2004

Embedded Security Improvements to IPv6

Mark Merlino

Embedded Security Improvements to IPv6

By

Mark Merlino

Thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Information Technology

Rochester Institute of Technology

B. Thomas Golisano College
of
Computing and Information Sciences

22 May 2004

Rochester Institute of Technology

B. Thomas Golisano College
of
Computing and Information Sciences

Master of Science in Information Technology

Thesis Approval Form

Student Name: Mark Merlino

Thesis Title: Embedded Security Improvements to Ipv6

Thesis Committee

Name	Signature	Date
Prof. Sharon Mason Chair		5-19-04
Evelyn Rozanski, Ph.D Committee Member		5-19-04
Prof. Dianne Bills Committee Member		5/19/04

Thesis Reproduction Permission Form

Rochester Institute of Technology

B. Thomas Golisano College of Computing and Information Sciences

Master of Science in Information Technology

Embedded Security Improvements to IPv6

I, Mark Merlino, hereby grant permission to the Wallace Library of the Rochester Institute of Technology to reproduce my thesis in whole or in part. Any reproduction must not be for commercial use or profit.

Date: 22 May 2004 Signature of Author:

Table of Contents

Introduction

Today's businesses and home consumers have spent vast amounts of money and financial resources on e-business commerce and enterprise solutions. These solutions and their associated applications are designed to acquire and build customer associations that allow business to grow, from both corporate and personal consumer perspectives. E-business and the Information Technology industry have grown dramatically over the last two decades allowing businesses to expand into the cyber-tech world of the Internet. In a short period of time, this technological development has permitted computer communications through vast networks used for entertainment, business, and services.

For these networks to operate, specific standards that allow communication to take place are necessary. These standards have changed dramatically as the type of information that is transmitted has changed. Communications involving merely voice and data are no longer sufficient. Today, communication systems that include image and video are essential. This type of information sharing has created new technologies that allow data transfer to support many hardware and software distributed systems.

TCP/IP is a protocol that is part of a communication standard that defines the groundwork for the Internet. There are other communication standards, but almost all computer and software vendors now utilize the TCP/IP protocol as part of an overall network that handles communications between computers. These standards permit basic services such as electronic mail, file transfer, and remote login capabilities across large numbers of client/server systems to, ultimately, provide end users with the ability to

communicate and share data with virtually anyone connected to a computer network. As much as this protocol provides increased communication capabilities, it has a down side. Ranges of inherent problems have surfaced -- from the system being fragile to external threats arising from unauthorized use of this protocol to access business and personal computers. The original concept of the Internet was an information-sharing medium. The development of this medium was shared among a few parties, the government and selected universities. It was essentially architected to transmit data. The complexities seen with today's Internet evolved from these original concepts. They also incorporate updates that address critical problems that developed through Internet usage.

The biggest concern for today's user is security. Because the Internet was not designed with security in mind, it contains many openings for intrusions. As development continued, changes were made to address these concerns, but the rapid growth of Internet usage prevented wholesale fixes from taking place in a timeframe that warranted secure implementation. Instead, something new needed to be devised that would address security along with other outstanding issues such as bandwidth and addressing. This solution was a new architected version of the Internet, known as IPv6. This version is to replace IPv4, which is currently in use. One of IPv6's main intentions is to address security issues by incorporating embedded security that can solve many of the common privacy and encryption problems to which the current IPv4 is subject. The goal of this thesis is to explore the aspects of this new architecture in relation to the old, and to determine whether or not Internet security issues can be minimized or even eliminated solely by the implementation of IPv6.

Networks

Computer interoperability is the manner in which computers work together as a networked system. For computers to work together, they need to share resources connected together with software and hardware components that make up a network. The guidelines that these networks follow are known as standards (expected performance of all networked elements) and protocols (interaction of these elements). Network architectures can be designed in many ways depending upon client needs. After establishing client requirements, then the type of network can be determined, from software operating systems to the software programs needed to allow communication between the hardware components of the system. The Internet utilizes these components in the same network model. Internet communication access is based upon the TCP/IP protocol and is readily used by many computer systems as their standard networking protocol. Because of the flexibility of the TCP/IP protocol, other protocols such as Apple's File Protocol, Microsoft NetBIOS, and Novell IPX can still be used. As indicated earlier, networks can be constructed in many different fashions depending upon the architectural requirements of the system. Examples of different networked systems are shown below:

- LAN's – A small number to many individual computer clients connected to a centralized computer (server). The server can be equipped with specific software that is shared among individual clients as well as specialized applications that monitor and manage additional programs.
- Ethernet – These systems are computers interconnected by cabling that run from one Ethernet interface card to another Ethernet interface card on another

computer. More often than not, Ethernet cards are located within the computer expansion slots and are connected at the interface point where the cable connector snaps into place. These cables may be attached to a hub (made for the various media types) that, depending upon signaling architecture, can accommodate up to a gigabit signal transmission rate.

- Token-Ring – This network configuration connects the computers and peripherals to separate wiring hubs. One disadvantage of a Token-Ring configuration is that, if power or connection is lost, the device will be disconnected from the system.
- Structured Wiring – This type of wiring system provides a standardized system for wiring a building to accommodate all types of networks. Cabling can be located in panels located in a centralized area for access that expands out to specific network connections in wall jacks as designed.
- Peer-to-Peer – This type of network does not contain a dedicated server, but instead shares the processes of the networked clients. File server programs can still be loaded and utilized, but they are resident on one of the networked computers and utilize the resources dictated by the user using that particular computer. This type of network makes it easy for others to share resources and can be economically satisfying if the system remains relatively small.
- Enterprise – These systems provide an overall management system that utilizes software programs called agents to gather information in a format known as a MIB. This information is transferred to additional programs, which can comprehend the information on overall system performance and create informative displays in detailed graphical formats such as charts and graphs. Enterprise networks can also be used to detect problems by watching for specific

conditions that exceed specified limits; inventory existing systems by gathering statistics on data transfer, perform data backups, and alert the appropriate system administrators in case of breaches.

Network Communications

The telegraph, using Morse Code as it's means of sending communications, key- punch terminals, and Baudot's teletypewriter code are the beginnings to today's ASCII code. It is widely accepted, but not necessarily universal in it's acceptance as a network code. IBM developed and still uses their own code, EBCDIC in current mainframes and computers. With increased computer availability and subsequent usage, it became apparent that they needed to work together as synchronized units. Continued development began spawning new technologies such as the Internet. Original intentions of the Internet, first proposed by the ARPA and later developed by the DARPA [1], were designed as a testing method for sending packets of information over networks. As the ARPA network, or ARPANET continued to develop, modifications allowed for increased usage, and expanded from predominant military use to commercial venues such as universities. This work led to the development of an early protocol, the network control program, and later became TCP/IP [2]. Quickly it was evident that the network could not handle the amount of network traffic it began receiving. It was also apparent that Network Administrators became reluctant to share their network resources because of concerns about security. Clearly, common technologies, or standards needed to be introduced to allow communication between different networks. The early 1970's showed how new communication functionality could be connected, regardless of the operating system platform. The ITU-T, along with the ISO, ARPA, and DARPA, developed the initial concepts of networking. These standards would allow any computer to be connected from any location to the network. TCP/IP in the current version 4, was standardized by the early 1980's. During this timeframe, Berkeley University released a

version of the TCP/IP protocol and made it available as public software. Because this software was not proprietary, both public and private sectors adopted it quickly. Many of today's versions of the TCP/IP protocol have their origins from the Berkeley University release, as it soon became the standard for data communications protocols.

Rapid development of the Internet forced the development of organizations to monitor expansion and maintain control. These organizations, or bodies, such as the IETF establish guidelines [3] that protocols follow regarding implementation as well as standards for future research. The IETF is composed of an open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The IETF is broken down into working groups and managed by Area Directors that are members of the Internet Engineering Steering Group. The Area Directors that provide architectural oversight is known as the IAB. The IAB also oversees appeals when there are registered complaints. The IANA is the central coordinator for the assignment of unique parameter values for Internet protocols. The IANA is chartered by the ISOC to act as the clearinghouse to assign and coordinate the use of numerous Internet protocol parameters. Within the IETF working group are specific areas and charters that are followed. There are 8 areas that form this group: Applications, General, Internet, Operations and Management, Routing, Security, Sub-IP, and Transport. Each of these areas is responsible for a specific aspect of the Internet. For example, the Operations and Management working group area houses (or holds or contains) additional sub-areas. These areas are assigned to specific groups who will oversee them. V6ops is one such area. The charter [4] of the v6ops work group is as follows:

The global deployment of IPv6 is underway, creating an IPv4/IPv6 Internet consisting of IPv4-only, IPv6-only and IPv4/IPv6 networks and nodes. This deployment must be properly handled to avoid the division of the Internet into separate IPv4 and IPv6 networks while ensuring global addressing and connectivity for all IPv4 and IPv6 nodes. The v6ops develops guidelines for the operation of a shared IPv4/IPv6 Internet and provides guidance for network operators on how to deploy IPv6 into existing IPv4-only networks, as well as into new network installations.

The v6ops working group will:

1. Solicit input from network operators and users to identify operational or security issues with the IPv4/IPv6 Internet, and determine solutions or workarounds to those issues. This includes identifying standards work that is needed in other IETF WGs or areas and working with those groups/areas to begin appropriate work. These issues will be documented in Informational or BCP RFC's, or in Internet-Drafts. For example, important pieces of the Internet infrastructure such as DNS, SMTP and SIP have specific operational issues when they operate in a shared IPv4/IPv6 network. The v6ops WG will cooperate with the relevant areas and WGs to document those issues, and find protocol or operational solutions to those problems.

2. Provide feedback to the IPv6 WG regarding portions of the IPv6 specifications that cause, or are likely to cause, operational or security concerns, and work with the IPv6 WG to resolve those concerns. This feedback will be published in Internet-Drafts or RFC's.

3. Publish Informational RFC's that help application developers (within and outside the IETF) understand how to develop IP version-independent applications. This working group will work with the Applications area, among others, to ensure that these documents answer the real-world concerns of application developers. This includes helping to identify IPv4 dependencies in existing IETF application protocols and working with other areas and/or groups within the IETF to resolve them.

4. Publish Informational or BCP RFC's that identify potential security risks in the operation of shared IPv4/IPv6 networks, and document operational practices to eliminate or mitigate those risks. This work will be done in cooperation with the Security area and other relevant areas or working groups.

5. Publish Informational or BCP RFC's that identify and analyze solutions for deploying IPv6 within common network environments, such as ISP Networks (including Core, HFC/Cable, DSL & Dial-up networks), Enterprise Networks, Unmanaged Networks (Home/Small Office), and Cellular Networks. These documents should serve as useful guides to network operators and users regarding how to deploy IPv6 within their existing IPv4 networks, as well as in new network installations.

6. Identify open operational or security issues with the deployment scenarios documented in (5) and fully document those open issues in Internet-Drafts or

Informational RFC's. They will work to find workarounds or solutions to basic, IP-level operational or security issues that can be solved using widely applicable transition mechanisms, such as dual-stack, tunneling or translation. If the satisfactory resolution of an operational or security issue requires the standardization of a new, widely-applicable transition mechanism that does not properly fit into any other IETF WG or area, the v6ops WG will standardize a transition mechanism to meet that need.

7. Assume responsibility for advancing the basic IPv6 transition mechanism RFC's along the standards track, if their applicability to common deployment scenarios is demonstrated in:

- Transition Mechanisms (RFC 2893)
- SIIT (RFC 2765)
- NAT-PT (RFC 2766)
- 6to4 (RFC 3056 & 3068)

This includes updating these mechanisms, as needed, to resolve problems. In some cases, these mechanisms may be deprecated (i.e. moved to Historic), if they are not found to be applicable to the deployment solutions described in (5) or if serious flaws are encountered that lead us to recommend against their use. IPv6 operational and deployment issues with specific protocols or technologies (such as Applications, Transport Protocols, Routing Protocols, DNS or Sub-IP Protocols) are the primary responsibility of the groups or areas responsible for those protocols or technologies. However, the v6ops group will provide input to

those areas/groups, as needed, and cooperate with those areas/groups in developing and reviewing solutions to IPv6 operational and deployment problems[5].

As of August, 2003 this group had only one RFC, 3574. RFC's are papers designed as information to be used by the Internet community. They are not in themselves a standard, but are used as a reference in helping to develop Internet standards.

This organization has become vital as other organizations utilizing the TCP/IP protocol began developing their own networks. The NSF established a network that was managed jointly by MCI, Sprintlink, and IBM. With this cooperative effort came the formation of ANS, which developed access to the Internet by using NAP.[6] This allowed connection to multiple networks in both public and private sectors. Since the initial design of the Internet did not anticipate the popularity and wide spread usage that occurred, ANS became vital. It was also important because it began to address the problem of electronic security intrusions, which were not anticipated with the initial design.

As the popularity of the Internet grew, so did the potential for unwanted access to computer systems. For a myriad of reasons, intruders began discovering ways to exploit software and the networks that tie them together. Controlling specific computers allowed intruders to mask their true identities and launch attacks through donor computers, causing damage by changing data or destroying components such as hard drives. Having the latest anti-virus software and operating system patches can minimize these risks, but will not totally eliminate them. These fixes do help in detection, but they only mask the root cause of security design deficiencies. A change in the way information is delivered was needed as a step towards protecting data. As the current

TCP/IP protocol continues to evolve, many of the inherent risks associated with it can be removed.

Still that does not alleviate issues surrounding current networked systems. In today's environment the majority of attacks on systems come from a relatively small number of software vulnerabilities. Attackers can be generally counted on to take the easiest, most exploited route, using very sophisticated tools to compromise a system. Often, they search the Internet for vulnerable systems, attacking indiscriminately.

Network Transmission Methods

Network transmission refers to the technology and lines that carry the data information. Digital services such as ISDN and DSL use existing telephone networks. Other common examples include coaxial cable modems, which transmit and receive data over local TV cables, twisted pair (including shielded), and fiber optic. These types of data transmission lines use devices such as hubs, switches, repeaters, bridges, and routers to direct and provide different levels of data handling over the network. Essentially, this allows applications on personal computers to engage, transfer, and deliver voice, fax, and data information to other personal computers. Each device has a specific role in delivering the information to its desired location while maintaining the integrity of the original message. These devices, also known as portal devices, are used as points in a network to monitor and detect incoming breaches, but also pose potential links that can be vulnerable to security intrusions. Exploring each component, the mediums that carry the information, and the information itself (electromagnetic signals) that makeup a network can expose security vulnerabilities that exist within each component of the network.

Data communications media that travel these different mediums can be categorized in the form of guided or unguided. Guided media carry electromagnetic signals along hardware such as coaxial cables, twisted pair, and optical fiber. Unguided media deals with (or encompasses) wireless communications. The quality of data transmissions is dependent upon the medium used and the characteristics of the electromagnetic signal. Both transmissions have characteristics that can impact the transmission quality. In guided mediums, the medium is more critical to the quality of the transmission than the

electromagnetic signal. For unguided media, the signal strength is more critical than the transmitting medium. There are basic factors that are key to determining correct transmission systems:

- Bandwidth – generally the greater the bandwidth, the greater the signal quality
- Impairments – can limit signal distance
- Interference – overlapping signals can impact or destroy signals
- Receivers – multiple receivers can introduce additional signal distortion

Mediums

The physical aspect of twisted pair mediums consists of two insulated copper wires twisted together in a spiral. These are then bundled together by the hundreds into a shielded cable. They have a twisted characteristic because it tends to reduce interference between other twisted pairs contained within the cable. Today, twisted pair is the most common medium used for both analog and digital transmissions. It is used extensively in telephone and office networks as well as private residences that are connected to the local telephone exchanges. The original concept of the twisted pair was to support voice traffic using analog signals, but with the advent of the modem, digital signaling can be transmitted along these wires. Digital signaling is common in offices that use local-area networks to support computer systems. Data rates can vary with twisted pair wiring with common transfer rates of approximately 10 Mbps to high-end rates of approximately 100 Mbps for very short distances. There are many factors that can determine rates from geographic distances to the number of devices connected to the network.

Twisted pair wiring has limitations that need to be considered. Distances of 5kilometers or more require amplifiers for analog signals and distances of 2 kilometers or more require repeaters for digital signals. Interference and noise can also impact signal strength and clarity. This impedance can be overcome with shielding of metallic braid or sheathing that surrounds the wire. Because twisted pair wiring is available in different shielded and unshielded categories, design needs to be taken into consideration to thoroughly understand the network requirements and types of peripherals that will be connected.

Coaxial cables are constructed differently than twisted pair and allow a greater number of frequencies to be transmitted. Both analog and digital signals can be transmitted at higher frequencies and data transfer rates than typical twisted pair wiring. Essentially, coaxial cable is a single copper inner wire surrounded by a conductor and shielded with an outer layer for protection. This outer protection, or shielding, offers greater interference protection than is offered by twisted pair wiring. Coaxial cabling offers a large variety of applications, from television and telephone systems to networked computer systems. The advantages of coaxial cables include the ability to provide high-speed data transfer to a large number of devices over shorter distances such as local building complexes. For longer distances coaxial cables are similar to twisted pair in that they require amplifiers for analog signals and repeaters for digital signals. Both twisted pair and coaxial cables are limited only by the inherent physical characteristics they possess.

Optical fiber technology, as opposed to twisted pair and coaxial cabling has created a networking breakthrough in communication systems. Its characteristics permit long-range communications with the associated benefits of greater capacity from a reduced cost base. Optical fibers consist of a thin, flexible medium (fibers that are made from various gasses and plastic materials) that transmits an optical impulse. These fibers are constructed by creating a core (two mediums that have different refraction characteristics) surrounded by cladding and a protective outer jacket. Optical cabling contains many independent fibers in a single package with far superior performance characteristics than seen in twisted pair and coaxial cables.

The advantages of fiber optic over twisted pair and coaxial mediums range from:

- Capacity – Increased bandwidth, allowing data rates of 2 Gbps over many kilometers have been achieved as compared to 100's of Mbps over a distance of up to 2 kilometers for coaxial cable and a few Mbps over a distance of up to a single kilometer for twisted pair.
- Size and Cost – Considerably smaller in size, it can translate into greatly reduced structural requirements creating cost savings during installation. Optical fiber does not require as many repeaters within the network.
- Interference – Fiber optic is not impacted by electromagnetic fields so interference and noise are greatly reduced.
- Security – Fiber optic provides a much higher degree of security because it is difficult to intercept transmissions without detection in the typical constructs used in point-to-point mediums.

As networked systems continue to evolve, fiber optic technologies will become more prevalent. They are increasingly being used in the telephone industry due to the benefits of increased bandwidth capacity and greater route distances. The greater bandwidth allows for greater capacity to handle the increased demand for voice, data, image, and video transfer. The greater distance means localized networked systems do not need the added repeaters seen in twisted pair and coaxial systems. Finally, the increased security of fiber optic cabling far outweighs the vulnerabilities exhibited by twisted pair and coaxial cables.

Other technologies such as wireless (radio, microwave, and satellite) do exist, but they present a completely different set of security issues. For the purposes of this discussion, the focus will be on guided mediums such as twisted pair, coaxial and fiber optic cabling, since the Internet, as used today, is predominantly using these types of mediums[7].

Electromagnetic Signals

All forms of data transmission, either by voice, data or video use electromagnetic signals that are transmitted over their corresponding medium. The information is created by a source such as a computer terminal. The information is converted into an electromagnetic signal, and then carried over a transmission medium, such as fiber optic cable, from the transmitter to the receiver. The receiver then retrieves the electromagnetic signal and reproduces it into the original (or approximate) form in which the information was sent (Figure 1).

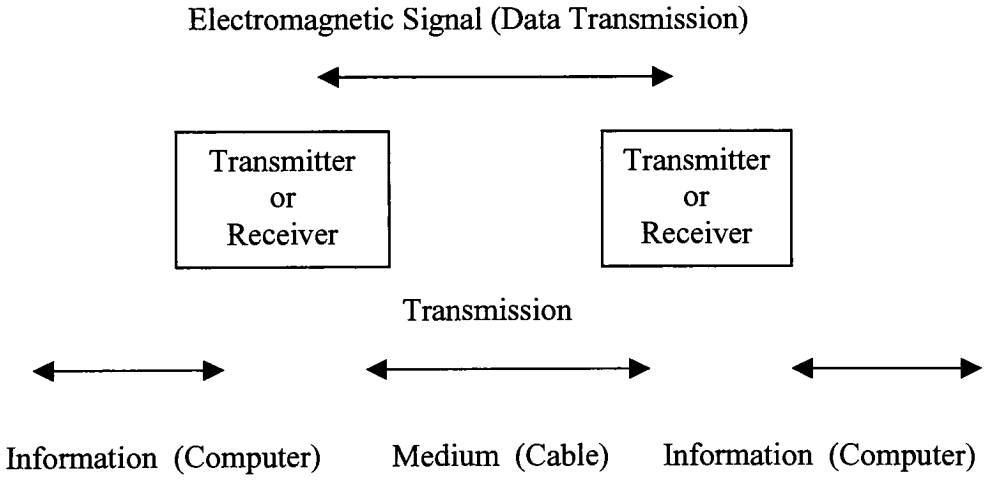


Figure 1 - Example of Data Transmission

Electromagnetic signals (either analog or digital) can be looked at from two different perspectives. The first such perspective, time-domain, is a function of time. An analog signal is a continuously varying electromagnetic wave that is sent over a period of time.

The wave of the analog signal is made up of three components:

- Amplitude – strength of the signal
- Frequency - rate at which the signal repeats itself. The range of frequencies is known as the spectrum of the signal.
- Phase – position in time within a single period of a signal

There are no breaks in an analog signal whereas a digital signal maintains a constant level for a period of time then changes to another constant level for a period of time. The second such perspective is a digital signal that is represented by electromagnetic pulses represented by two binary digits, 0 and 1. The wavelength is the distance of a single cycle and the bandwidth of a signal is the width of the spectrum. This information is critical because there is a direct relationship between the amount of information, and capacity of a signal and its bandwidth. Essentially, the greater the bandwidth, the greater the amount of information that can be transmitted. There is one downside to consider with bandwidth; the greater it is, the greater the associated cost. Mediums transfer information at different rates and, depending upon which medium is being utilized, will dictate bandwidth allocation and information transfer. Most business networks have associated costs that prohibit unlimited spending. This can dictate how a specific network will be set up. It will also dictate bandwidth size and data transfer. Limited bandwidths will limit signal strength, which can potentially create distortions or noise. These distortions, or noise, can make it difficult for the receiver to interpret the signal.

