

Computer Security

In this chapter, you will learn how to

- Explain the threats to your computers and data
- Describe how to control the local computing environment
- Explain how to protect computers from network threats

Your PC is under siege. Through your PC, a malicious person can gain valuable information about you and your habits. He can steal your files. He can run programs that log your keystrokes and thus gain account names and passwords, credit card information, and more. He can run software that takes over much of your computer processing time and use it to send spam or steal from others. The threat is real and right now. Worse, he's doing one or more of these things to your clients as I write these words. You need to secure your computer and your users from these attacks.

But what does computer security mean? Is it an antivirus program? Is it big, complex passwords? Sure, it's both of these things, but what about the fact that your laptop can be stolen easily? Before you run out in a panic to buy security applications, let's take a moment to understand the threat to your computers, see what needs to be protected, and how to do so.

Analyzing the Threat

Threats to your data and PC come from two directions: mistakes and malicious people. All sorts of things can go wrong with your computer, from a user getting access to a folder he or she shouldn't see to a virus striking and deleting folders. Files can get deleted, renamed, or simply lost. Hard drives can die, and CD- and DVD-media discs get scratched and rendered unreadable. Even well-meaning people can make mistakes.

Unfortunately, there are a lot of people out there who intend to do you harm. Add that intent together with a talent for computers, and you've got a deadly combination. Let's look at the following issues:

- Unauthorized access
- Data destruction, accidental or deliberate
- Administrative access
- Catastrophic hardware failures
- Viruses/spyware

Historical/Conceptual

Unauthorized Access

Unauthorized access occurs when a user accesses resources in an unauthorized way. Resources in this case mean data, applications, and hardware. A user can alter or delete data; access sensitive information, such as financial data, personnel files, or e-mail messages; or use a computer for purposes the owner did not intend.

Not all unauthorized access is malicious—often this problem arises when users who are randomly poking around in a computer discover that they can access resources in a fashion the primary user did not intend. Unauthorized access can sometimes be very malicious when outsiders knowingly and intentionally take advantage of weaknesses in your security to gain information, use resources, or destroy data!

Data Destruction

Often an extension of unauthorized access, data destruction means more than just intentionally or accidentally erasing or corrupting data. It's easy to imagine some evil hacker accessing your network and deleting all your important files, but consider the case where authorized users access certain data, but what they do to that data goes beyond what they are authorized to do. A good example is the person who legitimately accesses a Microsoft Access product database to modify the product descriptions, only to discover he or she can change the prices of the products, too.

This type of threat is particularly dangerous when users are not clearly informed about the extent to which they are authorized to make changes. A fellow tech once told me about a user who managed to mangle an important database due to someone giving them incorrect access. When confronted, the user said: "If I wasn't allowed to change it, the system wouldn't let me do it!" Many users believe that systems are configured in a paternalistic way that wouldn't allow them to do anything inappropriate. As a result, users will often assume they're authorized to make any changes they believe are necessary when working on a piece of data they know they're authorized to access.

Administrative Access

Every operating system enables you to create user accounts and grant those accounts a certain level of access to files and folders in that computer. As an administrator, supervisor, or root user, you have full control over just about every aspect of the computer. Windows XP, in particular, makes it entirely too easy to give users administrative access to the computer, especially Windows XP Home because it allows only two kinds of users, administrators and limited users. Because you can't do much as a limited user, most home and small office systems simply use multiple administrator accounts. If you need to control access, you really need to use Windows 2000 or XP Professional.

System Crash/Hardware Failure

Like any technology, computers can and will fail—usually when you can least afford for it to happen. Hard drives crash, the power fails—it's all part of the joy of working in the computing business. You need to create redundancy in areas prone to failure (like installing backup power in case of electrical failure) and perform those all-important data backups. Chapter 15, “Maintaining and Troubleshooting Windows,” goes into detail about using Microsoft Backup and other issues involved in creating a stable and reliable system.

Virus/Spyware

Networks are without a doubt the fastest and most efficient vehicles for transferring computer viruses among systems. News reports focus attention on the many virus attacks from the Internet, but a huge number of viruses still come from users who bring in programs on floppy disks, writable optical discs, and USB drives. This chapter describes the various methods of virus infection, and what you need to do to prevent virus infection of your networked systems in the “Network Security” section.

Essentials

Local Control

To create a secure computing environment, you need to establish control over local resources. You need to back up data and make sure that retired hard drives and optical discs have no sensitive data on them. You should recognize security issues and be able to respond properly. You need to implement good access control policies, such as having all computers in your care locked down with proper passwords or other devices that recognize who should have access. Finally, and this is particularly important for the IT Technician exam, you need to be able to implement methods for tracking computer usage. If someone is doing something wrong, you and the network or computer administrator should be able to catch him or her!

To mimic the physician's oath, here's the technician's oath: “Technician, first, secure your data.” You need to back up data on machines in your care properly. Also, techs need to follow correct practices when retiring or donating old equipment. Let's take a look.

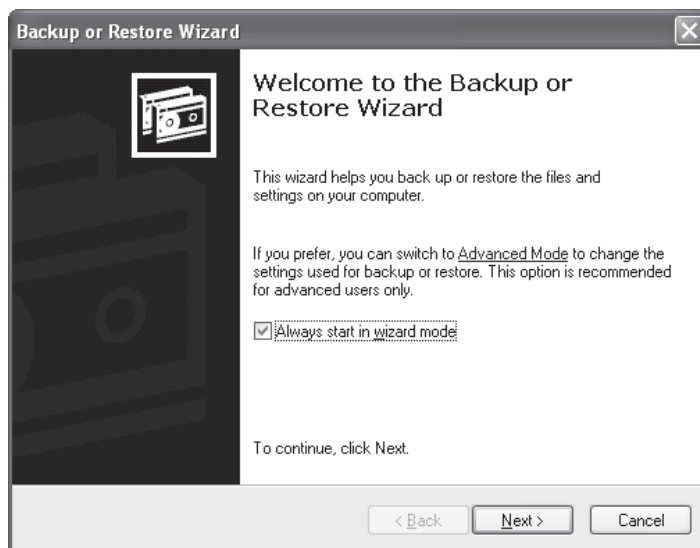
What to Back Up

Systems in your care should have regular backups performed of essential operating system files and, most importantly, data files. Chapter 15, “Maintaining and Troubleshooting Windows,” covers the process of backing up data, such as running the Backup or Restore Wizard in Windows 2000 and Windows XP, so the mechanics aren't covered here. Instead, this chapter looks more critically at what files to back up and how to protect those files.

Essential Data

By default, the Backup or Restore Wizard in Windows XP offers to back up your Documents and Settings folder (Figure 23-1). You also have options to back up everyone's documents and settings. That takes care of most, but not all, of your critical data. There are other issues to consider.

Figure 23-1
Backup or Restore Wizard



NOTE Windows 2000 and 2003 open the Backup Wizard with somewhat different settings. You are prompted to back up the entire drive initially, for example, rather than just Documents and Settings. This is also the case when you run the wizard in Windows XP in Advanced Mode.

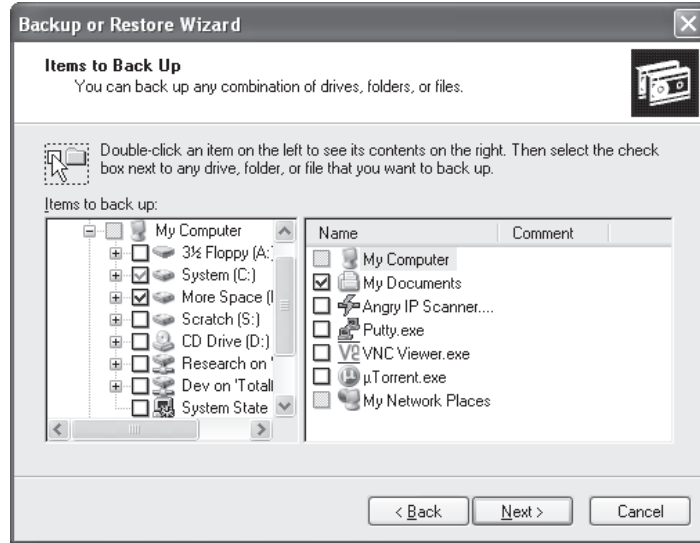
First, if you use Microsoft Outlook for your e-mail, the saved e-mail messages—both received and sent—will not be backed up. Neither will your address book. If you don't care about such things, then that's fine, but if you share a computer with multiple users, you need to make certain that you or the users back up both their mail and address book manually and then put the backed-up files in the Documents and Settings folder! That way, the Backup or Restore Wizard will grab those files.

Second, if you or others on the computer use any folders outside the Documents and Settings environment, then you need to select the *Let me choose what to back up* option from the Backup or Restore Wizard when prompted. This opens the Items to Back Up dialog where you can select individual files and folders to back up (Figure 23-2).

Server Environments

If you work in an environment that requires you to back up Windows 2000 Server or Windows Server 2003 computers, you need to back up some extra data. This is espe-

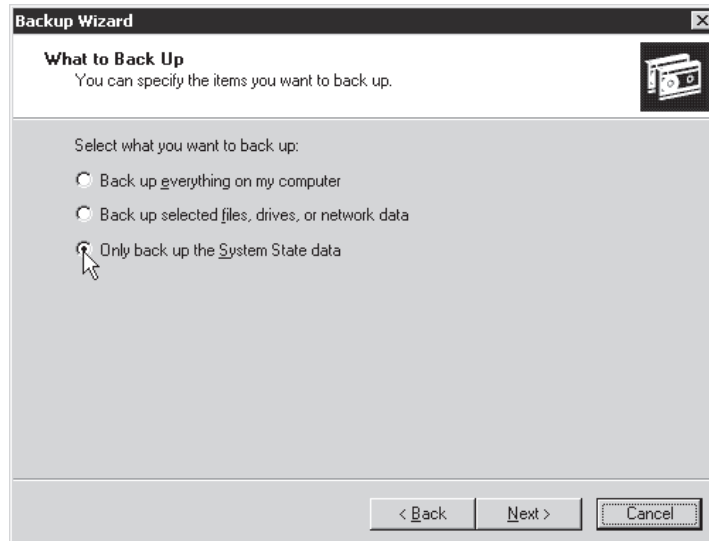
Figure 23-2
Selecting items
to back up



cially true if you have a Windows network running. Windows networking features *Active Directory*, a system that enables you to share files easily within the network, yet still maintain rock-solid security. A user only has to log in once to an Active Directory server and then they have access to resources throughout the Active Directory network (assuming, of course, that the user has permission to access those resources).

To back up the extra data, you need to run the Backup Wizard and select the radio button that says *Only back up the System State data* (Figure 23-3). This takes care of most of the registry, security settings, the Desktop files and folders, and the default user.

Figure 23-3
Backup Wizard



If you want to back up more than that, close the wizard and select the Backup tab in the Backup dialog box. Check the box next to System State and then check off any other file or folder that you want backed up (Figure 23-4). From this same dialog box, you can select where to back up the data, such as to a tape drive or external hard drive.

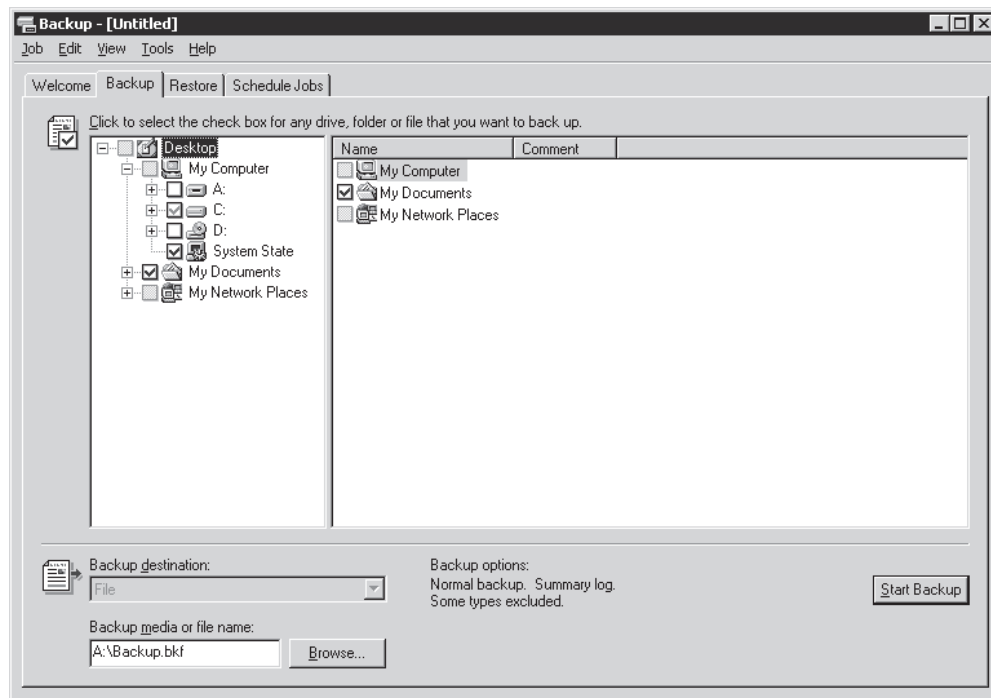


Figure 23-4 Backup tab in the Backup dialog box with System State and My Documents selected

Offsite Storage

Backing up your data and other important information enables you to restore easily in case of a system crash or malicious data destruction, but to ensure proper security, you need to store your backups somewhere other than your office. Offsite storage means that you take the tape or portable hard drive that contains your backup and lock it in a briefcase. Take it home and put it in your home safe, if you have one. This way, if the building burns down or some major flood renders your office inaccessible, your company can be up and running very quickly from a secondary location.



