Realtime publishers
"Leading the Conversation"

The Definitive Guide™ To

Information Theft Prevention

sponsored by

Dan Sullivan

Chapter 6: Protecting Information Use on Managed Devices 109
Types of Client Devices and Varying Security Needs..109
Desktops: The Easiest Case 109
Authentication...110
Access Controls 112
Auditing 113
Patch Management..114
Configuration Management 115
Laptops: Things Get Challenging 115
Laptop Vulnerabilities 116
Secure Communications 117
Encrypted Storage...117
Anti-Malware..118
Mobile Devices: They're Manageable? 118
New Acquisition Model..118
Something Old and Something New...119
Securing Client Devices...121
Configuring Authentication 121
Defining Authorizations..122
Configuring Update Procedures..123
Install and Configure Antivirus Software 123
Install and Configure Anti-Spyware Software..124
Install and Configure a Personal Firewall..125
Schedule Vulnerability Scanning...126
Securing an Intranet 129
Content Filtering 129
Intrusion Prevention..129
Summary 129

Copyright Statement

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimepublishers can be found at http://nexus.realtimepublishers.com.]

Chapter 6: Protecting Information Use on Managed Devices

By definition, managed devices are under the control of IT management, and security and systems management professionals have many options at their disposal for preventing information theft. Previous chapters have described methods for protecting information during transmission and when in use on unmanaged devices. This chapter will examine the varying security needs within a managed perimeter. The topics will include:

- The nature of different client devices and their security requirements
- The security needs of servers and applications
- Securing network infrastructure

Throughout, the chapter will examine common threats to protecting the confidentiality and integrity of information and countermeasures to those threats.

Types of Client Devices and Varying Security Needs

Prior to the widespread adoption of personal computing and client/server application models, applications typically ran on mainframe or mini computers with large numbers of dedicated terminals for user and administrator access. There was no concept of protecting the “client” that was different from protecting the “server” (with the possible exception of administrator consoles, which had privileged access and were typically locked in computer rooms with the mainframe or mini computer). Client devices have changed significantly since the advent of client/server computing.

Network administrators, systems managers, and application developers are now contending with at least three broad types of clients:

- Desktop devices
- Laptops
- Mobile devices

These all share many common functions but each has a distinct set of characteristics that require some device-specific types of security management.

Desktops: The Easiest Case

In many cases, desktop devices are the easiest clients to maintain. They are more or less permanently connected to an organization’s network, most are configured with a standard operating system (OS—for example, Windows XP) or at least a standard family of OS (for example, Windows), and most will run a similar array of desktop applications. Of course, there are some variations across the organization. Not all users will need data warehouse reporting tools or statistical analysis packages or other specialized software; however, most will be using browsers, word processors, spreadsheets, and related productivity applications (see Figure 6.1).

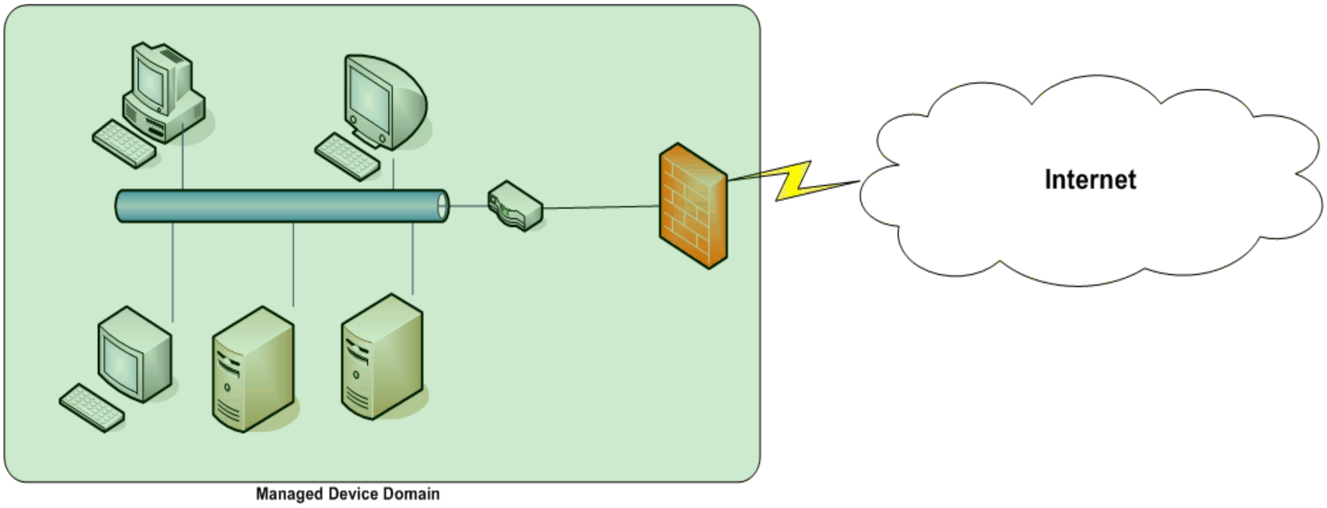


Figure 6.1: A managed device domain without laptop or mobile devices is the least challenging security environment in a typical IT organization.

Even within the relatively constrained variations of desktop devices, there are several types of systems management and security measures that must be implemented to prevent information theft:

- Authentication
- Access controls
- Auditing
- Patch management
- Configuration management

These apply to other types of clients as well. Desktops typically represent the least common denominator with regards to security measures across client types.

Authentication

Authentication is the process of verifying that a user is who he or she claims to be. Most authentication systems use passwords; systems and applications with greater security requirements use biometrics, smart cards, or a combination of authentication methods (see the sidebar, “Advanced Authentication Methods”).

The centralized model of one logon to a mainframe has given way to multiple authentication mechanisms in client/server and Web-based application models. For example, a user may need to log into a Windows network to access her desktop and shared directories on a file server. She might also need to authenticate to a financial management application that uses a client/server front end and an Oracle database. When she wants to check the status of her sales accounts in an online customer relationship management tool, such as SalesForce.com, she needs to log in again. The proliferation in separate authentication schemes prompted the use of centralized authentication and identity management systems.

Directories, such as ActiveX and Lightweight Directory Access Protocol (LDAP) directories, provide a centralized repository for user information that can be used by multiple applications (see Figure 6.2). In addition to storing typical directory information, they can store information about a person's role within an organization. For example, someone in the sales department may be granted read and write access to that department's shared network drive, but only members of that department that also have the role "Manager" associated with their name can access the management reporting system.

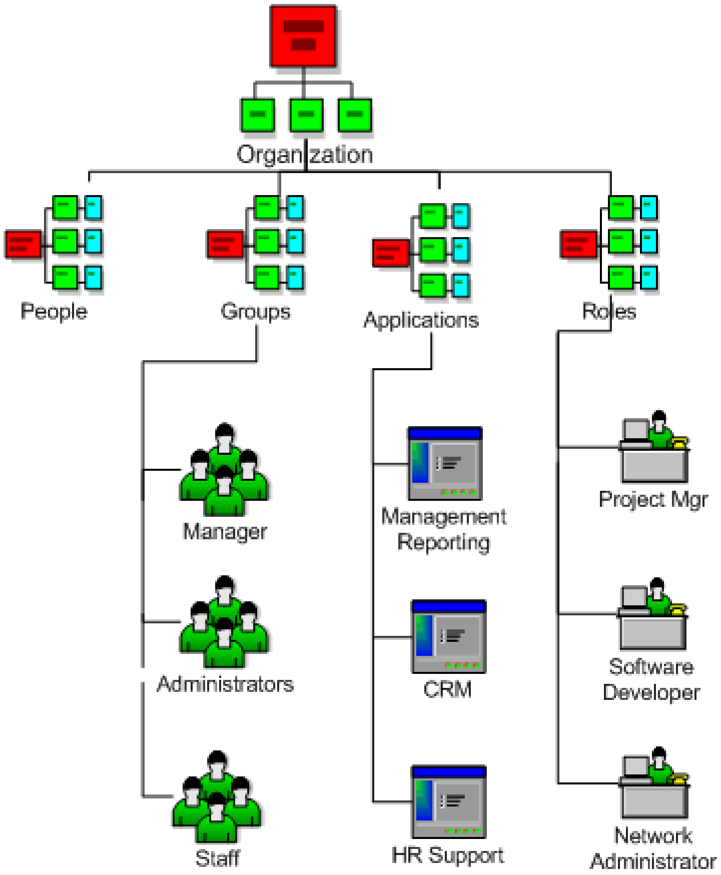


Figure 6.2: LDAP directories maintain information about users, groups, and roles that might be used for authentication and authorization.

