**A**
**Technical Outline**

# Computer Viruses & Attack Points: Methods to Reduce Threats to Security

**SPHTM**
**Academic Information Systems**
**October 18, 2001**

Prepared by
John Gerone

*Attached Overviews*
1) Microsoft's Strategic Technology Protection Program [STPP]
2) Microsoft Security Response Center Security Bulletin Severity Rating System

## Preface

The AIS department welcomes your additions, suggestions, expertise, comments in the areas outlined herein. As we go forward into the deep blue future of IT policy and operations concerning viruses and security we want to encourage the participation and interaction of other departments and centers. As with all areas of SPHTM technology infrastructure, we seek the continued support, guidance and leadership of TIS in this process. The AIS department wants to acknowledge the recent steps taken by this group and TIS to ensure network and PC security topics become an open dialogue and cooperative forum campus-wide.

## Concerning this Document

### 4 key-points

First, this document is intended to serve as a basic outline that provides a general overview of areas for discussion by this group. We are focused on viruses and PC/Network security and the best practices for protection, and operational support for solutions and remedies.

Secondly, and most importantly we hope this document can serve as a framework for specific discussion areas that have implications for IT policy and forming effective communication strategies for security and virus threats. Third, we hope this framework will help us discuss, identify and/or refine appropriate operational strategies for IT groups. Finally, we hope our experiences will benefit other persons confronted with the challenges maintaining of virus free PCs, servers and local network/computer security.

## About the Attachments

Attached to this document are two sections from Microsoft's web site. These outline their latest strategy to assist institutions and businesses with security, protection, under the "Strategic Technology Protection Program [STPP]". In addition to other tools and practices, this new program is utilizing a "severity ratings system" that interfaces with the new *hfnetchk* tool. In sum, the two briefs outline methods that include; step by step checklists, how to obtain and use tools, and best practices for dealing with virus and security threats. Finally, the ratings system is described that will be employed to rate individual security threats and severity by characterizing systems vulnerabilities.

These attachments are virus free and added here for your review and discussion whenever deemed appropriate.

***Q: Has the beast responded! ??***

**PC Viruses, Trojans, Worms and … oh no! Variants** 

## Targets

1. Servers
2. Workstations
3. Laptops
4. PDAs

## Sources of Infection – Spread

Email applications, PCs and Servers, Web Sites, Ftp Sites, portable media; floppies, and zip disks.

1. **E-Mail**
    a. attachments with viral payloads and/or macros
    b. Autorun Scripts (vbs, vb, vba)
    c. Run when you view the mail item
    d. Macros embedded in documents

## Methods vs E-mail Threats

MAILSERVER

- Virus wall Enterprise solution
- TIS filtering outside known virus payloads are bounced and or quarantined- senders are notified
- TIS filter within prevent bounces and mass mails or virus payloads

PC or Workstation

a. Virus Scan Software
    i. Must be up-to-date
    ii. Must be configured correctly
b. Webmail
    i. Is (TIS) scanning mail boxs on Majestic?
c. User vigilance
    i. Staff Training
d. Upgrades to Office XP and Outlook
    i. Auto blocks executable scripts .exe, vbs, bat, cmd etc

2. **Malicious or Infected Web-sites that propagate worms**
    a. Scripts embedded in Html –
        i. Run on url access (active scripts)
            1. ActiveX and JavaScripts
    b. Auto Downloads
        i. Run on page or link access

## Methods vs Web-Site Threats

Set up the Mcafee Internet Filter
    Active X and Java Filters
Lockdown Web Browsers (IE5.5 or 6) with policy and security settings
    Set up security Zones
    Block Active Scripting
    Block offending sites

3. **Internet and Network Attacks vs. Servers and Workstations (port scanning) From the Internet and/or within the local and wide area network.**

*Recall: Virus threats from worms and trojans generally are scripted to find and exploit security holes using, locally executable code, payloads via service ports to cause code to run via buffer overruns or systems processes. This is often accomplished using malformed urls and/or scripted urls.*

a. Hackers and blackhatters gain access with scripted attacks to leave worms and trojans behind that can compromise security, disable, damage, or destroy the system or its services and/or expose a port that can be further exploited by other attacks.

    i. These attacks target Servers and Workstations
        1. Attacks run from Unix/Linux Machines
        2. Attacks run from infected PCs on the LAN or WAN