EXAM TIP The CompTIA A+ certification exams most likely won't ask you about offsite storage, but in today's world, anything less would be illogical.

Migrating and Retiring

Seasons change and so does the state of the art in computing. At a certain point in a computer's life, you'll need to retire an old system. This means you must migrate the data and users to a new system or at least a new hard drive and then safely dispose of the old system. Chapter 15, "Maintaining and Troubleshooting Windows," went through the details of the Documents and Settings Transfer Wizard, so I won't bore you by repeating that here. When talking about migration or retirement in terms of security, you need to answer one question: what do you do with the old system or drive?

All but the most vanilla new installations have sensitive data on them, even if it's simply e-mail messages or notes-to-self that would cause embarrassment if discovered. Most PCs, especially in a work environment, contain a lot of sensitive data. You can't just format C: and hand over the drive.

Follow three principles when migrating or retiring a computer. First, migrate your users and data information in a secure environment. Until you get passwords properly in place and test the security of the new system, you can't consider that system secure. Second, remove data remnants from hard drives that you store or give to charity. Third, recycle the older equipment; don't throw it in the trash. PC recyclers go through a process of deconstructing hardware, breaking system units, keyboards, printers, and even monitors into their basic plastics, metals, and glass for reuse.

Migration Practices

Migrate your users and data information in a secure environment. Until you get passwords properly in place and test the security of the new system, you can't consider that system secure. Don't set a copy to run while you go out to lunch, but rather be there to supervise and remove any remnant data that might still reside on any mass storage devices, especially hard drives.

You might think that, as easy as it seems to be to lose data, that you could readily get rid of data if you tried. That's not the case, however, with magnetic media such as hard drives and flash memory. It's very difficult to clean a drive completely. Repeated formatting won't do the trick. Partitioning and formatting won't work. Data doesn't necessarily get written over in the same place every time, which means that a solid wipe of a hard drive by writing zeroes to all the clusters still potentially leaves a lot of sensitive and recoverable data, typically called *remnants*, on the drive.

Although you can't make data 100 percent unrecoverable short of physically shredding or pulverizing a drive, you can do well enough for donation purposes by using one of the better drive-wiping utilities, such as Webroot's Window Washer (Figure 23-5). Window Washer gives you the ability to erase your Web browsing history, your recent activity in Windows (such as what programs you ran), and even your e-mail messages permanently. As an added bonus, you can create a bootable disk that enables you to wipe a drive completely.

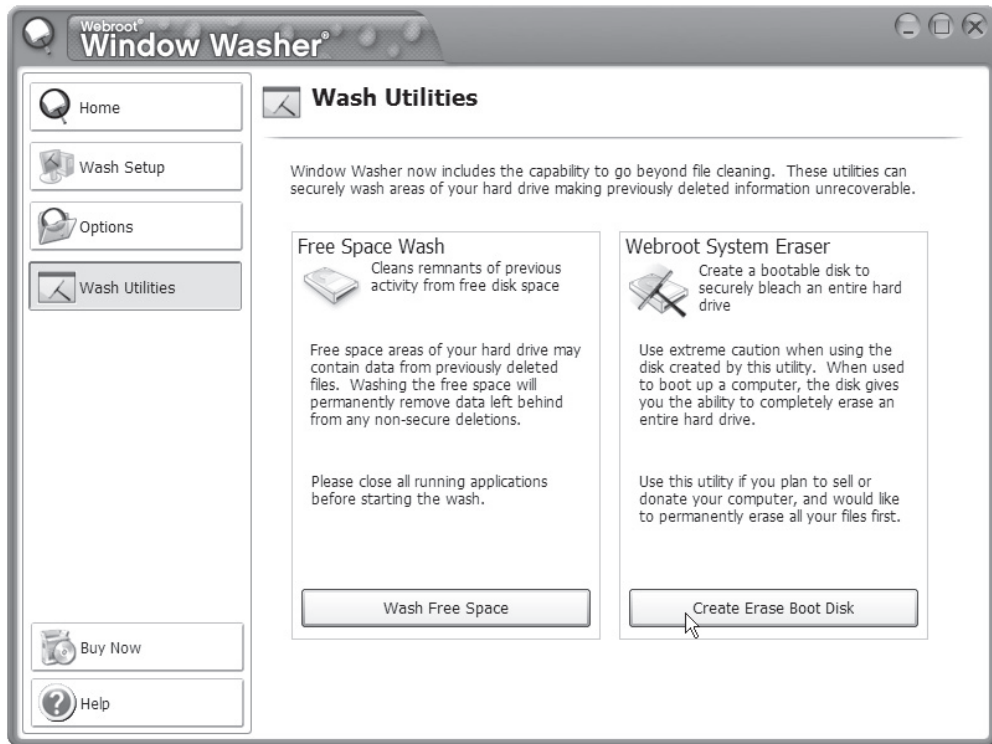


Figure 23-5 Webroot Window Washer security software

Recycle

An important and relatively easy way to be an environmentally conscious computer user is to *recycle*. Recycling products such as paper and printer cartridges not only keeps them out of overcrowded landfills, but also ensures that the more toxic products are disposed of in the right way. Safely disposing of hardware containing hazardous materials, such as computer monitors, protects both people and the environment.

Anyone who's ever tried to sell a computer more than three or four years old learns a hard lesson—they're not worth much if anything at all. It's a real temptation to take that old computer and just toss it in the garbage, but never do that!

First of all, many parts of your computer—such as your computer monitor—contain hazardous materials that pollute the environment. Luckily, thousands of companies now specialize in computer recycling and will gladly accept your old computer. If you have enough computers, they might even pick them up. If you can't find a recycler, call your local municipality's waste authority to see where to drop off your system.

An even better alternative for your old computer is donation. Many organizations actively look for old computers to refurbish and to donate to schools and other organizations. Just keep in mind that the computer can't be too old—not even a school wants a computer more than five or six years old.

IT Technician

Social Engineering

Although you're more likely to lose data through accident, the acts of malicious users get the vast majority of headlines. Most of these attacks come under the heading of *social engineering*—the process of using or manipulating people inside the networking environment to gain access to that network from the outside. The term “social engineering” covers the many ways humans can use other humans to gain unauthorized information. This unauthorized information may be a network login, a credit card number, company customer data—almost anything you might imagine that one person or organization may not want a person outside of that organization to access.



EXAM TIP CompTIA considers security to be an extremely important topic, whether you're at the Essentials level or any of the Technician levels. Unlike other chapters, almost every single topic covered in the IT Technician section of this chapter *applies equally to the Essentials section*. In other words, you need to know everything in this chapter to pass any of the four CompTIA A+ certification exams.

Social engineering attacks aren't hacking—at least in the classic sense of the word—although the goals are the same. Social engineering is where people attack an organization through the people in the organization or physically access the organization to get the information they need. Here are a few of the more classic types of social engineering attacks.



NOTE It's common for these attacks to be used together, so if you discover one of them being used against your organization, it's a good idea to look for others.

Infiltration

Hackers can physically enter your building under the guise of someone who might have a legitimate reason for being there, such as cleaning personnel, repair technicians, or messengers. They then snoop around desks, looking for whatever they can find. They might talk with people inside the organization, gathering names, office numbers, department names—little things in and of themselves, but powerful tools when combined later with other social engineering attacks.

Telephone Scams

Telephone scams are probably the most common social engineering attack. In this case, the attacker makes a phone call to someone in the organization to gain information. The attacker attempts to come across as someone inside the organization and uses this to get the desired information. Probably the most famous of these scams is the “I forgot

my user name and password” scam. In this gambit, the attacker first learns the account name of a legitimate person in the organization, usually using the infiltration method. The attacker then calls someone in the organization, usually the help desk, in an attempt to gather information, in this case a password.

Hacker: “Hi, this is John Anderson in accounting. I forgot my password. Can you reset it please?”

Help Desk : “Sure, what’s your user name?”

Hacker: “j_w_Anderson”

Help Desk: “OK, I reset it to e34rd3.”

Certainly telephone scams aren’t limited to attempts to get network access. There are documented telephone scams against organizations aimed at getting cash, black-mail material, or other valuables.

Dumpster Diving

Dumpster diving is the generic term for anytime a hacker goes through your refuse, looking for information. The amount of sensitive information that makes it into any organization’s trash bin boggles the mind! Years ago, I worked with an IT security guru who gave me and a few other IT people a tour of our office’s trash. In one 20-minute tour of the personal wastebaskets of one office area, we had enough information to access the network easily, as well as to embarrass seriously more than a few people. When it comes to getting information, the trash is the place to look!

Physical Theft

I once had a fellow network geek challenge me to try to bring down his newly installed network. He had just installed a powerful and expensive firewall router and was convinced that I couldn’t get to a test server he added to his network just for me to try to access. After a few attempts to hack in over the Internet, I saw that I wasn’t going to get anywhere that way. So I jumped in my car and drove to his office, having first outfitted myself in a techy-looking jumpsuit and an ancient ID badge I just happened to have in my sock drawer. I smiled sweetly at the receptionist and walked right by my friend’s office (I noticed he was smugly monitoring incoming IP traffic using some neat packet-sniffing program) to his new server. I quickly pulled the wires out of the back of his precious server, picked it up, and walked out the door. The receptionist was too busy trying to figure out why her e-mail wasn’t working to notice me as I whisked by her carrying the 65-pound server box. I stopped in the hall and called him from my cell phone.

Me (cheerily): “Dude, I got all your data!”

Him (not cheerily): “You rebooted my server! How did you do it?”

Me (smiling): “I didn’t reboot it—go over and look at it!”

Him (really mad now): “YOU <EXPLETIVE> THIEF! YOU STOLE MY SERVER!”

Me (cordially): “Why, yes. Yes, I did. Give me two days to hack your password in the comfort of my home, and I’ll see everything! Bye!”

I immediately walked back in and handed him the test server. It was fun. The moral here is simple—never forget that the best network software security measures can be rendered useless if you fail to protect your systems physically!

Access Control

Access is the key. If you can control access to the data, programs, and other computing resources, you've secured your system. Access control is composed of five interlinked areas that a good, security-minded tech should think about: physical security, authentication, the file system, users and groups, and security policies. Much of this you know from previous chapters, but this section should help tie it all together as a security topic.

Secure Physical Area and Lock Down Your System

The first order of security is to block access to the physical hardware from people who shouldn't have access. This isn't rocket science. Lock the door. Don't leave a PC unattended when logged in. In fact, don't ever leave a system logged in, even as a limited user. God help you if you walk away from a server still logged in as an administrator. You're tempting fate.

For that matter, when you see a user's computer logged in and unattended, do the user and your company a huge favor and lock the computer. Just walk up and press CTRL-L on the keyboard to lock the system. It works in Windows 2000 and all versions of Windows XP and Windows Vista.



EXAM TIP Expect questions on controlling access to computers and computer rooms on the CompTIA A+ 220-604 Depot Technician exam.

Authentication

Security starts with properly implemented *authentication*, which means in essence, how the computer determines who can or should access it. And, once accessed, what that user can do. A computer can authenticate users through software or hardware, or a combination of both.

Software Authentication: Proper Passwords It's still rather shocking to me to power up a friend's computer and go straight to his or her desktop; or with my married-with-kids friends, to click one of the parent's user account icons and not get prompted for a password. This is just wrong! I'm always tempted to assign passwords right then and there—and not tell them the passwords, of course—so they'll see the error of their ways when they try to log in next. I don't do it, but always try to explain gently the importance of good passwords.

You know about passwords from Chapter 15, "Maintaining and Troubleshooting Windows," so I won't belabor the point here. Suffice it to say that you need to make certain that all your users have proper passwords. Don't let them write passwords down or tape them to the underside of their mouse pads either!

It's not just access to Windows that you need to think about. If you have computers running in a public location, there's always the temptation for people to hack the system and do mean things, like change CMOS settings to render the computer inoperable to the casual user until a tech can undo the damage. All modern CMOS setup utilities come with an access password protection scheme (Figure 23-6).

Figure 23-6
CMOS access
password request

```
***  
[OS Extension v1.00  
ard Software, Inc.  
ry Master ... ST10232A  
ry Slave ... None  
lary  
lary
```

Enter Password:

Hardware Authentication Smart cards and biometric devices enable modern systems to authenticate users with more authority than mere passwords. Smart cards are credit-card-sized cards with circuitry that can be used to identify the bearer of the card. Smart cards are relatively common for tasks such as authenticating users for mass transit systems, for example, but fairly uncommon in computers. Figure 23-7 shows a smart card and keyboard combination.

Figure 23-7
Smart card and
keyboard reader
(photo courtesy
of Cherry Corp.)



