Threat, Attack and Vulnerability Play a Key Role in Cyber Security

B Satyanarayana

Assistant Professor, Dept. Of Computer Science, GITAM Institute of Science, GITAM (Deemed to be UNIVERSITY), A. P, INDIA.

---***---

Abstract – *Studying attacks, threats, and vulnerabilities of cyber infrastructure are composed of hardware and software systems, networks, corporate networks, intranets, and uses of cyber intrusions is the purpose of this study. The objective has Finished, the paper attempts to explain the importance of network intrusions and cyber theft. A brightly detailed discussion comprises the reasons behind the rapid surge in cybercrime. The paper also includes a complete explanation and classification of cyber security role-plays in network intrusion and cyber recognition theft, a discussion of the reasons for the growth in cybercrime and their impact. Lastly, the authors mention some measures and solutions to protect cyberspace from attacks, threats, and vulnerabilities. They conclude that even though technology has a role to play in reducing the effects of cyber attacks, we cannot underestimate the impact of cyber attacks on society., the vulnerability exists in While literature supports psychological susceptibilities in humans as dangerous, it is unclear whether psychological susceptibilities are equally dangerous in animals cyber attacks investment in organizational education*

Key Words: *Cyber-Warfare, Vulnerability, Cyber-attack, Threat*

1. INTRODUCTION

In recent times people are going on the digitalization or cashless transaction so multifold. Even the government and defense organizations have experienced significant cyber losses and disruptions. The crime environment in the online community is different from the webspace Because of this, enforcing cybercrime laws is extremely difficult proper space law in any society. If you contrast age in real life with age in the online community, you will find that age in real life is self-authenticating while age in the online community is not. A child under the age of 18 can easily hide his age in Cyberspace and can access the restricted resources whereas in true He would have difficulty securing the information in such a magnetic field. Cyber security involves the prevention, detection, and response to cyber-attacks.

The penetration of computers in society is a welcome step towards modernization but needs to provide keen competition with challenges associated with technology. Some of the advanced techniques for hacking used to penetrate the network, the security vulnerabilities which was not able to identify, it very difficult for the security professionals to find hackers

The defense mechanism is mainly concerned with the understanding of their Defend against future attacks by taking into consideration the network, the attacker, the attacker's inspiration, the attack method, and the network's security weaknesses.

2. Background

present media, Different sectors, and organizations are having hot discussions about The topic of cyber security is over-hyped and artificially inflated by fear-mongering firms, with misleading terms 'cyber-warfare 'In a recent study by Intelligence Squared, a variety of advertisements were designed to evoke an emotional response rather than a rational one. the number of threats like twenty and three, cyber-war has enhanced. Cyber security is the security concept of discussion topic that can inspire independent thinking researchers. In fact, many of those who call for caution suggest this type of discussion security experts.

Rather than lack of government involvement, poor security is the primary cause of many cybercrimes policies implementation. He offers suggestions against requiring Internet users to identify them. These countries are penalized for not complying with attribution requirements, which has led to censorship and international human rights violations. However, whichever perspective one may take, it is evident cyber-security is a very important and current subject that should be discussed.

This paper gives the general or realistic definition of cyber-security for the Information World accepts the concept, but suggests different key elements for activities inclusion.

Technology programs are based on a type of research documents and reports published. Because cyber-attacks are on the rise, governments and security companies all over the world are taking bold and preemptive action to reduce the risk of successful attacks against critical infrastructure . It means the relationship Physique and cyberspace are separate domains. By detecting and responding to incidents related to cyber security, that infrastructure is protected

Government-backed Internet suppression and military strikes on civilians was prevalent with physical actions following prepared the way for cyber-events. Recent cyber-events may be known to IT people Supervisory Control and Data Acquisition (SCADA) systems virus. SCADA malware uses The global financial and physical consequences of these vulnerabilities.

The Comprehensive National Cybersecurity Initiative (CNCI) is an updated national cyber-security strategy for the United States includes the following objectives:

(1)Build a initial sentance of (Cyber) threats of today's immediate nature.

(2) Full spectrum of threats.

(3)Strengthen the future of the cyber-security environment. These goals also underline the Comprehensive National Cybersecurity Initiative.

.Paper work by the Department of Homeland Security suggests that cyber security, which transcends national boundaries, is a global problem requiring global cooperation. No single group, nation, or agency can claim ownership. The report proposes a Roadmap for Cybersecurity exploration. In recognition of the presidential directives cited above, the roadmap draws on the second revision of the IRC's Hard Problem List from 2005 to identify the eleven "hard problems" to be addressed by research and development.

3. Methodology

Despite many changes since the first Symantec Internet Security Threat Report, this edition includes a lot of new information. It includes not only trends in the industry, but also focuses on threats from our research. There is a lot that goes into security, including attack, threat, and vulnerability. These terms are all closely related. One way an attack can be carried out is by exploiting a vulnerability in the system

. For example, if you have a computer with outdated software, it could be vulnerable to viruses and other attacks. This is why it is important to regularly update your computers and anti-virus software.

