<<Windows 7安全指南>>

图书基本信息

书名：<<Windows 7安全指南>>

13位ISBN编号：9787121112119

10位ISBN编号：7121112116

出版时间：2010-8

出版时间：电子工业

作者：刘晖//汤雷//张诚

页数：407

前言

很多人都认为，Windows操作系统的安全性太差。
其实，对于新的Windows操作系统，例如Windows Vista/7，系统的安全性已经得到了空前的加强，然而依然有很多人在使用这些操作系统的时候因为安全问题而受到损失，到底是什么原因？
其实在计算机安全方面，也一直存在“木桶原理”，就像一只用木板拼成的木桶，桶里能装多少水，并不取决于最长的木板，而取决于其中最短的木板。
可能操作系统本身已经很安全，但因为使用的人缺乏安全意识，也有可能导致操作系统在提高安全性方面所做的全部努力付之东流。
在现在的Windows操作系统中，几乎所有选项的默认设置都是以保证安全性为前提的。
然而安全性和易用性永远都是对立的，如果要实现更高的安全性，在易用性方面肯定会大打折扣。
因此，很多人在使用过程中为了贪图方便，往往会修改一些默认的系统设置，导致系统变得不够安全。
而一旦遇到安全性问题，往往会觉得这是操作系统做得不好，并不会想到是因为自己修改的设置导致了一系列的不安全问题。
对于使用Windows的大部分一般用户来说，他们并不需要对计算机有多么高深的了解，他们只需要像使用一般电器那样打开计算机，然后学习、工作或者娱乐，并在用完之后直接关掉就可以，Windows可以很好地满足这些人的需求。
也许有更加安全的操作系统，但对于大部分用户来说，这类系统无论是安装、设置还是使用，都存在不小的难度，甚至可能根本无法在这些操作系统上完成自己需要的工作。
因此，大部分人依然在使用Windows，并希望努力让Windows变得更安全，或者至少不要因为自己的疏忽带来安全问题。
一般来说，如果希望自己的计算机更安全，我们应该从以下方面着手：·随时保持操作系统和应用程序安装了最新的补丁：现在的软件越来越复杂，存在安全漏洞也是在所难免的。
因此，无论是操作系统还是一般的应用程序，只要有安全方面的更新，就应该尽快安装，只有这样才能保护计算机不被入侵或攻击。
·给每个使用电脑的人创建自己的账户，并设置强密码：这样，每个人的使用环境将会被隔离起来，并且可以根据不同的需要给不同用户指派不同的特权，这样才能保证每个用户只能做自己需要的工作，而不会“越权”。
同时强密码的存在也可以保证系统和数据不被未经授权的人访问。
·安装反病毒软件、网络防火墙及反间谍软件：这三类软件可以保护我们的系统不被攻击和感染，但不要忘记经常更新这类软件的定义文件，只有这样才能监测到最新类型的攻击或病毒。
·对于电子邮件中的可疑附件，绝对不能轻易打开：很多病毒在通过电子邮件传播，有时候可能看似来自朋友的邮件，其实可能是对方感染病毒后不知情的情况下发送的。
因此，在收到任何人发来的邮件时都要谨慎，在打开之前最好使用反病毒软件彻底检查。
·小心朋友通过IM软件发来的网页链接：如果朋友通过IM软件发来了某个网页的链接，在打开前最好先问问对方是否发送过这样的东西，因为有时候这可能是对方系统感染了病毒后自动发送的，如果直接单击这样的链接，我们的系统也有可能会中毒。
·安装软件一定要小心：现在很多软件的安装程序中都捆绑有其他非必要的软件，这类软件一旦安装，往往很难卸载，并且可能会给系统带来很多麻烦。
因此，在安装软件时一定要小心查看所有的选项，尽量不要安装来自陌生网站的软件。
其实现在很多人已经开始意识到这个问题，但关键在于，并不是每个人都能充分理解系统中不同选项对于安全性的影响。
而且很多人对于目前层出不穷的新安全问题也并不了解，因此，本书的主要目的是向大家介绍这些选项，并通过实例告诉大家在网络上遇到这类问题后应该处理。

<<Windows 7安全指南>>

内容概要

在客户端操作系统领域，Windows的使用率是最高的。
对于微软最新的Windows 7操作系统，虽然可以说是目前安全性最高的操作系统，但受限于所谓的“木桶原理”，如果在使用中不注意，依然可能遇到潜在的安全隐患，并可能导致严重后果。
对于目前较新版本的Windows系统，已经将安全性放在了第一位。
系统中的大部分默认设置都是以保证安全为前提的。
然而安全性和易用性就像鱼和熊掌，永远不可兼得。
因此，在实际使用的过程中，我们可能还需要根据具体情况调整设置，提高易用性。
如何在这两者之间进行取舍？
如何能够在提高易用性的同时尽可能保证安全？
这就是本书要介绍的内容。
本书将从具体应用角度出发，介绍Windows 7系统在不同场合需要注意的安全选项，介绍此类选项的用途，以及建议的设置方式。
另外，本书还将从更高层面的原理和原则进行介绍，这些内容不仅适合Windows 7，还可用于其他任何主流的客户端操作系统。
本书适合对Windows系统有基本了解和使用经验，并且对系统以及软件的安全性不够放心的人群。
相信通过阅读本书，您将对Windows 7的安全性有一个全新的认识，并且能更好地将其应用到实际使用中，不仅可以保护您的系统，而且可以让具体的使用更加便利、简单。