Portal Devices

Portal devices such as bridges, routers, gateways, and repeaters connect local area networks together and extend the distance capabilities of the network. Each of these components offers different degrees of data handling capabilities within a network. Bridges are devices that connect networks, filter data packets, and move them forward in the network. Bridges operate within the Data Link Layer of the OSI Model. They can read the specific physical addresses of devices on the network and filter the information before moving it forward to another network segment. Because they operate at the Data Link Layer or, more specifically, at the MAC sub-layer, they can clean an incoming signal, amplify it and pass it onto the next segment as a clean signal (eliminating signal noise). This filtering capability allows bridges to scan and reduce traffic between segments, generating a greater degree of security by selecting the specific data signals, or packets, that need to be sent. Specific applications of network architectures require different types of bridges. The following are examples of these bridges:

- Translating Bridges – These bridges link to similar MAC layer protocols. In cases where physical addressing is similar, bridges can be developed to link between MAC layer protocols that are not identical. An example of this would be a bridge connecting an Ethernet network to a Token Ring network.
- Learning Transparent Bridge – Has the capabilities to identify each network segment and creates address tables that originate from that specific network segment.

- Local Bridges – These are bridges that have a local area network connected on each side. If a bridge links a network over a wide area, it is referred to as a remote bridge. Each of these bridges has varying capabilities as far as transmitting data bandwidth. Remote bridges generally operate with lower bandwidth capabilities than local bridges.

Routers can provide greater control of data flow to a network as they become more complex. Routers operate at the Network layer of the OSI model. It works by opening the data packet delivered at the MAC layer and determines the routing destination by the information supplied. This additional work supplied by the router requires more processor time, memory, and network connections. Typical routers can support many protocols simultaneously, but this can lead to increased use of multiple third party routers on the network.

Routers work by forwarding a data packet to the appropriate network destination determined by the table of information that was created when the information was received. There are two types of tables that are created by the router, static and dynamic. The static table is updated manually as the network is modified while the dynamic table updates automatically as routers communicate via the RIP. This communication becomes important as networks continue to develop with increased data transfer speeds. As router technology develops, the ability to analyze data transfer on multiple network paths can provide added functionality for network load balancing and data backups. This functionality increases the ability to identify individual work groups as subnets, allowing for control of incoming and exiting data within the subnets and providing the greater

security controls needed to circumvent data intrusions. Security prevention may be as simple as applying password protection that restricts access to a particular network, workstation, or server, or may be as elaborate as using filters to limit access to specific routers subnets.

Gateways operate at all levels of the OSI model. They can provide content conversions between multiple environments and applications. Gateways contain both hardware and software components and provide both conversion and routing duties and can support full examination of data packet transfer. In other words, they can be used in situations to connect a network that contains different platforms and requires data translation or other application support. Examples may include connecting PC based workstations to a mainframe computer or connection of different mail based systems that are allowed to communicate with one another. There are different types of gateways that, depending upon the system architecture, can be used.

Repeaters amplify the electronic signal from one network segment to another. They are connected to similar segments that transmit similar data signals. Repeaters operate at the Physical Layer of the OSI Model and are not impacted by high-level protocol layers. From a basic perspective, the purpose of a repeater is to extend the physical length of a network segment. This remains one of the primary benefits, but there are potential issues such as:

- Repeaters don't filter out signal noise, so noise is amplified and sent with the signal. Because this problem exists, there is generally a limit on the number of repeaters that are used in a network segment.

- As signals are generated over large distances, time delays can occur which can generate timeout errors – keeping repeaters from being used for remote links.
- They do not help in reducing network traffic loads.

Internets

As mentioned earlier, DARPA's program helped introduce and develop the Internet, as we are accustomed to today. RFC 760 [8], published in January, 1980, was one of the earlier specifications that helped define the Internet. It was based upon five earlier versions of the ARPA Internet Protocol Specification. This specification describes the Internet Protocol as an interconnected system of packet-switched computer communications networks. Essentially, the Internet is a conglomerate of local area networks connected together by what is known as multiple 45-622 Mbps backbone circuits that are provided by a few dozen carriers across the continental United States. This system is considerably larger if considered (or looked at) from a worldwide perspective. There are four major access points in the continental United States along with multiple Metropolitan Area Exchanges where these circuits connect. From these points are hundreds of other carriers that interconnect at hundreds of points along these routes. Each of these carriers has redundant connections to points within the United States and points around the world. As these carriers continue to expand, network capacity increases, as does its ability to comprehend network failures and disasters.

Internet Service Providers

Carriers, or Internet Service Providers, use digital lines such as telephone lines from a local telephone company or cable lines leased from local cable companies to connect to the backbone circuits. This is a convenient and relatively inexpensive way to reach the end users. There are currently other vendors that are laying miles upon miles of fiber optic cabling, which at some point will replace the current mediums being used. Until that point, however, existing ISP's will continue to utilize present resources until the cost differentials force a change.

ISP's are comprised of telecommunications corporations such as telephone and cable corporations, and others that are specialized in the Internet business. They compete with each other to provide the end users Internet access. They provide high-speed connections to a backbone circuit along with hundreds of other lower speed connections to assure end users access when needed. The following diagram (Figure 2) depicts how an ISP might work.

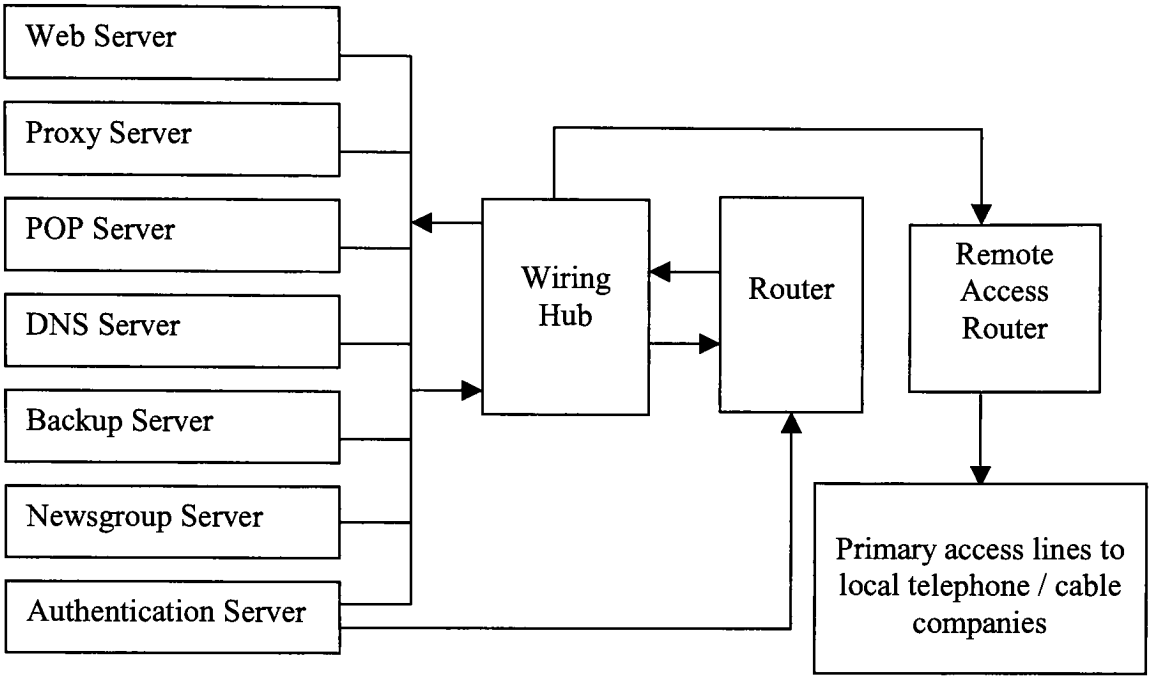


Figure 2 - Example of How an ISP Might Work

Domains

The structure of the Internet's naming convention, or IP addressing, can be cumbersome to both remember and use. Business organizations have adopted the use of acronyms to identify IP addresses. These acronyms represent a network device and can be easier to remember than an IP address. For this concept to work, a framework needs to be developed to map these names to their associated IP addresses. Originally, this framework was organized by the SRI Network Information Center. [9] They managed the specified names in a file called Host.txt that listed the names of the networks and gateways along with their associated IP addresses. This process worked adequately in the beginning of Internet usage, but as it grew, being able to administer this file became a huge (challenging, overwhelming task) job requiring large resources. To deal with this problem adequately, a system known as the DNS was devised. This system uses a hierarchical scheme to control the naming conventions. The advantage of this system is that it allows administrators the ability to manage network devices at a specific level of the hierarchy. For instance, a domain might have a subdomain as part of its tree, allowing the administrators to assign and control the rights without impacting other domains.

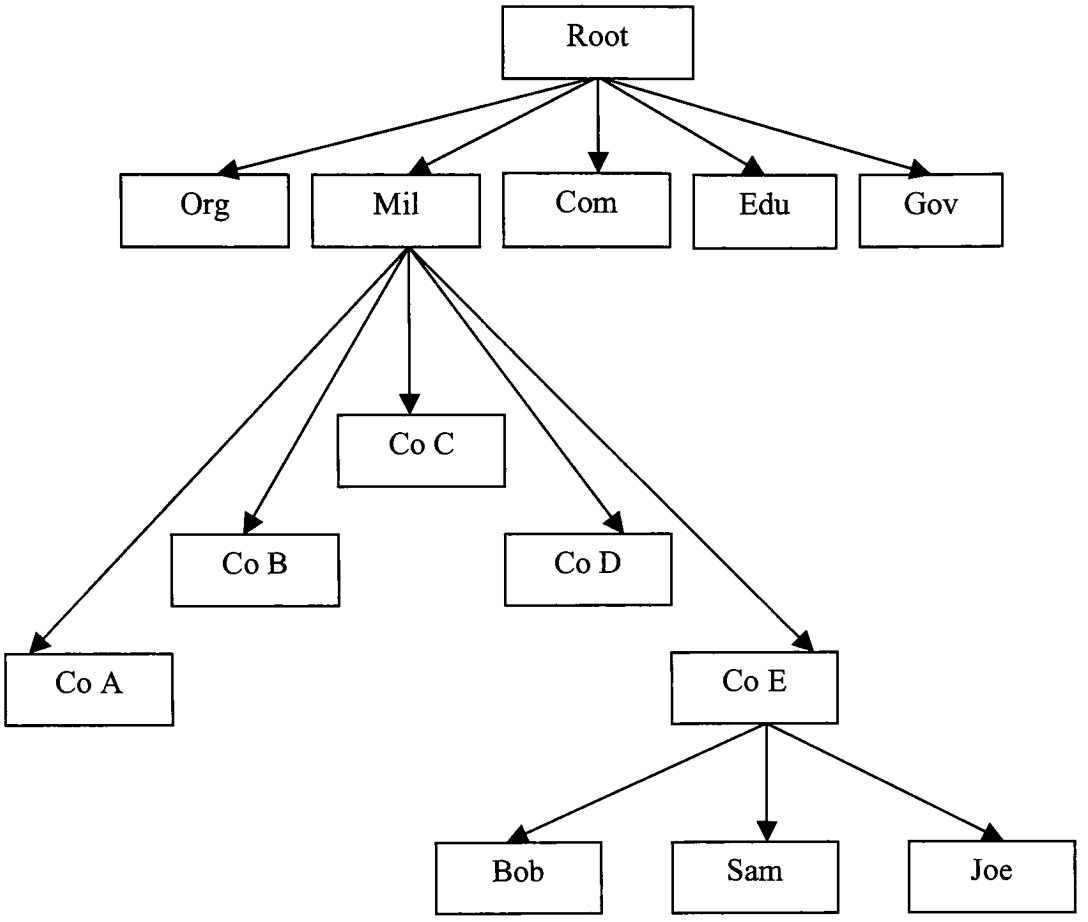


Figure 3 - Example of a DNS Structure

The example in Figure 3 is a representation of a hierarchical structure of a DNS that may exist somewhere in the Internet. The Root is the highest-level domain level of the tree represented by ORG (organizations not otherwise identified by other domains), MIL (military organizations), EDU (educational institutions), GOV (government), ARPA (arpanet), COM (commercial enterprises), and Con (countries using the ISO standard). Each of these root domains have subdomain levels of the tree which represent different companies such as Company A, Company B, etc. that represent zones of the domain.

Name servers have the responsibility of controlling specific zones or multiple zones and, for the most part, containing their own database structure. Name servers interact with other name servers by sending queries back and forth via TCP, which at the moment provides the greatest reliability and efficiency. The next subdomain level in the tree shows Company E with Bob, Sam, and Joe representing specific domains within the company structure. This level of the domain is the lowest level of the domain structure and is known as the leaf node because there are no dependencies associated with the domains. The DNS naming convention requires each name to be unique within the specific hierarchical level, but can use repetitive names in different layers. A major advantage of the DNS systems is that it gives the administrator the ability to set permissions and specific rights to specific domains as needed. The ability to manage these domains helps increase security by setting access rights and locking down end users and by controlling incoming and outgoing network traffic. Other advantages of DNS is its ability to support mail applications as well as containing information about local operating systems, device hardware, and specific applications that are being used.

Communication Architectures

Communication architectures allow a wide range of computer makes, models, and operating systems to communicate across a network or many networks. Architecture standards are based upon the very simple requirement that systems need to transfer data. Essentially, they are manufacturer's concepts for networking their devices together. From a simplistic viewpoint, a communication network consists of at least two communications centers (computers) and a medium to connect them. These computers and medium connections have associated tasks for which they are responsible. For example, Computer A will initiate a command to the network indicating a need to open a communication link to Computer B. File management applications on Computer A ascertain that Computer B is ready to accept a data transfer and needs to be prepared for file storage after it has been received. Once both systems agree on transmission and data integrity, file transfer takes place. This illustrates that many steps (or functions) need to take place for a successful exchange of data. These individual processes can be implemented as a single command, or can be broken down into different commands and implemented independently from each other. In this example, these tasks can be broken down into three tasks, which are structured modules. These modules implement communications functions and are referred to as a protocol architecture as depicted in Figure 4.

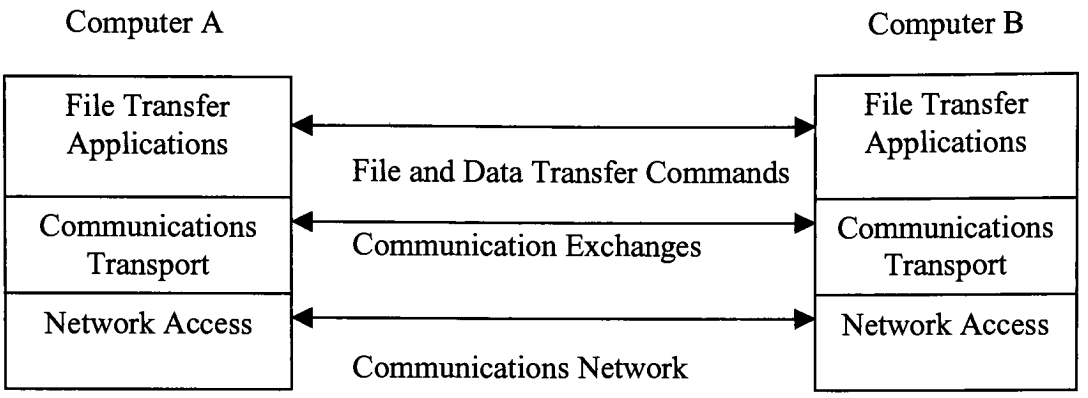


Figure 4 - Protocol Architecture

The three-layer model is organized as follows: network access, transport, and application. These layers are somewhat independent with feature sets particular to each.

The network access layer focuses on the exchange of data between the computer and network. Characteristics of this layer include providing network addresses and may include specialized services such as priorities. The transport layer verifies that the data arrives in the same order it was sent. The application layer contains the software needed to support any applications involved in the transfer, such as file transfer. These layers illustrate how network tasks can be broken apart into individual tasks, independent from each other. The advantages of this type of data structure are that vendors utilize different data formatting and exchange architectures, allowing communication from vendor to vendor without creating special purpose software to communicate. Common standards promote the benefits from a vendor's perspective, that implementation of their software will be widely accepted, and from the consumer's perspective, that they will not be forced to utilize one vendor's software. As business expands, the need for multiple vendor software programs to communicate is forcing these architectures to be

interconnected. Examples of vendor architectures include Digital Network Architecture (DEC), AdvanceNet (Hewlett Packard), Distributed Systems Architecture (Honeywell), Internet Packet Exchange (Novell Netware), and Xerox Network Systems (XNS). Today's standardized network architectures, or protocols, such as TCP/IP, OSI or SNA Systems Network Architecture, to name a few, were developed to permit allow manufacturers to attach communications devices of all makes and models to the network without having to redesign the network each time. These models in their early stages, however, did not provide for reliable communications. There were no acknowledgments as data packets traveled from point to point; nor were there acknowledgements from end to end transmissions. There was no error control feature for data, only a header checksum. If the ICMP detected an error, it would be recorded, but there were no re-transmissions. It became clear early on that IPv4 was not architected with security as a priority. It was only after its vulnerabilities were exposed that modifications became needed to protect the end user. In September, 1981, RFC 791[10] was published and became what is now known as IPv4. This specification replaced RFC 760, which describes the Internet's basic operations as follows:

1. The Internet protocol implements two basic functions: addressing and fragmentation. The Internet modules use the addresses carried in the Internet header to transmit Internet datagrams toward their destinations. The selection of a path for transmission is called routing. The Internet modules use fields in the Internet header to fragment and reassemble Internet datagrams when necessary for transmission through "small packet" networks.

2. The model of operation is that an Internet module resides in each host engaged in Internet communication and in each gateway that interconnects networks. These modules share common rules for interpreting address fields and for fragmenting and assembling Internet datagrams. In addition, these modules (especially in gateways) have procedures for making routing decisions and for other functions.
3. The Internet protocol treats each Internet datagram as an independent entity unrelated to any other Internet datagram. There are no connections or logical circuits (virtual or otherwise).
4. The Internet Protocol uses four key mechanisms in providing its service: Type of Service, Time to Live, Options, and Header Checksum (these mechanisms are described later).

With Internet specifications becoming standardized, virtually all computer vendors today support TCP/IP as the Internet based protocol to be used. OSI and SNA are other examples of important architecture supporting communications functions, but are not as predominant today as they once were. All protocol models have a corresponding function within its layering structure similar to the other models. For example, TCP operates at the OSI layer 4, and IP operates at the OSI layer 3. These common protocols allow tasks from one protocol to communicate with another protocol seamlessly to the end user. From these basic models, other protocols have evolved that supply other functionality such as SMTP, used for electronic mail, FTP, to transfer files, and SNMP, for network management activities. Figure 5 illustrates a high-level comparison between architecture protocols showing each protocol's corresponding layer to the other.

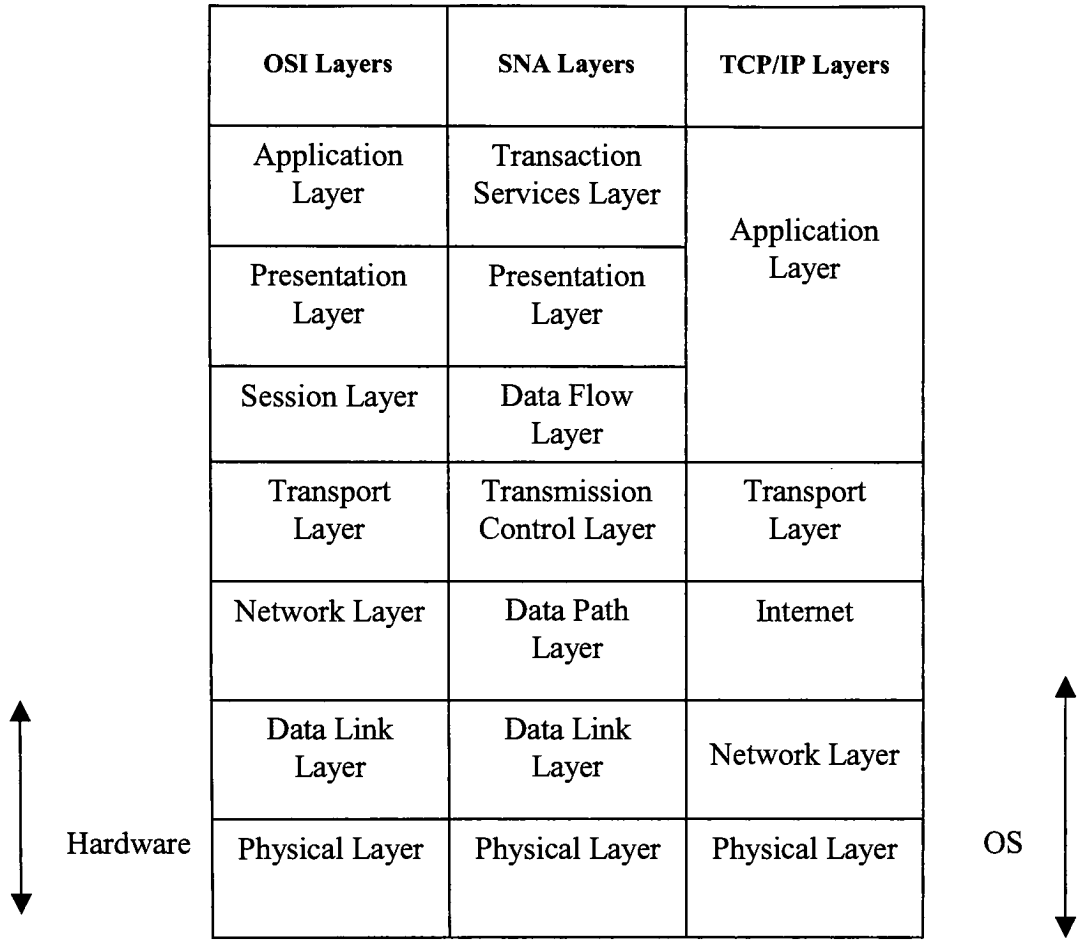


Figure 5 - Comparison Between Architecture Protocols

OSI Model

The OSI model was developed by the ISO as a model for protocol architecture standards and for other protocols to use as a guide for development. It is made up of seven layers that provide different functionality at each layer. The basic intent of the OSI model was for other developing protocols to develop their functionality using the layered concept, with the hope that proprietary implementations of specific protocols would eventually be replaced. As many functional protocols have been developed and have consistently used the OSI architectural model, the concept did not meet its anticipated growth and was instead replaced by TCP/IP. There are a number of reasons for this, including the complexity of the seven-layer approach, but the most predominant reason was, most likely, timing. The TCP/IP architecture was tested at a stable point when business needed an architecture that would address the need of operating across multiple networks. OSI was still in its development stages. Even so, the OSI model did have merit and was used extensively.

