RESEARCH REVIEW JOURNALS
Volume-04
Issue-03
March-2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com[UGC Listed Journal]

Cyber Crime and their Remedies: A Review

*1Monika Rana & 2Prof. Ajit Singh

[1]Student, MTech., Final Year, Dept. of Computer Sciences, BPS Mahila Vishwavidyalaya, Khanpur (India)
[2]Dean, Faculty of Engineering & Tech., & Chairperson, Dept. of Computer Sciences, BPS Mahila Vishwavidyalaya, Khanpur (India)

ARTICLE DETAILS

Article History
Published Online: 13 March2019

Keywords
Cyber crime, cyber security, Cyber attack, Cryptography, Malware, phishing
.

***Corresponding Author**
Email: monikansg[at]gmail.com

ABSTRACT

In this paper the review on cyber crime has been made. Cyber crime involves use of malware, hacking or phishing. Here different researches in field on cyber crime have been discussed. Various cyber crime and cyber attacks are explained here. There are some common attacks. These attacks may be System infiltration, Breach of access, Password sniffing. Along with these attacks, Website disfigurement, exploitation of Private and public Web browser direct abuse in messaging are also some major attacks. The remedies to tackle cyber crime are cyber security. Mechanism such as cryptography is the part of such remedies. The scope of cyber security is also considered in this research.

1. Introduction

The devices are used to progress other ends. For example scam and theft of identity is known as cyber crime. Cyber Crimes use the computer networks. Such activities make use of malware, hacking or phishing.

The Cybercrime Prevention Act of 2012 formally recorded as Republic Act No. 10175. It is a law in Philippines permitted on September 12, 2012. It objective is to highlight the legal challenges the concerning online communications and the Internet in Philippines. Five types of cybercrime are Phishing, Ransom ware, Malware, Identity Theft, Scams.

We can expressed the Cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)". Cybercrime can put the security of person or a nation in danger along with financial health.[4] challenges related to these kind of crimes have formulated itself in high-profile. Hacking and mass surveillance is cyber crime. Pornography and extortion have been considered as ciber crime. There are also issues related to privacy has been occurred when private data has been intercepted or released, it may be legal or illegal. Debarati Halder et al have explained cybercrime with gender viewpoint. He has expressed the cybercrime against women. These crimes are targeting women with a motive to harm them psychologically. It is done with the help of latest telecommunication networks such as internet and mobile phones.[3] at the International level, governmental and non-state actors have their involvement in cybercrimes. These crimes may be espionage, theft in economic, and several limit crossing offenses.

Cybercrimes have crossed the word wide limits. It included actions of country. That is called is cyber warfare.

2. Literature Review

There are several researches to provide security against cyber crime. In this section the related researches have been discussed.

In 2017 T. T. Teoh, et al [1] evaluated the intuition depended hidden markov model on high speed temporal cyber protection huge information.

Determination of time series data is done with the help of invisible Markov Models (HMM) .These models are problematic model. It is found that in fields such as investment, bioinformatics. Research also considered healthcare, farming along with AI.

In 2011 Gregory B. White [2] wrote on community cyber protection maturity model.

Cyber security crack's data has been considered generally in media and protection affairs have their effect on the millions. We are providing a huge attention towards cyber protection. But we are not able to resolve the issues because of the large dependency of sectors on significant cyber infrastructures.

In 2017 Maximilian Frank, et al[3] proposed design determination for cyber protection test beds. That is a case review on cyber protection testbed for education. Instructive test beds have been full-grown for a lot of years. It is possible to make small to medium size test beds at small and medium cost due to the progress of cloud-related storage setting with benefit of memory and storage methodology within the last 10years.

In 2016 Shipra Ravi Kumar,et al [4] suggested the effective cyber protection execution. Nowadays within computer age, the cyber security has been considered a huge challenge. How to secure the networks resources, private information and essential data in any company, it has been highlighted in this paper. The objective is several kinds of cyber threats and their techinque to avoid these types of fear.

