您的潜力，我们的动力

Microsoft
微软（中国）有限公司

如何使用 Windows XP Service Pack 2的新特性编写安全代码

讲师：吴涣

微软开发合作部

starzero@sohu.com

msdn

MSDN Webcasts

概述

- Windows XP SP2 对工具和技术的影响
- 增强的网络保护技术对应用程序的影响
- 内存保护和电子邮件处理技术对应用程序的影响
- 浏览器安全性技术对 Web 应用程序的影响
- 课时小结

Windows XP SP2 对工具和技术的影响

- Visual Studio 2005 与 Windows XP SP2 的集成
- 对 Visual Studio .NET 2002、Visual Studio .NET 2003 和 .NET Framework 1.1 的影响

Visual Studio 2005 与 Windows XP SP2 的集成

- 从 Visual Studio 2005 起的所有产品：
  - 将被设计为能在 Windows XP SP2 上很好地工作
  - 将使开发人员能够充分利用 Windows XP 中的安全增强功能

对 Visual Studio .NET 2002 Visual Studio .NET 2003 和 .NET Framework 1.1 的影响

.NET Framework 1.0 和 1.1	Visual Studio .NET 2002 和 2003
将被修补以使开发人员能够利用 Windows XP SP2 的增强功能	将被修补以使开发人员能够利用 Windows XP SP2 的增强功能
利用“执行保护”的 NET Framework Service Pack 将在 Windows XP SP2 RTM 期限内交运	将不会为了利用 XP SP2 而修补早于 VS .NET 2002 发布的工具
	影响 Visual SourceSafe、Visual Studio .NET Analyzer、SQL 调试和远程调试功能

增强的网络保护技术对应用程序的影响

- Windows 防火墙如何影响应用程序
- Windows 防火墙的"开并且无例外"功能
- Windows 防火墙中的配置设置
- 如何将应用程序添加到 Windows 防火墙权限列表
- 可编写 Windows 防火墙配置更改脚本的 Netsh 命令
- Windows 防火墙对创建 IPv4 入站和出站连接的应用程序的影响
- Windows 防火墙对在 RPC 端口上接受 IPv4 入站连接的
  应用程序的影响

Windows 防火墙如何影响应用程序

功能	对应用程序的影响
默认情况下开启	默认情况下，如果应用程序不能与全状态筛选协同工作，则会产生应用程序不兼容性
引导时安全性	如果 Windows 防火墙服务启动失败，则管理员将无法远程解决问题，这是因为所有端口都将被关闭
全局配置	使用户能更轻松地管理覆盖所有网络连接的防火墙策略
本地子网限制	限制可以访问端口的人员范围
多个配置文件	需要在 Internet 和受信任网络上工作的应用程序可能无法工作，原因是两个配置文件可能并不具有相同的策略集