The OSI model, as mentioned, is a seven-layered communications protocol, internetworked together to common communication devices. The development of ideas behind the OSI model followed a few basic concepts:

- Each layer performs its own function.
- Layers should be developed with the intent of future protocol standardization.
- Boundaries are clearly identified between layers.
- Develop enough layers so that specific data transfer functions can be distinct, and placed properly in a layer.

The OSI layers are:

- Application – enables access to the OSI architecture structure and provides informational services functionality. Other functions of this layer include file transfer that can handle services such as electronic mail and directory look-ups.
- Presentation – deals with the syntax of the data transmission by performing repeatable tasks. An example might be a specified, agreed upon encoding service among computers on different networks. The presentation layer verifies and corrects the incoming and outgoing data.
- Session - provides a structure between systems that allow connections and terminations.
- Transport – enables reliable data transport by monitoring data flow and providing error recovery by making sure the data arrives correctly. Data may be divided among networks to improve transport efficiency.
- Network – responsible for controlling the operation of the subnet by establishing, maintaining, and terminating connections
- Data Link – sends data frames of information across the network. This layer also checks for transmission errors by creating and recognizing data frame boundaries. The data link layer will solve issues that occur if data is lost, damaged, or duplicated.
- Physical – responsible for the basic transmission of data over the network medium.

Figure 6 depicts how data transfer occurs in the OSI model by each defined service providing a service to the layer above it. This hierarchical approach allows each layer to be developed and continue to evolve independently of the other layers.

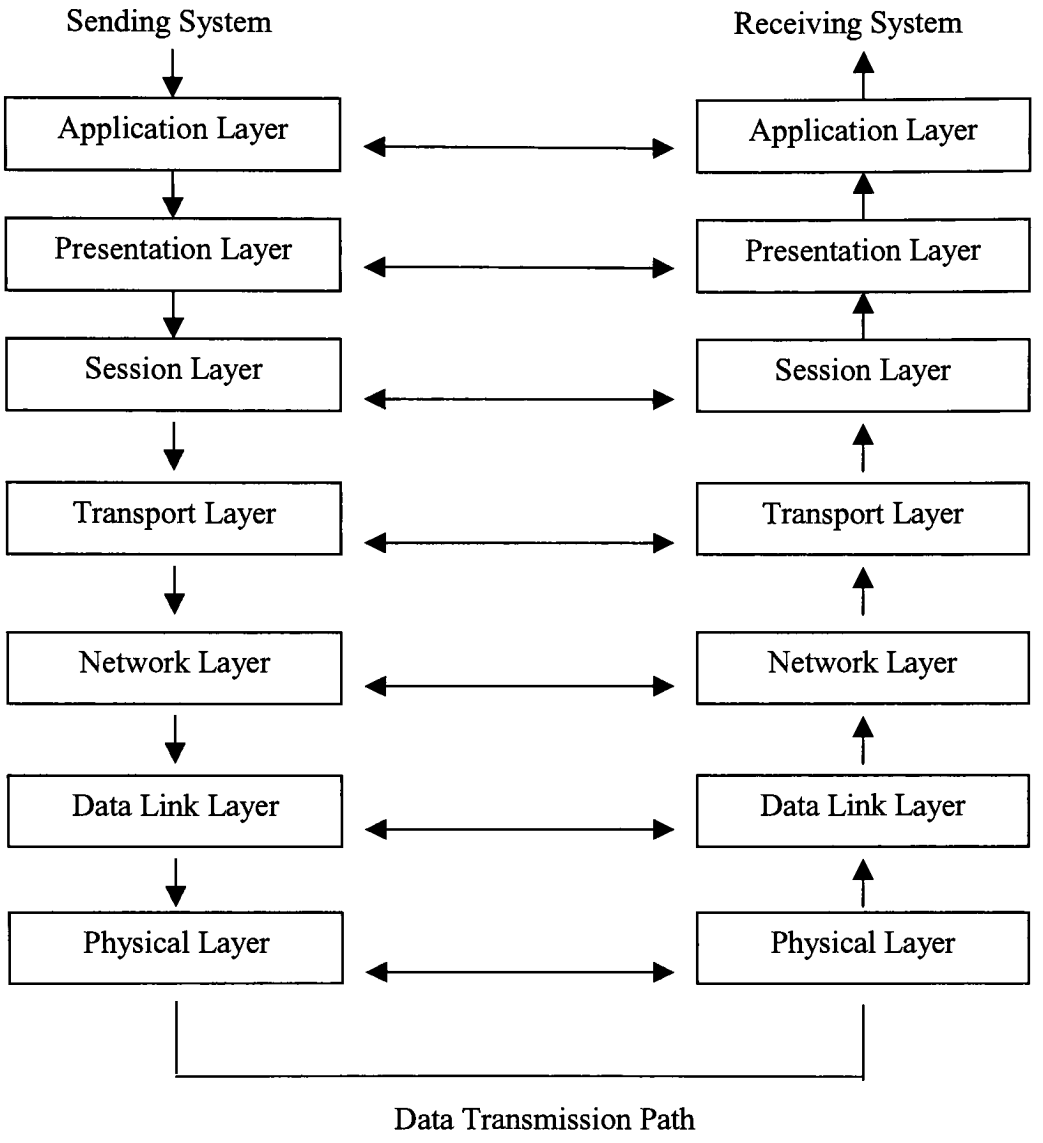


Figure 6 - OSI Data Transmission

TCP/IP

TCP packages and prepares data for transfer. IP is responsible for establishing the framework needed for getting the data transferred successfully across the network. It allows the exchange of information between different types of networks that attach to an IP gateway. Together, TCP/IP is a protocol suite that organizes software communications to share resources across networks. It is the Internet based standard and the framework for many other communication protocols. Within this protocol, data is passed through multiple layers of the protocol architecture that are identified to a device, operating system, or specific task. This process has been standardized by the IAB. Within the IAB are committees that issue RFC's and STD's. The advantages of having a common protocol are to allow computers with different operating systems to communicate. This advantage also has a downside by providing potential openings for security intrusions to take place. These layers of the protocol have different functions in data handling. The current model of the TCP/IP protocol suite can be grouped into five separate layers. These layers provide different tasks that allow the transfer of data from one host to another. These layers can be broken down as follows:

- Application Layer – physical interface between a device such as a computer and the network. This layer defines the transmission medium, type of signals used, rate at which data is transferred, and any other characteristics associated with moving the information through the network.
- Transport Layer – focuses on the data exchange between peripherals and the connected network.

- Internet Layer – these are the procedures or routing functions that allow data to be transmitted across multiple networks.
- Network Access Layer – deals with the exchange of data (accessing and routing) between computers and the network to which they are attached.
- Physical Layer – deals with the physical interfaces between data senders and receivers such as computers and the transmission medium. The concerns of this layer surround medium characteristics, signal characteristics, data transfer rates, and anything else that may impact the transmission.

Internet Protocol

IP is a connectionless service that permits network traffic between hosts, using a 32-bit address scheme to identify the host computer and associated network. IP does not have the capability to identify and reply to data transmission errors. Its design was meant to be transparent to or independent of the network. If, for example, a datagram transmission passes through a router and violates an established aspect such as size, the buffers will overflow and remove the remaining datagrams. Unless a higher-level protocol such as TCP recovers this type of information, datagrams can be lost, duplicated, or arrive in no specific order. The design of IP allows for easy installation and provides a robust protocol, but as indicated, no error recovery or data flow analysis. These responsibilities reside at the TCP layer.

When a computer is hooked up to the Internet through an ISP, an address is assigned that identifies that particular computer to the world. All devices that are connected to a network require an IP address that conforms to the Internet Protocol naming convention (Figure 7).

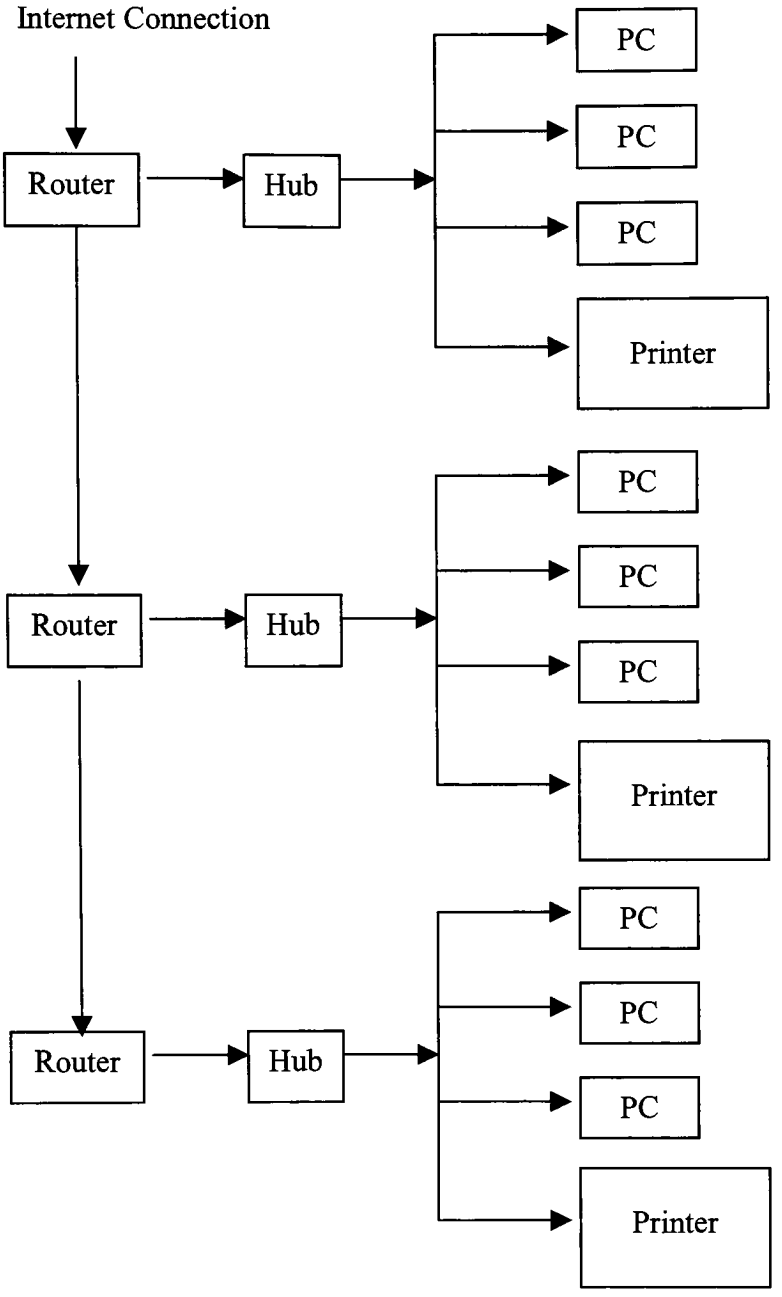


Figure 7 - Example of Multiple Devices Connected to a Network Requiring an IP Address that Conforms to the Internet Protocol Naming Convention

This naming convention was devised to allow administrators the ability to control networks within their LANs. The current addressing scheme within the IPv4 protocol uses an address with 32-bits. When traffic is initiated through the network by a device such as a computer, it passes through the transport layer, typically TPC or UDP. The address is broken into two parts, one that identifies the subnetwork and the other that identifies the node on the subnet. The data traffic is identified by a protocol ID. After the receiving device has acknowledged it is ready to receive the data traffic, it is passed to the network layer, which takes care of the network addresses, or IP addresses. IP addresses are used to determine where the traffic is to be routed in the Internet and are identified by formats known as Classes. There are four Classes: A, B, C, and D (Figure 8). The first portions, or bits, of the address indicate network identification addresses and the remainder of the class indicates the number of hosts that can be identified in the network. Each class signifies a different network addressing schemes that would be available if that specific architecture were selected.

Class A

0	Network (7 bits)	Host Address (24 bits)
Maximum number of network numbers is 126		
Maximum number of host numbers is 16, 777,124		
Nomenclature – network.host.host.host		

Class B

10	Network (14 bits)	Host Address (16 bits)
Maximum number of network numbers is 16,384		
Maximum number of host numbers is 65,534		
Nomenclature – network.network.host.host		

Class C

110	Network (21 bits)	Host Address (8 bits)
Maximum number of network numbers is 2,097,152		
Maximum number of host numbers is 254		
Nomenclature – network.network.network.host		

Class D

1110	Host Address (24 bits) – Multicast Format

Figure 8 - IP Address Formats

Depending upon network requirements, other variations of these classes can be chosen. These are specifically geared towards Internet usage. If a network is not going to be accessing the Internet, then choosing a class will depend upon considerations such as ratio of networks to host machines and future growth of both, networks and host machines.

The data sent by the host computer that is routed through a network is known as an IP datagram or PDU. These data units can be divided, or fragmented into smaller, more manageable units by a fragmentation process that is supported in the IP protocol. This is needed because node devices would be required to solve incompatible PDU sizes between devices otherwise. Figure 9 shows how an IP datagram, or PDU, can be broken down into fields that describe how information is processed when using the IP protocol.

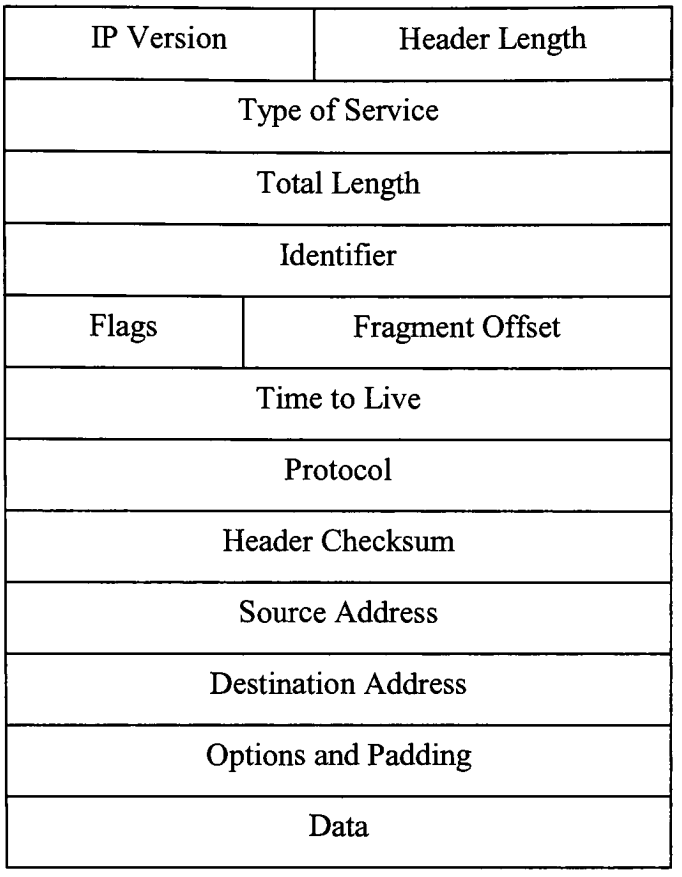


Figure 9 - IPv4 Datagram

IPv4 Datagram field descriptions:

- IP Version – identifies the version of IP in use. This is contained in most protocols with the current version at 4 or commonly referred to as IPv4. The next generation is identified as 6, or IPv6.
- Header Length – this field contains 4 bits that indicate the length of the datagram header.
- TOS –identify quality-of-service functions (data transit delays, data throughput, data precedence, and data reliability) that are provided for the Internet. Currently

some vendors do not use the TOS field in their implementations of IP, but increased capabilities of the Internet may promote increased usage.

- Total Length – this is the total length of the datagram measured in octets and includes the length of the header and associated data (determined by subtracting the header length from the total length of the field).
- Identifier– controls datagram fragmentation and repair along with Flags and Fragment Offset. This field identifies fragments in a datagram.
- Flags – this field determines whether the datagram can be fragmented.
- Fragment Offset – contains a value that specifies a position of a fragment within the original datagram.
- Time-to-Live – measures amount of time a datagram is in the network by adding a value to the parameter whenever a datagram passes through an IP node such as a router.
- Protocol – identifies the next layer protocol that will receive the datagram.
- Header Checksum – detects any errors that may have occurred in the header, but will still require a higher-level protocol to perform error checks on user data if required.
- Source Address – contains the Internet source address in the datagram.
- Destination Address – contains the Internet destination address in the datagram.
- Options – not used in all datagrams, but can be used for specific applications such as network management and diagnostics.
- Padding – ensures that the datagram header is aligned correctly.
- Data – contains user data.

IP datagrams identify how network information is broken down and evaluated at its lowest level, but also has specific services that it can perform for different vendor products. Depending upon the network architecture, some IP services will not be utilized. When information is received at a router, IP verifies the header to determine the type of network traffic it will be processing. If, for example, the information is a datagram, the router will pass the information onto the header check, which will check for header length, IP version numbers, message length, valid header checksum, and time in the network (making sure this value is not at zero). If the information is accepted, it will be passed to the next IP device; if the information is not accepted, it will be discarded.

IP also has different ways it can route information such as:

- Source routing, which allows the upper-layer protocol to determine how the routers will direct the datagrams. Looking at the addresses in the source routing field to determine the next IP destination accomplishes this. If the required datagram fields indicate that the routing list has been completed, then the destination IP address is used. If the routing list has not been completed, then the pointer increments IP addresses by one to the next address in the route.
- Route recording is another example where IP uses the next address in the data field to determine the next step the datagram will take. The difference here is that the receiving IP device will add its IP address to the route. This happens after the receiving IP device checks field lengths to determine if the recording list is full. If the module is full, it will forward the datagram without inserting an address to the next octet opening, where the address is inserted and the datagram is moved forward to the next IP device.

- Time stamping the datagram as it passes through IP devices is another service of IP. This allows for tracking the data route as it passes through the network and shows the amount of time it takes to process data between each IP device. The advantages of time stamping allow networks to be analyzed for efficiency.

Internet Protocol Version 6

The Internet has grown so rapidly that it has forced change in the way the original IPv4 protocol was designed. From a historical perspective, Arpanet was designed as a packet switching network that contained four nodes. It was designed at a reduced scale because the original concept was for its use in research, design and educational arenas. As visibility of the Internet gained momentum, organizations other than government and education took notice. The IETF began looking at proposals that would define the size of the address space required for the configuration. With the understanding that the Earth's population would grow substantially, and the belief that anyone who wants to access the Internet should be able to do so, technological progress became imminent. After taking into account that users will, most likely, be accessing multiple computers (not only the ones on our desktops, but those that are incorporated into our everyday lives), it became evident that a new version of the Internet Protocol would be needed to comprehend the added demand.

Essentially, the major difference between IPv4 and IPv6 [11] falls into the following areas:

1. Expanded Addressing Capabilities: IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy, a much greater number of addressable nodes, and simpler auto-configuration of addresses. The scalability of multicast routing is improved by adding a "scope" field to multicast addresses. And a new type of address called an "anycast address" is defined, used to send a packet to any one of a group of nodes.

2. Header Format Simplification: Some IPv4 header fields have been dropped or made optional, to reduce the common-case processing cost of packet handling and to limit the bandwidth cost of the IPv6 header.
3. Improved Support for Extensions and Options: Changes in the way IP header options are encoded allows for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.
4. Flow Labeling Capability: A new capability is added to enable the labeling of packets belonging to particular traffic "flows" for which the sender requests special handling, such as non-default quality of service or "real-time" service.
5. Authentication and Privacy Capabilities: Extensions to support authentication, data integrity, and (optional) data confidentiality are specified for IPv6.

Initial concepts of the design began in 1991, and by 1995 four RFC's (Figure 10) were introduced. These RFC's (1883-1886) [12] were to become the new version of the Internet, classified as IPv6, and will incorporate new features that comprehend increased usage and eliminate specific problems that have evolved in IPv4. Ipv6 will address specific issues such as address space, inefficient operations, and network architecture techniques that incorporate greater functionality and improved security. Many of the characteristics of the IPv4 protocol will be retained for the time being, because of their dependencies on other related protocols that have been developed extensively to support existing transmissions such as video, data, and voice. Considering that IPv4 uses 32-bit address spaces, the new configuration would allow for significant expansion to support the increased demand without the concern of running out of address spaces. From a

numerical value, there are many possible addresses that could be used, but partitioning of this address space into similar IPv4 classes (A, B, C, D) has increased space limitations, especially in the class C space which has the highest number of networks associated with it. Its possible to increase subnetting more classes into class C, but that was not a viable option for the IETF board because class networks have fixed boundaries between identification of network and nodes. When a network number is assigned, all the host addresses for that network are assigned to that network. For example, if a network needed 500 addresses, it would not be able to use class C addresses because it contains only 256 addresses. It would have to be assigned to class B which contains 65,536 addresses. Seeing that the network would only be using 500 addresses, the remaining 65,036 addresses would become invalid or wasted. The inefficient use of this IPv4 addressing scheme, coupled with the rapid increase in demand for IP addresses has led experts to anticipate running out of addresses in the next ten to fifteen years.

From a security standpoint, the importance of incorporating security mechanisms within TCP/IP applications became paramount in the 1990's as intrusions became more commonplace. Although many of the TCP/IP's applications have security mechanisms built into them, it is far more effective to have these mechanisms integrated at the lowest possible protocol layer. IPv4 was not designed with security in mind and, as a result, authentication and data verification were basically absent. IPv6 has deviated from the IPv4 architecture and integrated two security schemes, IP Authentication Header and IP Encapsulating Security Payload into its protocol.