Authentication is closely related to authorization, or what a user is allowed to do. Access controls enforce the authorizations granted to a user.

Advanced Authentication Methods

Although widely used for their ease and low cost, passwords are a relatively poor authentication method. Passwords may be cracked by dictionary attacks, guessing, or poor security practices on the part of the users. A wealth of methods and technologies are now available, including biometric systems such as:

- Fingerprint scanners that use the unique characteristics of ridge endings and bifurcations of ridges in fingerprints to identify users
- Palm scanners that use variations in creases, ridges, and grooves of palms
- Hand geometry techniques depend upon the shape of a user's hand and finger
- Retina scans distinguish users based on blood vessel patterns on the retina
- Iris scans use distinctive patterns of rifts, rings, colors, and furrows in a person's iris
- Signature dynamics examine the rate and manner in which someone signs their name
- Keyboard dynamics are similar to signature dynamics in that the rate and manner of typing can distinguish a user
- Voice prints use differences in people's speech sounds to identify users

In addition to biometrics, other options to traditional passwords include:

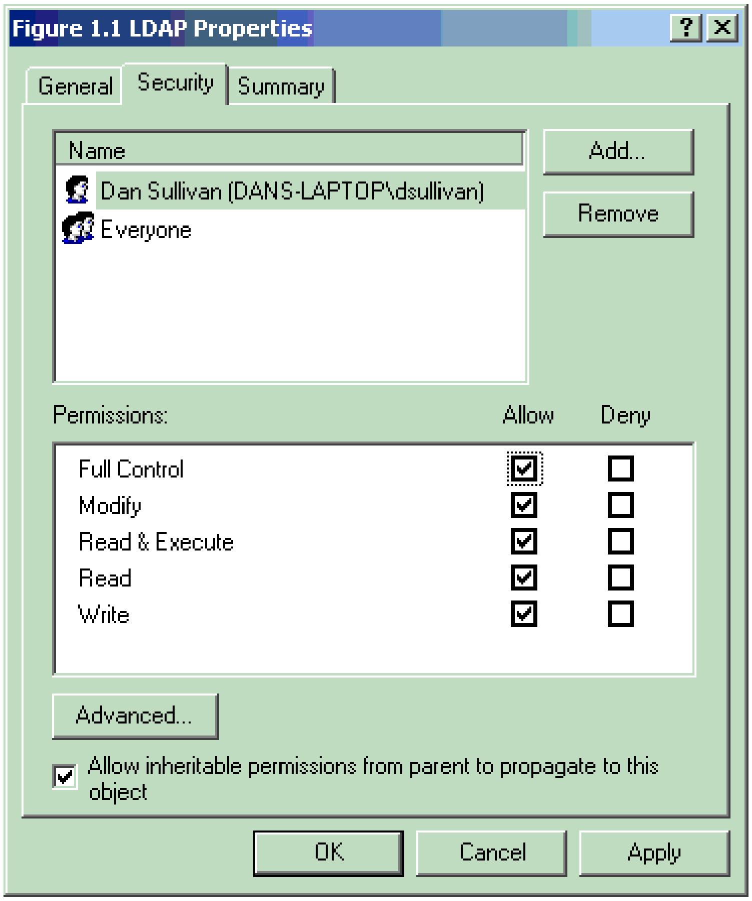
- Token devices that generate passwords entered by the user; the device is synchronized with a counterpart on the server
- Cryptographic keys used to create digital signatures
- Smart cards and memory cards that store a user's identification and authentication data

When two or more of these methods are used together, it is referred to as multi-factor authentication. Usually two-factor authentication combines different types of authentication methods, such as authenticating by something you know (for example, a password), something you are (for example, a retina scan), and something you have (for example, a smart card).

Access Controls

Access controls are mechanisms for controlling which operations a user may perform on an object. Like authentication, access controls have become more distributed along with client/server and Web-based applications.

Access controls apply to objects that are stored on a desktop device as well as objects that are accessible from the machine (see Figure 6.3). One of the key steps to preventing information theft is ensuring that users have access only to the information they need and that the operations they can perform on objects is the minimal set of operations they need to perform their duties. For example, a finance department staff member who must enter accounts receivables data should not have read or write access to the accounts payable data. Similarly, an analyst may have read access to a database of customer information but there is no reason that person should have update privileges to the same data.



Name

- Dan Sullivan (DANS-LAPTOP\dsullivan)
- Everyone

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
Read	☑	□
Write	☑	□

☑ Allow inheritable permissions from parent to propagate to this object

Figure 6.3: Access controls determine which operations a user may perform on an object.

Authentication and authorizations work together to restrict access to information; however, assessing whether the proper access controls are actually in place and enforced requires an auditing process.

Auditing

Auditing is the process of collecting and analyzing information on system activities. Events such as failed login attempts, attempted read operations on a file server to which the user does not have access, and the deletion of data in a database may all warrant review in some circumstances.

OSs and many enterprise applications provide excellent logging information on events within the system. The trick for application and systems administrators is to balance the need for details with the need to control the volume of data generated by logging facilities. Too much data makes information inaccessible and too little data can cause administrators to miss significant events. This problem is often managed with applications that monitor log files and notify administrators of high-priority events or when a threshold number of events of a particular type occur. In addition to implementing and enforcing adequate access controls, systems manager are responsible for ensuring applications and OSs are kept up to date.

Patch Management

Patch management is the process of updating software to correct bugs and vulnerabilities. Once again, the decentralization of today's applications adds a dimension of difficulty that has not existed in the past. Take OSs, for example. Windows may be the standard OS in an organization, but there may be several versions of Windows in use. Most desktops, for example, might run Windows XP, servers run Windows Server 2003 (WS2K3), and some older desktops run Windows 2000 (Win2K). When a patch is released, the standard procedure is to:

- Assess the value of the patch—What does the patch correct? Is that function in use?
- If the patch is relevant, test it in a controlled environment with representative configurations
- If the patch test is successful, deploy the patch and retain a copy of the patch in the definitive software library
- If the patch test is unsuccessful, systems administrators and managers will have to weigh the costs and benefits—Was the patch partially successful? Does the functionality disrupted by the patch outweigh the gains made by installing the patch? Are there workarounds for the problem?

Of course, methodical analysis might be a luxury you cannot afford if you are patching in response to a fast-moving threat, such as the SQL Slammer worm. Another aspect of desktop device management that influences the ability to prevent information theft is configuration management.

✎ Keeping up with patches and vulnerabilities is a challenging task. Software vendors often provide patch and vulnerability reports. Resources available for systems managers and applications administrators, include:

Microsoft Security Updates available at http://www.microsoft.com/athome/security/update/bulletins/default.mspx

National Vulnerability Database available at http://nvd.nist.gov/

Open Source Vulnerability Database available at http://www.osvdb.org/

Configuration Management

Configuration management is the practice of controlling the parameters that specify how a piece of software will function. This is especially important when dealing with servers and network devices that must take into account multiple dependencies from throughout the infrastructure, but the principles are relevant to desktop device management as well. Configuration management includes:

- Defining configuration items, such as hardware and software items
- Recording and reporting on the status of the settings of those items
- Managing change requests to modify configuration items
- Verifying and auditing configurations

Configuration management, along with patch management, helps to maintain the confidentiality of information on a device and the availability of the system after it has been initially secured.

