JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

DEFENCE MECHANISM AGAINST SECURITY THREATS

[1]Dr. Jasleen Kaur
[1]Post Graduate Deparment of Computer Science
[1]Gujranwala Guru Nanak Khalsa College
[1]Ludhiana, INDIA

***ABSTRACT*:** Today we are living in a global village. We have facilities like science, technology which have developed inter-connecting bonds among different countries on the globe. The science is working in the direction of making human life more comfortable and better than last decades. The technology has made life smoother, faster, and simpler. Through it, the single bit of information can be easily transmitted within seconds from one computer system to another around whole of the world. Gone are the days when we tried to communicate through post letters, fax machines and telephones. Now we have achieved our dreams. We have various facilities such as video chat, telemedicine, movies on demand, relay chat rooms, various e-business models which reminds us that distance and time barriers of communications are no more these days. One can enjoy all these benefits but this bright has dark side as well too. There are lots of threats which are dangerous for information security on the computer network such as phishers, hackers, viruses etc. A large portion of our system experts' efforts, their systems' energies, time, and investments are consumed by these security threats and their fixation. We are continuously working for the development of strong information security system with minimum amount of wastage for the efforts made. The objective of this paper is to discuss about the information security and the defense mechanisms used by it against security threats.

Keywords: - Information, Information Processing, Information Security, Defense Mechanisms, Security Threats.

I. INTRODUCTION

Today's era is an era of e-business, e-commerce. Numerous transactions such as online buying and selling are taking place on internet. We have EPS (Electronic Payment System) too. Credit cards, debit cards, e-cash, and net cash coins can all be used to make payments online with ease, but ongoing technological and commercial changes have also led to some serious security concerns. To handle such issues is a very tough job. There are many different types of people who can alter or destroy the computer security system and information security, including hackers, crackers, spies, scam artists, etc. The exposure, erasure, and change of data or information are caused by viruses, worms, and trojan horses. In the e-business and e-commerce world, one can freely thrive thanks to several powerful security systems.

II. INFORMATION SECURITY- WHAT IT INCLUDES?

1. Computer Security- It means protection of computer system including hardware as well as software.

2. Data and Information Security- It includes protection of data, databases, diagrams or charts, bar graphs, other information such as intellectual properties, audio-video files, digital certificates and signatures etc., at time of storage, transmission and use of such data and information. It includes protection of passwords and PIN numbers of credit or debit cards, bank accounts, e-wallets etc.

III. LITERATURE REVIEW

Information security (IS) was initially recognised for its ability to keep information private and secure while maintaining its integrity. The locations and hardware of mainframes used in the military at the time were not secured. The same circumstances were confirmed to exist in 1967. In 1980, the First National Bank of Chicago was hacked for 70 million $. During 1990's, the use of personal computers was increased. Online users were progressively disclosing private information, giving hackers and crackers easy access to potential targets for their nefarious activities. Since 2000, because of increased internet usage, their sources of happiness have grown. Various security risks have been introduced by the open-source software and the unprotected network. On the other hand, there is hope for a better future for information security because of white-hat hackers, legal sniffers, ethical crackers, and antivirus software, which serve as lifeguards against such fatal threats.

A literature is a storehouse of information which is reviewed in order to get a direction on the current state of a particular topic/work in hand of a researcher. For this paper, the review of literature is given below: -

1. The authors describe for documenting attacks on software systems using attack free information in a structured and reusable form. This approach is helpful to identify commonly occurring attack trees to enhance security developments [1].
2. The authors discuss about issues, challenges in wireless sensor network. It discusses about two types of wireless security attacks, one is, attack on security mechanisms and other one is, attack on the basic mechanisms. It explains the various security schemes for wireless sensor networks like use of random key, statistical enroute filtering. This study provides the holistic view of security in wireless sensor networks [3].

INFORMATION- Any fact, figure, or piece of information that has been specially organised so that the information recipient may understand it is referred to by this phrase. The recipient uses this information to respond to his query, offer an explanation, or carry out some other specific task or purpose.

INFORMATION PROCESSING- It involves a number of steps that are taken to convert unprocessed knowledge or information into knowledge that is meaningful, organized, and purposeful in order to produce an output or provide results.

INFORMATION SECURITY- It requires bringing or using some protective measures for the safe use, transmission, and storage of online information, whether it is in the form of text, audio, video, movies, or digital certificates or signatures, to control or minimize the risk of unauthorized use of such secured information or of decoding, disclosure, changing, or destroying such information with improper intentions.

DEFENSE MECHANISM- A defensive mechanism is a strategy, plan, or method used to counter threats or dangerous/harmful damage to informational or intellectual property.

SECURITY THREATS- A security hazard is something that could have a negative or harmful impact on how securely data is stored in a system. Data exposure, unauthorized access, data alteration, and computer system failure are all potential results.

