Cyber World-Digital Extension of Computer Loggers

Sachin Singh,Dr. Rakesh Kr Dwievedi
[1]Assistant Professor ,CCSIT TMU Moradabad
[2]Principal, CCSIT TMU Moradabad
Singh.sachin1986@gmail.com
csit@tmu.ac.in

*Abstract-"***The Cyber World is a digital extension of any one who interact with a digital extension of the real world in a Virtual enviornment. It should be obvious you can't build virtual extensions on a web or web pages. In this Paper we deal with various no of cyber attacks and cyber attackers We should have something much more sophisticated. So welcome to the Cyber World". It is the world of online computers and communicators which carry today's fast growing high-technology era online. WWW and other new electronic technologies may be soon become prime survey vehicles due to convenient, verifiable, low-cost delivery and return systems as well as easy access and feedback mechanisms.**

Keywords-Cyberworld,virtual,sophisticate,extension

I. Introduction

Yet now we've been having a lot of tasks online using a web of documents and data & After 20 years of surfing, maybe it's time to get serious.It seems we've gotten ourselves caught in a web and we don't know how to get out.

These digital extensions will give the ordinary user stunning capabilities according to todays standards.The Cyber World will allow the internet to grow to a more advanced level of online computing. Things like voting, online shopping, e marketing of homes automobiles, court proceedings, job interviews, grocery shopping, Medical care and diagnostics, computer and home appliance maintenance and diagnostics, real time monitoring and enforcement of cyber crime, etc.would be easy.. Must expected from the web to produce all these tasks, but the dot com meltdown was the first sign that web technology was not up to the mark this is common. might be not so simple for the web but we are creating implementations Super Technology. The Cyber World's aims one way to follow at it if you are into abstractions and distractions. We are interested in something more intersting and real; so we've declare the term to give it the power and meaning that it deserves. It is An online space where users have the mechanisms in place to carry out any business or personal activity as easily and freely as they can carry them in the physical world. It is an environment for sophisticated users who use it & acces it for their tasks. and is capable to reach much higher & higher. The Cyber World is able to set the human race free. Free from himself, business and government. If there is one thing we've learned from the web, is that freedom to grow anything. It is like growing tree. The Internet enhanced by the Web is the clear expression of liberty and Democracy the world has ever known. Yet, there are people who want to limit this liberty. They are trying to cope it control it – for the purpose of making money. This is easier that you only need a little imagination. Because we are living in a digital era, it is no more necessity to divide and conquer to profit. In a digital era, this will result for failure.There is a new method for profiting in this digital era. Adding "The fastest way to experience the Cyber World is to Contribute. Big business cannott and wouldnot build it because they cannot use it to control you. Take care yourself andsupport the Cyber World"

It is one of many outbursts which know what we've been saying since 2004. "The Web is a Dead End". That's a good thing. It's just the beginning - Not the End.

According to The New Frontier The Cyber World is really a new frontier. It will tell us the way to make lots of gains in many areas. This is only possible because it will form as a shadow of new world that is controlled and also controlled by the rest of the world. It would be like a fresh start on a whole new planet or continent, similar to events set in motion by the adventures of Christopher Columbus to the Americas.

II. Cyber attack

A cyber attack is intentional exploitation of computer systems, technology-dependent enterprises and networks. Cyber attacks use malicious code to change the computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and theft identity.Cyber attack is also known as a computer network attack (CNA).

Cyber attacks may include the following consequences:

- Identity theft, fraud, extortion
- Malware, pharming, phishing, spamming, spoofing, spyware, Trojans and viruses
- Stolen hardware, such as laptops or mobile devices
- Denial-of-service and distributed denial-of-service attacks
- Breach of access
- Password sniffing
- System infiltration
- Website defacement
- Private and public Web browser exploits
- Instant messaging abuse
- Intellectual property (IP) theft or unauthorized access

Cyber-attack is any type of annoyed movement posed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various ways of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system.

III. Factors for cyber-attacks

Three factors contribute to why cyber-attacks are launched against a state or an individual: the fear factor, spectacular factor, and vulnerability factor.

Fear factor

The most common, fear factor, a cyber terrorist would create fear amongst individuals, groups, or societies. The bombing of a Bali nightclub in 2002 created fear amongst the foreign tourists who frequently visited the venue. Once the bomb went off and casualties ensued, the influx of tourists to Bali significantly reduced due to fear of death.

Spectacular factor

With spectacular factors, it is the actual damage of the attack, meaning the attacks created direct losses and gained negative publicity. In 1999 a denial of service attack rendered Amazon.com unusable. Amazon experienced losses because of suspended trading and it was publicized worldwide

Vulnerability factor

Vulnerability factor exploits how easy an organization or government establishment is vulnerable to cyber-attacks. An organization can easily be vulnerable to a denial of service attack or a government establishment can be defaced on a web page. A computer network attack disrupts the integrity or authenticity of data, usually through malicious code that alters program logic that controls data, leading to errors in output.

