Can You Depend Totally on Computers?

Computer Security, Availability and Correctness

H N Mahabala

You can depend totally on computers provided you take some elementary precautions to protect yourself when failures occur. These measures require your time and some extra resources but are well worth the cost.

Prof. H N Mahabala retired as a Professor of Computer Science and Engineering from the Indian Institute of Technology, Madras in 1995 and is currently advising IT companies in Bangalore. He has been involved in Computer Science education at all levels and has interacted with the computer industry in India from the beginning.

Computer Systems Do Fail

Computers have become part of the system that manages any enterprise – be it small stores, service bureau or a complex organization. It is thus natural to ask whether one is risking too much in being so dependent on computers, for like any machine, computers and their associated interfaces do fail. This fear was widely expressed when one moved from the 'batch mode', i.e. use a computer when convenient, to the 'on-line mode' when a task is performed as and when needed (Real-Time) using a computer connected on-line. Failure of any part of a computer system not only has the potential to bring the work to a halt, but also the danger of accidental loss of valuable data. Whereas in early days one had the ability to switch to manual operation when the computer failed, one cannot do so now as the ledgers one needs for manual operation are no longer maintained since all ledgers have become electronic. Fortunately, techniques and practices are available to minimize the probability of disruption due to failure to as low a level as one desires. The area of fault-tolerant and reliable computing deals with measures which help to achieve non-stop and loss free computing.

Providing insurance against loss and failure involves extra cost and effort. The lower the probability of failure one wants to achieve, higher is the cost. As such, one should tailor the fault-tolerance to a level that the application requires. Whereas one

Availability and reliability of a computer system are two aspects important to business, and one has to choose a proper mix of them to achieve cost effective security.

wants true non-stop operation for launching a satellite, one needs only 'can-catch-up-later' capability for a PC. However, in both cases we have to protect the data in the system from loss or corruption. A telephone system, which today is computer based, must keep operational even when a disaster strikes, even if some calls are connected to a wrong party. A banking computer system, on the other hand, must work correctly or not work at all. Availability and reliability of a computer system are two aspects important to business, and one has to choose a proper mix of them to achieve cost effective security. Many users and even organizations get excited by the availability of a computer and carry on merrily till one day a failure causes irretrievable damage. It should be the responsibility of the computer professional in charge of computerization in such organizations, to implement adequate measures to protect the business against normally expected failures. Methods used to achieve reliability, availability and correctness will be described in the following pages.

Controlled Access

Controlling physical access to a computer with a lock and key is still a very effective first line of defence. A more common method of controlling access is use of a password. It is a string of characters which is known only to the particular user and the log-in software. An user who is registered is allotted a general password, but the user is expected to immediately change it to a personal choice, since the general password is known to many in the computer center.

Box 1. How to Choose a Password.

Many users make the mistake of choosing a password which is related to the name of a person or place close to him/her. There are many cases of crooks making a right guess and compromising the system in such cases. In one case a crook tried all words in a dictionary to find the password!. Hence, users are advised to choose a nonsense word as password, use some special characters such as % or $ in it and are urged to not even write it down on a piece of paper to be carried with him/her. Changing your password, say once in 2 months, is also desirable.

Reliable Components

Most computer failures are due to electro-mechanical components.

Reliability of a system depends on the reliability of its components and sub-systems. Good design ensures that components are operated well below their maximum rating to reduce effects of aging. It is good to have a burn-in phase so that weak components if any will fail. Life, however, of electronic components (after burn-in) is very long. Electronic components hardly fail even when they are continuously operated. They fail if there are excessive transients. It is thus advisable not to switch off your PC frequently in a day.

Most computer failures are due to electro-mechanical components. Units like key board and printers should preferably be of a heavy duty type, since one can easily overload them. Cleanliness of the computing environment helps to extend life of diskettes. It is good to read back diskettes after writing and check that the files have been written correctly. Periodic cleaning of mouse, keyboard etc., using a vacuum cleaner prolongs their life.