RFC 1883	This RFC specifies the basic IPv6 header and the initially defined IPv6 extension headers and options. It also discusses packet size issues, the semantics of flow labels and priority, and the effects of IPv6 on upper-layer protocols.
RFC 1884	This RFC defines the addressing architecture of the IP Version 6 protocol [IPV6]. The document includes the IPv6 addressing model, text representations of IPv6 addresses, definition of IPv6 unicast addresses, anycast addresses, and multicast addresses, and an IPv6 nodes required addresses.
RFC 1885	This document specifies a set of ICMP messages for use with version 6 of the Internet Protocol. The IGMP messages specified in STD 5, RFC 1112 have been merged into ICMP, for IPv6, and are included in this document.
RFC 1886	This document defines the changes that need to be made to the Domain Name System to support hosts running IPv6. The changes include a new resource record type to store an IPv6 address, a new domain to support lookups based on an IPv6 address, and updated definitions of existing query types that return Internet addresses as part of additional section processing. The extensions are designed to be compatible with existing applications and, in particular, DNS implementations themselves.

Figure 10 - RFC's 1883 – RFC's 1886

The IP AH is an extension header that provides authentication and integrity for data packet transfer. They compute a cryptographic authentication function over the IPv6 datagram utilizing an authentication key for encryption. Many other types of

authentication applications can be supported, but the use of the keyed MD5 [13] algorithm is needed to ensure proper operation. By using this algorithm, many network attacks such as spoofing can be eliminated. Because IP is located on the Internet layer, it can provide host authentication, which was a shortcoming with IPv4. IPv4 was only able to include the sending host's address as indicated by the sending host's datagram. The IPv6 extension headers are inserted between the Internet header and payload fields and used to identify the next header for the datagram (Figure 11 and Figure 12).

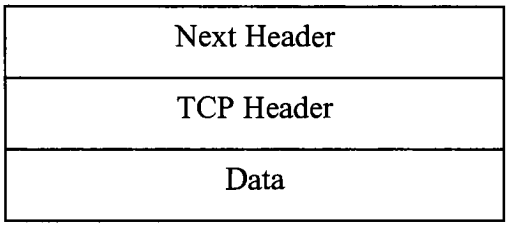


Figure 11 - Indicates No Header Extensions

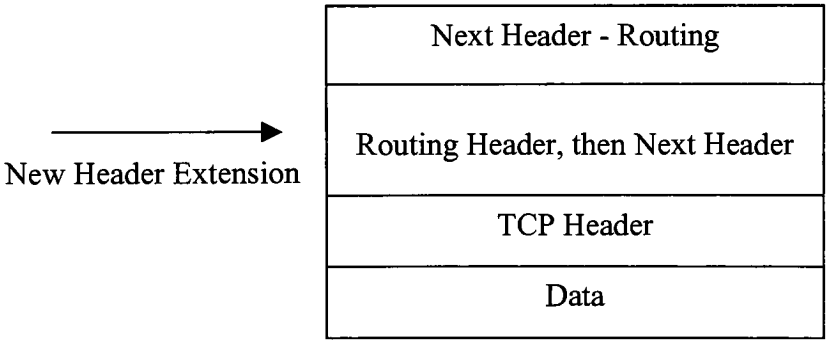


Figure 12 - Indicates One Header Extension

The header will be identified by its header type, which also contains the header type of the next header in succession. The IPv6 protocol identifies six extension headers:

- Fragment – IPv6 is similar to IPv4, but will not allow fragmentation of PDU as IPv4 did unless they were fragmented before entering the network. This will reduce the processing time required to route the datagram to the next device in the network.
- Hop-by-hop Options Header – used for in-process operations such as error detection and network management activities at intermediate devices, or nodes (also known as hops), during data transfer. A similar service is used in IPv4 (payload) that allow large PDU's whose lengths exceed the 16-bit length field to be sent. But, in IPv6, a processing node uses a field in the hop-by-hop options header to determine how to process the PDU before sending it onto the next device.
- Authentication – sending and receiving parties both agree on an encryption algorithm before data transfer takes place.
- Routing – similar to the IPv4 routing header, which carries an IP address list, which the datagram is routed to. The difference in IPv6 is the device node can identify a routing header by looking at the destination field of the header. If it is identified as a header extension address from a different source, it may be ignored, thereby reducing processing time to route the information.
- Encrypted Security Payload – data field authentication depending upon specific encryption and authentication algorithms used.

- Destination Options Header – provides for transparent relay of information through a network, but also contains an options field that has the ability to generate a report indicating a problem has occurred.

Figure 13 summarizes address header fields between IPv4 protocol and IPv6 protocol.

IPv4	IPv6
Contains a Version Identifier – 4	Contains a Version Identifier – 6
Contains header length field	Payload length replaces IPv4 total length field
Contains TOS field	Eliminated TOS field, but retains some functionality which is located in priority and flow label fields
Contains identification, flag, and fragment offset fields	Identification, flag, and fragment-offset fields are eliminated, but some functionality is retained and placed in optional header extension.
Contains Protocol field	Protocol function remains in another extension header
Contains TTL field	TTL field renamed to Hop limit field
Contains header checksum field	Header checksum field eliminated because most networks already contain error checking at different layers of the protocol
Contains Options field	Options field is replaced with

	header extensions

Figure 13 - Comparison Table Depicting IPv4 and IPv6 Header Fields

With authentication information located at the Internet Layer in IPv6, increased protection to higher layer protocols and applications will result in greater network security, as authentication protection is now part of the protocol.

The other integrated IPv6 security mechanism is IP Encapsulating Security Payload ESP. This mechanism is fully described in RFC 1827, and is an extension header that provides integrity, authentication, and confidentiality for IP data packets. As with the authentication header, ESP is algorithm independent, but should be used to ensure proper authentication effectiveness. ESP works in IPv6 by surrounding either the complete datagram or the upper layer protocol data inside the ESP, and encrypting the contents so a new IPv6 header is appended to the ESP. The receiver of the datagram then removes the appended header, decrypts the datagram, and processes the data in its original form. This mechanism can be used to encrypt an entire data packet or a portion of a higher layer segment located on the transport layer. This ability to encrypt and decrypt datagrams in IPv6 adds to the overall security while reducing the effort required to authenticate network data on both ends of a communication transfer.

To ensure an adequate supply of addresses, IPv6 is based on a 128-bit address scheme. In theory, this addressing scheme would be able to support 2^128 addresses. The new addressing scheme can be broken down into four-bit integers, each represented by a

hexadecimal digit. They will be clustered together as eight (4 hexadecimal digits) separated by colons (Figure 14).

U8H4:JD88:DKIE:3JDE:E03W:DJ39:DMC9:DI39

128-bit Address Scheme

Figure 14 - Example of 4 Hexadecimal Digits Separated by Colons

It is quite possible that early implementations will use zeros in place of some of the 128 bits. In this case, the address string can be shortened with a zero. If a complete 4 hex digit cluster has a value of zero, then colons can replace it as shown in Figure 15.

U8H4::DKIE:3JDE::DJ39:DMC9:DI39

128-bit Address Scheme

Figure 15 - Example of a Complete 4 Hex Digit Cluster with a Value of Zero

Even though IPv4 address schemes utilize a dot form (12.345.6.7), IPv6 will still be able to incorporate it into the new scheme by adding the colons where needed (::12.345.6.7). IPv6 also incorporates a hierarchical scheme compared to the flat address scheme used in IPv4. The format of the address contains a prefix with five hierarchical subfields listed in the specified order as shown below:

- Prefix – IP address
- Registry ID – allocating Internet addresses
- Provider ID – ISP

- Subnetwork ID – ISP assigned subscriber ID
- Subnetwork ID – subscriber subnetwork
- Interface ID – subnetwork host address

Other addresses such as OSI's Network Service Access Points and Novell's IPX are also supported in the IPv6 framework because of their current widespread use in IPv4. In these cases, a prefix can be used to support an organization's private addresses within its WAN, but cannot be utilized on the Internet. IPv6 also continues to support multicasting as did IPv4, but adds additional functionality that is able to contain the scope of the multicast function to a local network.

As mentioned earlier, data sent by the host computer that is routed through a network is known as an IP datagram. The IPv6 datagram has changed from its predecessor in IPv4. Figure 16 shows the datagram broken down into fields that describe how information is processed.

Version (4 bits)	Priority (4 bits)	Flow Label (24 bits)
Payload Length (16 bits)		
Next Header (8 bits)		
Hop Limit (8 bits)		
Source Address (128 bits)		
Destination Address (128 bits)		
Data Variable		

Figure 16 - IPv6 Datagram

IPv6 Datagram field descriptions:

- Version – identifies version of the protocol.
- Priority – similar in characteristics to the precedence field in IPv4, this field supports different types of network traffic such as voice, video, and data, and can be coded to indicate 16 possible values.
- Flow Label – new to IPv6 and designed to handle different types of network traffic such as voice, video, and data.
- Payload Length – identifies the length of the payload. Its length is 16 bits, but is supported within the protocol for longer lengths by utilizing the next header field.
- Next Header – replaces the option field in IPv4 and identifies the next header as either TCP or UDP. This identification scheme simplifies the processing of a data packet because the header is now a fixed length.

- Hop Limit – identifies the number of hops the datagram has while transmitting in the network.
- Source Address – contains the Internet source address in the datagram.
- Destination Address – contains the Internet destination address in the datagram.
- Data Variable - contains user data.

Intrusions and Detections

Computer intrusions or attacks can occur in several different areas of a networked system. Early intrusions were simplistic in nature, mainly associated with exploiting poor password practices or gaining access to systems that were not originally designed for security. Once these intruders gained access, they manulipated vulnerabilities that were well known, but went unrepaired. At this time sophisticated techniques were not needed because systems were designed with default settings that made accessing systems relatively easy. Taking security as a design consideration was not practical, nor did system administrators have the tools or expertise to modify or monitor their systems for intruder activity. As intruder knowledge became more sophisticated by an increased understanding of network integration, system operations, and network protocols, techniques to protect network system infrastructures also needed to become more complex to ward off attacks to known system vulnerabilities. Intruders began migrating to source code, looking for weaknesses in programs. Unfortunately, many programs were written without much thought focused on security. These programs became easy targets because of their easy accessibility on the Internet.

Before any action to introduce a security system into a network begins, an overview of system requirements should be taken. Specific objectives need to be in place regarding the amount of security needed that address disaster recovery plans should a breach occur. This is generally known as a company security policy and is a documented plan for organization wide computer and information security procedures. These plans are the

framework for making decisions that pertain to all aspects of a network. They include different aspects of a network:

- From a high level, these plans contain descriptions of the technical networked environment, legal aspects, if any, and any overall interpretations that may be required to operate the system.
- Some form of risk analysis that defines potential threats and recovery plans if the network should be compromised is recommended. Recovery plans generally define the critical business assets and which areas, functions, and or services would need to become operational in order of importance. There are trade-offs in these situations, and these types of policies require a risk/cost assessment analysis to determine the amount of investment needed to meet the overall business objective of that network. By identifying the risks and the potential consequences, a better-controlled detection and prevention environment exists. This allows the security strategies to be integrated into the overall policy and makes monitoring and tracking more efficient. Once understood, a plan, or a security system audit takes place that defines a business mentality towards security within that network.
- Guidelines for system administrators to define and manage systems under their control.
- Guidelines for users as defined by the overall security plan.
- Guidelines for dealing with legal aspects of an attack, from law enforcement with the intent of tracking the intruder to system shutdown and its associated ramifications.

These aspects of a plan are part of an overall framework that also requires management commitment to support the plan from enforcement to ensuring awareness that all users

are informed of policy specifics, as well as supplying adequate provisions for training and materials. These materials include systems that provide authentication tasking, system audits for security accountability issues, encryption systems and effective data storage facilities, and tools needed for hardware such as firewall and proxy servers. Other areas that should be looked at are security procedures that are based on the security plan that was drawn up for that network. These procedures might be implemented by system administrators with the intent of protecting data as well as ensuring that end users understand their roles in security maintenance. Recommended practices could entail aspects such as:

1. Accounts have valid passwords that are difficult to guess. Changing passwords regularly has its obvious advantages, but can also become frustrating for end users who need to keep changing them. This can lead to sloppy storage of passwords because users have a tendency to forget them, so they will post them in spots they remember and, therefore, can be easily found. Another way to prevent this is by using a one-time password system that initiates a password to make a connection before system confidentiality can be broken. An example of this is remote dial-up connections where a user is required to logon to a network before he/she can access personal data and other network resources. They are required to authenticate and identify themselves to the server by inputting a username and password. Because it is important that passwords are not reused, one-time password systems incorporate technology that synchronizes a code initiated by a device carried by the user and a corresponding code that will be recognized by the server. These devices work by displaying a random code, or numeric password, that remains in effect for a limited time. These codes are not repeated, and are

available for a short time span. Once this code is inputted as a password, the server in order to grant network access will verify it. If the user fails to input the correct code sequence, he/she will need to use the next random code that appears on the remote identification device. The constant changing of these password codes greatly reduces the chances of intruders accessing the network at entry points that require an initial password.

2. Utilizing strong encryption tools to maintain the integrity of the system. Intruders often try to gain access to networked systems by imposing themselves as trusted parties. They do this by acting as a trusted partner using a denial of service attack and attempt to connect to the target server as the original trusted party. To circumvent these types of attacks, it is necessary to monitor all incoming and outgoing network traffic. These devices are known as firewalls, which are a combination of hardware and software designed to monitor and analyze network data streams and service requests made upon the server. They analyze each data packet and eliminate the ones that do not meet the established security criteria. A firewall may be as simple as a router that filters data streams and discards unauthorized data packets that contain unrecognized sender addresses or attempt connection to unauthorized service ports. As firewalls become more sophisticated, they begin to incorporate proxy servers that authenticate requests, verify content integrity, and forward the data packets to the appropriate hosts. If a network is going to maintain a high level of security confidence, it will need to be monitored continuously. Additional tools to monitor the network can be placed at prescribed locations for effective monitoring. These tools can be setup to scan, monitor, and eliminate viruses that have been identified on the network. They are also used to

notify system administrators by various methods such as email and pager when a monitor detects unusual activity. Depending on the capabilities of the system, it is feasible to expect these tools to have the capabilities of not only isolating and detecting unwanted activity, but be able to counter it by blocking or disconnecting connections, limiting or removing services, and providing data analysis of the activity.

3. Developers incorporating security techniques when writing software code. This may require commitment from management as part of their security plan because it will usually entail longer timeframes to code the software, impacting schedules.
4. System administrators need to be kept abreast of vulnerabilities and incorporate the required changes in the system as soon as possible.
5. System Administrators need to keep up to date with the latest patches and fixes that become available from software vendors such as Microsoft.
6. Monitor any security instances that may impact networks by on-line security forums, which can show specific intrusion techniques and what preventative measures, can be taken to avoid them. A good example is the Melissa Virus, which was first, found in 1999 and executed a macro in a Word document that was attached to an incoming email. When the email attachment was opened, the macro forwarded the Word document to fifty additional users in the user's Outlook address book. This continued as each user opened the attachment and spread very quickly to thousands of computers. When Microsoft realized the virus was a problem, they posted, on their web site, the latest patches that would fix the problem. In this instance the system administrator would have needed to access the on-line site for instructions to install and implement the software. The site

would also explain any preventative measures that could be taken to prevent future outbreaks.

7. Checking for regular system audits to check system logs for any anomalies that can detect and trace intrusions.

Once overall procedures are in place or understood, two other aspects of a security system should be looked at when determining the objectives of a network, physical and logical. The physical aspect pertains to access to the system resources such as network and data equipment, including internal and external hard drives, CD's, and backup equipment. The logical looks at security that can be accessed through the Internet. [14] These areas can include:

- Monitoring of system resources and having access to root directories, files access, and registries.
- Network connections access.
- Defined security management of the users, groups, and monitoring of resources on the network. This includes permissions and user rights to specific directories.
- Accounts and administrative policies, which include licenses, expirations, auditing, and intruder detection.
- Authentication strategies of local and remote secure cards.
- Security strategies such as Certificate Authorities, encryption techniques, and digital signatures.

From a network security perspective, most intrusions occur from within corporate firewalls. Effectively deploying security functionality means systems need to be specifically designed and broadly employed to meet current and future breaches. Historical background information can help define some of the security perspectives we have today. The concepts of protocols are developed from a progression of changes in networking systems. Microsoft for instance, has identified a progression of changes since the early 1980's that have impacted their design philosophies of current Information Technology systems. [15] Some of the most prominent are:

- User-related data requiring a growing share of the computer's registry.
- Greater differentiation of "named objects" requiring greater organization.
- Additional services are utilizing their own process space in the operating system.
- Servers are becoming specialized, catering to specific applications.
- Functional management areas are becoming very application specific.
- Distributed systems are utilizing greater security systems in their networks.
- Distribution of security information improves performance and fault tolerance.

These trends show the transition from personal computers to workgroup models to domains as a step from stand-alone systems to distributed networking systems. Fundamental changes from workgroup methodologies to hierarchical methodologies helped form the structure seen with current scalable system architecture design. This is also evident in protocol design methodologies as seen in the TCP/IP, OSI, and SNA protocols. These hierarchical methodologies can also be cross-referenced against other protocols to identify functional area boundaries within security systems. The advantage of identifying functional areas within a protocol is that it allows for greater

troubleshooting capabilities when a security incident takes place. The ability to narrow components that may be a part of the intrusion can be advantageous in quickly getting the system cleaned and operational again.

Identifying the types of attacks on a network system can be a daunting task considering the sheer volume of attacks that occur and the many avenues from which they can occur. With intruders having access to networks via the Internet, infrastructure components such as routers, gateways, firewalls, etc., have provided avenues where illicit behavior can be hidden. A Trojan horse attack, for example, might be hidden by the fact that network authentication might be altered from system administrators, allowing access to a system without raising a red flag that indicates unauthorized use. Another example is Internet protocols such as the NFS, which allow systems to share files, but do not have the ability for user authentication. Software designers, especially with designs surrounding IPv4, often did not include security in the initial stages and found themselves adding these requirements after initial designs were completed and implemented. Consequently, these additional components of the design had holes in them, which were exploited.

Although design considerations are vital to the security of a networked system, vulnerabilities can exist from poor implementation procedures. This also can include flaws in the software that were not identified before its release. These types of vulnerabilities have a wide range of classes and subclasses that can be exploited by attackers utilizing their own tools. Examples of these types of classes are:

- Misuse of system calls.

- Reusing system modules for purposes other than their intended use.
- Ineffective checks of the operating system.
- Ineffective and incomplete checking of success or failure conditions.
- Inability to verify when resources are depleted.

These are examples of vulnerabilities caused by the particular way the protocol components have been setup. If, for example, a network protocol was setup with inadequate logon values or defaults, and system administrators fail to change them, this could potentially allow intruders to access the network. For instance, an FTP service generally requires their password files and associated logon files to be separate from the rest of the operating system. If the anonymous FTP logon defaults were configured improperly, unauthorized users might be able gain access to authentication information and use it to compromise the system.

Tools used by intruders also have led to attacks becoming more effective and devastating. As much as some of these tools help system administrators identify issues and monitor their network traffic, they can also facilitate attackers. Many of these tools have become automated, allowing attackers to gain information about Internet network hosts with minimum effort by scanning entire networks from remote locations. Other tools can attack components in phases that combined, contribute to a specified outcome. An example might be an intruder gaining access to a packet sniffer that has router or firewall passwords, eventually allowing the intruder the ability to access data on servers within that network. According to the CERT, [16] there are many automated software packages

that contain tools to exploit network vulnerabilities. Typically, a software package may include:

- Network scanners
- Password cracking tools with dictionaries
- Packet sniffers
- Trojan horse programs and their associated libraries
- Tools to modify system log files
- Tools to allow the attacker to remain anonymous
- Tools to modify system configuration files
- Tools to report false checksums

By breaking down security intrusions into categories, it becomes easier to define an attack. The following list describes the basic types of intrusions or attacks that take place over the Internet:

1. Probes – Probes can be looked at as attempts that are not normal to gain access to a specific system or an attempt to discover information about a specific system. An example might be as simple as an attempt to log onto a system account. Often these kinds of intrusions are the result of a mistake, but they can lead to a more serious security breach.
2. Scan – Using automated software tools, scan periodically or continuously probes or pings a specified system. Like probes, scans can at times be the result of an error, but can also lead to more serious security breaches.

3. Malicious Code – A basic term for software programs that can cause results on a system not intended by the original network design. These kinds of codes include Trojan horses, viruses, and worms. Trojan horses and viruses typically are hidden in legitimate files or programs that have been modified. Worms are replicating programs that can spread on their own after they have been initialized. Viruses are also replicating programs, but usually require an action on some part of the user to spread. An example is an email attachment that has no impact until opened. Then it alters other programs as they are opened. Generally, end users are unaware of these programs until some form of damage has taken place.
4. Denial of Service – The idea behind a denial of service attack to is prevent specified users from accessing a specific service. These kinds of attacks are not intended to gain access to specific machines or data. Examples might include an attacker flooding a network with large amounts of data or specifically targeting a resource that impacts another service, either by slowing it down or bringing it to a complete halt.
5. Account Compromise – Involves unauthorized use of a users account by someone not intended to have rights. This refers to an attacker that can compromise an account without having system or root level access privileges. The damage of this kind of attack can generally be minimized because the intruded does not have root access, but can still cause damage at the user level accounts. There can still be considerable loss of data or impact to services.
6. Packet Sniffer – This is a program that captures data from the information packets as they travel over the network. The data able to be captured can include usernames, passwords, and proprietary information. Packet sniffers can

sometimes be installed without having system privileges, and can capture sensitive data that can eventually lead to additional attacks on systems.

7. Root Compromise – This kind of compromise is similar to an Account Compromise, but the account compromised on the system has special privileges that may allow access to other system wide programs. If an attacker has root privileges, they can do anything they want, including changing or removing programs, changing system parameters, or injecting trace programs that can be used at a later time.
8. Exploitation of Trust – With security becoming a paramount issue, many systems are developing trust relationships. Trusts are essentially a check from one computer to another that each is who they claim to be. This is done before an exchange of files takes place. If an intruder can access a computer and appear to act as one of the trusted computers, he/she or it may be able to gain entry to other systems.
9. Internet Infrastructure Attacks – These are attacks that involve key aspects of the Internet such as network access providers instead of specific systems on a network. These attacks are usually widespread and impact the infrastructure, hampering daily activities of impacted sites.

