

# **Best Practices for Protecting against Viruses, Spyware, and Hacking**

(Version 4.0 December 18, 2008)

Copyright © 2008 by Capers Jones. All rights reserved.

Note: This is an excerpt from Chapter 1 of the author's book "Best Practices in Software Engineering" to be published by McGraw Hill in 2009. The first chapter discusses 50 best practice topics, and this is topic number 42. Because of the dangers of various forms of hacking and cyber crime to individuals, companies, and government agencies this section is also distributed as a stand-alone document and public service.

## **42) Best Practices for Protecting against Viruses, Spyware, and Hacking**

As of 2009 the value of information is approaching the value of gold, platinum, oil and other expensive commodities. In fact as the global recession expands, the value of information is rising faster than the value of natural products such as metals or oil. As the value of information goes up, it is attracting more sophisticated kinds of thievery. In the past hacking and viruses were often individual efforts, sometimes carried out by students and even by high-school students sometimes just for the thrill of accomplishing the act.

However in today's world theft of valuable information has migrated to organized crime, terrorist groups, and even to hostile foreign governments. Not only that but denial of service attacks and "search bots" that can take over computers are powerful and sophisticated enough to shut down corporate data centers and interfere with government operations. This situation is going to get worse as the global economy declines.

Since computers are used to store valuable information such as financial records, medical records, patents, trade secrets, classified military information, customer lists, addresses and email addresses, phone number, and social security numbers the total value of stored information is in the range of trillions of dollars. There is no other commodity in the modern world that is simultaneously so valuable and so easy to steal as information stored in a computer.

Not only are there increasing threats against software and financial data, but it is technically within the realm of possibility to hack into voting and election software as well. Any computer connected to the outside world by any means is at risk. Even computers that are physically isolated may be at some risk due to their electromagnetic emissions.

Although many individual organizations such as Homeland Security, the Department of Defense, the FBI, NSA, IBM, Microsoft, Google, Symantec, McAfee, Kaspersky, Computer Associates and scores of others have fairly competent security staffs and also security tools, the entire topic needs to have a central coordinating organization that would monitor security threats and

distribute data on best practices for preventing them. The fragmentation of the software security world makes it difficult to organize defenses against all known threats, and to monitor the horizon for future threats.

The FBI started a partnership organization with businesses called “InfraGuard” that is intended to share data on software and computer security issues. According to the InfraGuard web site, about 350 of the Fortune 500 companies are members. This organization has local branches affiliated with FBI field offices in most major cities such as Boston, Chicago, San Francisco, and the like. However smaller companies have not been as proactive as large corporations in dealing with security matters. Membership in InfraGuard would be a good first step and a “best practice” as well.

The Department of Homeland Security also has joint government-business group for Software Assurance (SwA). This group has published a Software Security State of the Art Report (SOAR) that summarizes current best practices for prevention, defense, and recovery of security flaws. Participation in this group and following the principles discussed in the SOAR report would be “best practices” too.

As this book is being written Homeland Security is planning to construct a major new security research facility that will probably serve as a central coordination location for civilian government agencies and will assist businesses as well.

A new government security report chaired by Representative James Langevin of Rhode Island is also about to be published, which deals with all of the issues shown here and others besides, and in greater detail. It will no doubt provide additional guidance beyond what is shown here.

Unfortunately, some of the security literature tends to deal with threats after development and deployment. The need to address security as a fundamental principle of architecture, design, and development is poorly covered. A book related to this one by Ken Hamer-Hodges, Authorization Oriented Architecture, will deal with more fundamental subjects. Among these is automating computer security to move the problem from the user to the system itself. The way to do this is through detailed boundary management. That is why objects plus capabilities matter. Also security frames such as Google Caja which prevent redirection to phishing sites are best practices. The new E programming language is also a best practice, since it is designed to ensure optimum security.

The training of business analysts, systems analysts, and architects in security topics has not keeping pace with the changes in malware, and this gap needs to be corrected quickly because threats are becoming more numerous and more serious.

It is useful to compare security infections with medical infections. Some defenses against infections such as firewalls are like bio-hazard suits, except the software biohazard suits tend to leak.

Other defenses such as antivirus and antispymware applications are like antibiotics that stop some infections from spreading and also kill some existing infections. However as with medical antibiotics, some infections are resistant and are not killed or stopped. Over time the resistant infections tend to evolve more rapidly than the infections that are killed, which explains why polymorphic viruses are now the virus of choice.

What might be the best long-term strategy for software would be to change the DNA of software applications and increase their natural immunity to infections via better architecture, better design, more secure programming languages, and better boundary controls.