Protecting desktop devices against information theft requires fundamental practices that apply across the IT infrastructure. In many ways, desktop devices are some of the easiest to secure. They usually do not run complex network applications, such as relational databases or application servers, which, because of their complexity, are prone to vulnerabilities. They tend to remain connected to the enterprise network and so protected by the perimeter defenses and other countermeasures deployed on the network. Other devices, such as laptops, personal digital assistants (PDAs), and smart phones are not always as well protected.

> 📖 Best practices in systems management are well developed; there is no need to reinvent the wheel. For more information about the topics discussed in this section, see the references on the IT Information Infrastructure Library (ITIL) such as ITIL Web site at http://www.itil.co.uk/ and Anil Desai and Don Jones' *The Reference Guide to Data Center Automation* at http://nexus.realtimepublishers.com/previews/RGDCA_vol1.htm.

Laptops: Things Get Challenging

Many of us live with our laptops. They are in our offices, our homes, our cars—some of us can't even leave them when we are on vacation. They allow us great flexibility and allow us to be productive where we want and when we want. In many ways, laptops were the first device to liberate many employees, contractors, and consultants from the tether of centralized offices.

With regard to laptops, there are several additional topics that must be addressed by systems managers in addition to those listed for desktop devices:

- Laptop-specific vulnerabilities
- The need for secure communications on potentially insecure networks
- The need for encryption of data stored on disk
- Local anti-malware protection

As is so often the case, their greatest advantages can also be their greatest disadvantage.

Laptop Vulnerabilities

Consider a few incidents involving laptops:

- A laptop from the University of California Berkeley in March 2005 exposes personal information about 98,400 people.
- In April 2005, a laptop belonging to MCI is stolen along with 16,500 personal names in Virginia.
- In June 2005, an Eastman Kodak laptop with personal information about 5800 individuals is stolen.
- In June 2005, a Bank of America laptop with personal information about 18,000 people is stolen.
- In November 2005, a Boeing laptop is stolen with information about 161,000 individuals; it contained Human Resources data, including Social Security numbers and bank account information.
- In February 2006, a laptop of an Ernst and Young employee is stolen from a car; the laptop contained personal information, including Social Security numbers, about 38,000 employees of BP in addition to Sun, Cisco, and IBM employees.

📖 The source of these statistics is the Privacy Rights Clearinghouse; more information is available at http://www.privacyrights.org/ar/ChronDataBreaches.htm. This is only a selection of the incidents listed; there are too many to include here.

Of course, these examples pale in comparison to the large-scale breach at the U.S. Veterans Administration (VA) in May 2006. A laptop with personal information about 26.5 million veterans and some of their spouses was stolen from an employee's home during a burglary. The employee had taken the data home in violation of VA policies.

📖 More information about the VA breach is available at http://www1.va.gov/opa/data/data.asp and http://www.firstgov.gov/veteransinfo.shtml.

All of a sudden, laptops do not sound so appealing. Actually, there are reasonable measures you can take to secure data on laptops so that you maintain the convenience of portable devices. You just need to keep in mind two facts about laptops that do not generally apply to desktop devices and servers. First, they are not always protected by perimeter defenses. You can unplug them and walk across the street to a coffee shop with a wireless hotspot and keep working. In that case, you are no longer behind the firewall, protected by content-filtering systems on the network, or receiving network traffic analyzed by an intrusion protection system. (Unless you route all traffic through a virtual private network—VPN—to the corporate network, but that does not eliminate all vulnerabilities.) Second, laptops are easily moved as seen in the litany of laptop thefts just listed. These conditions require countermeasures to prevent information theft.

Secure Communications

Communications from a laptop that is not connected to an organization's secure network can be compromised. When a wireless network is used, the signals themselves can be easily detected and monitored if they are not encrypted.

At first, you might think "Who would bother scanning an area in the hopes of finding interesting information? After all what are the chances?" On average, the chance may be poor, but in select areas, the likelihood of finding confidential information increases. Consider an airport waiting area or a coffee shop in the business district of a major city. How many managers, executives, and consultants are working in those areas with wireless communications?

Then again, if a thief does not have the electronics equipment to monitor wireless transmissions, he or she could just get the information the old fashioned way—by stealing the computer.

📖 For more information about secure communications, see Chapter 4.

Encrypted Storage

This section began with examples of information that was compromised because it was on a stolen laptop. Those of us who use laptops should assume that if our laptop is stolen, any unencrypted information on it will be disclosed. The options then are to only keep information we would want disclosed publicly kept on the laptop or we encrypt it.

Automatic encryption of data stored on hard drives can significantly increase the security of laptops. A number of commercially available software products are available with varying features, including:

- Full disk encryption of every sector of data or selected encryption of some folders and files
- Integration with centralized authentication mechanism, such as Active Directory (AD)
- Pre-boot authentication
- Support for advanced authentication mechanisms, such as smart cards

In addition, disk drive manufacturers are providing hardware-based solutions that are OS independent. They do not require additional software installations.

Software encryption does have some drawbacks. The initial encryption phase can be time consuming and some maintenance operations, such as recovering from bad sectors, can be more difficult than on non-encrypted drives.

📖 For data and disk encryption vendors, see http://dir.yahoo.com/Business_and_Economy/Business_to_Business/Computers/Security_and_Encryption/Software/.

Besides keeping data safe from laptop thieves, laptop users should keep their systems safe from malicious software.

Anti-Malware

When laptops connect to networks, laptops are protected by the security measures deployed on that network but they are also subject to the threats on that network. A seemingly safe network, like a home network, can be a host for multiple forms of malware. Consider online activities popular with teenagers: downloading music, instant messaging (IM), and browsing. Some of the by-products of these activities include:

- Unintentional downloading of malware. Trojan horses and spyware that are embedded in file-sharing programs; for example Kazaa, a popular peer-to-peer application, has carried spyware.
- Introduction of malware through IM clients. IM is now used as a vector by malware developers. For example, Kelvir, an IM worm, displayed a message during IM conversations and lured readers to click a link that downloaded a Trojan horse and infected their machines.
- Drive-by-downloads, software that is downloaded without users' knowledge or intervention, triggered by browsing to a site programmed for drive-by-downloads.

> 📖 See Mark H. Walker's "Drive-by Downloads: Stealthy Downloads and Internet Explorer's New Defense Against Them" at http://www.microsoft.com/windows/ie/community/columns/driveby.mspx.

If one is not careful (and sometimes even if one is) malware can spread from one device on the network to another. Up-to-date antivirus and anti-spyware tools should be deployed on all laptops. Laptops present more security challenges than desktops; mobile devices, such as smart phones, are bringing additional security challenges to IT departments.

Mobile Devices: They're Manageable?

Mobile devices have introduced a new set of management and security challenges in IT. Both the way these devices work their way into the organization and the vulnerabilities they bring with them are distinctly different from their predecessors.

New Acquisition Model

Unlike desktops and servers, which are usually introduced to an organization through the IT department, mobile devices are driven by grass roots adoption. PDAs and mobile email devices, such as RIM's Blackberry, often come in "under the radar" of IT management. Executives, managers, sales staff, and road warriors throughout an organization may be using these devices before reaching a critical mass, requiring IT to formulate policies governing their use.

If IT professionals are not careful, these devices could quickly come on the radar. If a wireless device user inadvertently becomes the conduit for introducing malware to the corporate network or a wireless device is hacked and allows thieves to download confidential information, mobile devices will have the attention of executive management as well as IT. This kind of rapid rise to a critical management concern is not always due to technical problems.

Research in Motion Ltd. (RIM), the maker of Blackberry mobile email devices, was sued for patent infringement; when the case was not quickly resolved and there was concern about a possible shutdown of the Blackberry service, many IT departments were expected to come up with a backup plan. In the minds of users, it does not matter how or why a particular type of device has woven itself into the fabric of the IT infrastructure; once it is there, it is the IT department’s responsibility. With that in mind, it is time to examine some of the similarities and differences between mobile device and other IT asset security.

