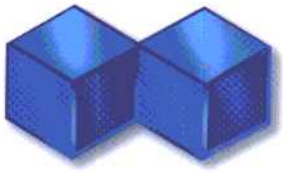
HZ BOOKS

Designed for Microsoft® Windows NT® Windows® 98

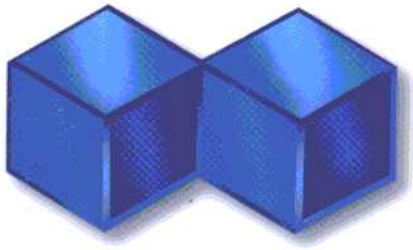
Microsoft Windows 2000 Security Technical Reference

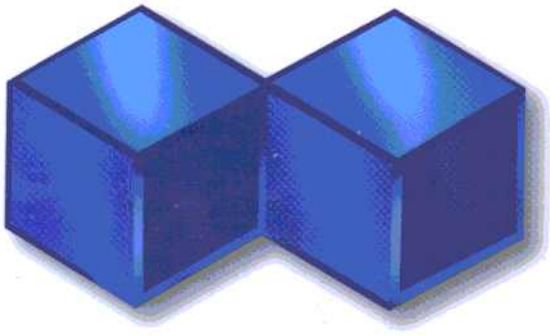
微软公司核心技术书库

(美) Internet Security Systems 公司 著
费晓飞 陈越 束妮娜 卢贤玲 等译



Windows 2000 安全技术参考





机械工业出版社
China Machine Press

Microsoft Press

微软公司核心技术书库

Windows 2000 安全技术参考

（美）Internet Security Systems公司 著

费晓飞 陈 越 束妮娜 卢贤玲 等译

王日光 审校

机械工业出版社
China Machine Press

本书是完整获得Windows 2000 安全特性与所用技术的实用详细资料的必备参考书，是对Windows 2000中强大安全特性全面、实用的指南。全书内容包括Windows NT 4.0安全特性回顾、Windows 2000安全模型与子系统、活动目录、身份验证、密码系统与微软公钥基础结构（PKI）、访问控制模型、组策略、安全配置与监视、审核、网络安全、终端服务以及IIS 5.0与IE 5.0实例介绍。两个附录分别介绍了Windows 2000资源工具箱与安全工具集模板。

本书可供广大计算机工程技术人员、系统管理员和安全管理员阅读，也可供广大安全技术爱好者和大专院校相关专业的师生学习和参考。

本书版权登记号：图字：01-2000-3408

图书在版编目(CIP)数据

Windows 2000安全技术参考/美国网络安全系统公司著；费晓飞等译. －北京：机械工业出版社，2001.7

（微软公司核心技术书库）

书名原名：Microsoft Windows 2000 Security Technical Reference

ISBN 7-111-09008-X

I. W… II.①美…②费… III.①服务器－操作系统（软件），Windows 2000②计算机网络－安全技术 Ⅳ.TP316.86

中国版本图书馆CIP数据核字（2001）第040848号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）

责任编辑：张鸿斌 肖志宏

北京第二外国语学院印刷厂印刷 · 新华书店北京发行所发行

2001年6月第1版第1次印刷

787mm × 1092mm1/16 · 28印张

印数：0 001-5 000册

定价：49.00元

前　言

当David Clark和Anne Hamiton最初要我承担写作此书的这个项目时，Windows 2000还处于第二个测试版。我曾经写过关于Windows NT 4.0的详细安全文档，原以为知道这项工作所涉及的规范，但看来是大错特错了。尚处于开发过程中的Windows 2000，就已经添加了部分特性并且其他特性也发生了改变。光是界面就经历了一系列的变化。有的变化是相当重要的，也有的不那么重要。我在测试期间发现了一些问题，其中有的后来被确定为错误并得到修正。使用尚处于开发过程中的产品是富有挑战性的。我避易就难，学到了不少东西，但这花了比预想中要多得多时间。另外还请Internet Security Systems公司Knowledge Services小组的其他成员给予帮助，并且许多长夜都花在了测试和解决某个特殊的难题上。