Redundancy

Traditional approach to achieving fail-safe feature is to use additional stand-by systems/sub-systems. The hand brake in a car is a stand by for the foot brake and can be used in case the brake fails. In India power failure is common. Power failure during computation is irritating and you may lose the data you entered unless you saved it in a disk. It is thus desirable to have an Uninterrupted Power Supply (UPS) system with a battery back up if your work is critical. The batteries in a UPS system normally provide back up supply for only about 15 to 30 minutes. Thus, if you expect longer power shut down you need a generator also.

Periodic cleaning of mouse, keyboard etc., using a vacuum cleaner prolongs their life.

Providing uninterrupted power supply may not be adequate in systems where operation has to continue without interruption, for example, a computer system in a race course during a racing

Even with the power-fail protect feature, content of the main memory is likely to be destroyed. To avoid such an inconvenience, an user should periodically save on the disk important sections of the memory.

event. One cannot permit the suspension of ticketing and other activities due to a disk failure. Here one talks of replicating the entire system so that one can use the *hot stand-by*. We refer to the stand-by as hot since it is running in parallel and has all the data and as such can take over instantly and continue without interruption.

Check point and Back-up

Whenever power is interrupted, the contents of the memory are destroyed. If a read/write from secondary storage is in progress, the current active file can also get corrupted. Since a file corruption is more serious, almost every PC has a power supply fail detection device which senses the decay of voltage and initiates a proper exit from the I/O module. Voltage does not decay instantly, it decays over several cycles (several 1/60th of a second). A modern fast processor can execute under hardware interrupt a fairly large service routine to ensure that all I/O activity are brought to normal closure. In fact, the PC is idling when the power finally decays to zero! But, it is very difficult to save the contents of the main memory, which is now-a-days rather large, in a temporary file. Hence, even with the power-fail protect feature, content of the main memory is likely to be destroyed. To avoid such an inconvenience, an user should periodically save on the disk important sections of the memory. This way, work done up to the last saving instant is recoverable, perhaps losing only a small amount of work done since the last update. Obviously, more frequent saving will reduce the amount of work to be redone. Hence, a professional sets up an adequate save feature, also referred to as "check-point" feature. Some software packages prompt the user to specify the periodicity of such check-point feature. One can restore the memory contents using the saved file, and back up as it were in time, provided all necessary register contents and status registers are also saved. However, work done since the last check point will be lost.

One can restore even the work done since the last check point by saving (journalizing) the transactions on a loss-less secondary storage such as a tape and re-running the transactions to create updated files. This way, cashing a cheque of a customer after last checkpoint can still be taken into account in maintaining the integrity of the master file. A bank customer would appreciate the need for such recovery, especially when it concerns a transaction of depositing cash into his/her account!

A sound back up policy and its stringent implementation is a must for responsible computerization.

Secondary storage does develop problems (such as crash) and files can get corrupted to such an extent that they become unusable. Ensuring against such a loss requires additional measures. One has to take periodic back up of the files and unload the storage medium from the computer system. If journalizing is set up, one can recover the last files using a recovery software utility. Such saving and unloading is referred to as *back-up*. However, backed up files must be stored safely. Since fire is a hazard that can destroy files, some organizations move back-up files to a remote place or keep them in a fire-proof area. It is quite possible that a back-up may become unreadable. As a hedge against such a possibility, one keeps several earlier back-ups (for two generations) with journal files so that even the back-up can be recreated. Since back-ups are used only to create a check point, one can save only the changes from the last back-up to reduce storage requirements. One can also use data compression techniques to reduce the size of the back-up. A sound back-up policy and its stringent implementation is a must for responsible computerization. Since good back-up depends on reliable secondary storage, it is natural to ask whether near perfect devices are available. Tapes come very near to perfection, but are slow for accessing a particular piece of information. Optical recording using etching of the disk surface using a laser beam offers a permanent (write once and read several times) back-up storage. Several banks use such writeable optical disks to create near permanent storage, almost similar to a conventional paper file. Note the

Optical recording using etching of the disk surface using a laser beam offers a permanent (write once and read several times) back-up storage.

Encryption is a method used to protect information from falling into wrong hands during communication.

use of the word near-permanent, for fire, water and chemicals can still damage the disk! Conventional CDROM disks also provide near-permanent storage.

