Computer Networks: Current Developments in its Security

V. B.Ambare
Asst. Prof. (IT Dept.)
AEC, Chikhli

B. A. Dongardive
I.T. Department
AEC, Chikhli

R.G.Bhople
I.T. Department
AEC,Chikhli

M.S.Chavan
I.T. Department
AEC, Chikhli

ABSTRACT
In this paper, we described the Computer network security because it has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The architecture of the internet, when modified can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the appropriate security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. The businesses create an "intranet" to remain connected to the internet but secured from possible threats.
The entire field of network security is vast and in an evolutionary stage. The range of study encompasses a brief history dating back to internet's beginnings and the current development in network security. In order to understand the research being performed today, background knowledge of the internet, its vulnerabilities, attack methods through the internet, and security technology is important and therefore they are reviewed.

Keywords
Intrane

1. INTRODUCTION
The world is becoming more interconnected with the advent of the Internet and new networking technology. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet. There are currently two fundamentally different networks, data networks and synchronous network comprised of switches. The internet is considered a data network. Since the current data network consists of computer-based routers, information

can be obtained by special programs, such as "Trojan horses," planted in the routers. The synchronous network that consists of switches does not buffer data and therefore are not threatened by attackers. That is why security is emphasized in data networks, such as the internet, and other networks that link to the internet.

2. BASIC SECURITY CONCEPT
It seems that every other day there is a story in the newspapers about a computer network being compromised by hackers. In fact, not too long ago the Department of Defense (DOD) was the victim of a successful hacker raid; hackers were able to penetrate DOD computers during a two-week period before they were detected. Fortunately, the computers contained only non-classified personnel and payroll information, so national security was not threatened. More recently, Yahoo, Amazon.com, eBay, and some other popular World Wide Web (WWW) sites were targets of what appears to have been a coordinated "denial-of-service" attack. During a three- or four-day period, the sites were overwhelmed with massive bombardments of false traffic from multiple sites.

As a result, the sites were shut down for hours at a time. These attacks illustrate how pervasive the threat from outside hackers has become. At the same time, every organization that uses computers faces the threat of hacking from individuals within the organization. Employees or former employees with malicious intent or who want to obtain information such as employee salaries or view other employee's files are also a threat to an organization's computers and networks.

Computerworld recently ran a story about a programmer employee of a company who allegedly launched a denial-of-service attack against his own company, a provider of on-line stock trading services. Apparently, this programmer was in negotiations with the company for more compensation. He became frustrated with the progress of the negotiations and decided to demonstrate to the company its vulnerability by launching an attack on its systems from the Internet. He was intimately familiar with the company's systems and software, and his inside knowledge enabled him to hit the firm in a manner that shut it down. In fact, the attack disrupted stock trading services at the company for three days. The U.S. Secret Service was eventually employed, and the attack was traced to the employee, who was subsequently arrested.

Every organization should monitor its systems for possible unauthorized intrusion and other attacks. This needs to be part of the daily routine of every organization's IT unit, as it is essential to safeguarding a company's information assets. The most reliable way to ensure the safety of a company's computers is to refrain from putting them on a network and to keep them behind locked doors. Unfortunately, however, that is not a very practical solution. Today, computers are most useful if they are networked together to share information and resources, and companies that put their computers on a

network need to take some simple precautions to reduce the risk of unauthorized access.

Every year, corporations, governments, and other organizations spend billions of dollars on expenditures related to network security. The rate at which these organizations are expending funds seems to be increasing. However, when companies need to find areas in which they can decrease spending, budget items such as security and business resumption planning have historically been some of the first to be cut.

3. NETWORK SECURITY

System and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. Although, network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented.

There exists a "communication gap" between the developers of security technology and developers of networks. Network design is a well-developed process that is based on the Open Systems Interface (OSI) model. The OSI model has several advantages when designing networks. It offers modularity, flexibility, ease-of-use, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allow modular development. The implementation of individual layers can be changed later without making other adjustments, allowing flexibility in development. In contrast to network design, secure network design is not a well developed process. There isn't a methodology to manage the complexity of security requirements. Secure network design does not contain the same advantages as network design.

When considering network security, it must be emphasized that the whole network is secure. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the data, decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message.

