Strategies of Cybercrime: Viruses and Security Sphere

K. Ganeshkumar*, D. Arivazhagan and S. Sundaram
Dept. of Information Technology, AMET University, Chennai, India
ganesheclipse@gmail.com*; +91 9790525505

Abstract
Cyber security is a major branch of computer technology covers all computer based equipment. The objective of computer security is protecting the system data from unauthorized access, change or destruction. Cyber security may be categorized in to eight spheres. Each and every security sphere has a separate mechanism to protect the system data. Nowadays cybercrime is becoming an emphasis issue even through it is impossible to eliminate from the globe but we can reduce the impact. Virus is the major part of computer security. Virus may have single line code or multiple pages and make small impact of our computer security. Cybercrime is not only a big crimes like transferring money and steeling data, it could include the wrong person using the computer technology to making wrong things. For an example, the google earth is the technology to provide the real map image of the world and it may be accessed by the thief or the terrorist to access the way of particular bank or organization which is a cybercrime. When, we focus on the huge evolution of computer network there are so much amount of algorithms, encryption techniques and antiviruses, unfortunately the latest technologies fail to protect the system security. The defense mechanism of computer security is still to be evolved to protect the system data. This review has active and passive attacks used by cyber criminal and focused on the evaluation of cybercrime and the need of high defense mechanism to protect them from cybercrime.

Keywords: Cyber security, cybercrime, viruses, system data, computer technology, system security.

Introduction
Every sector in the world relies on computer and internet, for example Communication (E-mail), Entertainment (Mp3, Video), Shopping (online stores, credit cards), Medicine (Medical records, treatment methods) etc. Today computers with neural networks and nanocomputing are promising to turn every single atom in a human body in to computer software, but even internet has some disadvantages (Ravisharma, 2012). Sometimes the disadvantages are more compared to advantages. The disadvantages includes attacks against a computer data, systems identity theft, hacking the penetration of online financial services and the deployment of virus and various email scams such as phishing. Cybercrime is a criminal activity done using computer and the internet and first cybercrime was recorded in 1920. While on the discussion of cyber crime, here we use a new term called ‘cyber space’ coined by William Gibson (Ravisharma, 2012). Cyberspace directly denotes the computer network place in which online communication takes place. For example, after sending an E-mail to your friend you could say you sent the message to him through cyber space (Hu et al., 2005). In effect, cyberspace can be thought of as the interconnection of human beings through computers and telecommunication without physical or geographical barriers. The next section of the review discusses about the strategies of cybercrime.

Strategies of Cybercrime
Cybercrime is one of the fastest growing areas of criminology. Most of the cybercrimes are performed by individuals or small group of people. Some large crime groups also take advantages of the internet and this kind of criminal communities share computer viruses like ‘Trojan horse’ across the internet for stealing (Mehra and Pateriya, 2013). Cracking the criminals is very difficult because the internet makes it easy for people to do this anonymously. The major crime in cyber space is spreading computer virus for accessing others and in fact every computer is vulnerable. A potent virus transmits from one system to another to corrupt or delete the data. Generally, the computer attacked by viruses face the following problem.

- Find address books and sends unwanted messages to all the address.
- The most common thing is to destroy the data.
- Disable printing in fact it can cause your computer to fail completely.

Most of the time, the viruses are spread by attachments of E-mail and by large community forwards. It can come attached with images, greeting cards, audio files and video files etc. (Joshi and Patil, 2012). Virus can also be inherited through downloading software on the internet and operating a pen drive or other detachable hard drivers (Olusegun and Ithnin, 2013).
Once our system infected by viruses it cannot be removed fully, removing the virus is better than preventing the virus infection. Here, we are displaying a small virus program in batch file which can shut down our system within 5 sec after opening the system (Anderson, 2001).

"@echo off
Attrib –h –v –s c:\htldr
Ren c:\htldr dhcwe691ldr
Shutdown.exe –r -f -t 05
Exit"

This virus program invokes the code to shutdown in operating system within 5 sec. Next, we see another virus that make our system always turn on the caps lock mode and this virus made by VB script file (Ning, 2007).

“Set wshshell =wscript.createobject("wscript.shell")
Do Wscript.sleep 100
Wshshell.sendkeys"[(CAPSLOCK)]"
Loop”

This two are the very small virus programs that do not make a huge impact on the computer systems. However, there are many viruses of nuisance value. The next section of the review will give an account on how to avoid viruses.

**How to avoid Viruses?**
The first method of avoiding virus is using a firewall. It is similar to locking the front door of our house. It will help to keep out the intruders (Anthony et al., 2006). The second most common thing is using the proper antivirus software to protect our computers from virus, spyware and other unwanted software. It is available as a free download from internet. If we can download programs from safe websites, it will avoid the spyware. Before downloading, the user must read all security warnings and license agreements (Brav et al., 2000). Always use a guest or any normal user account to login the system to avoid automatic downloading of bad software from internet.