Something Old and Something New

There are both similarities and differences between mobile devices and other IT equipment. Like other devices, mobile ones are:

- The target of viruses, worms, and other malware—The Palm OS/LibertyCrack Trojan, for example, appears to be a game that can be downloaded to PDAs but is actually a program that deletes other applications on the device
- In need of updates and patches to protect against vulnerabilities
- Store information that can be stolen in a number of ways, such as network monitoring or theft of the device
- Connect to corporate networks and could potentially put other devices and information at risk

These similarities make it clear that mobile devices require the same types of policy-driven procedures and controls to manage the risks associated with them. However, difference between mobile and other devices can make this difficult. Some of the most salient differences are:

- Mobile devices are often owned by employees, limiting the level of control IT can have over the devices; however, IT can, and should, define minimum security standards for any device accessing organizational resources.
- Mobile devices use a different class of OS and applications. Mobile Windows may share functionality with other Windows OSs, but it is different enough that policies and procedures should be adapted to it.
- Small mobile devices, such as PDAs and smart phones, are more likely to be lost (and possibly stolen) than desktops and laptops. Policies should clearly define what confidential data can be downloaded to such devices.

Mobile device vendors are aware of some of the potential problems and have responded with features such as built-in encryption and remote disabling of a device.

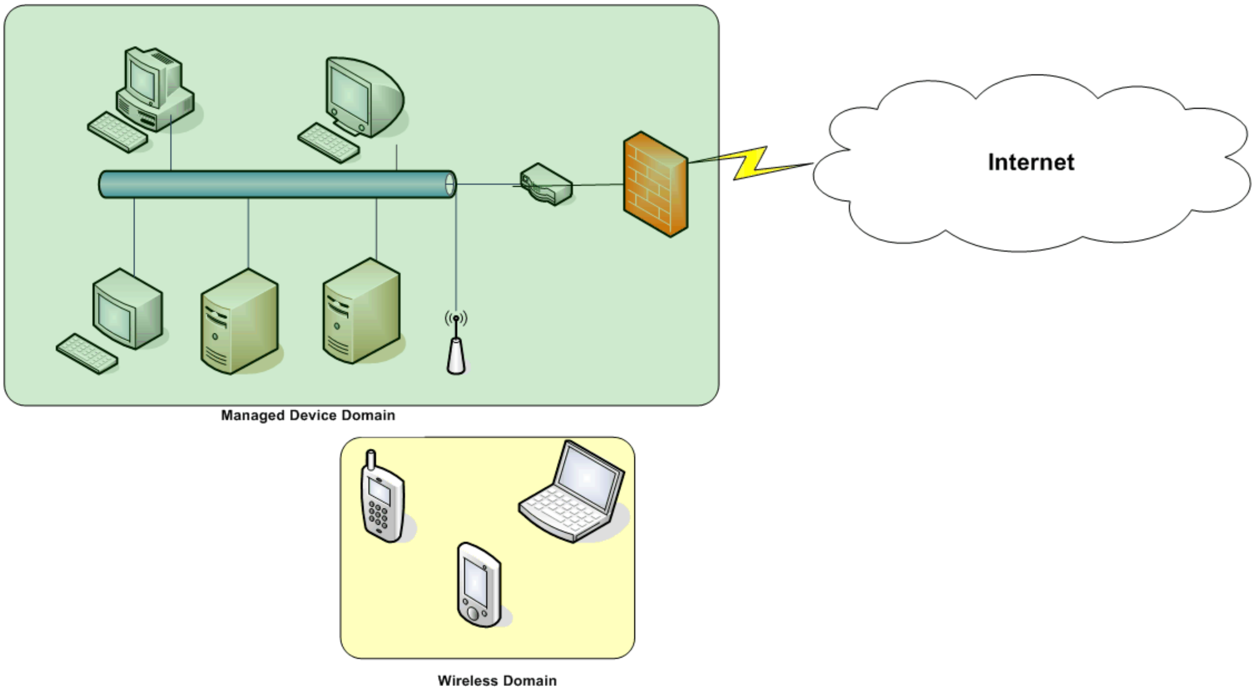


Figure 6.4: The addition of mobile wireless devices introduces new vulnerabilities into an IT infrastructure.

At the least, security policies governing mobile devices should address the following areas:

- Guidelines for determining when a personal mobile device is considered a managed asset—for example, any mobile device that exchanges data with a managed network device is governed by corporate policies
- The use of authentication mechanisms, such as username and password, to gain access to data and applications
- The use of strong encryption for data stored on the device
- Specifications on when to use secure communications protocols, such as SSL
- The use of unique device identification
- The need for remote disabling features if confidential information is stored on the device

> For more information about mobile device security on devices running Windows OSs, see Microsoft's "Windows Mobile-Based Devices and Security White Paper" at http://www.microsoft.com/windowsmobile/business/strategy/security.mspx. For details about PalmOS security, see http://www.palmsource.com/enterprise/security.html. For a summary of security features on these and other mobile device OSs, see Mark Komisky's "Mobile Device Security II: Handheld Operating Systems" at http://www.pdastreet.com/articles/2006/6/2006-6-1-Mobile-Device-Security.html.

Managed client devices—whether a desktop machine, a laptop, or one of several types of mobile devices—require a number of security measures to protect information from theft and improper disclosure. This section has described some of the common and device-specific security needs of managed client devices. The following section will look into some of the technologies that can meet those needs and discuss best practices for implementing and managing them.

Securing Client Devices

Securing client devices is a multi-step process that includes both the deployment of security countermeasures and the proper configuration of the devices. The following checklist includes the basic steps:

- □ Configure authentication mechanism
- □ Define authorizations
- □ Define update procedures
- □ Install and configure antivirus software
- □ Install and configure anti-spyware software
- □ Install and configure personal firewall
- □ Add device to vulnerability scanning schedule

The following discussion uses examples from Microsoft Windows clients, but the principles are generally applicable.

Configuring Authentication

Configuring authentication on a client device generally involves multiple steps because devices tend to depend on other network devices for services. For example, a laptop might be configured to use shared network drives and authenticate to a domain when connected to the corporate network. When used as a standalone system, laptop users authenticate to the local system.

The minimum steps for client configuration include:

- Defining device and users in AD, an LDAP directory, or other centralized authentication mechanism
- Adding user to appropriate groups
- Defining local authentication mechanism, if necessary
- Configuring event logging for audit purposes
- Configuring password lifetimes, minimum password strength, and so on according to policies

Closely related to authentication configuration is authorization configuration.

