ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 8, August 2018

Survey on Data Security and Security Risks

Varsha Bhosale[1], Simran Bhaldar[2], Prerana Ambavale[3], Chinmayee Achrekar[4], Swapnil Patil[5]

Students, Computer Technology Department, Bharati Vidyapeeth Institute of Technology, Navi Mumbai, India[1,2,3,4]

Lecturer, Computer Technology Department, Bharati Vidyapeeth Institute of Technology, Navi Mumbai, India[5]

Abstract: In this world, protecting our information has become an important part. Protecting our information means to protect it from an unauthorized access. This paper provides an excellent and easier way to protect your data from unauthorized access. Various viruses like Trojan horses, worms, malware and attacks like active and passive attack can be avoided by this system. We can also secure our system by using different security concepts i.e. confidentiality, integrity and availability. Nowadays each and every information is stored on electronic systems so this system provides easier way to secure information.

Keywords: Confidential Data, Data Security, Hackers, Attacks

I. INTRODUCTION

As everyday new technology comes up which makes the world much more connected and due to this there are more security techniques needed. The information which is stored on some of the medium is called as data. In last few years, the amount of information stored on electronic media has increased rapidly. However the information which is stored on electronically is more vulnerable. The Intruders which may not be even in the same country can steal the information without entering at home or in office.

Basic Security Concepts: Three basic security concepts are Confidentiality, Integrity and Availability, Authentication.

- Confidentiality: Here an unauthorized party has gained access to a resource, it can be a person, program or computer based system. The principle of confidentiality specifies that only sender and intended recipients should be able to access the message. Confidentiality gets compromised if an unauthorized person is able to access the contents of a message.
- Integrity: Here attackers may modify the values in the database. When the content of the message are changed after the sender sends it, but before it reaches the intended recipient we say that the integrity is lost. Integrity is a property that ensures authorized or unauthorized user of the system do not change the data that will result into loss of company's accounting records or assets.
- Availability: In this resources become unavailable, lost or unusable i.e. denial of service, problem causing to hardware device, erasing program, and data. Availability in the context of security refers to access computer system to the legitimate users. The legitimate users should be protected from malicious attacker.

II. DATABASE SECURITY

Computers have become an vital part of our life. Its security is the most important aspects. It includes various methods, tools, processes to ensure the security within a database environment. Some of the other ways in which the database security is analysed and implemented. Database security is needed for the following reasons:

1. To protect the valuable data or information from the unauthorized access and its misuse. The data or information must be kept intact. It could be business for personal data or information.
2. To keep the user names and passwords secret from other than authorized users.
3. To maintain the confidentiality and authenticity of the data or information.
4. To communicate the data or information over the networks without tampering it.
5. To secure computers on the network of phishing, hacker and cracker.
6. For protecting system from "intrusions". This can be done by implementing firewall.
7. To protect machines from breach or attacks.
8. For protection of the hardware that can be stolen or damage by unauthorized persons or users.
9. For protection of the software. If the software is damaged, the data or information can be lost forever.
10. To make the system secured from the attacks of spyware and malware.
11. To protect machine from destructive programs like viruses and worms.
12. To avoid the economical the economical loses because of any of the above reasons.
13. To make the system secured from the attacks of spyware and malware.

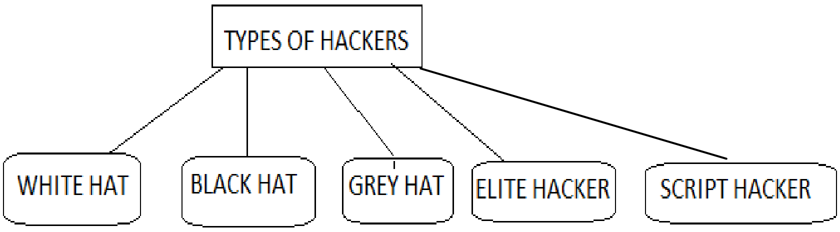
DOI 10.17148/IJARCCE.2018.788

14. To protect machine from destructive programs like viruses and worms.
15. To avoid the economical the economical loses because of any of the above reasons.

III. RISKS

Everyday hackers attack in different ways to confidential data. Databases are the key target for the cybercriminals to often leash the valuable information which is stored anywhere outside. The data can be financial or some intellectual secrets. Having rated values of assets, the criticality of vulnerabilities and the likelihood of threats, can give the result of calculating risks. In quantitative analysis, expected losses could be computed in the framework of probabilities theory, based on monetary values for the assets and probabilities for the likelihood of threads. There are areas of risk analysis where quantitative methods work but more often the lack of precision in the inputs does not justify a mathematical treatment. The different risks are:

- **Fake Anti-Viruses**: Everyday cybercriminals are constantly looking for new victims to gain their personal information and money. One of the ways to gain this information is fake Anti-Virus. The attackers they pose the real products and the victims need to think twice before clicking on it.
- **Hackers**: Hacking is one of the most well-known types of computer crime. The person who is engaged in hacking activities is called Hackers. A hacker is someone who finds out and exploits the weakness of computer systems or networks. A hacker is basically someone who breaks into computer networks or standalone personal computer systems for the challenge of it or because they want profit from their inmate hacking capabilities.