The way to solve security problems is to consider the very foundations of the science and to build boundary control in physical terms based on "Principle of Least Authority" where each and every subroutine call is to an instance of a protected class of object. Only the authorization for the use of the invoked code should be the local names instantiated for the small task at hand: No Global items, No Global Name Space, No Global path names like C:/directory/file or URL <http://123.456.789/file>. Every subroutine is a protected call with boundary checking and all program references are dynamically bound from a local name at runtime with access control check included at all times. , use a good O-Cap language (E and Caja today). Some suggested general "best practices" from this source include:

- Change passwords frequently (outdated by today's technology)
- Don't click on email links - Type the URL in manually
- Disable the preview pane in all inboxes
- Read email in plain text
- Don't open email attachments
- Don't enable Java, JS, or particularly ActiveX
- Don't display your email address on your web site
- Don't follow links without knowing what they link to
- Don't let the computer save your passwords
- Don't trust the "From" line in email messages
- Upgrade to latest security levels particularly for Internet Explorer
- Consider switching to Firefox or Chrome
- Never run a program unless it is trusted
- Read the User Agreement on downloads (they may sell your personal data)
- Expect email to carry worms and viruses.
- Just say no to Pop-Ups

- Say no if an application asks for additional or different authorities
- Say no if it asks to read or edit anything more than a Desktop folder
- Say no if it asks for edit authority on other stuff
- Say no if it asks for read authority on odd stuff, with a connection to the Web
- During an application install supply a new name, new icon, and a new folder path.
- Say no when anything asks for web access, beyond a specific site
- Always say **No** unless you want to be hit sooner or later

Internet security is so hazardous as of 2009 that one emerging “best practice” is for sophisticated computer users to have two computers. One of these would be used for web surfing and internet access. The second computer would not be connected to the internet and would accept only trusted inputs on physical media that are of course checked for viruses and spyware

It is quite alarming that hackers are now organized and have journals, web sites, and classes available for teaching hacking skills. In fact a review of the literature indicates that there is more information available about how to hack than on how to defend against hacking. As of 2009 the hacking “industry” seems to be larger and more sophisticated than the security industry, which is not surprising given the increasing value of information and the fundamental flaws in computer security methods. There is no real census of either hackers or security experts, but as of 2009 the hacking community may be growing at a faster rate than the security community.

Standard “best practices” include use of firewalls, antivirus packages, antispyware packages, and careful physical security. However as the race between hackers and security companies escalates, it is also necessary to use constant vigilance. Virus definitions should be updated daily for example. More recent “best practices” include biological defenses such as using finger prints or retina patterns in order to gain access to software and computers.

Two topics that have ambiguous results as of 2009 are those of identify theft insurance and certification of web sites by companies such as Verisign. As to identity theft insurance, the idea seems reasonable, but what is needed is more active support than just reimbursement for losses and expenses. What would perhaps be a “best practice” would be a company or non-profit that had direct connections to all credit card companies, credit bureaus, and police departments and could offer rapid response and assistance to consumers with stolen identities.

As to certification of web sites, an on-line search of that subject reveals almost as many problems and mistakes as benefits. Here too the idea may be valid, but the implementation is not yet perfect. Whenever problem reports begin to

approach benefit reports in numbers, the topic is not suitable for “best practice” status.

Some examples of the major threats in today’s cyber world are discussed below in alphabetical order:

**Adware:** Because computer usage is so common, computers have become a primary medium for advertising. A number of software companies generate income by placing ads in their software that are displayed when the software executes. In fact for “shareware” and “freeware” placing of ads may be the primary source of revenue. As an example the Eudora email client application has a full-featured version that is supported by advertising revenue. If adware were nothing but a passive display of information it would be annoying but not hazardous. However adware can also collect information as well as display it. When this occurs adware tends to move across a line and become spyware. As of 2009 ordinary consumers have trouble distinguishing between adware and spyware, so installation of anti-spyware tools is a best practice, even if not totally effective. In fact sophisticated computer users may install three or four different anti spyware tools because none are 100% effective by themselves.

**Authentication, Authorization, and Access:** Computers and software tend to have a hierarchy of methods for protection against unauthorized use. Many features are not accessible to ordinary users, but require some form of “administrative access.” Administrative access is assigned when the computer or software is first installed. The administrator then grants other users various permissions and access rights. In order to use the computer or software users need to be “authenticated” or identified to the application with the consent of the administrator. Not only human users but also software applications may need to be authenticated and given access rights. While authenticating human users is not trivial, it can be done without a great deal of ambiguity. For example, retina prints or finger prints provide an unambiguous identification of a human user. However authenticating and authorizing software seems to be a weak link in the security chain. Access control lists (ACL) are the only available best practice but for static files, services and networks. ACL cannot distinguish identities so a virus or Trojan have the same authorization as the session owner! If some authorized software contains worms, viruses, or other forms of malware they may use access rights to propagate. As of 2009 this problem is complex enough so there seem to be no best practices for day to day authorization. However a special form of authorization called “capability-based security” is at least in theory a best practice. Unfortunately capability-based security is complex and not widely utilized. Historically the Plessey 250 computer implemented a hardware-based capability model in order to prevent hacking and unauthorized changes of access lists circa 1975. This approach dropped from use for many years, but has resurfaced by means of Google’s Caja and the E programming language.