Phillip G. Schein identifies six information security controls (name, access, availability, integrity, authenticity, confidentiality, and nonrepudiation) and categorizes them into three attack modalities (each contains an active and a passive state) that describe Internet attacks. [17]

1. Interference – any form of security attack that renders a device or service inoperative.

   a. An active interference attack targets a device or service with the intent to disable or destroy. An example might be boot sector viruses that rewrite the master boot record on a hard drive or DOS attacks that overwhelm a service provider, rendering it inoperative.

   b. A passive interference attack, such as a virus or a bacterium, does not necessarily target the device or service directly, but tries to disable them through indirect activities. An example might be a virus that diverts all resources to a specific task, thereby denying needed resources to a required task.

2. Interception – an attack that captures a data stream by monitoring or redirecting it.

   a. An active interception intercepts data message flow and interprets the message content. When the content is verified, the attack can alter the content, and redirect it to another location, causing a change in actions or service for that particular application.

   b. A passive interception intercepts a data flow and analyzes the data content, but does not alter its content. Examples may include network traces.

3. Impersonation – any attack that allows a third party intruder to access a network, acting as one of the parties, to exchange data without the knowledge of the last party.

   a. An active impersonation can be spoofing or identifying an incorrect IP address of one of the parties without the other being aware of it.

   b. A Passive impersonation does not impact the data stream directly, but tries to work indirectly to create some unauthorized effect. An example might be renaming a DNS name causing the legitimate DNS lookup to respond to

illegitimate host names. This can also involve the creation of another access point that allows unauthorized access to system resources by the third party.

Many attacks will take a mixed form, with characteristics from each modality. Classifying these risks will help in identifying and resolving, or at least minimizing them. Figure 17 [18] shows examples of security intrusions within each modality.

	Active	**Passive**
Interference	Denial of Service	Active Viruses, Bacteria
Interception	Web Page Redirection	Wire Taps
Impersonation	Spoofs (attacker that impersonates a legitimate user), Rogue Users (authenticated user that can access an unauthorized system), Cracker (unauthorized user that has complete access to security systems.	Trap Doors, Trojan Horse

Figure 17 - Examples of Security Intrusions Within Each Modality

By identifying risks and categorizing them, it becomes more manageable to determine not only the source of the intrusion, but also where in the protocol the intrusion is taking

place. Essentially, intrusions occur at different layers of the TCP/IP or OSI protocol, so security protocols that ward off these attacks must also be a part of that layer. An example of this is shown in Figure 18.

<table>
<tr><th>OSI Layers</th><th>SNA Layers</th><th>TCP/IP Layers</th><th>Related Security Protocols</th></tr>
<tr><td>Application Layer</td><td>Transaction Services Layer</td><td rowspan="3">Application Layer</td><td rowspan="3">S/MIME, Kerberos Protocol, Proxy Services, Secure Electronic Transactions, IPSec, Internet Key Exchange Protocol</td></tr>
<tr><td>Presentation Layer</td><td>Presentation Layer</td></tr>
<tr><td>Session Layer</td><td>Data Flow Layer</td></tr>
<tr><td rowspan="2">Transport Layer</td><td rowspan="2">Transmission Control Layer</td><td>Transport Layer</td><td>SOCKS, Secure Sockets Layer, Transport Layer Security</td></tr>
<tr><td>Internet</td><td rowspan="3">IPSec, Authentication Header, Encapsulated Security Payload, Packet Filtering, Point-to-Point Tunneling Protocol, Handshake Authentication Protocol, Password Authentication Protocol</td></tr>
<tr><td>Network Layer</td><td>Data Path Layer</td><td rowspan="2">Network Layer</td></tr>
<tr><td>Data Link</td><td>Data Link Layer</td></tr>
<tr><td>Physical Layer</td><td>Physical Layer</td><td>Physical Layer</td><td>PPP</td></tr>
</table>

Figure 18 - Security Protocols and Their Corresponding Layer Listing to Other Protocols

In 2001 the SANS Institute, along with the NIPC released a document that summarized the ten most critical Internet Security vulnerabilities (Figure 19). [19] This list was used by thousands of organizations showing the top ten vulnerabilities with windows and the next ten showing vulnerabilities affecting UNIX systems. While this list is only the tip of the iceberg reflecting only a small portion of security infractions, it does allow administrators a viable resource for auditing their systems. It also indicates how a potential single remedy such as a software upgrade (patch or newer version) in many cases can fix the problem. The following table lists and describes the top vulnerabilities to both Windows and UNIX systems according to the SANS Institute.

Windows Systems	
Internet Information Services	Prone to vulnerabilities within three classes: 1. Failure to handle improperly formed HTTP requests. Depending upon the request, an attacker can view the source code, view files outside the root file, view other unauthorized web server files, and execute commands on the server. 2. Buffer overflows, which can result in denial of service and execution of commands in the web server's user directory. 3. Sample applications, which are used to demonstrate server functionality. An attack can allow creation or rewriting server files, remote viewing of specific files for information gathering, and potential remote access to server information.
MDAC – Remote Data Services	Older versions of MDAC have a program flaw that allows remote users to run commands with administrative privileges which may provide external access to internal databases.

Microsoft SQL Server	Contain vulnerabilities that allow remote attackers access to key information, ability to change database / server configurations.
NETBIOS – Unprotected Windows networking shares	Windows allows host machines to share files with other host machines through network shares. Using the SMB protocol, a host machine can control remote files.
Anonymous Logon – Null Sessions	Allows anonymous users to retrieve information without authentication.
LAN Manager Authentication	Legacy data stored locally with weaker encryption protection allows easier access.
General Windows Authentication	Most forms of authentication rely on user-supplied passwords. Common vulnerabilities are accounts with limited or no passwords, protection by the users to protect it, presence of password breaking algorithms.
Internet Explorer	IE has vulnerabilities including web page spoofing, ActiveX control, MIME-type misinterpretations and buffer overflows.
Remote Registry Access	Typical Windows systems use a hierarchical database (registry) to manage components such as software, device configurations and user settings. Ineffective settings or permissions can allow access.
Windows Scripting Host	Windows Scripting Host (WSH) allowed and file with a .vbs extension to be executed when that file was viewed by the user.
UNIX Systems	
RPC's	RPC's allow programs from one machine to execute procedures on another. Used mainly in distributed systems, RPC executes with root privileges, and if compromised can allow access to other systems at the root level

Apache Web Server	
SSH	Popular service for securing logins, command executions, and file transfers, but vulnerable to root access from a remote user.
SNMP	Used extensively to monitor and configure TCP/IP devices such as printers, routers, switches, and provides input for monitoring devices. The method which this protocol utilizes agent software (method which messages are handled) along with an authentication mechanism, provide vulnerabilities.
FTP	Used to distribute files to anonymous users. Generally does not require unique login and passwords.
R-Services / Trust Relationships	R-commands are extensively used and generally groups configure systems so that users do not need unique user ID's and passwords. These types of Services lack encryption and have poor authentication.
LPD	Service that allows connection of a local printer to a local machine utilizing TCP port 515. May contain programming flaws to allow access to root privileges.
Send mail	Program that sends, receives, and forwards electronic mail processed on UNIX systems. Risks can be caused by buffer overflows and improper configurations.
BIND / DNS	Allows location of a server by name without using its IP address. Potential attacks occur because of outdated configurations and bad configuration files.
General UNIX Authentication	Most forms of authentication rely on

	user-supplied passwords. Common vulnerabilities are accounts with limited or no passwords, protection by the users to protect it, presence of password breaking algorithms.

Figure 19 - 2001 SANS Institute Document that Summarized the Ten Most Critical Internet Security Vulnerabilities

Viruses

Computer viruses are programs that are designed to replicate and spread themselves. They usually require a host of some kind that will allow them to propagate and can have impact on all programs, files, and hard disks. Original theories [20] of self-replicating programs date back to around 1950, with test viruses first programmed in the 1960's. Figure 20 shows a generic timeline of some of the famous viruses.

Virus	Date	Description
Not Named	1950	Developed self-replicating programs
Not Named	Mid-1980's	Coined "Virus" phrase as a program that can affect other computer programs by replicate itself
Brain	1986	Boot sector virus that worked only on floppy disks, not hard drives and tried to hide itself from detection
Lehigh	1987	Gained control of opening system files
Jerusalem	1987	First memory resident file infector that attacked on specific dates
Internet Worm	1988	Crashed large numbers of computers
Cascade	1988	Was able to prevent system administrators from changing or removing the virus
Dark Avenger	1989	It was designed to damage system slowly, going

		unnoticed until it was too later for recovery
Frodo	1989	Fully stealth virus that attacked only on specific dates
Tequila	1991	One of the first viruses that had the capabilities to change it's appearance after detection
Michelangelo	1990	More hype than anything else – crashed fewer computers than was originally predicted
Pathogen	1994	Identified by Scotland Yard's crime unit
Concept	1994	Macro virus that worked in a Microsoft Word environment
Boza	1996	Infected Microsoft Excel spreadsheets
Laroux	1996	Infected Microsoft Excel spreadsheets
Melissa	1999	Executed a macro in a document that was attached to n email. When the attachment was opened, it was forwarded to fifty other users in the infected users Microsoft Outlook address book
Chernobyl	1999	Caused major damage by making the users hard drive inaccessible
Love Bug	2000	Similar to Melissa by sending itself through Microsoft Outlook. Also known as the Love Letter
W97M.Resume.A	2000	New version of Melissa
Stages	2000	Utilized .txt extensions to spread itself

Liberty	2000	Assumed to be the first Trojan Horse virus
The Anna Kournikova	2001	Similar to the Love Bug and Melissa viruses
Code I and Code II	2002	Worm spreads through internal and external networks
Klezworm	2002	It creates a hidden copy of the original host file, then overwrites the original file with itself
Nimda	2002	Infects both local and remote files by sending out emails, searching for open ports and attempts to copy itself

Figure 20 - Famous Virus Dates

The term "Virus" was coined because these programs were small, made copies of themselves, and could not exist without a host (similar in nature to a biological virus). Early incidents began appearing as the PC revolution began to take hold in the mid-to-late 1980's. As these incidents began increasing in frequency, the number of ways of spreading them grew as well. Viruses can propagate themselves in different ways. Email attachments appear to be one of the most popular ways of infecting computers. The viruses are resident in email attachments and propagate themselves when the attachments are read. Other means of virus transmission is through the World Wide Web (because of a lack of security surrounding data transmission), FTP (Internet protocol used to transmit information), and News Groups, which have become a widespread avenue for exchanging data among users.

Currently there are five types of recognized viruses. [21]

- Macro Viruses – These types of viruses infect data file and are the most common. They impact typical tools in use today such as Microsoft Office Suite that contains Word, PowerPoint, Excel, and Access. These viruses utilize internal programs that were designed to automate tasks within the program. Microsoft's Visual Basic code in the Microsoft Office application allowed a virus to be written that would infect its data files as well as other associated data files. This type of programming allowed viruses to be created relatively easily, sending many varieties into the computer mainstream. Some examples of these types of viruses include the Melissa, NiceDay, and Groov.
- File Infector Viruses – These types of viruses infect program executable code such as .exe files. They have the ability to infect other programs when the original infected program is run. These are memory resident viruses, which infect non-infected memory after being run. Examples of these types of viruses are Jerusalem and Cascade.
- Multi-Partite Viruses – These viruses infect computer's boot record and program files. A primary trait in these viruses is the difficulty in removing them from boot sectors. If the virus is not completely removed, it will be reinfected. This also holds true with infected files. If they are not removed completely, they can reinfect the system the next time the files are opened. Examples of Multi-Partite viruses are One_Half, Emperor, Anthrax, and Tequila.

- Boot Sector Viruses – When a computer system initiates, there is a small program in the boot sector that runs. These types of viruses become a part of this program and activate themselves when the user attempts to startup the computer. They are memory resident viruses and can impact all PC's floppy or hard drive boot sectors. Because they are memory resident, they remain in memory and will infect other files when run, unless they are write-protected. Examples of Boot Sector Viruses are Form, Disk Killer, Michelangelo, and Stoned.
- Master Boot Record Viruses – These viruses infect disks in the same manner Boot Sector Viruses do, but infect the area of the disk where a good copy of the boot record is stored. With certain operating systems such as Microsoft NT, if either the Boot Sector or Master Boot Record Sector is infected, the system will not initialize. This is primarily due to the fact that the NT operating system accesses the boot information from different locations than other operating systems. NT is formatted with FAT partitions, and if infected would allow boot-up from the DOS prompt. Examples of Master Boot Record Viruses are NYB, AntiExe, and Unashamed.

From a broad perspective there may be five types of viruses, but they can impact many different types of applications and programs. The following table (Figure 21) was compiled by Symatnec/Norton AntiVirus , [22] and shows the prefix of the virus, and the types of applications that can be affected.

A2KM	Access macro viruses are native to Access 2000.
A97M	Access macro viruses are native to Access 97.
AM	Access macro viruses are native to Access 95.
AOL	Trojan horses that are specific to America Online environments and usually steal AOL password information
BAT	Batch file threats.
Backdoor	Threats may allow unauthorized users to access your computer across the Internet.
Bloodhound	Bloodhound is the name of the Norton AntiVirus heuristic scanning technology for detecting new and unknown viruses
Ddos	Distributed Denial of Service threats. Distributed Denial of Service involves using zombie computers in an attempt to flood an Internet site with traffic.
DoS	Denial of Service threats. Not to be confused with DOS viruses, which are named without prefixes.
HLLC	High Level Language Companion viruses. These are usually DOS viruses that create an additional file (the companion) to spread.
HLLO	High Level Language Overwriting viruses. These are usually DOS viruses that overwrite host files with viral code.
HLLP	High Level Language Parasitic viruses. These are usually DOS viruses that attach themselves to host files.
HLLW	A worm that is compiled using a High Level Language. This modifier is not always a prefix, it is only a prefix in the case of a DOS High Level Language Worm. If the Worm is a Win32 file, the proper name would be W32.HLLW.
HTML	Threats that target HTML files.
IRC	Threats that target IRC applications.
JS	Threats that are written using the JavaScript programming language.
Java	Viruses that are written using the Java programming language.
Linux	Threats that target the Linux operating system.
O2KM	Office 2000 macro viruses. May infect across different types

	of Office 2000 documents.
O97M	Office 97 macro viruses. May infect across different types of Office 97 documents.
OM	Office macro viruses. May infect across different types of Office documents.
PWSTEAL	Trojan horses that steal passwords.
Palm	Threats that are designed to run specifically on the Palm OS.
Trojan/Troj	These files are not viruses, but Trojan horses. Trojan horses are files that masquerade as helpful programs, but are actually malicious code. Trojan horses do not replicate.
UNIX	Threats that run under any UNIX-based operating system.
VBS	Viruses that are written using the Visual Basic Script programming language.
W2KM	Word 2000 macro viruses. These are native to Word 2000 and replicate under Word 2000 only.
W32	32-bit Windows viruses that can infect under all 32-bit Windows platforms.
W95	Windows 95 viruses that infect files under the Windows 95 operating system. Windows 95 viruses often work in Windows 98 also.
W97M	Word 97 macro viruses. These are native to Word 97 and replicate under Word 97 only.
W98	Windows 98 threats that infect files under the Windows 98 operating system. Will only work in Windows 98.
WM	Word macro viruses that replicate under Word 6.0 and Word 95 (Word 7.0). They may also replicate under Word 97 (Word 8.0), but are not native to Word 97.
WNT	32-bit Windows viruses that can infect under the Windows NT operating system.
Win	Windows 3.x viruses that infect files under the Windows 3.x operating system.
X2KM	Excel macro viruses that are native to Excel 2000.
X97M	Excel macro viruses that are native to Excel 97. These viruses may replicate under Excel 5.0 and Excel 95 as well.

XF	Excel formula viruses are viruses using old Excel 4.0 embedded sheets within newer Excel documents.
XM	Excel macro viruses that are native to Excel 5.0 and Excel 95. These viruses may replicate in Excel 97 as well.

Figure 21 - Virus Prefix and Application Infected

Security Controls

Understanding security intrusions is part of an overall security protection strategy. As security risks increase and become more complex in nature, the need to interject security protection before an intrusion strikes becomes more critical. With protocol architectures becoming hierarchical in nature, as TCP/IP is, the ability to impose effective security measures at specific layers of the protocol is necessary to target specific intrusions. The basic aspects of security are confidentiality and authentication. To introduce these aspects, certain controls are needed to provide the confidentiality needed for secure data transactions between a service provider and the consumer.

These controls are application program interfaces that interact with security providers and security protocols such as Authentication Header Protocol and Encapsulated Security Payload Protocol to support a networked system. One of these controls is the PKI, which is a collection of tools, and technologies that provide a secure exchange of data from both an internal and external network architecture environment. PKI works to verify confidentiality and authenticity between information sharing networks. Security, or cryptographic technologies generate a specific component that provides measures against attacks. The basic components of cryptographic technologies are symmetric key encryption algorithms, asymmetric key encryption algorithms, and secure one-way hash functionality.

Today, one of the most common ways to encrypt a message is to use a single key that is known only to the parties that are sharing the data transfer. This type of encryption

requires the sender to use a key that scrambles a string of characters into an encrypted message. The receiver then uses the same key to unscramble the encrypted message back into the original form. This type of encryption is characterized as symmetric key encryption. The guarantee that the information is secure resides in the confidentiality of the key used (which may be public) and the length of the key. The encryption algorithm must be as strong as possible to improve confidentiality. The simpler the algorithm code, the easier it is to break it. Keys follow a standard that was developed by ANSI in 1975. [23] This standard is the Data Encryption Standard DES [24] that originally used a fixed length 56-bit key for encryption algorithms. Since this is no longer considered strong enough, a new key that uses three 128-bit keys has been implemented. Asymmetric key encryption uses a set of complimentary key algorithms. One of the keys is confidential while the other key is public. A standard known as RSA (for the last names of the inventors, Rivest, Shamir, and Adelman) uses asymmetric keys that are functions of two large numbers that can continually be increased to resist intrusions. These keys provide considerably more confidentiality and authenticity protection than symmetric key encryption algorithms, but are many times slower to process because of their size. The third cryptographic technique provides secure one-way hash functionality. Essentially the hash function takes a variable length message and converts it into a fix length string (also known as a hash value). A mathematical algorithm similar to the encryption algorithm generates a 128 bit to 256-bit value that is derived from the original message. The value is authenticated through comparison of the original message by generating a second hash function and comparing it to the first. If there are character discrepancies between the two, then the authenticity of the message needs to be questioned. If the two values agree, then the message is authenticated indicating there were no modifications during transit.

Using an encryption algorithm technique like this is relatively simple, yet the disadvantages of all the parties that are engaged in this information exchange, knowing the secret shared key, increases the likelihood that the key may be compromised.

Certificate Authority

Other forms of encryption and authentication (cryptography) technologies are being developed as a way of disguising information, as data transfer over private and public communications networks increases. For example, third party software companies such as VeriSign offer digital certificates or CA's, which allow unknown users to trust each other with all data transactions. These types of certificates are transmitted over networks known as SSL protocol, and are maintained through servers. These parties have what is known as a trust or trusted relationship with each other. This essentially indicates that the information shared by each party is private and trustworthy. A digital signature (regarded as an electronic signature) identifies that data transfer is original from the parties that possess the key. There is a standard (International Telecommunications Union Telecommunication Standard X.509) that companies such as Verisign Inc., use to maintain digital certificate integrity. Certain certificate vendors will do complete background searches of companies to verify that organizations are who they actually claim to be. VeriSign, for example, documents its practices in a Certificate Practices Statement, and undergoes an annual audit by KPMG for verification of its processes and procedures. [25]

Encryption techniques require the data sender and the data receiver to decipher a specific digital identifier code, or key. Everyday examples of digital ID's (keys) are computer passwords and bank PIN numbers. These keys are private because they are encrypted and decrypted only by the sending and receiving parties. Public keys can be issued, for example, in circumstances where multiple parties need to access a specific data server.

These keys were originally published by the U.S. Government in 1977 and known as Data Encryption Standards (DES) [26]. The goal was to establish an industry standardized encryption algorithm. The algorithm is plain text, and depending upon the number of characters used, creates different degrees of difficulty to decode. For example, if the degree of security warranted by a specific project requires low-level encryption, then a 40 –bit encryption code may be chosen. This would be a key of plain text that contains alphanumeric symbols placed in random order that only the trusted parties would be aware of. Figure 22 shows an example of an encryption key.

-----BEGIN-----

abcjl8Nyba4fmJHUMM8739imfd9v9234mdm9i9JJJBXddda7n9igcNnnnisjNNNWInKNNiINnINnI8NpOj

jiIHNihb8yyu6G6RhbUH8HHI9u90kkkoI9uhRF6r6gyg7y8H8Y7tg77tg77g7u877G8u8U9883ndnjbnuuuH

BYgYgGYgfg877g8UbgYF67g8Tt9yh8Gtg87T6Gg87T8Yuh99y998HHH88Tgh8hgbT56f7t6Rg887h9j0u

U0j0jYTRyuGTd4wZYbom-jNOPj98y6DvFeDuhj0U09I-K-

o=j89yF6d7f67r68abcjl8Nyba4fmJHUMM8739imfd9v9234mdm9i9JJJBXddda7n9igcNnnnisjNNNWInK

NNiINnINnI8NpOjjiIHNihb8yyu6G6RhbUH8HHI9u90kkkoI9uhRF6r6gyg7y8H8Y7tg77tg77g7u877G8u

8U9883ndnjbnuuuHBYgYgGYgfg877g8UbgYF67g8Tt9yh8Gtg87T6Gg87T8Yuh99y998HHH88Tgh8hgb

T56f7t6Rg887h9j0uU0j0jYTRyuGTd4wZYbom-jNOPj98y6DvFeDuhj0U09I-K-o=-

j89yF6d7f67r68abcjl8Nyba4fmJHUMM8739imfd9v9234mdm9i9JJJBXddda7n9igcNnnnisjNNNWInKNN

iINnINnI8NpOjjiIHNihb8yyu6G6RhbUH8HHI9u90kkkoI9uhRF6r6gyg7y8H8Y7tg77tg77g7u877G8u8U9

883ndnjbnuuuHBYgYgGYgfg877g8UbgYF67g8Tt9yh8Gtg87T6Gg87T8Yuh99y998HHH88Tgh8hgbT56f

7t6Rg887h9j0uU0j0jYTRyuGTd4wZYbom-jNOPj98y6DvFeDuhj0U09I-K-o=-

j89yF6d7f67r68abcjl8Nyba4fmJHUMM8739imfd9v9234mdm9i9JJJBXddda7n9igcNnnnisjNNNWInKNN

iINnINnI8NpOjjiIHNihb8yyu6G6RhbUH8HHI9u90kkkoI9uhRF6r6gyg7y8H8Y7tg77tg77g7u877G8u8U9

883ndnjbnuuuHBYgYgGYgfg877g8UbgYF67g8Tt9yh8Gtg87T6Gg87T8Yuh99y998HHH88Tgh8hgbT56f

7t6Rg887h9j0uU0j0jYTRyuGTd4wZYbom-jNOPj98y6DvFeDuhj0U09I

-----END -----

Figure 22 - Example of an Encryption Key

Note: This example is not an actual industry key, but only a representation of what an encryption key would look like. All keys require a beginning and ending value. A 40-bit key has over 70 quadrillion possible combinations that can be displayed and would be required to break the code. If additional security is needed, the encryption key can be increased to 128-bit.