如果没有Ivan Phillips和Dimitris Tsapakidis这两位小组成员的特别帮助，本书就不可能写成。他们共同的专业知识和努力工作是非常宝贵的。

还必须感谢Tom Fronckowiak、Linda J. Locher和Craig Zacher，正是由于他们在好几章中的通力合作才最终完成了本书的写作。

最后，还要对指导了本书整个写作过程的Maureen Zimmerman表示诚挚的谢意。

在写作此书的过程中我学到了不少东西。并希望读者能认为此书既可用于学习，同时又是实用的参考资料。微软已经在Windows 2000中提供了大量的功能。写作本书的目的就是为了帮助读者能够最大限度地应用这些功能。

John Hayday
Internet Security Systems公司
Knowledge Services小组主任

第1章 Windows 2000安全特性变化概览

Windows 2000代表着微软公司在其Windows NT产品系列的发展中，又向前迈出了重要的一步。Windows 2000在保留了部分内核的同时，为了提供业界所需的额外功能又增加了大量的内容。其中大部分新增内容都集中在安全方面，并与新的活动目录（Active Directory）目录服务结构完全集成到了一起。在可扩展性方面，Windows 2000在设计时就是为了能够有效地适用于广大范围系统，包括从完全支持即插即用与支持高级配置和电源接口（ACPI）的膝上型电脑，到支持负载平衡和群集的服务器与交叉体系结构。其互操作性也得到了增强，能够更好地支持包括NetWare、UNIX、MVS、AS400在内的异类环境，并采用了包括轻量级目录访问协议（Lightweight Directory Access Protocol，LDAP）、Kerberos v5协议和域名系统（DNS）在内的定义良好的标准。Windows 2000还被设计为比Windows以前版本具有更好的可靠性。由于具有更为灵活的管理工具和改进的数据中心（Data Center），其管理能力也得到了增强。

在硬件方面的改进包括支持ACPI、通用串行总线（USB）、IEEE 1394（Firewire）、加速图形端口（AGP）、多显示器、数字视频光盘（DVD）、即插即用以及Win32驱动程序模型（WDM）。对WDM的支持允许硬件厂商为Windows 2000和Windows 95/98平台编写同一个驱动程序。

在文件系统方面的变化包括支持通用磁盘格式（UDF）、FAT32（允许用户双重启动Windows 2000和Windows 95/98）、磁盘碎片整理、改进的备份功能以及允许在Windows 2000中引入NTFS。Windows 2000所用的NTFS版本引入了：加密文件系统（EFS）、属性集合的概念、磁盘限额以及改进的卷（volume）管理。

通过引入活动目录和Service Pack Slipstreaming、Windows Installation 服务、Diagnostic 引导选项、Windows Management Instrumentation（Windows管理规范，WMI）以及Microsoft Management Console（Microsoft管理控制台，MMC）等新工具，管理基础设施也得到了改进。

以活动目录为核心，存在着安全功能的诸多新方面。经过仔细筹划，活动目录的内建模块允许构建出自己的能够高效利用这些技术的商务应用模型。

1.1 Windows 2000的版本

Windows 2000有下面四个版本：

- Windows 2000 Professional。作为Windows NT 4.0 Workstation的替代产品，Windows 2000 Professional预期能够成为桌面用户和移动用户共同的标准操作系统。为了帮助实现迁移，新的安装管理器（Setup Manager）可以在保存用户信息的同时，从Windows NT 3.51/4.0、Windows 3.x以及Windows 95/98进行升级。Windows 2000 Professional包括改进的硬件支持、PCMCIA卡热插拔以及对ACPI与APM的支持。由于含有SysPrep工具，只用一个主磁盘映像就可以安全地为复制做好准备，所以部署能力也得到增强。对离线文件夹的支持使