People can guess or discover passwords, but it's a lot harder to forge someone's fingerprints. The keyboard in Figure 23-8 authenticates users on a local machine using fingerprints. Other devices that will do the trick are key fobs, retinal scanners, and PC cards for laptop computers.

Figure 23-8
Microsoft keyboard
with fingerprint
accessibility



NOTE Full disclosure time. Microsoft does not claim that the keyboard in Figure 23-8 offers any security at all. In fact, the documentation specifically claims that the fingerprint reader is an accessibility tool, not a security device. Because it enables a person to log onto a local machine, though, I think it falls into the category of authentication devices.

Clever manufacturers have developed key fobs and smart cards that use radio frequency identification (RFID) to transmit authentication information, so users don't have to insert something into a computer or card reader. The Privarius plusID combines, for example, a biometric fingerprint fob with an RFID tag that makes security as easy as opening a garage door remotely! Figure 23-9 shows a plusID device.

Figure 23-9
plusID (photo
courtesy of
Privaris, Inc.)



PRIVARIS

NTFS, not FAT32!

The file system on a hard drive matters a lot when it comes to security. On a Windows machine with multiple users, you simply must use NTFS or you have no security at all. Not just primary drives, but any secondary drives in computers in your care should be formatted as NTFS, with the exception of removable drives, such as the one you use to back up your system.

When you run into a multiple-drive system that has a second or third drive formatted as FAT32, you can use the *CONVERT* command-line utility to go from FAT to NTFS. The syntax is pretty straightforward. To convert a D: drive from FAT or FAT32 to NTFS, for example, you'd type the following:

```
CONVERT D: /FS:NTFS
```

You can substitute a mount name in place of the drive letter in case you have a mounted volume. The command has a few extra switches as well, so at the command prompt, type a */?* after the *CONVERT* command to see all your options.

Users and Groups

Windows uses user accounts and groups as the bedrock of access control. A user account gets assigned to a group, such as Users, Power Users, or Administrators, and by association gets certain permissions on the computer. Using NTFS enables the highest level of control over data resources.

Assigning users to groups is a great first step in controlling a local machine, but this feature really shines once you go to a networked environment. Let's go there now.

Network Security

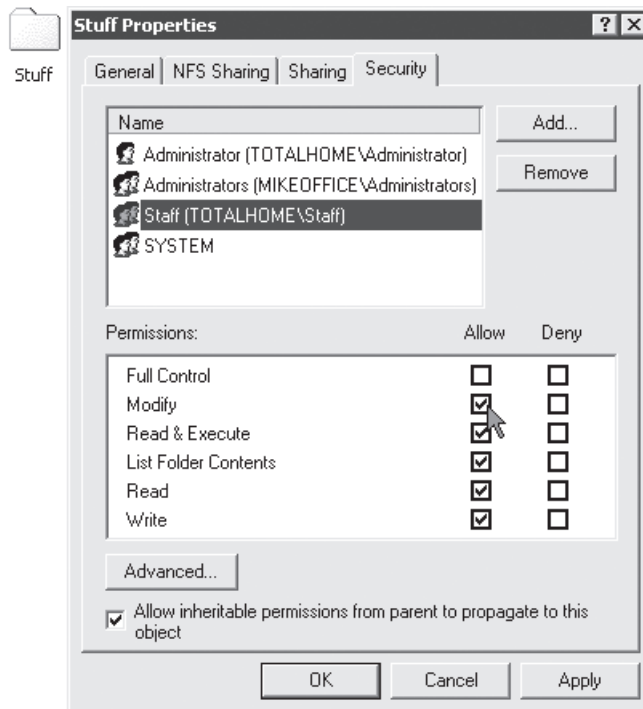
The vast majority of protective strategies related to internal threats are based on policies rather than technology. Even the smallest network will have a number of user accounts and groups scattered about with different levels of rights/permissions. Every time you give a user access to a resource, you create potential loopholes that can leave your network vulnerable to unauthorized access, data destruction, and other administrative nightmares. To protect your network from internal threats, you need to implement the correct controls over user accounts, permissions, and policies.

Networks are under threat from the outside as well, so this section looks at issues involving Internet-borne attacks, firewalls, and wireless networking. The section finishes with discussion of the tools you need to track computer and network activity and, if necessary, lock down your systems.

User Account Control Through Groups

Access to user accounts should be restricted to the assigned individuals, and those accounts should have permission to access only the resources they need, no more. Tight control of user accounts is critical to preventing unauthorized access. Disabling unused accounts is an important part of this strategy, but good user account control goes far deeper than that. One of your best tools for user account control is groups. Instead of giving permissions/rights to individual user accounts, give them to groups; this makes keeping track of the permissions assigned to individual user accounts much easier. Figure 23-10 shows me giving permissions to a group for a folder in Windows 2000. Once a group is created and its permissions set, you can then add user accounts to that group as needed. Any user account that becomes a member of a group automatically gets the permissions assigned to that group. Figure 23-11 shows me adding a user to a newly created group in the same Windows 2000 system.

Figure 23-10
Giving a group
permissions for a
folder in Windows
2000



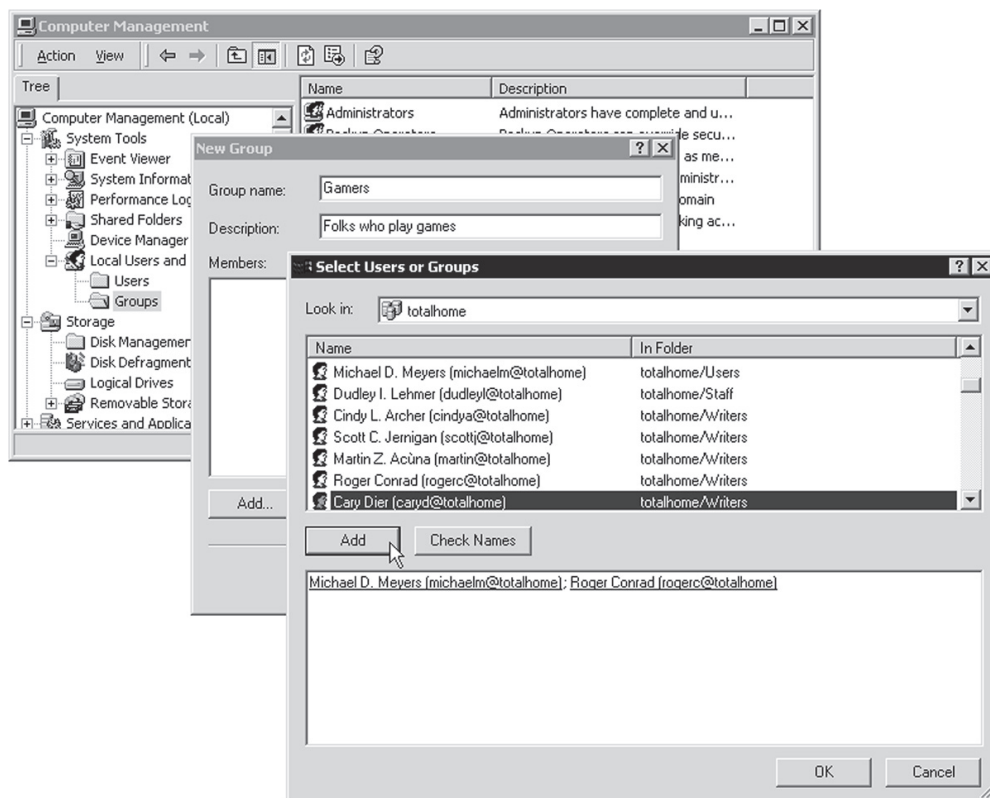


Figure 23-11 Adding a user to a newly created group in Windows 2000

Groups are a great way to get increased complexity without increasing the administrative burden on network administrators, because all network operating systems combine permissions. When a user is a member of more than one group, which permissions does he or she have with respect to any particular resource? In all network operating systems, the permissions of the groups are *combined*, and the result is what you call the *effective permissions* the user has to access the resource. Let's use an example from Windows 2000. If Rita is a member of the Sales group, which has List Folder Contents permission to a folder, and she is also a member of the Managers group, which has Read and Execute permissions to the same folder, Rita will have both List Folder Contents *and* Read and Execute permissions to that folder.

Watch out for *default* user accounts and groups—they can become secret backdoors to your network! All network operating systems have a default Everyone group, and it can be used to sneak into shared resources easily. This Everyone group, as its name implies, literally includes anyone who connects to that resource. Windows 2000 gives full control to the Everyone group by default, for example, so make sure you know to lock this down!

All of the default groups—Everyone, Guest, Users—define broad groups of users. Never use them unless you intend to permit all those folks to access a resource. If you use

one of the default groups, remember to configure them with the proper permissions to prevent users from doing things you don't want them to do with a shared resource!

All of these groups and organizational units only do one thing for you: They let you keep track of your user accounts, so you know they are only available for those who need them, and they only access the resources you want them to use.

Security Policies

While permissions control how users access shared resources, there are other functions you should control that are outside the scope of resources. For example, do you want users to be able to access a command prompt on their Windows system? Do you want users to be able to install software? Would you like to control what systems or what time of day a user can log in? All network operating systems provide you with some capability to control these and literally hundreds of other security parameters, under what Windows calls *policies*. I like to think of policies as permissions for activities as opposed to true permissions, which control access to resources.

A policy is usually applied to a user account, a computer, or a group. Let's use the example of a network composed of Windows XP Professional systems with a Windows 2000 Server system. Every Windows XP system has its own local policies program, which enables policies to be placed on that system only. Figure 23-12 shows the tool you use to set local policies on an individual system, called *Local Security Settings*, being used to deny the user account Danar the capability to log on locally.

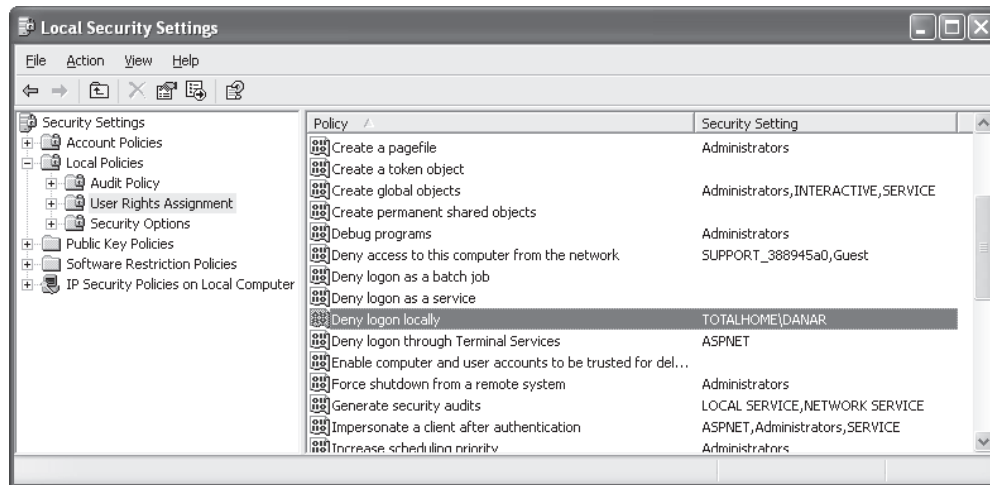


Figure 23-12 Local Security Settings

Local policies work great for individual systems, but they can be a pain to configure if you want to apply the same settings to more than one PC on your network. If you want to apply policy settings *en masse*, then you need to step up to Windows Active Directory domain-based *Group Policy*. Using Group Policy, you can exercise deity-like—Microsoft prefers to use the term *granular*—control over your network clients.

Want to set default wallpaper for every PC in your domain? Group Policy can do that. Want to make certain tools inaccessible to everyone except authorized users? Group Policy can do that, too. Want to control access to the Internet, redirect home folders, run scripts, deploy software, or just remind folks that unauthorized access to the network will get them nowhere fast? Group Policy is the answer. Figure 23-13 shows Group Policy; I'm about to change the default title on every instance of Internet Explorer on every computer in my domain!

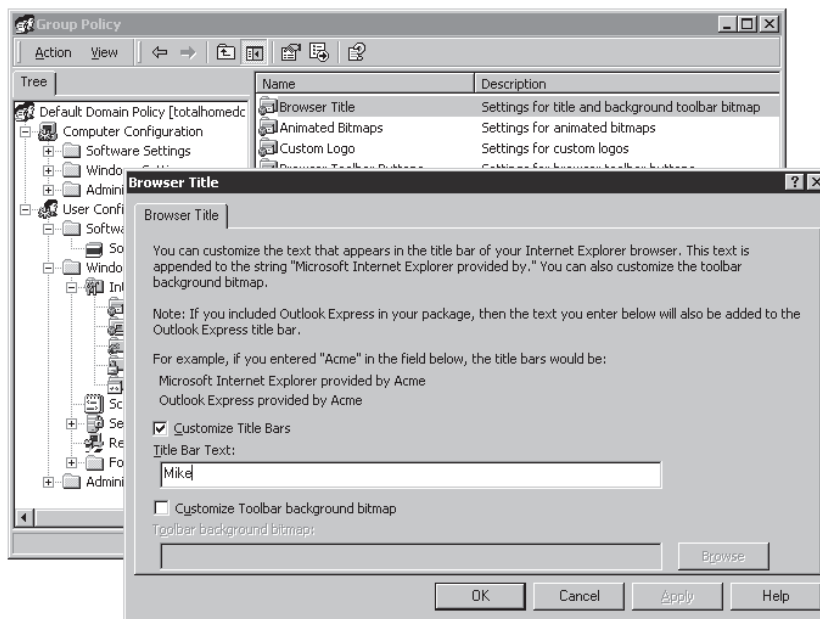


Figure 23-13 Using Group Policy to make IE title say “provided by Mike!”