**Back door:** Normally in order to use software some kind of login process and password are needed. The term “back door” refers to methods for gaining access to software while bypassing the normal entry points and avoiding the use of passwords, user names, and other protocols. Error-handling routines and buffer overruns are common back-door entry points. Some computer worms install backdoors that might be used to send spam or perform harmful actions. One surprising aspect of backdoors is that occasionally they are deliberately put into software by the programmers who developed the applications. This is why classified software and software that deals with financial data needs careful inspection, static analysis, and of course background security checks of the software development team. Alarming, back doors can also be inserted by compilers if the compiler developer put in such a function. The back door situation is subtle and hard to defend against. Special artificial intelligence routines in static analysis software may become a best practice, but the problem remains complex and hard to deal with. Currently several best practice rules include: 1. Assume errors are signs of an attack in process! 2. Never let user coded error recovery run at elevated privileged levels. 3. Never use global (path) addressing for URL or networked files. 4. Local name space only translated by a trusted device.

**Botnets:** The term “botnet” refers to a collection of “software robots” that act autonomously and attempt to seize control of hundreds or thousand of computers on a network and turn them into “zombie computers.” The bots are under control of a “bot herder” and can be used for a number of harmful purposes such as denial of service attacks or sending spam. In fact this method has become so pervasive that bot herders actually sell their services to spammers! Botnets tend to be sophisticated and hard to defend against. While firewalls and fingerprinting can be helpful, they are not 100% successful. Constant vigilance and top-gun security experts are a “best practice.” Some security companies are now offering botnet protection using fairly sophisticated artificial intelligence techniques. It is alarming that cyber criminals and cyber defenders are apparently in a heated technology race. Lack of boundary controls are what allow botnet to wander at will. Fundamental architectural changes, use of Caja, and secure languages such as E could stop botnets.

**Browser hijackers:** This annoying and hazardous security problem consists of software that overrides normal browser addresses and redirects the browser to some other site. Browser hijackers were used for marketing purposes, and sometimes to redirect to porn sites or other unsavory locations. A recent form of browser hijacking is termed “rogue security sites.” A pop up ad will display a message such as “YOUR COMPUTER IS INFECTED” and direct the user to some kind of security site that wants money. Of course it might also be a phishing site. Modern anti-spyware tools are now able to block and remove browser hijackers in most cases. They are a “best practice” for this problem, but they must be updated frequently with new definitions. Some browsers such as

Google Chrome and Firefox maintain lists of rogue web sites and caution users about them. This is a “best practice.”

**Cookies:** These are small pieces of data that are downloaded from websites onto user computers. Once downloaded, they then go back and forth between the user and the vendor. Cookies are not software but rather passive data, although they do contain information about the user. Benign uses of cookies are concerned with on-line shopping and with setting up user preferences on web sites such as Amazon. Harmful uses of cookies include capturing user information for unknown or perhaps harmful purposes. For several years both the CIA and NSA downloaded cookies into any computer that accessed their web sites for any reason, which might have allowed the creation of large lists of people who did nothing more than access web sites. Also, cookies can be hijacked or changed by a hacker. Unauthorized change of a cookie is called “cookie poisoning.” It could be used, for example, to change the amount of purchase at an on-line store. Cookies can be enabled or disabled on web browsers. Because cookies can be either beneficial or harmful, there is no general best practice for dealing with them. The author’s personal practice is to disable cookies unless a specific web site requires cookies for a business purpose originated by the author.

**Cyberextortion:** Once valuable information such as bank records, medical records, or trade secrets are stolen, what next? One alarming form of new crime is extortion, or selling the valuable data back to the original owner under threat of publishing it or selling it to competitors. This new crime is primarily aimed at companies rather than individuals. The more valuable the company’s data the more tempting it is as a target. Best practices in this area involve top-notch security personnel and constant vigilance as well as firewalls and the usual gamut of security software packages. Also, alerting authorities such as the FBI or the cybercrime units of large police forces if extortion is attempted.