IV. Types Of Cyber Attackers Insider

The disgruntled insider is a principal perpetrator of computer crimes.5 Insiders do not need a vast knowledge about computer intrusions, because their knowledge of the systems they are attacking may allow them unlimited access in order to damage the system or to steal system data. The 1999 Computer Security Institute/FBI report noted that 55 percent of respondents reported malicious activity by insiders. There have been many convictions involving disgruntled insiders. For example, an employee used her insider knowledge and another employee's password and log-in identification to delete data from a U.S. Coast Guard personnel database system. It took 115 agency employees over 1800 hours to recover and reenter the lost data.6 In another case, a former employee of the Forbes publishing concern hacked into the company's systems using another employee's password and login identification, caused the crash of over half of the

Criminal Groups

Criminal groups are increasing rapidly using cyber intrusions, attacking systems for the cause of monetary gain. In 1999, for example, members of a group dubbed the "Phonemasters" were sentenced after their conviction for theft and possession of unauthorized access devices and unauthorized access to a federal interest computer. This international group penetrated the computer systems of MCI, Sprint, AT&T, Equifax, and even the FBI's National Crime Information Center (NCIC). The Phonemasters' activities should serve as a wake-up call for corporate security. Their methods included "dumpster diving" to gather old phone books and technical manuals for systems, which they then used to trick employees into giving up their log-in and password information

Foreign Intelligence Services

Foreign intelligence services have begun using cyber tools as part of their information gathering and espionage tradecraft. Between 1986 and 1989, for example, a ring of West German hackers penetrated numerous military, scientific, and industry computers in the United States, Western Europe, and Japan, stealing passwords, programs, and other information which they sold to the Soviet KGB.13 Significantly, this was over a decade ago — ancient history in Internet years. It is clear that foreign intelligence services increasingly view computer intrusions as a useful tool for acquiring sensitive U.S. government and private sector information.14
Application security

- Information security
- Network security
- Disaster recovery / business continuity planning
- End-user education.

.

V. Types of Attacks

Syntactic attacks and semantic attacks

There are a number of techniques to utilize in cyber-attacks and a variety of ways to administer them to individuals or establishments on a broader scale. Attacks are broken down into two categories, Syntactic attacks and Semantic attacks. Syntactic attacks are straight forward; it is considered malicious software which includes viruses, worms, and Trojan horses.

Viruses

Viruses are a self-replicating program that can attach itself to another program or file in order to reproduce. The virus can hide in unlikely locations in the memory of a computer system and attach itself to whatever file it sees fit to execute its code. It can also change its digital footprint each time it reproduces making it even harder to track down in the computer.

Worms

Worms do not need another file or program to copy itself; it is a self-sustaining running program. Worms replicate over a network using protocols. The latest incarnation of worms make use of known vulnerabilities in systems to penetrate, execute their code, and replicate to other systems such as the Code Red II worm that infected more than 259 000 systems in less than 14 hours.[6] On a much larger scale, worms can be designed for industrial espionage to monitor and collect server and traffic activities then transmit it back to its creator.

Trojan horses

A Trojan horse is designed to perform legitimate tasks but it also performs unknown and unwanted activity. It can be the basis of many viruses and worms installing onto the computer as keyboard loggers and backdoor software. In a commercial sense, Trojans can be imbedded in trial versions of software and can gather additional intelligence about the target without the person even knowing it happening. All three of these are likely to attack an individual and establishment through emails, web browsers, chat clients, remote software, and updates.

Semantic attack is the modification and dissemination of correct and incorrect information. Information modified could have been done without the use of computers even though new opportunities can be found by using them. To set someone into the wrong direction or to cover your tracks, the dissemination of incorrect information can be utilized.

cybersecurity

Cyber security is the arena of technologies, processes and practices created to protect networks, personal computers, data files and data from attack, damage,loss or unauthorized access. In a computing environment, the term *security* intends cyber security. According to a December 2010 analysis of U.S. spending plans, the federal government has allotted over $13 billion annually to cybersecurity over the next five years.

Ensuring cybersecurity requires coordinated efforts throughout an information system. Elements of cybersecurity include:

- Application security
- Information security
- Network security
- Disaster recovery / business continuity planning
- End-user education.

Conclusion

In conclusion I want to say that if our government include private sectors to secure cyber world then it is great development in the growth of cyber world, if we want to really improve this technology we have to initiate these steps. India require a good combination of laws and technology in harmony with laws of other countries and keeping in mind common Security Standards. Cyber ethics is important in cyber life Although cyber World is not in reality life ,but we have to follow the ethics. The key to protect yourself is Be aware. Not all cybercriminals are Hackers.

References

1.Research Methodology: Taming the Cyber FrontierTechniques for Improving Online Surveys Barbara K. KayeValdosta State University, bkaye@valdosta.edu

2.Cyber Attacks: Protecting America's Security Against Digital Threats Michael Vatis ESDP-2002-04 June 2002

3. An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks Cesar Cerrudo (@cesarcer) Chief Technology Officer, IOActive Labs

4.Sybil Attacks In Network Security"3rd International conference on System Modeling and Advancement in Research Trends"(SMART 2014) S.Singh,M V Gupta,Namit Gupta

5.Cyber crime-A threat to persons property Government And Society."Inter national journal of advance Research in Computer Science and Software Engineering" Vol 3 Issue 5 May 2013 Er.Harpreet Singh Dalla,Ms Geeta