# Analysis of Network Security Threats, Vulnerabilities and Protection Strategy & Implementation of Security Network Monitoring Solution

Shweta Jha, Research Scholar, Department of Computer Science and Engineering, Sandip University, Nashik.
Dr Sajjidullah Khan, Associate Professor, School of Computer Sciences and Engineering, Sandip University, Nashik

## Abstract

*Communication of confidential data over the internet is becoming more frequent every day. Individuals and organizations are sending their confidential data electronically. It is also common that hackers target these networks. In current times, protecting the data, software and hardware from viruses is, now more than ever, a need and not just a concern. What you need to know about networks these days? How security is implemented to ensure a network? How is security managed? In this paper we will try to address the above questions and give an idea of where we are now standing with the security of the network. We have entered an era in which computers are not available in all walks of life. Among them, many important documents and materials will be stored in the form of electronic files in the computer. However, computers are not absolutely safe, and cases of information theft occur from time to time. Most people usually keep information confidential in the form of encryption. How to avoid the problem of computer information security. Computer network security involves all aspects. To solve these problems, there are many levels of technology, such as cryptography technology, network security technology and so on. Our country has also done a lot of research on the security protection of computer network technology, and these research results have also achieved certain results in the actual construction of computer network. In order to ensure the normal operation of computer networks, ensure information security and prevent information leakage and theft, a special protection system has been established to ensure the security of computer network information by setting up computer detection, security assessment and other links. However, with the rapid development of science and technology, the updating of electronic products is faster and faster, and the challenge of Wechat for network security information is more severe. How to protect computer network information security needs to be solved urgently, this paper discusses this.*

**Keywords:** *Computer network information; Information security; Network and protocols ; Security Countermeasures Techniques; Security protection*

The network layer protocols are the major part in a communication network. This paper includes the description of the role of network layer protocols in a communication model; it also explains the functional parameters of these protocols in different level of data communication. These parameters are in the form of protocol header fields. The header field of these protocols and analyze that how an attacker can use or change these protocol header fields to accomplish his/her malicious goals. The in-depth study of the structure of OSI layer protocols & TCP/IP layer protocols can carry out this objective.

The storage of massive data also brings certain challenges to computer technology. Many information security technologies and tools need to be solved urgently. Traditional information technology has been unable to meet the storage needs of massive data. At present, the most prominent and serious problems of computer information security in the era of big data are data theft, data improper addition and deletion and tampering, personal privacy disclosure and so on.

The protection of computer network information security also needs a certain system to protect, but also users themselves take reasonable protective measures and so on. The process of computer information security protection needs all kinds of strategies to be used together and deployed reasonably. Only in this way can we minimize the probability of infringement of information security and get security assurance.

## 1. Computer Network Information Security

### 1.1 **Virus attack Problem**

Many users do not have a good sense of safe operation in the process of using computer networks. For example, they can easily guess or crack account passwords by others, and then make their accounts stolen by setting up some important accounts in a simple and random way. In addition, other computer users' attacking behavior will also lead to computer network information security problems. This kind of attacking behavior includes not only other people's use of substantive network attacking behavior to destroy the integrity and security of computer network information, but also the user's own initiative to be attacked. For the sake of this, active attack means that there are some viruses in many computer networks in our country at present. Network viruses have strong latent and infectious characteristics. When users click on network links with viruses or use computer networks with viruses to edit relevant programs, they will rush out. Large viruses invade or cause viruses to hide in the execution program, which not only reduces the efficiency of the system, but also duplicates the relevant information in the computer system or deletes the important files in the system, thus bringing certain losses to the computer network users.

### 1.2 Mail Attack Problem

E-mail has the characteristics of easy dissemination and open account. With this feature, many lawless elements can send their own e-mail with various computer viruses to others by force through other people's e-mail account, which can directly destroy the information security of the computer system of the emailed users. Information security that borrows e-mail accounts has a negative impact.

### 1.3 Open Computer Network and free download of software

The computer network has the characteristics of openness in the process of operation. It is precisely because of its openness that the computer network is vulnerable to some extent. In the computer network, there are not too many restrictions on the dissemination, transmission and sharing of information. The computer network is also in an open and unprotected state, which makes it easy for some illegal elements to take advantage of the opennessof the network to commit illegal acts [2].

In order to popularize computer network technology, the modern network application market has launched a large number of life apps, game software and so on. The functions of these software often need to be downloaded before they can experience. In order to satisfy their curiosity, many users will download all kinds of apps at will, such as many users will download security at will. Unknown applications or pornographic video websites can destroy the security of their mobile phones or computer network systems. Although most computer network systems are equipped with tools and software to improve the quality of service and system management, there are still many illegal elements who can use these tools to collect illegal information and attack user information.