That’s just one simple example of the types of settings you can configure using Group Policy. There are literally hundreds of “tweaks” you can apply through Group Policy, from the great to the small, but don’t worry too much about familiarizing yourself with each and every one. Group Policy settings are a big topic in the Microsoft Certified Systems Administrator (MCSA) and Microsoft Certified Systems Engineer (MCSE) certification tracks, but for the purposes of the CompTIA A+ exams, you simply have to be comfortable with the concept behind Group Policy.



NOTE Linux doesn’t provide a single application that you open to set up policies, like Windows does. In fact, Linux doesn’t even use the name “policies.” Instead, Linux relies on individual applications to set up policies for whatever they’re doing. This is in keeping with the Linux paradigm of having lots of little programs that do one thing well, as opposed to the Windows paradigm of having one program try to be all things for all applications.

Although I could never list every possible policy you can enable on a Windows system, here's a list of some of those more commonly used:

- **Prevent Registry Edits** If you try to edit the Registry, you get a failure message.
- **Prevent Access to the Command Prompt** This policy keeps users from getting to the command prompt by turning off the Run command and the MS-DOS Prompt shortcut.
- **Log on Locally** This policy defines who may log on to the system locally.
- **Shut Down System** This policy defines who may shut down the system.
- **Minimum Password Length** This policy forces a minimum password length.
- **Account Lockout Threshold** This policy sets the maximum number of logon attempts a person can make before they are locked out of the account.
- **Disable Windows Installer** This policy prevents users from installing software.
- **Printer Browsing** This policy enables users to browse for printers on the network, as opposed to using only assigned printers.

While the CompTIA A+ exams don't expect you to know how to implement policies on any type of network, you are expected to understand that policies exist, especially on Windows networks, and that they can do amazing things in terms of controlling what users can do on their systems. If you ever try to get to a command prompt on a Windows system, only to discover the Run command is grayed out, blame it on a policy, not the computer!

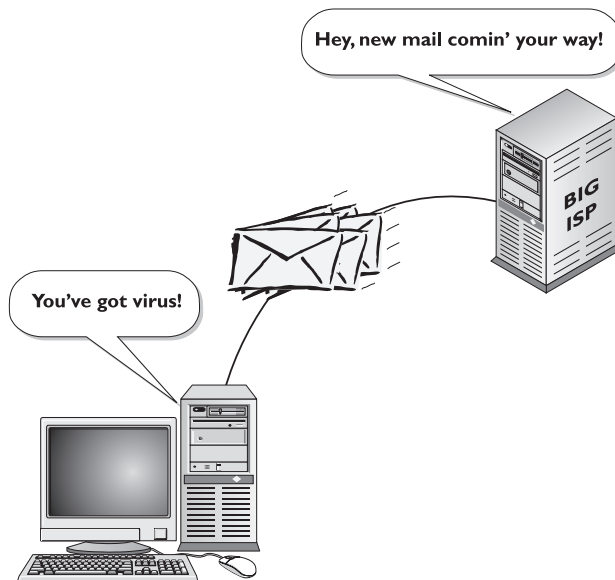
Malicious Software

The beauty of the Internet is the ease of accessing resources just about anywhere on the globe, all from the comfort of your favorite chair. This connection, however, runs both ways, and people from all over the world can potentially access your computer from the comfort of their evil lairs. The Internet is awash with malicious software (*malware*) that is—even at this moment—trying to infect your systems. Malware consists of computer programs designed to break into computers or cause havoc on computers. The most common types of malware are viruses, worms, spyware, Trojan horses, adware, and grayware. You need to understand the different types of malware so you can combat them for you and your users successfully.

Viruses

Just as a biological virus gets passed from person to person, a computer *virus* is a piece of malicious software that gets passed from computer to computer (Figure 23-14). A computer virus is designed to attach itself to a program on your computer. It could be your e-mail program, your word processor, or even a game. Whenever you use the infected program, the virus goes into action and does whatever it was designed to do. It can wipe out your e-mail or even erase your entire hard drive! Viruses are also sometimes used to steal information or send spam e-mails to everyone in your address book.

Figure 23-14
You've got mail!



Trojans

Trojans are true, freestanding programs that do something other than what the person who runs the program thinks they will do. An example of a *Trojan virus* is a program that a person thinks is a game but is actually a CMOS eraser. Some Trojans are quite sophisticated. It might be a game that works perfectly well, but when the user quits the game, it causes some type of damage.

Worms

Similar to a Trojan, a *worm* is a complete program that travels from machine to machine, usually through computer networks. Most worms are designed to take advantage of security problems in operating systems and install themselves on vulnerable machines. They can copy themselves over and over again on infected networks, and can create so much activity that they overload the network, in worst cases even bringing chunks of the entire Internet to a halt.

There are several things you can do to protect yourself and your data against these threats. First, make sure you are running up-to-date virus software—especially if you connect to the Internet via an always-on broadband connection. You should also be protected by a firewall, either as part of your network hardware or by means of a software program. (See the sections on antivirus programs and firewalls later in this chapter.)

Since worms most commonly infect systems because of security flaws in operating systems, the next defense against them is to make sure you have the most current version possible of your operating system and to check regularly for security patches. A *security patch* is an addition to the operating system to patch a hole in the operating system code. You can download security patches from the software vendor's Web site (Figure 23-15).

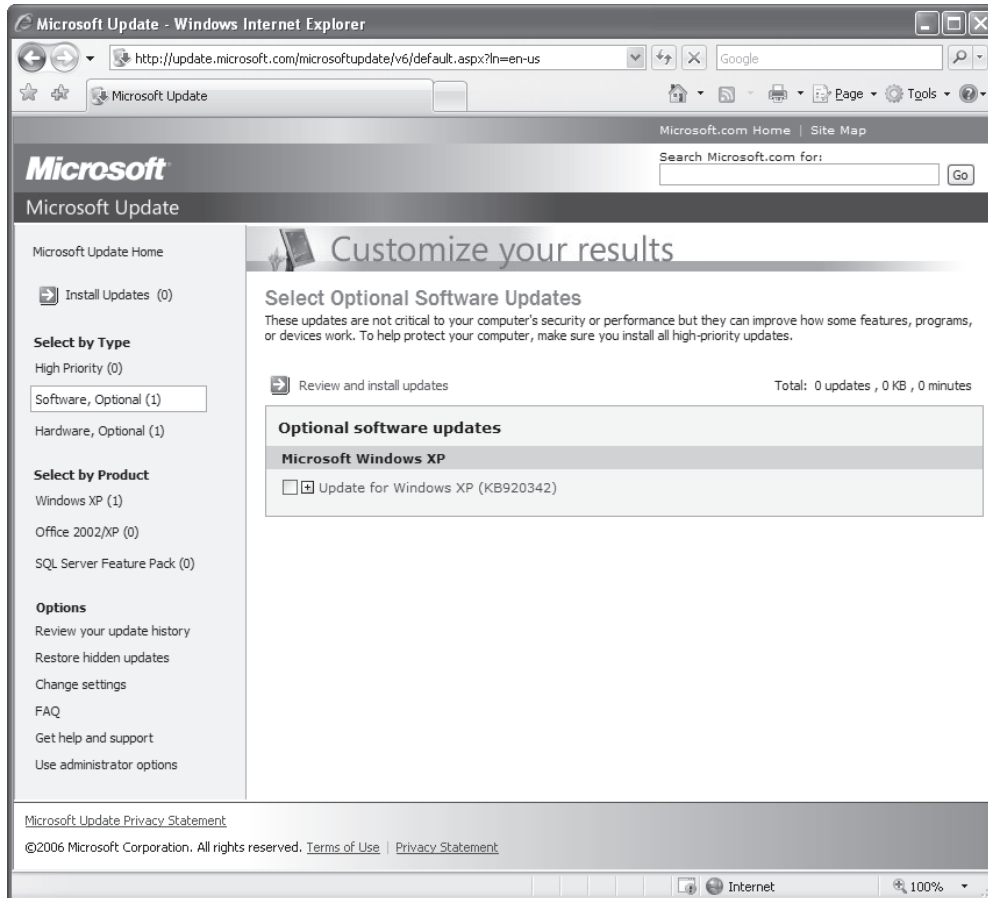


Figure 23-15 Microsoft Update

Microsoft's Windows Update tool is handy for Windows users as it provides a simple method to ensure that your version's security is up to date. The one downside is that not everyone remembers to run Windows Update. Don't wait until something goes wrong on your computer, or you hear on the news that another nasty program is running rampant across the Internet—Run Windows Update weekly (or even better automatically) as a part of your normal system maintenance. Keeping your patches up-to-date is called *patch management*, and it goes a long way toward keeping your system safe!

Antivirus Programs

The only way to protect your PC permanently from getting a virus is to disconnect from the Internet and never permit any potentially infected software to touch your precious computer. Because neither scenario is likely these days, you need to use a specialized antivirus program to help stave off the inevitable virus assaults.

An antivirus program protects your PC in two ways. It can be both sword and shield, working in an active seek-and-destroy mode and in a passive sentry mode. When ordered to seek and destroy, the program will scan the computer's boot sector and files for viruses, and if it finds any, present you with the available options for removing or disabling them. Antivirus programs can also operate as virus shields that passively monitor your computer's activity, checking for viruses only when certain events occur, such as a program executing or a file being downloaded.

Antivirus programs use different techniques to combat different types of viruses. They detect boot sector viruses simply by comparing the drive's boot sector to a standard boot sector. This works because most boot sectors are basically the same. Some antivirus programs make a backup copy of the boot sector. If they detect a virus, the programs will use that backup copy to replace the infected boot sector. Executable viruses are a little more difficult to find because they can be on any file in the drive. To detect executable viruses, the antivirus program uses a library of signatures. A *signature* is the code pattern of a known virus. The antivirus program compares an executable file to its library of signatures. There have been instances where a perfectly clean program coincidentally held a virus signature. Usually the antivirus program's creator will provide a patch to prevent further alarms. Antivirus programs detect macro viruses through the presence of virus signatures or certain macro commands that indicate a known macro virus. Now that we understand the types of viruses and how antivirus programs try to protect against them, let's review a few terms that are often used when describing certain traits of viruses.

Polymorphics/Polymorphs A *polymorph virus* attempts to change its signature to prevent detection by antivirus programs, usually by continually scrambling a bit of useless code. Fortunately, the scrambling code itself can be identified and used as the signature—once the antivirus makers become aware of the virus. One technique used to combat unknown polymorphs is to have the antivirus program create a checksum on every file in the drive. A *checksum* in this context is a number generated by the software based on the contents of the file rather than the name, date, or size of that file. The algorithms for creating these checksums vary among different antivirus programs (they are also usually kept secret to help prevent virus makers from coming up with ways to beat them). Every time a program is run, the antivirus program calculates a new checksum and compares it with the earlier calculation. If the checksums are different, it is a sure sign of a virus.

Stealth The term “stealth” is more of a concept than an actual virus function. Most *stealth virus* programs are boot sector viruses that use various methods to hide from antivirus software. The AntiEXE stealth virus will hook on to a little-known but often-used software interrupt, for example, running only when that interrupt runs. Others make copies of innocent-looking files.

Virus Prevention Tips The secret to preventing damage from a malicious software attack is to keep from getting a virus in the first place. As discussed earlier, all good antivirus programs include a virus shield that will scan e-mail, downloads, running programs, and so on automatically (see Figure 23-16).

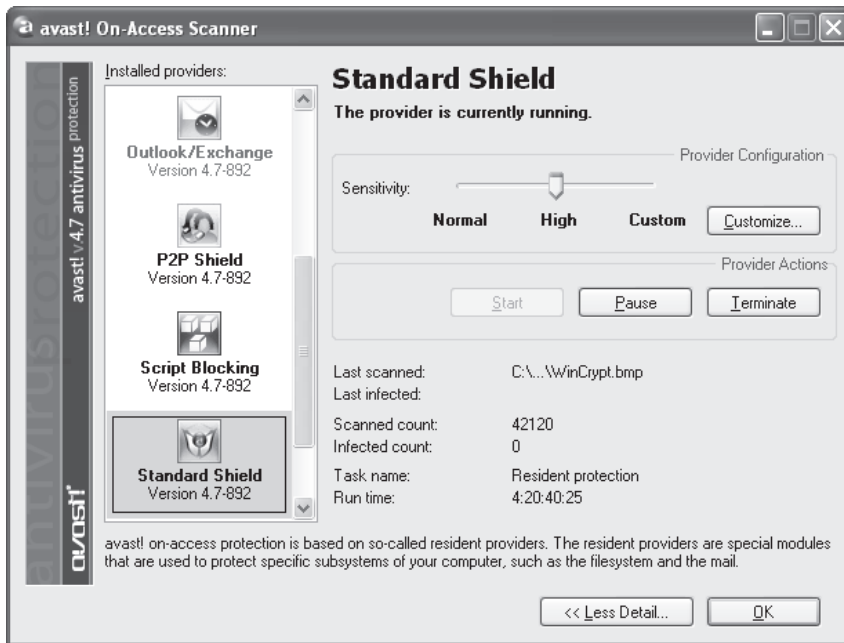


Figure 23-16 A virus shield in action

Use your antivirus shield. It is also a good idea to scan PCs daily for possible virus attacks. All antivirus programs include terminate-and-stay resident programs (TSRs) that will run every time the PC is booted. Last but not least, know where the source of any software before you load it. While the chance of commercial, shrink-wrapped software having a virus is virtually nil (there have been a couple of well-publicized exceptions), that illegal copy of Unreal Tournament you borrowed from a local hacker should definitely be inspected with care.