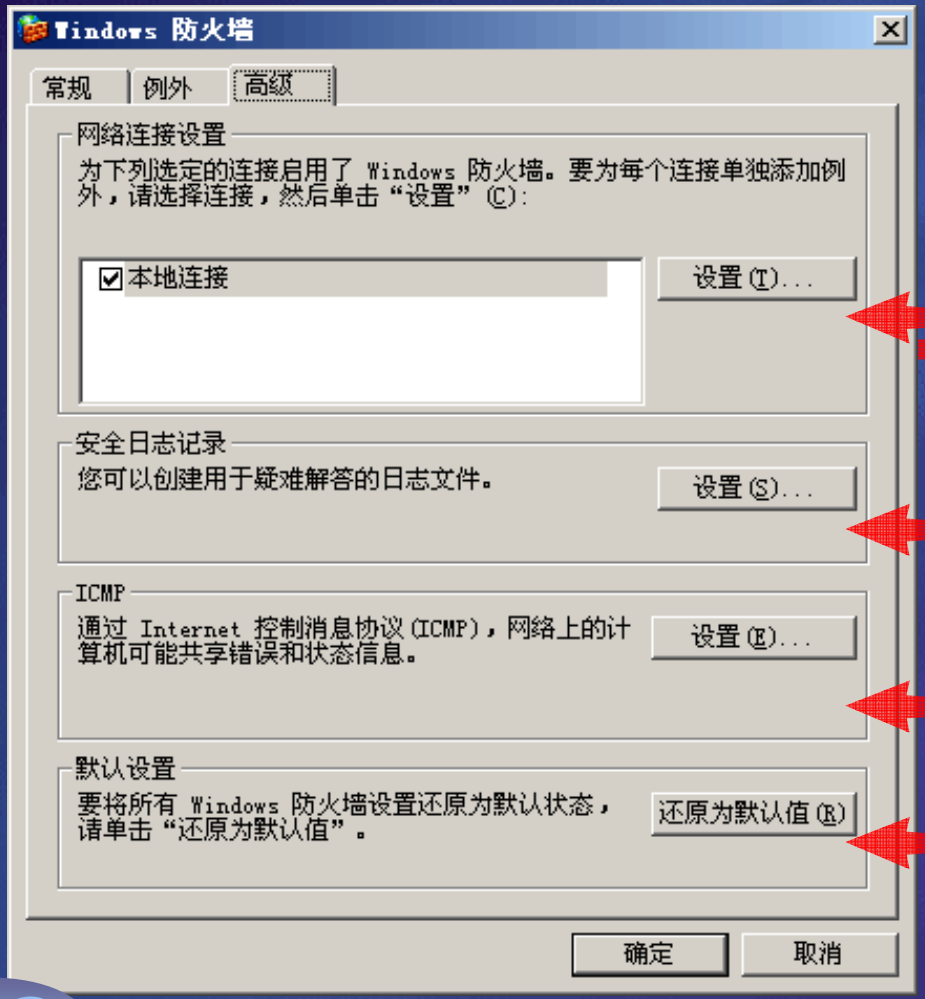
Windows 防火墙的“开并且无例外”功能

“开并且无例外”模式使 Windows 防火墙能够阻止未经请求的入站通信，而无需重新配置防火墙（如果防火墙已配置为允许所有通信的话）

“开并且无例外”模式的影响

- ✓ 计算机无法侦听源自网络中的请求
- ✓ 出站连接是唯一成功的连接
- ✓ 某些功能会因为严格的网络安全规定而失效

Windows 防火墙中的配置设置



指定在其上启用 Windows 防火墙的一组接口

指定 Windows 防火墙日志记录的配置

指定允许的 ICMP 通信类型

恢复默认设置

如何将应用程序添加到 Windows 防火墙权限列表

- 管理方式
  - 在“Windows 防火墙”对话框的“例外”选项卡上，单击“添加程序”
  - 如果您在要添加的程序的列表上未找到所需程序，请单击“浏览”以搜索它
  - 如果您仍未找到该程序，则可以改为打开端口
- 编程方式
  - 建议 ISV 在安装过程中将其用作网络侦听器的应用程序放在 Windows 防火墙的“例外”列表上

可编写 Windows 防火墙配置更改脚本的 Netsh 命令

Netsh 命令	用途
add allowedprogram	通过指定程序的文件名添加例外的通信
delete allowedprogram	删除现已允许的程序
add portopening	用于通过指定 TCP 或 UDP 端口添加例外的通信
set portopening	用于修改现已打开的 TCP 或 UDP 端口的设置
delete portopening	用于删除现已打开的 TCP 或 UDP 端口
set service	用于允许或禁止文件和打印机共享、远程管理、远程桌面和 UPnP 通信
set opmode	在全局范围或针对特定的连接（接口）指定 Windows 防火墙的操作模式

Windows 防火墙对创建 IPv4 入站和出站连接的应用程序的影响

- 对出站连接的影响
  - Windows 防火墙自动允许所有出站连接
- 对应用程序未经请求的入站连接的影响
  - 如果管理员安装需要侦听某个端口的应用程序，则用户必须指出他们是否想允许应用程序在防火墙中打开端口
- 对应用程序未经请求的入站连接的影响
  - 当服务需要侦听某个固定端口时，它必须询问用户是否应允许服务在防火墙中打开端口

Windows 防火墙对在 RPC 端口上接受 IPv4 入站连接的应用程序的影响

- AllowRpcPorts
  - 允许自动打开和关闭 RPC 端口的明确 Windows 防火墙设置
  - 默认情况下 Windows 防火墙会阻止 RPC
  - 应用程序或服务必须在 Windows 防火墙中启用 RPC 端口

内存保护和电子邮件处理技术对应用程序的影响

- 数据执行保护如何影响应用程序
- 附件管理器如何影响应用程序

数据执行保护如何影响应用程序

- 应用程序兼容性
  - 如果应用程序执行动态代码生成并且未利用“执行”权限明确标记生成的代码，则 DEP 会引起兼容性问题
- 系统兼容性
  - 当处理器运行在 PAE 模式中时，包含具有 NX 功能的处理器的系统会无法引导或遇到其他稳定性问题

