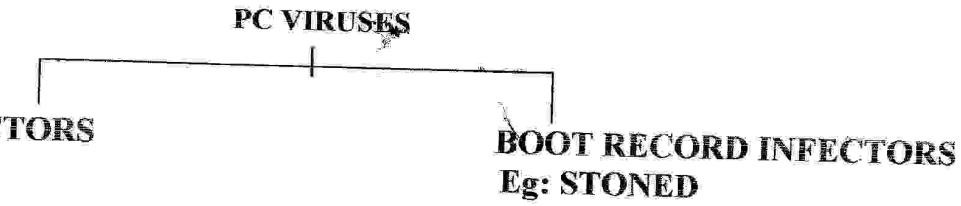
What are COMPUTER VIRUSES?

A Computer Virus is a SELF-REPLICATING program containing code that explicitly copies itself and that can "INFECT" other programs by modifying them or their environment such that a call to an infected program implies a call to a possibly evolved copy of the virus.



*DIRECT ACTION VIRUSES:

Infects not only programs which are executed but also programs which are opened.

Eg: DARTH VADER VIRUS

*RESIDENT VIRUSES:

Copies itself in the memory and then infects programs which are to be executed.

Eg: JERUSALEM

*MACRO VIRUSES:

Based on auto-open macros which are self replicating.

Eg: CONCEPT ,NUCLEAR,ADAM.

*POLYMORPHIC VIRUSES:

They alter their structure so as to avoid detection from anti- viruses

*STEALTH VIRUSES:

They hide the modification s made to the files or boot records so avoid detection.

Eg: BRAIN.

*VIRUSES SPREAD VERY QUICKLY DUE TO THE FOLLOWING FACTORS:

- A LARGE TARGET POPULATION
- A LARGE VIRUS POPULATION
- OUTDATED HARDWARE USED
- ABSENCE OF ANTI-VIRAL CHECKS FOR A LONG TIME

*VIRUS HOAXES:

They are delibrate email messages warning people about viruses. They include:

***WARNINGS ABOUT ALLEGED NEW VIRUSES AND THEIR DAMAGING CONSEQUENCES**

***DEMANDS TO FORWARD THIS MAIL TO WARN AS MANY PEOPLE AS POSSIBLE.**

*LAN AWARE VIRUSES:

Eg: KNOCK AND HACK VIRUSES demonstrate their effects on NETWARE 3.10 AND BELOW.

VIRUSES : A MODE OF TERRORIST ATTACK

ANTIVIRUS TECHNIQUES:

*ACTIVE MONITORING SYSTEM:

They look out for virus like activities.

*INTEGRITY CHECKERS:

They compute a hash value for the uninfected program and then compare it with the modified program to check for viral infections.

What are computer viruses ?

First, what is a virus? A virus is simply a computer program that is intentionally written to attach itself to other programs or disk boot sectors and replicate whenever those programs are executed or those infected disks are accessed. Viruses, as purely replicating entities, will not harm your system as long as they are coded properly. Any system damage resulting from a purely replicating virus happens because of bugs in the code that conflict with the system's configuration. In other words, a well-written virus that only contains code to infect programs will not damage your system. Your programs will contain the virus, but no other harm is done. The real damage--the erasing of files, the formatting of hard drives, the scrambling of partition tables, etc.--is caused by intentional destructive code contained within the virus. Generally, the destructive part of a virus is programmed to execute when certain conditions are met, usually a certain date, day, time, or number of infections. An example is the now infamous Michelangelo virus. This virus can run rampant on your computer for months and you won't notice that anything is wrong. That is because even though your hard disk's master boot record is infected with the virus, the destructive code has not yet been executed. The virus is programmed to trigger its destructive code on March 6, Michelangelo's birthday. Therefore, if Michelangelo contained no destructive code, nothing bad would happen to your computer even though it was infected with a virus.

An important thing to remember is that not all virus attacks produce catastrophic results. Fred Cohen "wrote the book" on computer viruses, through his Ph.D. research, dissertation and various related scholarly publications. He developed a theoretical, mathematical model of computer virus behaviour, and used this to test various hypotheses about virus spread.

A computer virus is a self-replicating program containing code that explicitly copies itself and that can "infect" other programs by modifying them or their environment such that a call to an infected program implies a call to a possibly evolved copy of the virus.

These software "pranks" are very serious; they are spreading faster than they are being stopped, and even the least harmful of viruses could be life-threatening. For example, in the context of a hospital life-support system, a virus that "simply" stops a computer and displays a message until a key is pressed, could be fatal. Further, those who create viruses can not halt their spread, even if they wanted to.

