A Study on Increasing Cyber Crimes on Internet

Kavita Manikrao
Bidar, Karnataka State ,India
Email id: kavi_sachhi@yahoo.co.in

Sachhidanand
Asst .Professor,
Dept. of Computer Science,
Govt. First Grade College, Aurad(B), India.
Email id: sachhi.r@gmail.com

Abstract: The facilities of computer technology have not come out without drawbacks. Even though it makes the life so fast and speedy but hurled under the eclipse of threat from the deadliest type of criminality termed as 'Cyber crime'. Cyber-crime involves the breakdown of privacy and damage to the computer system properties such as files, website pages or software. So, it is required the deep knowledge about the cyber –crime and it prevention dependencies on internet for small task is increasing so that more use of internet inviting different kind of criminal activities. If the crime increases then it is also possible to find out many possible solutions. In this paper we describe the detail of various crime aspects, effect and prospects of this cyber-technology and threat poses of cyber crime. Efforts have been made to analyze the availability of legal framework. Here, the numbers of cyber crime activities are studied and tried to alert the current internet users who are willing to do some unusual activities over the internet.

Keywords: *Cyber Crime, Computer Forensics, Cyber Security, SQL Injection, Phishing*

*****

1. Introduction

Crime is a legal concept and has the sanction of the law. An offence or crime is a legal wrong that can be followed by criminal proceedings which may result into punishment. Cyber crime can be defined as any criminal act dealing with laptop, computers, networks and server. Additionally, such crimes is also includes traditional crimes conducted through the Internet. Internet is increasingly being used for communication, commerce, advertising, banking, education, research and entertainment. It has become a place to do all sort of activities which are prohibited by law. It is increasingly being used for fraud ,trafficking in human organs pornography, gambling, and prohibited drugs, hacking, infringing copyright, terrorism, violating individual privacy, money laundering, , software piracy etc..

1.1 Computer Forensics

Computer forensics involves the identification, extraction, preservation, interpretation and documentation of computer data. Computer forensics (sometimes known as computer forensic science) is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. Its goal is to examine digital media in a forensically sound manner with the aim of identify, preserve, recover, analyze and present the facts and opinions about the digital information.

Computer forensics is similar to the field of forensics. Analyzer use the science of forensics to hunt a crime scene for evidence of what happened, by whom it happened, and who did what to whom.[1]. Although, it is most often associated with the investigation of a wide variety of internet crimes. The computer forensics may also be used in civil proceedings and the discipline involves similar techniques and principles to data recovery but with additional guidelines and practices designed to create a legal audit trail. The evidence from computer forensics investigations is usually subjected to the same guidelines and practices of other digital evidence. This has been used in a number of high-profile cases and is becoming widely accepted as reliable within U.S. and European court systems.[2]

The following are the major components of Computer Forensics. Firstly, Identifying the Crime, Secondly, Detecting the cause, Then Preserving, Analyzing and then Presenting.

Increasing use of laptops, smart phones and internet are playing a big role in increasing cyber crimes.

International trends have shown that there is an exponential increase in Cyber Crime with an increase in the availability of technology.

1.2 How Cyber Crime is Increasing

Most of the techniques of hacking is directly available on internet for study purpose. But the users are misusing of such facility.

- Easy to Access
- Negligence
- Complex
- A cleaver user can easily erase evidence

2. Classification of Cyber Crime Activities

The Cyber crime may be broadly classified under the following categories.

- **Targeting Individual**

  - Phishing Emails and Web forms
  - Installing adware's via Scripts
  - Internet time Thefts
  - URL redirection
  - The Email spoofing

- **Targeting Organizations.**
  - Unauthorized access and control over Server and Computers.
  - Leaking Company Information

Phishing have been tackled to a good extent by informing genuine users of the perils of publishing their confidential information to unauthorized information seekers. .The phishing Websites are those which shows you the exact snippet of the targeted site with a similar name. The content of e-mail often directs the consumers to the fake website in order to lure them to fill their personal information such as credit card or bank account's details. This technique is called phishing. In the Identity theft**,** people can easily store and access the personal information on the Internet. But, it's also easy for people to obtain this information illegally. This is identity theft, stolen information like name, dob, address and account number that can be used to commit fraud. Wire transfer is one of the safe way to move money around. A spoofed e-mail may be said to be one, which misrepresents its origin. And it shows its origin to be different from which actually it originates. Cracking is the most common cyber crimes known till date. Suppose a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information. Assault by Threat is refers to threatening a person with fear for their lives through the use of a computer network that is E-mail, mobile phones etc.

There are some other ways of hacking any information or hacking a computer system. Normally attackers attract users by providing misleading information via Fake Lottery, porn sites & Url Redirections etc. Some of the hacking modes are shown in the figure below:

The most popular hacking modes are:

- Hacking
- Cyber Terrorism
- Information Theft
- E-mail Bombing
- Web Jacking
- Phishing
- Denial of Service Attack
- Web Jacking
- Trojan Attacks
- Child Pornography
- Online Gambling

3. SQL Injection

SQL injection has become a predominant type of attacks that target web applications. It will allow the attackers to obtain unauthorized access to the database to change the intended application-generated by the SQL queries. The attacks may vary from gathering of sensitive data to manipulating database information and from executing system-level commands to denial of service of the application. The impact also depends on the database on the target machine and the roles and privileges the SQL statement runs with.

