International Journal of Applied Research 2017; 3(3): 369-371

ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 5.2
IJAR 2017; 3(3): 369-371
www.allresearchjournal.com
Received: 20-01-2017
Accepted: 21-02-2017

S Geethamani
Department of Corporate Secretaryship, PSG College of Arts and Science, Coimbatore, Tamil Nadu, India

Correspondence
S Geethamani
Department of Corporate Secretaryship, PSG College of Arts and Science, Coimbatore, Tamil Nadu, India

Risk in cyber security

S Geethamani

Abstract
Computer security rests on confidentiality, integrity, and availability. The interpretations of these three aspects vary, as do the contexts in which they arise. The interpretation of an aspect in a given environment is dictated by the needs of the individuals, customs, and laws of the particular organisation. The information should be kept carefully and it should be protected from the hackers. The awareness of hackings and using the technologies are perfect way to avoid hacking.

Keywords: Cyber security, Vulnerability, Attacks, Hackers, Security mechanism

Introduction
The network security and cyber security has become a very critical aspects of modern computing systems. With the global acceptance of Internet, virtually, every computer is connected to each other. While this has created tremendous productivity and unprecedented opportunities in the world and it has created new risks for the users of these computers. The users, businesses and organisations worldwide have to live with a constant threat from hackers and attackers, who use variety of techniques and tools in order to harm the computer, break the computer system, steal the information and change the data. The human risks and error are involved in the social engineering. Cryptography and digital signature are some of the ways to secure the computer data. Privacy violation is the major risk in computer, network and cyber security.

Objectives
The main objective is to know about security, vulnerabilities, security challenges, hackers, cryptography and digital signature. The cryptography and digital signature issues in cyber security. The antispyware program spread via Trojans, additional spyware installations and how to repair the files.

Vulnerabilities
In computer security, the term vulnerabilities is a weakness which allows an attackers to reduce a system's information assurance. Vulnerabilities is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. To be vulnerable, an attackers must have at least one applicable tool or technique that can connect to a system weakness. In thus frame, vulnerability is also known as the attack surface.
A security risk may be classified as vulnerability. Vulnerability with one or more known instances of working and fully-implemented attacks is classified as an exploit. The window of vulnerability is the time from when the security hole was introduced or manifested in deployed software, to whom access was removed, a security fix was available/deployed, or the attacker was disable.

Causes of vulnerability
- **Complexity:** large, complex systems increase the probability of flaws and unintended access points.
- **Familiarity:** using common, well known code, software, operating systems, and hardware increases the probability an attacker has or can find the knowledge and tools to exploit the flaw.

- **Connectivity:** more physical connections, privileges, ports, protocols, and services and time each of these are accessible increase vulnerability.
- **Password management flaws:** the computer user uses weak passwords that could be discovered by brute force. The computer user stores the password on the computer where a program can access it. Users re-use passwords between many programs and websites.
- **Software bugs:** the programmer leaves an exploitable bug in a software program. The software bug may allow an attacker to misuse an application.
- **Unchecked user input:** the program assumes that all user input is safe. Programs that do not check user input can allow unintended direct execution of commands.

Cyber security

It seems that everything relies on computers and the internet now- communication (email, cellphones), entertainment (digital cable, mp3s, DVD's), transactions (car engine system, naval navigation, air plane navigation), shopping (online shopping, credit cards, debit cards), medicine (equipment, CTS scan, medical records), etc., how much of your daily life relies on computers? How much of your personal information is stored either on your own computers or on someone else's system?

Cyber security involves protecting that information by preventing, detecting, and responding to attacks.

Risks in cyber security

There are many risks, some more serious than others. Among these dangers are viruses erasing your entire system, someone breaking into your system and altering files, someone using your computer to attack others, or someone stealing your credit card information and making unauthorised purchases. Unfortunately there's no 100% guarantee that even with the best precautions some of these things won't happen to you, but there are steps you can take to minimise the changes.

Hacker, attacker, intruder: these terms are applied to the people who seek to exploit weakness in software and computer systems for their own gains. Although their intentions are sometimes fairly being motivated solely by curiosity, their actions are typically in violation of the intended use of the systems they are exploiting.

Malicious code: malicious code sometimes called malware, is a broad category that includes any code that could be used to attack your computer. It have following characteristics:

- It might require you to actually do something before it infects your computer. This action could be opening an email attachment or going to a particular web page or by cd's.
- Some forms propagate without user intervention and typically start by exploiting a software vulnerability.
- Some malicious code claims to be one thing while in fact doing something different behind the scenes.

Attacks

Bad things can happen to an organisation's information or computer systems in many ways. Some of these bad things are done on purpose (maliciously) and others occur by accident.

