iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** III **Month of publication:** March 2022

DOI: https://doi.org/10.22214/ijraset.2022.40821

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

Analysis of the Main Problems in Computer Network Security and Some Suggestions and Measures to Prevent Them

Nuria Mohamed Hider
Elmergib University, Faculty of Science, Computer Department

Abstract: ***With the rapid development and application of the computer network technology, computer network system has brought many unsafe hidden dangers to the user. The computer network security has got more and more attentions of people. Therefore, this paper analyzes the main problems in computer network security and proposes some effective preventive measures. The author hopes these will help the computer network plays better role for people.***
Keywords: Computer Network Security, Computer Virus, Confidentiality, Preventive Measures.

I. INTRODUCTION

Along with the rapid development of computer technology, the computer has penetrated into all walks of life. Especially the internet has become an indispensable part of our daily life [1]. The network plays a more and more important role in our life and study. The connecting forms of computer are various; the terminal distributes uneven; the internet is open to everyone [2]. All these features make the network is vulnerable to hackers, malwares and malicious attack. So it is of great importance to ensure the security, integrity and availability of network information. The research on
it has practical value and necessity [3]. In this paper, the author will introduce the definition of computer network security, the main problems of computer network security and the preventive measures.

A. The Definition of Computer Network Security

Computer network security is a subject involving computer science, network technology, communication technology, encryption technology, information security technology, applied mathematics, number theory, information theory and so on.
According to the definition given by international organization for standardization, computer network security generally refers that by applying relevant management, technique and measures protects the hardware, software and data resources in computer network system from being changed, released and damaged [4-6]. In this way, the computer network system can operate normally. And the network can play its role better.The specific implication of computer network security varies according to different users. Different users have different cognition and demand for the computer network security. For example, from the perspective of ordinary users, it is only needed to protect their privacy or confidential information from being eavesdropped, changed or forged. However, the network provider also has to consider how to deal with the damage of unpredictable natural disasters and
Military strikes as well as how to maintain the recover the network communication when the network occur exception.

II. THE CHARACTERISTICS OF COMPUTER NETWORK ATTACK THE LOSS IS HUGE

For the attack and hack object is the computer, once they succeed, thousands of computers will be in state of paralysis. This will cause huge economic loss for the computer users [7]. For example, in America, the computer crime causes multi-billion-dollar loss every year. In average, the loss caused by one computer crime is hundred times of the general crime. Besides, for several reasons, some computer network attackers always view the government department and state secret department's computers as attack objects. This absolutely will threaten the safety of society and nation and the loss must be huge.

A. The Devices And Methods Are Various And Hidden

The attack devices are various. The network attackers not only can acquire others' confidential information through keeping watch on data online. They also can enter others' computer system by capturing their account and command.Besides, they can break the computer system by some special methods to bypass the elaborate firewall. All these can be done in a short time by a connecting computer, as Fig.1. So, the crime is hidden and traceless.

Fig. 1 The attack devices are various

Besides, almost all the network intrusions carry on by capturing and attack the software to destroy the whole computer system. It is totally different from the physical harm on machinery equipment.