Once a certificate is issued, only each party knows the key for the transaction to occur. For this type of relationship to exist, three specific functions [27] must be supported:

- Mutual authentication where the identity of the server and the customer are mutually recognizable.
- Secure messaging is engaged between the server and the customer using the assigned key.
- The integrity of the message is protected from intrusion.

Figure 23, according to Verisign, illustrates how the client/server communicate when requesting an encrypted communication session. These types of digital encryption techniques help protect users who are concerned about Internet security. Although considerably more secure than not having any encryption protection, vulnerabilities still exist in various forms such as:

- Spoofing – creating illegitimate web sites that appear to replicate legitimate sites.
- Disclosure of unauthorized information where information is stolen during data transmission and altered.
- Unwarranted actions by personnel.

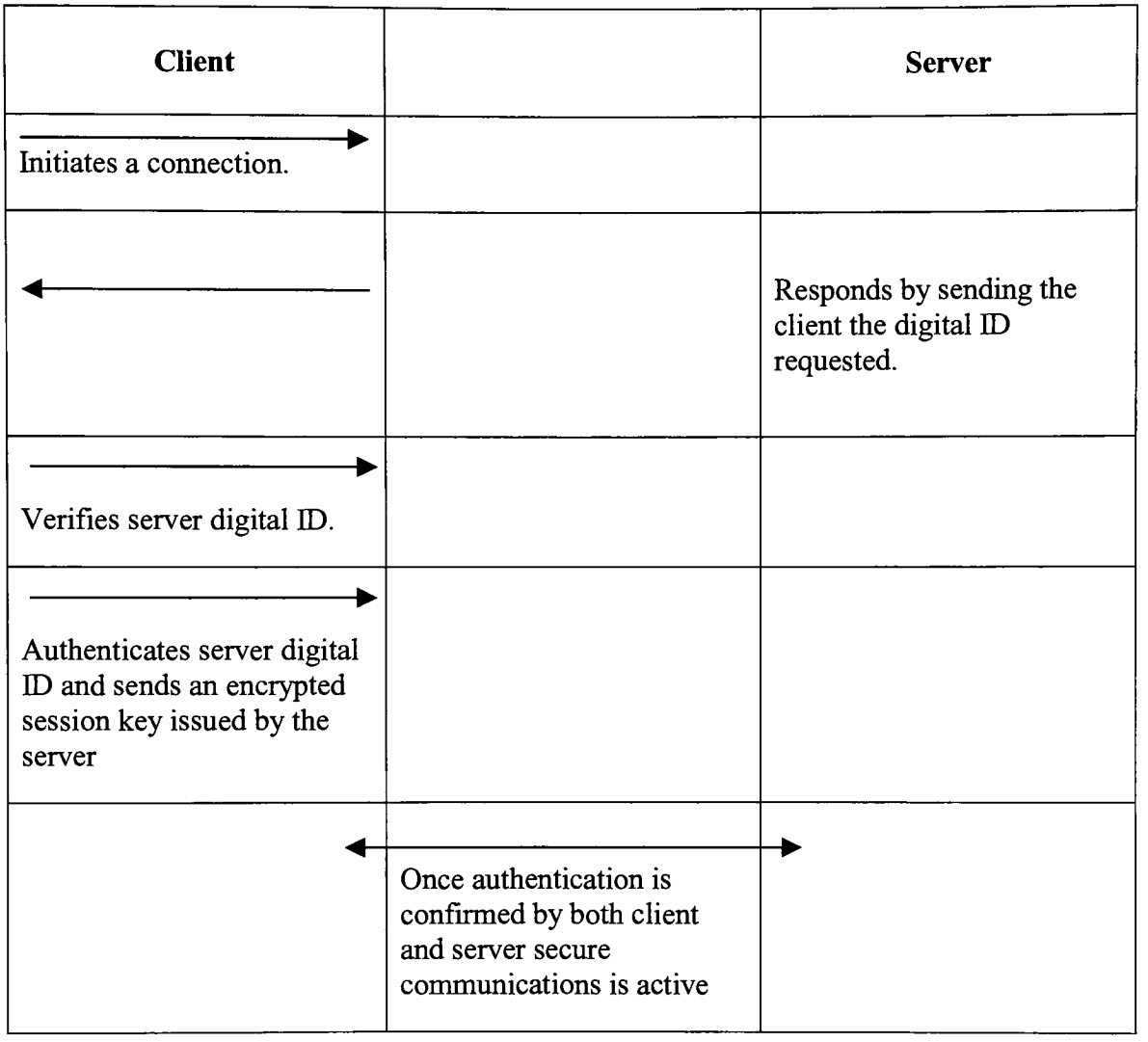


Figure 23 - Example of an Encrypted Client/Server Communication Session

Often organizations may require additional certificate authorities. A hierarchy of CA's can be deployed where the original certificate is the root certificate and the most trusted (certificate issued by a 3rd party commercial vendor). These additional CA's are subordinates to the root CA and may issue additional certificates as needed. The reasons

for adding additional CA's within an organization span from organization support for administrative functions to maintenance functions of specific security applications that need separation form other applications. Creating a trust that is supported by the same CA can also create certificate relationships to work across organizations and can be issued through a variety of transport mechanisms.

IP Security Architecture

IPSec, as defined by the IETF, uses two OSI network layer security protocols: the AH and the ESP protocols. The AH protocol provides a source for authentication and data integrity and ESP provides a source for confidentiality, as well as authentication and data integrity. These services operate only in a way that is recognized by the parties engaged in information sharing activities. It is generally given that if the data information was authenticated in transit, the message recipient is assured that the information is intact without modification.

The impact of new-sophisticated software has created opportunities for intrusions to occur in the IP protocol in increased numbers with expanding varieties of attacks. The OSI network layer does not offer the protection needed, especially in the current version. The original design never anticipated the hostility of the current network environment nor did it realize the scale of network hackers and the level of sophistication that would be used. It also was never designed to perform security services that it is clearly performing in today's environment. While the original intent of the IP protocol was to transfer data packets across the network, there were few inquiries made about what other computers or devices on the same network were doing. An example might be a packet analyzer that reads data packets in transit on the network. This is known as network sniffing or eavesdropping. Susceptibility to passive data interception can vary according to the protocol structure and data packet design used, but common data transfer channels are probably at the highest risk for attacks. An example of attacks commonly seen with common data transfer channels is utilizing IP addresses for authentication purposes. This

kind of practice has led to system security vulnerabilities such as client flooding (overwhelming a client with responses), false cache loading, and server attacks that overwhelm the server with tasks and should be avoided in network security design.

Encryption of the data transfer is one of the primary ways to help circumvent intrusions. There are several methods [28] that can be used:

- Link Level Encryption – the data packet is automatically encrypted at transmission time over unsecured channels, then un-encrypted at the receiving end.
- End-to-end Encryption – the data packet stream is automatically encrypted at the encryption router at transmission time, then un-encrypted at the receiving end router.
- Application Level Encryption – data packet encryption is done at the application layer of the TCP/IP and OSI protocols.

The frequency of Internet attacks and lack of security imposed in the IPv4 protocol has yielded recommendations that the IPv6 protocol include greater authentication and encryption capabilities. Deployment of the 128 bit-addressing scheme of the IPv6 protocol will probably take years to implement, so many TCP/IP and OSI network security improvements have been designed and implemented for the current IPv4 protocol.

These enhancements include:

- Improvements to remote site connectivity where organizations can utilize the Internet, yet maintain Intranet security by communicating through VPN. Encryption technology of IPSec architecture can also be utilized by VPN's.
- Reliable and trusted key exchanges for data transfer that provides authentication and confidentiality in applications surrounding e-commerce business ventures.
- Extranet connectivity that provides authentication and confidentiality in applications that apply to business ventures outside an organization's network.
- Remote access services that are provided by ISP's over phone or cable lines.

With IPSec working below the TCP/IP transport layer, it can provide enterprise-wide security protection that would normally be provided by specific security software applications. According to Phillip G. Schein, [29] the IPSec architecture has many advantages because of its invisibility to the TCP/IP Application layer and end user (Figure 24).

Full support for the IETF industry standards	Network interoperability is guaranteed by providing an open industry standard as opposed to IP encryption technologies
Flexible security protocols and polices	Easily implemented in existing network protocols
Transparent to applications and end users	Works with the IP network layer and is invisible to end user applications

Authentication	Strong encryption technologies enable strong defense against attacks
Confidentiality	Information technology security controls that can prevent unauthorized access during data transfer
Data Integrity	IP authentication headers and variations of hash messaging authentication code ensures data integrity exchanges
Dynamic Re-keying	Dynamic re-keying during data transfer increases security prevention by eliminating interception
Secure end-to end linking	Provides secure end-to-end linking that helps ensure data integrity after transfer of information
Ease of implementation and administrative maintenance	Reduced administrative management is required because of the security filters and policies employed with IPSec architectures
Scalability	IPSec architectures have the ability to enact policies at a single user workstation through an enterprise wide network

Figure 24 - IPSec Architecture Advantages

In order for a IPSec connection to take place, there needs to be a negotiation between devices that agree on encryption algorithms, key generation methods and whatever security protocols are going to be used. This is known as an SA and is responsible for the terms of the data transfer and the associated protocols that will be engaged during the

transfer. The SA defines the security protocol that will be used when datagrams are sent to a specific IP address. When information is sent, a packet descriptor mode is identified within the specified protocol. For example, the SA might identify the protocol as transport. SA's identify one-way traffic, so if the transmission is bi-directional, then two SA's would be required, one for each direction. Basically, the SA identifies a specific security protocol that is carrying a specific encryption service in one specified direction. If a particular data transmission session is carrying more than one protocol, the SA's will form a bundle, which do not have the same IP address destination. This means that part of the SA in an SA bundle might indicate that the AH protocol will support a specific application like a firewall, and another part of the SA might indicate that the ESP protocol will support another specific application behind the firewall.

There are different types of security protocols that are used and operate at different layers of the TCP/IP or OSI protocols. For instance, Secure Channel services operate at the transport layer and provide security services to specific applications like Web browsers and applications. The security risk entails authentication of the web browser, web client, and service provider. Secure Channel protocols deliver end-to-end security, beginning with SSL and TSL. These protocols rely on public key authentication. SSL, originally developed by Netscape, allows encrypted information between a web browser and web server using public key encryption and digital certificates. TSL is a standard that has essentially the same features as SSL. Other security protocols described earlier such as AH and ESP provide lower level security services similar to Secure Channel services. AH services provide authentication and data integrity by performing integrity checks on each IP datagram that is sent. AH does not offer confidentiality as a service, but ESP does

along with the other services that are provided by AH. IPSec provides all three services, authentication, data integrity verification, and confidentiality at each end of the data transfer. Another example of a security protocol is HTTPS, developed in 1995 by Enterprise Integration Technologies. This is a secure protocol used with TCP and provides web browser end-to-end secure connections over the Internet.

When a security system is being developed for a specific network, a list of security policies needs to be established that lists various negotiation protocol policies that will be needed to effectively enable that security strategy. By analyzing the exchanges of data over a period of time, negotiation protocol policies can be determined for any appropriate security services for that particular network configuration. An IP security policy may be assigned to a specific network and when activated will automatically load these security policies. This helps lower administrative costs by eliminating many of the tasks an administrator would have to manually perform on each workstation. Generally, each one of these security policies contains rules, which have an associated filters list and actions. These security rules are composed of components (Figure 25) that match up with target computers to define network traffic actions.

IP Filter List	**Data Packets are Defined by IP Address**
Filter Actions	Specific actions that permit, block, and negotiate data transfer are identified when the target packet matches the filter information in the filter list
Security Methods	Data is exchanged using three levels of security intensity – high, medium, and custom. The high method uses ESP and has services such as confidentiality, authentication, and integrity. The medium level uses AH and has services such as confidentiality, and integrity with no encryption. The custom level allows for creation of an integrity algorithm with or without using encryption, and session key settings.
Authentication Methods	Defines the trust between devices. It can be Kerberos, Digital Signatures, CA, or some predefined key that only the associated parties know of.
Tunnel Settings	Specifies the "data packet inside another data packet" format that is transmitted in the transport layer and provides end-to-end security in network systems that lie outside a typical LAN environment.
Connection Types	Specifies where the data transmission will pass; over the entire network or LAN's

Figure 25 - Components that match with Target Computers to Define Network Traffic Actions

Filter actions include the source and destination IP addresses, clients, network identifiers, or specific DNS names on a matching network. The filter actions permit (no security actions are taken with the transfer of data), block (all data traffic is denied), and negotiate security (must be compatible with a security protocol) and are applied as soon as a connection is established within a specified protocol. If an action cannot be completed, then the next defaulted action will be applied. If no action takes place, then the specified service will fail to execute the specified security policy.

As seen, there are many different protocols for different network scenarios and applications that need to be evaluated before implementing a security system. SSL and TLS, along with Unix sockets (SOCKS), and HTTPS, along with others, can provide network security with applications that are directly interacting with the TCP/IP and OSI Transport layers. These protocols provide complimentary services within VPN's and extranets that support secured exchanges of information by authenticating data transfers. Private and trusted networks enable security through isolation. They can be secure, but are limited in terms of scalability because of the initial investment needed to set them up and maintain them. End-to-end security systems can be more functional than private networks because they are utilizing technologies and protocols from support services that are applied to each layer of the network. This simplifies administration and maintenance issues and lends itself to a reduced cost base while being able to implement security services integrated directly with the specified applications needed for the network.

Human Interaction

Even though viruses can be detected and removed, there are other aspects that need to be addressed to completely understand the issues. All viruses and security issues are the result of some form of human interaction. They need to be written, verified, and placed into an environment where they can do their damage. Viruses are created for a multitude of reasons such as the technological challenge of creating one that is unique, undetectable, and disastrous to the end user. There are other reasons such as vanity where the creator will become known within their world, becoming notorious when anti-virus software is required as a solution. Others can range from testing a code writer's ability to watching a virus spread, to creating a virus that makes a specific point where people will be forced to listen. The reasons are numerous, but the end results can be devastating. [30]

According to Sarah Gordon, [31] renown expert in computer viruses and security technology, "The kind of person who creates such disruption differs in age, income, location, social/peer interaction, educational level, likes, dislikes and communication style." She continues with the stereotypical image of a virus creator, the schoolboy who has the tools to do it and something to prove, still exists, but here is, however, an increasingly dark side to the virus writer. Motivated by financial gain, they are more and more likely to be working with Spam creators and hackers. The money is coming from these code writers and they seem to be employing the best of virus writers to help them. "It sounds like a conspiracy theory, but they are becoming very advanced now in organized hi-tech criminal activity". [32] This is evident in Sobig F, which turns a computer into a host to send out millions of Spam e-mails, often without the owner's knowledge. With the clampdown on unsolicited e-mail, which now accounts for a large percentage of

e-mail traffic, Spam creators need to find new ways to continue their work. As much as there is a thrill for virus creation, there remains a profit to be made from a successful virus. Andy Bissett and Geraldine Shipton [33] at the University of Sheffield believe it is much more complicated than that and have identified both unconscious and conscious motives behind virus writers. Such conscious motives include "non-specific malice," revenge, cyber-espionage and commercial sabotage. Regardless of the reasons, virus programmers are not going away.

Hackers

Virus writers come from many different backgrounds, but can generally be described in the following social groups. Socially accepted people who write viruses in order to make the public aware of security flaws in software. Others, known simply as Hackers are people who are intelligent, yet like the challenge. Crackers are the people who break into systems with the intent to do damage. Regardless of what group a writer may fall into, he/she has his/her specific agenda that, essentially, is tasked to bringing computer operation to a standstill. They prey on human weakness to achieve their goals. "It's the trust factor you are exploiting," said Oliver Friedrichs, [34] senior research manager with anti-virus vendor Symantec Corp told The Associated Press. "Most people, when they receive something, they want to trust it. You don't want to miss something people may be sending you."

Ryan Schuster [35] defines Hackers and Crackers in the following way:

> Hackers: The term "Hacker" dates back to the very beginning of the computer age. At that time being called a Hacker was something positive. Hackers possess advanced computer skills and are considered intelligent without bounds. They live by the belief that anything that teaches us something new and betters our lives should be free. Their intent on "hacking" into a system or writing a virus is benign. A virus written by a Hacker is often created for fun, or to learn something new, or to impress other people. A Hacker virus usually has no discernable destructive payload and often the virus never enters mainstream because the Hacker turns it over to security firms as a lab virus. Other groups of Hackers have a specific intent. They "hack" into computer systems or write viruses to make a

point. Often they are the people we hear about who explain their actions by saying that corporate America refused to listen to them about dangerous security holes, so it was up to them to gain everyone's attention. These coders may write a virus that is often a "concept" virus in that it blatantly displays previously undisclosed security holes that a virus can use to infect. However, there is another side that may seek out one group of people or a certain company that they feel is unjust in someway. A virus created in this vain for example, may only attack people with "@microsoft.com" e-mail addresses or sites with ".gov" extensions.

Crackers, on the other hand, have a destructive intent. Like Hackers, they believe they should have access to anything they want. They get a thrill from destruction and they get high from the chase as world governments and big business hunt them down. They consider the old Hacker's Code Of Ethics to be corny (or at the very least outdated). A Cracker virus often actively seeks destruction. The W32/Naked virus is a good example of a Cracker virus that attempted to destroy all data. Crackers can be users who illegally hack into files/servers and load automated programs that can run independently of the user's commands once activated. These people designed these programs for the sole purpose of breaking into computer systems and networks. They would send messages to vulnerable servers, which would cause the host computer to respond. The amount of required responses would effectively block any legitimate traffic. Creating automated programs is illegal when their intentions are to harm other systems.

Coding Ethics

Computer users and coders are responsible for adhering to accepted standards of ethical behavior. Any unethical use of resources information, software, or hardware can be treated like any other ethical violation. Computer information should be treated the same as any piece of proprietary information, regardless if it is business or personal property. Viewing and using information such as programs, files or any other software data without authorized permission is an invasion of privacy and can be punishable by law. Other acts such as modifying information and preventing or delaying access to resources are considered acts of destruction. These types of ethical standards also apply, even when information is left unprotected.

Every establishment, whether business or personal, has its own set of rules or guidelines that need to be followed. There are also other organizations such as the Association of Computing Machinery ACM that has guidelines of ethical professional conduct expected to be followed by its members. One of its main principles [36] is to avoid harm to others. "Harm" means injury or negative consequences, such as the undesirable loss of information, loss of property, property damage, or unwanted environmental impacts. This principle prohibits use of computing technology in ways that result in harm to any of the following: users, the general public, employees, and employers. Harmful actions include intentional destruction or modification of files and programs leading to serious loss of resources or unnecessary expenditure of human resources such as the time and effort required to purge systems of "computer viruses." [37] Code writers who create viruses with the intent to do harm are subject to the local and federal laws that apply.

Spreading of Viruses

As discussed earlier, attacks are used to exploit weaknesses within the TCP/IP protocol or associated protocols. Packets of information send data from a sending address to a receiving address. The information that contains sending and receiving addresses utilizes the IP portion of the protocol. The remainder of the data transfer is handled by the TCP protocol. Data communication at the sender and receiver requires a port where the information can enter or exit the computer. These ports have specified numbers that determine the type of information the sender wants to transmit to the receiver. For example, port 21 is used for FTP, port 25 is used for SMTP, and port 80 is used for HTTP.

With normal client/server communications over secure connections, a message is sent to a server from the client that needs to be authenticated. When the server receives the message, it authenticates it and returns an acceptance to the sender, thereby allowing access to the server. In Denial of Service attacks, these requests are code, or scripts created specifically for the purpose of searching for vulnerabilities in systems that will allow installation and implementation. Once these scripts have been installed on an unprotected computer, they can be executed at any time by generating large numbers of requests to a server. These requests have invalid return addresses, sometimes using the server address as the return address. The lack of a valid return address does not allow the server to authenticate and respond back to the incoming requests. Depending upon the server configuration setup, a specific amount of time will elapse before the sever will close the connection. Upon receipt of the closed connection, the attacks begin tying up

the server continuously as it attempts to authenticate all the incoming requests. The number of requests can be so large that they tie up or crash the server resources, effectively disabling it.

