The Importance, Future and implementation of Network Security

Hassan Khan Mukhlis[1*] and Khan Mohammad Wafa[2]

[1]Lecturer, Department of Information Technology, Computer Science Faculty, Bost University, Email: hkmukhlis@gmail.com

[2]Lecturer and Dean of Faculty, Department of Information Technology, Computer Science Faculty, Bost University

Abstract

The world is becoming more interconnected with the advent of the Internet and new networking technology. it has become more important that organizations and individuals take the necessary steps to protect their networks. Through the history of security, it has been able to gain a better understanding of how security technology has evolved. One of the most important factors that businesses can consider when it comes to protecting their networks is the architecture of the internet. This can be done through the use of various security measures such as firewalls and encryption. The field of network security is in an evolutionary stage and has a wide range of study. This section covers a brief history of the internet and its evolution, as well as the current state of security technology. In order to gain a deeper understanding of how security has evolved, it is essential to have a good knowledge of the various vulnerabilities of the internet and security technology.

Keywords: Network security, history, importance, future and implementation

Introduction

Due to the rise of the internet and the increasing number of people using networking technology, the world has become more interconnected (Dowd & Mchenry, 1998). There is a huge amount of information that can be collected and stored on various networking infrastructures. Network security is becoming an important issue due to the availability of intellectual property. There are two types of networks: a data network and a synchronous network. The former is referred to as a data network while the latter is a synchronous network. A data network is usually composed of routers, which are computer-based devices. Information can be obtained by programs such as "Trojan horses." On the other hand, a synchronous network is composed of switches, which do not store data. This type of network is very secure as it does not allow attackers to access it. The extensive topic of network security is inspected by researching the following:

1. History of security in networks

2. Internet architecture and vulnerable security aspects of the Internet

3. Types of internet attacks and security methods

4. Security for networks with internet access

5. Current development in network security hardware and software

Based on this topic, the future of network security is predicted. New inclination that are emerging will also be considered to understand where network security is heading.

Network Security:

System and network technology is a crucial technology for a vast variety of applications. Security is very important for networks and applications. Although, network security is an important requirement in emerging networks, there is a remarkable lack of security techniques that can be easily implemented.

There exists a communication breaches between the developers of security technology and developers of networks. Network design is a well-developed procedure that is based on the Open Systems Interface (OSI) model. The OSI model has various advantages when designing networks. It offers flexibility, modularity ease-of-use, and standardization of protocols. The protocols of different layers can be simply aggregated 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, and 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 (Dowd & Mchenry, 1998).

Access – authorized users are provided the means to communicate to and from a particular network

Confidentiality – Information in the network remains private

Authentication – Ensure the users of the network are who they say they are

Integrity – Ensure the message has not been modified in transit

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 (Dowd & Mchenry, 1998). 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.

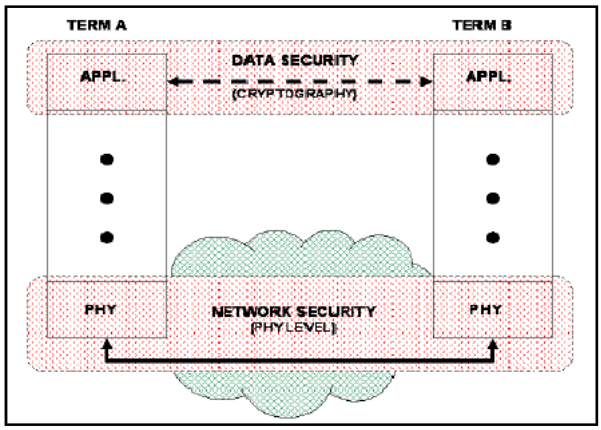
Typical security currently exists on the computers connected to the network. Security protocols sometimes usually appear as part of a single layer of the OSI network reference model. Current work is being performed in using a layered approach to secure network design. The layers of the security model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

Discriminating the Network Security and Data Security

Data security is the aspect of security that allows a client’s data to be transformed into unintelligible data for transmission. Even if this unintelligible data is intercepted, a key is needed to decode the message. This method of security is effective to a certain degree. Strong cryptography in the past can be easily broken today. Cryptographic methods have to continue to advance due to the advancement of the hackers as well.

