ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

Cyber Crime: Prevention & Detection

Ms M Lakshmi Prasanthi[1], Tata A S K Ishwarya[2]

Associate Professor, CSE Dept.,Vardhaman college of Engineering,Shamshabad,Hyderabad, Telangana, India[1]

Student, M.Tech CSE Dept., Vardhaman college of Engineering, Shamshabad, Hyderabad, Telangana, India[2]

Abstract: Cybercrime is a complex and ever changing phenomenon. Cyber criminals are becoming more sophisticated and are targeting consumers as well as public and private organizations. Therefore, additional layers of defense are needed. Cyber crime has been increasing in complexity and financial costs since corporations started to utilize computers in the course of doing business. Some of the case studies of cyber crime include Parliament attack case. In this paper we have discussed about Cyber crime and cyber security and different cyber crimes that we come across and prevention techniques and detection techniques such as Tripwires, configuration checking tools, Honey Pots, anomaly detection system and operating system commands. In this we also discuss about regulation acts imposed against Cyber crime and also online safety tips.

Keywords: Cyber Crime, Cyber Security, Honey pots, Trip wires, Anomaly detection, Case Study, Regulation Acts, Online safety tips

1. INTRODUCTION

"Ever since men began to modify their lives by using technology they have found themselves in a series of technological traps".

One of the best example for technological trap is cyber crime.

Cyber crime also referred as computer crimes, electronic crimes or e crimes. "Cyber " is short for "cyber space". The electronic medium of computer network. In which online communication takes place.

"Cyber crime is regarded as computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. Cybercrimes describe criminal activity in which the computer or network is a necessary part of the crime". cyber crime was broken into two categories and defined thus:

1. Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.
2. Cybercrime in a broader sense (computer-related crime): Any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network

2. ORIGIN OF CYBER CRIME

It is believed the first recorded cyber crime took place in the year 1820.This can be true with the fact that, computer did exist since 3500 BC in India, China and Japan.The modern computer began with the analytical engine of Charles Babbage

3. CYBER SECURITY

A crime such as spamming, passing on computer viruses, harassment, cyber stalking, and others have become common in our modern world. While these issues do not carry potential monetary loss, they are just as harmful in the possibility of losing files, information and access to your computer. This is why Cyber Security is needed.

Cyber security means protecting information, equipment, devices, computer, computer resources, communication device and information stored therein from unauthorized access, use, disclosure disruption, modification or destruction.

Why Cyber Security?

Computer security is important because it can provide the opportunity for the users to protect their important information present on the network and also in the system (right to privacy).

It also helps in defending the computer system against different types of destructive technologies and protects the PC from damage (viruses, worms, bugs and bacteria).

It also helps in monitoring the network and protects it also from different threats. So, we should use computer security solution on some level to protect our data from different type of sniffing stolen problem.

In general, Computer Security is vital for protecting the confidentiality, integrity, and availability of computer systems, resources, and data.

Without confidentiality, trade secrets or personally identifying information can be lost. Without integrity, we cannot be sure that the data we have is the same data that was initially sent (i.e., Altered data).

Without availability, we may be denied access to computing resources (i.e., A virus that disables your keyboard and mouse).

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

4. DIFFERENT TYPES OF CYBER CRIMES

Financial	Using fake websites to market products so as to get the credit Numbers
Marketing Strategies	Selling narcotics or weapons online
Intellectual Property	Software piracy, copyright infringement, trademark violations, theft of computer code
Email spoofing	Hacking email/password; sending unwanted message to others ruining a person's image
E-Murder	Manipulating medical records
transfer fraud	hackers intercept them and divert the funds
Hate/commercial	Building a website to promote hate or racial hate.
Altering websites	deleting web pages, uploading new pages; controlling messages conveyed by the website

5. ELECTRONIC CRIME DETECTION

Typically electronic crimes are detected by one or more types of intrusion detection techniques. Such techniques include

- Tripwires;
- Configuration checking tools;
- Honey pots;
- Anomaly detection systems; and
- Operating system commands.

Brief overview of each of these intrusion techniques follows:

5.1 Tripwires: snooping

Tripwires are software programs that take snapshots of key system characteristics which can be used to detect critical file changes.