**Wired and Wireless Network**
In the networking environment, wireless communication brings a tremendous change and facilitates user mobility (Brealey and Myers, 2000). People are mostly using wireless networks, so the cyber crime activities are more in the wireless networks. The basic technology in the wireless network system is wireless access points (Brealey and Myers, 2000). It is a hardware that enables data communication between wired and wireless network, incidentally, it must be borne in mind that the wired network is the backbone of wireless networks. In comparison of wired network to wireless network, the wireless network is most vulnerable to attacks (Campbell et al., 2003).

If we are deploying a common firewall to separate the wireless and wired network, it can be easily cracked by the cyber criminals.

**AD-HOC MODE:** It refers the wireless devices directly communicating with each other without involving the central access points. However, this topology can’t scale for large networks. It is staying from lack of security features like MAC filtering and access control (Cavusoglu et al., 2004).

**Cyber Security Spheres**
The ultimate aim of the cyber security is to maintain the integrity, keeping safe of confidentiality and persuade availability of the information system with reference to such security requirements (Cooper et al., 2005).

**Connection control:** The organization provides the connection control to rightful users to prevent unauthorized users from retrieving or altering the information (Santos et al., 1993). The connection controls are done with 3 mechanisms namely Preventing, Detecting and Corrective mechanisms.

**Connection control process:**

<table>
<thead>
<tr>
<th>Description (Who are you?)</th>
<th>Certification (Prove it)</th>
<th>Endorsement (Permission)</th>
<th>Computing (What are you doing?)</th>
</tr>
</thead>
</table>

Description is an assignment of a unique user id and certification is the process of proving a user identify before entering a system. The user access privileges are based upon some certification like PIN and Password (Ettredge and Richardson, 2003). Computing is the final step in this process including audit control.

**Media communication and cloud security:** Media communication is the most technical domain in the world. It has the IP address and various structures of a network. Media communication has so many methods to communicate, so many formats to transporting data hence, it has the major issues (Fama and French, 1993). This domain issues regarding confidentiality, integrity and availability in cloud security, firewall services, fault tolerance and data availability.
Websites and web development security: In the current situation, cyber attacks directly focused on websites rather than network attacks. One of the survey reports of 2009 revealed more than half of the attacks happen in only websites. Generally, developing and installing software has major domain experts such as planning experts, design experts, installation experts etc., but none for security aspects (Franks et al., 2011). Generally, the developer takes care of security by default. It is essential to increase the security experts at the development of software.

Cryptanalysis: Cryptanalysis is the most common security providing technology over the network. This domain ensures the information which is going to be transferred. It is commonly referred as encryption and decryption (Garg et al., 2003). We are using two types of cryptanalysis, one is symmetrical and asymmetrical. Symmetrical uses the same private key or secret key to encrypt and decipher the message (Gatzlaff and McCullough, 2008). Asymmetric uses two different keys, a private key and a public key, the public key to encrypt and private key to decrypt. The process of encryption and description is given below:

- Normal text message “the cyber law”
- Encryption using algorithm
  - [Private key(for symmetrical)
  - Public key(for asymmetrical)]
- Chipper text[Encrypted message] ["h37fkhDF8d3kF"]
- Decryption algorithm
  - Private key(symmetric and asymmetric)
- Plain text message ["the cyber law"]

Activity security: This sphere implements proper controls and keep safe on hardware and other resources (Gordon and Loeb, 2002). Activity security focuses on controlling proper auditing, calculating threats to security and vulnerabilities (Ramot et al., 2003). This involves writing a tailor model security for a limited hardware and software. There are number of controls that are given below.

- Physical layer security: Physical and coincidental threats may have been identified using a hazard vulnerability assessment. Coincidental security must be monitored and noticed around electrical power, humidity, fire detection and ventilation (Lin et al., 2009).

Proposal for Business continuity and Disaster restore: This domain provides two types of proposal
- Proposal for Business continuity
- Proposal for Disaster recovery

The two proposals are nearly same but have some difference. Business proposal contains process assessment and approval of business. Disaster recovering proposal aids the organizations in making critical decision and guiding action in the event of a disaster.

Act, analysis and conventions: Security professionals must understand the Act of the land pertaining to information security, the types of computer crimes that can be committed and the issues unique to analysis a computer crime, such as the legal way to collect, monitoring and keep evidence.