3.1 Threats :

Cybersecurity threats encompass a wide range of potentially illegal activities on the internet. Cybersecurity threats against utility assets have been recognized for decades, but with the rise of new cyber attacks over recent years commercial power distribution systems are also being targeted by criminal organizations and foreign governments. These attacks can result in massive blackouts that could seriously affect economies and health. The terrorist's attacks so give the attention has been paid to the security of critical infrastructures. Computers that are not secure may lead to fatal disruptions, the exposure of private information, and fraud. Cyber threats result from the exploitation of cyber system vulnerabilities by users with unauthorized access. Some crimes target computer networks or services directly like malware, viruses, or denial of service attacks and Fraud, identity theft, phishing scams, cyberbullying, or other crimes perpetuated by networks or devices that have no connection with those networks or devices, cyberstalking.

a. **Cyber Theft**: This is the most common cyber-attack committed in cyberspace. This one type offense is normally referred to as hacking in the generic sense. It involves using the internet to steal information or assets. It is also called illegal access, by using the malicious code to crack machines or network security beyond user knowledge or consent, for tampering with the complex data .Cyber thieves use methods such as plagiarism, hacking, piracy, espionage, DNS cache poisoning, and identity theft in order to gain access to your information. The Most of the security websites has described the various cyber threats

b. **Cyber Vandalism**: When data is damaged or exploited rather than stolen or misused, then it is called cyber vandalism. It means the effect on network services is disrupted or stopped. This deprives the authorized users of accessing the information contained on the network. Cybercrime such as this can act as a time bomb, causing damage at a precise moment. These are very severe kinds of cybercrime: creating and distributing harmful software that damages computer systems, intentionally inserting malicious code, such as viruses, into a network for monitoring, following, disrupting, stopping, or performing any other action, without the permission of the owner of the network.

C. Web Jacking: Web jacking is gaining access and controlling another website in order to gain control of a web server, intrudrer may be chance control the data on the real space.

d. Stealing cards information: cheating of credit or debit card information by stealing into the e-commerce server.

e. Cyber Terrorism: Use of, or misuse of, the internet and misuse of this information to commit violence against civilians that is usually politically motivated

f. Child Pornography: The act of creating, distributing, or accessing pornographic material sexually exploiting underage children through computer networks

g. Cyber Contraband: sending of illegal items or information through the internet that is banned in some locations, like prohibited material.

h. Spam: It includes the Violation of SPAM Act, through the unauthorized transmission of spam by transfer illegal product marketing or immoral content proliferation via emails

i. Cyber Assault by Threat: The advantages of network such as electronic mails, multimedia objects , or phones for scare People who fear for their own life, the lives of their families, or the welfare of people for whom they are responsible . This is accomplished by blackmailing a person until he is forced to transfer funds to an untraceable bank account through an online payment service.

j.Denial of service: Defeating a denial of service attack or distributed denial of service attack by affecting the availability of the computer resource is known as a denial of service attack (DoS).Due to more requests than the computer can handle, the victim's computer crashes. DoS attacks may vary in their methods, motives, and targets, but they generally involve a person or people trying to halt the functioning of an Internet service or site, for a temporary or indefinite period of time. These are also known as email bombing if via used is email. E-bay, Yahoo, Amazon suffered from this attack

3.2 Attacks

As a result of the effect on critical infrastructure and data, cyber-attacks are a huge problems in the world ,that needs to be addressed. The increase of technology is attend Attacks and threats are difficult to identify, and prevention is not easy. the users are not confirm the new technology due to the frequent cyber-attacks less security of data. A cyber-attack is when someone gains or attempts to gain unauthorized access to a computer maliciously

a. Untargeted attacks: non-targeted attacks in attackers indiscriminately target as users and services as possible. They notice the vulnerabilities of the service or network. The attacker can take the advantage of technologies like Phishing: Phishing means fake people sending emails to several users and asking them for personal information like baking, credit card. They encourage the visits of fake websites and give good offers. The customers open the links on the electronic mails to enter their information, and so they remain unaware that the fraud has occurred.

Water holing: A fake website or dummy site can be published or a legitimate website can be compromised to obtain personal information from visitors.

Ransomware: It is one type of malware, it can spread, disk encrypting extortion malware application.

Scanning: Hacking a wide swath of the Internet at random

b. Targeted attacks: Targeted attacks in attackers, attacks on the targeted users in the cyber world. Email-borne spear-phishing Sends links to malicious software and advertisements containing links for downloads to targeted individuals. Deploying a botnet. It delivers a DDOS (Distributed Denial of Service) attack Subverting the supply chain.

To attack In general, attackers will first probe your systems for a possible vulnerability in the network or software being delivered to your organization.