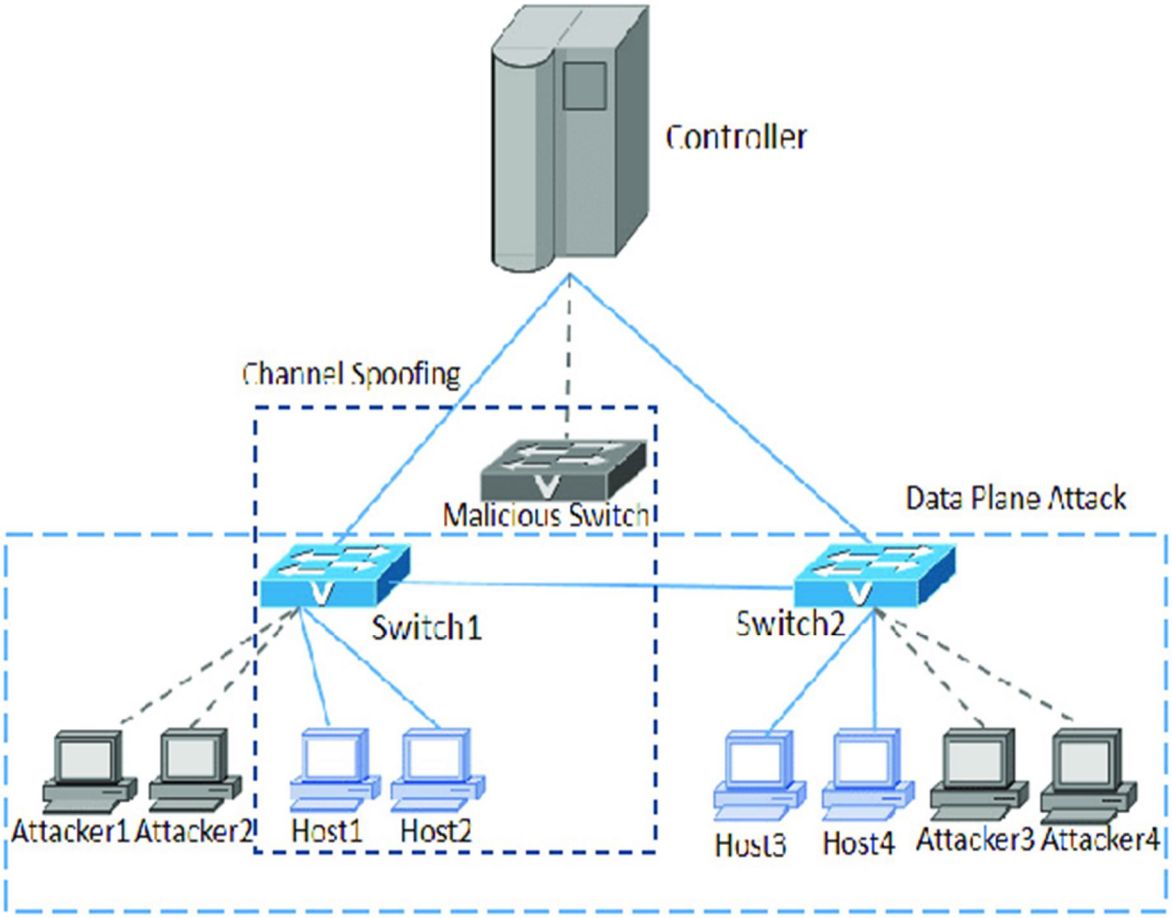


Fig 2 Various-attack-scenarios-implemented-for-web-service-performance-analysis-The-data-plane

A. The Main Problems of Computer Network Security The Computer Virus

The computer virus is defined as the computer command or procedure code inserted in computer programs to destroy the computer function or data. It can self replicate
and impact the use of computer. The computer virus is hidden, latent, ruinous and infectious. It is the most pervasive threaten of computer network security. It is various, harmful and spread-fast, such as the Network Worm, Trojan Virus, Stuxnet and Worm.Win32.Flame.

1) *IP Address Being Embezzled:* The IP address often is embezzled in local area network. Then, the user's computer will appear the being occupied prompt dialog, which leads to the user cannot use the network normally. Generally speaking, the privilege of the being occupied IP address is high.The embezzler generally harasses and attacks the user by hiding his identity. This will cause heavy loss for the user. Besides, the network user's legal interest is seriously infringed. It brings great threaten for the network security.
2) *Network Hacker:* Network hacker refers to the attackers who illegally visit, destroy and attack the user's network through Internet. The harmfulness is decided by the hacker's intention. Some hackers only pry into the user's privacy or secret out of curiosity. This will not destroy the computer system and its harm is little. In contrast, some hackers are out of anger, revenge, and protest to illegally intrude and tamper the user's target page and content in order to humiliate and attack the user, which will force the network paralysis. Some hackers steal the confidential of national defense, military and politics. These absolutely harm the individual and collective interests and endanger the national security. Besides, some hackers illegally embezzle other's bank account to withdraw deposits or carry on blackmail through network. From these we can see that the harm of hacker cannot be imagined.