Classification of Cyber attacks
Cyber criminals use many methods and tools to locate the vulnerabilities of their target. The target may be an individual or organization. Cyber attacks are classified into two types namely active attacks and passive attacks. Active attacks are usually used to alter the system whereas passive attacks attempt to gain information about the target. Active attacks may affect the availability, integrity and authenticity of data whereas passive attacks lead to breaches of confidentiality, in addition to the active and passive categories, attacks can be categorized as inside or outside attacks (Hovav and D'arcy, 2004). An attack originating and or attempted within the security perimeter of an organization is an inside attack, usually attempted by an insider who gains access to more resources than expected. An outside attack is attempted by a source outside the security perimeter, which is indirectly associated with the organization attempted through the internet or a remote access connection.

Passive attacks: Some tools used during passive attacks are given below.

- GOOGLE EARTH: It is a virtual map of globe and geographic information program. It maps the earth by the superimposition of images obtained from satellite imagery and provides aerial photography of the globe (www.earth.google.com).

- INTERNET ARCHIVE: The internet archive is an internet library with the purpose of offering permanent access for researchers, historians and scholars to historical collections that exist in digital format (Ramot et al., 2003). It includes texts, Audio moving images and software as well as archived web pages in our collections (www.archiv.org).

- PEOPLE SEARCH: People search provides details about personal information, date of birth, residential address, contact number etc. (www.whitepagesinc.com).
**DOMAIN NAME CONFIRMATION:** To perform searches for domain names using multiple keywords, this helps to find every registered domain name in “com”, “net”, “org”, “edu” (www.namedroppers.com).

**WHOIS:** This is a domain registration lookup tool. This utility is used for communicating with WHOIS servers located around the world to obtain domain registration information. WHOIS supports IP address queries and automatically selects the appropriate server for IP address. This tool will lookup information on a domain IP address or a domain registration server or you can use the default option which will select a server for you (www.whois.net).

**NSLOOKUP:** The name nslookup means “name server lookup”, the tool is used on windows and Unix to query details, including up addresses of a particular computer and other technical details such as mail exchanger records for a domain and name severs of a domain (www.nslookup.downloadsoftware4free.com).

**eMailTrackerPro:** eMailTrackerPro analyzes the E-mail header and provides the IP address of the system that send the mail (www.emailtrackerpro.com).

**HTTrack:** This tool acts like an offline browser. It can mirror the entire website to a desktop. One can analyze the entire websites by being offline (www.httrack.com).

**Active Attacks:** An active attack involves probing the network to discover individual hosts to confirm the information gathered in the passive attack phase which involves the risk of detection and is also called “rattling the doorknobs” (Lin et al., 2009). Given below the list of tools used for active attacks also used during vulnerability assessment and penetration testing.

**ARPING:** This is a network tool that broadcasts arp packets and receive replies similar to “ping”. It is good for mapping a local network and finding used IP space (Hovav and D’arcy, 2004). It broadcasts, who has an arp packet on the network and prints answers. It is very useful when trying to pick an unused IP for a net to which routing does not exist as yet (Iheagwara et al., 2004).

**Bing:** This tool is used for pinging the bandwidth. It is one of the point-to-point bandwidth measurement tool (Smith et al., 2002). It can calculate the blank throughput between any couple of networks. The Bing tool is a open source software. Easily we can download and measure the bandwidth (http://ai3.asti.dost.gov.ph/sat/bing.html).

**DNStracer:** This tool is used for determining the data source of a DNS server and notifies the continuous process of DNS server (mavetju.org/unix/dnstracer.php).

**Hmap:** This tool is used to getting the fingerprinting of web servers to identify the version of server, vender of the server, model of the server and more (http://ujeni.murkyroc.com/hmap).

**Nmap:** This tool is used to scan the port address of the network, it also takes the fingerprint of operating system version, service and it can scan the network rapidly (http://insecure.org/nmap).

**Conclusion**

Computers and internet have become common place in today’s society. This new technology has resulted in the development of a new form of crime viz. cybercrime. This review has provided a background to the cybercrime problems. Cyber criminals have existed almost as long as computers have existed. They take more advantage of e-commerce and violating intellectual properties both in India and abroad. Cyber criminals, hackers and new viruses emerge day-by-day. Government is introducing cyber law to catch up those criminals and hackers. We have to study the past incidents, learn from them and use that information to prevent future crimes. Even India needs a good combination of law and technology in harmony with the laws of other countries and keeping in mind common security standards. This review has provided a look at what we know about cybercrime and victimization, a little more than a decade into the new century. This information can be used to develop research questions to address what we do not know about this form of crime and victimization. As the use of computers, internet becomes further engrained into our society and this problem will continue to daunt legislators and law enforcement officials. The fluidity of technology will make it difficult to develop programs and policies to help protect people. Cybercrime research will be an important area of study for future criminologists as we move farther into the digital age.

**References**