Types of Viruses

The classes of virus outlined here are not the only ones in existence. Further, most effective viruses are actually a combination of multiple varieties.

File Infectors

File infectors are textbook-perfect viruses. They most often attach to program files, but can infect any file with executable code, including script files or program configuration files. When the program, script, or configuration is executed, the virus is executed as well.

System or Boot-record Infectors

A system or boot-record infector does not necessarily infect a file. It targets, instead, certain areas of a hard disk used exclusively for system processes. These areas include the boot-record. The boot-record is a section of the disk dedicated to booting the operating system. On a diskette, these infectors attach themselves to the DOS boot sector; on a hard disk, onto the Master Boot

Record. Having infected a Master Boot Record, the virus spreads to the boot sectors of insertable media.

Multi-partite Viruses

Multi-partite viruses infect boot records as well as files. With its hybrid nature, a multi-partite virus gains the worst qualities of each of its parents, and consequently is far more contagious and destructive than either.

What Is A Macro Virus?

The most common viruses that infect computers today--viruses such as Concept, Nuclear, Showoff, Adam, Wazzu, and Laroux--are macro viruses. They replicate by a completely different method than conventional viruses. We said earlier that a virus is a small computer program that needs to be executed by either running it or having it load from the boot sector of a disk. These types of viruses can spread through any program that they attach themselves to. Macro viruses can not attach themselves to just any program. Rather, each one can only spread through one specific program. The two most common types of macro viruses are Microsoft Word and Microsoft Excel viruses. These two programs are equipped with sophisticated macro languages so that many tasks can be automated with little or no input from the user. Virus writers quickly realized that it would be possible to construct self-replicating macros using these languages. The reason why this is possible is because Word documents and Excel spreadsheets can contain auto open macros. This means that when you open a Word Document in Word or an Excel spreadsheet in Excel any auto open macros contained within the document will execute automatically and you won't even know it's happening. In addition to auto open macros, both of these programs make use of a global macro template, which means that any macros stored in this global file will automatically execute whenever something is opened in that program. Macro viruses exploit these two aspects to enable themselves to replicate.

Here's how it works... You open an infected document in Microsoft Word. (Remember, Word documents can contain auto open macros). These macros, which in this example, contain a virus, execute when the document is opened and copy themselves into the global template that Word uses to store global macros. Now, since the infected macros are now part of your global template file they will automatically execute and copy themselves into other word documents whenever you open any document in Microsoft Word. Excel macro viruses work in relatively the same way. Because Word documents and Excel spreadsheets contain auto open macros it is important to think of them as computer programs in a sense. In other words, when you open Word documents in Word, or excel spreadsheets in Excel, you could be executing harmful code that is built right into the objects you're opening.

Polymorphic Virus

Polymorphic viruses create varied (though fully functional) copies of themselves as a way to avoid detection from anti-virus software. Some polymorphic virus use different encryption schemes and requires different decryption routines. Thus, the same virus may look completely different on different systems or even within different files. Other polymorphic viruses vary instruction sequences and use false commands in the attempt to thwart anti-virus software. One of the most advanced polymorphic viruses uses a mutation-engine and random-number generators to change the virus code and its decryption routine. See Also: Mutating Virus. A polymorphic virus tries to evade detection by altering its structure or its encryption techniques. Each time an infection occurs, a polymorphic virus changes its form, confusing antivirus

scanners. Because scanners use certain unique "signature" characteristics to identify viruses, any virus that changes its form presents a formidable new challenge.

Trojan Horse Program

A Trojan horse program is a malicious program that pretends to be a benign application; a Trojan horse program purposefully does something the user does not expect. Trojans are not viruses since they do not replicate, but Trojan horse programs can be just as destructive. Many people use the term to refer only to non-replicating malicious programs, thus making a distinction between Trojans and viruses. Also: Trojan

Tunneling

A virus technique designed to prevent anti-virus applications from working correctly. Anti-virus programs work by intercepting the operating system actions before the OS can execute a virus. Tunneling viruses try to intercept the actions before the anti-virus software can detect the malicious code. New anti-virus programs can recognize many viruses with tunneling behavior.

What is a Worm?

