was created in 2001 following the successful detection, analysis, and widespread warning of the Li0n worm. Today, the ISC provides a free analysis and warning service to thousands of Internet users and organizations, and is actively working with Internet Service Providers to fight back against the most malicious attackers.

---



<http://www.computer.org/portal/site/security/>

The Institute for Electrical and Electronic Engineers is one of the oldest professional organizations and is dedicated to fostering computer and electrical engineering. This site provides information that organizations relying on the Internet need to know to ensure that their networks operate safely. “To help you stay one step ahead of these and other threats, the IEEE Computer Society published a new periodical in 2003, IEEE Security & Privacy magazine.”

IEEE Security & Privacy will rethink the role and importance of networked infrastructure and help you develop lasting security solutions. Topics covered include:

- Wireless Security
  - Designing for Security
  - Privacy Issues
  - Digital Rights Management
  - Cybercrime
  - Intellectual Property Protection, and Piracy
  - The Security Profession
-

# National Security Agency Central Security Service



[http://www.nsa.gov/home\\_html.cfm](http://www.nsa.gov/home_html.cfm)

The National Security Agency/Central Security Service is America's cryptologic organization. It coordinates, directs, and performs highly specialized activities to protect U.S. government information systems and produce foreign signals intelligence information. A high technology organization, NSA is on the frontiers of communications and data processing. It is also one of the most important centers of foreign language analysis and research within the government.

---

## References

Comer, C.E. (2004). Computer Networks and Internets with Internet Applications. (4th ed.). New Jersey: Pearson Prentice Hall.

Presentation Summary Santoro. Social Networking Tools. Retrieved April 13, 2008

Physical Site Security Info Resources. (2007). INFOSYSSEC - The Security Portal for Information System Security Professionals. Retrieved May 2, 2008 from <http://www.infosyssec.com/infosyssec/security/physfac1.htm>

Wikipedia, The Free Encyclopedia. (2008). Computer Network. Retrieved April 13, 2008, from [http://en.wikipedia.org/wiki/Computer\\_network](http://en.wikipedia.org/wiki/Computer_network)