得网络文件在离线时也是可用的，而EFS则可确保移动系统上的敏感信息在系统被盗的情况下仍能得到保护。

- Windows 2000 Server。作为Windows NT 4.0 Server的替代产品，Windows 2000 Server估计通过支持基础设施服务、文件/打印与Web服务、应用服务以及通信服务，能够成为主流的工作组和部门商务服务器。它支持四路对称多处理（SMP），也引入了活动目录。通过把管理任务统一到MMC中并引入组策略（Group Policy），从而使管理得到简化。其终端服务（Terminal Services）允许继续支持传统桌上型电脑的硬件。
- Windows 2000 Advanced Server。作为Windows NT 4.0 Server Enterprise Edition的替代产品，Windows 2000 Advanced Server打算通过提供Windows 2000 Server标准版具有的全部特性以及额外支持八路SMP、企业存储体系结构（EMA）、群集和负载平衡，从而成为一种中等应用范围（midrange）的服务器解决方案。
- Windows 2000 Datacenter Server。Windows 2000新增的Datacenter Server（数据中心服务器）提供了最高等级的性能和对32路SMP的支持。Datacenter Server也具有Windows 2000 Server标准版的全部特性，但针对企业部署与解决方案进行了优化。

1.2 Windows 2000新增安全特性

本书将研究的不仅是Windows 2000的新增安全功能，同时也包括在安全方面发生了微妙变化的部分。本章将先概述新增的与安全相关功能的主要方面，然后再对每一方面进行详细讨论。

- 活动目录。活动目录是Windows 2000安全模型灵活性与可扩展性的核心，它提供了关于网络中所有对象的信息，并简化了一般的管理任务。
- Kerberos。Kerberos已经替代NT LAN Manager（NTLM）成为交叉域内的默认身份验证协议。它提供了工作站与服务器之间的相互验证，以及增强的在异类环境中的互操作性。
- 公钥基础结构。Windows 2000公钥基础结构（PKI）是许多Windows 2000新增安全功能的核心，它使得许多安全功能都广泛采用了证书（certificate）。
- 组策略对象。新增的组策略模型允许对安全策略实行集中控制，但同时也允许用分散的方式控制各种安全功能设置，这样就提供了一定的灵活性。
- IP安全协议。IP安全协议（IPsec）提供了高级的网络安全性，可以确保数据的验证、完整性和机密性（可选）。
- 加密文件系统。加密文件系统（EFS）允许有选择性加密在系统硬盘上的数据，这样即使硬盘被盗或者面临其他威胁也能确保数据的机密性。
- 安全配置工具集。安全配置工具集（Security Configuration Tool Set）中的大量工具都是为集中设计、应用以及监视安全策略而设计的。

1.2.1 活动目录

Windows 2000新增的活动目录的目录服务是系统安全的核心。它提供了完全集成在Windows 2000中的一个安全、分布式、可扩展以及重复的分层目录服务。活动目录替代Windows NT早期版本中域控制器的注册表数据库内的安全帐户管理器部分（Security Accounts Manager，SAM，

安全访问管理器），而成为了用户帐户、工作组和口令等安全信息的主要存储区域。同样地，活动目录形成了本地安全授权（LSA）的一个可信任组件。活动目录既为支持验证而存储了用户证书，也为支持授权访问系统资源而存储了访问控制信息。成员服务器和工作站则为本地定义的用户和工作组保留了本地SAM数据库。

通过把名称空间的Internet域名系统（DNS）概念集成到操作系统的目录服务之中，活动目录可以帮助统一和管理多个现有的名称空间，并提供对所有资源的一个单一管理点。活动目录并非X.500目录。它把轻量级目录访问协议（LDAP）作为核心的访问协议，并且也支持X.500信息模型。与Windows NT 4.0相同，域保留了主要的安全和管理部件，既可以在最高层级把多个域连接成一个树型结构，也可以在低层级为反映组织内部结构而建立一个组织单位（Organizational Unit，OU）层，由此得到的分层结构形成了一个DNS定位器服务所提供的名称空间，为目录中的所有对象都提供了唯一的名称。活动目录与DNS的集成还允许活动目录在DNS服务器位置记录中注册服务器位置信息，这样就可以在登录过程中用这些记录来识别域控制器。Windows NT 4.0要求Netlogon服务必须使用一个NetBIOS广播。采用Kerberos协议的服务器中的位置记录，还能使客户确定运行Kerberos v5密钥分配中心（KDC）服务的服务器位置。

