STM JOURNALS

Recent Trends in Programming Languages
ISSN: 2455-1821 (Online)
Volume 4, Issue 2
www.stmjournals.com

World of Cyber Security and Cybercrime

Rachna Buch*, Dhatri Ganda, Pooja Kalola, Nirali Borad
Department of Computer Engineering, Atmiya Institute of Technology and Science, Kalawad Road, Rajkot, Gujarat, India

Abstract

Nowadays, cybercrime is one of the major crimes done by computer expert. In this paper, need of cyber security is mentioned and some of the impacts of the cybercrime. Cyber security is to provide prevention against the cybercrime, while cybercrime is that group of activities made by the people by creating disturbance in network, stealing others important and private data, documents, hack bank details and accounts and transferring money to their own. This paper gives detailed information regarding cyber security and cybercrime. It includes types of cyber security, need of cyber security, issues in cyber security, its advantages and disadvantages, history of cybercrime, types of cybercrime.

Keywords: *Cyber, cybercrime, cyber security, crime, security, network, hacking, steal data, information security, network security, operational security, communicational security, application security*

**Author for Correspondence* E-mail: rrbuch@aits.edu.in

INTRODUCTION OF CYBER SECURITY

It is a combining form relating to information and technology, the internet, and virtual reality. The term cyber security is used to refer to the security offered through on-line services to protect your online information. It additionally refers to the technologies and tactics designed to secure computer systems, computer networks and information from unauthorized access, susceptibilities and attacks delivered though the internet. Cyber security is an all-encompassing domain of information technology it comprises the entire set of security-related technologies.

Cyber security is also body of technologies, processes and practices designed to protect and secure networks, computer systems, various programs and data from cyber-attack, damage all these things or unauthorized access these. In a computing context, security includes both cyber security and physical security.

Security standards which are enable organizations to practice safe security techniques to minimize the number of successful cyber security attacks and prevent their data or systems. Though, cyber security is important for network security, data security, communication security, operational security and application security [2][3].

Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment [5]. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality

ELEMENTS OF CYBER SECURITY

Elements of cyber security include: Application security is the use of software, hardware, and procedural methods to protect application from external threats, viruses,

malwares or attacks. At the time of software design, security is becoming a very important concern during development of applications [1].

It would become more and more accessible over networks, and as a result, there are possibilities to a wide variety of threats entered to harm software or application and its data. Security measures at the time of building applications and application security routines which minimize the unauthorized code will be able to manipulate applications to access, steal, modify, or delete sensitive data. Actions to be taken to secure applications are called counter measures. The most basic software for countermeasure is application firewall that secures files or the handling of data by specific installed programs. The most common hardware countermeasure is a router that can secure the IP addresses of an individual computer system to being directly visible on the internet. Other countermeasures include conventional firewalls, programs or algorithms for encryption or decryption processes, anti-virus programs, spyware detection or removal programs and biometric authentication systems.

1. *Communication Security:* Communication security is also known as COMSEC. COMSEC is the process to secure or prevent unauthorized access to traffic will be generated from telecommunication systems, or it will also help for any written information that is transmitted or transferred to another device via any other medium. There are several COMSEC disciplines, including:

- *Cryptographic security:* It encrypts data of sender side and makes it unreadable until the data is decrypted by receiver side.
- *Emission security:* It is used to prevent the release or capture of equipment emanations to prevent information from unauthorized interception.
- *Physical security:* It ensures by giving prevention of unauthorized access to a network's cryptographic information, documents and equipment.
- *Transmission security:* It is used to protect unauthorized access when data is physically transferred from one side to other side or one medium to other medium to prevent issues such as service interruption, steal data by malicious person.
- *Information security:* It is used to protect information or data and its critical elements, including the systems software and hardware that use to store or transmit that information. Information security is also known as Infosec. Infosec is a set of strategies for managing the processes, tools which are used in software and policies of software that are mainly for security purpose and necessary to prevent, detect and counter threats to digital and non-digital information [4]. Infosec responsibilities include a set of business processes that will protect information assets of how the information is formatted or whether it is transit or not, is being processed or is at rest in storage. Infosec programs are follow the core objectives of the CIA (confidentiality, integrity and availability): it maintaining the confidentiality ensure that sensitive information is only disclosed to authorized parties, integrity stands for prevention of unauthorized modification of data and availability that guarantees the data can be accessed by authorized parties when requested of IT systems and business data.

