Computer Security

By Selvadurai Jeyarajah

Contents

Introduction

Computer crimes and information theft have become a serious problem. Computer security can be loosely separated into two parts. The first is **logical security** that deal with access to and use of data and programs in the conventional programming environment. The second is the **physical security** . Physical security deals with access to data and programs outside of the normal environment by physical means (accessing the operator's console, removing a tape or disk, probing circuits). Logical security is usually implemented in the designing the operating system and system software, while physical security has usually been implemented using walls and doors. classically the problem of physical security has been addressed by limiting physical access to the machine room. However as personal and other small computer have come into common use, this approach become impractical. Cryptograpy is the science of techniques which make data unintelligible and unmodifiable by outsiders (without detection) and still accessible or verifiable by the legitimate receiver. It has been called by " **The premier safeguard against computer crimes**".

Security Principals

Computer systems are usually designed to perform certain functions and to provide essential or important services for an organisation. The systems may hold and process data vital to the organisation. Computer system have in fact become an essential part of modern business and administration. We have come to expect good performance and behaviour of our computer. Today people expect these systems to work properly and be available when required.

"Secure" may be designed as safe against attack or failure. Computer systems are part of corporate systems. The step taken to protect against attack or failure are security measures. They include validation checks on input data and fire resistant safes to protect media and the data that they contain. Data encryption on communication circuits, and personal badge-reader identity passes are other examples of security measures.

There are countless threats, some obvious, some undiscovered until too late. Obviously, power supplies to a computer may fail from time to time especially in bad weather during winter. Programs may contain undiscovered bugs. Media, such as disks or tapes, may become corrupted.

Threats are of two kinds

1. Accidental
2. Deliberate

Physical Security

The physical environment has enormous influence on the security of a computer system. Proper consideration of factors like location and building design and construction is vital, especially at the planning stage. It is much easier to eliminate potential security problems or minimise their effects at this stage. An existing building may have insolvable security problems.

Location

A computer installation's location determines of the risks that affect it. Any site is subject to many natural risks such as the weather and the stability of the ground itself. The site is also subject to neighbourhood risks that result from mankind's activities nearby.

Natural Risks

Weather and its consequences are the most important natural risk for most locations. Wind, rain, snow and ice have obvious and often dramatic affects.

Building Construction and Design

The building housing the installation makes a most important contribution to its security. Its provides accommodation for the computer system, personnel and ancillary services. Failures or shortcomings in the design will affect the installation in all sorts of ways.

Electric Power Supply

We take electric power for granted. No computer can operate without it, but many less obvious services and ancillaries are totally dependent upon continued electricity supply. Lighting and alarm systems, as well as air conditioning, will fail without it. Public supplies are generally very reliable indeed. Except in outlying areas the supply rarely fails by accident. Most major consumers can arrange to have two independent supply routes, so that there is fall-back if one should fail.

The following preventive measures can be taken of physical security for computers

- The placing of the computer room, communications centre and other key areas has direct affect on their vulnerability to physical damages.
- IT systems depend on there being a power supply, air conditioning and communications facilities. These should also be placed out of harm's way ie where they are unlikely to be affected by fire, water, impact or other dangers.
- The local fire prevention officer should be consulted whenever a new computer room is planned or extensive alterations for an existing one are in mind.
- Flammable materials should not be stored in or near computer room.

Logical Security

A logical breach affects the data and software without physically affecting the hardware. The damage is often invisible until someone tries to process or display the data. Fraud and unauthorised access are examples of malicious logical breach, and though it may have been introduced accidentally onto a personal computer(PC), its original conception was malicious.

Logical security comprises the following

- Viruses

- Untested
- User error
- Operator error
- Computer misuse
- Computer fraud
- Student unauthorised access
- External unauthorised access

One of the problems with any logical breach of security is that the damage is invisible and its extent is unknown. Investigation costs are therefore likely to be high.

This is particularly true of virus infections. In some cases they can be just an annoyance, and little damage is caused to the data or software, but there malicious infections may erase (or, even worse, corrupt) the data on an entire disc. The virus may be transferred to any floppy disc that comes into contact with an infected PC, and a long incubation period may mean it could be many months before the infection becomes apparent.

Every other PC that those disks have come into contact with must then be checked, and every floppy disc that has been loaded on any of those PCs, and then every other PC that those discs have been loaded on, and so on. Thousands of PCs and discs may have to be checked in a large organisation. Virus infections may also be transmitted to other PCs over a network if infected software is sent.

Summary

Computer security is becoming a very important issue in the modern computer world. There are mainly two types of computer security should be considered and they are **Physical security** and **Logical security** . Physical security is access to data by physical means and logical security is concerned with the software level.

In order to implement Physical security; physical contact to the data should be prevented. Likewise access to data should be prevented in the software level as a measure of logical security. Nowdays computer crimes are increasing both physically and logically, measures should be taken to prevent both physical logical access to computer.

References

1. Computer Security Handbook by R.A.Elbra
   NCC Publications 1992
2. Introducing Computer Security by M.B.Wood
   NCC Publications 1982
3. The Cost of Computer Crime by C.Hook
   IEE review January 1995
4. 1987 IEEE Symposium on Security and Privacy
   April 27 to 29 1987, Oakland, California