        Specific Targets:
            a. Servers IIS5 service ports
            b. Personal Web servers (win98 /Windows Professional)
            c. Network Shares
                i. Non-NTFS
                ii. Non password-protected shares
            d. Ftp Sites (write access)
            e. Web-sites (ports)

## Methods for Protecting Servers:

Install and Run NetSheild
- -Setup and schedule auto updates
- -Setup Alert features of Netshield

Keep servers patched
- -Stay up-to-date with
  - -MS-security bulletins
  - -Security Sites Alerts

Run periodical security scans with hfnetchk.exe
- -Patch machines with holes

Lockdown Service ports not used

Disable services not needed
- -RAS
- -Remote Services
- -TFPT

Restrict Port Access on Web

Enable IP filtering (ports/packets)
- -UDP
- -TCP
- -IP

Minimize Exposure
- -Reduce servers and services exposed to the network

Throw away IIS5 and get Apache running under NT
- Not a solution for everyone

## Trapping Intruders and uncovering Viruses on the Network

Audit Security
- Particularly logon Failures

Read Security Logs
- -Identify intruders

Read Web and FTP logs
- -Look for suspicious activity such as access errors and watch for non-Tulane IP addresses

**Methods for Protecting the Network (TIS)**

Virus Walls
Firewalls
Proxy Servers
Proxy Ports
V-lans
e.g. CAEPH
Network Sniffers and tracers

**Server and Win2k Security Issues**

**NT and Win2k Server - Windows Updates – Critical Updates Notification**

-Run routinely
-Should we do do Mailouts re: security?
-Training- Workshop

**Methods for Protection using Web IIS5**

i. Pray and meditate daily for auto updates for service packs from Redmond – Why not?
ii. Change default locations of Web/ Ftp directories
iii. Set up IP security to various webpages
iv. Set up NTLM for websites /pages
v. Disable the admin web account
vi. Reset NTFS on the dynamic libraries and scripts
    a. asp.dll
vii. Disable ISAPI maping if you don't use them
viii. Enforce NTLM for authentication (disable plain text)
ix. Watch your access logs by auditing security
x. Protect your registry – Reset Security
xi. Use the MS checklist for locking down IIS5
xii. Use the IIS5 lockdown tool if you have read all the disclaimers and followed the threads on problems – e.g. exchange server hassles

**General Admin Methods against Security threats**

1. Disable guest accounts
2. Check and re-do your ACLs
3. Tighten Registry Permissions
4. Rename administrator accounts
5. Set a policy on password changes
6. Always use NTFS (convert your fat)
7. Turn off unneeded services
8. Run a personal firewall e.g Zone Alarm

# Get and Stay Secure: Microsoft Announces Strategic Technology Protection Program

*Recent viruses on the Internet underscore the threat to all computer users and highlight challenges facing the entire industry in providing security that everyone needs to conduct business. Microsoft has a special obligation to help ensure the security of the Internet and our customers' data. Today, we are announcing a comprehensive program to help customers get and stay secure. We will not rest until your business is secure. Period.*

## Introduction

Microsoft announces the **Strategic Technology Protection Program (STPP)**. This two-phase program represents an unprecedented mobilization of Microsoft's people and resources to integrate product, services and support.

## Phase 1: Get Secure

We will help you get secure right now. Here's how.

If your business has been affected by a virus-related incident and you need help, please call 1-866-PC SAFETY in the U.S. (Outside the U.S., please contact your local Microsoft subsidiary.)

The Microsoft Security Tool Kit CD includes best practice guides, information on securing your system, and service packs and patches that can help ensure your system is protected against attacks. It also provides tools that Microsoft has developed to help you secure your systems and keep them secure. Your English Security Tool Kit for U.S. and Canada customers will ship in 3 to 6 weeks free of charge. (Outside the U.S. and Canada, please contact your local Microsoft subsidiary.)

You can take these steps now:

- Order the Microsoft Security Tool Kit*
- Access the Online Microsoft Security Tool Kit
- Get Free Virus-Related Telephone Support: Call 1-866-PC SAFETY (U.S. only)

## Phase 2: Stay Secure

We are working proactively with our customers to define, install, and maintain secure, reliable computing environments over the Internet by:

- Launching security readiness events for our customers around the world.
- Making it more manageable to "stay secure" by developing enterprise security tools, creating auto-update functionality via Windows Update, and by producing bi-monthly product roll-up patches.