Keep your antivirus program updated. New viruses appear daily, and your program needs to know about them. The list of viruses your antivirus program can recognize is called the *definition file*, and you must keep that definition file up-to-date. Fortunately, most antivirus programs will update themselves automatically.

Get into the habit of keeping around an antivirus CD-R—a bootable, CD-R disc with a copy of an antivirus program. If you suspect a virus, use the disc, even if your antivirus program claims to have eliminated the virus. Turn off the PC and reboot it from the antivirus disc. (You might have to change CMOS settings to boot to optical media.) Run your antivirus program's most comprehensive virus scan. Then check all removable media that were exposed to the system, and any other machine that might have received data from it or that is networked to the cleaned machine. A virus or other malicious program can often lie dormant for months before anyone knows of its presence.

E-mail is still a common source of viruses, and opening infected e-mails is a common way to get infected. If you view an e-mail in a preview window, that opens the e-mail message and exposes your computer to some viruses. Download files only from

sites you know to be safe, and of course the less reputable corners of the Internet are the most likely places to pick up computer infections.

Viruses are not, however, the only malicious software lurking in e-mail. Sometimes the e-mail itself is the problem.

Spam

E-mail that comes into your Inbox from a source that's not a friend, family member, or colleague, and that you didn't ask for, can create huge problems for your computer and you. This unsolicited e-mail, called *spam*, accounts for a huge percentage of traffic on the Internet. Spam comes in many flavors, from legitimate businesses trying to sell you products to scammers who just want to take your money. Hoaxes, pornography, and get-rich-quick schemes pour into the Inboxes of most e-mail users. They waste your time and can easily offend.

You can use several options to cope with the flood of spam. The first option is defense. Never post your e-mail address on the Internet. One study tested this theory and found that *over 97 percent* of the spam received during the study went to e-mail addresses they had posted on the public Internet.



NOTE The Center for Democracy and Technology conducted the study in 2003, entitled “Why Am I Getting All This Spam? Unsolicited Commercial E-mail Research Six Month Report.” Here’s the Web link if you’re curious: www.cdt.org/speech/spam/030319spamreport.shtml.

Filters and filtering software can block spam at your mail server and at your computer. AOL implemented blocking schemes in 2004, for example, that dropped the average spam received by its subscribers by a large percentage, perhaps as much as 50 percent. You can set most e-mail programs to block e-mail from specific people—good to use if someone is harassing you—or to specific people. You can block by subject line or keywords. Most people use a third-party anti-spam program instead of using the filters in their e-mail program.

Pop-ups, Spyware, and Adware

On most systems, the Internet Web browser client is the most often used piece of software. Over the years, Web sites have come up with more and more ways to try to get you to see what they want you to see: their advertising. When the Web first got underway, we were forced to look at an occasional banner ad. In the last few years, Web site designers have become much more sophisticated, creating a number of intrusive and irritating ways to get you to part with your money in one form or another.

There are basically three irritating Web browser problems: pop-ups, spyware, and adware. *Pop-ups* are those surprise browser windows that appear automatically when you visit a Web site, proving themselves irritating and unwanted and nothing else. *Spyware*, meanwhile, defines a family of programs that run in the background on your PC, sending information about your browsing habits to the company that installed it on your system. *Adware* is not generally as malicious as spyware, but it works similarly to display ads on your system. As such, these programs download new ads and generate

undesirable network traffic. Of the three, spyware is much less noticeable but far more nefarious. At its worst, spyware can fire up pop-up windows of competing products on the Web site you're currently viewing. For example, you might be perusing a bookseller's Web site only to have a pop-up from a competitor's site appear.

Pop-Ups Getting rid of pop-ups is actually rather tricky. You've probably noticed that most of these pop-up browser windows don't look like browser windows at all. There's no menu bar, button bar, or address window, yet they are each separate browser windows. HTML coding permits Web site and advertising designers to remove the usual navigation aids from a browser window so all you're left with is the content. In fact, as I'll describe in a minute, some pop-up browser windows are deliberately designed to mimic similar pop-up alerts from the Windows OS. They might even have buttons similar to Windows' own exit buttons, but you might find that when you click them, you wind up with more pop-up windows instead! What to do?

The first thing you need to know when dealing with pop-ups is how to close them without actually having to risk clicking them. As I said, most pop-ups have removed all navigation aids, and many are also configured to appear on your monitor screen in a position that places the browser window's exit button—the little X button in the upper right-hand corner—outside of your visible screen area. Some even pop up behind the active browser window and wait there in the background. Most annoying! To remedy this, use alternate means to close the pop-up browser window. For instance, you can right-click the browser window's taskbar icon to generate a pop-up menu of your own. Select Close, and the window should go away. You can also bring the browser window in question to the forefront by pressing ALT-TAB until it becomes visible, and then press ALT-F4 to close it.

Most Web browsers have features to prevent pop-up ads in the first place, but I've found that these types of applications are sometimes *too* thorough. That is, they tend to prevent *all* new browser windows from opening, even those you want to view. Still, they're free to try, so have a look to see if they suit your needs. Applications such as Ad-Subtract control a variety of Internet annoyances, including pop-up windows, cookies, and Java applets, and are more configurable—you can specify what you want to allow on any particular domain address—but the fully functional versions usually cost at least something, and that much control is too confusing for most novice-level users.

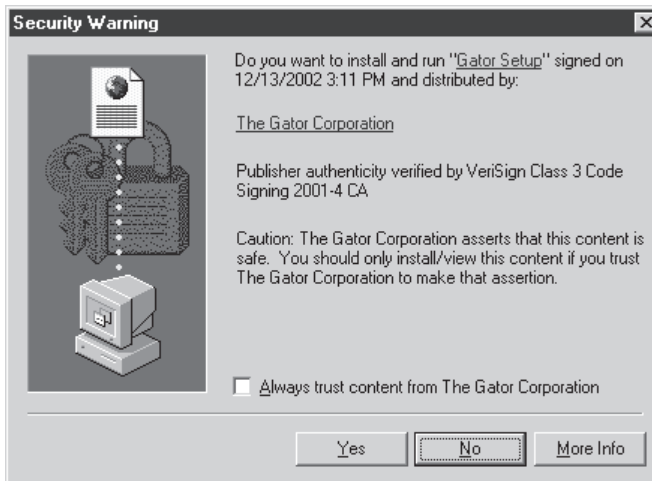
Dealing with Spyware Some types of spyware go considerably beyond this level of intrusion. They can use your computer's resources to run *distributed computing* applications, capture your keystrokes to steal passwords, reconfigure your dial-up settings to use a different phone number at a much higher connection charge, or even use your Internet connection and e-mail address list to propagate itself to other computers in a virus-like fashion! Are you concerned yet?

Setting aside the legal and ethical issues, and there are many, you should at least appreciate that spyware can seriously impact your PC's performance and cause problems with your Internet connection. The threat is real, so what practical steps can you take to protect yourself? Let's look at how to prevent spyware installation, and how to detect and remove any installed spyware.

Preventing Spyware Installation How does this spyware get into your system in the first place? Obviously, a sensible person doesn't download and install something that they know is going to compromise their computer. Makers of spyware know this, so they bundle their software with some other program or utility that purports to give you some benefit.

What kind of benefit? How about free access to MP3 music files? A popular program called Kazaa does that. How about a handy *e-wallet* utility that remembers your many screen names, passwords, and even your credit-card numbers to make online purchases easier and faster? A program called Gator does that, and many other functions as well. How about browser enhancements, performance boosters, custom cursor effects, search utilities, buddy lists, file savers, or media players? The list goes on and on, yet they all share one thing—they're simply window-dressing for the *real* purpose of the software. So you see, for the most part spyware doesn't need to force its way into your PC. Instead they saunter calmly through the front door. If the graphic in Figure 23-17 looks familiar, you might have installed some of this software yourself.

Figure 23-17
Gator Corporation's
acknowledgment
warning



Some spyware makers use more aggressive means to get you to install their software. Instead of offering you some sort of attractive utility, they instead use fear tactics and deception to try to trick you into installing their software. One popular method is to use pop-up browser windows crudely disguised as Windows' own system warnings (Figure 23-18). When clicked, these may trigger a flood of other browser windows, or may even start a file download.

The lesson here is simple—*don't install these programs!* Careful reading of the software's license agreement before you install a program is a good idea, but realistically, it does little to protect your PC. With that in mind, here are a couple of preventative measures you can take to keep parasitic software off of your system.

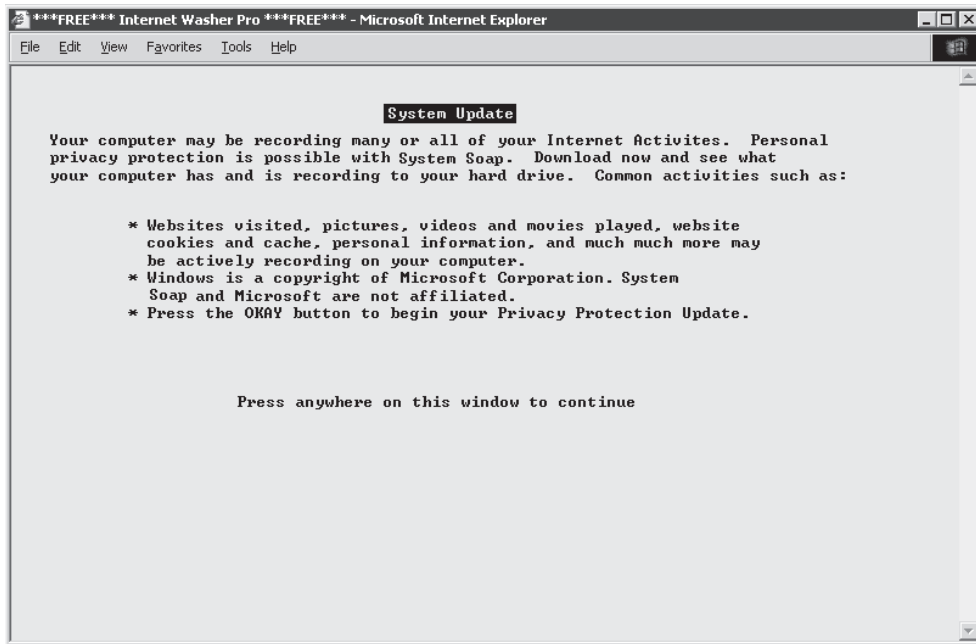


Figure 23-18 A spyware pop-up browser window, disguised as a Windows alert

If you visit a Web site and are prompted to install a third-party application or plug-in that you've never heard of, *don't install it*. Well-known and reputable plug-ins, such as Adobe's *Shockwave* or *Flash*, are safe, but be suspicious of any others. Don't click *anywhere* inside of a pop-up browser window, even if it looks just like a Windows alert window or DOS command-line prompt—as I just mentioned, it's probably fake and the Close button is likely a hyperlink. Instead, use other means to close the window, such as pressing ATL-F4 or right-clicking the browser window's icon on the taskbar and selecting Close.

You can also install spyware detection and removal software on your system and run it regularly. Let's look at how to do that.

Removing Spyware Some spyware makers are reputable enough to include a routine for uninstalling their software. Gator, for instance, makes it fairly easy to get rid of their programs—just use the Windows Add/Remove Programs applet in the Control Panel. Others, however, aren't quite so cooperative. In fact, because spyware is so—well, *sneaky*—it's entirely possible that your system already has some installed that you don't even know about. How do you find out?

Windows comes with Windows Defender, a fine tool for catching most spyware but it's not perfect. The better solution is to back up Windows Defender with a second spyware removal program. There are several on the market, but two that I highly recommend are Lavasoft's Ad-Aware (Figure 23-19) and PepiMK's Spybot Search & Destroy.