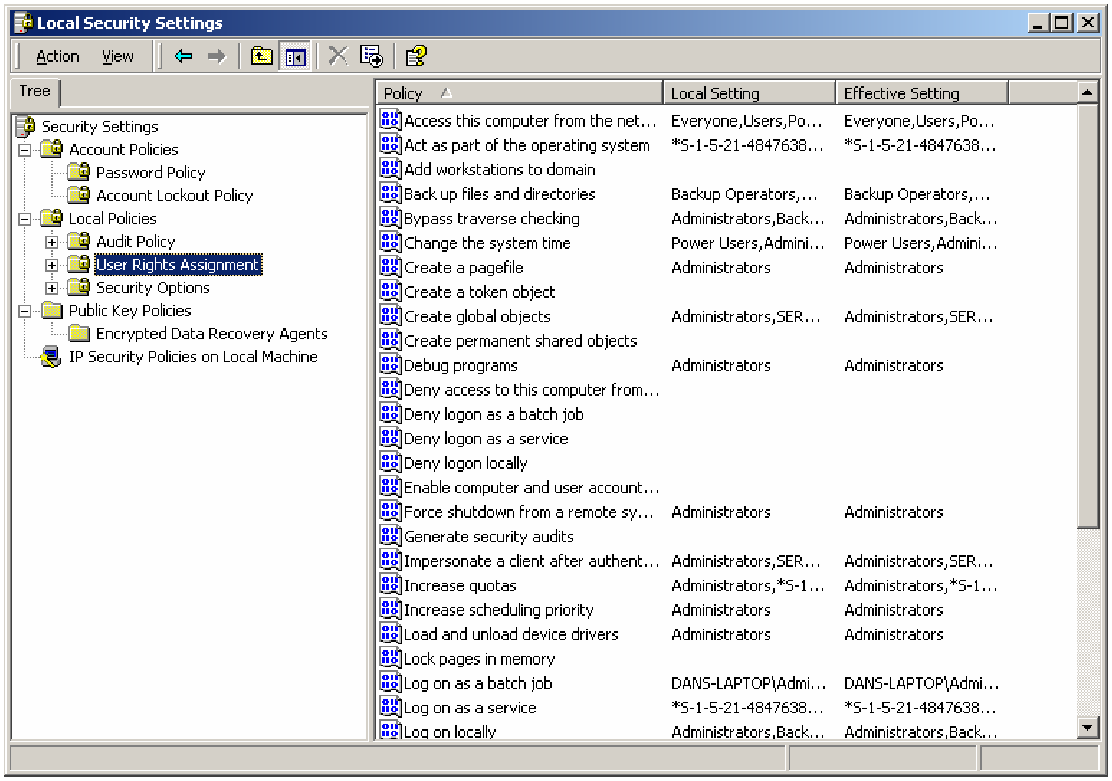
Defining Authorizations

Authorizations dictate what a user can do once the user has gained access to a system by the authentication process. The steps in this process are:

- Assigning user rights to local system (see Figure 6.5)
- Determining the set of roles relevant to user
- Assigning users to appropriate roles in a centralized access control system (for example, AD) as well as local roles, if appropriate—for example, a user may be granted administrator privileges to her laptop but not to other devices on the network

Roles are an important mechanism for implementing and managing authorizations. Roles are defined for functions within an organization that require a set of privileges. For example, only members of a department may have rights to read and write files to a shared departmental folder, print to a particular printer, or execute a departmental application. Rather than assign the required privileges directly to a user, the privileges should be assigned to a role and the role assigned to the user. This method has several advantages, including ensuring consistent granting and revoking of privileges to users; when users are assigned a role, all privileges associated with it are granted. Similarly, when a role is removed, all privileges associated with it are revoked.

Once authentication and authorizations are in place, a device is minimally protected. To ensure adequate protection against information theft several other steps are needed.



Policy	Local Setting	Effective Setting
Access this computer from the net…	Everyone,Users,Po…	Everyone,Users,Po…
Act as part of the operating system	*S-1-5-21-4847638…	*S-1-5-21-4847638…
Add workstations to domain		
Back up files and directories	Backup Operators,…	Backup Operators,…
Bypass traverse checking	Administrators,Back…	Administrators,Back…
Change the system time	Power Users,Admini…	Power Users,Admini…
Create a pagefile	Administrators	Administrators
Create a token object		
Create global objects	Administrators,SER…	Administrators,SER…
Create permanent shared objects		
Debug programs	Administrators	Administrators
Deny access to this computer from…		
Deny logon as a batch job		
Deny logon as a service		
Deny logon locally		
Enable computer and user account…		
Force shutdown from a remote sy…	Administrators	Administrators
Generate security audits		
Impersonate a client after authent…	Administrators,SER…	Administrators,SER…
Increase quotas	Administrators,*S-1…	Administrators,*S-1…
Increase scheduling priority	Administrators	Administrators
Load and unload device drivers	Administrators	Administrators
Lock pages in memory		
Log on as a batch job	DANS-LAPTOP\Admi…	DANS-LAPTOP\Admi…
Log on as a service	*S-1-5-21-4847638…	*S-1-5-21-4847638…
Log on locally	Administrators,Back…	Administrators,Back…

Figure 6.5: In addition to well-known file access privileges, systems administrators should review access rights to OS services.

Configuring Update Procedures

Any device, from a smart phone to a high-end server, will require patching at some point in its lifetime. The OSs and applications running on these devices are sufficiently complex that it is virtually impossible to ensure they will not present some vulnerability that could be exploited for malicious purposes.

When devices are deployed, they should be configured to either automatically download critical updates, or a centralized patch distribution system should be used to push patches to devices. The former approach is easier to implement and can work well in small environments or with groups of technically proficient users. A disadvantage of automatic updates is that it limits systems administrators from reviewing a patch before it is installed. It can also lead to different configurations running at the same time if some updates fail, are canceled by a user, or are never performed.

Centralized patch distribution provides for greater control by IT staff. Standard scripts can be defined to distribute patches consistently; errors are recorded in a single log; and an audit trail can be maintained. Centralized updates can also distribute patches for applications that do not provide automatic update mechanisms, such as small applications and library routines. For example, a vulnerability that requires a patch might be detected in a Java database connectivity driver (JDBC, a widely used method for accessing databases). With no update mechanism in such small programs, users would have to install the update themselves (and potentially introduce errors) or the update would have to be installed manually by a systems administrator—a time-consuming and expensive task.

> Tools such as the Microsoft Baseline Security Analyzer, described later, can identity missing patches in some Microsoft applications as well as the OS. See http://office.microsoft.com/en-au/officeupdate/default.aspx for more information about updating Microsoft Office.

Install and Configure Antivirus Software

Today, antivirus software is one of the first applications installed after the OS is installed and updated (perhaps even before the OS updates). It is well understood that without antivirus protection, a system is vulnerable, but there are several points worth emphasizing. First, for high-security environments an option is to use two different antivirus applications. One application can run on client devices and the other can run as a network service scanning traffic before it reaches the client. (Antivirus applications typically do not run when another one is already running on a client device, so two cannot be run on a single device). By using two different antivirus programs, an organization does not put all its proverbial eggs in one basket. Different vendors use different virus signatures and their behavior-based analysis may use different criteria; a threat missed by one system may be caught by the other.

The second point to keep in mind is that virus signature databases are updated frequently and clients should download updates often. Be sure to keep subscription and maintenance contracts up to date. Although antivirus programs will continue to run once update subscriptions expire, they will not run the latest signatures and may miss new threats.

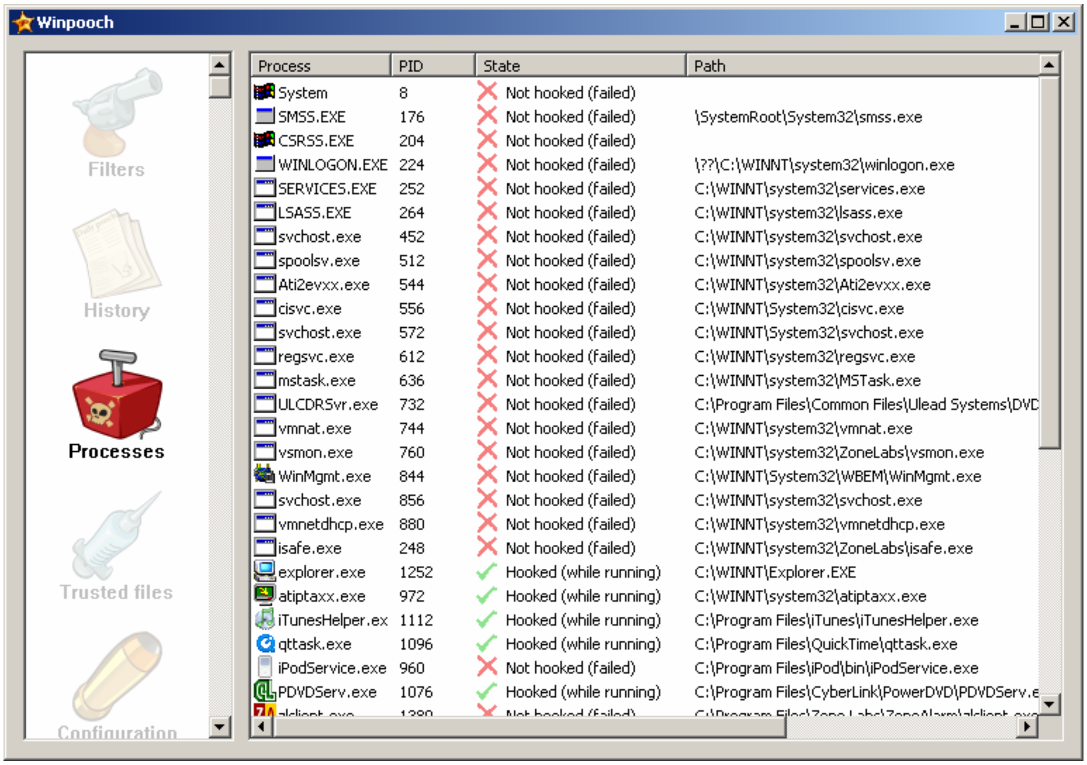
Finally, antivirus software is one application worth upgrading. Although the word processor and spreadsheet program may be suffering from feature bloat, it is not safe to assume the same for security software. Updates to antivirus software can include improvements to signature matching engines as well as to behavior-based detection modules. As antivirus software has improved, it has taken on some of the features of other security programs, such as intrusion prevention systems (IPSs).