- Delivering thousands of Microsoft Security Tool Kits to customers for free.

Microsoft is committed to doing everything possible to make certain that every customer can work, communicate, and do business securely over the Internet.

Read the Q&A with Brian Valentine, senior vice president of the Windows division at Microsoft, to learn more about the impetus for the security initiative and the steps Microsoft is taking to protect its customers from Internet threats and system vulnerabilities.

*TechNet subscribers, click here to learn how you'll be receiving the Microsoft Security Toolkit.

## The Microsoft Security Tool Kit

The aim of the Microsoft Security Tool Kit is to help customers protect their systems from common and dangerous threats that they are likely to encounter on the Internet. The Security Tool Kit includes tools that provide a baseline level of security for servers that are connected to the Internet. It also includes security patches for vulnerabilities that the Microsoft Security Response Center has determined to be of potentially high severity for systems that are connected to the Internet.

Customers who are concerned about the threat from users internal to their organization – users who may be “inside” the organization’s firewall – need to take additional steps in configuring their systems and might need to install additional security patches. Such organizations’ choices will be guided by their own security policies.

You can order The Security Tool Kit CD at no charge for US customers. It includes automation scripts to quickly install all the security hotfixes recommended in the kit. It also includes all the content available in this online version of the kit.

**Note:** If you are a TechNet DVD or CD subscriber, you will receive all the contents of the Security Tool Kit except for the automated installation in your November shipment. The stand-alone Security Tool Kit CD will be included with your December shipment.

already in operation or if you are building new systems.

**For Windows 2000**

- New installation Existing installation

**For Windows NT 4.0**

- New installation Existing installation

**For Windows NT Server 4.0 Terminal Server Edition**

- New installation Existing installation
- Security Tool Kit Contents

## Windows 2000 Server Baseline Security Checklist

This checklist outlines the steps you should take to secure computers running Windows 2000 Server either on their own or as part of a Windows NT or Windows 2000 domain. These steps apply to Windows 2000 Server and Advanced Server.

**Important** The purpose of this checklist is to give instructions for configuring a baseline level of security on computers running Windows 2000 Server. Security settings can be configured and applied to local servers via the Security Configuration Tool Set. Domain security policies can be created by using the Security Configuration Tool Set and distributed and applied via Group Policy. This guide outlines recommended security settings for Windows 2000. A step-by-step guide to configuring enterprise security policies using the Security Configuration Tool Set is located on the Microsoft TechNet Security Web site.

http://www.microsoft.com/TechNet/prodtechnol/windows2000serv/deploy/confeat/entsec.asp

This checklist contains information about editing the registry. Before you edit the registry, make sure you understand how to restore it if a problem occurs. For information about how to do this, view the

"Restoring the Registry" Help topic in Regedit.exe or the "Restoring a Registry Key" Help topic in Regedt32.exe.

**Windows 2000 Server Configuration**

| | Steps |
|---|---|
| ☐ | Verify that all disk partitions are formatted with NTFS |
| ☐ | Verify that the Administrator account has a strong password |
| ☐ | Disable unnecessary services |
| ☐ | Disable or delete unnecessary accounts |
| ☐ | Protect files and directories |
| ☐ | Make sure the Guest account is disabled |
| ☐ | Protect the registry from anonymous access |
| ☐ | Apply appropriate registry ACLs |
| ☐ | Restrict access to public Local Security Authority (LSA) information |
| ☐ | Set stronger password policies |
| ☐ | Set account lockout policy |
| ☐ | Configure the Administrator account |
| ☐ | Remove all unnecessary file shares |
| ☐ | Set appropriate ACLs on all necessary file shares |
| ☐ | Install antivirus software and updates |
| ☐ | Install the latest Service Pack |
| ☐ | Install the appropriate post-Service Pack security hotfixes |

## Windows 2000 Server Configuration Checklist: Further Details

**Verify that all disk partitions are formatted with NTFS** NTFS partitions offer access controls and protections that aren't available with the FAT, FAT32, or FAT32x file systems. Make sure that all partitions on your server are formatted using NTFS. If necessary, use the *convert* utility to non-destructively convert your FAT partitions to NTFS.

