Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 11, November 2019, pg.1 – 6

CYBER SECURITY ISSUES AND CHALLENGES - A REVIEW

Dr. V.Kavitha[1]; Dr. S.Preetha[2]

[1]Professor, Department of MCA, Hindusthan College of Arts and Science
[2]Associate Professor, Department of Computer Science, Sri Ramakrishna College of Arts and Science for Women

Abstract: Cyber security plays a vital role in the discipline of information security. Preventing the information has become one of the major challenges in the current scenario. Cybercrime is one of the significant factors in cyber security, it increased day by day. Numerous governments and private sectors are taking many measures in order to secure these cybercrimes. Handling cyber security is still a very huge concern. This research paper mainly focuses on challenges faced by cyber security on the latest technologies .It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security.
Keywords: Cyber Security, Cyber Crime, Cyber Ethics

I. Introduction

Data communication is playing a major role in today's human life through sending and receiving any form of data like text, image, video or audio files just by click the button but that person don't know whether that message transmitted or sent to the other person safely without any leakage of information. In today's technical environment many recent technologies are belonging to the fast growth of internet technology. But according to these emerging technologies are unable to prevent the private information in a very effective way and hence these days cyber crimes are increasing day by day. Recently, more than 60 percent of total commercial transactions are done through online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a latest issue in the IT sector. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc. The latest technologies like cloud computing, green computing, mobile computing, E-commerce, net banking are required high level of information security.

Cyber crime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cyber crime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cyber crimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually in common man's language cyber crime may be defined as crime committed using a

computer and the internet to steal a person's identity or sell contraband or stalk victims or disrupt operations with malevolent

II. Cyber Security

Cyber security is a term of security which is implicated through diversified disciplines, most of them focusing on technical or psychological problems such as computer science, criminology, economics, engineering, information systems, management, medicare, neurophysiology, psychology, sociology, etc. It afford the people with discussions about behaviours and motivations, benefits and consequences about cyber crime and security.

Cyber security will be used to represent the security issues of information systems:

Cyber security is one of the information system management by individuals or organizations to direct end-users security behaviours, on the basis of personal perceived behaviours toward potential security breach in work and non-work environment. The extant study of cyber security explores three main streams: individual behaviours toward information security in non-work setting, employee behaviours toward information security in work setting, and organization information system security policy (ISSP) compliance and the related issues.

III. Cyber Security Parameters

Cyber security has some of the parameters which are as follows. Figure 1 depicts about the various kinds of cyber security parameters.

- Identify threats
- Identify vulnerabilities
- Access risk explore
- Establish contingency plan
- Respond to cyber security accident
- Establish contingency plan