Install and Configure Anti-Spyware Software

Anti-spyware is still a separate category of tool from antivirus, although the lines distinguishing these tools are starting to blur. Like antivirus, anti-spyware programs depend on signatures to detect spyware, such as keyloggers, and adware-related artifacts, such as browser helper objects (BHOs) and tracking cookies (see Figure 6.6). When choosing an anti-spyware tool, it is important to consider several factors in addition to the obvious factors of cost and ease of use:

- Size of signature database and frequency of update
- Speed of full disk scans
- Ability to block spyware in browsers
- Ability to analyze processes that may behave like spyware

> Spyware regularly makes use of Windows OS hooks to intercept information flowing through the OS. For more information about keyloggers, see Chapter 5.



Process	PID	State	Path
System	8	✗ Not hooked (failed)	
SMSS.EXE	176	✗ Not hooked (failed)	\SystemRoot\System32\smss.exe
CSRSS.EXE	204	✗ Not hooked (failed)	
WINLOGON.EXE	224	✗ Not hooked (failed)	\??\C:\WINNT\system32\winlogon.exe
SERVICES.EXE	252	✗ Not hooked (failed)	C:\WINNT\system32\services.exe
LSASS.EXE	264	✗ Not hooked (failed)	C:\WINNT\system32\lsass.exe
svchost.exe	452	✗ Not hooked (failed)	C:\WINNT\system32\svchost.exe
spoolsv.exe	512	✗ Not hooked (failed)	C:\WINNT\system32\spoolsv.exe
Ati2evxx.exe	544	✗ Not hooked (failed)	C:\WINNT\system32\Ati2evxx.exe
cisvc.exe	556	✗ Not hooked (failed)	C:\WINNT\System32\cisvc.exe
svchost.exe	572	✗ Not hooked (failed)	C:\WINNT\System32\svchost.exe
regsvc.exe	612	✗ Not hooked (failed)	C:\WINNT\system32\regsvc.exe
mstask.exe	636	✗ Not hooked (failed)	C:\WINNT\system32\MSTask.exe
ULCDRSvr.exe	732	✗ Not hooked (failed)	C:\Program Files\Common Files\Ulead Systems\DVD
vmnat.exe	744	✗ Not hooked (failed)	C:\WINNT\system32\vmnat.exe
vsmon.exe	760	✗ Not hooked (failed)	C:\WINNT\system32\ZoneLabs\vsmon.exe
WinMgmt.exe	844	✗ Not hooked (failed)	C:\WINNT\System32\WBEM\WinMgmt.exe
svchost.exe	856	✗ Not hooked (failed)	C:\WINNT\system32\svchost.exe
vmnetdhcp.exe	880	✗ Not hooked (failed)	C:\WINNT\system32\vmnetdhcp.exe
isafe.exe	248	✗ Not hooked (failed)	C:\WINNT\system32\ZoneLabs\isafe.exe
explorer.exe	1252	✓ Hooked (while running)	C:\WINNT\Explorer.EXE
atiptaxx.exe	972	✓ Hooked (while running)	C:\WINNT\system32\atiptaxx.exe
iTunesHelper.ex	1112	✓ Hooked (while running)	C:\Program Files\iTunes\iTunesHelper.exe
qttask.exe	1096	✓ Hooked (while running)	C:\Program Files\QuickTime\qttask.exe
iPodService.exe	960	✗ Not hooked (failed)	C:\Program Files\iPod\bin\iPodService.exe
PDVDServ.exe	1076	✓ Hooked (while running)	C:\Program Files\CyberLink\PowerDVD\PDVDServ.e
alclient.exe	1380	✗ Not hooked (failed)	C:\Program Files\Zone Labs\ZoneAlarm\alclient.exe

Figure 6.6: Anti-spyware software, such as Winpooch (http://winpooch.free.fr/home/index.php) can catch spyware and Trojan horses that use the Windows hook mechanism.

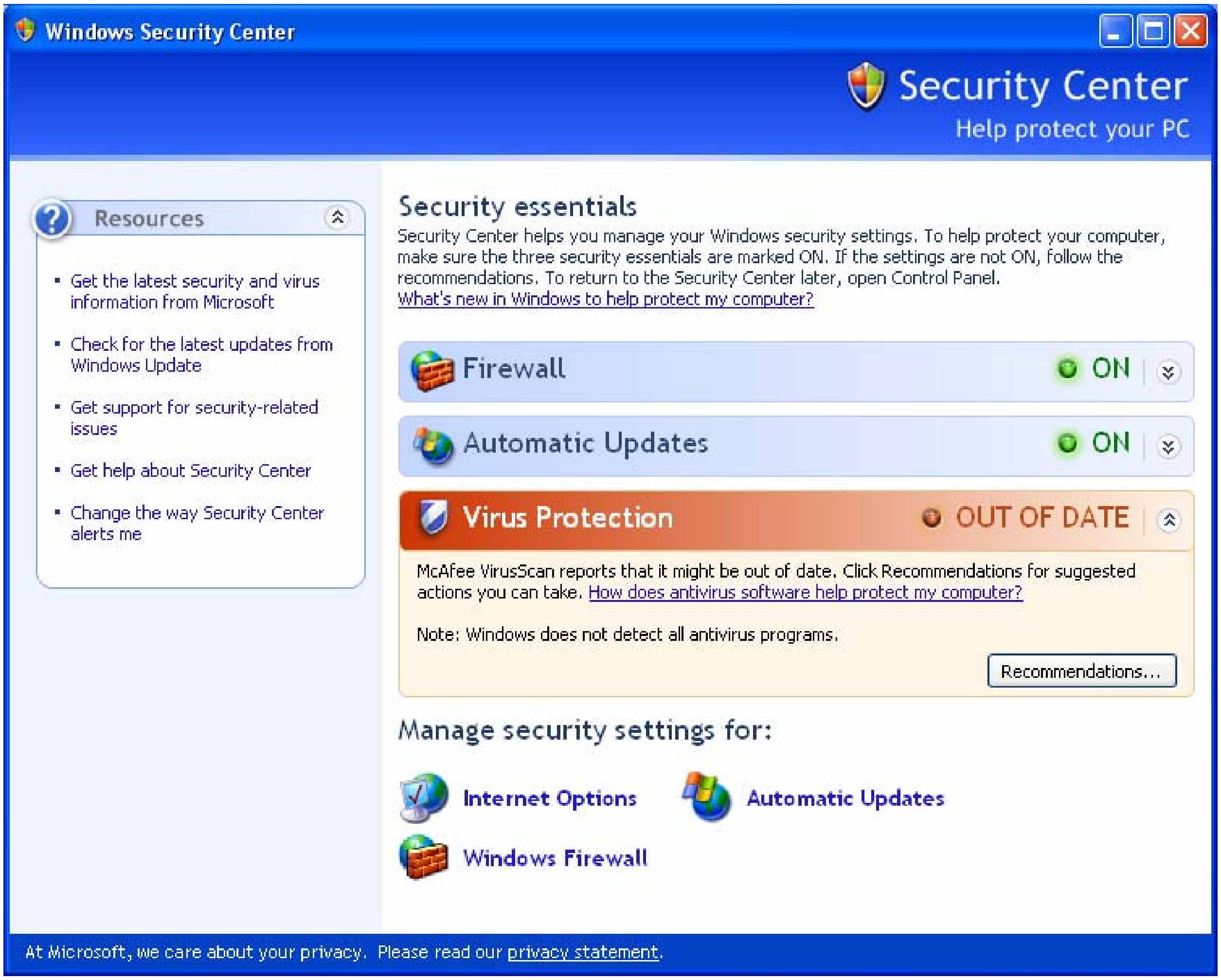
Install and Configure a Personal Firewall

Personal firewalls are essential for laptop devices that do not always have the benefit of network firewalls, but personal firewalls are also useful for desktop devices and servers. Personal firewalls allow users and systems administrators fine-grained control over network traffic flowing into and out of devices.