附件管理器如何影响应用程序

- 适用于任何生产电子邮件或聊天客户端软件的开发商
- 在内部，附件管理器会根据扩展情况、内容类型、注册的处理程序为每个附件指定一个风险等级
- 风险等级被映射到使用 **Internet Explorer** 区域（受限制的、**Internet**、**Intranet**、本地和受信任的）检查的策略
- 不提供任何会破坏过程和防护的解决方法

浏览器安全性技术对 Web 应用程序的影响

- 本地计算机区域锁定功能如何影响 Web 应用程序
- 与 Internet Explorer 相关的新的注册表设置
- 弹出管理器如何影响 Web 应用程序
- 弹出管理器中的配置设置

本地计算机区域锁定功能如何影响 Web 应用程序

- 本地计算机区域锁定功能的影响
  - 影响在 Internet Explorer 中承载本地 HTML 文件的应用程序
  - 不会影响在 Internet 或本地 Intranet 区域承载的 Web 站点的开发人员
  - 要求开发人员注册应用程序（如果他们想确保不能通过应用程序运行恶意代码的话）
- 克服由本地计算机区域锁定功能引发的限制
  - 将内容保存为 HTA 文件
  - 将置于 HTML 文件中的“Web 标记”注释添加到 Web 页
  - 创建承载 HTML 内容 Internet Explorer Web 对象控件 (WebOC) 的单独应用程序

与 Internet Explorer 相关新的注册表设置

设置	用途
URLACTION_FEATURE_MIME_SNIFFING	允许根据"MIME 探查"将文件从一种类型升级到另一种类型
URLACTION_FEATURE_ZONE_ELEVATION	减少许多特权升级的攻击
URLACTION_FEATURE_WINDOW_RESTRICTIONS	限制脚本启动式弹出窗口和包含标题及状态栏的窗口

弹出管理器如何影响 Web 应用程序

- 弹出管理器的影响
  - 影响 Web 站点打开的窗口的行为，例如，使用以下方法打开的窗口：
    - window.open()
    - window.showModelessDialog(),window.showModalDialog()
    - window.navigateAndFind()
    - showHelp()
  - 提供 INewWindowManager 接口，它允许使用 Internet Explorer 中的呈现引擎的应用程序：
    - 显示 HTML 以使用或扩展弹出管理器功能
    - 使用您自己的弹出管理器
    - 禁用弹出管理器