域仍由域控制器管理，但是主域控制器（PDC）与备份域控制器（BDC）的概念已有了很大变化。所有的升级都必须在PDC上进行。域中的服务器现在只能是域控制器（保存有活动目录的一份拷贝）或者是成员服务器。活动目录只使用域控制器（DC），并且所有DC都是平等的。管理员可以改变任何一个DC，并且对活动目录的升级会通过远程过程调用（RPC）自动复制到站点内的所有其他DC上。这样就可以在域内提供更大的弹性和负载平衡能力。虽然可以把变化写入所有DC，但是当域工作在Windows 2000/Windows NT 4.0混合模式下的时候，PDC仿真器保留了完整Windows 2000本地模式下的一些功能。在一个混合了Windows 2000/Windows NT 4.0的网络中，PDC仿真器就作为对Windows NT 4.0 BDC的PDC。PDC仿真器在本地模式中的继续出现就提供了架构（目录结构）的完整性，并确保在关键之处复制延迟不会对安全功能造成负面影响。口令可以在任何一个DC上修改，但随后会优先复制到作为PDC仿真器的DC上去（默认为域中的第一个DC）。如果一个后继的验证请求因口令错误而失败，那么该请求也会在验证被拒绝之前传送到PDC仿真器上（万一是刚修改了口令）。帐户封锁也是在PDC仿真器上进行处理。

活动目录的分层本质也为一种具有很好粒度的管理结构做好准备，该结构能够很好地适用于分散管理，同时又不会损害安全特性。活动目录对信任传递关系的支持简化了对多域的管理。如果每个域都作为安全边界，那么多个安全边界就成为可能。在最高层，A域的管理员并不能自动成为B域的管理员。在域内，管理员的默认作用范围是整个域，并且管理员对该域内的每个对象和服务都具有管理权力。活动目录允许根据用户在给定范围内必须执行的功能来为用户授予（委派）特权。在Windows 2000中，管理范围可以包括整个域（默认情况），也可以是域内OU的一个子树，还可以仅限于单独一个OU。有了这种灵活性，就不再需要为特定事务为单位内只简单执行一个管理功能的大量用户去大规模地授予特权（例如重置用户口令）。你可以把事务单位模型化为一个独立模块或是OU的一个层，从而只在一个特定的OU内授予用户重置用户口令的特权。可以用这种方式在管理范围内授予或禁止活动目录的特定权限。Delegation of Control

Wizard工具大大简化了对委派（Delegation）选项的设置。

在活动目录内，访问控制列表（ACL）按照与使用NTFS保护文件和文件夹相同的方式保护所有的对象。ACL与对特定对象访问事件所需审核（auditing）级别的信息一起，组成了对象的安全描述。一个ACL由大量访问控制项（ACE）组成。目录对象的ACL既包括适用于整个对象的ACE，也包括只适用于对象个别属性的ACE。每个ACE定义了某个特定用户或工作组对某个给定对象或特定对象属性的访问权限。活动目录自动实现ACL的继承，因此，适用于一个容器对象的ACL就会自动遗传给所有子对象和子容器。这样还有一个好处，就是可以减少重复的通信量。比如当只有单独一个权限需要复制给其他活动目录副本时，每个副本随后都可以在本地传播所继承来的ACL权限。在活动目录内使用ACL就允许管理员不但可以控制用户是否能够看到某个给定的对象，而且还可以控制用户能够看到该对象的哪些独立属性。例如，可以允许所有用户看到其他用户的基本细节，但不让他们看到其他用户的家庭地址。也可能会限制有关个人和人力资源部的成员拥有这一级别的访问权限。管理优先权的授予就是通过以这种方式使用ACL来加以控制的。