In this regard, tripwires provide evidence of electronic crimes because most of the intruding hackers make modifications when they install backdoor entry points or alter file system and directory characteristics unknowingly while snooping.

5.2 Configuration checking tools

Configuration checking tools are also called as vulnerability assessment tools, referred to a software programs used to detect insecure systems. though configuration checking tools are primarily preventive in nature, they use as monitoring devices can also provide evidence regarding electronic crimes.

Specifically, configuration checking tools can be particularly useful in detecting suspicious patterns of system misconfiguration that might be malicious in nature. Admittedly further investigation will be necessary to determine if a system misconfiguration is an electronic crime.

5.3 Honey pots:

Honey pots or Honey pot lures are employed to entrap and keep an electronic criminal occupied long enough to allow for identification and even apprehension of the preparatory.

These lures can be bogus system administration accounts, fictitious product or client information, or a myriad of created files that appear to contain sensitive information. In addition to facilitating perpetrator identification, honey pots also store the evidence of the electronic crime itself.

5.4 Anomaly detection systems:

Anomaly detection system focus on unusual patterns of activity. In essence, anomaly detection systems develop and analyze user profiles, host and network activity, or system programs in hopes of discovering deviations from expected activity.

Unusual key stroke intervals, abnormal commands, and unconventional program activities can provide evidence regarding the existence can provide evidence regarding the existence of an electronic crime.

5.5 Operating system commands:

Intrusion detection is also possible through the use of certain operating system commands, for example checking log files and comparing outputs of similar programs are among the numerous manual techniques involving operating system commands. Typically these commands are used on daily bases by system administrators to search for evidence suggesting the possibility of electronic crimes.

6. PREVENTIVE MEASURES TO OPPOSE CYBER CRIME

Reduce Opportunities	Reduce Opportunities to the Criminals Develop elaborate system design so that hacker does not hack the computer
Use Authentication Technology	Use password bio-metric devices, finger print or voice recognition technology and retinal imaging, greatly immense the difficulty of obtaining unauthorized access to information systems. Attention to be paid to bio-metric technology as this recognizes the particular user's authentication for using the particular computer
Lay a trap	Bait a trap to catch the attacker in our computer.
Develop New Technology	Develop Technology of encryption and anonymity and also for protecting infrastructure as hackers or cyber terrorists can attack over any nation's infrastructure resulting in massive losses
Understand Cyber	For volume, impact and legal

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

Crime	challenges. Understand the benefit of proper equipment training and tools to control cyber crime
Think about Nature of Crime	Computer crime is diverse, a deep thought to be given, what cyber crime can take place in one's particular organization, so that different types of monitoring/security system can be designed and proper documentation can be written for security system
Adopt Computer Security	Avail new sophisticated products and advice for computer crime prevention which is available free or paid in the market
Use Blocking and Filtering Programs	For detecting virus, since virus can identify and block malicious computer code. Anti Spyware software helps stopping the criminals from taking hold of one's PC and helps to cleanup the PC if the same has been hit.
Monitoring Controls	Separate monitoring to be done for (a) Monetary files (b) Business information
Design Different Tools	For different needs rather than using one particular tool
Data Recovery	Develop tools for data recovery and analysis
Reporting	Always report the crime to cyber fraud complaint center in one's country as they maintain huge data and have better tools for controlling cyber crime.
Educate Children	Children should be taught about the child pornography crime used by criminals and how to avoid that
Design Alert Systems	Design the alert system when there is actual intrusion
Install Firewalls	(a) As they block particular network traffic according to security policy. (b) Patches are generally installed automatically and automatically fixes the software security flaws.
Install Original Software	As they contain many security measures. Pirated softwares do not contain many security abilities which exist in the original software.
Online Assistance	Develop regular online assistance to employees. Learn Internet to one's advantage only and understand all tips to stay online safe
Avoid Infection	Avoid infection rather than cleaning it afterwards Keep browser upto date for security Measures
Avoid bogus Security Products	As many anti-spyware activists' runs a website that list bogus security products. Read the license agreement before installing any program
Attachments	Avoid opening attachments or e-mails which were not expecting and have come from unknown source or person
Cross Check	Cross check regularly the statements of financial accounts and internet banking

Few Online safety tips:

1) Protect yourself from viruses by installing anti-virus software and updating it regularly. You can download anti-virus software from the Web sites of software companies, or buy it in retail stores; the best recognize old and new viruses and update automatically.