When developing a secure network, the following need to be considered [1]:

1. Access – authorized users are provided the means to communicate to and from a particular network
2. Confidentiality – Information in the network remains private
3. Authentication – Ensure the users of the network are who they say they are
4. Integrity – Ensure the message has not been modified in transit
5. Non-repudiation – Ensure the user does not refute that he used the network

An effective network security plan is developed with the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack [1]. The steps involved in understanding the composition of a secure network, internet or otherwise, is followed throughout this research endeavor.

To lessen the vulnerability of the computer to the network there are many products available. These tools are encryption, authentication mechanisms, intrusion-detection, security management and firewalls. Businesses throughout the world are using a combination of some of these tools. "Intranets" are both connected to the internet and reasonably protected from it. The internet architecture itself leads to vulnerabilities in the network. Understanding the security issues of the internet greatly assists in developing new security technologies and approaches for networks with internet access and internet security itself.

The types of attacks through the internet need to also be studied to be able to detect and guard against them. Intrusion detection systems are established based on the types of attacks most commonly used. Network intrusions consist of packets that are introduced to cause problems for the following reasons:

- To consume resources uselessly
- To interfere with any system resource's intended function
- To gain system knowledge that can be exploited in later attacks

The last reason for a network intrusion is most commonly guarded against and considered by most as the only intrusion motive. The other reasons mentioned need to be thwarted as well.

Typical security currently exists on the computers connected to the network. Security protocols sometimes usually appear as part of a single layer of the OSI network reference model. Current work is being performed in using a layered approach to secure network design. The layers of the security model correspond to the OSI model layers. This security approach leads to an effective and efficient design which circumvents some of the common security problems.

4. TECHNOLOGY FOR INTERNET SECURITY

Internet threats will continue to be a major issue in the global world as long as information is accessible and transferred across the Internet. Different defense and detection mechanisms were developed to deal with these attacks.

4.1 Cryptographic systems

Cryptography is a useful and widely used tool in security engineering today. It involved the use of codes and ciphers to transform information into unintelligible data.

4.2 Firewall

A firewall is a typical border control mechanism or perimeter defense. The purpose of a firewall is to block traffic from the outside, but it could also be used to block traffic from the inside. A firewall is the front line defense mechanism against intruders. It is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both [2].

5. SECURITY IN DIFFERENT NETWORKS

The businesses today use combinations of firewalls, encryption, and authentication mechanisms to create "intranets" that are connected to the internet but protected from it at the same time.Intranet is a private computer

network that uses internet protocols. Intranets differ from "Extranets" in that the former are generally restricted to employees of the organization while extranets can generally be accessed by customers, suppliers, or other approved parties.

There does not necessarily have to be any access from the organization's internal network to the Internet itself. When such access is provided it is usually through a gateway with a firewall, along with user authentication, encryption of messages, and often makes use of virtual private networks (VPNs).

Although intranets can be set up quickly to share data in a controlled environment, that data is still at risk unless there is tight security. The disadvantage of a closed intranet is that vital data might not get into the hands of those who need it. Intranets have a place within agencies. But for broader data sharing, it might be better to keep the networks open, with these safeguards:

a) Firewalls that detect and report intrusion attemptsSophisticated virus checking at the firewall
b) Enforced rules for employee opening of email attachments
c) Encryption for all connections and data transfers
d) Authentication by synchronized, timed passwords or security certificates

It was mentioned that if the intranet wanted access to the internet, virtual private networks are often used. Intranets that exist across multiple locations generally run over separate leased lines or a newer approach of VPN can be utilized. VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together.

Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee. Figure is a graphical representation of an organization and VPN network.

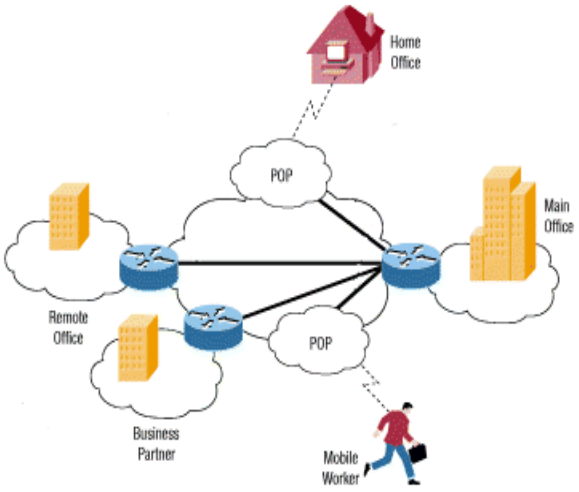

Fig.1: A typical VPN might have a main LAN at the corporate headquarters of a company, other LANs at remote offices or facilities and individual users connecting from out in the field. [3]