A computer WORM is a self-contained program (or set of programs), that is able to spread functional copies of itself or its segments to other computer systems (usually via network connections).
Note that unlike viruses, worms do not need to attach themselves to a host program. There are two types of worms--host computer worms and network worms.
Host computer worms are entirely contained in the computer they run on and use network connections only to copy themselves to other computers. Host computer worms where the original terminates itself after launching a copy on another host (so there is only one copy of the worm running somewhere on the network at any given moment), are sometimes called "rabbits."
Network worms consist of multiple parts (called "segments"), each running on different machines (and possibly performing different actions) and using the network for several communication purposes. Propagating a segment from one machine to another is only one of those purposes. Network worms that have one main segment which coordinates the work of the other segments are sometimes called "octopuses."

What are the main types of PC viruses?

Generally, there are two main classes of viruses. The first class consists of the FILE INFECTORS which attach themselves to ordinary program files. These usually infect arbitrary COM and/or EXE programs, though some can infect any program for which execution or interpretation is requested, such as SYS, OVL, OBJ, PRG, MNU and BAT files.
File infectors can be either DIRECT-ACTION or RESIDENT. A direct-action virus selects one or more programs to infect each time a program infected by it is executed. A resident virus installs itself somewhere in memory (RAM) the first time an infected program is executed, and thereafter infects other programs when they are executed (as in the case of the Jerusalem virus) or when other conditions are fulfilled. Direct-action viruses are also sometimes referred to as NON-RESIDENT. The Vienna virus is an example of a direct-action virus. Most viruses are resident.
The second main category of viruses is SYSTEM or BOOT-RECORD INFECTORS: these viruses infect executable code found in certain system areas on a disk. On PCs there are ordinary

boot-sector viruses, which infect only the DOS boot sector, and MBR viruses which infect the Master Boot Record on fixed disks and the DOS boot sector on diskettes. Examples include Brain, Stoned, Empire, Azusa and Michelangelo. All common boot sector and MBR viruses are memory resident.

To confuse this classification somewhat, a few viruses are able to infect both files and boot sectors (the Tequila virus is one example). These are often called "MULTI-PARTITE" viruses, though there has been criticism of this name; another name is "BOOT-AND-FILE" virus.

Aside from the two main classes described above, many antivirus researchers distinguish either or both of the following as distinct classes of virus:

FILE SYSTEM or CLUSTER viruses (e.g. Dir-II) are those that modify directory table entries so that the virus is loaded and executed before the desired program is. The program itself is not physically altered, only the directory entry of the program file is. Some consider these to be a third category of viruses, while others consider them to be a sub-category of the file infectors.

KERNEL viruses target specific features of the programs that contain the "core" (or "kernel") of an operating system (3APA3A is a DOS kernel virus and is also multipartite).

What is a stealth virus?

A STEALTH virus is one that, while "active", hides the modifications it has made to files or boot records. This is usually achieved by monitoring the system functions used to read files or sectors from storage media and forging the results of calls to such functions. This means programs that try to read infected files or sectors see the original, uninfected form instead of the actual, infected form. Thus the virus's modifications may go undetected by antivirus programs. However, in order to do this, the virus must be resident in memory when the antivirus program is executed and this may be detected by an antivirus program.

Example: The very first DOS virus, Brain, a boot-sector infector, monitors physical disk I/O and re-directs any attempt to read a Brain-infected boot sector to the disk area where the original boot sector is stored.

B7) What are "fast" and "slow" infectors?

SLOW INFECTOR:

A typical file infector (such as the Jerusalem) copies itself to memory when a program infected by it is executed, and then infects other programs when they are executed.

A FAST infector is a virus that, when it is active in memory, infects not only programs which are executed, but even those that are merely opened. The result is that if such a virus is in memory, running a scanner or integrity checker can result in all (or at least many) programs becoming infected. Examples are the Dark Avenger and the Frodo viruses.

An example is the Darth Vader virus.

B8) What is a sparse infector?

The term "sparse infector" is sometimes used to describe a virus that infects only occasionally (e.g. every tenth program executed), or only files whose lengths fall within a narrow range, etc. By infecting less often, such viruses try to minimize the probability of being discovered.

B9) What is a companion virus?

A COMPANION virus is one that, instead of modifying an existing file, creates a new program which (unknown to the user) is executed instead of the intended program. On exit, the new program executes the original program so that things appear normal. On PCs this has usually been accomplished by creating an infected .COM file with the same name as an existing .EXE file. Integrity checking antivirus software that only looks for modifications in existing files will fail to detect such viruses.

B12) What is a tunnelling virus?

A TUNNELLING VIRUS is one that finds the original interrupt handlers in DOS and the BIOS and calls them directly, thus bypassing any activity monitoring program which may be loaded and have intercepted the respective interrupt vectors in its attempt to detect viral activity.

