COMPUTER SECURITY AND TYPES OF ATTACKS

Priyanka Paulraj[1] , Vijaya Shinde[2] , Kartika Sonawane[3], Prof. Suwarana Nimkarde [4]

[1]*Student, Computer Technology, Bharati Vidyapeeth Institute of Technology, Maharashtra, India*
[2]*Student, Computer Technology, Bharati Vidyapeeth Institute of Technology, Maharashtra, India*
[3]*Student, Computer Technology, Bharati Vidyapeeth Institute of Technology, Maharashtra, India*
[4]*Prof, Computer Technology, Bharati Vidyapeeth Institute of Technology, Maharashtra, India*

ABSTRACT

The computer security has become foremost now-a-days. There is rapidly development of internet technology which is aware the people about the importance of computer security. The main issue of computer security is their types of attacks which are increasing day by day. Computer security is a comprehensive term that covers cyber security, information or data security, hardware and software security. The malicious node create problem in networks system and also act as selfishness that use other node information and preserve the information of its own. This paper describes computer security and also some major types of attacks faced by network security.

Keywords: *Computer security, Attacks, IDS (Intrusion Detection System)*

1. INTRODUCTION

Computer security which means dealing with the prevention and detection of unauthorized action which is done by the user of that computer. It is not about the computer but also about the information technology as it covers about cyber security. Computer security has been evolved over the period of time. As computer became popular as the day passes, its security become more and more essential. Computer play an important role in our daily life. Its security is the most important part of it. Computer not only stores the business details, it also has some personal storage which is related to persons. Communication and storage is also important function done by machine.

Utility of the computer have increased a lot as compare to its utility before last decade because of internet. The word "Online" is part of our everyone discourse. The era of internet we have to live in information technology where computer are used to manipulate, communicate and store our data or information. Computer security is needed for to protect the valuable data or information from the unauthorized access and its misuse. It could be business or personal data or information .To keeps the user name and password secret saving from unauthorized access. To protect the system from "intrusion" can be done by implementing firewall. The process of promoting of information technology and internet which has become very important for all human being .It is not possible survives without computer. For this computer should be secured from various threats, attack and risk. Computer security plays an important role in network system.

2. LITERATURE REVIEW

The main issue is protecting the system against total network failure, since adding integrity checking tools to the network doesn't give a good metric of how much less frequently the network is unavailable or degraded for security reasons. In a highly switched network, monitoring the integrity of the network becomes a very difficult task. Successful integration of these tools requires understanding of what the threats are and how to detect them.[1]

As the popularity of e-commerce, many organizations are facing security challenges. Security techniques and management tools have achieved a lot of attention from enterprise. Since, there is lacking a theoretical framework

for computer security management. In this paper the author suggests that an integrated system theory is useful for understanding computer security management and also its strategies.[2]

In this paper the authors explain the process of Traditional approaches to security architecture and how designs have attempted to achieve the goal of the elimination of risk factors. The author focuses on Technical and Insurance Controls for Enterprise-Level Security.[3]

The goal of enterprise networking is about providing a connectivity to anyone, anywhere, from any device, to any application or service reliably and securely. This paper discusses to come with a large potential for increasing operational efficiency and ability of operated network.[4]

3. METHODOLOGY

3.1 Security Principles of Computer Security

The key security principle of computer security as follows:

1. Confidentiality
2. Integrity
3. Availability
4. Accountability
5. Non-repudiation

1. Confidentiality
Confidentiality is nothing but privacy or secrecy. It is a concept of hiding of important data or information from unauthorized. Privacy means the context of personal data and secrecy means the context of data pertaining to organization or business.

2. Integrity
Integrity is a property that ensures authorized or unauthorized user of the system which does not change the data that will results into the loss of company's accounting records or assets.

3. Availability
In computer security the concept of availability is refers to the access to the computer system to the valid user. The users should be protected from malicious attacker. The example of availability is Denial of service.

4. Accountability
Accountability is mainly about the awareness of the people what he or she has done for their computer usage. Auditing is needed to be done for accountability. It tells us about who has done what .It keeps the information properly and protected. It also tells us about what have actually happen in the security. If the security is violated, the steps for recovery can be taken.

5. Non-repudiation
Non-repudiation is a kind of service that provides unforgivable evidence for particular action has to take place. In computer security it is useful for analyzing security part with helps for cryptographic mechanism.

3.2 TYPES OF ATTACKS:

Here we are going to tells you about the various types of attacks which occur in computer security.

1. Active attack:

Active attack is defined as an attack that modifies the whole or partial data which is present in the hacked system .They are classified into several of following as follow:

i) Masquerade:

In this attack the third computer acts as computer network or device. It is quite difficult to identity that the mail which is sender by a computer to a particular computer is reached or not.

ii) Modification of data:

Changing of data very smartly .This data might be recorded or delayed.

iii) Replay:

In this the third party captures the data in wrong way and the data re-transmitted to the actual user.

iv) Denial of service:

The actual user may get fake message regarding stopping their service or terminating.

2. Passive attack:

Passive attack is defined as an indirect attack on the system or data. In this attack the attacker might keep watching in your websites or system to gain its controls. As it is passive attack, so its won't affect data or system. But it is quite difficult to detect his type of attack as attacker do not change or modify the information present on the system.

3. Denial of service (DOS):

Denial of service (DOS) attack scan exploits a known vulnerability in a specific application or operating system. In this form of attack, the attacker is attempting to deny authorized user access either to specific information.
The main purpose of this attack is to access to the target system or the attack can be used in conjunction with other actions in order to gain unauthorized access to a computer.