**Warning** If you use the convert utility, it will set the ACLs for the converted drive to Everyone: Full Control. Use the fixacls.exe utility from the Windows NT Server Resource Kit to reset them to more

reasonable values.

**Verify that the Administrator account has a strong password**

Windows 2000 allows passwords of up to 127 characters. In general, longer passwords are stronger than shorter ones, and passwords with several character types (letters, numbers, punctuation marks, and nonprinting ASCII characters generated by using the ALT key and three-digit key codes on the numeric keypad) are stronger than alphabetic or alphanumeric-only passwords. For maximum protection, make sure the Administrator account password is at least nine characters long and that it includes at least one punctuation mark or nonprinting ASCII character in the first seven characters. In addition, the Administrator account password should not be synchronized across multiple servers. Different passwords should be used on each server to raise the level of security in the workgroup or domain.

**Disable unnecessary services**

After installing Windows 2000 Server, you should disable any network services not required for the server role. In particular, you should consider whether your server needs any IIS components and whether it should be running the Server service for file and print sharing. You should also avoid installing applications on the server unless they are absolutely necessary to the server's function. For example, don't install e-mail clients, office productivity tools, or utilities that are not strictly required for the server to do its job.

**Disable or delete unnecessary accounts**

You should review the list of active accounts (for both users and applications) on the system in the Computer Management snap-in, and disable any non-active accounts, and delete accounts which are no longer required.

**Protect files and directories**

Refer to Default Access Control Settings in Windows 2000 document on the Microsoft TechNet Security

Web site for details on the default Windows 2000 file system ACLs and how to make any necessary modifications.

**Make sure the Guest account is disabled**

By default, the Guest account is disabled on systems running Windows 2000 Server. If the Guest account is enabled, disable it.

**Protect the registry from anonymous access**

The default permissions do not restrict remote access to the registry. Only administrators should have remote access to the registry, because the Windows 2000 registry editing tools support remote access by default. To restrict network access to the registry:

1. Add the following key to the registry:

| | |
|---|---|
| Hive | HKEY_LOCAL_MACHINE \SYSTEM |
| Key | \CurrentControlSet\Control\SecurePipeServers |
| Value Name | \winreg |

2. Select winreg, click the Security menu, and then click Permissions.
3. Set the Administrators permission to Full Control, make sure no other users or groups are listed, and then click OK.

The security permissions (ACLs) set on this key define which users or groups can connect to the system for remote registry access. In addition, the AllowedPaths subkey contains a list of keys to which

members of the Everyone group have access, notwithstanding the ACLs on the winreg key. This allows specific system functions, such as checking printer status, to work correctly regardless of how access is restricted via the winreg registry key. The default security on the AllowedPaths registry key grants only Administrators the ability to manage these paths. The AllowedPaths key, and its proper use, is documented in Microsoft Knowledge Base article Q155363.

**Apply appropriate registry ACLs**

Refer to to Default Access Control Settings in Windows 2000 document on the Microsoft TechNet Security Web site for details on the default Windows 2000 registry ACLs and how to make any necessary modifications.

**Restrict access to public Local Security Authority (LSA) information**

You need to be able to identify all users on your system, so you should restrict anonymous users so that the amount of public information they can obtain about the LSA component of the Windows NT Security Subsystem is reduced. The LSA handles aspects of security administration on the local computer, including access and permissions. To implement this restriction, create and set the following registry entry:

| | |
|---|---|
| Hive | HKEY_LOCAL_MACHINE \SYSTEM |
| Key | CurrentControlSet\Control\LSA |
| Value Name | RestrictAnonymous |
| Type | REG_DWORD |
| Value | 1 |

**Set stronger password policies**

Use the Domain Security Policy (or Local Security Policy) snap-in to strengthen the system policies for password acceptance. Microsoft suggests that you make the following changes:

- Set the minimum password length to at least 8 characters
- Set a minimum password age appropriate to your network (typically between 1 and 7 days)
- Set a maximum password age appropriate to your network (typically no more than 42 days)
- Set a password history maintenance (using the "Remember passwords" option) of at least 6