2. *Network Security:* Network security is used to protect the networking components, connection of networks and con- tent related to network. A network security system typically relies on layers of security and it consists of more than one component that including in to the network for monitoring network and security software and hardware, and it appliances. All components work together to increase the overall security and performance of the computer network.
3. *Operational Security:* Operational security is an analytical process that classifies information assets and determines the controls required to secure these assets. Operational security is also known as OPSEC. Operational security typically consists of a five-step iterative process:

- *Identify critical information:* The first step is to find out which data would be particularly affect to an organization or harmful for organization if it was obtained by an adversary. This includes intellectual property, employees' and/or customers' personally information and financial statements.

- *Determine threats:* The next step is to determine which code or program represents a threat to the organization's private or sensitive information. There may be numerous adversaries that target different pieces of information, and companies must consider any competitors or hackers that may target the data.
- *Analyze vulnerabilities:* In the vulnerability analysis stage, the organization examines potential weaknesses among the safeguards in place to protect the private information that leave it vulnerable to potential adversaries [6]. This step includes identifying any potential lapses in physical/electronic processes designed to protect against the predetermined threats, or areas where lack of security awareness training leaves information open to attack.
- *Assess risks:* After vulnerabilities have been determined, the next step is to find the threat level associated with each of them. Companies rank the risks according to factors such as the chances a specific attack will occur and how damaging such an attack would be to operations. The higher the risk, the more pressing it will be for the organization to implement risk management controls.
- *Apply appropriate countermeasures:* The final step consists of implementing a plan to mitigate the risks beginning with those that pose the biggest threat to operations. Potential security improvements stemming from the risk mitigation plan include implementing additional hardware and training or developing new information governance policies.

PROBLEMATIC ELEMENTS OF CYBER SECURITY

One of the most problematic elements of cyber security is the security risks. The traditional approach has been focus most resources on the most crucial system components and protect against the threats, which necessitated leaving some less important system components undefended and some less dangerous risks, i.e., not protected. Such an approach is insufficient in the current environment.

1. *Major Security Problems:*

- *Virus:* A Virus is a program that is loaded onto your computer without your knowledge and runs against your wishes. These are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network by clicking on it, through mail, through external devices, etc. They disrupt the computer operation and affect the data stored either by modifying it or by removing it altogether.
- Example of viruses: (1) Melissa, (2) Sasser, (3) Zeus, (4) Conficker, (5) Stuxnet, (6) Mydoom, (7) Code Red.
- *Warms:* Worms unlike viruses do not need a host to cling on to. They merely replicate until they eat up all available memory in the system. The term worm is sometimes used to mean self-replicating malware (MALicious softWARE). It occupies some free memory of drives or external devices.
- Example of warms: (1) Badtrans, (2) Bagle, (3) Blaster, (4) ExploreZip, (5) Kak worm, (6) Netsky, (7) SQL Slammer, (8) Supernova Worm
- *Hacker:* In common a hacker is a person who breaks into computers, usually by gaining access to administrative controls. *Types of hackers:*

a. White Hat Hacker: A white hat hacker is a computer security specialist who breaks into protected systems and networks to test and asses their security. White hat hacker's use their skills to improve security by exposing vulnerabilities before malicious hackers (known as black hat hackers) can detect and exploit them. Although the methods used are similar, if not identical, to those employed by malicious hackers, white hat hackers have permission to employ them against the organization that has hired them.

b. Grey Hat Hacker: The term "grey hat" or "gray hat" refers to a computer hacker or computer security expert who may sometimes violate laws or typical ethical standards, but does not have the malicious intent typical of a black hat hacker.

c. Black Hat Hacker: A black hat hacker is an individual with extensive computer knowledge whose purpose is to breach or bypass internet security. Black hat hackers are also known as crackers or dark-side hackers. The general view is that, while hackers build things, crackers break things.

- *Malware:* The word "malware" comes from the term "MALicious softWARE." Malware is any software that infects and damages a computer system without the owner's knowledge or permission. (1) Viruses, (2) Warms, (3) Root kits, (4) Trojans, (5) Spyware, (6) Crime ware, (7) Adware
- *Trojan horses:* Trojan horses are email viruses that can duplicate themselves, steal information, or harm the computer system. These viruses are the most serious threats to computers.
- *Password Cracking:* Password attacks are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas and social network sites.