4. Backdoors and Trapdoors:

Backdoor is defined as the way that is used by the attacker to ensure that they should gain an access to the computer system.
Trapdoor is defined as if the attacker is successful in establishing the backdoor, the whole system and software can become vulnerable.

5. Sniffing:

The process of examining the network traffic that goes through their network interface card and check whether that traffic addressed for those interface card or not.

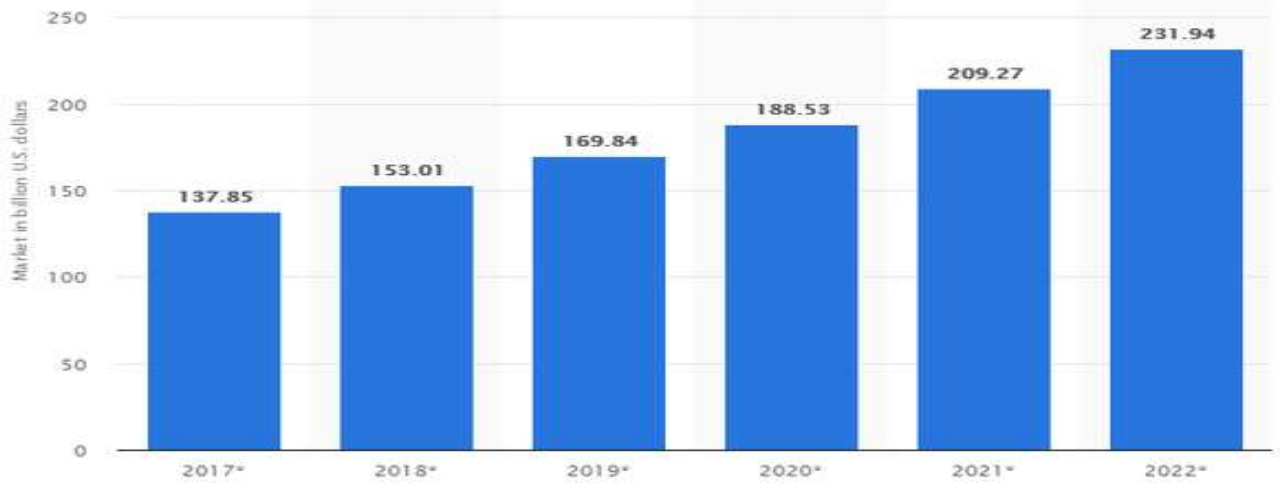
6. Spoofing:
The technique in which it looks like that the data has come from the various sources. It is possible to execute in such technique in TCP/TP as the TCP/TP protocol provides user friendly environment.

7. Man in the middle attack:
It occur when attacker are able to place themselves in the middle of two host which are communicating .Make sure the all communication going from the host is routed through the attacker host. Attacker is able to observe all traffic before transmitting it can actually block traffic.

8. Replay attack:
In this type of attack the attacker captures the part of the communication that is taking place between two parties and then later on retransmits it.

4. Future Scope

The future scope in computer security has been increasing day by day as increase in attacks and crime. Government or private companies stores their data or any important information in the computer, they provide security to the system .So that no one can hack their information and misused it. In future computer security will play an important role in the world. As the marketing values of computer security is increase to 232 billion by 2020 according to reports. There is a good scope in computer security in future.



5. Conclusion

In this we have concluded that Computer security attempts to ensure the confidentiality, integrity, and availability of computing systems and their components. Three parts of a computing system attacks: hardware, software, and data. These concepts are basis that we need to study, understand and master computer security.

6. REFERENCES

[1] Leonard L Mutembei , Aloys N Mvuma and Tabu S Kondo " Network Security Analysis in the Enterprise LANS." http://www.ijcaonline.org/archives/volume101/number13/17751-8837/

[2]Kwo Shing Hong, Yen Ping Chi, Louis R. Chao & Jih Hsing Tang, "Information Management & Computer Security" http://www.emeraldinsight.com/doi/abs/10.1108/09685220310500153

[3] Jose de la Pena Munoz "Information Security Industry" http://link.springer.com/chapter/10.1007/978-3-8348-9283-6_8 /

[4]Plamen Nedeltchev "The new opportunities of enterprise Networking" http://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-oncisco/extended_enterprise_network.html

[5]Homer, J. Kansas "SAT-solving approaches to context-aware enterprise network security management" http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4808475&url=http%3A%2F%2 Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4808475

[6] Igor Kotenko, Mikhail Stepashkin "Attack Graph Based Evaluation of Network Security" http://link.springer.com/chapter/10.1007/11909033_20#page-1

[7]Andrew R. McGee, S. Rao Vasireddy, Chen Xie1, David D. Picklesimer, Uma Chandrashekhar and Steven H, "A framework for ensuring network security" http://onlinelibrary.wiley.com/doi/10.1002/bltj.10083/abstract

[8]ISBN "E-commerce Security Strategies: Protecting the Enterprise",http://www.dpu.se/ctrecs_e.html

[9] SULAIMON ADENIJI ADEBAYO, "NETWORK SECURITY" https://publications.theseus.fi/bitstream/handle/10024/47351/Sulaimon_Adeniji.pdf?sequ ence=1

[10] Umesh Kumar and Sapna Gambhir "A Literature Review of Security Threats to Wireless Networks" http://www.sersc.org/journals/IJFGCN/vol7_no4/3.p

[11] A.J. Siroin "Securing the Corporate Network" http://www2.uwstout.edu/content/lib/thesis/2005/2005siroina

[12] American Water "Arbor Networks traffic-centric approach to network security" http://www.arbornetworks.com/solutions/enterprise