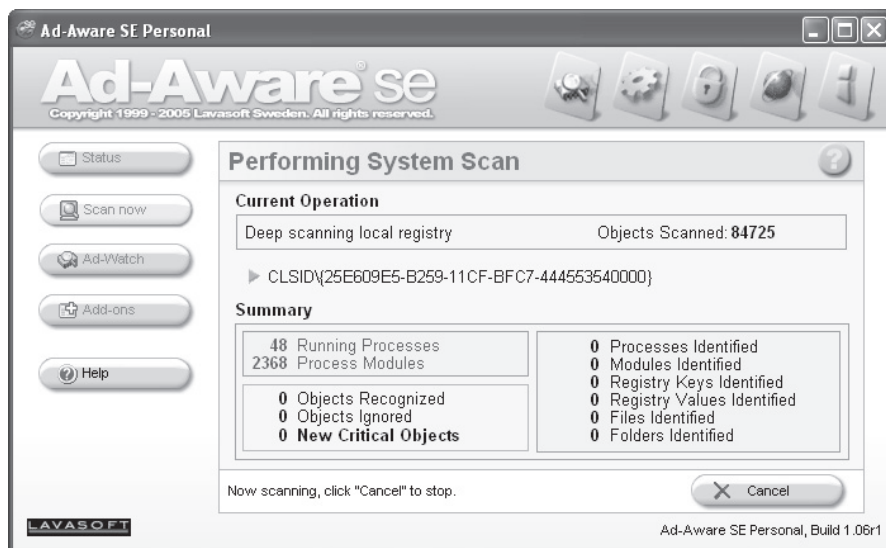


Figure 23-19 Lavasoft's Ad-Aware

Both of these applications work exactly as advertised. They detect and delete spyware of all sorts—hidden files and folders, cookies, registry keys and values, you name it. Ad-Aware is free for personal use, while Spybot Search & Destroy is shareware (Figure 23-20). Many times I've used both programs at the same time because one tends to catch what the other misses.

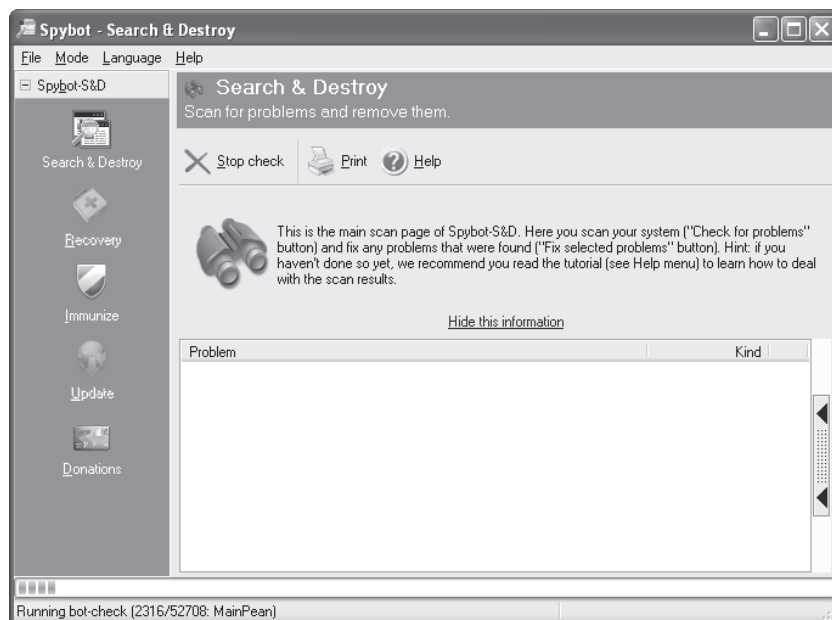


Figure 23-20 Spybot Search & Destroy

Grayware

Some programs, called *grayware*, are not destructive in and of themselves, but they leach bandwidth in networks and can turn a speedy machine into a doddering shell of a modern computer. These programs are called grayware because some people consider them beneficial. They might even be beneficial in the right setting. The primary example of grayware is the highly popular peer-to-peer file sharing programs, such as Bittorrent. Peer-to-peer file sharing programs enable a lot of users to upload portions of files on demand so that other users can download them. By splitting the load to many computers, the overall demand on a single computer is light.

The problem is that if you have a tight network with lots of traffic and suddenly you have a bunch of that bandwidth hogged by uploading and downloading files, then your network performance can degrade badly overall. So, is the grayware bad? Only in some environments. You need to judge each network or computer according to the situation.

Knowledge is Power

The best way to keep from having to deal with malware and grayware is education. It's your job as the IT person to talk to users, especially the ones whose systems you've just spent the last hour cleaning of nasties, about how to avoid these programs. Show them samples of dangerous e-mails they should not open, Web sites to avoid, and the types of programs they should not install and use on the network. Any user who understands the risks of questionable actions on their computers will usually do the right thing and stay away from malware.

Firewalls

Firewalls are an essential tool in the fight against malicious programs on the Internet. Firewalls are devices or software that protect an internal network from unauthorized access to and from the Internet at large. Hardware firewalls protect networks using a number of methods, such as hiding IP addresses and blocking TCP/IP ports. Most SOHO networks use a hardware firewall, such as the Linksys router in Figure 23-21. These devices do a great job.

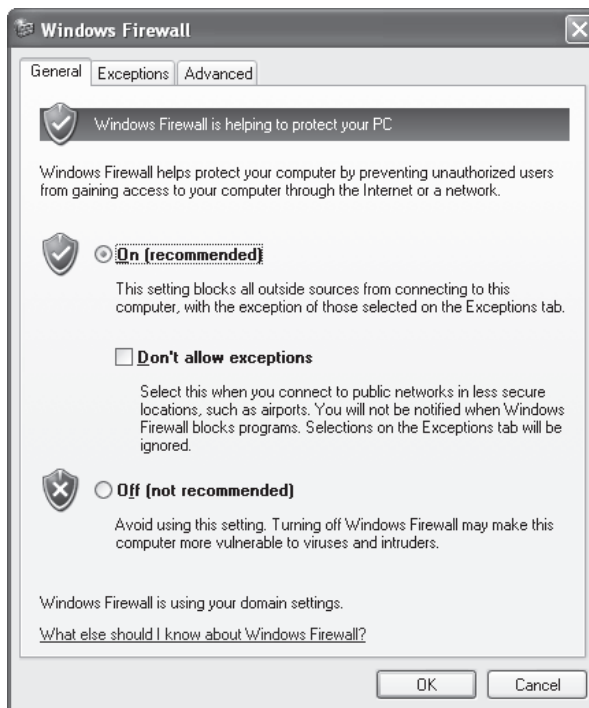
Figure 23-21

Linksys router
as a firewall



Windows XP comes with an excellent software firewall, called the Windows Firewall (Figure 23-22). It can also handle the heavy lifting of port blocking, security logging, and more.

Figure 23-22
Windows Firewall



You can access the Windows Firewall by opening the Windows Firewall applet in the Control Panel. If you're running the Control Panel in Category view, click the Security Center icon (Figure 23-23), and then click the Windows Firewall option in the Windows Security Center dialog box. Figure 23-24 illustrates the Exceptions tab on the Windows Firewall, showing the applications allowed to use the TCP/IP ports on my computer.

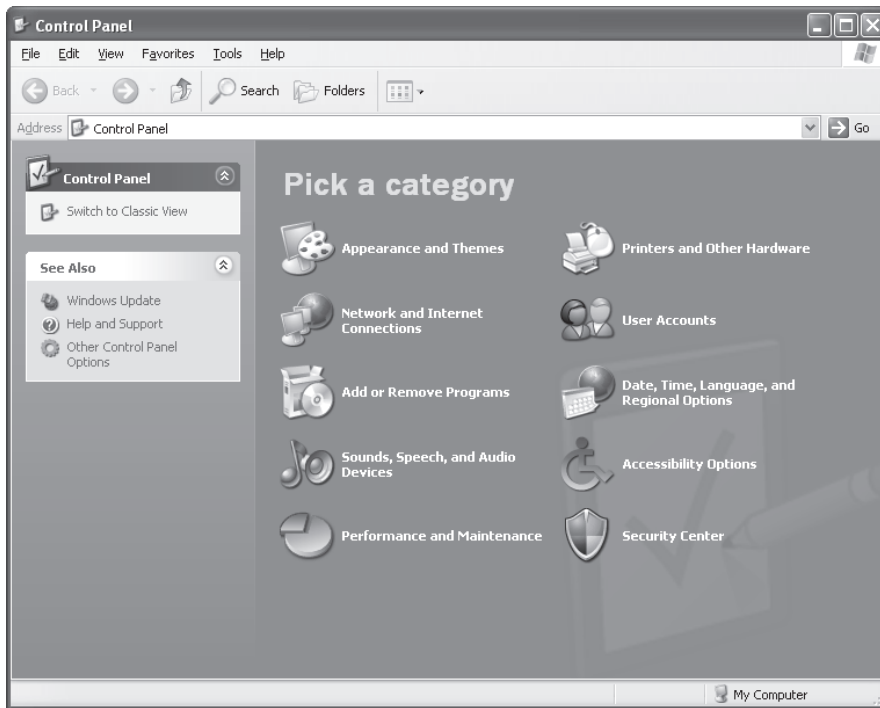
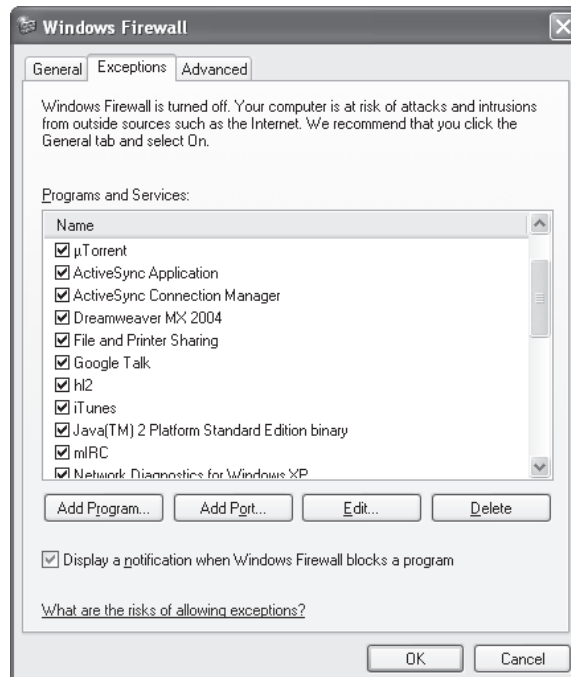


Figure 23-23 Control Panel, Category view

Figure 23-24
Essential programs
(doesn't everyone
need to run
Half-Life 2?)



Encryption

Firewalls do a great job controlling traffic coming into or out of a network from the Internet, but they do nothing to stop interceptor hackers who monitor traffic on the public Internet looking for vulnerabilities. Once a packet is on the Internet itself, anyone with the right equipment can intercept and inspect it. Inspected packets are a cornucopia of passwords, account names, and other tidbits that hackers can use to intrude into your network. Because we can't stop hackers from inspecting these packets, we must turn to *encryption* to make them unreadable.

Network encryption occurs at many different levels and is in no way limited to Internet-based activities. Not only are there many levels of network encryption, but each encryption level provides multiple standards and options, making encryption one of the most complicated of all networking issues. You need to understand where encryption comes into play, what options are available, and what you can use to protect your network.

Network Authentication

Have you ever considered the process that takes place each time a person types in a user name and password to access a network, rather than just a local machine? What happens when this *network* authentication is requested? If you're thinking that when a user types in a user name and password, that information is sent to a server of some sort to be authenticated, you're right—but do you know how the user name and password get to the serving system? That's where encryption becomes important in authentication.

In a local network, encryption is usually handled by the NOS. Because NOS makers usually control software development of both the client and the server, they can create their own proprietary encryptions. However, in today's increasingly interconnected and diverse networking environment, there is a motivation to enable different network operating systems to authenticate any client system from any other NOS. Modern network operating systems such as Windows NT/2000/XP/2003 and NetWare 4.x/5.x/6.x use standard authentication encryptions like MIT's *Kerberos*, enabling multiple brands of servers to authenticate multiple brands of clients. These LAN encryptions are usually transparent and work quite nicely even in mixed networks.

Unfortunately, this uniformity falls away as you begin to add remote access authentications. There are so many different remote access tools, based on UNIX/Linux, Novell NetWare, and Windows serving programs, that most remote access systems have to support a variety of different authentication methods.

PAP *Password Authentication Protocol (PAP)* is the oldest and most basic form of authentication. It's also the least safe, because it sends all passwords in clear text. No NOS uses PAP for a client system's login, but almost all network operating systems that provide remote access service will support PAP for backward compatibility with a host of older programs (like Telnet) that only use PAP.

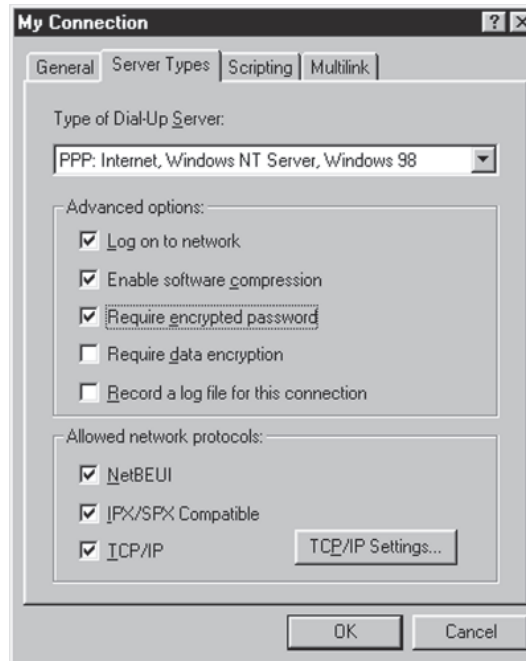
CHAP *Challenge Handshake Authentication Protocol (CHAP)* is the most common remote access protocol. CHAP has the serving system challenge the remote client. A *challenge* is where the host system asks the remote client some secret—usually a password—that the remote client must then respond with for the host to allow the connection.