Encryption and Decryption

Encryption, a method of transforming a data file into a coded form which can be decrypted only by the intended receiver, is a method used to protect information from falling into wrong hands during communication. A simple method of encryption is to substitute each alphabet by another using a table. The intended user knows the table and uses it to get the original message back. An eavesdropper has to try several tables (decryption method) before finding the right one. Many of the simple encryption schemes are good enough in ordinary situations where there is no serious attempt to eavesdrop. However, banks naturally want more secure systems, because they don't want crooks to send fake payment orders copying a true one which they have intercepted. Here, one is looking for an encryption scheme which is virtually unbreakable, in a reasonable time (few days), even by using a supercomputer. Further, there is another interesting requirement of being able to identify, without dispute, the sender of the message, as if it has been signed by the sender. There are what are called trap functions which make the reverse transformation by trial and error that take rather large time. One method of such encryption goes by the name of public key encryption system (PKES). PKES is based on the fact that it is very difficult (computationally complex) to find the factors of a very large number, which is a product of two prime numbers, by trial and error. One can derive a public key from such a product which is used for encrypting (multiply and shift) at the sending end. The coded message can then be decoded effortlessly by using the corresponding private key which is known only to the intended receiver. Every person who intends to use PKES will publicize a public key to be used for encrypting messages to be sent to him, and only he can decode the message using the private key.

Viruses are codes (programs) written by aberrant individuals to create problems which can sometimes be highly destructive.

Virus Detection and Clean up

Viruses are codes (programs) written by aberrant individuals to create problems which can sometimes be highly destructive. These codes have to get into a system and get executed to create the havoc. Hence, the best defence against viruses is to check every file or medium that enters a computer system. Viruses get attached to boot-strap routines on disk or diskette, which are executed (.com files) while starting the system. When executed, they can replicate themselves or overwrite other files. Replication can reduce available memory or disk space and can lead to slowing down of the system. Overwriting can corrupt files. The ego of the virus creator may also present itself as modification to screens on the monitor which can be irritating.

The best defence against viruses is to check every file or medium that enters a computer system.

Some viruses do no more damage than taunting the user. Trojans are codes that lie dormant in a well behaved software until they are triggered by an event such as a particular date, time or incident (dismiss the perpetrator or add a new employee). Some trojans write garbage on files or attach themselves to files so that they can create damage when the file is executed.

Virus is detected by checking whether files on a system have been altered. One common sign of alteration is increase/decrease in length of files One can also use special error detection tests to sense alteration. The pattern of change allows one to identify the virus and one can remove it by appropriate modification. Antivirus software look for tell tale signs of each virus known or each type of modification and do the cleaning up. It may not always be possible to restore an infected file. Hence, it is a good practice to keep back-ups to use after cleaning up. Anything unexpected, such as slowing down, increase in file lengths, alteration of screens, etc. is a sign of virus infection. An user must learn to suspect virus.

Anything unexpected such as slowing down, increase in file lengths, alteration of screens, etc. is a sign of virus infection.

Preventing entry is the best protection against viruses. All incoming files on diskettes must be scanned for virus using a popular antivirus software. Some viruses can enter even through

Game diskettes are likely to be infected often, since there is indiscriminate copying and they pass through several systems. Banning of entry of game diskettes into serious computing environments is worth considering.

commercial software packages ; a virus affected the popular word processing software WORD by Microsoft. It is best to set up in an organization, a PC only for scanning for virus; diskettes are used on other systems only after they are found to be free from virus.

Game diskettes are likely to be infected often, since there is indiscriminate copying and they pass through several systems. Banning of entry of game diskettes into serious computing environments is worth considering. Several servers on the Internet which host public files such as bulletin board, free ware etc. are likely to have infected files. One should be careful in down loading from such sources. One can very well imagine how a virus developer will take advantage of the habit of individuals to down load whatever is free and looks attractive on the net. One should down load into a sentry (with antivirus software) machine and disinfect the files before loading them into work machines.

Fault Tolerant Coding and Algorithms

The nomenclature 'fault tolerant' should not be interpreted as tolerating faults, but the algorithm is designed to check for faults and eliminate them or at least warn the user. Ever since

Box 2. Virus from Internet?