**Set account lockout policy**

Windows 2000 includes an account lockout feature that will disable an account after an administrator-specified number of logon failures. For maximum security, enable lockout after 3 to 5 failed attempts, reset the count after not less than 30 minutes, and set the lockout duration to "Forever (until admin unlocks)". The Windows NT Server Resource Kit includes a tool that allows you to adjust some account properties that aren't accessible through the normal management tools. This tool, passprop.exe, allows you to lock out the administrator account:

- The */adminlockout* switch allows the administrator account to be locked out

**Configure the Administrator account**

Because the Administrator account is built in to every copy of Windows 2000, it presents a well-known objective for attackers. To make it more difficult to attack the Administrator account, do the following both for the domain Administrator account and the local Administrator account on each server:

- Rename the account to a nonobvious name (e.g., not "admin," "root," etc.) Establish a decoy account named "Administrator" with no privileges. Scan the event log regularly looking for attempts to use this account.
- 
- Enable account lockout on the real Administrator accounts by using the passprop utility
- Disable the local computer's Administrator account.

**Remove all unnecessary file shares**

All unnecessary file shares on the system should be removed to prevent possible information disclosure and to prevent malicious users from leveraging the shares as an entry to the local system.

**Set appropriate ACLs on all necessary file shares**

By default all users have Full Control permissions on newly created file shares. All shares that are required on the system should be ACL'd such that users have the appropriate share-level access (e.g., Everyone = Read).

**Note** The NTFS file system must be used to set ACLs on individual files in addition to share-level permissions.

**Install antivirus software and updates**

It is imperative to install antivirus software and keep up-to-date on the latest virus signatures on all Internet and intranet systems. More security antivirus information is available on the Microsoft TechNet Security Web site at:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/virus/virus.asp

**Install the latest Service Pack**

Each Service Pack for Windows includes all security fixes from previous Service Packs. Microsoft recommends that you keep up-to-date on Service Pack releases and install the correct Service Pack for your servers as soon as your operational circumstances allow. The current Service Pack for Windows 2000, SP2, is available at: http://www.microsoft.com/windows2000/downloads/servicepacks/sp2/ Service Packs are also available through Microsoft Product Support. Information about contacting Microsoft Product Support is available at http://support.microsoft.com/support/contact/default.asp.

**Install the appropriate post-Service Pack security hotfixes**

Microsoft issues security bulletins through its Security Notification Service. When these bulletins recommend installation of a security hotfix, you should immediately download and install the hotfix on your member servers.

Addition security settings

There are additional security features not covered in this document that should be leveraged when

# IIS 5.0 Baseline Security Checklist

This document lists some recommendations and best practices to secure a server on the Web running Internet Information Services (IIS) 5.

**Important** The purpose of this article is to give instructions for configuring a baseline level of security on IIS 5 servers. Additional advanced settings are provided in the complete IIS 5 security checklist on the Microsoft TechNet Security Web site.

#### Internet Information Server 5 Settings

| | Step |
|---|---|
| ☐ | Set appropriate ACLs on virtual directories |
| ☐ | Set appropriate IIS Log file ACLs |
| ☐ | Enable logging |
| ☐ | Disable or remove all sample applications |
| ☐ | Remove the iisadmpwd virtual directory |
| ☐ | Remove unused script mappings |

# Microsoft Internet Information Server 5 Security Checklist: Further Details

#### Set Appropriate ACLs on Virtual Directories

Although this procedure is somewhat application-dependent, some rules of thumb apply:

| File Type | Access Control Lists |
|---|---|
| CGI (.exe, .dll, .cmd, .pl) | Everyone (X)<br>Administrators (Full Control)<br>System (Full Control) |
| Script files (.asp) | Everyone (X)<br>Administrators (Full Control)<br>System (Full Control) |
| Include files (.inc, .shtm, .shtml) | Everyone (X)<br>Administrators (Full Control)<br>System (Full Control) |
| Static content (.txt, .gif, .jpg, .html) | Everyone (R)<br>Administrators (Full Control)<br>System (Full Control) |

**Recommended default ACLs by file type.**

Rather than setting ACLs on each file, you are better off creating new directories for each file type, setting ACLs on the directory, and allowing the ACLs to inherit to the files. For example, a directory structure might look like this:

- C:\inetpub\wwwroot\myserver\static (.html)
- C:\inetpub\wwwroot\myserver\include (.inc)
- C:\inetpub\wwwroot\myserver\script (.asp)
- C:\inetpub\wwwroot\myserver\executable (.dll)
- C:\inetpub\wwwroot\myserver\images (.gif, .jpeg)

Also, be aware that two directories need special attention:

- C:\inetpub\ftproot (FTP server)
- C:\inetpub\mailroot (SMTP server)

The ACLs on both these directories are Everyone (Full Control) and should be overridden with something tighter, depending on your level of functionality. Place the folder on a different volume than the IIS server if you're going to support Everyone (Write), or use Windows 2000 disk quotas to limit the amount data that can be written to these directories.

**Set Appropriate IIS Log File ACLs**

Make sure the ACLs on the IIS-generated log files (%systemroot%\system32\LogFiles) are

- Administrators (Full Control)
- System (Full Control)
- Everyone (RWC)

This is to help prevent malicious users from deleting the files to cover their tracks.

**Enable Logging**

Logging is paramount when you want to determine whether your server is being attacked. You should use W3C Extended Logging format by following this procedure:

1. Load the Internet Information Services tool.
2. Right-click the site in question, and choose Properties from the context menu.
3. Click the Web Site tab.
4. Check the Enable Logging check box.
5. Choose W3C Extended Log File Format from the Active Log Format drop-down list.
6. Click Properties.

Click the Extended Properties tab, and set the following properties:

- Client IP Address
- User Name
- Method
- URI Stem
- HTTP Status
- Win32 Status
- User Agent
- Server IP Address
- Server Port

The latter two properties are useful only if you host multiple Web servers on a single computer. The *Win32 Status* property is useful for debugging purposes. When you examine the log, look out for error 5, which means access denied. You can find out what other Win32 errors mean by entering *net helpmsg err* on the command line, where *err* is the error number you are interested in.

**Disable or Remove All Sample Applications**

Samples are just that, samples; they are not installed by default and should never be installed on a production server. Note that some samples install so that they can be accessed only from http://localhost, or 127.0.0.1; however, they should still be removed.

The following table lists the default locations for some of the samples.

| Sample | Virtual Directory | Location |
|---|---|---|
| IIS Samples | \IISSamples | c:\inetpub\iissamples |
| IIS Documentation | \IISHelp | c:\winnt\help\iishelp |
| Data Access | \MSADC | c:\program files\common files\system\msadc |

**Sample files included with Internet Information Server 5.**

**Remove the IISADMPWD Virtual Directory**

This directory allows you to reset Windows NT and Windows 2000 passwords. It is designed primarily for intranet scenarios and is not installed as part of IIS 5, but it is not removed when an IIS 4 server is upgraded to IIS 5. It should be removed if you don't use an intranet or if you connect the server to the Web. Refer to Microsoft Knowledge Base article Q184619 for more information about this functionality.

**Remove Unused Script Mappings**

IIS is preconfigured to support common filename extensions such as .asp and .shtm files. When IIS receives a request for a file of one of these types, the call is handled by a DLL. If you don't use some of these extensions or functionality, you should remove the mappings by following this procedure:

1. Open Internet Services Manager.
2. Right-click the Web server, and choose Properties.
3. Click Master Properties
4. Select WWW Service, click Edit, click HomeDirectory, and then click Configuration

Remove these references:

| If you don't use... | Remove this entry: |
|---|---|
| Web-based password reset | .htr |
| Internet Database Connector (all IIS 5 Web sites should use ADO or similar technology) | .idc |
| Server-side Includes | .stm, .shtm, and .shtml |
| Internet Printing | .printer |
| Index Server | .htw, .ida and .idq |

**Note** Internet Printing can be configured through group policy as well as via the Internet Services Manager. If there is a conflict between the group policy settings and those in the Internet Service Manager, the group policy settings take precedence. If you remove Internet Printing via the Internet Services Manager, be sure to verify that it won't be re-enabled by either local or domain group policies. (The default group policy neither enables nor disables Internet Printing.) In the MMC Group Policy snap-in, click Computer Configuration, click Administrative Templates, click Printing, and then click Web-based Printing.