**Cyberstalking:** The emergence of social networks such as YouTube, MySpace, and Facebook has allowed millions of individuals to communicate who never (or seldom) meet each other face to face. These same networks have also created new kinds of threats for individuals such as “cyberbullying” and “cyberstalking.” Using search engines and the internet it is fairly easy to accumulate personal information. It is even easier to plant rumors, make false accusations, and damage the reputations of individuals by broadcasting such information on the web or using social networks. Because cyberstalking can be done anonymously it is hard to trace, although some cyberstalkers have been arrested and charged. As this problem becomes more widespread states are passing new laws against it as is the Federal Government. Defenses against cyberstalking include contacting police or other authorities, plus contacting the stalkers internet service provider if it is known. While it might be possible to slow down or prevent this crime by using anonymous avatars for all social networks, that more or less defeats the purpose of social networking.

**Denial of service:** This form of cyber crime attempts to stop specific computers, networks, or servers from carrying out normal operations by saturating them with phony messages or data. This is a sophisticated form of attack that requires considerable skill and effort to set up, and of course considerable skill and effort to prevent or stop. Denial of service attacks seemed to start about 2001 with an attack against American on Line (AOL) that took about a week to stop. Since then numerous forms of DoS attacks have been developed. A precursor to a denial of service attack may include sending out worms or search robots to infiltrate scores of computers and turn them into “zombies” which will then unknowingly participate in the attack. This is a complex problem and the “best practice” for dealing with it is to have top-notch security experts available and to use constant vigilance.

**Electromagnetic pulse (EMP):** A byproduct of nuclear explosions is a pulse of electromagnetic radiation that is strong enough to damage transistors and other electrical devices. Indeed such a pulse could shut down almost all electrical devices within perhaps 15 miles. The damage may be so severe that repair of many devices would be impossible; i.e. computers, audio equipment, cell phones, etc. The electromagnetic pulse effect has led to research in “e bombs” or high-altitude bombs that explode perhaps 50 miles up and shut down electrical power and damage equipment for hundreds of square miles, but do not kill people or destroy buildings. Not only nuclear explosions but other forms of detonation can trigger such pulses. While it is possible to shield electronic devices using Faraday cages or surrounding them in metallic layers, this is infeasible for most civilians. The major military countries such as the United States and Russia have been carrying out active research in e bombs and probably have them already available. It is also possible that other countries such as North Korea may have such devices. The presence of e bombs is a considerable threat to the economies of every country, and no doubt the wealthier terrorist organizations would like to gain access to such devices. There are no best practices to defend against this for ordinary citizens.

**Electromagnetic radiation:** Ordinary consumers using home computers probably don’t have to worry about loss of data due to electromagnetic radiation, but this is a serious issue for military and classified data centers. While operating, computers radiate various kinds of electromagnetic energy, and some of these can be picked up remotely and deciphered in order to collect information about both applications and data. That information could be extracted from electromagnetic radiation was first discovered in the 1960’s. Capturing electromagnetic radiation requires rather specialized equipment and also specialized personnel and software that would be outside the range of day to day hackers. Some civilian threats do exist such as the possibility of capturing electromagnetic radiation to crack “smart cards” when they are being processed. Best practices include physical isolation of equipment behind copper or steel enclosures, and of course constant vigilance and top-notch security experts.

Another “best practice” would be to install electromagnetic generators in data centers that would be more powerful than computer signals and hence interfere with detection. This approach is similar to jamming to shut down pirate radio stations.

**Hacking:** The word “hack” is older than the computer era and has meaning in many fields, such as golf. However in this book “hacking” refers to deliberate attempts to penetrate a computer or software application with the intent to modify how it operates. While some hacking is harmful and malicious, some may be beneficial. Indeed many security companies and software producers employ hackers who attempt to penetrate software and hardware to find vulnerabilities that can then be fixed. While firewalls, antivirus, and antispyware programs are all good practices, what is probably the “best practice” is to employ ethical hackers to attempt penetration of key applications and computer systems.

**Identity theft:** Stealing an individual’s identity in order to make purchases, set up credit card accounts, or even to withdraw funds from banks is one of the fastest growing crimes in human history. A new use of identity theft is to apply for medical benefits. In fact identity theft of physicians’ identities can even be used to bill Medicare and insurance companies with fraudulent claims. Unfortunately this crime is far too easy to perform, since it requires only moderate computer skills plus commonly available information such as social security numbers, birth dates, parents’ names, and a few other topics. It is alarming that many identity thefts are carried out by relatives and “friends” of the victims. Also, identity information is being sold and traded by hackers. Almost every computer user receives daily “phishing” emails that attempt to trick them into providing their account numbers and other identifying information. As the global economy declines into recession, identity theft will accelerate. The author estimates that at least 15% of the U.S. population is at risk. Best practices to avoid identity theft include frequent credit checks, using antivirus and anti-spyware software, and also physical security of credits cards, social security cards, and other physical media.