B. The Preventive Measures to Computer Network Security Firewall

The firewall is an exclusive hardware or a set of software erected on general hardware. In logical, it is a segregator, limiter and analyzer. Its main function is to control the scale of visit and filter information when two or several networks communicate. The application of firewall can ensure the network operate normally. However, it cannot prevent the attack from the LAN interior, which is the biggest limitation of the firewall. With the development of technology, some decoding
methods can break into the firewall. Therefore, better firewall is expected to be developed. The frequently-used firewalls are Skeynet, Rising, 360 Firewall and so on.

1) *The Access Control Technology:* When refers to the access control technology, we must first talk about the 3 basic concepts, that is, subject, object and access authorization. The subject sometimes called user or visitor, includes the user itself, terminal, card machine and so on. The object can be information, document and record. It also can be a processor and storage. The access authorization is the right that the subject can visit the object. It is given for each pair of subject and object. The access control technology restricts the visit of the subject to the object by setting the access authorization. Its main task is to ensure the network resources cannot be illegally used nor visited. It contains many aspects, such as network access control, directory-level control, attribute control and so on.
2) *Anti-virus Technology:* As we all know, the computer virus can be a program or executable code. It can destroy the computer's normal operation. It even can ruin the whole operation system or hard disk. The anti-virus technology can be divided into virus defense technology, virus detection technology, virus removal technology according to the effect of the computer network virus. The network generally applies the Client-Server working mode. It combines the service station and workstation to deal with the virus problem. With the development of computer network technology, the anti-virus technology has updated with each passing day. To build a set of Omni bearing and multi-level anti-virus system and update it timely is of great significance to protect the network from the invasion of virus.

III. CONCLUSIONS

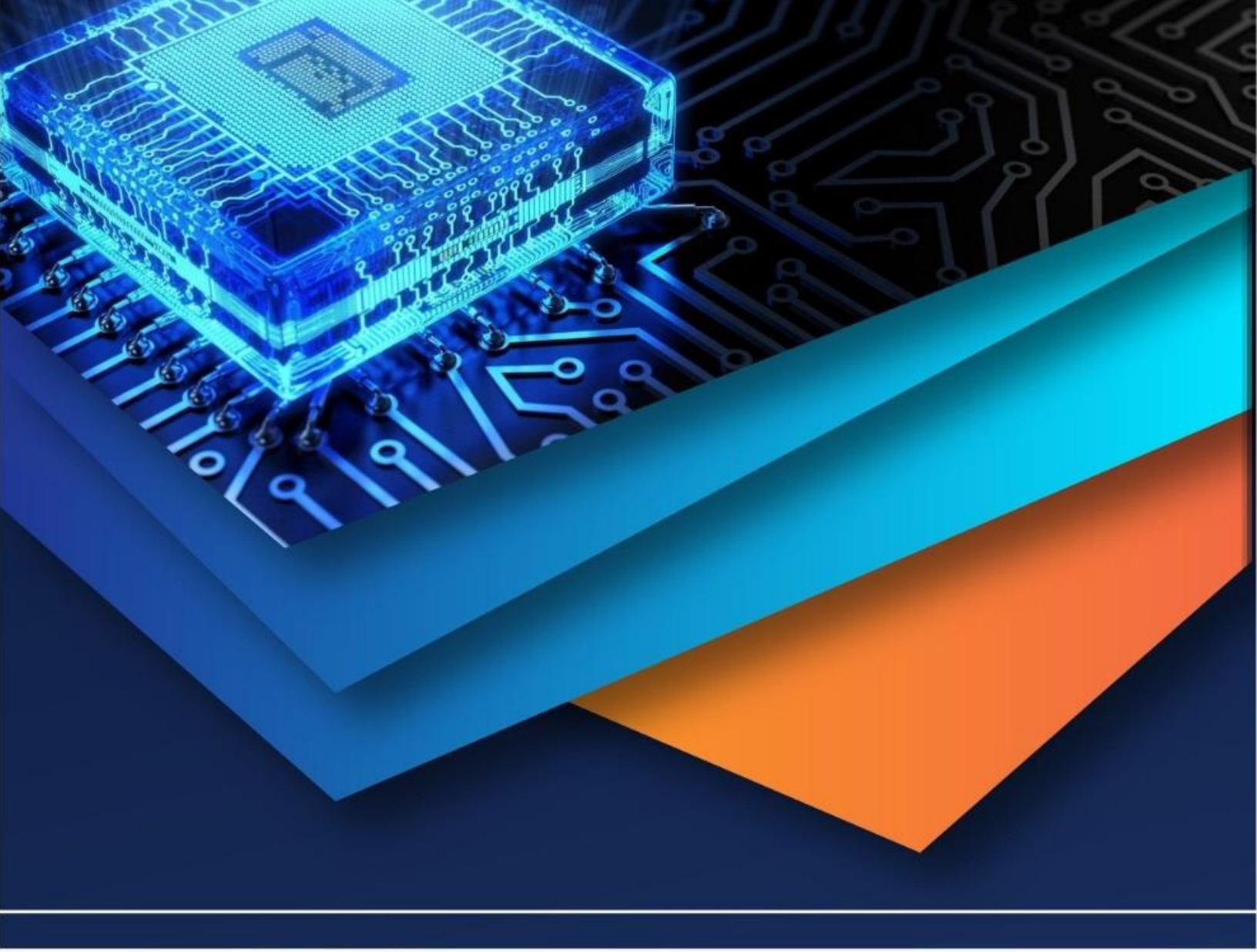
To conclude, the computer network security is a comprehensive and complex system project. With the development of network technology, the network security is facing more severe challenge. So, we must improve our consciousness of network security and service our network system regularly. It is also necessary for us to learn, accumulate and master the computer network security technology in order to protect the computer network system from the attack of hacker. Besides, we should check and kill virus frequently as well as take effective measures to ensure the computer network system operate efficiently.