From an input perspective, firewalls can be configured to block access to other devices, possibly with varying degrees of restriction. For example, a laptop can be configured to block incoming ICMP traffic, such as ping echo requests, so it does not appear online to others on the Internet; it may also be configured to allow access to other devices on the same network segment.

Personal firewalls are also effective countermeasures to Trojan horses, keyloggers, and other programs that might attempt to send data from the device. The firewall may block all outgoing traffic except traffic from programs explicitly registered with the firewall.

The combination of antivirus, anti-spyware, and personal firewalls can provide substantial protection against threats. The state of these basic countermeasures are easily monitored, even by non-technical users. For example, the Windows XP Security Center (see Figure 6.7) shows an example warning of an antivirus application that may not be up to date.



Security essentials

Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.
What's new in Windows to help protect my computer?

- Get the latest security and virus information from Microsoft
- Check for the latest updates from Windows Update
- Get support for security-related issues
- Get help about Security Center
- Change the way Security Center alerts me

Firewall ● ON

Automatic Updates ● ON

Virus Protection ● OUT OF DATE

McAfee VirusScan reports that it might be out of date. Click Recommendations for suggested actions you can take. How does antivirus software help protect my computer?

Note: Windows does not detect all antivirus programs.

Manage security settings for:

Internet Options

Automatic Updates

Windows Firewall

At Microsoft, we care about your privacy. Please read our privacy statement.

Figure 6.7: Improved security reporting, such as Windows XP Security Center, make it easy for even non-technical users to identify problems with basic security countermeasures.

Another effective countermeasure that improves on that trio is vulnerability scanning.

Schedule Vulnerability Scanning

Getting a device properly configured is necessary, but it is not sufficient to ensure the device remains secure. Vulnerabilities are discovered in OSs and applications fairly often. Many of these are patched before damage is done, but, unfortunately, a single vulnerability, properly exploited, can disrupt many operations.

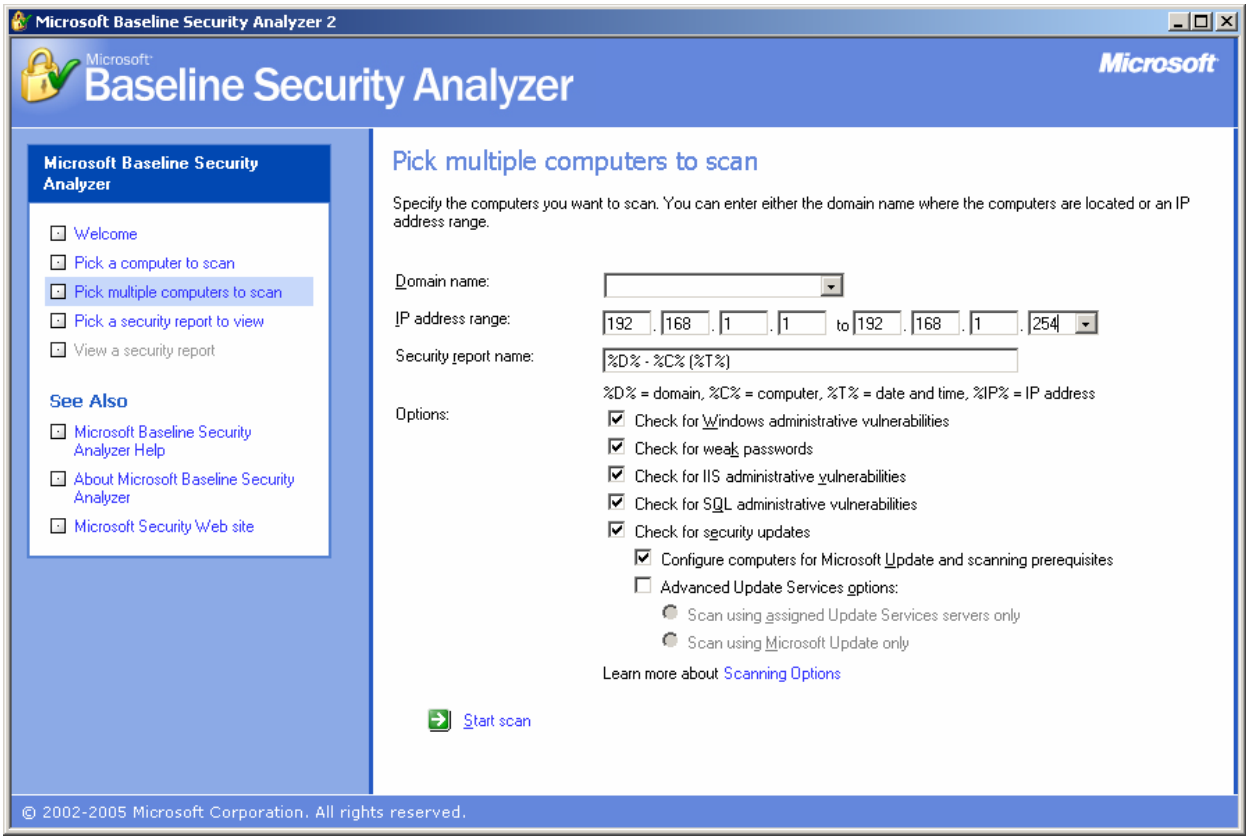
The SQL Slammer worm, for example, spread so quickly that segments of the Internet were effectively shutdown within 15 minutes of its launch. The speed with which it spread was due in part to the fact that the vulnerability existed not only in the SQL Server database, which is typically installed and managed by database professionals, but also in the Microsoft SQL Server Desktop Engine (MSDE), which was embedded in some desktop applications. Few users of these applications would have suspected they had parts of a complex relational database engine running on their computers let alone understood the need to patch such software.

A basic vulnerability scan of client devices should include:

- Verification of OS updates
- Verification of application updates, especially Web browsers, email clients, and office productivity tools
- Password strength and adherence to password policies
- Use of antivirus and personal firewall software
- Use of potentially vulnerable services, such as ftp
- Use of potentially vulnerable guest accounts
- Verification of event logging for login attempts and failures

Vulnerability scans can be run by end users (assuming they have sufficient privileges), but correcting problems may require IT support. For consistency and to ensure security policies are enforced across the organization, regular vulnerability scans should be performed by IT staff. Even basic vulnerability scanners can scan multiple remote devices (see Figure 6.8).

> 📖 The Microsoft Baseline Security Analyzer is available free of charge from Microsoft at http://www.microsoft.com/technet/security/tools/mbsahome.mspx.



Microsoft Baseline Security Analyzer 2

Microsoft Baseline Security Analyzer

Microsoft

Microsoft Baseline Security Analyzer

- Welcome
- Pick a computer to scan
- Pick multiple computers to scan
- Pick a security report to view
- View a security report

See Also

- Microsoft Baseline Security Analyzer Help
- About Microsoft Baseline Security Analyzer
- Microsoft Security Web site

Pick multiple computers to scan

Specify the computers you want to scan. You can enter either the domain name where the computers are located or an IP address range.