Apart from this, the several aspects of cyber crime and its security in the global world have been mention here.

In 2017 Cyril Onwubiko, et al [5] stated security operations centre: situation awareness, threat intelligence and cybercrime.

It is come in to notice that from last few years that cyber security and cyber-threats both are continuously approaching. At present some methods are available to us due to it is possible to identify an individual physically because of the cyber security. These are the methods from which it is possible to capture all the types of electronic communications. Invisible images and information in electronic devices are making visible with help of these methods.

In 2012 Jan Kallberg, et al [6] explained cyber operations. It is the innovative function of academic cyber protection research and education.

The cyber operations shift indicates the defense establishment's worldwide shift. Parallel to this it is also cyber protection research and education.

In the present time all the research and study which is done related to cyber security helps us to provide information in the field of forensics, network protection as well as penetration experiments. All the research and study which is done related to cyber security is associated with homeland safety agencies.

In 2017 T.T. Teoh, et al [7] analyst the intuition influenced the high velocity big data evaluation. That is with the use of PCA ranked fuzzy k-means clustering along with (MLP). It is to prevent the challenges related to cyber security.

Every network user is disturbing because of the emergent occurrence of cyber threats in the world. In order to guard computer networks and resources so that they cannot suffered from cyber-attacks a lot of safety monitoring systems is being in use. An efficient security checking system is urgently required to keep an eye on the hefty network datasets which was achieved as a result of this process.

In 2018 Evgeny Pavlenko, Dmitry Zegzhda , et al [8] discussed the retain ability of cyber and physical environment. It is discussed at contrast of aimed critical effects. A new method is put forward for security appraisal of cyber physical systems by writer in this work. In this work all the safety methods which are utilized by data environment is useless. For cyber physical environment, this has data information along with physical elements.

In 2017 Mahmoud Elfar, et al [9] stated WiP abstract. It is platform for protected design of human-on-loop cyber physical systems.

A human-on-the-loop (HOL) look after one or more independent systems in cyber-physical systems (CPS).Therefore they are usually known as management control systems .Due to the implantation of independence the operators are able to occasionally concentrate to the system and other responsibilities.

In 2014 Luis Parrondo [10] provided his view on industrial cyber security solutions for the connected enterprise"

Safe and appropriate information; associated and available industrial control systems; safety threats; cyber safety; safety principles; defense-in-depth; inheritance control systems; integrated risk management units; and industrial demilitarized zone are the things which comes under the recent presentation.

3. Cyber crime and cyber attack

In this section the discussion of various cyber crimes and cyber attacks are made.

An offense, in which a computer is the main element, is Cybercrime. It has been applied as a device to assign the crime related to child pornography, disgust offenses. The criminals that are Cybercriminals use computer methodology to take confidential data, secrets of business. They take the help of the internet to exploit other people. Computers are applied for transmission and document or data storage by the Criminals. Criminals who do these not legal tasks are called hackers and these types of Cybercrime called computer crime.

Cyber Attack

A cyber attack has been considered the purposeful misuse of computer environment, technical activities with internet. Cyber attacks take help of tough code that changes the code of computer, logic along with date. It cooperates with data and help in cybercrimes. It is also said that it is a computer network attack.

Identity theft, fraud, extortion Malware comes under cyber attacks. Cyber attecks also include the pharming, phishing, and spamming, spoofing, spyware. The Trojans and viruses stolen hardware also come under crime.

These attacks may be System infiltration, Breach of access, Password sniffing. Along with these attacks, Website disfigurement, exploitation of Private and public Web browser direct abuse in messaging are also some major attacks. IP theft with illegal use is also considered as cyber crime.

The Institute for Security Technology performed the researches at Dartmouth University. These researches find out the challenges of cyber attack handling law enforcement searching. It concentrates at regular expansion of intellectual property tracing, data analysis. It also focuses on real-time interception along with national data sharing.

Brute force attack

This attack has been considered hit and trial way which is applied for getting data for example a user password or PIN. With the use of automated software, a huge size of successive presumptions is generated like to value of required information. In Brute force attacks the criminals take the encrypted information in illegal way. These are also used, or by security analysts to check the network security of company.