2) Don't open a file attached to an e-mail unless you are expecting it or know what it contains. If you send an attachment, type a message explaining what it is. Never forward any e-mail warning about a new virus. It may be a hoax and could be used to spread a virus.

3) Confirm the site you are doing business with. Secure yourself against "Web-Spoofing". Do not go to websites from email links.

4) Create passwords containing atleast 8 digits. They should not be dictionary words. They should combine upper and lower case characters.

5) Send credit card information only to secure sites.

6) Never give out your address, telephone number, hangout spots or links to other websites or pages where this information is available

7. CYBER CRIME CASE STUDY

1) PARLIAMENT ATTACK CASE

Details about incident:

a) The top cyber cases, including analysing and retrieving information from the laptop recovered from terrorist, who attacked Parliament.

b) The laptop contained several evidences that confirmed of the two terrorists' motives, namely the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and the the fake ID card that one of the

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

two terrorists was carrying with a Government of India emblem and seal.
c)The emblems (of the three lions) were carefully scanned and the seal was also craftly made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop.

8. DIFFERENT LEGAL ACTS AGAINST CYBER CRIME

"There can be no peace without justice, no justice without law and no meaning law \without a Court to decide what is just and lawful under any given circumstances".

Benjamin B. Ferenez

Once Mahatma Gandhi, argued that,
"We get the Government we deserve. When we improve, the Government is also
bound to improve"
It is the duty of the government to ensure that its laws cope with the development of science and technology, and fully participate in the legislative enactment

- The India Information Technology Act of 2000.
- The Philippines Electronic Commerce Act No 8792 of 2000
- The Philippines Cybercrime Prevention Act of 2012 No. 10175
- USA Cyber Intelligence Sharing and Protection Act of 2011 (CISPA).
- USA Cyber Security Enhancement Act of 2009 (S.773).

8.1 Important Cyberlaw Provisions in India

Offence	**Section under IT Act**
Tampering with Computer source documents	Sec.65
Hacking with Computer systems, Data alteration	Sec.66
Publishing obscene information	Sec.67
Un-authorized access to protected system	Sec.70
Breach of Confidentiality and Privacy	Sec.72
Publishing false digital signature certificates	Sec.73

NOTE: Sec.78 of I.T. Act empowers Deputy Superintendent Of Police to investigate cases falling under this Act.
Computer Related Crimes Covered under Indian Penal Code and Special Laws

Offence	**Section**
Sending threatening messages by email	Sec 503 IPC
Sending defamatory messages by email	Sec 499 IPC
Forgery of electronic records	Sec 463 IPC
Bogus websites, cyber frauds	Sec 420 IPC
Email spoofing	Sec 463 IPC
Web-Jacking	Sec 383 IPC
E-Mail Abuse	Sec 500 IPC
Online sale of Drugs	NDPS Act
Online sale of Arms	Arms Act

CONCLUSION

The internet is very powerful tool and effective means of communication but it is vulnerable just like anything else. To defend against Cyber crimes, intrusion detection techniques should be designed, implemented, and administrated. The way to protect it for now is for everyone to be smart and to follow preventive measures, individuals, institutions, and government alike should all follow these measures.

REFERENCES

[1] http://www.infosecwriters.com/text_ resources/pdf/BPlad na_Cybercr ime.pdf
[2] http://www.itu.int/osg/spu/c ybersecurity/docs/Background_Pa per_Comparative _Analys is_Cyb ersecurity_Initiatives_ Worldwid e.pdf

Internet Resources
[1] http://en.wikipedia.org/ wiki/Security
[2] http://en.wikipedia.org/wiki/Data_ security
[3] http://en.wikipedia.org/wiki/Information_security
[4] http://en.wikipedia.org/wiki/Computer_ security
[5] http://www.cyberlawclinic.org/casestudy. asp
[6] http://www.cyberlawsindia. net/cases.html