Linux与Windows的安全性比较 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/225/2021_2022_Linux_E4_B8_8EWi_c103_225035.htm 安全问题对于IT管理员来说是需要长期关注的。主管们需要一套框架来对操作系统的安全性进行合理的评估，包括：基本安全、网络安全和协议，应用协议、发布与操作、确信度、可信计算、开放标准。在本文中，我们将按照这七个类别比较微软Windows和Linux的安全性。最终的定性结论是：目前为止，Linux提供了相对于Windows更好的安全性能，只有一个方面例外（确信度）。 无论按照什么标准对Windows和Linux进行评估，都存在一定的问题：每个操作系统都不止一个版本。微软的操作系统有Windows98、Windows NT、 Windows 2000、 Windows 2003 Server和Windows CE，而Linux的发行版由于内核（基于2.2、2.4、2.6）的不同和软件包的不同也有较大的差异。我们本文所使用的操作系统，都是目前的技术而不是那些"古老"的解决方案。 用户需要记住：Linux和Windows在设计上就存在哲学性的区别。Windows操作系统倾向于将更多的功能集成到操作系统内部，并将程序与内核相结合；而Linux不同于Windows，它的内核空间与用户空间有明显的界限。根据设计架构的不同，两者都可以使操作系统更加安全。 Linux和Windows安全性的基本改变 对于用户来说，Linux和Windows的不断更新引发了两者之间的竞争。用户可以有自己喜欢的系统，同时也在关注竞争的发展。微软的主动性似乎更高一些——这是由于业界"冷嘲热讽"的"激励"与Linux的不断发展。微软将在下几个月对Windows安全进行改观，届

时微软会发布Windows XP的Service Pack2。这一服务包增强了Windows的安全性，关闭了原先默认开放的许多服务，也提供了新的补丁管理工具，例如：为了避免受到过多无用的信息，警告服务和信使服务都被关闭。大多数情况下，关闭这些特性对于增强系统安全性是有好处的，不过很难在安全性与软件的功能性、灵活性之间作出折衷。 最显著的表现是：微软更加关注改进可用性的同时增强系统的安全性。比如：2003年许多针对微软的漏洞攻击程序都使用可执行文件作为电子邮件的附件（例如MyDoom）。Service Pack2包括一个附件执行服务，为Outlook/Exchange、 Windows Messenger和Internet Explorer提供了统一的环境。这样就能降低用户运行可执行文件时感染病毒或者蠕虫的威胁性。另外，禁止数据页的可执行性也会限制潜在的缓冲区溢出的威胁。不过，微软在Service Pack2中并没有修改Windows有问题的架构以及安全传输的部分，而是将这部分重担交给了用户。 微软的重点显然是支持应用程序的安全性。Service Pack2中增强的许多方面都是以Outlook/Exchange和Internet Explorer作为对象的。例如：Internet Explorer中有一个智能的MIME类型检查，会对目标的内容类型进行检查，用户可以获悉该内容中是否存在潜在的有害程序。不过这一软件是不是能将病毒与同事的电子数据表区分开来呢？ Service Pack2的另一个新特性是能够卸载浏览器的多余插件，这需要终端用户检查并判断需要卸载哪些插件。Outlook/Exchange可以预览电子邮件消息，因此用户可以在打开之前就将电子邮件删除。另一个应用安全的增强，防火墙在网络协议栈之前启动。对于软件开发者来说，远方过程调用中权限的改变，使得安全性差的代码难以工作