A brute force attack can explained as brute force cracking. it is also called simply brute force.

In dictionary attack, works with all words exist in dictionary. The other brute force attack can try usually applied letters with numbers arrangement.

This type of attack takes a lot of time as well as resource. So, the success of brute force attack is commonly depended on computing power as well as number of arrangements used more willingly as compare to an ingenious algorithm.

The following measures are applied to prevent the brute force attacks:

1. It is required that the users make complicated passwords
2. There should be time Limit. Thus anyone can't successfully try to log in.

Man in middle

A man-in-the-middle attack that has been considered kind of cyber attack in which any cruel user sets himself/herself into dealing between two users, imitates both sides. With this, he can gain the access of information. This data is that data to which one person wants to transfer to other side.

A man-in-the-middle attack enables a misuse to interrupt, transfer and get the information meant for someone else. It is less supposed for sending at all. It is unknown to outside parson if it is getting not on time. We can reduce the Man-in-the-middle attacks by several methods. These methods include MITM, MitM. Along with these MiM and MIM are also some techniques.

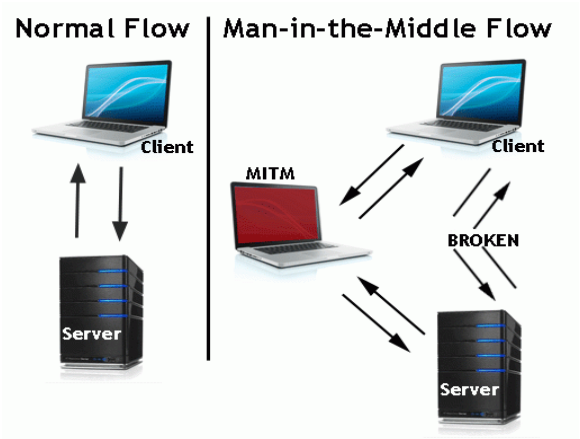

Fig 1 Man in middle attack

Man-in-the-Middle Attack's Key perception:

Man-in-the-middle has been considered as an eavesdropping attack. It kind takes place as a miss user situated him as a relay/proxy into a transmission session in the middle of user and systems.

A MITM attack misuses the real-time processing of communication, discussions or sent related information.

Man-in-the-middle attacks enable the hackers to capture; transfer along with get the information data is useless for them.

Timing Attack

A timing attack is similar to a burglar guessing. It is guessing combination of a safe. It is done by checking how much time it is taking for someone to turn dial. It is checked that RSA algorithm is consuming less time to implements its tasks. It depends on the key value.

Estimate is performed of private key according to duration needed to apply private key to some information.

The importance of this risk increases when an attacker could get to process implementing crypto operation. The attack is not feasible until attacker could monitor the processing duration closely.

Methodology of Timing Attack

A timing attack has been considered as security exploit. It is allowing attacker to find vulnerabilities. It is found in the security system of a network system. It is studied how much time it is taking to respond to various inputs.

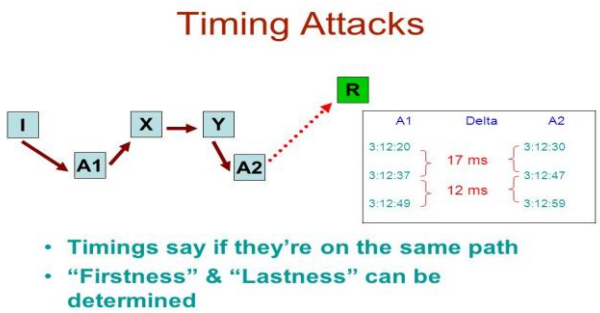

Fig 2 Methodology of Timing Attack

4. Remedies For Cyber Crime

It is required for all the organization whose work are depends upon internet that they make use of various categories of cyber safety and security measures. It is required in order to put a stop on data theft or disruption of business. Therefore at present or in future the business of cyber security specialist is in great demand.