6. IMPORTANCE OF COMPUTER NETWORK AND SECURITY

6.1 To protect company assets

One of the primary goals of computer and network security is the protection of company assets. By "assets," I do not mean the hardware and software that constitute the company's computers and networks. The assets are Developing and maintaining effective security measures can provide an organization with a competitive advantage over its competition. Network security is particularly important in the arena of Internet financial services and e-commerce. It can mean the difference between wide acceptance of a service and a mediocre customer response. For example, how many people do you know who would use a bank's Internet banking system if they knew that the system had been successfully hacked in the past? Not many. They would go to the competition for their Internet banking services. comprised of the "information" that is housed on a company's computers and networks. Information is a vital organizational asset. Network and computer security is concerned, above all else, with the protection, integrity, and availability of information. Information can be defined as data that is organized and accessible in a coherent and meaningful manner.

6.2 To Comply With Regulatory Requirements And Fiduciary Responsibilities

Corporate officers of every company have a responsibility to ensure the safety and soundness of the organization. Part of that responsibility includes ensuring the continuing operation of the organization. Accordingly, organizations that rely on computers for their continuing operation must develop policies and procedures that address organizational security requirements. Such policies and procedures are necessary not only to protect company assets but also to protect the organization from liability. For-profit organizations must also protect shareholders' investments and maximize return. In addition, many organizations are subject to governmental regulation, which often stipulates requirements for the safety and security of an organization. For example, most financial institutions are subject to federal regulation. Failure to comply with federal guidelines can result in the seizure of a financial institution by federal regulators. In some cases, corporate officers who have not properly performed their regulatory and fiduciary responsibilities are personally liable for any losses incurred by the financial institution that employs them.

6.3 To keep your job

Finally, to secure one's position within an organization and to ensure future career prospects, it is important to put into place measures that protect organizational assets. Security should be part of every network or systems administrator's job. Failure to perform adequately can result in termination. Termination should not be the automatic result of a security failure, but if, after a thorough postmortem, it is determined that the failure was the result of inadequate policies and procedures or failure to comply with existing procedures, then management needs to step in and make some changes.

One thing to keep in mind is that network security costs money: It costs money to hire, train, and retain personnel; to buy hardware and software to secure an organization's networks; and to pay for the increased overhead and degraded network and system performance that results from firewalls, filters, and intrusion detection systems (IDSs). As a result, network security is not cheap. However, it is probably cheaper

than the costs associated with having an organization's network compromised.[6]

7. CURRENT DEVELOPMENTS IN NETWORK SECURITY

The network security field is continuing down the same route. The same methodologies are being used with the addition of biometric identification. Biometrics provides a better method of authentication than passwords. This might greatly reduce the unauthorized access of secure systems. New technology such as the smart card is surfacing in research on network security. The software aspect of network security is very dynamic. Constantly new firewalls and encryption schemes are being implemented.

The research being performed assists in understanding current development and projecting the future developments of the field.

7.1 Hardware Developments

Hardware developments are not developing rapidly. Biometric systems and smart cards are the only new hardware technologies that are widely impacting security.

The most obvious use of biometrics for network security is for secure workstation logons for a workstation connected to a network. Each workstation requires some software support for biometric identification of the user as well as, depending on the biometric being used, some hardware device. The cost of hardware devices is one thing that may lead to the widespread use of voice biometric security identification, especially among companies and organizations on a low budget. Hardware device such as computer mice with built in thumbprint readers would be the next step up. These devices would be more expensive to implement on several computers, as each machine would require its own hardware device. A biometric mouse, with the software to support it, is available from around $120 in the U.S. The advantage of voice recognition software is that it can be centralized, thus reducing the cost of implementation per machine. At top of the range a centralized voice biometric package can cost up to

$50,000 but may be able to manage the secure login of up to 5000 machines.

The main use of Biometric network security will be to replace the current password system. Maintaining password security can be a major task for even a small organization. Passwords have to be changed every few months and people forget their password or lock themselves out of the system by incorrectly entering their password repeatedly. Very often people write their password down and keep it near their computer. This is of course completely undermines any effort at network security. Biometrics can replace this security identification method. The use of biometric identification stops this problem and while it may be expensive to set up at first, these devices save on administration and user assistance costs.

