Notes for Internet Security, B.Sc. (I.T.) Semester – V

Chapter 1 - Introduction

In general, *Computer security* means keeping anyone from doing anything, which is unwanted or undesired, relating to computers & peripherals. It is the way of protecting your precious assets in terms of information or resources.

Why require security: -

There are various ways in which the functionality of computer systems is threatened. We would require security to safeguard the information or resources, which are assets to the organization. Now days, we hear that many systems run by Govt. & other organizations have been disrupted or penetrated. These kinds of activities are now increasing & there is a computer related security issue worth considering. This would require some policy formulated by the organization to keep protected from these kinds of attacks. Once this consideration is made, the further questions are: *what* resources should be protected? *Who* is going to disrupt the systems & *How*. Consider an example of household security. You clearly know what resources to protect (e.g. cash /jewellery, other valuable items etc.) & so also you know the ways in which these things can be stolen. Hence you protect these items by keeping them in safe & secure places.

The job of a Network Administrator is similar in the organization that is to protect the resources & information from prying eyes, hackers or attackers whether from inside or even outside. Another important difference in house security & Computer security is that in later case, many times the attacker is too far away & even unidentified. The attack in such case is in *logica*l form.

Picking a security policy: -

A 'Security Policy' describes your plan, methodology to safeguard your assets or what measures / precautions you take (or do not take) in order to keep your assets secured. A security policy differs from organization to organization. All the decisions are then based on this formulated policy. The first step here is to perform a *Risk Analysis*. It is a process of examining all your risks & then finding a cost-effective decision to recover from it. Two important steps in this are:

1. Finding out what resources you wish to protect: Resources may include (a) physical resources like printers, monitors, keyboards, drives, modems etc. & (b) logical resources like source & object programs, data, utilities, operating system, applications etc.

2. Find out who can disrupt them & in what ways: The threats to your assets may include (a) Physical threats to the resources such as stealing, malfunctioning devices, (b) Logical threats such as unauthorized access to data, information, resources (c) Unintended disclosure of your information.

The attackers here are normally known as *Hackers* by the terminology. A hacker is an individual who finds ways of exploiting your systems & looks for known loopholes (vulnerabilities) & further can disclose, or use them for personal gains. A hacker is technically sound, not satisfied with just

running programs, but needs to understand how it works. A hacker may also be an individual who is employed as a security consultant. Many companies do that. (Thieves know their own ways & methods. So, why not use a thief to track another?)

Once you know why you require security, what resources you have to protect & from whom you need to protect them, you are ready to form your policy to safeguard. A good security policy should have following characteristics:

* Should define a clear set of security goals.
* Accurately define each issue discussed in the policy.
* Define under what circumstances each issue is applicable.
* Should be enforceable with security tools wherever appropriate.
* Should clearly define the areas of responsibility for users, administrators & management.
* Should have acceptance within the organization

Hence, a security policy is a document, which describes the acceptable network activity as well as the penalties for misuse of it.

Strategies for a secure Network: -

Before you can decide on how to safeguard your network, you must identify what *level* of security you require, i.e. whether you want a lower, medium or a very tight security. (For example, famous personalities will require more life security - Y level, Z level etc., than a common man.) Once this job is done, you are ready to make your strategies to secure your network.

The various strategies used further to secure the network will include the following:

1. Host security – securing the prime, host machines by logically isolating them.
2. Authentication of users – checking the identity of valid users keeping the unauthorized users away.
3. Choosing good passwords & protecting them - A good password should be developed using various criteria & safeguarding it as well. Also making sure it is not reused & changed frequently.
4. Using firewalls & proxy servers while accessing Internet – using these tools to act like logical security guards to monitor traffic in & out of your local network (protected) & the Internet (unprotected).
5. Making use of Encryption techniques – used to encrypt the sensitive information to be sent out, making it harder to crack if intercepted. Involves using various algorithms based on the Data Encryption Standard for this purpose.

Ethics of Computer security: -

While we are applying ourselves to keep our assets protected & secured, we must consider the ethics of computer security. These are the morals / principles to be followed while using computer security aspects. There may be several issues of security policy that may affect individuals outside the organization, even though the policy is formed for the organization. Also the consideration to the privacy of the individual should be made. The ethical issues say even further that there is no harm in monitoring our own systems & equipments and that the *counterattacking* on the attacker is also

possible in self-defense. In short, so long as we stay within the frame of law, computer security is ethical.

Security threats & levels: -

There are various ways & means in which threats can be given to the security. Generally, the two main *levels* in which threats can be given to the system security are:

1. Inside attacks: Studies have shown that around 70% of the attacks come from someone within the organization or someone with inside information. This is because the insider has a better knowledge of your system's functioning & hence it is easier to attack. These may be either ex-employees or unsatisfied employees.

2. Attacks from outside: The outsiders who would attack your security may be either your competitors (desperately needing the sensitive internal information of your organization) or someone just making fun or trying out their luck or experimenting by disturbing your systems without any special reasons.

In general the natures of threats to the system security are found as:

(a) Threat to Availability – Information is not available whenever demanded.
(b) Threat to Integrity – Information is tampered with by someone deliberately.
(c) Threat to Confidentiality – Information illegally accessed by someone.
(d) Threat to Authentication – Valid user identity is penetrated.

Security Plan (RFC 2196): -

The overall security plan is discussed in the Request for Comments No. 2196. For this RFC2196 document, please refer the link: http://rajeshwatve.tripod.com/rfc2196.zip

End of Chapter 1 : Notes for Internet Security B.Sc. I.T. Sub: Internet Security.