正常。 Service Pack2也为Windows用户提供了许多华丽的新特性，但是问题仍然存在：这些特性会不会对管理员甚至是终端用户造成负担？是不是在增加了Windows操作系统代码安全性的同时让系统变得更加复杂？ 开放源代码、共享源代码Linux和Windows对于代码透明度这一哲学问题上是完全不同的。Linux符合GNU通用公用许可证，用户可以拷贝、复制并分发源代码。Windows使用的是封闭源代码，因此微软的安全方法被称为"通过隐藏来保证安全"。2001年，微软为了响应客户与共享源代码计划的要求，提供了对Windows源代码的访问权。现在，共享源代码计划有一百万的参与者，可以访问的源代码包括Windows2000、WindowsXP、Windows Server2003、Windows CE 3.0、Windows CE 、C#/CLI实现和ASP.NET与Visual Studio.NET。共享源代码计划许可证的对象包括公司用户、政府、合作者、学术机构与个人。 微软的共享源代码计划政策属于"可看但不可修改"，例外的情况是Windows CE共享源代码许可证计划。对于公司来说，可以将基于Windows CE的设备和解决方案推向市场。这是微软共享源代码计划下，源设备制造商（OEM）、半导体提供商、系统集成商可以完全访问Windows CE源代码的唯一项目。所有许可证持有者都有对源代码的完全访问权，当然可以修改代码，但只有OEM才能发布对基于WinCE设备的修改。所有其他的共享源代码许可证持有者，如果要访问该项目不允许的源代码，需要向Redmond.Wash的微软总部请示。 某些用户认为共享源代码计划对于调试程序会有帮助，微软要求编译的时候必须在微软总部，这不得不说是一个很大的限制。尽管微软想尽力增加透明，如果无法编译，就很难确定源代码

在真实的IT环境中是否能正常工作。限制用户修改并编译Windows的源代码，降低了人们访问Windows共享源代码并寻找安全漏洞的热情。 数据中心和桌面下Linux的安全收益 在未来的12个月里，Linux将加强在数据中心的份额，并试图冲击微软在桌面上的垄断。这很大程度上是受益于Linux2.6版内核的新特性与新功能。有了Linux v2.6，安全框架现在已经模块化了。在这种模型下，Linux内核的所有方面都提供了细粒度的用户访问控制，而以前的版本的内核允许超级用户完全控制。现在的实现仍然支持root完全访问系统，但完全可以创建一个不遵循该模型的Liinux系统。 Linux v2.6内核的一个主要变化，就是新增的Linux安全模块（LSM），用户不需要打内核补丁就能为Linux增加更多的安全机制。新版内核，在LSM上建立了多个访问控制机制，其中包括美国国安局（NSA）的Securiy Enhanced Linux（SELinux）。由于国安局对操作系统安全与强制访问控制的兴趣，产生了SELinux。国安局的研究人员正在开发Linux的安全模块，可以支持2.6内核的类型加强、基于脚色的访问控制、多层次安全。SELinux使用了命为"域类型强制"的安全模型，可以将应用程序互相隔离，同时也与基本的操作系统隔离，从而限制入侵后程序或者网络服务造成的影响。 Linux的2.6内核中已经加入了对SELinux的细粒度布尔值标签的支持，其他的厂商也开始利用国安局的SELinux。例如，Immunix提供了一些列产品，包括StackGuard和子域StackGuard模块，可以配置进程只使用某些系统调用。RedHat声称SELinux将在RedHat企业服务器4.0的安全架构上起重要的作用。 今天，Linux的内核中已经有一个功能强大、灵活的强制访问控制子系统。这个系统强制隔离