One can now down load from the Internet a code called Applet, which can be executed . Since use of Applets is an attractive proposition, both for the vendor and user, there has been concern about Applets being used as carrier of virus. JAVA language designed to develop Applets has been designed to prevent an Applet from accessing any files local to the running system. Hence, a virus on an Applet can do damage only to itself and not to the visiting system. All this works fine if one uses a clean JAVA compiler. How does one prevent virus developers distributing unsafe compilers and execution software? Obviously, one must be careful about JAVA tools from unknown sources. Since pointer variables are useful to sneak into forbidden areas of main memory, JAVA has excluded pointer feature in the language. Since global networking has come to stay, geographic boundaries are no barrier to virus. Virus has become part of life and one should not get paranoid about it. The safest approach is to set up a sound virus control procedure and use it religiously.

Box 3. Minimum Security Measures Mandatory While Using a PC

1. Protect PC from high voltages and spikes by using a voltage stabilizer and a spike buster.
2. Save your work periodically (every 30 mins.) on disk. Some software packages such as WORD can be set to do it automatically.
3. Back-up important files on diskettes periodically (every week or more frequently) to enable recovery in case of disk problems. One can use data compression to reduce the storage space required.
4. Install an anti-virus software to check all incoming diskettes and clean up as required. One has to be quite religious about this.
5. Avoid down loading software from unreliable network sources, especially such as bulletin boards, freeware etc.
6. Use screen saver to reduce burn-in of the monitor screen. It is better to leave the power on, rather than subject it to frequent shut downs and start ups.
7. Use password protection wherever possible and change the password often to avoid it being compromised.
8. Write *protect* against writing on to sensitive files so that one does not accidentally modify it.
9. Use some simple encryption, if you are worried that a file will be read by unintended persons.
10. Use molded plastic key board covers to prevent dust getting in between keys.
11. Use heavy duty printers if the printing load is heavy.
12. Clean periodically old generation (5.25 in) floppy drives to avoid file reading errors.

one found that components can fail and produce wrong answers, not so glaring as to be easily detectable, one has looked for ways of programmatically checking the correctness of the answer by building error detecting features in programs. An example of error (or fault) checking is that whenever at least one multiplicand is even, the answer of that multiplication should be even. Performing calculation in two different ways and comparing the answers is another method of detecting a fault. Unfortunately, in case of difference, one cannot decide which one of the answers is correct!

It is possible to design algorithms, actually extensions to an algorithm, to make it fault tolerant.

One can also use redundant data to check for errors. If one is entering a large number of amounts (say amounts on cheques) one can also enter their total and the number of those amounts. Missing or repetition of amounts can be detected by checking against the total number of entries and the control total can be used to detect error in entering an amount. A good systems analyst will routinely use such error control measures. Entering the amounts all over again by a different operator is a good way to detect data entry errors. It is possible to design algorithms, actually extensions to an algorithm, to make it fault tolerant. Error detecting and correcting codes are one such method. (See article in *Resonance*, Vol. 1, No.10).

Conclusions

It is not enough to build systems, which expect everything to work correctly, for them to operate satisfactorily. There will be many a 'slip between the cup and the lip'. A professional approach to building a reliable system would be to build in necessary fault tolerance so that the users are fully protected. To ignore security aspects is like embarking on a long journey into a jungle without even the first aid kit. In *Box 3* we give a list of measures that every PC user has to take to avoid catastrophes.

Suggested Reading

- **Ferbrache D. *A Pathology of Computer Viruses*. Springer-Verlag. Berlin, 1992.**
- **Leveson N G. *Software: System Safety and the Computer Age*. Addison-Wesley. Reading. MA, 1995.**
- **Peter G Neuman. *Computer Related Risks*. Addison-Wesley. Reading. MA, 1995.**
- **Rajaraman V and Mandke V V (Editors). *Information Integrity - Issues and Approaches*. Information Integrity Foundation. New Delhi, 1996.**

Address for Correspondence
H N Mahabala
Infosys Technologies Ltd.
Electronics City, Hosur Road
Bangalore 561 229, India
email: mahabala@inf.com

It is a mistake to believe that a science consists in nothing but conclusively proved propositions, and it is unjust to demand that it should. It is a demand only from those who feel a craving for authority in some form and a need to replace the religious catechism by something else, even if it be a scientific one.

Sigmund Freud