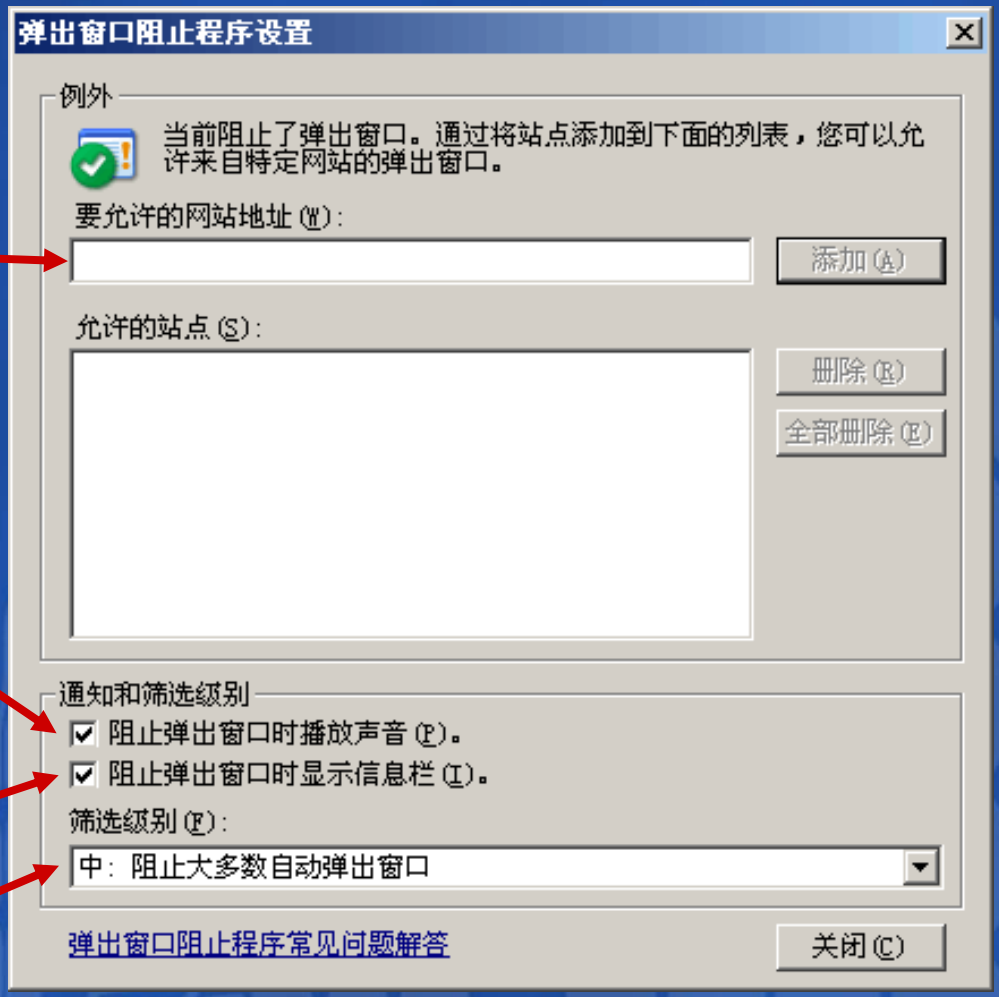
弹出管理器中的配置设置

允许“允许的站点”列表中的所有站点打开弹出窗口

在阻止弹出时播放声音

显示信息栏

阻止通过链接打开的窗口



小结

- Windows XP SP2 对工具和技术的影响
- 增强的网络保护技术对应用程序的影响
- 内存保护和电子邮件处理技术对应用程序的影响
- 浏览器安全性技术对 Web 应用程序的影响

获取更多MSDN资源

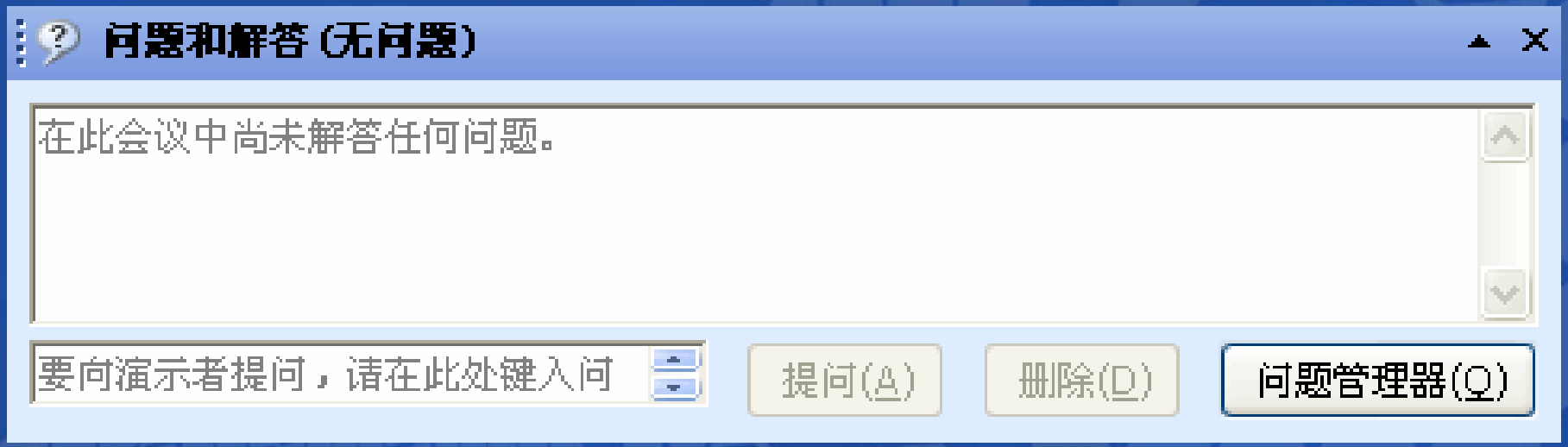
您的潜力，我们的动力

Microsoft
微软（中国）有限公司

- 微软学生中心
  http://www.msuniversity.edu.cn
- **MSDN**中文网站
  http://www.microsoft.com/china/msdn
- **MSDN**中文网络广播
  http://www.msdnwebcast.com.cn
- **MSDN Flash**
  http://www.microsoft.com/china/newsletter/case/msdn.aspx
- **MSDN**开发中心
  http://www.microsoft.com/china/msdn/DeveloperCenter/default.mspx

Question & Answer

如需提出问题，请单击“提问”按钮并在随后显示的浮动面板中输入问题内容。一旦完成问题输入后，请单击“提问”按钮。




您的潜力，我们的动力
Microsoft
微软（中国）有限公司
Microsoft
msdn
MSDN Webcasts