**Keystroke loggers:** This alarming technology represents one of the most serious threats to home computers users since the industry began. Both hardware and software keystroke logging methods exist, but computer users are more likely to encounter software keystroke logging. Interestingly, keystroke logging also has benign uses in studying user performance. In today’s world not only keystrokes but also mouse movements and touch-screen movements need to be recorded for the technology to work. The most malicious use of keystroke logging is to intercept passwords and security codes so that bank accounts, medical records, and other proprietary data can be stolen. Not only computers are at risk, but also ATM machines. In fact, this technology could also be used on voting machines; possibly with the effect of influencing elections. Anti-spyware programs are somewhat useful and there are other methods too such as one-time passwords. This is such a complex problem that the current best

practice is to do almost daily research on the issue and look for emerging solutions.

**Malware:** This is a hybrid term that combines one syllable from “malicious” and one syllable from “software.” The term is a generic descriptor for a variety of troublesome security problems including viruses, spyware, Trojans, worms, etc.

**Phishing:** This phrase is derived from “fishing” and refers to attempts to get computer users to reveal confidential information such as account numbers by having them respond to bogus emails that appear to be from banks or other legitimate businesses. A classic example of phishing are emails that purport to be from a government executive in Nigeria who is having trouble getting funds out of the country, and wants to deposit them in a U.S. account. The emails ask the readers to respond by sending back their account information. This early attempt at phishing was so obviously bogus that hardly anyone responded to, but surprisingly a few people might have. Unfortunately modern attempts at phishing are much more sophisticated and are very difficult to detect. The best practice is never to respond to requests for personal or account information that you did not originate. However, even newer forms are more sophisticated and can intercept browsers when they attempt to go to popular web sites such as EBay or PayPal. The browser can be redirected to a phony web site that looks just like the real one. Not only do phony web sites exist, but also phony telephone sites. However as phishing becomes more sophisticated it is harder to detect. Fortunately credit card companies, banks, and other institutions at risk have formed a non-profit Anti-Phishing Working Group. For software companies affiliation with this group would be a best practice. For individuals checking by phone and refusing to respond to email requests for personal and account data are best practices. Many browsers such as Firefox and Internet Explorer have anti-phishing “blacklists” of known phishing sites and warn users if they are routed to them. Boundary control, Caja, and languages such as E are also effective against phishing.

**Physical security:** Physical security of data centers, notebook computers, thumb drives, and wireless transmission remains a best practice. Almost every week articles appear in papers and journals about loss or theft of confidential data when notebook computers are lost or stolen. There are dozens of effective physical security systems and all of them should be considered. A modern form of physical security involves using fingerprints or retina patterns as passwords for computers and applications.

**Piracy:** Piracy in several forms is a major problem in the modern world. The piracy of actual ships is increasing alarmingly near the African coast. However software piracy is also increasing alarmingly. While China and the Asia Pacific region are well known as sources of piracy, the dispute between Iran and the USA has led Iran to allow unlimited copying of software and intellectual property, which means that the Middle East is also a hotbed of software piracy. In the

United States and other countries with strong intellectual property laws Microsoft and other large software vendors are active in bringing legal charges against pirates. The non-profit Business Software Alliance even offers rewards for turning in pirates. However unauthorized copies of software remain a serious problem. For smaller software vendors the usual precautions include registration and activation of software before it can be utilized. It is interesting that the open-source and freeware communities deal with the problem in rather different ways.

**Rootkits:** In the Unix operating the term “root user” refers to someone having authorization to modify the operating system or the kernel. For Windows having “administrative rights” is equivalent. Rootkits are programs that infiltrate computers and seize control of the operating system. Once that control is achieved, then the rootkit can be used to launch denial of service attacks, steal information, reformat disk drives, or perform many other kinds of mischief. Several years ago in 2005 the Sony corporation deliberately issued a rootkit on music CD’s in an attempt to prevent music piracy via peer to peer and computer copying. However an unintended consequence of this rootkit was to open up backdoor access to computers that could be used by hackers, spyware, and viruses. Needless to say once the Sony rootkit was revealed to the press, the outcry was sufficient for Sony to withdraw the rootkit. Rootkits tend to be subtle and not only slip past some antivirus software, but indeed may attack the antivirus software itself. There seem to be no best practices as of 2009, although some security companies such as Kaspersky and Norton have development methods for finding some rootkits and protecting themselves as well.