3.3 Vulnerability

Intruders are capable of executing commands, accessing unauthorized data, and/or striking denial-of-service attacks by exploiting vulnerabilities in systems or designs. Vulnerabilities can be found in a variety of areas in the systems. Weaknesses in the hardware or software of a system, weaknesses in policies and procedures adopted in its implementation, and weaknesses within the system users themselves all contribute to system weaknesses. These weaknesses can be caused by hardware or software failures, policies, and procedures employed by the system, and by the system's users. It is possible to find software vulnerabilities in operating systems, application software, and control software like communication protocols and device drives. Software design flaws are caused by a variety of factors, including human factors and software complexity. Technical vulnerabilities frequently occur due to human weaknesses.

Complacency, negligence, and incompetence all pose risks to systems, and ignoring them has severe consequences. In 2015, an unexpected number of vulnerabilities were identified as zero-day exploits that have been weaponized, and web attack exploit kits are adapting and evolving them more quickly than ever. As more devices are connected, vulnerabilities will be exploited

4. Results and Analysis

Secure the System: There are basically three methods to secure the system from outside threats and attacks. *Prevention*: Security would be achieved by using a firewall, security software, and antivirus software for users. You are doing everything possible to keep the threat out. *Detection*: to be sure you detect when such failures happen. Every day update the infrastructure like security software and hardware.

Reaction: Detect the failure has little value if you cannot respond. If anything it's happens so your security software warns.

4.1Preventing from Attack and Threats

- Recovering from Viruses, Worms, and Trojan Horses
- Avoiding Social Engineering and Networking Attacks
- Avoiding the Pitfalls of Online Trading
- Using Caution with USB Drives
- Securing Wireless Networks

4.2 Preventing from Email and communication

- Using Caution with Email Attachments

- Reducing Spam
- Using Caution With Digital Signatures
- Using Instant Messaging and Chat Rooms Safely
- Staying safe on social Network Sites

4.3 Safe Browsing

- Evaluating Your Web Browser's Security Settings
- Shopping Safely Online
- Web Site Certificates
- Bluetooth Technology

5. Conclusion

Researchers have found that users with computer literacy are the best defense against cyber attacks and it is most vulnerable which are identified in this research as new employees within an organization, as specified, with the attacker seeking personally noticeable data. From those engaged and Further supported in this research are the psychological variables that contribute to the user , network vulnerability. This paper consummate that, while technology has a role to play in reducing the impact of cyber attacks, threat and vulnerability reside with human , impulses behavior and psychological predispositions that can be influenced through education. Despite efforts to reduce cyberattacks, there has yet to be a solution to overcome the threat of cybercrime. The future work of the cyber attack, threat and vulnerability reduction in the network implement the cyber security model.

REFERENCES

1. "Data Protection Using Random Number In Association With ASCII Values", M. Suresh Kumar, G. Babu Rao, International Research Journal of Engineering and Technology (IRJET), Volume: 03, Issue: 06, June-2016.
2. Abomhara, Mohamed, and G. M. Kien. "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks." Journal of Cyber Security 4 (2015): 65-88
3. "Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users" International Journal of Computer, Electrical, Automation, Control, and Information Engineering Vol:9, No:3, 2015
4. "Detection and Prevention of Passive Attacks in Network Security" ISSN: 2319-5967 ISO 9001:2008 Certified International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 6, November 2013
5. Al-Mohannadi, Hamad, et al. "Cyber-Attack Modeling Analysis Techniques: An Overview." Future Internet of Things and Cloud Workshops (FiCloudW), IEEE International Conference on. IEEE, 2016.
6. "Internet Security Threat Report Internet Report "VOLUME 21, APRIL 2016https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
7. Rowe, Dale C., Barry M. Lunt, and Joseph J. Ekstrom. "The role of cyber-security in information technology education." Proceedings of the 2011 conference on Information technology education.ACM, 2011
8. Razzaq, Abdul, et al. "Cyber security: Threats, reasons, challenges, methodologies, and state of the art solutions for industrial applications. "Autonomous Decentralized Systems (ISADS), 2013 IEEE Eleventh International Symposium on. IEEE, 2013
9. . Byres, Eric, and Justin Lowe. "The myths and facts behind cyber security risks for industrial control systems." Proceedings of the VDE Kongress. Vol. 116. 2004
10. "Common Cyber Attacks: Reducing The Impact Gov.UK" https://www.gov.uk/...data/.../Common_Cyber_Attacks-Reducing_The_Impact.pd
11. "CYBERSECURITY: CHALLENGES FROM A SYSTEMS, COMPLEXITY, KNOWLEDGE MANAGEMENT AND BUSINESS INTELLIGENCE PERSPECTIVE" Issues in Information Systems Volume 16, Issue III, pp. 191-198, 2015
12. Ahmad, Ateeq. "Type of Security Threats and Its Prevention." Int. J. Computer Technology & Applications, ISSN (2012): 2229-6093
13. Ten, Chee-Wooi, Chen-Ching Liu, and Govindarasu Manimaran. "Vulnerability assessment of cyber

BIOGRAPHY

Mr. B Satyanarayana
Assistant Professor
Dept of Computer Science,
GITAM INSTITUTE OF SCIENCE
GITAM (DEEMED TO BE UNIVERSITY),
VISAKHAPATNAM