MS-CHAP *MS-CHAP* is Microsoft's variation of the CHAP protocol. It uses a slightly more advanced encryption protocol.

Configuring Dial-up Encryption

It's the server not the client that controls the choice of dial-up encryption. Microsoft clients can handle a broad selection of authentication encryption methods, including no authentication at all. On the rare occasion when you have to change your client's default encryption settings for a dial-up connection, you'll need to journey deep into the bowels of its properties. Figure 23-25 shows the Windows 2000 dialog box, called Advanced Security Settings, where you configure encryption. The person who controls the server's configuration will tell you which encryption method to select here.

Figure 23-25
Setting dial-up
encryption in the
Windows 2000
Advanced Security
Settings dialog box



Data Encryption

Encryption methods don't stop at the authentication level. There are a number of ways to encrypt network *data* as well. The choice of encryption method is dictated to a large degree by the method used by the communicating systems to connect. Many networks

consist of multiple networks linked together by some sort of private connection, usually some kind of telephone line like ISDN or T1. Microsoft's encryption method of choice for this type of network is called *IPSec* (derived from *IP security*). IPSec provides transparent encryption between the server and the client. IPSec will also work in VPNs, but other encryption methods are more commonly used in those situations.

Application Encryption

When it comes to encryption, even TCP/IP applications can get into the swing of things. The most famous of all application encryptions is Netscape's *Secure Sockets Layer (SSL)* security protocol, which is used to create secure Web sites. Microsoft incorporates SSL into its more far-reaching HTTPS (HTTP over SSL) protocol. These protocols make it possible to create the secure Web sites used to make purchases over the Internet. HTTPS Web sites can be identified by the *HTTPS://* included in their URL (see Figure 23-26).

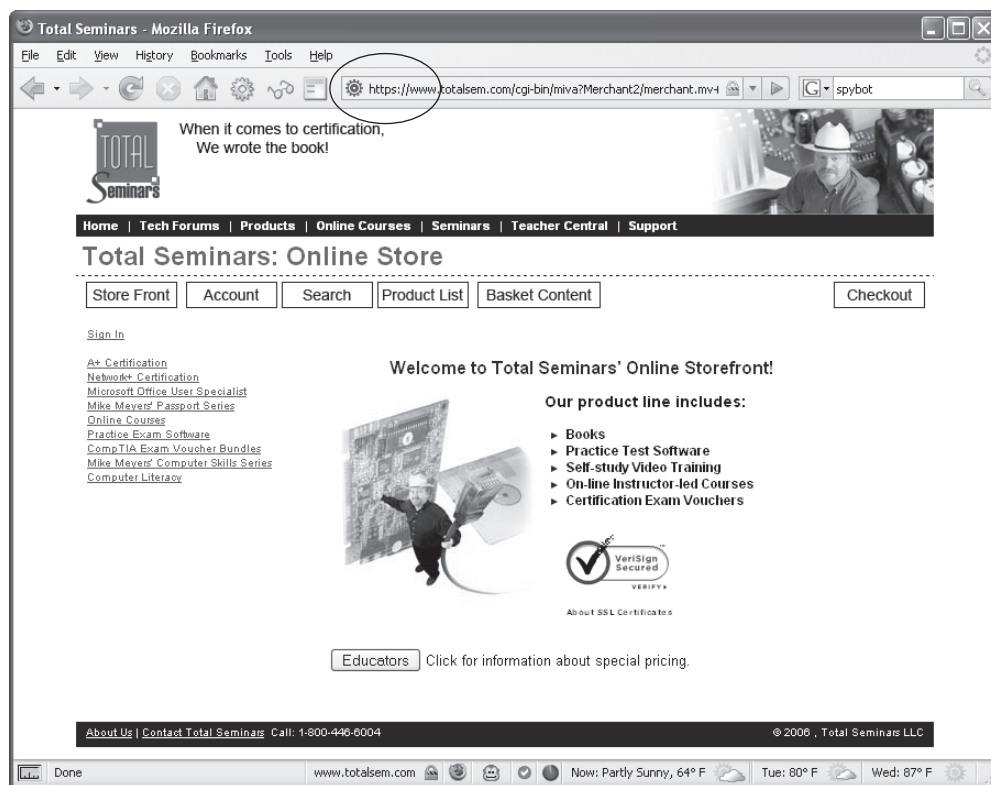


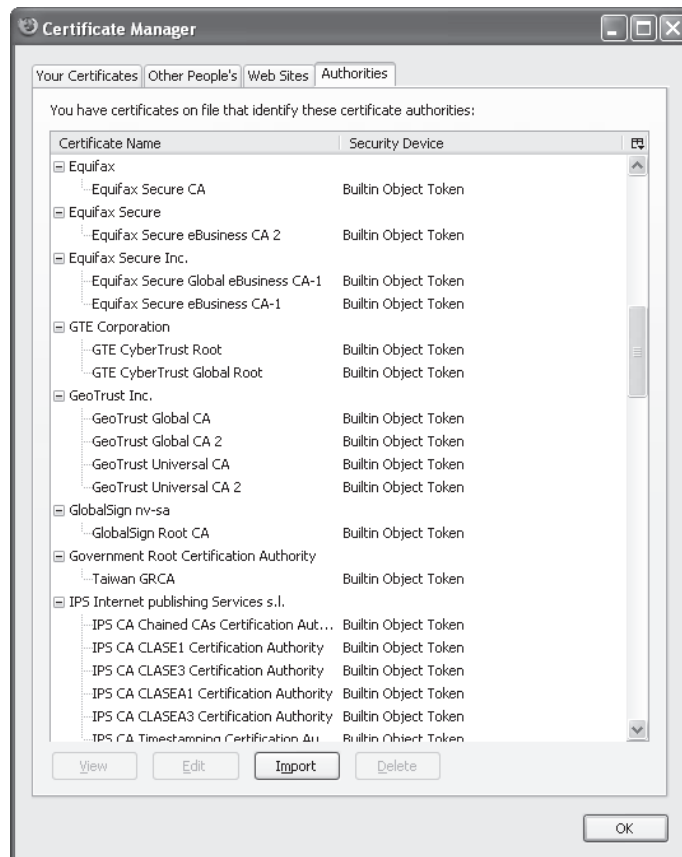
Figure 23-26 A secure Web site

To make a secure connection, your Web browser and the Web server must encrypt their data. That means there must be a way for both the Web server and your browser to encrypt and decrypt each other's data. This is done by the server sending a public key

to your Web browser so the browser knows how to decrypt the incoming data. These public keys are sent in the form of a digital certificate. This certificate not only provides the public key but also is signed by a trusted authority that guarantees the public key you are about to get is actually from the Web server and not from some evil person trying to pretend to be the Web server. There are a number of companies that issue digital certificates to Web sites, probably the most famous is Verisign, Inc.

Your Web browser has a built-in list of trusted authorities. If a certificate comes in from a Web site that uses one of these highly respected companies, you won't see anything happen in your browser; you'll just go to the secure Web page and a small lock will appear in the lower right-hand corner of your browser. Figure 23-27 shows the list of trusted authorities built into the Firefox Web browser.

Figure 23-27
Trusted authorities



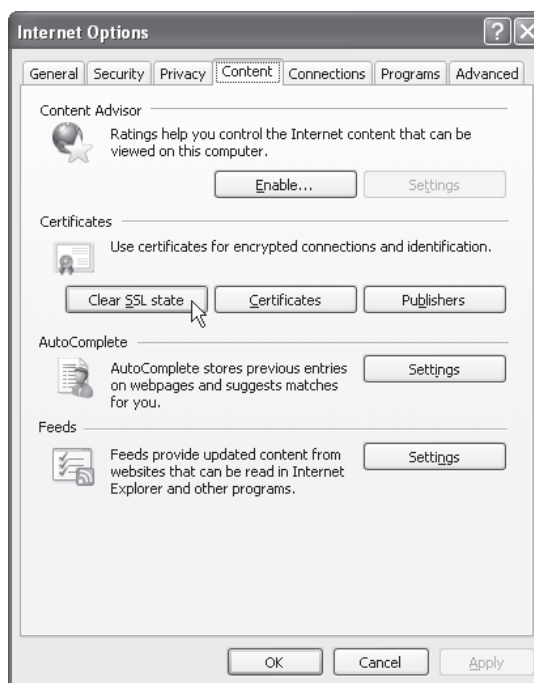
However, if you receive a certificate from someone *not* listed in your browser, the browser will warn you and ask if you wish to accept the certificate, as shown in Figure 23-28.

Figure 23-28
Incoming certificate



What you do here is up to you. Do you wish to trust this certificate? In most cases, you simply say yes, and this certificate is added to your SSL cache of certificates. However, there are occasions where an accepted certificate becomes invalid, usually due to something boring, for instance, it goes out of date or the public key changes. This never happens with the "big name" certificates built into your browser—you'll see this more often when a certificate is used, for example, in-house on a company intranet and the administrator forgets to update their certificates. If a certificate goes bad, your browser issues a warning the next time you visit that site. To clear invalid certificates, you need to clear the SSL cache. The process varies on every browser, but on Internet Explorer, go to the Content tab under Internet Options and click the Clear SSL state button (Figure 23-29).

Figure 23-29
Content tab



Wireless Issues

Wireless networks add a whole level of additional security headaches for techs to face, as you know from Chapter 21, “Local Area Networking.” Some of the points to remember or to go back and look up are as follows:

- Set up wireless encryption, at least WEP but preferably WPA or the more secure WPA2, and configure clients to use them.
- Disable DHCP and require your wireless clients to use a static IP address.
- If you need to use DHCP, only allot enough DHCP addresses to meet the needs of your network to avoid unused wireless connections.
- Change the WAP’s SSID from default and disable SSID broadcast.
- Filter by MAC address to allow only known clients on the network.
- Change the default user name and password. Every hacker has memorized the default user names and passwords.
- Update the firmware as needed.
- If available, make sure the WAP’s firewall settings are turned on.

Reporting

As a final weapon in your security arsenal, you need to report any security issues so a network administrator or technician can take steps to make them go away. You can set up two tools within Windows so that the OS reports problems to you: Event Viewer and Auditing. You can then do your work and report those problems, which is called *incidence reporting*. Let’s take a look.

Event Viewer

Event Viewer is Window’s default tattletale program, spilling the beans about many things that happen on the system. You can find Event Viewer in Administrative Tools in the Control Panel. By default, Event Viewer has three sections, Application, Security, and System, and if you’ve downloaded Internet Explorer 7, you’ll see a fourth option for the browser, Internet Explorer (Figure 23-30). As you’ll recall from Chapter 15, the most common use for Event Viewer is to view application or system errors for troubleshooting (Figure 23-31).

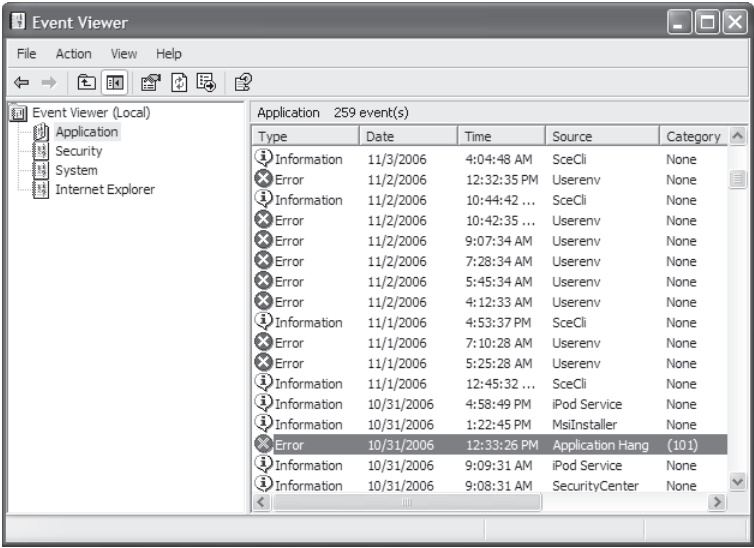


Figure 23-30 Event Viewer

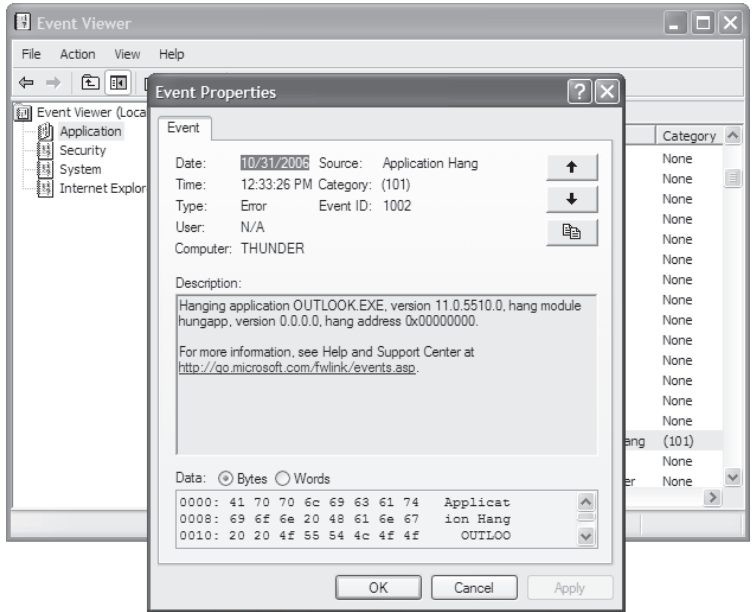


Figure 23-31 Typical application error message

One very cool feature of Event Viewer is that you can click the link to take you to the online Help and Support Center at Microsoft.com, and the software reports your error (Figure 23-32), checks the online database, and comes back with a more or less useful explanation (Figure 23-33).