**Note** Unless you have a mission-critical reason to use the .htr functionality, you should remove the .htr extension.

# Microsoft Security Response Center Security Bulletin Severity Rating System

## Introduction

The primary mission of the Microsoft Security Response Center (MSRC) is helping our customers operate their systems and networks securely. A major part of this mission involves evaluating customers' reports of suspected vulnerabilities in Microsoft products and, when necessary, ensuring that patches and security bulletins that respond to bona fide reports are produced and disseminated. A previous essay titled "A Tour of the MSRC" describes how we execute this mission on a day-to-day basis.

One of our major concerns is that, all too often, customers fail to install the security patches that would

However, both large and small customers have encouraged us to add this sort of information to our bulletins to help them assess risk, and we believe that we should respond to those requests. The rating system categorizes each vulnerability that is the subject of a security bulletin, according to the impact that could potentially result from exploitation of the vulnerability and the likelihood that the vulnerability could be exploited as a function of system configuration. Because systems are used in differing network and application environments, each vulnerability is rated for each of three critical environments.

In introducing the severity rating system, it's important for us to stress that we are providing our overall **estimate** of potential impact in the context of millions of customers worldwide; the severity ratings are based on our past experience and subjective judgment and may not be accurate predictors of impact for any individual customer. In the end, every customer must be responsible for deciding whether or not to apply a particular patch, based on the particulars of their computing environment

## System Environments

The major factor that we believe will help us provide useful severity ratings for customers is the environment in which affected systems operate. We believe that there are clear distinctions between desktop systems and servers, and between Internet-facing and internal servers (that is, between systems that are and are not protected by an organization's firewall). The severity of many vulnerabilities is mitigated if the affected system is behind a firewall – in particular, network ports should be protected by the firewall, and attacks exploiting a vulnerability may be stopped at the firewall. Similarly, an attack that may be devastating if targeted at a server may be a mere nuisance if targeted at an individual's desktop or laptop system.

Because of this, we have chosen to classify vulnerability ratings by system environment.

- Internet-facing server (e.g. an organization's web server or firewall);
- Internal server (e.g. a domain controller, member server or terminal server that is protected by a firewall but exposed to an organization's internal users; and
- Client system (e.g. office desktops, home PCs, or traveling laptops)

## Severity Ratings

The primary factor in rating the severity of security vulnerabilities is the potential impact that could result from successful exploitation of a particular vulnerability. At one extreme, we have seen vulnerabilities whose exploitation could result in an intruder gaining administrative control of a web server or require a

customer to reinstall the operating system on his or her computer and recreate all application data. At the other extreme are "reconnaissance" vulnerabilities that can reveal information about a system but not impact it directly.

We've distinguished "critical," "moderate," and "low" severity ratings for each of the three environments listed above. The ratings are discussed and defined as follows:

### *Internet Servers*

Internet servers are the most exposed components of any organization's IT environment. It is not possible to block access to an Internet server without keeping it from performing its intended functions. A serious vulnerability affecting an Internet server can be exploited from the Internet over a port that must be accessible in order for the server to perform its intended function. We define a serious vulnerability as one that will normally be exploitable if the server is operated in a secured or default configuration, according to normal system administration practices. Such a vulnerability could result in the defacement of a web server, or in an intruder gaining the ability to assume complete control of the server and observe or modify any transaction that passes through the server or to reliably and effectively keep it from providing service. We characterize such serious vulnerabilities as **critical** severity.

Some otherwise serious vulnerabilities can be mitigated by configuration or best practices. For example, a vulnerability that can have significant impact, but that can only be exploited with difficulty or on a server that offers unusual services or is unusually configured should not receive the same severity rating as one that affects servers in their default configurations. We will characterize vulnerabilities whose exploitation is difficult or requires a server in an unusual configuration as **moderate** severity. We will also characterize as **moderate** severity vulnerabilities that can result in transient disruption of the service rendered by Internet servers. We assume that exploitation of vulnerabilities will be facilitated by widely available scripts, so difficulty of exploitation refers to the intrinsic difficulty resulting from factors of configuration, timing, or other circumstances rather than the complexity of the script that must be developed to exploit the vulnerability.

Some vulnerabilities are simply not capable of causing much damage. For example, we have issued some security bulletins in response to vulnerabilities that could result in disclosure of web server scripts. Assuming that customers have followed basic security practices, such disclosures do not result in major impact. We will characterize vulnerabilities that can cause only limited impact as **low** severity.