**Spam:** Although the original meaning of “spam” referred to a meat product, the cyber definition refers to unwanted ads, emails, or instant messages that contain advertizing. Now that the internet is the world’s primary communication medium and reaches perhaps 1/5<sup>th</sup> of all humans on the planet, using the internet for ads and marketing is going to continue. The volume of spam is alarming and is estimated at topping 85% of all email traffic, which obviously slows down the internet and slows down many servers as well. Spam is hard to combat because some of it comes from “zombie computers” that have hijacked by worms or viruses and then unknowingly used for transmitting spam. Some localities have made spamming illegal, but it is easy for spammers to outsource to some other locality where it is not illegal. Related to spamming is a new sub industry called “email address harvesting.” Email addresses can be found by search robots, and once found and created the lists are sold as commercial products. Another form of address harvesting is from the fine print of the service agreements of social networks, which state that a user’s email address may not be kept private (and will probably be sold as a profit-making undertaking). A best practice against spam is to use spyware and spam blockers, but these are not 100% effective. Some spam networks can be “de-peered” or cut off from other networks, but this is technically challenging and may lead to litigation.

**Spear Phishing:** The term “spear phishing” refers to a new and very sophisticated form of phishing where a great deal of personal information is included in the phishing email to deceive possible victims. The main difference between phishing and spear phishing is the inclusion of personal information. For example an email that identifies itself as coming from a friend or colleague is more likely to be trusted than one coming from a random source. Thus spear phishing is a great deal harder to defend against. Often hackers break into corporate computers and then send spear phishing emails to all employees, with disinformation indicating that the email is from accounting, human factors, or some other legitimate organization. In fact the real name of the manager might also be included. The only “best practice” for spear phishing is to avoid sending personal or financial information in response to any email. If the email seems legitimate, check by phone before responding. However, spear phishing is not just a computer scam, but also includes phony telephone messages and text messages as well.

**Spyware:** Software that installs itself on a host computer and takes partial control of the operating system and web browser is termed “spyware.” The purpose of spyware is to display unwanted ads, redirect browsers to specific sites, and also to extract personal information that might be used for purposes such as identity theft. Prior to version 7 of Microsoft Internet Explorer almost any Active X program could be downloaded and start executing. This was soon discovered by hackers as a way to put ads and browser hijackers on computers. Because spyware often embedded itself in the registry, it was difficult to remove. In today’s world circa 2009 a combination of firewalls and modern anti-spyware software can keep most spyware from penetrating computers, and can eliminate most spyware as well. However there is a heated technology race between hackers and protectors and sometimes the hackers pull ahead. Although the Macintosh has less spyware than computers running Microsoft windows, no computers or operating systems in the modern world are immune to spyware.

**Trojans:** This term is of course derived from the famous Trojan horse. In a software context a Trojan is something that seems to be useful so that users are deceived into installing it via download or by disk. Once installed some kind of malicious software then begins to take control of the computer or access personal data. One classic form of distributing Trojans involves screen savers. Some beautiful view such as a waterfall or a lagoon is offered as a free download. However there are also malicious software routines hidden in the screen saver that can cause harm. Trojans are often involved in denial of service attacks, in identity theft, in keystroke logging, and in many other harmful actions. Modern anti-virus software is usually effective against Trojans so installing, running, and updating such software is a “best practice.”

**Viruses:** Computer viruses originated in the 1970’s and started to become troublesome in the 1980’s. As with disease viruses, computer viruses attempt to penetrate a host, and then attempt to reproduce themselves in large numbers,

and then attempt to leave the original host and enter new hosts. Merely reproducing and spreading can slow networks and cause performance slowdowns, but in addition some viruses also have functions that deliberately damage computers, steal private information, or perform other malicious acts. For example viruses can steal address books and then send infected emails to every friend and contact of the original host. Macro viruses transmitted by documents created using Microsoft Word or Microsoft Excel have been particularly common and particularly troublesome. Viruses spread by instant messaging are also troublesome. Viruses are normally transmitted by attaching themselves to a document, email, or instant message. While anti-virus software is generally effective and a “best practice” virus developers tend to be active, energetic, and clever. Some newer viruses morph or change themselves spontaneously to avoid anti-virus software. These mutating viruses are called polymorphic viruses. Although viruses primarily attack Microsoft Windows all operating systems are at risk, including Linux, Unix, Mac OS, Symbian, and all others. Best practices for avoiding viruses are to install anti-virus software and keep the virus definitions up to date. Taking frequent checkpoints and restore points is also a best practice.

**Whaling:** This is a form of phishing that targets very high-level executives such as company presidents, senior vice presidents, CEO’s, CIO’s, board members, and so forth. Whaling tends to be very sophisticated. An example might be an email that purports to be from a well-known law firm and discusses possible litigation against the target or his or her company. Other devices would include “who’s who” email requests, or requests from famous business journals. The only best practice is to avoid responding without checking the situation out by phone or some other method.