Domain name:

IP address range: 192 . 168 . 1 . 1 to 192 . 168 . 1 . 254

Security report name: %D% - %C% (%T%)

%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address

Options:

☑ Check for Windows administrative vulnerabilities
☑ Check for weak passwords
☑ Check for IIS administrative vulnerabilities
☑ Check for SQL administrative vulnerabilities
☑ Check for security updates
☑ Configure computers for Microsoft Update and scanning prerequisites
☐ Advanced Update Services options:
○ Scan using assigned Update Services servers only
○ Scan using Microsoft Update only

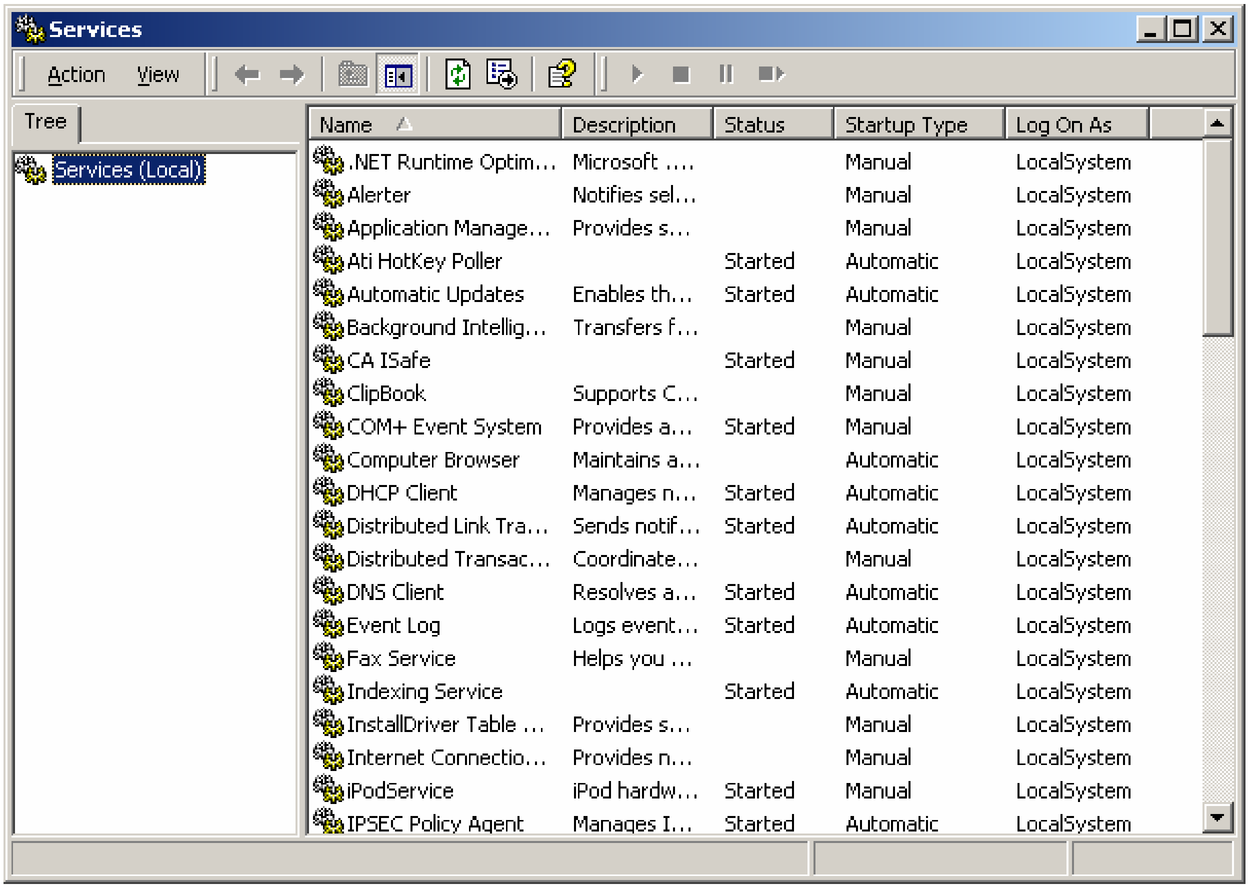
Learn more about Scanning Options

Start scan

© 2002-2005 Microsoft Corporation. All rights reserved.

Figure 6.8: Tools such as the Microsoft Baseline Security Analyzer can scan for vulnerabilities on remote devices.

If vulnerability scanning tools do not provide all the information required, systems administrators might have to resort to more time-consuming techniques. For example, if a listing of potentially vulnerable system services currently executing on a device is not available, a manual review is required (see Figure 6.9).



Name	Description	Status	Startup Type	Log On As
.NET Runtime Optim…	Microsoft ….		Manual	LocalSystem
Alerter	Notifies sel…		Manual	LocalSystem
Application Manage…	Provides s…		Manual	LocalSystem
Ati HotKey Poller		Started	Automatic	LocalSystem
Automatic Updates	Enables th…	Started	Automatic	LocalSystem
Background Intellig…	Transfers f…		Manual	LocalSystem
CA ISafe		Started	Manual	LocalSystem
ClipBook	Supports C…		Manual	LocalSystem
COM+ Event System	Provides a…	Started	Manual	LocalSystem
Computer Browser	Maintains a…		Automatic	LocalSystem
DHCP Client	Manages n…	Started	Automatic	LocalSystem
Distributed Link Tra…	Sends notif…	Started	Automatic	LocalSystem
Distributed Transac…	Coordinate…		Manual	LocalSystem
DNS Client	Resolves a…	Started	Automatic	LocalSystem
Event Log	Logs event…	Started	Automatic	LocalSystem
Fax Service	Helps you …		Manual	LocalSystem
Indexing Service		Started	Automatic	LocalSystem
InstallDriver Table …	Provides s…		Manual	LocalSystem
Internet Connectio…	Provides n…		Manual	LocalSystem
iPodService	iPod hardw…	Started	Manual	LocalSystem
IPSEC Policy Agent	Manages I…	Started	Automatic	LocalSystem

Figure 6.9: Services (also known as daemons in Linux/UNIX) should be reviewed to ensure only necessary processes are executing.

The countermeasures and procedures outlined in this chapter have been discussed in the context of client devices, but many of the measures are also applicable to servers. These same countermeasures, when applied to an entire network, can promote the security of an intranet as well.

Securing an Intranet

In addition to deploying countermeasures on client and server devices, the same countermeasures are often deployed at the network level along with additional security systems. Common security measures deployed at the network level include:

- Content filtering
- Intrusion prevention
- Antivirus and anti-spyware
- Firewalls

Antivirus, anti-spyware, and firewalls have been discussed earlier; the general principles continue to apply to network protection.

Content Filtering

Content filtering has emerged as a de facto standard countermeasure on organizational networks of any significant size. Businesses, governments, and other organizations need to preserve the integrity of the workplace. Offensive material cannot be allowed into the organization—whether it is brought in on paper, in speech, or over the Internet—without risking a hostile work environment. The same content-filtering technologies that are used to prevent hostile work environments are also helpful in reducing the use of organizational resources for non-business activities such as shopping and gambling.

Intrusion Prevention

Network IPSs, improved versions of intrusion detection systems (IDSs), analyze network traffic to detect anomalous and possibly threatening patterns. An IPS can use both attack signatures, analogous to virus signatures but based on patterns in network traffic, and variations from normal operating behaviors to identify possible attacks. Host-based IDSs are especially useful for detecting unauthorized changes to servers.

Securing an intranet is a constant challenge; however, a common set of countermeasures are useful both at the client and the network level and can contribute significantly to preventing information theft.

Summary

It is said that a chain is no stronger than its weakest link. The same is often true of information security measures. Even with managed devices—that is, the clients and servers under the control of your organization—the number and types of threats that can result in information theft present formidable challenges. By securing individual devices by using a combination of the latest security measures available and sound practices dictated by established policies, organizations can reduce the risk of information theft. The risks are further mitigated when those measures are combined with sound security practices at the intranet level. Even with these measures, risks will continue to exist; the next chapter will focus on risk analysis and incident response.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit http://nexus.realtimepublishers.com.