有机密和完整性要求的数据，因此任何潜在的破坏，即时是由超级用户进程所造成的，都被Linux系统限制起来了。Linux v2.6还提供了对加密安全的支持，包括了IPSec使用的加密API。这样，在网络和存储加密时就可以使用多种算法（例如：SHA-1、DES、三重DES、MD4、HMAC、EDE、和Blowfish）。Linux对IPSec IPv4和IPv6协议的支持是一个很大的进步。由于安全抽象到了协议层，用户程序对潜在攻击程序的脆弱性有所降低。密码加密模块目前还不是Linux内核的一部分，如果Linux真的实现了这样的特性，就可以阻止未签名的模块被内核访问。 现在仍然困扰Windows用户的一个问题就是缓冲区溢出。Linux用户从2.6内核开始就会收益于exec-shield补丁。exec-shield可以阻止许多漏洞攻击程序覆盖数据结构并向这些结构中插入代码的企图。由于不需要重新编译应用程序就能使exec-shield补丁奏效，实现起来很方便。 另外，2.6内核中的抢占式内核，也减少了延迟，使得Linux不但可以应用到数据中心，甚至可以在有软实时要求的应用程序使用。许多Linux用户使用的是硬件厂商和系统提供商的不开源的驱动程序（二进制模块）。问题在于：虽然添加这些驱动和模块有用，对于Linux系统并不一定有益。例如，一个未开源的驱动模块有可能控制系统调用并修改系统调用表。2.6的内核提供了特殊的保护措施，可以对限制未开源驱动或者模块对内核的访问。这一特性增加了稳定性，但从安全角度并没有增加新的限制，也不能阻止黑客编写恶意模块。 许多Linux用户来说，最有创造性的特性就是用户模式Linux了（UML），UML是Linux内核的一个补丁，可以允许可执行二进制文件在Linux宿主主机上编译并运行。使

用UML有很多好处，最有用的特性就是虚拟机。由于对UML的操作不会影响宿主主机，可以把它作为测试软件、运行不稳定发行版、检查有威胁活动的平台。UML最终会创建一个安全架构上完全虚拟的环境。Linux与Windows安全性能的重要结论 对操作系统的安全性进行定性分析，很容易包含主观意见，得到的结论会由于过去和现在的经验而有很大的不同。本文的目标是给用户提供一个框架，让他们更多的理解Windows和Linux的安全性能。下面的分析并不全面，只是终端用户进行评估的起点。Linux和Windows在技术上不断进步，究竟哪个系统更安全的结论也会不断变化。本文分析的结果：Linux提供了比Windows更好的安全特性。 基本安全 微软和Linux都提供了对验证、访问控制、记帐／日至、受控的访问保护实体、加密的支持。不过Linux的表现更好一些，因为Linux还提供了Linux安全模块、SELinux和winbind。Linux用户不需对内核打补丁就能增加额外的安全机制。 Linux在LSM之上构建了多种访问控制机制，例如：为应用程序建立了单独的空间，使它们之间相互分离，也与基本的操作系统隔离，这样即使应用程序出现了安全问题也不会影响操作系统。Linux的基本安全也可以通过应用程序增强，比如Tripwire（可以定期对系统进行关键文件的完整性检查，如果文件的内容或者属性有变化就通知系统管理员）。 Windows的限制在于基本安全是依靠MSCAPI的，在代码签名时信任多个密钥。微软的模型重点在于可以同时对一个产品使用弱加密或者强加密。尽管模块不是以相同的密钥进行签名，MSCAPI却信任许多根验证机构，代码签名也信任多个密钥。因此只要有一个密钥被泄露就会使整个系统异常脆弱。密钥泄漏的情况：

授权的代码签名者不小心纰漏了自己的私钥，或者签名机构错误的签发了一个证书。这些情况曾经发生，有一次Verisign错误的以微软的名义签发了两个证书，并将这些证书的控制权交给了未授权的个人。 网络安全与协议 Linux与Windows对网络安全和协议的支持都很不错。两者都支持IPSec，这是一个运行于IP层的开放的基于加密的保护方式。IPSec能够识别终端主机，同时能够对网络传输数据和加密数据的过程中的修改作出判断。Linux下使用OpenSSH、OpenSSL和OpenLDAP，分别对应微软系统下闭合源码的SSH、SSL和LDAP。 应用安全 由于微软IIS和Exchange/Outlook不断出现的安全问题，Linux显得更胜一筹。Apache和Postfix都是跨平台的应用程序，比微软的相应产品更加安全。由于Linux有内建的防火墙使得其安全性有所增强，Snort也是一个优秀的入侵检测系统。关于基于x86系统的Linux内核，一个很重要的特性就是IngoMolnar的exec-shield，可以保护系统不受缓冲区或者函数指针溢出的攻击，从而对那些通过覆盖数据结果或者插入代码的攻击程序有所防护。exec-shield补丁使攻击者很难实现基于shell-code的攻击程序，因为exec-shield的实现对于应用程序是透明的，因此不需要应用程序的重新编译。 微软正在大刀阔斧的重新设计产品的安全架构，并为已安装的系统提供补丁。不过旧版本的Windows产品仍然存在安全问题，这使得任务变得复杂。许多微软用户正面临安全威胁，而补丁在发布之前必须做好文档。另外，微软倾向于将应用程序的数据和程序代码混合在一起，比如ActiveX，这使得系统外的不可信数据也能被使用，甚至是利用不可信数据执行任意代码。某些情况下，Windows甚至允许外部系统提供数据