### *Internal Servers*

In most organizations, only personnel who are trusted to some extent have access to internal servers. While most organizations' security policies do recognize a threat from authorized users and restrict their activities, employee or contractor agreements and the capability of auditing actions on an internal network tend to restrict the threat to internal servers.

One of the lessons of the Code Red and Nimda worm viruses was that hostile code can begin to propagate via the Internet but then penetrate organizations' internal networks and continue to propagate to unpatched systems on those internal networks. For that reason, we will always identify a vulnerability that applies to Internet servers as being applicable to internal servers as well.

We will characterize as **critical** severity a vulnerability affecting an internal server that can cause very significant impact (escalation of privilege, destruction of the server, reliable and targeted data theft or modification) to a server whose configuration follows default or best practices. A vulnerability of critical severity is also one whose exploitation is difficult or impossible to audit.

Because internal servers should be protected from attack by unknown parties, and because attacks on internal servers are usually subject to auditing, we characterize other vulnerabilities that can result in denial of service or data disclosure or modification on internal servers as **moderate** severity.

We characterize vulnerabilities that can cause only limited impact to internal servers or are difficult to exploit as **low** severity. By limited impact, we mean untargeted or fragmentary data theft or modification, or denial of service that is limited in scope or impact.

### *Client Systems*

Exploitation of security vulnerabilities can result in two broad classes of consequences for client systems. The first class is similar to the set of consequences that can affect servers, and encompasses data disclosure, destruction and modification, privilege escalation, and destruction of the entire client system. The second class encompasses the situation when a virus, Trojan Horse, or other hostile code runs on a client system and launches a worm that propagates through an entire network.

We characterize client system vulnerabilities as **critical** severity if they can cause hostile code to propagate from a properly or default configured client system without requiring the user to run a program or click on an attachment. We also apply the **critical** severity rating to vulnerabilities that can result in client system destruction or in escalation of privilege by an attacker remote from the client system.

We characterize client system vulnerabilities as **moderate** severity if they can result in local escalation of privilege (i.e. the user whose privilege is escalated is logged on to the console of the client system) or in remote but unreliable or untargeted data disclosure or modification. In general, we will use at most the **moderate** severity rating for vulnerabilities that can only be exploited if the client user can be tricked into taking an action on his system (opening a file or running a program).

We characterize client system vulnerabilities as **low** severity if they are difficult to execute or cause limited impact. We also use the **low** severity rating for vulnerabilities that can only be exploited if a user must be enticed into manually clicking on a link to a hostile web site.

### Summary

The following table summarizes the severity rating system by severity level and system environment.

| | **Critical** | **Moderate** | **Low** |
|---|---|---|---|
| Internet Servers | Web site defacement, denial of service or full control | Difficult to exploit, unusual configuration, or transient effect | Limited impact such as disclosure of scripts |
| Internal Servers | Elevation of privilege, data disclosure, or modification. Auditing difficult | Auditable data disclosure, modification, or denial of service | Untargeted or fragmentary data theft or modification, limited denial of service |
| Client Systems | Run arbitrary code without user action; remote escalation of privilege | Local escalation of privilege; untargeted data disclosure or denial of service; exploitation of user actions | Limited or fragmentary data theft or modification; hostile web site attacks |

### Using the System

We will apply this severity rating system to each newly-issued security bulletin from this point forward. Initially, we will include information about system environments and associated severity in the text of each bulletin. Over time, we plan to enhance our security bulletin search page to allow users to select bulletins by environment and severity.

With regard to security rollup fixes, we will label each according to the most serious vulnerability it eliminates. In addition, the associated bulletin will always provide ratings for each issue described.

We are also planning to reflect the severity rating system in the automated tools that we provide to customers for security patch installation and checking. We are planning to designate "critical" severity vulnerabilities as critical updates on Windows Updates, and "moderate" and "low" severity vulnerabilities as recommended updates. In addition, we will be including the severity ratings in the XML file that the Microsoft Personal Security Advisor and HFNetChk tools use to determine what security patches are needed.

Because neither Windows Update, the Microsoft Personal Security Advisor, nor HFNetChk can tell in which environment a particular system is being used, they will always characterize a vulnerability according to the highest (most severe or serious) rating associated with it.