MANAGEMENT OF CYBER SECURITY RISKS

The risk associated with any attack depend on three factors: threats (who is attacking), vulnerabilities (the weaknesses they are attacking), and impacts (what the attack does). The management of risk to information systems is considered fundamental to effective cyber security [7].

What Are the Threats? People who actually perform cyber- attacks are widely cited as falling into one or more of five categories: criminals intent on monetary gain from crimes such as theft or extortion or spoil the system spies, intent on stealing classified or proprietary information used by government or private entities; nation-state warriors who develop capabilities and undertake cyber-attacks in support of a countries strategic objectives; activists who perform cyber-attacks for nonmonetary reasons; and terrorists who engage in cyber-attacks as a form of non-state or state-sponsored warfare.

What Are the Vulnerabilities? Cyber security is in many ways an arms race between attackers and defenders. ICT systems are very complex, and attackers are constantly probing for weaknesses, which can occur at many points. Defenders can often protect against weaknesses, but three are particularly challenging: inadvertent or intentional acts by insiders with access to a system; supply chain vulnerabilities, which can permit the insertion of malicious software or hardware during the acquisition process; and previously unknown, or zero-day, vulnerabilities with no established fix. Even for vulnerabilities where remedies are known, they may not be implemented in many cases because of budgetary or operational constraints. Network administrator will use these types of software by trying that if any attacker can easily attack on database or not? Are there any weaknesses which harm the software security or database security? Whereas hacker will use these types of vulnerable software for hacking the details of user [6].

What Are the Impacts? A successful attack can compromise the confidentiality, integrity, and availability of an ICT system and the information it handles. Cyber theft or cyber espionage can result in ex-filtration of financial, proprietary, or personal information from which the attacker can benefit, often without the knowledge of the victim [2]. Denial-of-service attacks can slow or prevent legitimate users from accessing a system. Botnet malware can give an attacker command of a system for use in cyber-attacks on other systems.

Advantages of Cyber Security

1. Improved security of cyberspace
2. Increase in cyber defense
3. Increase in cyber speed
4. Protecting company data and information
5. Protects systems and computers against virus, worms, malware and spyware, etc.
6. Protects individual private information
7. Protects networks and resources
8. Fight against computer hackers and identity theft
9. Minimizes computer freezing and crashes.
10. Gives privacy to users

Disadvantages of Cyber Security

1. It will be costly for average users
2. Firewalls can be difficult to configure correctly
3. Need to keep updating the new software in order to keep security up to date.
4. Make system slower than before.
5. Incorrectly configured firewalls may block users from performing certain actions on the Internet, until the firewall configured correctly.

Safety Tips for Cyber Security

1. Use antivirus software
2. Insert firewalls, pop up blocker

3. Uninstall unnecessary software
4. Maintain backup
5. Check security settings
6. Use secure connection
7. Open attachments carefully
8. Use strong passwords, (keep combination of uppercase, lowercase, special characters etc.) do not give personal information unless required

ISSUES IN CYBER SECURITY

1. Better end user education it's sort of expressing the self-evident, however most frameworks are just as secure as the propensities for the general population utilizing them. Terrible on-screen characters abuse this to exploiting powerless passwords and un patched programming and utilizing complex phishing strategies [8].
2. Security mindful programming advancement: They are sufficiently not individuals centered on security. With an expanding measure of individuals getting associated with Internet, the security dangers that reason more hazards to hurt information, programming and gadget too.

Cybercrime

Cyber security is needed when crime will be performed: The former descriptions were "computer crime", "computer related crime" or "crime by computer". With the pervasion of digital technology, some new terms like "high-technology" or "information age" crime were added to the definition. [6] Also, Internet brought other new terms, like "cybercrime" and "net" crime. Other forms include "digital", "electronic", "virtual", "IT", "high-tech" and technology enabled" crime. It will do by that people who are mostly connected to internet, online activities, social activities, etc.

History of Cybercrime

1. The first recorded cybercrime was recorded in the year 1820.
2. The first spam email took place in 1978 when it was sent over the Arpanet.
3. The first Virus was installed on an Apple Computer in 1982.