IV. NEED OF INFORMATION SECURITY

1. VALID TRANSMISSION OF INFORMATION- Information security system aids in reliable information delivery. Without any adjustments by outside parties, the information can be easily received by the recipient.

2. NON-REPUDIATION- It indicates that linked parties should not object to an e-contract. As an illustration, once a customer has given the recipient an order for the purchase of goods, the customer cannot cancel the transaction. It is now achievable thanks to information security.

3. AUTHORIZATION MANAGEMENT- Information security enables users to make targeted use of their resources. It enables a user to legitimately access websites or information in an appropriate manner.

4. DATA SECURITY AND CONFIDENTIALITY- Information security keeps data and information shared among related parties secure and private, preventing unauthorized parties from accessing it. Data encryption and decryption are part of data security.

5. STRICT CONTROL AND MANAGEMENT OF DATA ACCESS- A user must sign in with a valid ID and password to access a system or social media platform, and information security carefully regulates and manages data and information access. Thus, it offers security against data theft as well as against data removal, erasure, or alteration.

6. SECURITY FOR BANKING TRANSACTIONS- Information security aids in the secure transfer of data or money when conducting online banking transactions. When conducting online banking transactions, it facilitates the transmission of encrypted data.

7. AUTHENTICATION AND IDENTIFICATION- In order to create, store, and use digital signatures securely during e-commerce and e-banking transactions, information security systems are helpful. Digital signatures give the recipient a good reason to believe that he is receiving a valid document from a valid sender over the Internet, and on the sender's side, the sender cannot dispute having sent that message to the recipient. Digital certificates issued by certifying authorities can also be created, transmitted, and stored with the aid of information security. This certification authority signs the certification, demonstrating that it is legitimate and capable of being validated later. Through its cryptographic technology, it also aids in verifying the authenticity of digital certificates.

8. COMMUNICATION-CHANNEL'S SECURITY- Using HTTP and secure hypertext transfer protocol, information security systems assist in safeguarding communication channels.

9. THE PROTECTION OF CLIENTS AND SERVER ON THE NETWORK- Information security helps to safeguard clients and servers on a network by preventing viruses and worms from infiltrating the network using hardware or software. This secures the network.

10. IT IMPROVES WEB PERFORMANCE- Using a proxy server improves web performance while maintaining information security. A proxy server is a computer that stands between a client and a server. By removing incoming and outgoing Internet content, a proxy server enhances web performance.

V. SECURITY THREATS TO INFORMATION SECURITY

It means any condition that poses danger to computer, its data, network resources etc. It includes following points: -

1. **CRACKERS-** He is a person who can steal someone's data online or can break/crack someone's online account password.

2. CONMAN- He is a person who steals credit card information or credit card numbers for sale.

3. INSIDER ATTACK- People who are given permission to access computer resources, such as data, files, etc., may utilize those resources improperly in order to benefit personally or financially from them or others. It is particularly challenging to track down such attackers because they are present within the firm and possess in-depth knowledge of computer information systems.

4. PHARMING- Pharming is an act in which a person known as a pharmer attempts to mimic certain previously existing official or genuine websites to steal other people's personal data. Pharmers typically target banking or e-commerce websites to steal personal information.

5. SNIFFING- A person or software known as a sniffer engages in the illicit act of sniffing. Its goal is to read, check, and monitor network traffic, as well as to steal data like computer files and passwords or to keep a watch on computer networks and their resources a process known as "sniffing the network."

6. HACKING- It means to illegally take control of a computer, its network source, and any other systems connected to it. The perpetrator is referred to as a hacker. He can break into the systems for his own benefit or to commit crimes, such as stealing and selling personal

information to other users or hackers, or stealing credit card numbers or banking information. There are many different types of hackers, including white hat hackers, grey hat hackers, and black hat hackers, the latter of which are very risky.

7. PHISHING- Phishing is typically carried out using e-mail scam letters that link to bogus web pages that imitate real pages from reputable businesses. Phishing is the practice of asking email recipients to visit fictitious websites to trick them into divulging personal information like bank account numbers and ATM passwords. Users may occasionally receive offers from phishers to provide information fast and within a certain time frame so that the user will feel pressured and respond appropriately.

8. VIRUSES- A virus is a piece of harmful software that has the ability to replicate itself and then run itself in computer files to corrupt them. It can attack computer hard discs, software programmes like Microsoft Word and Power Point, and executable files like *.exe and *.com, among others.

9. WORMS- Worms are malicious scripts that do not replicate themselves, making them distinct from viruses. By locating security flaws in software, they travel from computer to computer and attack through networks. Worms can also launch attacks by breaching firewalls.

10. TROJAN-HORSE AND BOTS- Trojan horses are security risks that can hijack any program, delete computer files, and disable the processor by gaining unauthorized access to the target computer. On the other hand, bots are covert software applications that are installed on a specific computer system and contain malicious code.