Security is quality of keeping information secure from treats. The security mechanisms are discussed under-

Physical security - In this all the issues in which we need to save physical items. It also protects objects or areas of an organization. Such protection is made from illegal access as well as exploitation.

Personal security - In this all the issues in which we need to protect individual or group of individuals who are sanctioned to access the organization and its operations.

However there are several types of cyber crime in existence and in order to prevent access of useful information the use of cryptography and stenography is made.

Cryptography

Cryptography has been considered the information security science. The word "Cryptography" has been taken from the Greek kryptos. The meaning of this word is hidden.

Cryptography has relation with the cryptology and cryptanalysis obedience. Cryptography involves the methodology lke microdots. It merges the words with graphics. It is another method to secure the information in storage or transportation. Thus, computer-centric world of today, the cryptography is mostly connected with scrambling plaintext into cipher text, and then back again known as decryption. Persons who perform in this sector are described as cryptographers.

Modern cryptography concerns itself with the below given aims:

1. Confidentiality
2. Integrity Non-repudiation
3. Authentication

Stenography

Technology has enabled integration of hidden messages. It is done efficiently and early. Several computerized tools are needed to encode data and hide it. Data is hidden within another file. Stenography is a technique of concealing availability of data within apparently harmless carriers. It adds an encrypted message. Objective is to conceal that the fact that data even exists in first place. The embedded data is information required to be hidden. Data is hidden in the cover. This data could be image, audio, text, or video. Operation is considered integration and cover and embedded information together. It creates the stego data.

5. Scope of cyber security

Cyber security will help in defending from hacking and viruses. The application of cyber security which is installed in our computer needs update every week. The developers also updated their database every week. Therefore new the new virus is self deleted. Cryptography helps in reducing the probability of cyber crime. It would save data from unauthentic use. Thus there is needed to make up gradation in cryptographic algorithms to introduce security against cyber crime. Cryptography includes the formulating written or creating codes. It enables the data security. Cryptography alters the information into a format. That format is not easy to understand for an illegal person. Such systems are not allowing data transmission without unauthorized entities decoding.

Reference

1. T. T. Teoh, Y. Y. Nguwi, Yuval Elovici, N. M. Cheung, W. L. Ng "Analyst intuition based Hidden Markov Model on high speed, temporal cyber security big data"2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD).
2. Gregory B. White"The community cyber security maturity model"2011 IEEE International Conference on Technologies for Homeland Security (HST).
3. Maximilian Frank, Maria Leitner, Timea Pahi"Design Considerations for Cyber Security Testbeds: A Case Study on a Cyber Security Testbed for Education"2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech).
4. Shipra Ravi Kumar, Suman Avdhesh Yadav, Smita Sharma, Akansha Singh "Recommendations for effective cyber security execution" 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH).
5. Cyril Onwubiko"Security operations centre: Situation awareness, threat intelligence and cybercrime"2017 International Conference on Cyber Security and Protection of Digital Services (Cyber Security).
6. Jan Kallberg, Bhavani Thuraisingham "Towards cyber operations - The new role of academic cyber security research and education"2012 IEEE International Conference on Intelligence and Security Informatics.
7. T.T. Teoh, Yue Zhang, Y.Y. Nguwi, Yuval Elovici, W.L. Ng "Analyst intuition inspired high velocity big data analysis using PCA ranked fuzzy k-means clustering with multi-layer perceptron (MLP) to obviate cyber security risk"2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD).
8. Evgeny Pavlenko, Dmitry Zegzhda "Sustainability of cyber-physical systems in the context of targeted destructive influences" 2018.
9. Mahmoud Elfar, Haibei Zhu, Adithya Raghunathan, Yi Y. Tay, Jeffrey Wubbenhorst, M. L. Cummings, "WiP Abstract: Platform for Security-Aware Design of Human-on-the-Loop Cyber-Physical Systems" 2017.
10. Luis Parrondo "Industrial cyber security solutions for the connected enterprise" 2014.