Types of Cybercrime

There are 12 types of cybercrimes

- *Hacking*
  In simple words, hacking is an act committed by an intruder by accessing your computer system without your permission. Hackers (the people doing the hacking) are basically computer programmers, who have an advanced understanding of computers and commonly misuse this knowledge for devious reasons.

a. SQL injections
b. Theft of FTP passwords
c. Cross site scripting

- *Virus dissemination*
  Viruses are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network. They disrupt the computer operation and affect the data stored either by modifying it or by deleting it altogether.
- *Logic bombs*
  A logic bomb, also known as slag code, is a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event.
- *Denial-of-Service attack*
  A Denial-of-Service (DoS) attack is an explicit attempt by attackers to deny service to intended users of that service. It involves flooding a computer resource with more requests than it can handle consuming its available bandwidth which results in server overload.
- *Phishing*
  This is a technique of extracting confidential information such as credit card numbers and username password combos by masquerading as a legitimate enterprise.
- *Bombing and spamming*
  Email bombing is characterized by an abuser sending huge volumes of email to a target address resulting in victims email account or mail servers crashing.
- *Jacking*
  Web jacking derives its name from hijacking. Here, the hacker takes control of a web site fraudulently. He may change the content of the original site or even redirect the user to another fake similar looking page controlled by him.

- *Cyber stalking*
  Cyber stalking is a new form of internet crime in our society when a person is pursued or followed online

a. Internet stalking, *b*. Computer stalking.

- *Data diddling*
  Data Diddling is unauthorized altering of data before or during entry into a computer system, and then changing it back after processing is done.
- *Theft and Credit Card Fraud*
  Identity theft occurs when someone steals your identity and pretends to be you to access resources such as credit cards, bank accounts and other benefits in your name.
- *Slicing attack*
  A salami slicing attack or salami fraud is a technique by which cyber criminals steal money or resources a bit at a time so that there no noticeable difference in overall size.
- *Software Piracy*
  Internet piracy is an integral part of our lives which knowingly or unknowingly we all contribute to.

Cybercrime includes

- Illegal access
- Illegal interception system
- Interference data
- Interference misuse of devices fraud.

CONCLUSION

Any intelligent device that can pass data to one or more other devices (either through a network or not) is encompassed within the scope of Cyber Security that includes pretty much the entire foundation of modern society. All need to be aware of cyber security as well as cybercrimes and its causes. There is little seriousness about security regarding online, social and other activities through which probability of risk will be higher. It causes loss of data, modifying data, removing useful information as personal details, passwords of mail accounts, social accounts or bank accounts. People may also know about laws against cybercrimes or cyber laws and actions which will be taken and how to fight against crime.

REFERENCES

1. Sergey, Melnik, Smirnov Nikolay, Erokhin Sergey. Cyber security concept for Internet of Everything (IoE). *Systems of Signal Synchronization, Generating and Processing in Telecommunications.* 2017. IEEE, 2017.
2. Martin, Nigel, John Rice. Cybercrime: Understanding and addressing the concerns of stakeholders. Computers and Security. 2011; 30(8): 803–814.
3. Shang H, Jiang R, Li A. A Framework to Construct Knowledge Base for Cyber Security. *2017 IEEE Second International Conference on Data Science in Cyberspace (DSC)*. IEEE, 2017.
4. Manmohan Chaturvedi, Aynur Unal, Shilpa Bahl. International cooperation in cyber space to combat cyber crime and terrorism. *2014 IEEE Conference on Norbert Wiener in the 21st Century (21CW)*. IEEE, 2014.
5. Rayne Reid, Johan Van Niekerk. From information security to cyber security cultures. *Information Security for South Africa (ISSA)*. 2014. IEEE, 2014.
6. R. Hewett, S. Rudrapattana, P. Kijsanayoth. Cyber-security analysis of smart SCADA systems with game models. *Proceedings of the 9th annual cyber and information security research conference*, ACM, 2014, pp. 109–112.
7. Von Solms, Rossouw, Johan Van Niekerk. From information security to cyber security. Computers and Security. 2013; 38: 97–102.
8. Eric A. Fischer. (2106). Cybersecurity Issues and Challenges: In Brief. [Online]. Available from https://fas.org/sgp/crs/misc/R43831.pdf [Accessed on October 2017].

Cite this Article
Rachna Buch, Dhatri Ganda, Pooja Kalola *et al.* World of Cyber Security and Cybercrime. *Recent Trends in Programming Languages*. 2017; 4(2): 18–23p.