B13) What is a dropper?

A DROPPER is a program that has been designed or modified to "install" a virus onto the target system. The virus code is usually contained in a dropper in such a way that it won't be detected by virus scanners that normally detect that virus (i.e., the dropper program is not infected with the virus). While quite uncommon, a few droppers have been discovered.

B14) What is an ANSI bomb?

An "ANSI bomb" is a sequence of characters, usually embedded in a text file, that reprograms various keyboard functions of computers with ANSI console (screen and keyboard) drivers. In theory a special sequence of characters could have been included in this FAQ sheet to reprogram your Enter key to issue the command "format c:" with a return character tacked on the end. Such a possibility however, need not translate into much of a threat. It is rare for modern software to require the computer it runs on to have an ANSI console, so few PCs or other machines should load ANSI drivers.

How many viruses are there?

It is not possible to give an exact number because new viruses are literally being created every day. Furthermore, different antivirus researchers use different criteria to decide whether two viruses are different or one and the same. Some count viruses as different if they differ by at least one bit in their non-variable code. Others group viruses in families and do not count the closely related variants within a family as different viruses.

Further, some antivirus researchers have samples in their collections that they count as viruses, but that several other experts strongly deny are viruses. Sometimes these are "partial viruses", where a virus has not properly infected a host and are therefore non-infective, other times they are well-known non-viruses. As some of these non-viruses are known to be in some of the common test sets, some antivirus software vendors count them amongst the viruses they detect.

As of January 1995 there were about 5,600 PC viruses, about 150 Amiga viruses, about 100 Acorn Archimedes viruses, about 45 Macintosh viruses, several Atari ST viruses, a few Apple II

viruses, four Unix viruses, three MS Windows viruses, at least two OS/2 viruses and two VMS DCL-based viruses.
Fortunately, few of the existing viruses are widespread. For instance, only about three dozen of the known PC viruses cause most of the reported infections and fewer than 200 PC viruses have been found in the wild at all.

F2) How do viruses spread so quickly?

This is a very complex issue, and some viruses don't spread quickly at all (though talk of them often does!).
Those that do spread widely are able to do so for a variety of reasons. A large target population--millions of compatible computers--helps. A large virus population helps. Vendors whose quality assurance relies on, for example, outdated scanners, help. Users who gratuitously install new software on their systems without making any attempt to test for viruses help. All of these things are factors.

F7) I've heard talk of "good viruses". Is it possible to use a computer virus for something useful?

Companion Virus
Companion viruses use a feature of DOS that allows software programs with the same name, but with different extensions, to operate with different priorities. Most companion viruses create a COM file which has a higher priority than an EXE file with the same name.
Thus, a virus may see a system contains the file PROGRAM.EXE and create a file called PROGRAM.COM. When the computer executes PROGRAM from the command line, the virus (PROGRAM.COM) runs before the actual PROGRAM.EXE. Often the virus will execute the original program afterwards so the system appears normal.

Logic Bomb
A logic bomb is a type of trojan horse that executes when specific conditions occur. Triggers for logic bombs can include a change in a file, by a particular series of keystrokes, or at a specific time or date. See: Time Bomb

Mailbomb
n. Excessively large e-mail (typically many thousands of messages) or one large message sent to a user's e-mail account, for the purpose of crashing the system, or preventing genuine messages from being received.
v. To send a mailbomb.

Virus Hoaxes
Hoaxes are not viruses, but are usually deliberate or unintentional e-messages warning people about a virus or other malicious software program. Some hoaxes cause as much trouble as viruses by causing massive amounts of unnecessary e-mail.
Most hoaxes contain one or more of the following characteristics:
Warnings about alleged new viruses and its damaging consequences,
Demands the reader forward the warning to as many people as possible,
Pseudo-technical "information" describing the virus,
Bogus comments from officials: FBI, software companies, news agencies, etc.

Targetted Attacks.

Another trend that we can see nowadays is the creation of viruses designed to target particular anti-virus products. The more popular the anti-virus product is, the more likely that it will be attacked.
The attacks can range from benign ones - just avoiding infecting a program known to perform some kind of self-checking - to sophisticated ones, designed to fool the user that the protection is still in place and working, while actually disabling it.
Just a few examples. There are already many viruses which avoid infecting programs with names beginning with "SC" or something like that. The Tequila virus removes the checksums that the program ViruScan (from McAfee) adds to the files (when used with the /AV option). The Peach virus successfully attacks the integrity checking in Central Point Anti-Virus by simply deleting the databases of checksums that the product creates.

