INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

TECHNICAL DEVELOPMENT IN NETWORK SECURITY MODELS

MISS SNEHAL V. RAUT[1], ANKIT R. MUNE[2], DR. H. R. DESHMUKH[3],

1. M E. Scholar, Department of Computer Science, IBSS COE Amravati, India.
2. Professor, Department of Computer Science, IBSS COE Amravati, India.
3. Professor& HOD, Department of Computer Science, IBSS COE Amravati, India.

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: Computer and network security is both fascinating and complex. Computer and network security is essentially between a perpetrator who tries to find holes and the designer or administrator who tries to close them. The difficulties just enumerated will be encountered to enormous ways as I examine the various security threats and mechanisms through this paper. With the development of computer network technology, computer network security problems happen all the time. Therefore, people hold worries towards the development of computer network technology. Since computer network security influences people's life, researches to build a computer network security model must be continued.

Keywords: Network security, Attacks, Vulnerability of network, Secure coding

Corresponding Author: MISS SNEHAL V. RAUT

Access Online On:

www.ijpret.com

How to Cite This Article:

PAPER-QR CODE

Snehal V. Raut, IJPRET, 2015; Volume 3 (9): 274-283

INTRODUCTION

With the introduction of the computer, the need for automated tools for protecting files and other information stored on the computer became evident. This is especially for a shared system and the need is even more acute for systems that can be accessed over a public telephone network, data network or the internet.

The second major change that affected security is the introduction of distributed systems and the use of networks and communications facilities. Network security measures are needed to protect data during their transmission. In fact, the term network security is somewhat misleading, because virtually all business, government, and academic organizations interconnect their data processing equipment with a collection of interconnected networks. Such a collection is often referred to as an internet, and the term internet security is used.

Computer and network security is both fascinating and complex. Computer and network security is essentially between a perpetrator who tries to find holes and the designer or administrator who tries to close them. The difficulties just enumerated will be encountered to enormous ways as I examine the various security threats and mechanisms through this paper.

Review of the literature:

Sutapa Sarkar & Brindha.M (2014) discusses the merit of FPGA devices to be used in network intrusion detection system implementation. **Ailin Zeng (2014)** analysis about computer network security is to integrate resources related to computer network technology and security system to build a computer network security model. **Priyanka Sharma, Dr. Kamal Sharma,, Surjeet Dalal (2014)**presents a survey of the main types of attack at the network layer, and review Sybil attack.**Bart Preneel (2014)** discusses the state of the art of cryptographic algorithms as deployed for securing computing networks. **Kartikey Agarwal*, Dr. Sanjay Kumar Dubey(2014)**outlines the various attack methods which are used, as well as various defense mechanism against them.

Present scenario of computer network security:

The computer network security is the security of computer network, security of important data in the network system and the structural completion of computer network. To accomplish computer network security is to protect users' data and computer system from malicious attacks and steals from outside. People who work on protection of computer network security are technical material analysis engineer of computer network security. They protect the network system from computer security problems that would influence the security of users' computers, like steal, collapse, interrupt and etc.

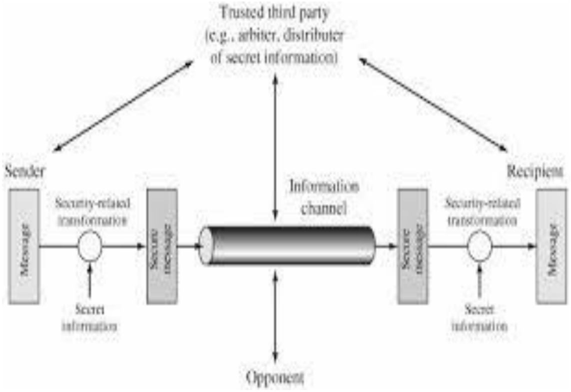

Fig.1- Network Security Model

Nowadays, computers are popularized and became an indispensable part in people's life. People use computer network communication technology to communicate with friends, finish works, learn new knowledge and entertain themselves. The development of computer technology is changing people's way of living and improving the quality of life.

There are a lot of computer network security specialists working on in-depths researches in computer network security. They have set up special researches on the maintaining, destruction and repairmen of computer network security. Based on these research results, specialists built the PPDRR computer network security model.[3] Through this model, people can accomplish monitoring and analyzing computer network security & specialist can detect the vulnerabilities of computer network system and react in time to protect computer network system from leak of information and economical loss.

The designing of computer network security involves a wide range of specialties. Any professional knowledge related to computer could be involved, for example software design of computer software development, monitoring and maintenance of software could all use the protection of computer network security.