When transferring cipher text over a network, it is helpful to have a secure network. This will allow for the cipher text to be protected, so that it is less likely for many people to even attempt to break the code. A secure network will also prevent someone from inserting unauthorized messages into the network. Therefore, hard ciphers are needed as well as attack-hard networks (Kartalopoulos,2008).

Figure 1: Based on the OSI model, data security and network security have a different security function



Source: Security Overview

The relationship of network security and data security to the OSI model is shown in Figure.

1. It can be seen that the cryptography occurs at the application layer; therefore, the application writers are aware of its existence. The user can possibly choose different methods of data security. Network security is mostly contained within the physical layer. Layers above the physical layer are also used to accomplish the network security required (Kartalopoulos, 2008).
Authentication is performed on a layer above the physical layer. Network security in the physical layer requires failure detection, attack detection mechanisms, and intelligent countermeasure strategies (Kartalopoulos, 2008).

Figure 1: Based on the OSI model, data security and network security have a different security function (Security Overview).

Network Security History:

Recent interest in security was fueled by the crime committed by Kevin Mitnick. Kevin Mitnick committed the largest computer-related crime in

U.S. history. The losses were eighty million dollars in U.S. intellectual property and source code from a variety of companies (Molva, 1999). Since then, information security came into the spotlight.

Public networks are being relied upon to deliver financial and personal information. Due to the evolution of information that is made available through the internet, information security is also required to evolve. Due to Kevin Mitnick's offense, companies are emphasizing security for the intellectual property. Internet has been a driving force for data security improvement.

Internet protocols in the past were not developed to secure themselves. Within the TCP/IP communication stack, security protocols are not implemented. This leaves the internet open to attacks. Modern developments in the internet architecture have made communication more secure.

Brief History of Internet:

The Start of the interne takes place in 1969 when Advanced Research Projects Agency Network (ARPANET) is commissioned by the department of defense (DOD) for research in networking.

The ARPANET is a success from the very beginning. Although originally designed to allow scientists to share data and access remote computers, e-mail quickly becomes the most popular application. The ARPANET becomes a high-speed digital post office as people use it to collaborate on research projects and discuss topics of various interests. The Inter Networking Working Group becomes the first of several standards-setting entities to govern the growing network (Marin, 2005). Vinton Cerf is elected the first chairman of the INWG, and later becomes known as a "Father of the Internet." .

In the 1980s, Bob Kahn and Vinton Cerf are key members of a team that create TCP/IP, the common language of all Internet computers. For the first time the loose collection of networks which made up the ARPANET is seen as an "Internet", and the Internet as we know it today is born. The mid-80s marks a boom in the personal computer and super-minicomputer industries. The combination of inexpensive desktop machines and powerful, network-ready servers allows many companies to join the Internet for the first time. Corporations begin to use the Internet to communicate with each other and with their customers.

In the 1990s, the internet began to become available to the public. The World Wide Web was born. Netscape and Microsoft were both competing on developing a browser for the internet. Internet continues to grow and surfing the internet has become equivalent to TV viewing for many users.

Security Timeline:

Different key events contributed to the birth and evolution of computer and network security. The timeline can be started as far back as the 1930s.

Polish cryptographers created an enigma machine in 1918 that converted plain messages to encrypted text. In 1930, Alan Turing, a brilliant mathematician broke the code for the Enigma. Securing communications was essential in World War II.

In the 1960s, the term "hacker" is coined by a couple of Massachusetts Institute of Technology (MIT) students. The Department of Defense began the ARPANET, which gains popularity as a conduit for the electronic exchange of data and information. This paves the way for the creation of the carrier network known today as the Internet. During the 1970s, the Telnet protocol was developed. This opened the door for public use of data networks that were originally restricted to government contractors and academic researchers (Sotillo, 2006).

During the 1980s, the hackers and crimes relating to computers were beginning to emerge. The 414 gang are raided by authorities after a nine-day cracking spree where they break into top-secret systems. The Computer Fraud and Abuse Act of 1986 was created because of Ian Murphy's crime of stealing information from military computers. A graduate student, Robert Morris, was convicted for unleashing the Morris Worm to over 6,000

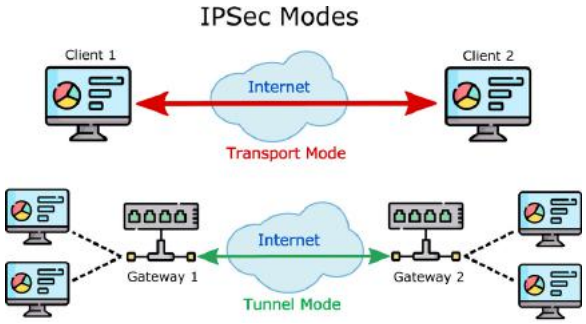
vulnerable computers connected to the Internet. Based on concerns that the Morris Worm ordeal could be replicated, the Computer Emergency Response Team (CERT) was created to alert computer users of network security issues.