LAN-aware Viruses.

Many of the currently existing viruses simply crash when executed on a computer with a LAN shell loaded. There are also, however, many that behave well enough and are able to successfully run and infect. If the security settings of the LAN allow them to modify the files, of course. At last, there are about a dozen (actually - variants of two main families), which are LAN-aware. Currently, this awareness consists in monitoring some of the undocumented interrupts used in Novell NetWare and using them to steal passwords that are sent in unencrypted packets. This is, however, still too primitive - we must expect significant sophistication in this area in the future. The LAN hackers have discovered some very serious security holes in Novell NetWare. They have created two programs that demonstrate these holes - KNOCK and HACK .
KNOCK works successfully on NetWare versions 3.10 and below. It is able to log into any given account, without knowing the password for this account, exploiting a bug in the NetWare's encryption algorithm. Of course, the supervisor account represents the greatest danger, because it has the highest privileges.
HACK is another program which, reportedly, is able to log in from a workstation as any user (the supervisor is the most interesting one, of course), which is already logged in - from another workstation. The method used by HACK relies on spoofing IPX packets. It is based on a very serious design bug in the NetWare, which can be fixed only with a complete re-design of the system or with full public-key based encryption of the packets that pass through the line. Novell has solved the problem in version 4.x of NetWare. Meanwhile, they have distributed security patches for the users of the older versions. Unfortunately, those patches seem to cause additional problems when installed - they occasionally log out perfectly legitimate users. Therefore, until version 4.x becomes widely used, this security hole is likely to be present on many networked computers. It is only a question of time until the viruses begin to use it. The main question is whether this time will be enough to replace the old versions of NetWare.
Another LAN-related virus problem has nothing to do with bugs and security holes and is connected to the ability of the viruses to spread transitively. Most LAN administrators are reasonable enough to set the protection settings in the directories that contain the executable files used by everybody in such a way, that the users are able only to list, read, and execute the files. However, viruses don't need to have direct access to the files in order to infect them. All they need is to have access to the files of somebody who has access to the protected files, or to somebody who has access to the files of somebody who has access to the protected files, or... In

short, there must be a transitive path of information flow between somebody who has access to the protected files (at least the supervisor does) and some other, already infected account. Additionally, viruses could use other LAN-oriented features. For instance, if the virus has Create rights in a directory, it is possible to use a companion-type attack to infect the EXE files in it, even if the files themselves are write-protected . Next, if a user does not have Write rights to the files but does have the right to Modify the rights, a virus could use this to temporary grant itself Write rights, in order to infect the files. It is important to note that a virus always runs with the effective rights of the user whose workstation is infected. For this reason, the users with supervisor privileges are particularly vulnerable and dangerous. Therefore, they should use extreme care when logging into their accounts with such privileges.

Viruses for Other Operating Systems and Computers.

Nowadays, the platform that is most attacked by viruses is the IBM PC compatible computer running MS-DOS. Viruses for the Macintosh platform are very widespread too, but there are not very many of them and the existing anti-virus software is able to handle all of them properly. As alternative operating systems to MS-DOS become more widely used, viruses that attack them will appear. We already have several Windows-specific and OS/2-specific viruses. They are relatively simple, but much more sophisticated ones are possible. The DR-DOS (and Novell DOS 7) operating system has begun to gain popularity. The currently existing protections in it (passwords) are trivial to bypass by a knowledgeable attacker, but they are able to stop most of the currently existing viruses. Nevertheless, we expect to see viruses in the future that will be able to detect this operating system and to modify, disable, bypass, or even use its security features.

Multi-Platform Viruses.

This problem is somehow related to the previous one, although we do not expect it to become a serious threat in the future.
The current viruses are limited to a particular platform. There is no way for an MS-DOS virus to infect a Macintosh computer - unless the latter is running some kind of MS-DOS emulator. And even then, the infection will be limited within the emulated environment.
It must not be necessarily so. It is perfectly possible to write a virus that will be able to work on more than one kind of CPU. In particular, a boot sector infector for both IBM PCs and Atari STs is particularly easy - because the two computers use almost the same file systems [Ferbrache]. A Mac-IBM infector is more difficult to write, but still perfectly possible. One could even imagine a program that spreads like a worm between Internet-connected Unix machines. Once it succeeds to install itself on a machine, it could use virus techniques specific to the particular hardware, in order to gain full control of the machine and spread further.
Nevertheless, we believe that the multi-platform viruses will not represent a considerable problem in the future. It is much easier to write two viruses for two different platforms than a single virus that is able to spread on any of the two platforms. In the same time, such multi-platform virus will not spread easily between the two platforms, because the software exchange between them is relatively low.

Viruses Used as Weapons.

Several countries are reportedly researching into the possibilities to use viruses as a weapon against an enemy. However, it is unlikely that the outcome of such research will be positive - computer viruses are too difficult to aim towards a particular target. They could be used much

more successfully in a terrorist attack - when the attacker does not know and does not care how much and which particular targets will be hit.
The countries which are more vulnerable to this kind of attack are the most developed ones - the ones which are widely relying on computers in their economics. A virus attack could be even more successful if performed on a cluster of highly networked computers, especially if the virus used knows and uses the security holes in the network to spread itself faster.

Spying Agents
The threat of spying, or espionage-enabled, malicious agents gained spotlight in 1999 with the emergence of viruses such as Caligula and Marker, which demonstrated the growing trend of virus authors to create agents that take advantage of the Internet connectivity in one way or another.
Spying agents are especially dangerous because they can transmit sensitive information from the organization to the author of the virus. Much like the Melissa Virus, these programs typically infiltrate the network defense perimeter via open channels such as e-mail or Web browsing. To increase the likelihood of establishing a successful link back to the home base, spying agents typically mask outbound transmissions as mundane e-mail or Web browsing traffic.

The Caligula Virus
The Caligula Virus, known to virus enthusiasts as W97M/Caligula, caught the public's eye around January 1999 [SYM1] primarily because of its attack on PGP, which is a common encryption program hailed for effective confidentiality features. When activated, the virus attempted to locate a PGP secret keyring file, which stores sensitive user information, and transmitted it to the author of the virus.
Although a password was usually required to read contents the PGP secret keyring, Caligula demonstrated a powerful technique for obtaining sensitive information from an attack target – the virus initiated outbound sessions using the computer's built-in ftp.exe command to communicate with the author. [TR] Because most firewall policies allow users to retrieve FTP files from the outside, the virus can use a protocol such as FTP to initiate connections to the home base from inside the victim's network.

Antivirus:
ACTIVITY MONITORING programs. These try to prevent infection before it happens by looking for virus-like activity, such as attempts to write to another executable, reformat the disk, etc. An alternative term is **BEHAVIOR BLOCKER**.

Examples: SECURE and FluShot+ (PC), and GateKeeper (Macintosh).
These programs are considered the weakest line of defense against viruses on a system that does not have memory protection, because in such an environment it is possible for a tunnelling virus to bypass or disable them.

1. **SCANNERS**. Most look for known viruses by searching your disks and files for "scan strings" or patterns, but a few use heuristic techniques to recognize viral code. Most now also include some form of "algorithmic scanning" in order to detect known polymorphic viruses. A scanner may be designed to examine specified disks or files on demand, or it may be resident, examining each program which is about to be executed. Most scanners also include virus removers.

Scanners are the most convenient and the most widely used kind of antivirus programs. They are a relatively weak line of defense because even the simplest virus can bypass them if it is new and unknown to the scanner. Therefore, your virus protection system should not rely on a scanner alone.

2. **INTEGRITY CHECKERS** or **MODIFICATION DETECTORS**. These compute a small "checksum" or "hash value" (usually CRC or cryptographic) for files when they are presumably uninfected, and later compare newly calculated values with the original ones to see if the files have been modified. This catches unknown viruses as well as known ones and thus provides **generic** detection. On the other hand, modifications can also be due to reasons other than viruses. Usually, it is up to the user to decide which modifications are intentional and which might be due to viruses, although a few products give the user help in making this decision. As in the case of scanners, integrity checkers may be called to checksum entire disks or specified files on demand, or they may be resident, checking each program which is about to be executed (the latter is sometimes called an **INTEGRITY** SHELL). A third implementation is as a **SELF-TEST**, where the checksumming code is attached to each executable file so they check themselves just before execution. It is generally considered a bad idea to add such code to existing executables.
   Examples: ASP Integrity Toolkit (commercial), and Integrity Master and VDS (shareware), all for the PC.
   Integrity checkers are considered to be the strongest line of defense against computer viruses, because they are not virus-specific and can detect new viruses without being constantly updated. However, they should not be considered as an absolute protection--they have several drawbacks, cannot identify the particular virus that has attacked the system, and there are successful methods of attack against them too.