Through large amount of researches, specialists proposed a new analysis method of computer network security--"attack-tree". Specialists integrate past attacking data and use mathematical formulas to represent them. This kind of method is called "attack-tree". Although this method still have some flaws and disagreements in integrating and explaining the "leaves". Therefore some specialists also proposed “privilege graph” analysis method to improve past computer network security analysis methods.

With the development of technology, there have been continuous innovations of computer network security analysis methods and model building of computer network security has matured continuously. But the way of scientific is being continued. Computer network security model building is still being worked on.

1. Attack of hackers:

Hacker refers to people with great computer network skills but use them to sabotage the internet or steal information. Currently, hackers are the **number 1 influential element of computer network security.** The main operational principle of hackers’ attackis to use their great skills of computer network to enter the system to collect data. Most hacked use Trojan horses and worm virus to attack users’ computers. In order to protect users’ personal information and avoid malicious consequences, we need to set up a computer network security model to monitor internet security.

Types of attack:

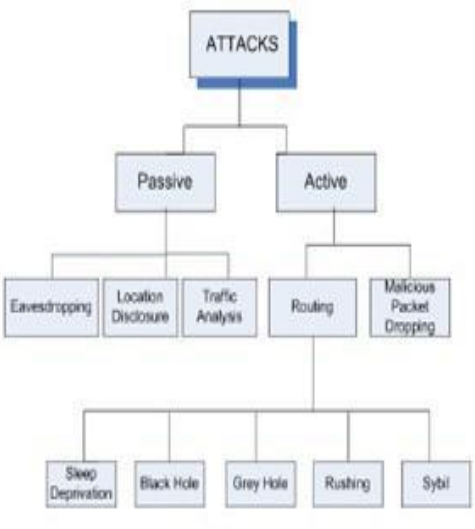

Fig.2- Types of attacks

Passive Attack

A **passive attack** monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. **Passive attacks** include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user. **[9]**

Active Attack

In an **active attack,** the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data. **[9]**

Distributed Attack

A **distributed attack** requires that the adversary introduce code, such as a Trojan horse or back-door program, to a “trusted” component or software that will later be distributed to many other companies and users. Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks introduce malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date. **[9]**

Insider Attack

An **insider attack** involves someone from the inside, such as a disgruntled employee, attacking the network Insider attacks can be malicious or no malicious. **[9]**

Close-in Attack

A close-in attack involves someone attempting to get physically close to network components, data, and systems in order to learn more about a network. **[9]**

Phishing Attack

In phishing attack the hacker creates a fake web site that looks exactly like a popular site such as the SBI bank. The phishing part of the attack is that the hacker then sends an e-mail message trying to trick the user into clicking a link that leads to the fake site. **[9]**

Hijack attack

In a hijack attack, a hacker takes over a session between you and another individual and disconnects the other individual from the communication. **[9]**

Spoof attack

In a spoof attack, the hacker modifies the source address of the packets he or she is sending so that they appear to be coming from someone else. **[9]**

Buffer overflow

A buffer overflow attack is when the attacker sends more data to an application than is expected. **[9]**

Exploit attack

In this type of attack, the attacker knows of a security problem within an operating system or a piece of software and leverages that knowledge by exploiting the vulnerability. **[9]**

Password attack

An attacker tries to crack the passwords stored in a network account database or a password-protected file. There are three major types of password attacks: a dictionary attack, a brute-force attack, and a hybrid attack. **[9]**

2. Software system and vulnerability of network system:

In computer network security, vulnerability of network and software is the **second influential element of computer network security after hacker attack.** Vulnerability of computer network and software includes vulnerability in computer system and software design, lack of protection of computer network and software security, illegal users enter users' computer through computer network vulnerability and computer being controlled maliciously by unknown users. This high-risk vulnerability could severely influence user's daily use of computer and normal network communication. It would cause users' information cannot spread and receive. With this high-risk vulnerability, computers could be attacked; information could be steeled any time by any unknown people. It would directly influence the security of computer network system and cause great loss. [10]

3. Falsification of users' personal information and leak of classified information

Falsification of users' personal information and leak of classified information is **the third element of computer security**. Therefore, we must pay special attention to the protection of users' personal information and classified materials. Falsification of users' personal information refers to the action that with the transfer of users' information, a third party intercept, falsify and delete the information to result in the interception and steal of users' information. Computer network technology has influences on people's life, economy and politics.

1)Security measures:

Different professions have different requirements of the security of computer network system. The protection ranges are also different. Specialists put the relationship between security requirements and different threats.

In the actual use of computer network system could be set to give different users' different levels of access. Foreign counties have analyzed this kind of usage carefully and designed to limit different users' access of the system.

A state of computer "security" is the conceptual ideal, attained by the use of the three processes: threat prevention, detection, and response. These processes are based on various policies and system components, which include the following: **[9]**

- **User account access controls and cryptography** can protect systems files and data, respectively.

- **Firewalls** are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering. Firewalls can be both hardware- or software-based.

- **Intrusion Detection Systems (IDSs)** are designed to detect network attacks in progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.

- **"Response"** is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of legal authorities, counter-attacks, and the like. In some special cases, a complete destruction of the compromised system is favored, as it may happen that not all the compromised resources are detected.

2) *Reducing vulnerabilities*

Social engineering and direct computer access (physical) attacks can only be prevented by non-computer means, which can be difficult to enforce, relative to the sensitivity of the information. Even in a highly disciplined environment, such as in military organizations, social engineering attacks can still be difficult to foresee and prevent.

3) *Hardware protection mechanisms:*

While hardware may be a source of insecurity, such as with microchip vulnerabilities maliciously introduced during the manufacturing process, hardware-based or assisted computer security also offers an alternative to software-only computer security. Using devices and methods such as dongles, trusted platform modules, intrusion-aware cases, drive locks, disabling USB ports, and mobile-enabled access may be considered more secure due to the physical access (or sophisticated backdoor access) required in order to be compromised.

4) *Secure operating systems*

Systems designed represent the state of the art of computer security. Secure operating systems designed are used primarily to protect national security information, military secrets, and the data of international financial institutions. These are very powerful security tools and very few secure operating systems have been certified at the highest levelto operate over the range of "Top Secret" to "unclassified".

5) *Secure coding*

If the operating environment is not based on a secure operating system, then high degrees of security are understandably not possible. While such secure operating systems are possible and have been implemented, most commercial systems fall in a 'low security' category because they rely on features not supported by secure operating systems (like portability, and others).

Some common languages such as C and C++ are vulnerable to all of these defects Other languages, such as Java, are more resistant to some of these defects, but are still prone to code/command injection and other software defects which facilitate subversion.

Unfortunately, there is no theoretical model of "secure coding" practices, nor is one practically achievable, insofar as the code (ideally, read-only) and data (generally read/write) generally tends to have some form of defect.

CONCLUSION

With the development of computer network technology, computer network security problems happen all the time. Therefore, people hold worries towards the development of computer network technology. Since computer network security influences people's life, researches to build a computer network security model must be continued.

ACKNOWLEDGMENT

I express my sincere gratitude to Dr. H. R. Deshmukh, Head& Professor, Department of CSE, IBSS COE, Amravati for his valuable guidance and advice. Also I would like to thanks to my guide Prof. Ankit Mune and the faculty members for their continuous support and encouragement.

REFERENCES:

1. Zhang Tao; Hu Mingzeng; Yun Xiaochun, Zhang Yongzheng. Research on computer network security analysis model [J]. Journal of communications, 2005(12).

2. Hong Yaling. On modeling of computer network security [J]. Computer CD Software and Applications, 2013(02).

3. Xv Liuwei. Modeling of computer network security [J]. Computer CD Software and Applications, 2013 (06).

4. Huang Zhilong. Research on computer network security analysis model [J]. Research on computer network security analysis model, 2014(05).

5. Zhang Baoshi. Research on computer network security analysis model [J]. Electronic technology and software engineering, 2014(04).

6. Ailin Zeng, "Discussion and research of computer network security" Journal of Chemical and Pharmaceutical Research, 2014, 6(7):780-783

7. Priyanka Sharma, Dr. Kamal Sharma, Surjeet Dalal, "Reviewing MANET Network Security Threats" International Journal of Recent Research Aspects, Vol. 1, Issue 2, Sept. 2014, pp. 25-30

8. Sutapa Sarkar &Brindha.M, “High Performance Network Security Using NIDS Approach”, I.J. Information Technology and Computer Science, 2014, 07, 47-55

9. Kartikey Agarwal & Dr. Sanjay Kumar Dubey “Network Security : Attacks and Defence’ International Journal of Advance Foundation and Research in Science & Engineering (IJAFRSE) Volume 1, Issue 3, August 2014.

10. Jaykumar Shantilal Patel and Dr. Vijaykumar M. Chavda, “Security Vulnerability and Robust Security Requirements using Key Management in Sensor Network”, International Journal of Grid Distribution Computing Vol.7, no.3 (2014), pp.23-28

11. Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal,Abdul Hanan Abdullah and Kashif Naseer Qureshi “Security Issues and Attacks in Wireless Sensor Network” World Applied Sciences Journal 30 (10): 1224-1227, 2014

12. Bart Preneel, “Cryptography for Network Security: Failures, Successes and Challenges” (2014)