Smart cards are usually a credit-card-sized digital electronic media. The card itself is designed to store encryption keys and other information used in authentication and other identification processes. The main idea behind smart cards is to provide undeniable proof of a user's identity. Smart cards can be used for everything from logging in to the network to providing secure Web communications and secure e-mail transactions.

It may seem that smart cards are nothing more than a repository for storing passwords. Obviously, someone can easily steal a smart card from someone else. Fortunately, there are safety features built into smart cards to prevent someone from using a stolen card. Smart cards require anyone who is using them to enter a personal identification number (PIN) before they'll be granted any level of access into the system. The PIN is similar to the PIN used by ATM machines.

When a user inserts the smart card into the card reader, the smart card prompts the user for a PIN. This PIN was assigned to the user by the administrator at the time the administrator issued the card to the user. Because the PIN is short and purely numeric, the user should have no trouble remembering it and therefore would be unlikely to write the PIN down.

But the interesting thing is what happens when the user inputs the PIN. The PIN is verified from inside the smart card. Because the PIN is never transmitted across the network, there's absolutely no danger of it being intercepted. The main benefit, though, is that the PIN is useless without the smart card, and the smart card is useless without the PIN.

There are other security issues of the smart card. The smart card is cost-effective but not as secure as the biometric identification devices.

7.2 Software Developments

The software aspect of network security is very vast. It includes firewalls, antivirus, vpn, intrusion detection, and much more. The research development of all security software is not feasible to study at this point. The goal is to obtain a view of where the security software is heading based on emphasis being placed now.

The improvement of the standard security software still remains the same. When new viruses emerge, the antivirus is updated to be able to guard against those threats. This process is the same for firewalls and intrusion detection systems. Many research papers that have been skimmed were based on analyzing attack patterns in order to create smarter security software.

As the security hardware transitions to biometrics, the software also needs to be able to use the information appropriately. Current research is being performed on security software using neural networks. The objective of the research is to use neural networks for the facial recognition software.

Many small and complex devices can be connected to the internet. Most of the current security algorithms are computational intensive and require substantial processing power. This power, however, is not available in small devices like sensors. Therefore, there is a need for designing light-weight security algorithms. Research in this area is currently being performed.

8. FUTURE TRENDS IN SECURITY

What is going to drive the Internet security is the set of applications more than anything else. The future will possibly be that the security is similar to an immune system. The immune system fights off attacks and builds itself to fight tougher enemies.

Similarly, the network security will be able to function as an immune system.

The trend towards biometrics could have taken place a while ago, but it seems that it isn't being actively pursued. Many security developments that are taking place are within the same set of security technology that is being used today with some minor adjustments.

9. CONCLUSION

Network security is an important field that is increasingly gaining attention as the internet expands. The security threats and internet protocol were analyzed to determine the necessary security technology. The security technology is mostly software based, but many common hardware devices are used. The current development in network security is not very impressive.

Originally it was assumed that with the importance of the network security field, new approaches to security, both hardware and software, would be actively researched. It was a surprise to see most of the development taking place in the same technologies being currently used. The embedded security of the new internet protocol IPv6 may provide many benefits to internet users. Although some security issues were observed, the IPv6 internet protocol seems to evade many of the current popular attacks. Combined use of IPv6 and security tools such as firewalls, intrusion detection, and authentication mechanisms will prove effective in guarding intellectual property for the near future. The network security field may have to evolve more rapidly to deal with the threats further in the future.

10. REFERENCES

[1] Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously," Computer, vol.31, no.9, pp.24-28, Sep 1998

[2] Adeyinka, O., "Internet Attack Methods and Internet Security Technology," Modeling & Simulation, 2008. AICMS08. Second Asia International Conference on, vol., no., pp.77-82, 13-15 May 2008

[3] Tyson, J., "How Virtual private networks work,"http://www.howstuffworks.com/vpn.htm .

[4] Al-Salqan, Y.Y., "Future trends in Internet security," Distributed Computing Systems, 1997., Proceedings of the Sixth IEEE Computer Society Workshop on Future Trends of , vol., no., pp.216-217, 29-31 Oct 1997

[5] Curtin, M. "Introduction to Network Security," http://www.interhack.net/pubs/network-security.

[6] Fundamentals of network security / John E. Canavan, p. cm.—(Artech House telecommunications library) Includes bibliographical references and index.ISBN 1-58053-176-8 (alk. paper)