In the 1990s, Internet became public and the security concerns increased tremendously. Approximately 950 million people use the internet today worldwide. On any day, there are approximately 225 major incidences of a security

Breach (Andress, 2005). These security breaches could also result in monetary losses of a large degree. Investment in proper security should be a priority for large organizations as well as common users.

Internet architecture and susceptible security aspects

Fear of security breaches on the Internet is causing organizations to use protected private networks or intranets (Molva,1999). The Internet Engineering Task Force (IETF) has introduced security mechanisms at various layers of the Internet Protocol Suite. These security mechanisms allow for the logical protection of data units that are transferred across the network.



IPsec contains a gateway and tunnel

Figure 2: IPsec contains a gateway and a tunnel in order to secure communications (Improving Security)

The current version and new version of the Internet Protocol are analyzed to determine the security implications. Although security may exist within the protocol, certain attacks cannot be guarded against. These attacks are analyzed to determine other security mechanisms that may be necessary.

The security architecture of the internet protocol, known as IP Security, is a standardization of internet security. IP security, IPsec, covers the new generation of IP (IPv6) as well as the current version (IPv4). Although new techniques, such as IPsec, have been developed to overcome internet's best-known deficiencies, they seem to be insufficient (Sotillo, 2006). Figure 2 shows a visual representation of how IPsec is implemented to provide secure communications.

IPSec is a point-to-point protocol, one side encrypts, the other decrypts and both sides share key or keys. IPSec can be used in two modes, namely transport mode and tunnel modes.

IPv4 and IPv6 Architectures:

IPv4 was design in 1980 to replace the NCP protocol on the ARPANET. The IPv4 displayed many limitations after two decades (Andress, 2005). The IPv6 protocol was designed with IPv4's shortcomings in mind. IPv6 is not a superset of the IPv4 protocol; instead it is a new design.

The internet protocol's design is so vast and cannot be covered fully. The main parts of the architecture relating to security are discussed in detail.

IPv4 Architecture:

This protocol contains a couple side which caused problems with its use. These problems do not all relate to security. They are mentioned to gain a comprehensive understanding of the internet protocol and its shortcomings. The causes of problems with the protocol are:

- Address Space
- Routing
- Configuration
- Security
- Quality of Service

The IPv4 architecture has an address that is 32 bits wide (Andress, 2005). This limits the maximum number of computers that can be connected to the internet. The 32 bit address provides for a maximum of two billions computers to be connected to the internet. The problem of exceeding that number was not foreseen when the protocol was created. The small address space of the IPv4 facilitates malicious code distribution (Sotillo, 2006).

Routing is a problem for this protocol because the routing tables are constantly increasing in size. The maximum theoretical size of the global routing tables was 2.1 million entries (Andress, 2005). Methods have been adopted to reduce the number of entries in the routing table. This is helpful for a short period of time, but drastic change needs to be made to address this problem.

The TCP/IP-based networking of IPv4 requires that the user supplies some data in order to configure a network. Some of the information required is the IP address, routing gateway address, subnet mask, and DNS server. The simplicity of configuring the network is not evident in the IPv4 protocol. The user can request appropriate network configuration from a central server (Andress, 2005). This eases configuration hassles for the user but not the network's administrators.

The lack of embedded security within the IPv4 protocol has led to the many attacks seen today. Mechanisms to secure IPv4 do exist, but there are no requirements for their use (Andress, 2005). IPsec is a specific mechanism used to secure the protocol. IPsec secures the packet payloads by means of cryptography. IPsec provides the services of confidentiality, integrity, and authentication (Andress, 2005). This form of protection does not account for the skilled hacker who may be able to break the encryption method and obtain the key.

When internet was created, the quality of service (QoS) was standardized according to the information that was transferred across the network. The original transfer of information was mostly text-based. As the internet expanded and technology evolved, other forms of communication began to be transmitted across the internet. The quality of service for streaming videos and music are much different than the standard text. The protocol does not have the functionality of dynamic QoS that changes based on the type of data being communicated (Andress, 2005).