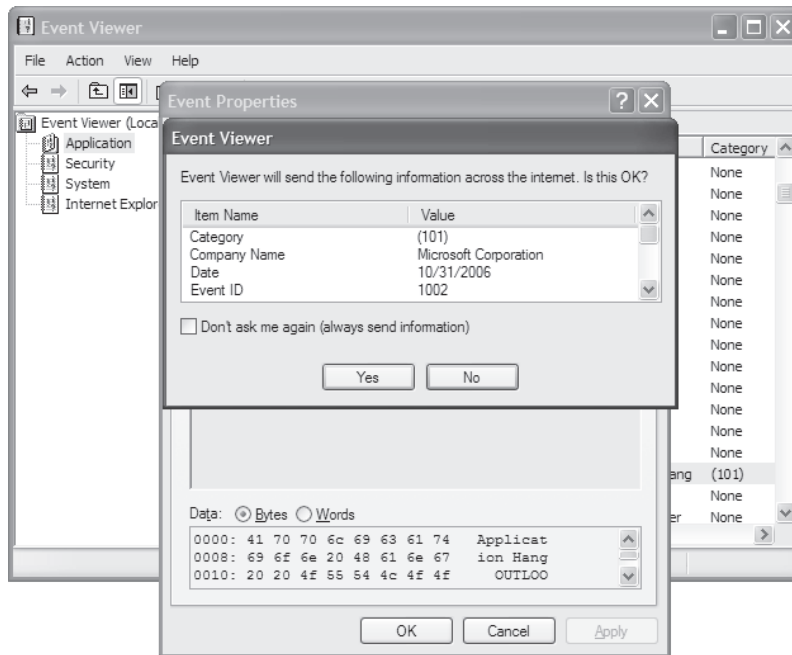


Figure 23-32 Details about to be sent

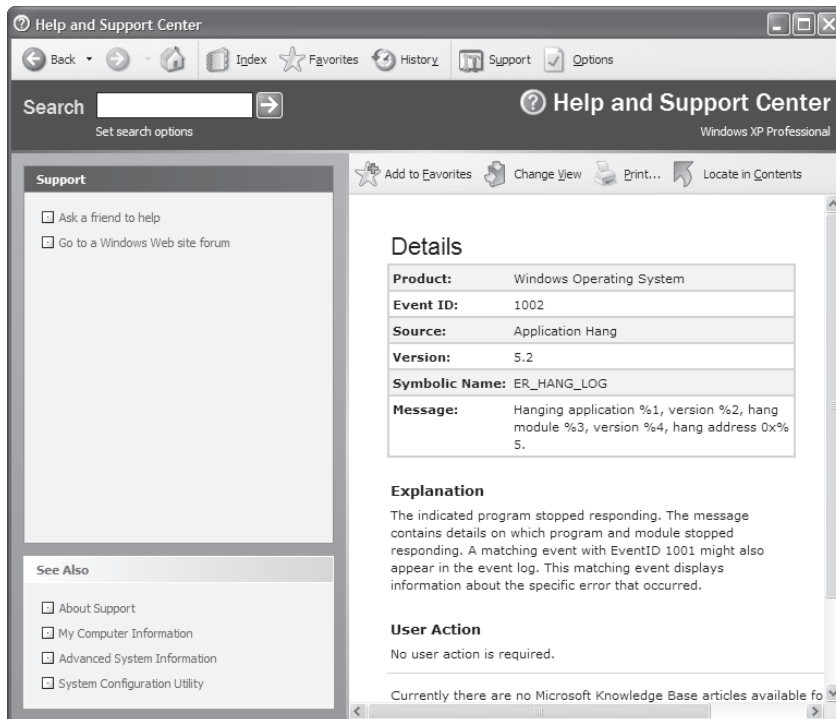


Figure 23-33 Help and Support Center being helpful

Auditing

The Security section of Event Viewer doesn't show you anything by default. To unlock the full potential of Event Viewer, you need to set up auditing. *Auditing* in the security sense means to tell Windows to create an entry in the Security Log when certain events happen, for example, a user logs on—called *event auditing*—or tries to access a certain file or folder—called *object access auditing*. Figure 23-34 shows Event Viewer tracking logon and logoff events.

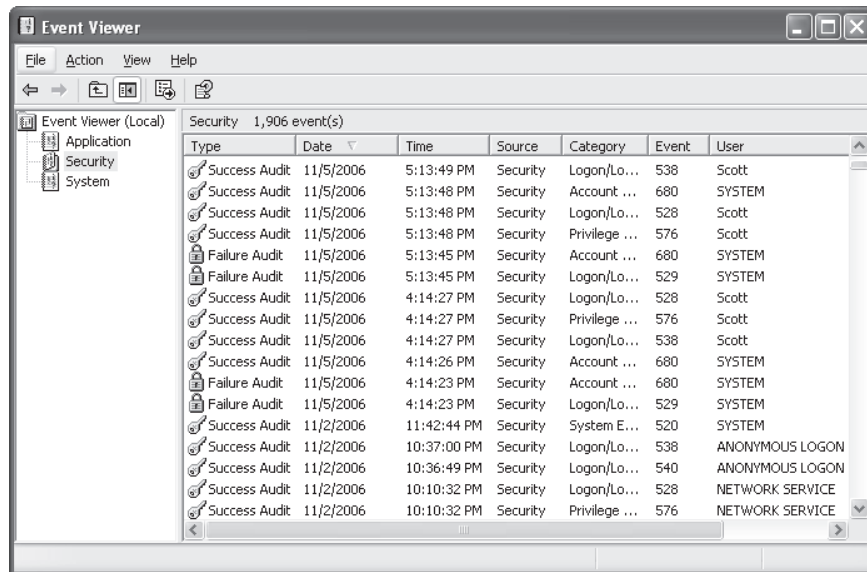


Figure 23-34 Event Viewer displaying security alerts

The CompTIA A+ certification exams don't test you on creating a brilliant auditing policy for your office—that's what network administrators do. You simply need to know what auditing does and how to turn it on or off so that you can provide support for the network administrators in the field. To turn on auditing at a local level, go to Local Security Settings in Administrative Tools. Select Local Policies and then click Audit Policies. Double-click one of the policy options and select one or both of the check boxes. Figure 23-35 shows the Audit object access dialog box.

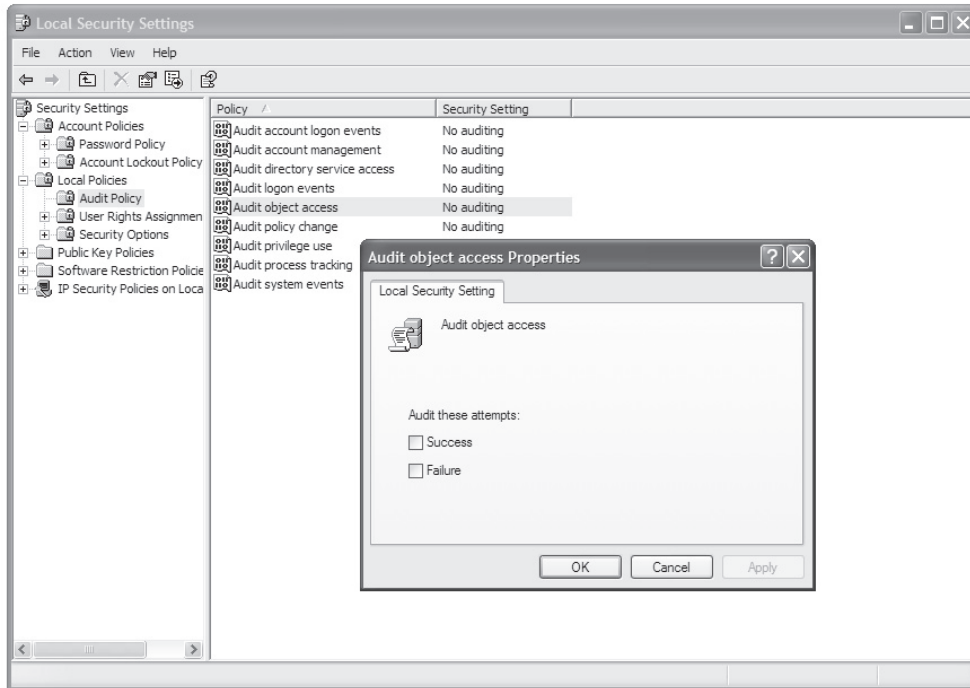


Figure 23-35 Audit object access with the Local Security Settings dialog box open in the foreground

Incidence Reporting

Once you've gathered data about a particular system or you've dealt with a computer or network problem, you need to complete the mission by telling your supervisor. This is called *incidence reporting*. Many companies have pre-made forms that you simply fill out and submit. Other places are less formal. Regardless, you need to do this!

Incidence reporting does a couple of things for you. First, it provides a record of work you've done and accomplished. Second, it provides a piece of information that, when combined with other information that you might or might not know, reveals a pattern or bigger problem to someone higher up the chain. A seemingly innocuous security audit report, for example, might match other such events in numerous places in the building at the same time and thus show conscious, coordinated action rather than a glitch was at work.

Chapter Review Questions

1. Which of the following would you select if you need to back up an Active Directory server?
 - A. Registry
 - B. System state data
 - C. My Computer
 - D. My Server
2. Johan migrated his server data to a bigger, faster hard drive. At the end of the process, he partitioned and formatted the older hard drive before removing it to donate to charity. How secure is his company's data?
 - A. Completely secured. The drive is blank after partitioning and formatting.
 - B. Mostly secured. Only super skilled professionals have the tools to recover data after partitioning and formatting.
 - C. Very unsecured. Simple software tools can recover a lot of data, even after partitioning and formatting.
 - D. Completely unsecured. The data on the drive will show up in the Recycle Bin as soon as someone installs it on a system.
3. What is the process of using or manipulating people to gain access to network resources?
 - A. Cracking
 - B. Hacking
 - C. Network engineering
 - D. Social engineering
4. Which of the following might offer good hardware authentication?
 - A. Strong passwords
 - B. Encrypted passwords
 - C. NTFS
 - D. Smart cards
5. Randall needs to change the file system on his second hard drive (currently the D: drive) from FAT32 to NTFS. Which of the following commands would do the trick?
 - A. `CONVERT D: /FS:NTFS`
 - B. `CONVERT D: NTFS`
 - C. `CONVERT /FS:NTFS D:`
 - D. `CONVERT NTFS D:`

6. Which of the following tools would enable you to stop a user from logging on to a local machine, but still enable him to log on to the domain?
 - A. AD Policy
 - B. Group Policy
 - C. Local Security Settings
 - D. User Settings
7. Which type of encryption offers the most security?
 - A. MS-CHAP
 - B. PAP
 - C. POP3
 - D. SMTP
8. Zander downloaded a game off the Internet and installed it, but as soon as he started to play he got a blue screen of death. Upon rebooting, he discovered that his My Documents folder had been erased. What happened?
 - A. He installed spyware.
 - B. He installed a Trojan.
 - C. He broke the Group Policy.
 - D. He broke the Local Security Settings.
9. Which of the following should Mary set up on her Wi-Fi router to make it the most secure?
 - A. NTFS
 - B. WEP
 - C. WPA
 - D. WPA2
10. What tool would you use to enable auditing on a local level?
 - A. AD Policy
 - B. Group Policy
 - C. Local Security Settings
 - D. User Settings

Answers

1. B. Backing up the system state data gets the Registry, Active Directory files, and more.
2. C. Although it would take a little work, simple software tools can recover a lot of data, even after partitioning and formatting.

3. D. Social engineering is the process of using or manipulating people to gain access to network resources.
4. D. Smart cards are an example of hardware authentication devices.
5. A. Use the following command to convert from FAT32 to NTFS:
CONVERT D: /FS:NTFS
6. C. Local Security Settings enable you stop someone from logging on to a local machine.
7. A. Of the choices here, MS-CHAP offers the most security.
8. B. Zander clearly installed a Trojan, a virus masquerading as a game.
9. D. Mary should set up WPA2 on her Wi-Fi router.
10. C. You can enable local auditing through Local Security Settings.