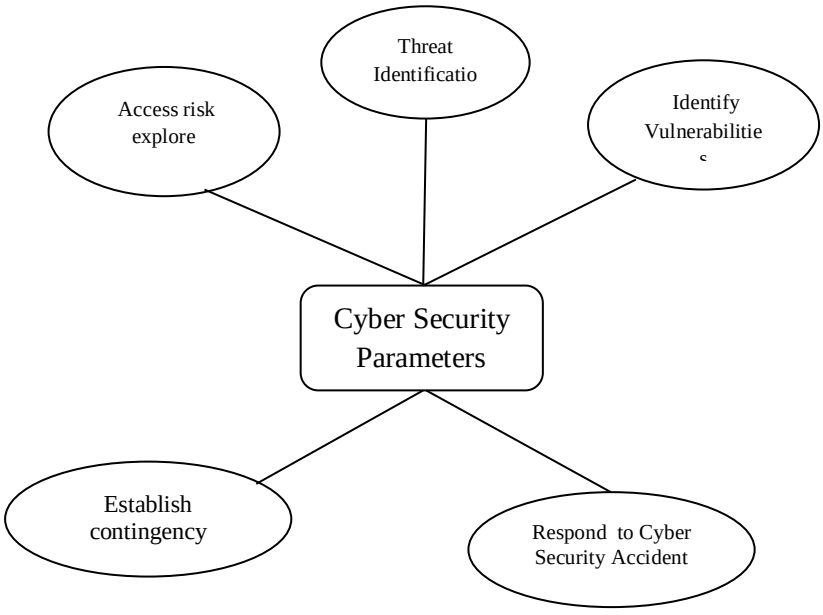

Fig 1 Cyber Security Parameters

IV. Various Kinds of Cyber Attacks

The attacker will expect the procedure to be synchronized in order to contaminate the system. Synchronization of the steps concerned to steal the information directs them to attain what they expect. The hackers will get their result in time, in step and in their line. An organized form of the methods will be used by the attacker or hacker lead to infect the system very easily. The usage of logically organized methods leads them to get more well-organized outputs. The attacks are closely controlled with perfect sequence and in such a way that the resulting damage is severe enough to compromise the working of the organization. Generally various kinds of Cyber attacks available which are listed in the following.

Denial of Service Attacks(DOS)

DOS is one of the attack where an attacker creates a memory resource or computing too full or too engaged to handle legitimate queries, thus denying legitimate user access a machine.

Remote to Local Attacks

A remote to local (R2L) attack is a kind of attack where an attacker send packets to a machine over networks, then exploits the machine's vulnerability to illegitimately increase local access to a machine. It happens when an attacker who has the capability to send packets to a machine over a network but who does not have an account on that machine develops some vulnerability to achieve local access as a user of that machine.

User to Root Attacks

User to root attacks is a kind of attacks where an attacker initiates with access to a moderate user account on the system and is able to expand vulnerability to grow root access to the system in which the attacker starts out with access to a normal user account on the system and is able to exploit some vulnerability to gain root access to the system.

Probing

Probing is another kind of attack where an attacker scans a network to gather information or discover known vulnerabilities. An attacker with map of machine and services that are available on a network can use the information to notice for exploit.

Attacks Detection Strategies

Attacks Deletion Strategies is one of the attack. Modern cyber attack detection systems monitor either host computers or network links to capture cyber attack data.

Signature based Approach

Signature based approach of mishandling discovery works just comparable to the existing anti-virus software. In this approach the semantic description of an attack is analyzed and details is used to structure attack signatures. The attack signatures are structured in such a way that they can be searched using information in audit data logs produced by computer systems.

Misuse/Misbehavior

Misuse (signature) recognition is based on the awareness of system vulnerabilities and known attack patterns. Misuse detection is concerned with discovering intruders who are attempting to break into a system by exploiting some known vulnerability. Ideally, a system security administrator should be aware of all the acknowledged vulnerabilities and eradicate them.

Reconnaissance Attacks

Reconnaissance attacks is the type of attack which involve unauthorized detection system mapping and services to steal data.

Access Attacks

An attack where intruder increase access to a device to which he has no right for access.

Cyber crime

The use of computers and the internet to exploit users for materialistic gain.

Cyber espionage

The act of using the internet to spy on others for gaining benefit.

Cyber terrorism

The use of cyber space for creating large scale disruption and destruction of life and property.

Cyber war

The act of a nation with the intention of disruption of another nations network to gain tactical and military.

Active Attacks

An attack with data transmission to all parties thereby acting as a liaison enabling severe compromise.

Passive Attacks

An attack which is primarily eaves dropping without meddling with the database.

Malicious Attacks

An attack with a deliberate intent to cause harm resulting in large scale disruption.

Non Malicious Attacks

Unintentional attack due to mishandling or operational mistakes with minor loss of data.

Attacks in MANET

Attacks which aims to slow or stop the flow of information between the nodes.

Attacks on WSN

An attack which prevents the sensors from detecting and transmitting information through the network.

V. Cyber Ethics

Cyber ethics are nothing but the code of the internet. Practicing cyber ethics are good chances to use the internet in a correct and protected way. The below are a few cyber ethics one must follow while using the internet.

Ethics 1: To communicate and interact people with each other with the assistant of internet. Instant messages and email make it contact to stay in connect with the family members and friends, share knowledge and information with people among the country with the specific organization and all around the world.

Ethics 2: Internet is measured as world's leading library with information on all the topic in any specific subject area, hence using this information in a proper and legal way is always essential.

Ethics 3: People are not able to operate other persons mail account with their passwords.

Ethics 4: On no account try to send any kind of malware to other's systems and make them fraudulent and damage.

Ethics 5: Do not share the personal details to anyone as there is a good opportunity of other persons mishandling the mail account and finally that person must be in a problem.