**Wireless security leaks:** In the modern world usage of wireless computer networks is about as popular as cell phone usage. Many homes have wireless networks as do public buildings. Indeed some towns and cities offer wireless coverage throughout. As wireless communication becomes a standard method for business-to-business and person-to-person communication, it has attracted many hackers, identify thieves, and other forms of cyber criminals. Unprotected wireless networks allow cyber criminals to access and control computers, redirect browsers, and steal private information. Other less overt activities are also harmful. For example unprotected wireless networks can be used to access porn sites or send malicious emails to third parties without the network owner being aware of it. Because many consumers and computer users are not versed in computer and wireless network issues, probably 75% of home computer networks -are not protected. Some hackers even drive through large cities looking for unprotected networks (this is called “war driving.”) In fact, there may even be special signs and symbols chalked on sidewalks and buildings to indicate unprotected networks. Many networks in coffee shops and hotels are also unprotected. Best practices for avoiding wireless security breaches include

using the latest password and protection tools, using encryption, and frequently changing passwords.

**Worms:** Small software applications that reproduce themselves and spread from computer to computer over networks are called “worms.” Worms are similar to viruses but tend to self-propagating rather than spreading by means of emails or documents. While a few worms are benign (Microsoft once tried to install operating system patches using worms) many are harmful. If worms are successful in reproducing and moving through a network they use bandwidth and slow down performance. Worse, some worms have “payloads” or subroutines that perform harmful and malicious activities such as erasing files. Worms can also be used to create zombie computers that might take part in denial of service attacks. Best practices for avoiding worms include installing the latest security updates from operating vendors such as Microsoft, using antivirus software (with frequent definition updates) and using firewalls.

As can be seen from the variety of computer and software hazards in the modern world, protection of computers and software from harmful attacks requires constant vigilance. It also requires installation and usage of several kinds of protective software. Finally, both physical security and careless usage of computers by friends and relatives need to be considered. Security problems will become more pervasive the global economy sinks into recession. Information is one commodity that will increase in value no matter what is happening to the rest of the economy. Moreover both organized crime and major terrorist groups are now active players in hacking, denial of service, and other forms of cyber warfare.

If you break down the economics of software security, the distribution of costs is far from optimal in 2009. From partial data it looks like about 60% of annual corporate security costs are spent on defensive measures for data centers and installed software, about 35% is spent on recovering from attacks such as denial of service, and only about 5% is spent on preventive measures. Assuming an annual cost of \$50,000,000 on security per Fortune 500 company, the breakdown might be \$30,000,000 on defense, \$17,500,000 for recovery, and only \$2,500,000 on prevention during development of applications.

With more effective prevention in the form of better architecture, design, secure coding practices, boundary controls, and languages such as E, a future cost distribution for security might be prevention 60%, defense 35%, and recovery 5%. With better prevention the total security costs would be lower: perhaps \$25,000,000 per year instead of \$50,000,000 per year. In this case the prevention costs would be \$15,000,000; defensive costs would be \$8,750,000, and recovery costs would be only \$1,250,000. Table 2.8 shows the two cost profiles:

**Table 2.8 Estimated Software Security Costs in 2009 and 2019  
(Assumes Fortune 500 Company)**

	2009	2019	Difference
Prevention	\$2,500,000	\$15,000,000	\$12,500,000
Defense	\$30,000,000	\$8,750,000	-\$21,250,000
Recovery	\$17,500,000	\$1,250,000	-\$16,250,000
TOTAL	\$50,000,000	\$25,000,000	-\$25,000,000

So long as software security depends largely upon human beings acting wisely by updating virus definitions and installing anti-spyware, it cannot be fully successful. What the software industry needs is to design and develop much better preventive methods for building applications and operating systems, and then to fully automate defensive approaches with little or no human intervention being needed.

### **Books and Readings on Software Security, Hacking, and Malware Prevention**

Acohido, Byron and Swartz, John: Zero Day Threat: The Shocking Truth of How Banks and Credit Bureaus Help Cyber Crooks Steal Your Money and Identity; Union Square Press; ISBN 10: 140275695X; 2008; 304 pages.

Allen, Julia; Barnum, Sean; Ellison, Robert; McGraw, Gary; and Mead, Nancy; Software Security: A Guide for Project Managers (An SEI book sponsored by the Department of Homeland Security); Addison Wesley Professional, Boston, MA; ISBN 032150917X; 2008.

Anley, Chris, Heasman, John, Lindner, Felix, and Richarte, Gerardo; The Shellcoders Handbook: Discovering and Exploiting Security Holes; Wiley, New York; ISBN 10: 047008023X; 2007; 718 pages.

Chess, Brian; Secure Programming with Static Analysis; Addison Wesley Professional, Boston, MA; ISBN 10: 0321424778; 2007; 624 pages.