There are some primary categories of attacks:

- Denial of service
- DDoS
- DNS
- NNTP

Attacks may occur through technical means such as specific tools designed for attacks or exploiting of vulnerabilities in a computer system, or they may occur through social engineering technical means to gain unauthorized access. Attacks against information in electronic form have another interesting characteristics; information can be copied, but is normally not stolen. In other words, an attacker may gain access to information, but the original owner and the attackers hands. This is not to say that damage is not done, but it may be much harder to detect since the original owner is not deprived of the information.

Types of attacks

1. Denial of service attacks

Denial of service attacks are not used to gain unauthorised access or control of a system. They are instead designed to render it unusable. Attackers can deny service to individual victims, such as by deliberately entering a wrong password three consecutive times thus causing the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once.

2. Indirect attacks

An indirect attack is an attack launched by a third party computer. By using someone else's computer to launch an attack, it becomes far more difficult to track down the actual attacker. There have also been cases where attackers took advantages of public anonymising systems.

3. Direct access attacks

Someone who has gained access to a computer can install any type of devices to compromise security, including operating system modifications, software worms, key loggers, and covert listening devices. The attackers can also easily download large quantities of data onto backup media, for instance CD-R/DVD-R, tape; or portable devices such as key drive, digital cameras or digital audio players.

4. Computer crime

Computer crime includes traditional criminal acts committed with a computer, as well as new offences that lack any parallels with non-computer crimes. The diversity of offences renders any narrow definition unworkable.

5. Cyber terrorism

The number of publicized terrorist attacks started to escalate beginning in the mid-1990s. From the attacks that received wide coverage by the world press, we have arrived to the point where not a single day passes without a terrorist committing such acts. It is the spectacular that is getting first-page coverage by the mass media. The basic mechanics of these attacks is usually through the use of explosives denoted remotely or by a suicidal person intent on taking others with them into the next life.

Cyber-attacks consist

- Virus and worm attacks that are delivered via e-mail attachments, web browser scripts, and vulnerability exploit engines.

- Denial of service attacks designed to prevent the use of public systems by legitimate users by overloading the normal mechanisms inherent in establishing and maintaining computer to computer connections.
- Web defacements of informational sites that service governmental and commercial interests in order to spread disinformation, propaganda, and disrupt information flows.
- Unauthorised intrusions into systems that lead to the theft of confidential and proprietary information, modification or corruption of data, and the inappropriate usage of a system for launching attacks on other systems.

Hackers

A hacker was anybody who tinkered with any kind of system, mechanical or electrical, in order to better understand how it worked. Today hackers are persons who create or modify computer software, typically with the goal of using software in a manner not intended by the original computer programmer.

The hacker's ethics

As levy stated, the general principles of hackers ethic include:

- Sharing
- Openness
- Decentralization
- Free access to computers
- All information should be free
- Hackers should be judged by their hacking not criteria such as degrees, age, race, sex or position
- Can create art and beauty on a computer
- Computers can change our life or the better

Security mechanisms

Following are the ways of secure our information from the hackers:

- Selecting good password
- Determining password strength
- Entropy, or bit strength
- Random passwords
- Securing passwords with Encryption and securing the password file
- Central storage, password comparison and network authentication

Avoid being a victim

- Be suspicious of unsolicited phone calls, visits or e-mail message from individuals asking about employees or other internal informations.
- Do not provide personal information or information about your organisation including its structure or networks, unless you are certain of a persons authority to have the information
- Do not reveal personal of financial information in email, do not respond to e-mail solicitations for this information.
- Don't send sensitive information over the internet before checking a websites security
- Pay attention to the URL of a website. Malicious website may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain.(e.g. .com vs .net)
- If you are unsure whether an email request is legitimate try to verify it by contacting the company directly.
- Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group
- Install and maintain anti-virus software, firewalls, and emails filters to reduce some of this traffic
- Take advantage of any anti-phishing features offered by your email client and web browser

Conclusion

Dangerous things are unsuspected in cyberspace. Every business, regardless of size of industry should have an easily understood, consistently enforceable policy to protect trade secrets, maintain the integrity and security of all networks and servers, protects sensitive customer information, protect the organisation from lawsuits by third party, protect the integrity and reputation of the organisation and its business and ensure achievement and productivity. Keeping the networks secure from hackers is just as critical to protect your private information. Information security requires effective policies and consistent enforcement.

Reference

1. John W Rittinghouse, William M Hancock, Cyber security operations handbook, Reed Elsevier, 2008.
2. Sara Qamar, Zahid Anwar, Mohammad Ashiqur Rahman, Ehab Al-Shaer, Bei-Tseng Chu "Data-driven analytics for cyber-threat intelligence and information sharing**.**
3. Markus Wagner, Alexander Rind, Niklas Thür, Wolfgang Aigner, "A knowledge-assisted visual malware analysis system: Design, validation, and reflection of KAMAS/