Ethics 6: When the person is in online do not pretend to the other person and never try to make any fake account on some other people as it would become a trouble.

Ethics 7: Always adhere to copyrighted information and download games or videos only if they are permissible.

VI. Conclusion

Cyber security is a vast issue that is becoming more essential because the world is becoming extremely interconnected, with networks being used to carry out critical transactions. Security is a very complicated and vital important topic of today's information technology. Everyone has a different idea regarding security policies and levels of risks. The key for building a secure network is to define what security need of the time and use. Once that has been defined, everything that goes on with the network can be evaluated with respect to that policy. Hence security plays a vital role in information security.

Cyber crime continues to deviate down different paths with each novel Year that passes and so does the security of the information. The newest and disturbing technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no proper solution for cyber crimes but using recent techniques to minimize the cyber crime in cyber space.

References

[1] D. Quist and Valsmith "Covert Debugging Circumventing Software Armoring Techniques," Presented at Black Hat USA 2007

[2] A. Sternstein, "Pentagon Disconnects iPhone, Android Security Service, Forcing a Return to BlackBerry for Some," Presented at NextGov, Dec. 3, 2013.

[3] International Telecommunication Union (ITU), "Global Cybersecurity Index (GCI) 2017," 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

[4] Broadhurst, R., & Chang, L. Y. C. (2013). Cybercrime in Asia: Trends and Challenges. In J. Liu, B. Hebenton, & S. Jou (Eds.), *Handbook of Asian Criminology* (pp. 49–63). New York: Springer.

[5] Chang, L. Y. C. (2012). *Cybercrime in the Greater China Region: Regulatory responses and crime prevention across the Taiwan Strait*. Cheltenham: Edward Elgar Publishing.

[6] Etter,B. (2001), The forensic challenges of E-Crime, Current Commentary No. 3 Australasian Centre for Policing Research, Adelaide.

[7] Etter B. (2002), The challenges of Policing Cyberspace, presented to the Netsafe: Society, Safety and the Internet Conference, Auckland, New Zealand.

[8] Eric J. Sinrod and William P Reilly, Cyber Crimes (2000), A Practical Approach to the Application of Federal Computer crime Laws, Santa Clara University, Vol 16, Number 2.

[9] Seamus O Clardhuanin , An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence, Summer 2004, Vol 3, Issue 1. 2004.

[10] International crime and Cyber Terrorism, http://www.dfait-maeci.gc.ca/international crime/cybercrime-en.asp.

[11] Farmer, Dan. & Charles, Mann C. Surveillance nation. Technology Review; Vol. 106, No. 4, 2003: Pp. 46.

[12] Harrison, A. Privacy group critical of release of carnivore data. Computerworld; Vol. 34, No. 41, 2006: Pp. 24.

AUTHORS PROFILE

Dr. V.Kavitha had pursued B.Sc., Computer Science from Bharathiar University in 1998, Coimbatore and Master of Computer Applications (MCA) from Bharathidasan University, Trichy in 2009, Master of Philosophy in Computer Science from Alagappa University, Coimbatore in 2005 and Ph.D in Computer Science from Karpagam University, Coimbatore in the year 2014. Area of research is Data Mining. Serving as a Reviewer and Editor in various International and National Journals. At present working as a professor in the Department of PG and Research Department of Computer Applications (MCA) at Hindusthan College of Arts and Science, Coimbatore-641 028. She published 41 papers in International Journals, presented 40 papers in International Conferences and National Conferences. She has 16 years of teaching experience and 10 yrs of Research experience.

Dr. S.Preetha has received her Ph.D degree in Software Engineering from Karpagam University, Coimbatore in 2015. She has received her M.Phil degree in Computer Science from Madurai Kamaraj University in 2004. She has received her MCA from Sree Saraswathi Thyagaraja College, Pollachi affiliated to Bharathiar University in 2003 and Bachelor's Degree in Computer Science from Vidyasagar college of Arts & Science, Udumalpet affliated to Bharathiar University in 2000. Currently she is with Department of Computer Science, Sri Ramakrishna College of Arts and Science for Women for past 13 years. She has academic experience for 17 years. Her research interests are in Software Testing, Cloud Computing and Big Data. She has published 10 research papers in Journals and presented 25 research papers in National and International Conferences.