Dowd, Mark, McDonald, John, and Schuh, Justin; The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities; Addison Wesley Professional, Boston, Ma; ISBN 10: 0321444426; 2006; 1200 pages.

Ericson, John; Hacking: The Art of Exploitation; 2<sup>nd</sup> edition; No Starch Press; ISBN 10: 1593271441; 2008; 488 pages.

Gallager, Tom; Landauer, Lawrence; and Jeffries, Brian; Hunting Security Bugs; Microsoft Press, Redmond WA; ISBN 10: 0735621879; 2006; 592 pages.

- Hamer-Hodges, Ken; Authorization Oriented Architecture – Open Application Networking and Security in the 21<sup>st</sup> Century; Auerbach Publications, Philadelphia, PA; to be published in December 2009; ISBN 10: 1439800545; pages nnn. (To be published in 2009)
- Hogland, Greg and McGraw, Gary; Exploiting Software: How to Break Code; Addison Wesley Professional, Boston, MA; ISBN 10: 0201786598; 2004; 512 pages.
- Hogland, Greg and Butler, Jamie; Rootkits: Exploiting the Windows Kernel; Addison Wesley Professional, Boston, MA; ISBN 10: 0321291349; 2005; 352 pages.
- Howard, Michael and Lippner, Steve; The Security Development Lifecycle; Microsoft Press, Redmond, WA; ISBN 10: 0735622140; 2006; 352 pages.
- Howard, Michael and LeBlanc, David; Writing Secure Code; Microsoft Press, Redmond, WA; ISBN 10: 0735617228; 2003; 798 pages.
- Jones, Andy and Ashenden, Debi; Risk Management for Computer Security: Protecting Your Network and Information Assets; Butterworth-Heinemann; ISBN 10: 0750677953; 2005; 296 pages.
- Landoll, Douglas J.; The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments; CRC; ISBN 10: 0849339981; 2005; 504 pages.
- McGraw, Gary; Software Security – Building Security In; Addison Wesley Professional, Boston, MA; ISBN 10-0321356705; 2006; 448 pages.
- Rice, David; Geekonomics: The Real Cost of Insecure Software; Addison Wesley Professional, Boston, MA; ISBN 10: 0321477898; 2007; 384 pages.
- Scambray, Joel; Hacking Exposed Windows: Microsoft Windows Security Secrets and Solutions; 3<sup>rd</sup> edition; McGraw Hill Osborne, New York, NY; ISBN 10: 007149426X; 2007; 451 pages.
- Scambray, Joel; Hacking Exposed Web Applications; 2nd edition; McGraw Hill Osborne, New York, NY; ISBN 10: 0072262990; 2006; 520 pages.
- Sherwood, John; Clark, Andrew; and Lynas, David; Enterprise Security Architecture: A Business-Driven Approach; CMP; ISBN 10: 157820318X; 2005; 608 pages.

Skudis, Edward and Liston, Tom; Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses; Prentice Hall PTR, Englewood Cliffs, NJ; ISBN 10: 0131481045; 2006; 784 pages.

Skudis, Edward and Zeltzer, Lenny; Malware: Fighting Malicious Code; Prentice Hall PTR, Englewood Cliffs, NJ; ISBN 10: 0131014056; 2003; 676 pages.

Shostack, Adam and Stewart, Andrews; The New School of Information Security; Addison Wesley Professional, Boston, MA; ISBN 10: 0321502787; 2008; 288 pages.

Stuttard, Dafydd and Pinto, Marcus; The Web Application Hackers Handbook: Discovering and Exploiting Security Flaws; Wiley, New York; ISBN 10: 0470170778; 2007; 768 pages.

Szor, Peter; The Art of Computer Virus Research and Defense; Addison Wesley Professional, Boston, Ma; ISBN 10: 0321304543; 2005; 744 pages.

Thompson, Herbert and Chase, Scott; The Software Vulnerability Guide; Charles River Media, Boston, MA; ISBN 10: 1584503580; 2005; 354 pages.

Viega, John and McGraw, Gary; Building Secure Software: How to Avoid Security Problems the Right Way; Addison Wesley Professional, Boston, MA; ISBN 10: 020172152X; 2001; 528 pages.

Whittaker, James A. and Thompson, Herbert H.; How to Break Software Security; Addison Wesley, Boston, MA; ISBN 10: 0321194330; 2003; 208 pages.

Wysopal, Chris; Nelson, Lucas; Zovi, Dino Dai; and Dustin, Elfriede; The Art of Software Security Testing: Identifying Software Security Flaws; Addison Wesley Professional, Boston, MA; ISBN 10: 0321304861; 2006; 321 pages.