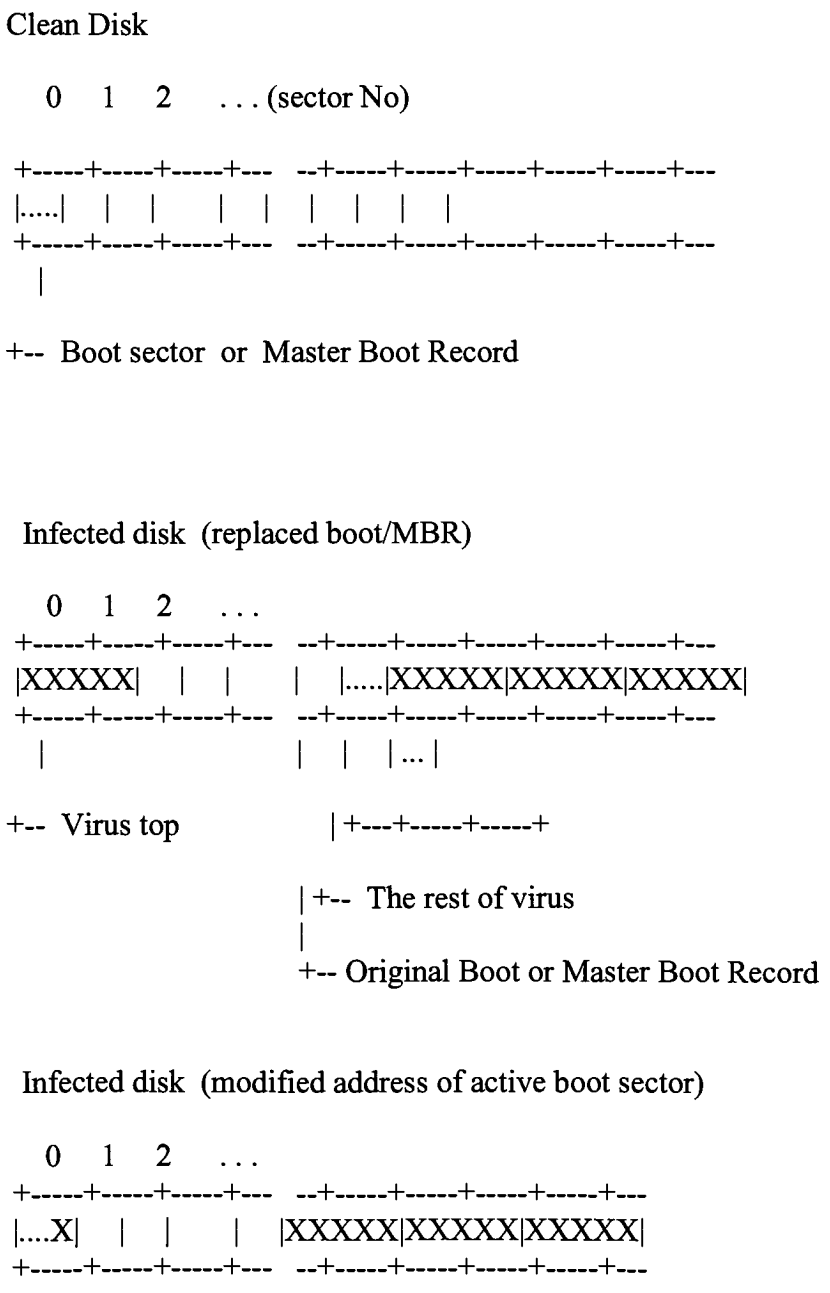
Detection of a virus can sometimes be tricky. Unless an anti-virus program detects and removes it, a virus may go unnoticed for a period of time, infecting local programs and applications. Depending upon the virus type, they can impact different aspects of your system in different ways. The common thread is that they are transmitted through the Internet transmissions and can impact, depending upon the transmission protocol, system data and end user applications. Examples of these viruses include Boot, File, Macro, TSR (Terminate and Stay Resident), and Windows. The basic startup operations of a computer allow the specific virus to load and execute. These startup operations essentially consist of the computer at startup going to the boot sector of the hard disk to obtain information about the disk such as its physical characteristics, any pertinent information regarding how the disk is partitioned, and specific instructions on loading the operating system. Once these instructions are received, the operating system initializes and begins computer operations. The operating system then accesses the FAT to find the specific addresses of files needed to perform its operations. Essentially, the virus will attach itself to a file when that file is opened, viewed, or executed. They then launch themselves as soon as the computer boots from the hard drive. Typically, denial of service viruses impact three main places: [38]

1. Boot sector of the hard drive:

These types of viruses attack the boot sector of a floppy disk or the boot sector of a hard disk. The main aspect of a boot virus is centered on the algorithms used at startup of an operating system at power up. When an operating system has initialized and passed all its startup tests (all operating systems perform system tests to validate operational hardware and software), the system begins to read the first physical sector of the boot disk. The first physical sector of the boot disk is dependent upon how the BIOS are setup. For example, if the BIOS are setup to read the CD-ROM first, the boot sector analyzes the BPB, which identifies the operating system file addresses, reads them into system memory, and begins to execute them. If these files are not present in the operating system, the boot sector will identify this as an error and request a change to the boot disk. This startup process also occurs if the system boots to the hard disk. In this case, the startup routine is placed in the master boot record, which analyzes the disk partition table, identifies the addresses in the C drive and loads this information into memory. As in the case of the CD- ROM, if these files are not present in the operating system, the boot sector will identify this as an error and request a change to the boot disk.

The original virus code was contained in a file or attachment that the user downloaded and copied onto the disk or loaded directly to the users hard drive. The startup operations become infected because the code used to run these programs is transferred to the virus code, which is then executed upon operating system startup. As the system initializes, the virus forces the software to read its code and not the original system boot code. A diskette virus is loaded by the diskette and overwrites the startup boot sector code with the malicious code.

These viruses typically corrupt the first free boot sector of the disk, but can target other areas of the disk if the size of the virus is larger than the original target sector of the disk. In this case, the virus can then occupy the first free sector space it finds. The following diagram (Figure 26) according to the Metropolitan Network BBS Inc., [39] depicts an example of an uninfected disk and an infected disk.



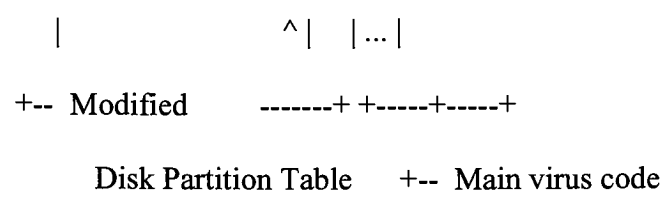


Figure 26 - Diagram According to the Metropolitan Network BBS Inc.

Depicting an Uninfected Disk and an Infected Disk

Each virus family has specific ways in which it acts on system boot sectors. Brain and Ping Pong viruses analyze file allocation tables, marking specific sectors as bad and forcing the startup algorithms to use the virus coding instead of the original coding in the boot sector. The Stoned family of viruses moves the original boot sector to other parts of the hard disk, allowing them to install their code in the now available open sector space. Other viruses such as the Asuza viruses contain their own MBR loader in the body of their code and, after infecting the boot sectors, replace their MBR loader with the original piece of coding. These types of viruses can be overcome by overwriting the existing boot sector code with an uninfected system disk. They can be more difficult to find and remove if the virus is encrypted or uses other programs to initialize calls to the boot sectors. These types of viruses can cause loss of hard disk sector information in the Disk Partition Table, possibly requiring the hard disk to be reformatted to correct the virus problem.

2. Create a bad sector where the virus writes itself to a sector on the hard disk, then using the FAT table, marks that sector as bad so the specific program utilities will not use that sector.

3. Command.com, which contains the basic commands that the operating system uses to access files. [40]

Profits from Viruses Propagation

There is another aspect of virus creation and their impending spread throughout the computer world that needs to be addressed. Virus creation from Hackers and Crackers, etc. is commonly known as an issue. These people create the virus code for various reasons, but there is always the lesser-known perspective that there may be money to be made from a virus. Large corporations such as anti-virus corporations make their money from selling anti-virus software to their customers. These customers are your average homeowners and also large corporations. If a virus spreads to a corporation and disrupts their day-to-day operations, the potential for large monetary losses exist. Rob Rosenberger, [41] who is well-known in the anti-virus community for dispelling myths gives the following account in his article, "McAfee's Media-Assault Tactics" regarding large corporation tactics. "Did you know McAfee Associates pays employees to find flaws in competitors' products? This fact came to light when McAfee launched a new volley of media assaults against Symantec and Dr. Solomon's Software, two major rivals in the anti-virus market. In the first case, McAfee's beta-test division discovered an obscure flaw in Symantec's Norton Utilities. Instead of notifying Symantec, McAfee chose to notify only the media. They even wrote a blatant demonstration program so Windows Sources magazine could include it as part of a fear-inducing online story. Symantec believes McAfee should have notified them instead of helping the media write stories about a trivial flaw. Product manager Tom Andrus told the Associated Press, "We were taken aback that they would go to the press, create something akin to a virus and then basically show the world how to do that." [42] Symantec also berated Windows Sources for providing McAfee's code to any malicious hacker who wanted it.

Editors pulled McAfee's blatant demo from the Windows Sources website the next day. Symantec quickly released a software patch to calm the nerves of frightened customers -- and paid PRNewswire to distribute an extremely polite press release announcing the patch. In the second case, McAfee's beta-test division discovered a supposed "cheat mode" in Dr. Solomon's Anti-Virus Toolkit. McAfee went on the warpath, paying PRNewswire to distribute a press release accusing Solomon's of committing heinous crimes against humanity. "The cheat mode can cause Dr. Solomon's Anti-Virus Toolkit to show inflated virus detection results when the product is being reviewed by trade publications or independent third party testing organizations. McAfee has forwarded its evidence to the National Computer Security Association". Solomon struck back with a hilarious press release: "McAfee Pleads with Dr Solomon's to Reduce Dr Solomon's Virus Detection Rate." They proudly admit their "heuristic" function works exactly as described. "The product given to reviewers is exactly the same product delivered to customers. The technology is available to every user." McAfee responded with another inflammatory press release claiming that Solomon had engaged in a "disinformation campaign."

The article continues, but the important fact remains that two adversaries in the anti-virus corporate world exploited the other's weaknesses for the benefit of themselves. It's important to understand that, in a free market society, the bottom line for a business to stay gainfully employed is to make a profit. As a competitor, it makes complete sense not to help others out, but from a consumer perspective, these may be examples of how big business can work. It is possible to carry this mindset further to the point where the possibility exists for anti-virus corporations to be at the root of some of these viruses, or at least withhold specific information about impending viruses, because it is, after all,

their bottom line that matters and selling anti-virus software to consumers and corporations is what keeps them in business. According to ACM, "Computing professionals have a responsibility to share technical knowledge with the public by encouraging an understanding of computing, including the impact of computer systems and their limitations. This imperative implies an obligation to counter any false views related to computing." [43] In the previous example, both these companies intentionally disregarded this concept, ultimately showing that their priorities lie elsewhere.

Role of Government Agencies

The government recognizes that any forms of computer intrusions via unauthorized access to computers with intentions that may or may not be malicious are crimes that are punishable by law. The problem of Internet security does not necessarily lie within the control of the federal government and may not specifically be a problem that is solved through the criminal justice system, that is until the law has been broken. Internet security has been essentially an issue for the private sector, and has been increasing its security efforts to match the pace of technological changes. One of the issues that face today's government agencies is whether or not the current laws are effective, or whether they have been outdated by changes in technology. According to James X. Dempsey in his testimony before the Subcommittee on Crime of the House Judiciary Committee and the Subcommittee on Criminal Justice Oversight of the Senate Judiciary Committee on February 29, 2000, several proposals have been under consideration since before the recent attacks to amend the computer crime statute and the electronic surveillance laws to enhance law enforcement authorities. [44] He indicates that the Subcommittees, after careful analysis, may find that some modest changes are appropriate. "We urge caution, especially in terms of any changes that would enhance surveillance powers or government access to information. Americans are already deeply concerned about their privacy, especially online." He goes on to say, "You must be careful to ensure that the recent Internet attacks do not serve as justification for legislation or other government mandates that will be harmful to civil liberties and the positive aspects of the openness and relative anonymity of the Internet. Such a course is especially unjustified when there is so much to be done to improve security without changing the architecture or protocols of the Internet or further eroding privacy."[45]

One of the issues seen in the current legal environment is that the standard for government access to information does not completely protect the privacy of legitimate computer users. If government agencies dictate that any legislative changes are necessary in response to Internet security issues, then those changes need to be balanced with measures to improve privacy by tightening the standards for government surveillance and access to information. [46] Security and privacy are intertwined and trying to improve security without addressing end user privacy will create an even greater gap between imposing additional government regulations and the freedom of speech that the Internet now extensively enjoys. This includes imposing additional regulations requiring better records, allowing improved monitoring of Internet service providers. They may pose risks to privacy and may actually harm security in the longer term by impeding technological growth and creating an even more explosive government interference scenario.

In the same testimony, an example of denial of service attacks is used to illustrate how the tools for these attacks, and the knowledge to create these attacks are well known within the private community. By creating legislature to combat these issues without being cautious about impacting personal rights, might create additional friction as the general public might consider these measures invasive. These attacks target e-commerce web sites with phony messages requiring the targeted computers to respond, thereby creating an atmosphere where legitimate traffic cannot get through. The tools for warning, diagnosing, and preventing Internet attacks are in the hands of the general public. Because this type of crime is very different from what we refer to as typical crimes, government agencies are limited in their responses, both in the ability to catch the

perpetrators and in the ability to do so in a timely fashion. The issue itself is that the original concept of the Internet was an open architecture-sharing medium, with little or no security measures incorporated into its design. There are actions government agencies can take to help incorporate improved security within the Internet without impacting personal freedoms.

James X. Dempsey has suggested in the following in his testimony, "The government should do more to support basic research and development in computer security." He also asks, "What changes in law, if any, would likely have deterred or made it easier to investigate and prosecute the denial of service attacks, or other exploitations of Internet vulnerability?" [47] He indicates that there are three major laws setting privacy standards for government interception of communications and access to subscriber information that need updating to reflect new technological advances. [48]

1. The federal wiretap statute ("Title III"), 18 USC 2510 et seq., requiring a probable cause order from a judge for real-time interception of voice and data communications

2. The Electronic Communications Privacy Act of 1986 (ECPA), 18 USC 2701 et seq., setting standards for access to stored electronic communications and transactional records (subscriber identifying information, logs, toll records)

3. The pen register and trap and trace statute, enacted as part of ECPA, 18 USC 3121 et seq., governing real-time interception of "the numbers dialed or otherwise transmitted on a telephone line."

He also points out in the following list that existing laws provide inadequate protection.

1. The standard for pen registers (which collect phone dialing information in real time) is minimal - judges must rubber stamp any application presented to them.

2. Many of the protections in the wiretap law, including the special approval requirements and the statutory rule against use of illegally obtained evidence, do not apply to email and other Internet communications.

3. Data stored on networks is not afforded full privacy protection.

4. ISP customers are not entitled to notice when personal information is subpoenaed in civil lawsuits; notice of government requests can be delayed until it is too late to object.

5. Amend the Computer Fraud and Abuse Act to allow federal investigation and prosecution in cases where the total damage is less than $5,000. The Act already allows accumulation of loss to cover hacks that cause a small amount of damage to a large number of computers so long as the total damage in the course of any 1-year period is at least $5,000.

6. Authorize judges in one jurisdiction to issue pen register and trap and trace orders to service providers anywhere in the country.

7. Increasing computer crime prosecutions by modifying a sentencing directive requiring a mandatory minimum sentence of six months in prison for violations.

8. Make juveniles 15 years of age and older eligible for federal prosecution in cases where the Attorney General certifies that such prosecution is appropriate.

9. Add computers located outside the United States to the definition of protected computers.

10. Add forfeiture of any property used or intended to be used to commit or facilitate the crime to the penalties and forfeiture of any device used to copy a computer program or other item to which a counterfeit label is affixed.

11. Permit interception without a court order upon consent of an operator of a system when the system is the subject of attack.

The issues surrounding these enhancements do reflect upon the privacy of individuals. These issues are being addressed to the point where any legislation proposed will need to be balanced in proportion to the privacy of the Internet user. Some of these enhancements include:

1. Limit the pen register/trap and trace authority to improve further the privacy protections adopted for pen register and trap and trace investigations.

2. Add electronic communications that respond by prohibiting the government from using improperly obtained information about electronic communications.

3. Require notice and an opportunity to object when civil subpoenas seek personal information about Internet usage.

4. Improve the notice requirements to ensure that consumers receive notice whenever the government obtains information about their Internet transactions.

5. Limit sale and disclosure of transactional information about Internet usage

6. Clarify whether Internet queries are content, which cannot be disclosed without consent or legal process.

7. Provide enhanced protection for information on networks: probable cause for seizure without prior notice, opportunity to object for subpoena access.

8. Limit authority for roving taps.

9. Establish probable cause standard for access to wireless phone location data in real-time.

10. Enact clearer standard for interception of conference calls.

11. Extend to law enforcement interceptions overseas.

12. Privacy standards for government access to data collected by DNS registrars and registries.

Essentially, the Internet security issue is a known problem. The solution, however, may reside in the hands of the private end user rather than through government mandated legislation. Building more secure networks is largely within the realm of the companies who create the software. New government legislation controls need to balance the individual's privacy with enough assertion to help prevent and ultimately punish those responsible for Internet violations.

Vendor Support of IPv6

Today, IPv6 appeals to people and vendors alike in various networking industries, research organizations, as well as military and government agencies in the United States and abroad. Internet service providers worldwide will incorporate IPv6 as market requirements mature and adoption continues to grow with systems at home that are, and will be connected to, a network that will require an enormous increase of global IP addresses. Growing demands for wireless Internet addresses, and expanding development in integrating Internet connectivity into devices such as automobiles and appliances will result in the demand for IPv4 addresses to exceed supply. IPv6 overcomes this, as well as other IPv4 limitations, by expanding addresses to 128 bits and offering other functionality to support future growth. According to Agilent Technologies, "In order to migrate networks to IPv6, network equipment developers and service providers must ensure that core routers and networks can support both IPv4 and IPv6 traffic during the transitional period. In addition, core network routers must be able to deliver IPv6 forwarding at wire rates, without sacrificing performance or reliability. IPv6 core routers must also support IPv6 routing protocols, as well as migration mechanisms such as tunneling, dual stacks and protocol translation". [49] The advantages to migrating to IPv6 are numerous. Examples include deploying IPv6 on existing production networks, increased end user problem resolution capabilities that incorporate additional third party solutions, and additional features that can be incorporated by new software upgrades. These features will offer increased services for current firewall, web browser, server, and desktop applications. There are also additional advantages that can be currently employed by vendors. IPv6 products currently being released are architected to be deployed on the current IPv4 production networks. These products offer increased problem resolution

support between the vendor and end user, along with increased web browser, server, firewall, and desktop capabilities. These services can be provided by software upgrades to the product, which allow vendors to begin deploying an IPv6 infrastructure. This becomes advantageous to the vendors because these mechanisms were designed to be interoperable with the current IPv4 infrastructure. Because it may take many years for the existing IPv4 infrastructure to be replaced, vendors will ship their products with dual capabilities of supporting both IPv4 and IPv6. There are exceptions to this in specific markets such as cell phones and Internet appliances. [50] These markets are releasing their product lines utilizing IPv6 technologies only. Currently though, these are emerging technology based products using IPv6 because they do not have applications that are using older IPv4 applications.

Third party software companies such as Cisco Systems have adapted to deliver additional standards-compliant IPv6 features and solutions across multiple platforms. [51] Cisco software, for example, will deliver broad and advanced IPv6 routing capabilities to fully utilize the latest in transmission protocol upgrades. According to Stephen Deering, Cisco Fellow and lead designer, "While many vendors have been focused on delivering the 'wireless Internet' or the 'optical Internet,' Cisco has been working on integrating these and other technologies into the current Internet. By building IPv6 into Cisco IOS software, we are enabling continued growth of the Internet and its expansion into new applications and capabilities in a way that maintains compatibility with existing Internet services. Furthermore, Cisco is the only major networking vendor to deliver IPv6 across multiple platforms, thus ensuring that our customers and partners can deploy IPv6 when and where required." [52]

Deployment of IPv6 will still have unknowns associated with it for some time to come. Large corporations will continue looking at their applications as the technology evolves. March 4, 2003, the Beijing Internet Institute (BII), a leading global research and testing facility, announced the results of the world's first public core router trial which is designed to test IPv6 interoperability and performance. [53] This test had participants from four network equipment developers, Fujitsu, Ltd., Hitachi, Ltd., Juniper Networks, and NEC Networks. The core routers tested were the Fujitsu GeostreamR920, the Hitachi GR2000-20H, the Juniper Networks M20, and the NEC CX5210. Agilent Technologies provided test systems, IPv6 test methodologies, and technical support for the testing. Using the Agilent Router Tester, BII conducted independent tests of each core router, including routing protocol conformance testing, OC-48 IPv6 performance testing, IPv6 routing stress tests and BGP4+ and OSPFv3 interoperability tests, to verify the feasibility of IPv6 deployment. Based on test results and measurements, all participating routers successfully demonstrated the ability to support commercial IPv6 networks and provide basic IPv6 capabilities, including support for IPv6 routing protocols, forwarding of IPv6 datagrams at wire rate, and IPv6 interoperability between the equipment tested. " This event marks an important step forward in advancing the deployment of the next-generation IPv6 protocol, and delivering the many benefits it brings to the world's core networks," said Hua Ning, chief technology officer of BII. "We were extremely pleased to host China's first IPv6 test event and to make the results available to the world's networking community. While this was not a comparative performance test of different router vendors, we achieved our collective purpose by publicly verifying the feasibility of IPv6 deployment." [54]

Other vendors have shown their support for IPv6 as seen at the 2001 Vendor exhibition [55] in Japan. Examples of some of the software vendors IPv6 support intentions are:

1. As already indicated, Cisco will support IPv6 in a distribution-type layer 3 switching solution designed to provide high-performance capabilities for its high-end router series, with the ultimate goal of building a large-scale IPv6 backbone network. They also intend to proceed with development for implementing IPv6 support in their switch products and for implementing hardware-based IPv6 high-speed forwarding.

2. Foundry Networks plans on delivering a multi-phased approach for IPv6 solutions including full IPv6 protocol routing support in their software. These high end products provide reliable IP routing functions and deliver new functionality for Ethernet solutions.

3. Juniper Networks routers are purpose-built to meet the challenges of the new IP infrastructure used in critical applications such as core routing, dedicated access, peering, and data center hosting by service providers.

Even with the current support of IPv6 technologies, there are inherent risks associated with it. Businesses that are looking at IPv6 as a viable technology upgrade are concerned with basic issues like cost, implementation, and support. There is also the concern of knowing when there will be sufficient market penetration of the new technology to consider rolling IPv6 capabilities on the existing core routers and switches. According to Richard A. Steenbergen, in an article titled, "When IPv6 ... if ever?" he writes, "There are two key problems which are preventing the widespread use of IPv6, IP Allocation, and

network vendor support. Support for all hosts is actually one of the least of the problems." Major business networks want to deploy IPv6, but are not sure of the proper way of accomplishing it. "They certainly can't do it on their primary backbone links and routers, the support from vendors is simply not there. Even if there was working code, they wouldn't dare deploy it on their production network, the code is too unstable (especially IPv6 routing protocols), and they risk looking unreliable in comparison to those who don't even make the attempt to support IPv6." [56] Without the network there is limited demand for high traffic IPv6, and without the demand there is little desire to build the network. He questions, "Should they buy separate routers, try desperately to make IPv6 work well on a spare 7200, and hope not to get a black eye from customers who expect the same level of routine-ness we are experienced with in IPv4? Should they provision more circuits because of this? Build a parallel network supporting IPv6, without a current customer demand? Or do they say, "We'll wait until the vendors get it right?" These are valid points. Also to be considered is the fact that IPv4 is currently running at an effective level of stability and speed and the new IPv6 infrastructure may take time to achieve current IPv4 levels of performance. If, in fact, this is true, then infrastructure support may also be lagging behind. Technological advances are, in part, based on customer demand and, if the demand is somewhat minimalized by the end user community that would slow down development from vendors. As much as there will always be issues surrounding the deployment of new technologies, eventually new software technologies, or next generation technologies such as IPv6, will be incorporated into the Internet mainstream.