Researchers generally divide injection attacks into three categories:

SQL injection attacks do not have to return data directly to the user to be useful. "Blind" attacks (for example, that create a database user, but otherwise return no data) can still be very useful to an attacker.

SQL Injection Attacks (SQLIAs) have known as one of the most common threats to the security of database-driven applications. So there is not enough assurance for confidentiality and integrity of this information.[3]

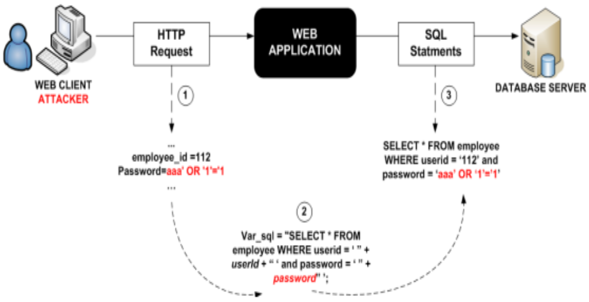
WEB CLIENT
ATTACKER
HTTP Request
WEB APPLICATION
SQL Statments
DATABASE SERVER
1
...
employee_id =112
Password=aaa' OR '1'='1
...
2
Var_sql = "SELECT * FROM employee WHERE userid = ' " + userId + " ' and password = ' " + password" ';
3
SELECT * FROM employee WHERE userid = '112' and password = 'aaa' OR '1'='1'

Fig. 1 Example of a SQL Injection Attack[3]

4. Cyber Crimes in India

Crime is both a social and economic phenomenon. In India , security initiatives to be taken by the rulers, possible crimes and also advocates punishment for the list of some stipulated offences. But, the following figs shows the figures about the crimes.

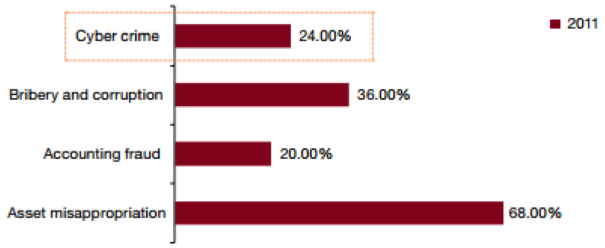

Fig. 2 Top economic crimes experienced by organization in india[4]
Source: National Crime Record Bureau

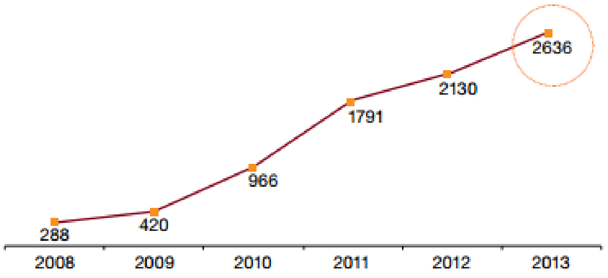

Fig. 3 Number of cyber crime cases registered under the IT Act [4]
Source: National Crime Record Bureau

5. Information Technology Act 2000

Information technology is one of the important law relating to Indian cyber laws. It had passed in Indian parliament in 2000. This act is helpful to promote business with the help of internet. It also set of rules and regulations which apply on any electronic business transaction. Due to increasing crime in internet, Govt. of India understood the problems of internet user and for safeguarding the interest of internet users, this act was made. The Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature and also further states that any person can verify an electronic record by use of a public key of the subscriber.

6. Prevention for Cyber Crimes.

Although there are Cyber Crime Security experts to handle criminal activities over the internet, but still there are some ways you can use that will make less possibility your likelihood of attack. The below mentioned security guidelines and good practices may be followed to minimize the security risk of Cyber crime:

a) By updating the computer
b) By choosing strong passwords
c) By protecting computer with security software
d) Shield personal information
e) Review bank and credit card statements regularly
f) Be Social-Media Savvy
g) Secure Mobile Devices
h) Secure wireless network[5]

7. Challenges Faced in Cyber Crime.

In the past decade, advances in communications technologies and the "informatization" of society have converged as never before in human history. The government is actively focused on fighting and preventing cyber criminals from damaging infrastructure, the very nature of cyberspace poses a number of challenges to the implementation of cyber regulations in any country

- Attacker always tries to break the security where the other one tries to secure network.
- Leaking information or attacker are more dangerous than a hacker from outside.
- The encryption is not making life simpler.
- Inadequate in-house manpower or skills to investigate/examine.
- Feeling no one can hack us is the open invitation to hackers.

8. Conclusions

Nowadays cyber crime is the most concerning issue for all developed and developing countries because it harms governmental confidential data as well as people in daily life transactions. Due to immense increase in the use of Internet and dependency of individuals in every field, a number of new crimes related to internet have evolved in the society. Hence it can be said that technology is growing day by day. Along with this growth the hackers are also trying to find out loop holes in the functionality of technology. Even handling cyber crime is tough but not impossible.

References

[1] Mayank Saxena," A Review of Computer forensic & Logging System", January 2012
[2] https://en.wikipedia.org/wiki/Computer_forensics
[3] Atefeh Tajpour," Web Application Security by SQL Injection DetectionTools", Mar 2012.
[4] Cyber crimes on the rise, Crime in India report 2007-2011, (National Crime Record Bureau)
[5] Vineet Kandpal," Latest Face of Cybercrime and Its Prevention In India",2013.