### 1.4 Hacker Intrusion

Hacking is one of the important factors of computer network security problems. Hacker intrusion is generally an artificial security problem. Hackers invade users' computers by means of relevant means and technologies, and then attack and destroy information and data in computers, thus causing data damage and omission. This kind of man-made data destruction, attacks and so on are likely to cause the paralysis of the computer network system, and then cause tremendous losses and impact on people's production, work and life [3].

### 1.5 Security Velnerabilities

Vulnerabilities defined as the weakness in any network that can be exploited by a threat. Recently almost in all areas network technologies have been applied, such as banking, tax, E-Commerce. These applications are consist of different network devices and computers and it is very important to protect these applications and devices from malicious hackers so that chances to exploit the vulnerabilities may reduce. There are different hardware and software tools available in the market to protect against these attacks, such as firewalls, Intrusion Detection Systems (IDS), antivirus software and vulnerability scanning software. However the usage of these hardware and software cannot guarantee the network against attacks. “The only truly secure system is that which is powered off – and even then I have my doubts", a quotation by a leading security expert [21]. According to the statistic from the reports of Computer Emergency Response Team/Coordination Center (CERT/CC), the number of exploited vulnerabilities increases dramatically [22], as shown in figure:

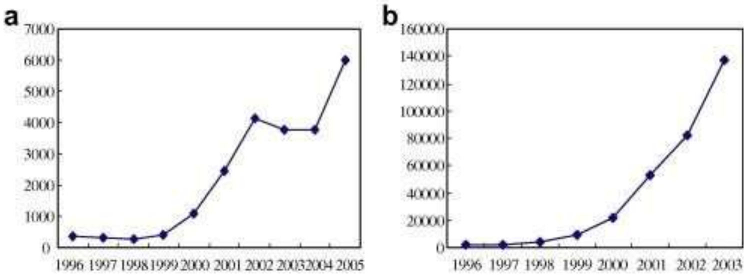
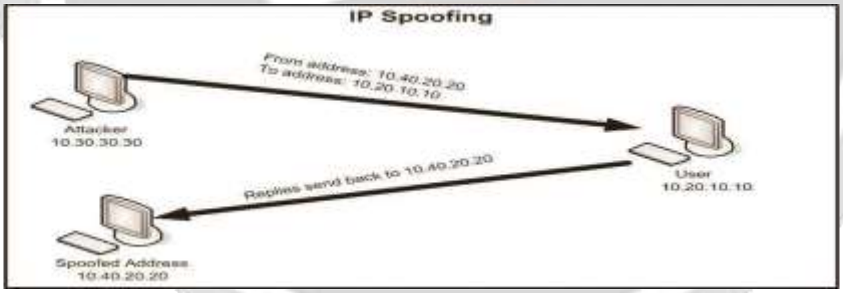


**Fig.1.1**. (A) The number of found vulnerabilities (B) the number of reported events

## 1.6 Disruption of Network Function

Basic function of any network is to share the resources and information. A disruption occurs when network did not provide the needed functionality on time. Interruption in network can affect on one type of functionality or on different functionalities. Several reasons may lay behind the disruption on network

- Network has no ability to detect the traffic, some time network goes down because ofthe useless traffic.
- Network with single point of failure.Hardware failure.
- Improper maintenance of network equipment.
- Unauthorized access to network components may cause the changing in the configuration of the components which also disrupt the network function



## 2 Computer Network Security Protection Strategy

### 2.1 Strengthen account management

There are many kinds of account types in computer network. When security problems or deviations occur in network system, illegal elements often steal user's account information and password. Therefore, network users are required to increase the close complexity when setting account password, such as combining numbers, letters or other symbols to account password. Setting up, rather than using simple numbers or letters as passwords, can make its network close and not easy to be guessed or stolen by others, and try not to use the same password to set different accounts, which will lead to its multiple account passwords are easy to steal. In addition, in the process of network account registration and password login, the account information also needs to be strictly and carefully protected [4].

### 2.2 Security Policies

A strong security policy performs an efficient role in a network. If policy develops after analyzing the network and behavior of its components then it results a much secure and smooth network.

### **2.3** Authority of resources

The authorization of systems or network resources has an important role in security countermeasure. After a fair survey of network we may assign a proper level of authority for accessing the system resources. The policies of antivirus or the access control list of router or firewall can define an authority for accessing network resources in a proper manner.

### **2.4** Detect malicious activities

The presence of intrusion detection system has an important role in security countermeasure. The study and analyzing the log files against malicious activities in network can save a system. It provides a futuristic safety approach against many other malicious aims.