1.White Hat Hacker: The white hacker can be a person who spends lot of time and find hacking or he/she can be a master of hacking who wants good money or a person who wants to dominate the world with the use of internet
2.Black Hat Hacker: Black hat hacker is also called as crackers. Black hat represents hacker or cracker who enters into the computer or network with malicious intention in authorized or unauthorized way.
3.GreyHat Hacker: A grey hat hacker is a person who is exactly between white hat hacker and black hat hacker. This person can use his skills either for legal or illegal acts. He generally doesn't do this act for his personal gain.

- **Worms**: Worms are malicious program that spread them automatically. It spreads from computer to computer without any human action intervention. Worm is designed to copy itself from PC to PC via networks or internet. It requires a human to move it forward. However, computer worm may have a "payload" that can delete files, encrypt files or e-mail files on the host computer.

Example of Worms:
1.Storm Worm
2.The Morris Worm
3.The Anna Kounrikova Worm
4.The Blaster Worm
5.Netsky and Sasser

- **Trojan Horses**: It takes the name from the classical story of Trojan horse, which imitates the different techniques to infect computer. A Trojan horse may be included as an attachment or as part of an installation program. It can be used to compromise the security of your system, and they can exist on a system for years before they are detected. Trojan can enable cyber criminals to keep a spy on you or steal your sensitive information which include:

  1.Deletion of data
  2.Modification of data
  3.Blocking of data
  4.Copying of data

- **Malware:** It is malicious software that is harmful to a computer user. Malware is software designed to cause damage to a computer, computer networks or servers. Malware and malicious code is defined as the piece of program code that causes loss of harm to the computing system degrading or disrupting the functionality and services provided by the system. The malicious program can perform a variety of different functions which includes stealing, encryption of sensitive data, deletion of data, or altering without users permission. Types of Malware are:

DOI 10.17148/IJARCCE.2018.788

1. Trojan horse
2. Virus
3. Spyware
4. Worm
5. Spam
6. Logic Bomb
7. Time Bomb

IV. ATTACKS

There are two types of Attacks:
• **Active Attack**: Active attack can be defined as an attack that modifies or delete partial or whole data present on the hacked systems. Active attacks results in the disclosure of dissemination of data files, DoS, or modification of data. It can be subdivided into four categories:
1.Masquerade
2.Modification of a data
3.Replay
4.Denial of service

• **Passive Attack:** Passive attack can be defined as an indirect attack on the system or data. Attackers keep watch on the websites or system for gaining its control. Since, this attack is passive it won't affect data, protocol, or system. It is quite difficult to detect such attacks as attackers do not change or modify the information present on the system. Even though passive attacks sounds less harmful, the damage in the end can just be as severe if the right type of information is obtained. There are two types of passive attacks: i) Release of Message Contents ii) Traffic Analysis.

V. PROTECTION OF DATA

- Encrypt your data
- Backup of Data
- Anti-Malware software is must
- Install Operating System updates
- Don't store passwords with your laptop or mobile device
- Delete old files from cloud backup
- Maintain Anti-Virus software
- Scan computer for spyware
- Create separate user account
- Password protect documents

VI. CONCLUSION

After studying this system model we can conclude that this system can help to understand how to make data and information secure and also can control the cybercrimes.

REFERENCES

[1]. Sangita Rautela, Arvind Negi, Prashant Chaudhary "Data Security and Updation of Data Lifecycle in Cloud computing using Key-Exchange Algorithm" https://ijarcce.com/wp-content/uploads/2015/09/IJARCCE-83.pdf

[2]. M. Tech Computer Science Department, United College of Engineering & Research, Allahabad, India " Enhancing Information Security in Big Data" https://www.ijarcce.com/upload/2016/august-16/IJARCCE%2064.pdf

[3]. Chandni Patel, SameerSingh Chauhan, Bhavesh Patel "A Data Security Framework for Mobile Cloud Computing" https://ijarcce.com/wp-content/uploads/2015/03/IJARCCE4K.pdf

[4]. Brindha. M ,Prof. S.V.Hemalatha "A Survey on Privacy and Security of Data Classification" https://ijarcce.com/wp-content/uploads/2015/12/IJARCCE-61.pdf

[5]. Dr. L. Arockiam, S. Monikandan "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm" https://www.ijarcce.com/upload/2013/august/23-o-Moni%20Tamil%20-data%20security%20and%20privacy%20in%20cloud.pdf

[6]. Ankit R. Mune, P. R. Pardhi " Security for cloud computing data using a security cloud as a Third party auditor (TPA): A Survey" https://ijarcce.com/wp-content/uploads/2012/03/IJARCCE3C-a-ankit-Security-for-cloud.pdf

[7]. T. Shanmuga Vadivu, D. Saranya, S.Karthika "Security and Privacy in Big Data" https://ijarcce.com/upload/2017/si/ICITCSA-17/IJARCCE-ICITCSA%2025.pdf

[8]. Yaquob H. A. Alkandary, Eng. Fawzyeya M. A. Alhallaq "Computer security" https://ijarcce.com/wp-content/uploads/2016/02/IJARCCE-1.pdf

DOI 10.17148/IJARCCE.2018.788