IPv6 Architecture:

When IPv6 was being developed, emphasis was placed on aspects of the IPv4 protocol that needed to be improved. The development efforts were placed in the following areas:

1. Routing and addressing
2. Multi-protocol architecture
3. Security architecture
4. Traffic control

The IPv6 protocol's address space was extended by supporting 128 bit addresses. With 128 bit addresses, the protocol can support up to3.4 * (10) ^38 machines. The address bits are used less efficiently in this protocol because it simplifies addressing configuration.

The IPv6 routing system is more efficient and enables smaller global routing tables. The host configuration is also simplified. Hosts can automatically configure themselves. This new design allows ease of configuration for the user as well as network administrator.

The security architecture of the IPv6 protocol is of great interest. IPsec is embedded within the IPv6 protocol. IPsec functionality is the same for IPv4 and IPv6. The only difference is that IPv6 can utilize the security mechanism along the entire route (Andress, 2005).

The quality of service problem is handled with IPv6. The internet protocol allows for special handling of certain packets with a higher quality of service.

From a high-level view, the major benefits of IPv6 are its scalability and increased security. IPv6 also offers other interesting features that are beyond the scope of this paper.

It must be emphasized that after researching IPv6 and its security features, it is not necessarily more secure than IPv4. The approach to security is only slightly better, not a radical improvement.

Common attack methods and the security technology will be briefly discussed. Not all of the methods in the table above are discussed. The current technology for dealing with attacks is understood in order to comprehend the current research developments in security hardware and software (Andress, 2005).

The Current Attacks through Internet Protocol IPv4

There are four main computer security attributes. They were mentioned before in a slightly different form, but are restated for convenience and emphasis. These security attributes are confidentiality, integrity, privacy, and availability.

Confidentiality and integrity still hold to the same definition. Availability means the computer assets can be accessed by authorized people. Privacy is the right to protect personal secrets (Adeyinka, 2008). Various attack methods relate to these four security attributes.

Internet Common Attack Methods:

Common internet attacks methods are broken down into categories. Some attacks gain system knowledge or personal information, such as eavesdropping and phishing. Attacks can also interfere with the system's intended function, such as viruses, worms and trojans. The other form of attack is when the system's resources are consumes uselessly, these can be caused by denial of service (DoS) attack. Other forms of network intrusions also exist, such as land attacks, smurf attacks, and teardrop attacks. These attacks are not as well-known as DoS attacks, but they are used in some form or another even if they aren't mentioned by name (Landwehr & Goldschlag, 1997).

IP Spoofing Attacks:

Spoofing means to have the address of the computer mirror the address of a trusted computer in order to gain access to other computers. The identity of the intruder is hidden by different means making detection and prevention difficult. With the current IP protocol technology, IP- spoofed packets cannot be eliminated (Adeyinka, 2008).

Denial of Service:

Denial of Service is an attack when the system receiving too many requests cannot return communication with the requestors. The system then consumes resources waiting for the handshake to complete. Eventually, the system cannot respond to any more requests rendering it without service (Marin, 2005).

Worms:

A worm is similar to a virus because they both are self-replicating, but the worm does not require a file to allow it to propagate. There are two main types of worms, mass-mailing worms and network-aware worms. Mass mailing worms use email as a means to infect other computers. Network-aware worms are a major problem for the Internet. A network-aware worm selects a target and once the worm accesses the target host, it can infect it by means of a Trojan or otherwise (Adeyinka, 2008).

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 future (Ohta & Chikaraishi 1993).

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 (Tyson, 2018).

Trojans:

Trojans appear to be benign programs to the user, but will actually have some malicious purpose. Trojans usually carry some payload such as a virus (Adeyinka, 2008).

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 beused 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 (Adeyinka, 2008).

Different networks security:

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:

- Firewalls that detect and report intrusion attempts
- Sophisticated virus checking at the firewall
- Enforced rules for employee opening of e-mail attachments
- Encryption for all connections and data transfers
- 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 (Landwehr & Goldschlag, 1997).

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 (Salqan, 1997).

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 (Serpanos & Voyiatzis, 2002).

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.

References

Dowd, P.W., & McHenry, J.T. (1998). Network security: it's time to take it seriously. Computer, 31(9), 24- 28.