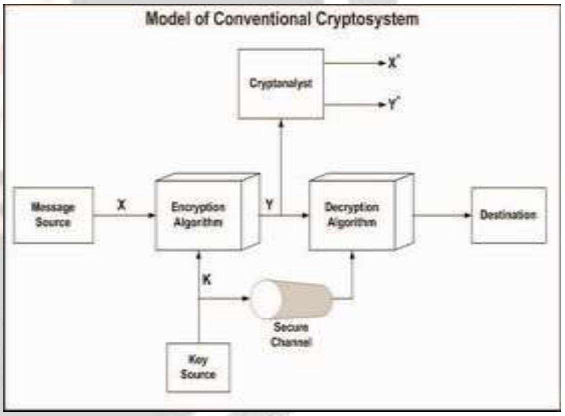
### **2.5** Security Countermeasures Tools - Cryptography

Cryptography is used to protect data from interception. We have to be sure that our confidential data cannot be understood by an unintended user. Cryptography is the study of methods to send data in unrecognizable form so that only the intended user can recognize and read the message. There are two basic cryptographic terms, *Plain Text,* the text or data which we want to encrypt, and *Cipher Text,* the encrypted form of plain text.

### **2.6 Conventional or Symmetric Encryption**

It was the only encryption scheme available before the public-key encryption. One secret key is shared among the sender and the receiver. Whole procedure of conventional encryption consistsof five stages:

1. Plain Text: The original message or data which we want to be encrypted.
2. Encryption Algorithm: Encryption algorithm performs different transformations on thedata.
3. Secret Key: Secret key is the input to the encryption algorithm. Different transformations performed by the encryption algorithms depend on the secret key.
4. Cipher Text: This is the out put of scrambled message.
5. Decryption Algorithm: Reverse of the encryption algorithm, it produces the plain textwith the help of same secret key and the cipher text.



## 3.0 CONCLUSION

The network vulnerabilities and in-depth analysis of differentsecurity attacks and security solutions. Security is not about a specific firewall, product, brand and operating system. Properly configured firewalls, strong passwords that changed on regular basis, antivirusupdate on regular basis etc all these elements used collectively to good security practices. Deficiencies in bad products can defeat with good practice, whereas bad process can be diluted otherwise excellent products. It is better to have no security devices instead of incorrectly configured security devices. As we observed in first scenario of simulation, in which configuring the network parameters on default mode will allow resources even to use by unauthorized users. Similarly in second scenario setting the network on deny everyone will cause to stop working even network administrators. Some time deployment of security can affect the QoS of network as we observed in third scenario that tunnel mode utilizes half of the network bandwidth which decreases QoS and introduces delay factor. The bottom line is that a network cannot 100 percent secure. However we can guarantee better security by analysis our network. This analysis will helpful to find out the vulnerabilities in network. For example before introducing a firewall in network first analyze it that, does it integrate with the network, will it fulfills your future demands, will it reliable, scalable and maintainable, is it possible to upgrade it and compatible with new products and new softwares. This analysis will use as a baseline for designing a better security plan.

**References:**

[1] William Stallings, *Network Security Essentials Applications and Standards*, 2nd ed., New Jersey: Pearson Education, 2003, pp. 6

[2] http://www.brainwavecc.com/TechDocs/Security.html

[3] http://www.queencitynews.com/modules.php?op=modload&name=News&file=article&sid=1666

[4] Network Model, http://www.tcpipguide.com/free/t_TheBenefitsofNetworkingModels.htm

[5] JOHN D. DAY AND HUBERT ZIMMERMANN, "The OS1 Reference Model" *in proc*. THE IEFJ2, VOL. 71, NO. 12, Dec. 1983

*[6]* Gilbert Held, *TCP/IP Professional Reference Guide*

*[7]* Charles M. Kozierok, *The TCP/IP Guide: a comprehensive, illustrated internet protocols reference*

[8] TCP dump, http://www.usenix.org/publications/login/1998-8/tcpdump.html

[9] Mail Transfer Agent, http://en.wikipedia.org/wiki/Message_transfer_agent

[10] "Glossary of Internet Security Terms", http://www.auditmypc.com/glossary-of-internet-security-terms.asp

[11] Yang Junsheng. Application of Virus Protection Technology in Computer Network Security in Big Data Environment [J]. Computer Fan, 2018 (11): 77-78.

[12] Dong Chengwu. Brief discussion on campus information network security protection and management in Higher Vocational Colleges [J]. Information recording materials, 2018, 19(11):141-142.

[13] Chen Liangliang. Analysis of the main hidden dangers and management measures of computer network security [J]. Network security technology and application, 2018 (10): 6 + 64.