签名的代码，这就意味着本地的系统管理员也不能审查代码，不过他仍然知道是谁对代码签的名。 在.NET框架下，微软应用程序的安全性有所改进。当然，对于那些异构平台，例如Linux、Windows、Unix尤其是建立在Java平台下的应用程序，微软的产品是有很大局限性的。 分发和操作 关于分发和操作，Linux与微软的侧重点不同，Linux下大部分的管理都通过命令行接口。Linux的发行商也提供了各种安装和配置工具，例如：up2date、YaST2和Webmin。Bastille Linux是一个支持Red Hat、Debian、Mandrake、SUSE和Turbolinux的加固工具。相比之下，Windows的系统管理员使用简单易用的GUI工具，配置的时候也很容易出错误。尽管一些人认为，一个周之内将任何人都可能成为Windows的系统管理员，问题是他们到底对管理了解多少？微软的安全问题，绝大多数都是由于发布与操作时的拙劣配置。Windows自带安装和配置工具，微软也为加固域控制器、架构服务器、文件服务器、打印服务器、IAS服务器、证书服务器和堡垒主机提供了向导，不过加固架构与加固操作系统还是有区别的。 确信度 定义操作系统确信度的标准是公共标准（CC），这是ISO标准（ISO 15408）。关于确信度的等级有一个层次结构 —— 从EAL1到EAL7。只有在特定的软件、硬件和系统配置下，公共标准的评估才是有效的。Windows的EAL比Linux要高，达到了EAL4，而Linux目前只达到了EAL3。SUSE正计划在年底达到EAL4。政府机构大部分都需要CC的确信度。即使只有政府客户（甚至特指美国国防部）才需要确信度，商业产品满足这一要求也是一件好事。不过大部分的用户都不需要达到国防部的标准。 可信计算 可信计算是一种架构，可以避免对应

用程序的修改，与厂商的通信也是安全的。许多厂商，比如Intel、微软和IBM，都在欢迎这项新兴的技术。目前，这一功能只供展示，现实中并没有可用的系统，因此Linux和Windows都不能胜任。微软的可信计算与数字权力管理有关，而开源社区目前没有可信计算的项目。 开放标准 Linux要优于Windows，因为它支持所有的开放标准（尽管Windows也支持许多相同的开放便准，如IPSec、IKE和IPv6，也乐意扩展标准）。对于使用异构系统并有互操作需求的公司，"标准"如果代有私有代码，就使得对缺陷的检测和错误的修正更困难、耗费的时间也更多。一个例子就是微软对Kerberos标准协议的扩展。微软提供了对Kerberos票据的授权功能，尽管Kerberos一开始也是按照这个目的设计的，这一功能却一直没有使用。微软扩展了Kerberos标准，在处理过程中也期望其它程序共享票据的授权数据字段。因此，微软的Kerberos版本与标准不能完全交互。IT经理会发现：在一个异构的IT环境中，使用微软Kerberos会使得整个环境难以管理，它们需要完全的Windows IT架构。 开源 如果安全操作系统的标准就是开源，那么Linux显然要优于Windows。微软的共享源代码计划就是为了满足用户对源代码的需要。不过，该计划的大部分内容都是"可看但不可修改"的情况。俄罗斯、英国、中国和北约参与了微软的政府安全计划。尽管该计划的目标是增加透明度和加强合作，如果某组织需要访问微软的源代码，需要遵守各种各样的要求。例如：并不是所有的Windows源代码都可以在线查看，因此如果用户需要编译并测试应用程序，必须亲自访问微软的总部。 推荐 Linux和Windows的安全性必定会引起持续的争论，到底是开源的操作系统好，还是封