Conclusion

The major thrust of IPv6 is to address security issues by incorporating embedded security technology that can solve many of the common privacy and encryption problems to which the current IPv4 is subjected. A conclusion can be drawn that IPv6's enhanced security functionality does solve many of the current known issues that surround IPv4 architecture, but will not be able to solve all of them.

Advances in technology, along with the rapid spread of Internet usage by consumers, has forced changes in the way computer use and its associated applications are now architected. This is evident with new software programs such as online banking that are being integrated into everyday activities. These changes have also brought with them the downside of increased network breaches and intrusions. Computer security has become a major concern to businesses and individuals who use this technology as a way of life. These programs have become easy targets for intrusions because of their easy accessibility on the Internet.

Data intrusions can occur along many areas of a network, from interception of data transfers at access points such as routers, to gaining permission to account information such as root passwords, thereby allowing intruders the ability to overwrite existing boot files and take control of the system. Early intrusions simply exploited poor system design to gain access to system files. Intruders understood that networked systems were designed with default settings in place, making access relatively easy. Considerations to

incorporate security into system design were not practical because administrators did not have the resources or tools to actively monitor their networks for any unwanted activity.

It became clear that the current IPv4 architecture needed to be changed to reflect the need for better network security. IPv4, designed initially for use in educational and research endeavors to exchange electronic data without regard to network security, incurred many upgrades into its architectural scheme to help combat existing shortcomings. With these upgrades came more complex security breaches as intruders began migrating to source code, looking for weaknesses in programs. Security upgrades, such as encryption technology helped secure data, but were only patches to cover the deeper problems. The correct fix was IPv6, a new Internet architecture that incorporated the embedded technology needed to enhance security to meet today's security demands.

IPv6 addresses many of the IPv4 shortcomings. IPv6 increases the addressing capabilities to a 128-bit addressing scheme, from the 32-bit addressing scheme used in IPv4. This greatly increases the number of addressable nodes, reducing the potential problem of running out of IP addresses. Security enhancements such as IP Authentication Header, and IP Encapsulating Security Payload mechanisms were also included in the core design. These features incorporated into the core architectural design of IPv6, allow for increased data authentication and integrity by verifying the data sent in a transmission will be received intact and unchanged.

There are though, other issues that need to be addressed when looking at security intrusions in a networked system. It is not the technical aspect of software coding or the

hardware components that connect the network, but the human aspect that creates the intrusions. Exploiting a computer system to gain access to sensitive data is for some a challenge to see if it can be done, and for others, it represents a statement of defiance to try to do something we are told we cannot. A business that proclaims their networked system is secure just may pose enough of a challenge for an intruder to attempt access. As technological changes continue to develop, security techniques required to protect network system infrastructures will continue to become more complex to ward off increasingly complex attacks to existing known vulnerabilities. The continued problem is these security fixes incorporated into today's applications will not resolve the network breaches from advanced technology gains tomorrow because the intruder's knowledge will become more sophisticated, especially as they gain increased understanding of network integration, system operations, and architectural protocol design. Elimination of these types of attacks will only occur when the incentive for intruders has changed to the point where reward or gain, either personal or financial, has been eliminated.

Acronyms

Note: Unless otherwise noted these are the acronyms used in this paper.

ACM - Association of Computing Machinery
AD – Area Directors
AH – Authentication Header
ANS - Advanced Network Services
ANSI - American National Standards Institute
ARPA - Advanced Research Projects Agency
ASCII - American Standard Code for Information Interchange
BIND - Berkley Internet Name Domain
BIOS – Basic Input/Output System
BPB – BIOS Parameter Block
CA - Certificate Authority
CD-ROM – Compact Disk – Read Only Memory
DARPA - Defense Advanced Research Projects Agency
DES - Data Encryption Standard
DNS – Domain Name System
DSL - Digital Subscriber Line
EBCDIC - Extended Binary Coded Decimal Interchange Code
ESP - Encapsulating Security Payload
FAT - File Allocation Table
FTP - File Transfer Protocol
Gbps – Giga-bytes per second
HTTPS - Secure Hyper Text Transfer Protocol
IAB Internet Architecture Board
IANA - Internet Assigned Numbers Authority
ICMP - Internet Control Message Protocol
IE – Internet Explorer
IESG - Internet Engineering Steering Group
IETF - Internet Engineering Task Force
IGMP - Internet Group Management Protocol
IP – Internet Protocol
IPSec – Internet Protocol Security
IPv4 – Internet Protocol version 4
IPv6 – Internet Protocol version 6
ISDN - Integrated Services Digital Network
ISO - International Standards Organization
ISOC – Internet Society
ISP – Internet Service Provider
ITUT - International Telecommunication Union- Telecommunications Standardization Sector
LAN – Local Area Network
LPD - Line Printer Daemon
MAC – Media Access Control
Mbps – Mega-bytes per second
MBR – Master Boot Record

MD5 - Message Digest 5
MDAC – Microsoft Data Access Components
MIB - Management Information Base
NAP - Network Access Points
NFS – Network File System
NIPC - National Infrastructure Protection Center
NSF - National Science Foundation
OSI – Open Systems Interconnection
PDU – Protocol Data Unit
PKI - Public Key Infrastructure
RFC – Request for Comment
RIP - Routing Information Protocol
RPC – Remote Procedure Calls
SA - Security Association
SANS Institute -
S/MIME - Secure Multipurpose Internet Mail Extensions
SMB - Server Message Block
SMTP - Simple Mail Transfer Protocol
SNA - Systems Network Architecture
SNMP - Simple Network Management Protocol
SSH – Secure Shell
SSL - Secure Socket Layer
STD -Standards
TCP – Transfer Communications Protocol
TCP/IP - Transfer Communications Protocol / Internet Protocol
TOS - Type of Service
TSL - Transport Layer Security
TTL – Time to Live
V6ops – Internet Protocol version 6 Operations Working Group
VPN – Virtual Private Network

Endnotes

[1] James, Leon. Psychology of Computer Viruses. Retrieved August 2003. http://www.soc.hawaii.edu/leonj/409bf98/altenburg/hoax

[2] Introduction to TCP/IP. 2 February 1995. http://www.yale.edu/pclt/COMM/TCPIP.HTM

[3] Overview of the IETF. Retrieved December 2003. http://www.ietf.org/overview.html

[4] Virus Naming Conventions. Retrieved May 2003. http://www.mat.uni.torun.pl/~gracjan/english/index.htm

[5] IPv6 Operations (v6ops). 15 March 2003. http://www.ietf.org/html.charters/v6ops-charter.html

[6] What is NAP?. 12 February 2004. http://www.webopedia.com/TERM/N/NAP.html

[7] Wave Technologies International. Networking Essentials. Retrieved May 2003.http:www.wavetech.com

[8] DOD Standard Internet Protocol. January 1980. http://www.ietf.org/rfc/rfc0760.txt?number=760

[9] RFC 223. 14 September 1971. http://www.faqs.org/rfcs/rfc223.html

[10] Internet Protocol. DARPA Internet Program Protocol Specification. September 1981.http://www.ietf.org/rfc/rfc0791.txt?number=791

[11] Strong Security on Multiple Server Environments. Retrieved 20 January 2003. http://www.verisign.com/resources/wp/secureEnvs/secureEnvs.html

[12] Deering, S. Internet Protocol, Version 6 (IPv6) Specification. December, 1995.http://www.ietf.org/rfc/rfc1883.txt?number=1883

[13] IPv6 Security Improvements. Retrieved January 2003. http://docs.sun.com/db/doc/806-0916/6ja8539bk?a=view

[14] Dekker Marcel. Security of the Internet. Retrieved January 2003. http://www.isc.org/ds/

[15] A beginner's Guide to Computer Viruses. Retrieved 12 December 2003. http://www.5star-shareware.com/avc/guide.html

[16] Cert Coordination Center. 10 May 2004. http://www.cert.org/

[17] Overview of the IETF. Retrieved December 2003.
http://www.ietf.org/overview.html

[18] Miller, Toby. Rating the Enemy: How to identify the Enemy. Retrieved May 2003.http://www.incidents.org/detect/rating.html

[19] Wave Technologies International. Networking Essentials. Retrieved May 2003.http:www.wavetech.com

[20] Types of Viruses. Retrieved May 2003.
http://www.mat.uni.torun.pl/~gracjan/english/index.htm

[21] Types of Viruses. Retrieved May 2003.
http://www.mat.uni.torun.pl/~gracjan/english/index.htm

[22] Types of Viruses. Retrieved May 2003.
http://www.mat.uni.torun.pl/~gracjan/english/index.htm

[23] What is ANSI?. 22 June 2001.
http://www.webopedia.com/TERM/A/ANSI.html

[24] What is DES?. 22 October 2003.
http://www.webopedia.com/TERM/A/ANSI.html

[25] Strong Security on Multiple Server Environments. Retrieved 20 January 2003.
http://www.verisign.com/resources/wp/secureEnvs/secureEnvs.html

[26] Strong Security on Multiple Server Environments. Retrieved 20 January 2003.
http://www.verisign.com/resources/wp/secureEnvs/secureEnvs.html

[27] Strong Security on Multiple Server Environments. Retrieved 20 January 2003.
http://www.verisign.com/resources/wp/secureEnvs/secureEnvs.html

[28] Bound, Jim. How to get to IPv6. March 2000.
http://www.ipv6forum.org/navbar/events/telluride00/presentations/ppt/jimbound-compaq.ppt

[29] ACM Code of Ethics and Professional Conduct. 14July2003.
http://www.ccsr.cse.dmu.ac.uk/resources/professionalism/codes/acm.html

[30] The Sandrin Anti Virus Connection. 18 April 2004.
http://www.sandrin.com/sandrin/faq.htm

[31] A beginner's Guide to Computer Viruses. Retrieved 12 December 2003.
http://www.5star-shareware.com/avc/guide.html

[32] A beginner's Guide to Computer Viruses. Retrieved 12 December 2003.
http://www.5star-shareware.com/avc/guide.html

[33] Twist, Jo, BBC News. Why People Write Computer Viruses. 25 August 2003.

http://www.frame4.com/php/article702.html

[34] Garcia, Beatrice E. Virus Writers get Smarter, Tricky. Retrieved October 2003.http://www.miami.com/mld/miamiherald/7811390.htm

[35] Schuster, Ryan R. Why do Viruses Exist. January 2004. http://www.avcollective.com/Exsist.htm

[36] Ethics Document for the ChemISTS application. Retrieved 14July2003. http://www.cs.siue.edu/seniorprojects/group1/documents/ethics.htm

[37] Twist, Jo, BBC News. Why People Write Computer Viruses. 25 August 2003. http://www.frame4.com/php/article702.html

[38] How Viruses Work - II. 5 July 2002. http://www.funducode.com/freec/misc_c/new_misc_c19/Article19.htm

[39] Computer Viruses by Eugene Kaspersky. Retrieved 14July2003. http://www.viruslist.com

[40] Rhode Island Soft Systems, Inc. A Beginners Guide to Vmyths. 2000. http://vmyths.com/resource.cfm?id=56&page=1

[41] Rosenberger, Rob. McAfee's Media-Assult Tactics. 22 April 1997. http://vmyths.com/rant.cfm?id=279&page=4

[42] Rosenberger, Rob. McAfee's Media-Assult Tactics. 22 April 1997. http://vmyths.com/rant.cfm?id=279&page=4

[43] ACM Code of Ethics and Professional Conduct. 14July2003. http://www.ccsr.cse.dmu.ac.uk/resources/professionalism/codes/acm.html

[44] Dempsey, James X. Internet Denial of Service Attacks and the Federal Response. 29 February 2000.http://www.cdt.org/security/000229judiciary.shtml

[45] Dempsey, James X. Internet Denial of Service Attacks and the Federal Response. 29 February 2000.http://www.cdt.org/security/000229judiciary.shtml

[46] Dempsey, James X. Internet Denial of Service Attacks and the Federal Response. 29 February 2000.http://www.cdt.org/security/000229judiciary.shtml

[47] Dempsey, James X. Internet Denial of Service Attacks and the Federal Response. 29 February 2000.http://www.cdt.org/security/000229judiciary.shtml

[48] Dempsey, James X. Internet Denial of Service Attacks and the Federal Response. 29 February 2000.http://www.cdt.org/security/000229judiciary.shtml

[49] Router Test Solution. News and Press Releases. 4 march 2003. http://advanced.comms.agilent.com/RouterTester/news/Mar03_BII.htm

[50] Bound, Jim. How to get to IPv6. March 2000.
http://www.ipv6forum.org/navbar/events/telluride00/presentations/ppt/jimbound-compaq.ppt

[51] Cisco's IPv6 Solution. 15 may 2003.
http://www.voipwatch.com/print_article.php3?sid=622

[52] Cisco's IPv6 Solution. 15 may 2003.
http://www.voipwatch.com/print_article.php3?sid=622

[53] Router Test Solution. News and Press Releases. 4 march 2003.
http://advanced.comms.agilent.com/RouterTester/news/Mar03_BII.htm

[54] Router Test Solution. News and Press Releases. 4 march 2003.
http://advanced.comms.agilent.com/RouterTester/news/Mar03_BII.htm

[55] Steenbergen, Richard A. When IPv6...if ever?. 2 September 2000.
http://www.merit.edu/mail.archives/nanog/2000-09/msg00080.html

[56] Steenbergen, Richard A. When IPv6...if ever?. 2 September 2000.
http://www.merit.edu/mail.archives/nanog/2000-09/msg00080.html

Bibliography

Atkins, John and Norris, Mark. Total Area Networking. West Sussex, England: John Wiley & Sons Ltd, 1995.

Beyda, William J. Data Communications from Basics to Broadband. Upper Saddle River, New Jersey: Prentice Hall PTR, 1996.

Black, Uyless. TCP/IP and Related Protocols. New York, New York: McGraw-Hill, Inc., 1998.

Miller, Lawrence and Gregory, Peter H. CISSP for Dummies. New York, New York: Wiley Publishing, Inc., 2002.

Naugle, Matthew and Black, Uyless. Network Protocol Handbook. New York, New York: McGraw-Hill, Inc., 1994.

Rosenfeld, Louis and Morville, Peter. Information Architecture for the World Wide Web. Sebastopol, CA, 1998.

Schein, Phillip G. Windows 2000 Security Design. Scottsdale, Arizona: The Coriolis Group, LLC. 2000.

Stallings, William and Van Slyke, Richard. Business Data Communications. Upper Saddle River, New Jersey: Prentice Hall PTR, 1998.

Tanenbaum, Andrew S. Computer Networks. Upper Saddle River, New Jersey: Prentice Hall PTR, 1996.

Tannenbaum, Andrew S. Structured Computer Organization. Englewood Cliffs, New Jersey: Prentice Hall, Inc., 1990.

Addendum A – Figures

Addendum B – Presentation Slides

The following slides are the thesis presentation slides.

Embedded Security Improvements to IPv6

Presentation Agenda

- Assertion statement
- Project scope
- Discussion Topics
  - Introduction
  - Need for Standardization
  - Data Transfer
  - Communication Architectures
  - OSI
  - TCP/IP
  - Internet Protocol
  - IP Datagrams
  - IPv4 Datagram

Presentation Agenda

- Discussion Topics Continued
  - IPv6
  - Major Differences Between IPv4 and IPv6
  - IPv6 Security Schemes
  - IPv6 Datagram
  - IPv4 vs. IPv6 Address Header Field Differences
  - Intrusions and Detections
  - Viruses
    Security Controls
  - IP Security Architecture
  - Human Interaction
  - Conclusion

Assertion Statement

- IPv6's embedded security can solve many of the common privacy and encryption problems to which the current IPv4 is subject.

Project Scope

- Defme and analyze the TCP/IP communications protocol in IPv4 and evaluate how the security changes in IPv6 will overcome security shortcomings

Introduction

- Reasons for the IPv6 upgrades
  - Security
  - Functional Expandability

Need for Standardization

- TCP/IP Standardization
- Roles of development organizations – IETF, IAB, Working Groups (V6ops)
- Working Group Charters
  - Solicit input
  - Provide feedback
  - Publish informational RFCs that help developers understand real world issues, identify security risks, analyze deployment solutions, assume responsibilities for IPv6 transition

Data Transfer

- All forms of data transmission, either data, voice, or video use electromagnetic signals transmitted over their corresponding medium
  - Data is converted from original source (computer) into a signal (analog or digital), transmitted over medium, then reconverted into original source

Communication Architectures

- Manufacturers concepts for networking their devices together. Examples include:
  - Digital Network Architecture (DEC)
  - AdvanceNet (HP)
  - Distributed Systems Architecture (Honeywell)
  - Internet Packet Exchange (Novell)
  - Xerox Network Systems (XNS)
- Allow a wide range of computer makes, models, and operating systems to communicate across networks. Examples include:
  - TCP/IP
  - OSI

OSI Model

- Developed by ISO as a model to be used as a guide for other protocols. Each layer (7) has its own functionality
- Layers were developed so specific data transfer functions were distinct
- Eventually replaced by TCP/IP because it did not meet the anticipated growth of the Internet
- Has corresponding layers to other protocols such as TCP/IP

TCP/IP

- Has become standard Internet framework for communication protocols
- Standardized by the IAB to maintain commonality among protocols to connect different operating systems
- IAB made up of committees that issue standards

TCP/IP

- Made up of multiple protocols
- TCP – packages and prepares data for transfer. Provides error recovery and data analysis
- IP – establishes the framework needed for successful data transfer using a common address scheme to identify host computer and network
- Has corresponding layers to other protocols such as the OSI Model

TCP/IP

- Current protocol encompasses five layers that provide different tasks
  - Application
  - Transport
  - Internet
  - Network Access
  - Physical

Internet Protocol

- Computers installed on Internet through an ISP requires an IP address that conforms to IP naming conventions
- Current IPv4 uses 32-bit addressing scheme
- IP addresses are used to determine where network traffic is to be routed

IP Datagrams

- The data sent from a computer through a network is known as an IP Datagram
- These data units are divided into smaller units that describe how the information is processed by the IP protocol

IPv4 Datagram

IP Version	Protocol
Header Length	Header Checksum
TOS	Source Address
Total Length	Destination Address
Identifier	Options
Flags	Padding
Fragment Offset	Data
Time-To-Live	

IPv6

- RFCs 1883-1886
- Updated version from IPv4 that incorporates changes in address space, improved network architecture techniques, and incorporate greater security
- Many characteristics of IPv4 will temporarily remain because of dependencies with other protocols
- Seamless upgrade from IPv4

Major Differences Between IPv4 and IPv6

- Expanded Addressing Capabilities
  - Increase the IP address size from 32 bits to 128 bits
- Header Format Simplification
  - Simplified IPv4 header fields
- Improved Support for Extensions
  - More improved data forwarding and greater flexibility for future functionality
- Flow Labeling Capabilities
  - New capabilities to label data packets
- Authentication and Encryption Capabilities
  - Support for Data authentication, integrity, and confidentiality

IPv6 Security Schemes

- IPv4 not designed with security in mind
- IPv6 integrated two security schemes into lower protocol layers
  - IP Authentication Header
  - IP Encapsulating Security Payload

IPv6 Datagram

IP Version	Hop Limit
Priority	Source Address
Flow Label	Destination Address
Payload Length	Data
Next Header	

IPv4 vs. IPv6 Address Header Field Differences

IPv4	IPv6
Version Identifier - 4	Version Identifier - 6
Header length field	Payload length replaces IPv4 total length field
TOS field	Eliminates TOS field
Identification, flag, and fragment offset fields	Eliminates identification, flag, and fragment offset fields
Protocol field	Remains in another extension header
Time-To-Live	Renamed to Hop Limit field
Header Checksum field	Eliminated Header Checksum field
Options field	Replaced with header extensions

Intrusions and Detections

- Can occur in different areas of a network such as:
  - Gaining access to root directories
  - Network connection access as administrators
  - Permissions to specific directories and users on a network

Intrusions and Detections

- Automated software programs used by intruders have led to attacks becoming more effective and devastating. Tools include:
  - Network scanners
  - Password cracking tools
  - Packet sniffers
  - Trojan Horse programs
  - Tools to modify system log files
  - Tools to allow the attacker to remain anonymous
  - Tools to modify system configuration files

Intrusions and Detections

- Internet security intrusions can be broken down into basic types:
  - Probes
  - Scan
  - Malicious Code
  - Denial of Service
  - Account Compromise
  - Packet Sniffer
  - Root Compromise
  - Exploitation of Trust
    Infrastructure Attacks

Viruses

- Software programs designed to replicate and spread themselves
- Usually require host to allow them to propagate
- Can have an impact on all programs, files, and hard disks

Viruses

- Examples of recognized virus types:
  - Macro
  - File Infector
  - Multi-Partite
  - Boot Sector
  - Master Boot Records

Security Controls

- Other forms of encryption and authentication technologies are being implemented
  - PKI verifies confidentiality and authenticity between information sharing networks
  - Certificate Authorities offer a digital trust between parties that verify that sending and receiving parties are who they claim to be

IP Security Architecture

- Because it will take years to fully implement IPv6 128 bit addressing scheme, other improvements are being deployed in IPv4
- IPSec architecture uses two network layer security protocols, AH and ESP and are recognized by all sharing parties
  - AH provides authentication and data integrity
  - ESP provides confidentiality

Human Interaction

- Understanding intrusion attacks requires an understanding of why the attacks occur
  - Hackers / Crackers
  - Coding Ethics
  - Virus Propagation Profits
- Role of government agencies
- Vendor support of IPv6

Conclusion

- Does IPv6 solve IPv4 security issues?
- Where do we go next for security prevention?