12. INADEQUATE TOUGH SECURITY SYSTEM- Although significant progress has been made and ongoing efforts are made to combat system security threats and preserve information, hackers still manage to exploit security flaws and get access to systems in order to manipulate the data. There are many security system suppliers, but only a select number can perform well.

13. USE OF WIRELESS FIDELITY- 'Wi-Fi, often known as "Wireless Fidelity," is susceptible to security breaches that have a negative impact on users. The user connects to the internet using Wi-Fi. Due to the widespread availability of Wi-Fi in public spaces today, including hotels, colleges, and cyber cafes, users are vulnerable to this hazard.

14. RANSOMWARE- A malicious programme is installed on another person's computer, preventing him from accessing or using it. The afflicted person's important and non-sensitive information is all accessible to the cybercriminal, who grants the user access to the information in exchange for the ransom sought. A recent attack that affected nearly 100 countries worldwide in 2017, including their governmental systems, is an illustration of the security risks that today's security system must contend with.

VI. DEFENCE MECHANISMS TO COMBAT INFORMATION SECURITY

1. PROTECTION OF INFORMATION ON PHONE, COMPUTERS- The simplest way to protect information is to secure one's computer and phone, which are where the data is stored. Information can be protected by employing security features like firewalls, updated anti-virus software, and passwords.

2. USE OF STRONG PASSWORDS FOR BANK ACCOUNTS- For online banking transactions, one should use a secure password. Additionally, one should avoid using the same password for all social media and banking accounts.

3. OPTIMUM USE OF PRIVATE SETTINGS- Facebook, WhatsApp, and other social media accounts can be utilised with privacy settings. Making profiles and entering personal information like contact information and email addresses leaves a user open to unwanted behaviour. Maintaining profile privacy can assist ensure a secure and welcoming social media experience by putting snoopers and sniffers to rest.

4. USE CARDS PROPERLY- Credit cards offer the best level of legal protection for e-payments. However, compared to credit cards, debit cards provide less legal protection in the event of fraudulent purchases.

5. HANDLE CREDIT CARD REPORT/INFORMATION CAREFULLY- Credit card information should be handled with caution as it is a useful tool for lowering the risk of identity theft.

6. USE OF BIOMETRICS FOR AUTHENTICATION AND IDENTIFICATION PURPOSES- Biometrics, which verify that a person is who they say they are, can be used for authentication and identification. Examples include fingerprints, facial expressions, birthmarks, signatures, writing styles, and eye retinas.

7. DIGITAL CERTIFICATES- Information may be exchanged over the Internet safely thanks to digital certificates. A PKI is utilized here. The term "public key infrastructure" (PKI) is used. As long as they are issued by legitimate certificate authority, digital certificates are resistant to counterfeit and may be cross-verified at any moment.

8. FIREWALLS- As it prevents or blocks data from entering the network, a firewall aids in the inspection of both incoming and outgoing information. As a result, it protects data across the whole network.

9. ANTIVIRUS SOFTWARE- It is a safe procedure or technique for maintaining data security. It provides protection against various security risks including hackers, Trojan horses, sniffers, malware, DDoS assaults, bots, etc., as well as the detection and elimination of computer infections.

10. SHUNNING SUSPICIOUS MAILS OR ADVERTISEMENTS- One should avoid to open any mail which looks suspicious to him.

11. REGULAR DATA BACKUP- One should keep information with its back up data to a safe place on regular intervals to secure the information from any cyber-attack or errors in future.

VII. CONCLUSION

E-commerce is still in its early stages today. It indicates that we are rapidly shifting from relying on retail purchases to a culture of internet shopping. People frequently divulge their personal and financial information when engaging in internet activities, and this information can occasionally be easily obtained by unfavorable parties. Therefore, security risks that compromise information security are ever-present. However, we have a wide range of researchers, technologies, tools, and policies to combat these threats, which serve as defense mechanisms or safety for online information as well as protection of individual privacy and autonomy.

REFERENCES

[1]. Moore A., Ellison R., and Linger R., “Attack Modeling for Information Security and Survivability”, Technical Note, CMU/SEI-2001-TN-001, Software Engineering Institute, Carnegie Mellon University, 2001.

[2]. Byres E. and J. Lowe J., “Insidious Threat to Control Systems”, In Tech, Vol.52, No.1, P.28, 2005.

[3]. L. Hyung-Woo L., Pathan A. S. K., and C.S. Hong C.S., “Security in Wireless Sensor Networks: Issues and Challenges”, ICACT, Phoenix Park, 2006.

[4]. Juneja and Gurpreet K. “Use of Modeling Language to Deploy Applications in Clouds.”

[5]. Sen, Santanu K., and D. Sharmistha, “An Investigation towards Security Threats for Cloud Computing.”