闭源代码的操作系统好？业界的逻辑是：基于开放标准与开放源代码的操作系统，能提供更好的互用性，更好的错误发现和修正机制，这要比通过隐藏来达到安全的模型优秀。开源也促使Linux的发行提供商对生产过程完全透明。每一步对于用户来说都是可再现的，因此能够逐渐的增强安全。
而Windows的源代码并不易获得，因此不能提供等价的透明。 Linux提供了至少不逊于Windows的安全性能。Linux系统的安全取决于对Linux发行版的选择、使用的内核版本、实现与支持系统的IT员工的水平。一旦你选定了产品，实现并维护操作系统的安全就完全依靠IT员工了，你需要对他们进行培训，让他们掌握足够的专业技能，完成分发、管理和故障排除的任务。要让IT经理和系统管理员明白如何应用这些惯例。 我们推荐各种机构首先了解自己的功能需要，然后熟悉一下操作系统关键性的安全性能，这样就能减少使用操作系统的风险，确保一致性。 如果你正考虑移植到另一个操作系统或者是升级目前的产品，你需要按照安全性能的要求来选择操作系统的环境。把你的商业需要与对操作系统安全性的理解相结合，就能在实现功能的同时，兼顾一致性与风险最小化。 表一：Linux和Windows操作系统重要的安全特性分类特性LinuxWindows定性得分基本安全验证、访问控制加密、记帐／日至可插入的认证模块、插件模块、Kerberos、PKI、Winbind、 ACLs、 LSM、、SELinux、 受控的访问保护实体检测、内核加密Kerberos、PKI、 访问控制列表、受控的访问保护实体检测、微软的应用程序加密程序接口。Linux 更加出色 网络安全与协议验证、层、网络层OpenSSL、Open SSH、OpenLDAP、 IPSec SSL、 SSH、 LDAP、 AD、 IPSec两者都

很不错应用安全防病毒、 防火墙、 入侵检测软件、 Web服务器、 email、 智能卡支持 OpenAV、 Panda、 TrendMicro、 内核内建的防火墙功能、 Snort、 Apache、 sendmail、 Postfix、 PKCS 11、 exec-shieldMcAfee、 Symantec、 Check Point、 IIS、 Exchange/Outlook、 PCKS 11Linux略胜一筹 分发与操作安装、配置、 加固、 管理、 漏洞扫描器安装与配置工具、 Bastille、大部分的管理通过命令行完成、 Nessus、 发行版相关的Up2Date、 YaST、 WebminWindows自带的安装和配置工具、没有特定的加固工具、 管理GUI、 使用默认安装的配置。两者都很不错确信度常见的公共标准证书、 缺陷处理Linux达到了 EAL3，有较好的缺陷处理能力Windows 达到了 EAL4，有较好的缺陷处理能力Windows更加出色可信计算 可信平台的模块、可信计算软件栈、工具、验证 由IBM开发的基于可信平台模块的开源驱动程序、可信计算组的软件栈可望在2005年推出下一代安全计算基础、有可能在2006年的Longhorn中出现。两者都不够出色 开放标准IPSec、 POSIX、 传输层安全、 常见标准 Linux 遵循所有的开放标准Microsoft也参与了开放标准，但仍有一些私有标准。Linux 更加出色 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com