Kartalopoulos, S. V. (2008). Differentiating Data Security and Network Security. Communications, 2008. ICC '08. IEEE International Conference, 1469-1473.

"Security Overview," www.redhat.com/docs/manuals/enterprise/RHEL-4- Manual/security-guide/ch-sgs-ov.html.

Molva, R (1999). Internet Security Architecture. Computer Networks & ISDN Systems Journal, 31, 787-804.

Sotillo, S. (2006). Security Issues. East Carolina University.

"www.infosecwriters.com/text_resources/pdf/IPv6_SSot illo.pdf.

Andress J. (2005). IPv6: the next internet protocol. www.usenix.com/publications/login/2005-04/pdfs/andress0504.pdf.

Adeyinka, O. (2008). Internet Attack Methods and Internet Security Technology, Modeling & Simulation. AICMS 08. Second Asia International Conference, 13 (15), 77-82.

Marin, G.A. (2005). Network security basics. Security & Privacy, IEEE , 3(6), 68-72.

Serpanos, D.N., & Voyiatzis, A.G. (2002). Secure network design: A layered approach," Autonomous Decentralized System. The 2nd International Workshop, 6(7), 95-100.

Landwehr, C.E., & Goldschlag, D.M. (1997). Security issues in networks with Internet access. Proceedings of the IEEE, 85(12), 2034-2051.

Ohta, T., & Chikaraishi, T. (1993). Network security model, "Networks. Proceedings of IEEE Singapore International Conference, 2 (6), 507-511.

Tyson, J. (2018). How Virtual private networks work. http://www.howstuffworks.com/vpn.htm Oct 2018 .

Al-Salqan, Y.Y. (1997). Future trends in Internet security. Distributed Computing Systems Proceedings of the Sixth IEEE Computer Society Workshop on Future Trends, 29(31), 216-217.

د شبکي امنيت اهميت، راتلونکي او پلي کول

حسن خان مخلص[۱*]، خان محمد وفا[۲]

[۱،۲]د معلوماتي ټکنالوژۍ څانګه، کمپيوټر ساينس پوهنځی، بُست پوهنتون

د مسؤل ايميل ادرس: hkmukhlis@gmail.com

لنډيز

د شبکي امنيت د کمپيوټر ساينس يوه څانګه ده، چې پکې د کمپيوټر د شبکي او د شبکي د وسايلو خوندي کول شامل دي ترڅو د غير قانوني لاسرسي، معلوماتود غلا ، د شبکي څخه د ناوړه ګټه اخيستني مخه ونيسي. يا په بل عبارت د شبکي امنيت د غيرقانوني لاسرسي، ناوړه ګټي اخيستني، يا غلا څخه د شبکي د زيربناوو ساتنه ده. په دې کي د وسيلو، غوښتنليکونو، کارونکو او غوښتنليکونو لپاره خوندي زيربنا رامينځته کول شامل دي ترڅو په خوندي ډول کار وکړي. د شبکي امنيت بله دنده د (DoS=denial of service) بريدونو مخنيوی دی او د مشروع/قانوني شبکي کارووونکو لپاره دوامداره خدمات وړاندي کول. د شبکي په امنيت راوستلو کي فعال دفاعي ميتودونه او ميکانيزمونه شامل دي ترڅو ډاټا، شبکه او د شبکي وسايل د بهرنيو او داخلي ګواښونو څخه خوندي کړي. لوړ سوداګريز سازمانونه هر کال په ملياردونو ډالر مصرفوي ترڅو د دوی کمپيوټري شبکي خوندي کړي او د دوی سوداګريز معلومات خوندي وساتي. د ټولو مهمو څېړنيزو معلوماتو له لاسه ورکولو تصور وکړئ چې شرکت يې په ملیونونو ډالر پانګونه کړې او د کلونو لپاره کار کوي، مور نن ورځ د بانکونو، بيمې، بازارونو، مخابراتو ، بريښنايې توزيع، روغتيا، طبي برخو، اټومي بريښنايې فابريکو، فضائي څېړنو او د لويو پيسو ليږد د کنټرول لپاره دشبکي په کمپيوټرونو تکيه کوو. مور په دې حساسو حالتو کي د شبکي امنيت ته اړتيا لرو.

کليدي کليمې: شبکې امنيت، تاريخچه، اهميت، راتلونکي او پلي کول.