作者简介

刘晖，自由撰稿人，微软最有价值专家（MVP），精通Windows技术。
曾在各计算机类杂志上发表过大量原创文章，并已出版多本原创和翻译的微软技术图书，包括《Windows安全指南》、《精通Windows XP》、《Windows 7使用大全》等Windows操作系统技术。
汤雷，（湖北武汉）微软MCSE，曾多年从事计算机和Windows网络管理、软件研发等工作。
对于Winldows管理、优化及实践有着丰富的经验，精通Wirldows Server服务器平台和客户端操作系统，具有丰富的管理经验。
在软件研发工作上，开发过基于中小型数据库的管理系统，为用户提供数据库管理、优化及技术支持等服务。
从200 7年起主要从事管理工作，致力于普及Windows使用知识和技巧，发现新功能，提升管理者的管理效能，提高用户的应用技巧。
张诚，网名Asuka，IT基础架构专家，毕业于上海海洋大学，现就职于某大型国企信息中心。
两次获得微软全球最有价值专家（MVP）称号，担任微软Technet特约讲师。
他是微软中文社区Wiridows版的版主，ITECN技术博客作者，熟悉Windows操作系统和Active Directorv，具有多年微软服务器产品的项目和培训经验，现致力于促进绿色IT事业的发展。

<<Windows 7安全指南>>

书籍目录

章节摘录

插图：对于缺少的软件，例如缺少网络防火墙、反病毒软件或者反问谍软件，只要安装了支持WIM的软件，然后重新启动系统，操作中心就可以识别出新安装的软件，并更新相应类别的状态。
但如果自己不知道有哪些安全软件是兼容windows 7的，例如，还没有安装反病毒软件，希望使用一个微软推荐的软件，则可以单击相应的类别（例如，反病毒软件对应的“ 恶意软件保护 ”类别），然后单击“ 查找程序 ”按钮，这样系统会自动调用浏览器访问微软网站上的相关页面，在那里可以看到微软推荐的所有软件，并可下载和试用。
对于错误的设置，操作中心则会在对应的类别下提供一个“ 还原设置 ”按钮，只要单击这个按钮，不用知道具体有哪些设置需要改变，操作中心就会自动将不安全的设置修改为推荐的安全的设置。
如果已经安装了反病毒软件，但操作中心无法检测到该软件的存在，依然报告说没有安装反病毒软件，这时候可以单击对应类别下的“ 关闭有关×××的消息 ”链接，这样的内容就会被操作中心隐藏，不再反复提示。
另外还可能存在一种情况，为了满足使用上的特殊需要，我们可能需要使用一些不够安全的设置，例如，确实需要禁用用户账户控制功能（虽然强烈推荐不这样做），或者确实需要使用不够安全的Intemet EXplorer设置，但操作中心总会频繁地告诉我们这样做不够安全，显得有些烦人。
这时候我们可以告诉操作中心，自己需要它监视哪些类别的安全问题，同时忽略哪些类别的安全问题。
方法很简单，只要单击操作中心主窗口左侧的“ 更改操作中心设置 ”链接，随后可以看到如图1-38所示的界面。
在这里可以根据实际需要进行选择，例如，如果不希望操作中心频繁通知我们已经知道的安全问题，可将对应的类别反选。
如果随后希望重新看到相关类别的通知，也只需要在这里将其选中即可。

编辑推荐

《Windows 7安全指南》：“十一五”国家重点图书出版规划项目。
计算机十大安全准则如果攻击者能够说服你在自己的计算机上运行他的程序，那么该计算机便不再属于你了。
如果攻击者能够在你的计算机上更改操作系统，那么该计算机便不再属于你了。
如果攻击者能够不受限制地实地访问你的计算机，那么该计算机便不再属于你了。
如果你允许攻击者上传程序到你的网站，那么该网站就不再属于你了。
再强大的安全性也会葬送在脆弱的密码手里。
计算机的安全性受制于管理员的可靠性。
加密数据的安全性受制于解密密钥的安全性。
过时的病毒扫描程序比没有病毒扫描程序好不了多少。
绝对的匿名无论在现实中还是在网络上都不切实际。
技术不是万能药。

版权说明