IV. SUMMARY

Computer network security has become an important issue of network development at this stage, to ensure the network information security. We must depart from security threats through the use of advanced security technology and software technology to effectively monitor potential threats, and timely warning, response, to prevent malicious behavior. And should raise awareness of network security, improve the morality of the whole society, reduce network violations, efforts to establish a secure network environment.

REFERENCES

[1] L. Zhao. Computer network securigy and firewall technology. In: Jouranla of Xinjiang Agricultural Vocational Technical College, 2007(1), 45-47.
[2] L. Du and S.Y. Li. The computer network security and protective measures. In: Computer Knowledge and Technology. 2009(21), 34-37.
[3] X.Q. Ma and Q.L. Wang. Analysis of the computer network security. In: Network Information. 2009(5), 12-15.
[4] L. Zhao and X.F. Qiu. Talk about the computer environment security threat and protection. In: Telecommunications Science. 2010(8), 11-15.
[5] B.Q. Luo and J. Zhang. Analysis of the harm and protection of computer virus. In: Journal of Economic and Technological Cooperation Information. 2012(20), 39-42.
[6] Y.Y. Zhao and Q.J. Pan. The key technology of computer security. In: Telecommunicaitons Science. 2010(9), 21-24.
[7] Y.F. Bao. Analysis of the network firewall technology. In: Modern Science. 2008(2), 11-13.
[8] Q.X. Zhao and Z.Q. Liu, The information age of computer network security, Information security and confidentiality of communications, 2009, pp.12-16.
[9] X.Q. Su and Zh.H. Sheng, Computer network security and firewall technology to explore the development of technology, Science and technology innovation Herald, 2012, pp. 34-37.
[10] D.M. Liu, The computer and network security prevention strategies, Heilongjiang Science and technology information, 2010, pp.43-48.
[11] Y.L. Sun, Security and prevention of computer network technology, Metallurgy Heilongjiang, 2013, pp.65-68.
[12] Zh. Xu , Computer and network security countermeasures, computer knowledge and technology, 2011, pp.7-10.
[13] Q.Y. Huang, Based on Intranet information secure digital signature technology, Computer knowledge and technology, 2014, pp.70-74.
[14] J. Wang, Digital signature technology, Computer Engineering and Science, 2013, pp.67-70.
[15] X.G. Bai, Principle and application of digital signature technology, computer Fujian, 2010, pp.15-19.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY