Answers to Exercises

> A bird does not sing because he has an answer,
> he sings because he has a song.
>
> —Chinese Proverb

Pre.1: One approach to this problem is to sabotage the computer from time to time by creating a short circuit. When the technicians arrive in the computer room, you can cut short your shift and go home. The author isn't recommending such a solution, but similar stories (some perhaps true) have been circulating in the computer security community for many years.

Intro.1: The car industry. A modern car has several computers that control its operations and sense failures. As a result, many millions of small, specialized computers are purchased and installed by car manufacturers every year. Fortunately, there haven't been yet any security problems with those special, embedded computers, but they have become themselves a major source of car trouble.

Reference [per-capita 10] has a list of countries sorted by the number of computers per million people. Surprisingly, Switzerland is the first.

Intro.2: The question is meaningless. A computer is a machine and as such is neither trustworthy nor untrustworthy. These terms are attributes of humans, which implies that trusting a computer really means trusting those who designed and built it.

> The question of whether computers can think is just like the question of whether submarines can swim.
>
> —Edsger W. Dijkstra

Intro.3: A hacker who has physical access to your computer can replace your keyboard with a rigged one that has a radio transmitter. The hacker would then receive and record all your keystrokes even if you check for spyware and remove all of it.

Intro.4: Your accent can tell much about your origin, as the following quotation illustrates.

> Simply phonetics. The science of speech. That's my profession; also my hobby. Happy is the man who can make a living by his hobby! You can spot an Irishman or a Yorkshireman by his brogue. I can place any man within six miles. I can place him within two miles in London. Sometimes within two streets.
> —George Bernard Shaw, *Pygmalion* (1916).

Intro.5: The following is an example: Security holes and weaknesses lurk everywhere and no amount of user testing and expert tinkering can find them all. They are discovered slowly, one by one, but every new piece of software written and every new piece of hardware built may contain a new security flaw.

1.1: Yes, because of two reasons. (1) Most passwords are short enough such that 20% of the password is just one character, which makes it easy to use a brute-force approach to guess the missing character. (2) A computer user may enter the same password several times a day, making it trivial for a spy to complete a missing character.

1.2: Two things. A hard disk may crash and files may be left open and become inaccessible as a result.

1.3: Because basements are prone to flooding.

1.4: The first step is to consult a `whois` data base such as [Network solutions 04] to locate the owner of the IP number in question. This is either an ISP or a large organization that has been assigned a block of IP numbers. The second step is to convince the owner to identify the user located at the IP number.

1.5: Given an unknown data item A, if we repeatedly add to it random numbers that are distributed normally with mean m, we end up with random numbers that are distributed normally with mean $m + A$, thereby allowing an accurate estimation of the unknown data.

2.1: A personal computer may be used by several users (such as the members of a family). At any given time, only one user can use the keyboard and display, but in principle a user can log in, start a program, and leave, only for another user to log in and start another task. Thus, the operating system of such a computer should allow each user access only to their files and should be able to allocate time slices to several programs. However, an operating system on a personal computer can restrict the use of the computer to one user at a time (a user has to log off before another user can log on) which means that only the programs of one user can reside simultaneously in memory. Even in such a case, the operating system has to protect each program

from all the other ones. Thus, the answer is yes, a personal computer can be considered a multiuser computer, with the single exception that only one user sits at the keyboard at any time.

2.2: Here is one in Java (it should be typed on a single line).

```
class s{static public void main(String[]x)
{String a="class s{static
public void main(String[]x){String a=;System.out.print
(a.substring(0,52)+(char)34+a+(char)34+a.substring(52));}}";
System.out.print
(a.substring(0,52)+(char)34+a+(char)34+a.substring(52));}}
```

2.3: Most computer peripherals have moving parts and can be damaged by forcing them to repeat certain operations many times. Here are some examples.

■ A DVD is normally read-only, but there are recordable DVDs (DVD-R) that can be recorded once by the computer, and even recordable rewritable DVDs (DVD-RW), that can be recorded, erased, and reused by the computer many times. Malicious software can erase such a DVD every time it is inserted into the optical drive. Even worse, it can erase the DVD many times in a short period of time, thereby shortening its life.

■ The popular flash memories can be damaged in the same way.

■ An uninterruptible power supply (UPS) is the next example. Such a device uses a line-voltage battery to support the computer for a short time in case of a power failure. Many UPS devices are connected to the computer with a USB cable and can launch a utility that closes all the open files and active applications, and turns the computer off when the battery runs low. Malicious software can corrupt this utility such that it opens many files and continually spins the hard drive. When battery power runs out, there is a good chance that the read/write head of the hard drive will crash, thereby physically damaging the drive.

■ Old dot-matrix printers had many small moving parts and it was possible to damage the printing head and the platen in such a printer by printing a dot pattern, backspacing the printing head, and repeating this many times.

■ A CRT has a screen coated with a phosphor compound. When a beam of electrons hits the screen, it is stopped and its kinetic energy is converted to visible light. Screen savers are programs that move the beam continually when the computer is not in use, or simply dim the screen, to make sure that no point on the screen will be exposed to the beam for a long time. Malicious software can corrupt the screen saver so it concentrates the beam at one point on the screen long enough to burn the phosphor coating at the point, and then move the beam to another point, to repeat the damage. Fortunately, CRTs are currently being phased out in favor of LCD display monitors, which don't have this vulnerability.

■ Modern personal computers have several cooling fans in them. The fans are turned on and off by the operating system depending on the temperature at various points inside the computer. Rogue software can interfere with this operation in an obvious way and can seriously damage the computer as a result of high temperature.

■ A computer virus in a laptop can spin the disk continuously and drain the battery very quickly. This does not damage the computer, but is annoying. A similar virus in a mobile device can achieve the same result even in the absence of a disk.

2.4: When a disk is infected, the virus saves the original boot sector to a different location L on the disk. If an infected disk is reinfected, the virus would save the *modified* boot sector to L. Thus, any virus detective trying to read the boot sector would read the infected version, whether it came from its original position or from L. This would make it easy to identify the virus.

2.5: An extra track may be used for copy protection. Only utilities that know about the track can fully copy the disk.

2.6: The Pareto principle (also known as the 80–20 rule) is named after Vilfredo Pareto, an Italian economist, and was popularized by Joseph M. Juran. It claims that 80% of the results of an operation often stem from 20% of the causes of the operation. This is a useful idea that can be employed as a rule of thumb in many situations, but can also be misused. Examples of this rule are: (1) 80% of the real properties in a certain region may be owned by 20% of the population. (2) 80% of the sales of a company may be due to 20% of its customers. (3) 80% of the execution time of a computer program is caused by 20% of its instructions. However, the claim "80% of the work is done by 20% of the workers" is, in general, wrong.

2.7: The virus selects a few bytes from the middle of the program, and replaces them with a jump instruction to the virus. When execution of the program gets to the jump, it jumps to the virus, which then executes, restores the selected bytes, and resumes the program. This method makes it difficult to detect the virus, but requires an experienced virus writer, because modern computers have variable-size instructions (an instruction may occupy one byte or several bytes) and the virus has to place the jump between two original instructions, not inside an instruction.

2.8: If the virus came from the boot sector of a removable volume, then the computer has a port for removable volumes and there is a chance that more removable volumes will be connected in the future. If such a virus tries to infect only executable files, it will miss all the future removable volumes. On the other hand, if the virus is residing in an executable file (it is a file infector), it may be the case that no external volumes will be connected to the computer and the virus will never propagate.

2.9: The date is different, but the word processor (or other software) has a command, such as "\date," to obtain the date from the operating system, which is why the header is always the same.

2.10: A virus may do nothing because of a bug in its code. Some viruses are written by researchers as a proof of concept, to study a certain aspect of virus propagation or infection, and such a virus may also be benign.

2.11: Changing one bit in a text file modifies one character of text. Often, this may not constitute significant damage, especially since the text in question may have mistypes to begin with. A corrupted character in a poem may never be discovered, even by its author, but legal or medical texts may be sensitive to even small corruptions. Modifying one bit in an image changes the color of one pixel. If the color changes significantly, the modification may be noticeable. In medical (X ray) images and images taken by spy satellites, every pixel may be important, and a corrupt pixel may lead to wrong diagnosis (in the former case) or wrong military decision (in the latter). It's difficult to think of a case where one bad bit in a video file would be noticeable, but a single bad bit in an audio file may be noticed if it changes a short interval of silence to a loud sound. Changing one bit in an executable file corrupts either an instruction or a data item. In either case the program will get corrupted, but may still do its job most of the time. We know that a typical program spends most of its time in small regions (loops) of instructions, while most of its instructions are rarely executed. If one instruction in an error-handling procedure is damaged, the program will still run correctly until the error actually occurs.

2.12: The virus may go into action when the user closes a document in a word processor. Before the virus closes the document, it may make random changes in the text. A sophisticated data diddling virus may simply check every text file found in the computer, scan it for predetermined keywords or phrases, and change each. Thus, each occurrence of "vice president" may be changed to "president" and each "buy" changed to "sell." Another nasty idea is to search for spreadsheet files and change them along the same lines. A file may be changed each time it is saved, or only when the user closes it, or when the virus finds it on the disk. The virus may modify data items or formulas; it may follow guidelines (such as change every "+" to "−" or swap every data item with the one to its left) or may do its damage at random. The point is that it's easy to come up with ideas for inflicting subtle damage, but it is difficult, perhaps even impossible, to correct such damage once it is discovered.

2.13: A vice-president trying to get rid of the president quickly and fill his place. One partner trying to drive the other partner crazy and buy his share of the business awfully cheap. A student trying to have a fellow student fail a class project.

2.14: If a low-clearance user can see the names of high-level files, then S can temporarily modify the name of such a file to signal a 0 or a 1 to R. If S can control the existence of a shared resource, then it can signal a 0 or a 1 by the presence or absence of the resource. Similarly, S can send bits to R by deleting and creating a file each time it receives a synchronization signal from R.

2.15: Because in general it is easier to do evil than to do good, as can be seen by many real-life examples. It takes years to build a large building, but only seconds to bring it down in an earthquake. Similarly, raising a child requires years of effort, but killing someone is much easier and quicker.

2.16: Yes, if the executable file is small to begin with or if it does not compress very well (which happens if it is random or close to random).

2.17: Yes, but I promise to do my best to educate myself and follow the examples, tips, and advice given here and in many other books, articles, and Web sites to try to keep my computer, backups, and network clean.

2.18: (1) Execute a `clear` instruction. Such an instruction clears its operand, which may be a register or a memory location. (2) Subtract register 4 from itself. (3) Prepare the constant zero in location `cons` and execute a `mov` instruction to move that location to register 4. (4) Multiply register 4 by zero. (5) Shift the register n positions to the left or to the right, where n is the register size. (6) Perform an exclusive OR (XOR) of the register with itself.

2.19: On the author's Macintosh, the activity monitor indicates the following: Alias menu (displays a menu of files at the top of the screen, for easy launching), TypeIt4Me (a simple macro processor that types a character string when the user types its name), Wacom tablet driver (looking for activity in the tablet), HP Scanjet manager (looking for data from the scanner), and Dropbox (a file synchronization program).

2.20: When a virus senses that new, unfamiliar software has been installed and is scanning disk directories or memory, the virus may react by erasing several important operating system routines from memory (and also deleting them from the disk). This leads to a crash, where the computer behaves erratically or seems frozen. Such a stealth technique is extreme and immediately raises suspicion of a virus, but it may delay the detection and extermination of the virus, or at least may annoy the computer user a while longer.

2.21: Restarting (or rebooting) a computer is done by an interrupt. The user presses a restart button (or a key combination) that generates a special interrupt, and the handling routing for that interrupt closes all the open files and restarts the computer. (On a PC, the key combination CTRL-ALT-DEL is used for this purpose.) This is why a computer can be restarted at any time,

even in the middle of a program, and even if the program is stuck in an infinite loop. A virus that infects the reboot interrupt-handling routine can therefore survive a restart. The virus copies itself as a temporary file on the startup disk, it modifies the operating system routine that boots the computer, and then executes the normal routine for closing down the computer. When the computer restarts, it executes the modified booting routine. The routine boots the computer normally, and then reads the virus from the temporary file, stores it in memory, and deletes the file. As a precaution, the virus may modify the booting routine such that its last step is to remove the modification, leaving nothing suspicious behind. Notice that DVDs are read only, so this technique will not work if the startup volume is a DVD.

3.1: Try to obtain it from the maker of the vulnerable software. A large software maker that sells, for example, a web server (where the hacker has discovered a security hole) will have a list of customers who purchased the software. Such a list will not have the IP numbers, but they can be obtained automatically from the URLs of the customers. The list will not be complete, but it doesn't have to be.

3.2: One such example is a dictionary server. The client sends a word, and the server responds by sending back the definition of the word, or its synonyms. Another example is a street-address server, such as [mapquest 04] or [maporama 04]. The client sends the latitude and longitude coordinates of a point on Earth, and the server sends back the street address, if any.

3.3: It is true that any experiments with rogue software, not just worms, should produce best results if carried out "in the field," rather than in a laboratory. However, the public would have to be notified, and there will be tough resistance to such an experiment, because people are scared of anything they don't understand. Also, the benign worm may contain a bug that will turn it into a bad worm. Even worse, a hacker may find a way to release a private, bad worm, similar to the good one during the experiment and that worm would spread with the good one, finding no resistance.

3.4: When a worm generates children and sends them out, each child should get a list of IP addresses as before, but also including the addresses of its older siblings. Thus, if a worm generates children A, B, and C, then B will get a list that has, among other addresses, the address of A, and C will get a list with both A's and B's addresses.

3.5: We know that it's virtually impossible to completely test and debug a worm (or any other type of rogue software) in the laboratory. Thus, once a worm has been sent into the Internet, its creator may discover a bug in the code. Another reason may be a worm's author who has just finished reading this section and is eager to employ the techniques found here to "improve" an existing worm.

4.1: A word processor or an editor runs with a user's own file access privileges, because it must have full access to all the user's files. A Trojan horse in a word processor can therefore read, write, or delete any file opened by the word processor. The horse could, for example, examine the content of the file, and upon finding a keyword (such as `key` or `bomb`), send the entire text to its creator, create a publicly-accessible copy, or change the access permission of the file to make it generally accessible.

4.2: Many of the spyware applications discussed in Chapter 9 are Trojans. Symantec and other security organizations maintain lists of recent threats that also includes Trojans.

4.3: There aren't many. Perhaps the most important ones are the `mail` routine, the `passwd` routine (to let users change their passwords), the `ps` command (examines the status of all processes in the computer), routine `lquota` (to enforce disk quotas), and the `df` command (which indicates the amount of free disk space).

4.4: The code of line 3 identifies the fact that the compiler is compiling itself, but this code is weak, because even minimal changes to the source line "`compile(s) {`" will defeat the test of line 3.

4.5: The original virus can check to see whether a file with a certain name exists. Once the hacker decides that the original virus has done its job, he creates such a file. Whenever any copy of the virus notices the existence of this file, it deletes itself from its host. A variation is to have the original virus itself create this flag file once it has infected the compiler and thus accomplished its mission (see the discussion of antibodies on Page 80).

6.1: A dentist's office, as discussed on page 156.

6.2: Yes, to some extent, because many new viruses are created from virus kits and are therefore modified versions of existing viruses, so their codes are similar. Old versions of Norton anti-virus software for the Macintosh, made by Symantec, promised to do just that.

6.3: An image file tends to be big and is almost always kept in compressed form. Even a small image may consist of a million pixels, each occupying three bytes. Current digital cameras are already in the 12 megapixel range, and create image files that are at least 36 Mbyte long in raw, uncompressed form. Video files are much bigger. A document with tax information may be needed only once a year. X-ray images in a hospital's archive may remain untouched for years. Pictures taken by astronomical telescopes are stored in archives and may be used years later to compare a newly-discovered astronomical event with the same patch of sky in the past.

6.4: Because the activity monitor is called by the break routine and this call places another return address at the top of the stack. Thus, when the activity monitor is executing, the address at the top of the stack is the address the activity monitor will use to return to the break routine. The address below it is the address the break routine will use to return to F.

6.5: Many applications are installed by an installer that decompresses the files needed by the application and writes them in the appropriate places on a disk. When such an installer finds files left from an older version of the application, it may get confused. If the access permission of a folder has changed and the installer can no longer write to it, it may skip part of the installation or terminate abnormally. If power to the computer is cut off during the installation, the installer may not be able to complete its task later.

6.6: A screen saver. See Section 9.3.

6.7: When a program terminates normally, it returns control to the operating system by creating an artificial interrupt called a break or a supervisor call. When the hardware senses this interrupt, it invokes an interrupt service routine (part of the operating system) that either examines user commands that are pending or decides what program will be next to execute. If the virus writer is familiar with the details of the operating system, the virus may modify this routine such that it first infects whatever program has just finished, then executes normally. Notice that in order to infect an operating system routine, the virus has to obtain high privilege, but such viruses have been detected in the past.

6.8: The voting circuit cannot decide which result is correct, if any. In such a case, the circuit can only detect an error and cannot correct it. An improvement is to have five copies, or even a larger (odd) number of copies.

7.1: Because the association between a URL and its IP may change at any time, especially if the site in question is hosted by an ISP that provides dynamic IPs.

7.2: Cheap (but possibly bad) prescription drugs, drugs that enlarge or enhance body parts, herbal remedies, weight loss drugs, get-rich-quick schemes, and financial services such as mortgage offers or schemes for reducing debts. Qualifications, such as university degrees or professional titles. On-line gambling. Cut-price or pirated software.

7.3: Just do it.

7.4: At the time of this writing they are `thunderfap.com`, `absurdly-cool.com`, and `shop4freebies.com/`.

7.5: The term zombie is used in UNIX to indicate a child program that was started by a parent program but was later abandoned by it. This is not the same as a zombie computer or a zombie server.

8.1: If you know a person, you can ask him an array of personal questions. If you are satisfied with the answers, you authenticate the person. If you don't know a person, you can receive the answers beforehand, and conduct the authentication process by computer, but this method is still experimental and should not be trusted.

8.2: A natural eye can be distinguished from a glass eye by shining light of varying intensities on the eye and making sure that its pupil dilates normally.

8.3: Another variation is to prepare a large number of different permutations, then compute numbers a, b, and so on from the password, and finally perform permutation a on the password, then apply permutation b on the result, and so on.

8.4: Typical default passwords are the following: guest, test, tester, system, admin, manager, sysman, sysop, engineer, ops, operations, central, demo, demonstration, aid, display, call, terminal, external, remote, check, net, network, phone, and fred.

8.5: Yes, it is secure, because there are so many possible permutations. However, it may be easier to memorize a random password than to memorize a specific permutation of 16 characters, again because there are so many permutations.

8.6: It is likely `';lkjh` or `lkjhgf` (look at your qwerty keyboard).

8.7: Products are continually becoming more reliable, easier to use even with a personal computer, and less expensive. Use a search engine and search, for example, under "fingerprint identification."

8.8: Ask a friend to let you use their account. Try to guess a password by using the birthday of its owner, the number of his children, or their birthdays.

8.9: The name of the person, as in Larry's case.

8.10: In the case in question, the hacker identified a computer that ran an early version of `PC AnyWhere`. This software [remotelyanywhere 04] makes it easy to remotely control a PC and the early version had a security flaw that made it possible to login to a remote PC while bypassing the password protection (a classic example of a security compromise). Once gaining control of the computer, the hacker identified its IP address, then used `telnet` software to try nearby IP numbers to break into other computers on campus.

9.1: Are there any complaints on the Internet, especially on popular technical message boards, about the program using deceptive advertising or spam?

9.2: No. If this poor, old, and inexperienced author could come up with such a frightening scenario, imagine what a group of well-determined, well-funded, and well-trained terrorists could come up with when they really put their minds to it. The only remedy to this scenario is for a government agency to check the background of every affiliate network and to scan for a Trojan horse every computer program that seems too good to be true; not very practical.

9.3: A search in early 2010 discloses that on 24 October 2008, Richard M. Nixon, an appliance specialist from Moon Township, PA, 15108, USA, contributed $250 to the Republican National Committee.

9.4: This is easy. A search for `spyware audit` has returned about 1,940,000 results.

9.5: This is easy. A search for "spyware removal" returns several million results, among them [Spybot 04], makers of *Spybot - Search and Destroy*; [snapfiles 04], that advertises *STOPzilla*; [lavasoft 04] with its *Ad-Aware*; and [SearchAndDestroy 04] that offers free spyware removal.

10.1: This author cannot think of any.

10.2: (1) Open a text file, find the characters of the password one by one in the text, copy them individually, and paste each character where you need to type the password. (2) Start by typing a string of `a`s, then type the characters of the password in random order in between the `a`s, and finally delete the `a`s with the delete key. As an example, consider password `ChHaakon`. It can be typed surreptitiously in the following steps

$$\text{aaaaaaaa} \to \text{aaaaakaaa} \to \text{aaaHaakaaa} \to \text{aaaHaakaoaa} \to$$
$$\text{aCaaHaakaoaa} \to \text{aCaaHaakaoana} \to \text{aCahaHaakaoana} \to \text{ChHaakon}.$$

(3) Use a virtual keyboard. This is a program that displays a keyboard on the screen. The user clicks on keys, and the corresponding characters are displayed at the cursor's location. An example of a virtual keyboard is [corallosoftware 05]. These methods are safe but tedious, which illustrates the tradeoff between security and ease of use.

10.3: Here are some examples: (1) A bank statement with cancelled checks. A sophisticated thief can wash off any traces of ink from a check, then use it in an obvious way. (2) A box full of newly-printed checks. (3) A preapproved credit card offer. It is always a good idea to opt out of such offers and in the United States this is possible by calling 888-5-OPT-OUT. (4) New credit cards issued for old, expired ones. (5) Letters (with checks, official forms, or money orders) you leave in your mailbox for the mailman to pick up.

10.4: Marketers and spammers send unwanted advertisements and spam targeted by IP numbers. Hackers and snoops track a victim's Internet surfing habits by his IP address, and this increases one's chances of becoming a victim of identity theft.

10.5: Profiling and targeted advertising are popular applications of cookies. You surf to a magazine's site and decide to read an article on weight loss. The site sends your computer a cookie that identifies you as one who is interested in weight loss. On every subsequent visit to the magazine's site, the cookie is read by the site, which then displays ads for weight loss.

The biggest online advertising company is DoubleClick. Relatively few have heard of this company and even fewer have visited their Web site. However, chances are that you have a cookie in your browser from DoubleClick even if you have never visited that site [cookiecentral 04]. This is a third-party cookie, sent by a site that you have visited. When you visit a commercial Web site X that employs DoubleClick as its online advertising company, X retrieves any DoubleClick cookies that you may have and sends them to DoubleClick, which then sends X ads based on those cookies for you to watch. Site X then sends you another DoubleClick cookie identifying you as a visitor of X.

10.6: By spreading false rumors about a new, revolutionary product about to be released by Microsoft and including a link to his site for anyone to click on instead of typing.

10.7: You cannot. A search at [Network solutions 04] indicates that this domain has already been registered (by Alon Swartz) and so have virtually all the domain names that are typographically similar to `microsoft.com`. (Note. On April 15, 2010, this URL was for sale.)

11.1: A news agency may want to customize news it carries in its Web site by time zones.

11.2: A redundancy. Similar to phrases such as absolutely necessary, advance warning, boiling hot, hot water heater, my personal opinion, and newborn baby.

11.3: Yes, because a child, especially a pre-teen, may not fully grasp the risk of opening an email attachment or may easily forget any warnings they received about this danger.

11.4: Here is an example of such a set.

■ Search the Internet for Web sites that carry news about new malware. Browse 2–3 such sites every morning. The few minutes that this takes are time well spent. Search the Internet for security news and white papers on security.

■ Obtain a firewall, use it, and update its rules as needed.

■ Obtain anti-virus software, update it and run it regularly.

■ Shut down your computer when you are not using it.

■ Enable other operating system services only when necessary and only on a temporary basis.

■ Use robust passwords that include letters, digits, and other characters in a hard-to-guess string. Remember! Sophisticated dictionary attacks are being carried out all the time.

■ Keep up to date with security patches for (1) your operating system, (2) your Web browser, and (3) other software, especially any servers or communications software.

■ Keep a sharp eye out for domain name trickery.

■ Never download anything from any source you don't know and trust, and be sure it really is the source you think it is. As this book explains elsewhere, it's easy to create a convincing fake version of any Web site.

■ Delete, without reading or opening, email attachments from anyone you don't know and trust. Be wary of attachments even from known, trusted persons, whose computers may have been compromised.

A.1: Auditing the auditors is fairly easy because the auditors don't write any software and are not supposed to modify existing software. Thus, auditing the auditors is done by making sure they haven't made any changes. This is a straightforward task that can be done by one person who is trusted by the owners/directors of the bank.

B.1: No answer provided, but if you cannot easily read that (and I hope that you cannot), then you are not a good hacker.

C.1: Imagine an anti-virus program that does not yet recognize `Dark Avenger.1800`. The program works by opening executable files and checking them, with the result that they all become infected even though they are not executed.

C.2: Grim.

Conc.1: The IBM S/360 family was succeeded by the S/370, and 3080, 3090, and 43xx families, all upward compatible. The DEC PDP-11/20 was the first model (made in 1970) of the famous PDP-11 family of upward compatible mini and microcomputers, whose last descendant was the Micro PDP-11/94 (made in 1990). The Intel 80x86 family of microprocessors was based on the 8086 chip, introduced in 1978. The last member of this family was the 80486, first made in 1989.

Conc.2: Banks have to transfer large amounts of cash and they spend much effort and money on securing these transfers. They employ specially-designed armored trucks, trained security personnel, and special cameras and other security equipment. It would be easier and cheaper (and not much slower) to simply use a delivery service such as Federal Express to perform this task, but it would also be extremely nonsecure. The compromise in this case is extreme.

Compromise

Noun:
1. A middle way between two extremes.
2. Accommodation in which both sides make concessions.

Verb:
1. Make a compromise; arrive at a compromise.
2. Settle by concession.
3. Expose or make liable to danger, suspicion, or disrepute.

If love is the answer, could you rephrase the question?

—Lily Tomlin