1. 域

活动目录由一个或多个域组成，每个域在Windows 2000网络中构成了一个管理与安全边界。域可以跨越多个物理位置。每个域都有其自身的安全策略和设置，包括管理员与用户的权限、EFS策略以及ACL。每个域还可能与其他域具有安全关系（信任）。当多个域通过信任关系连接起来并共享一个通用架构、配置和全局目录的时候，就组成了一个域树。多个域树又可以连接到一起组成森林。

在Windows NT 4.0中，注册表的大小限制了域内用户帐户的数量。这样，较大的组织就不得不人为地把其基础设施分成多个域，每个域都有其自身的目录和用户帐户。但在Windows 2000中，活动目录在存储用户、工作组和计算机的帐户方面具有更强的能力。因此，原则上说，大型组织也可以把所有用户帐户和资源都合并到单独一个域中。实际上，各组织也可以出于安全或者其他原因而决定保留多个域。

2. 树和森林

一个域树由多个域组成，这些域共享一个通用的架构和配置，在活动目录内形成一个连续的名称空间。树内的所有域都通过具有传递性的信任关系链接在一起。一个域层次允许在不损害安全特性的情况下实现更佳的管理粒度。为了适应组织的变化，你可以把用户和工作组帐户从一个域移动到另一个域。

森林是指没有形成连续名称空间的一个或多个树。森林中的所有树都共享一个通用的架构、配置和全局目录。一个给定森林中的所有树都通过具有双向传递性的信任关系而彼此相互信任。与树不同的是，森林不需要截然不同的名称。一个组织可以包含具有非连续DNS名称的Windows 2000域。

3. 组织单位

在活动目录的层次结构中，组织单位（Organizational Unit，OU）是一种逻辑上的容器。它位于域的下级，可以在其中放置用户、工作组、计算机和其他OU。一个域可以具有任意数量的自己组织成为分层名称空间的OU。这些OU可以模型化，以反映公司内的部门和组织。一个定

义良好的OU结构将会大大简化安全管理和管理控制权的授予。在域树内很容易为OU重命名，如果有必要的话还可以把它们移动到不同的位置。

访问权限可以沿树向下传递。在OU基础上既可以为用户授权，也可以为一组用户授权。

4. 域间信任关系

Windows 2000域可以被组织成域树。域间的信任关系允许在一个域中有帐户定义的用户获得另一个域中资源服务器的授权。在Windows NT 4.0的多域环境中，域在逻辑上要么被分类为帐户域，要么被分类为资源域。单向的域间信任关系一般定义为从资源域到帐户域。在帐户域中创建的用户帐户可以受到所有资源域的信任，但是在资源域中创建的用户帐户却并不能得到除资源域外的其他域的信任。在大型网络中管理帐户域和资源域的信任关系是一项复杂的任务，并且企业多主域模型会造成众多的单向信任关系。

与Windows NT 4.0不同的是，当你向域树中增加每一个域的时候，Windows 2000都会自动创建域间双向传递的信任关系。与Windows NT 4.0类似，这种信任也是定义在两个域之间共享密钥基础之上的，该密钥按照某种规则进行更新。当你在域中创建第一个域控制器的时候，会遇到一个把该域加入一个现存域树的选项。如果选择了该选项，就会自动创建与特定父域之间的父子信任关系（当然必须提供域管理证书），从而所有域都隐含自动地信任树中的其他域。当客户和服务器位于森林中的不同域时，Kerberos v5验证协议就会用到信任关系。

如图1-1所示，Windows NT 4.0中的信任可以是单向或双向的，但并不具有传递性。也就是说，如果A域信任B域，那么B域也可能信任A域；但是如果B域与C域之间还具有单向的信任关系，那么A域与C域却毫无关系。所有Windows 2000中的信任关系（在森林范围内）都默认是双向和可传递的：如果A域与B域具有双向信任关系，并且B域与C域也具有双向信任关系，那么A域就信任C域并且C域也信任A域。如果需要的话，也可以在Windows NT 4.0域或者另一个森林中的Windows 2000域中建立单向或双向的非传递的信任关系。对于具有多个域的组织来说，应该减少明确具有的单向信任关系的总数。

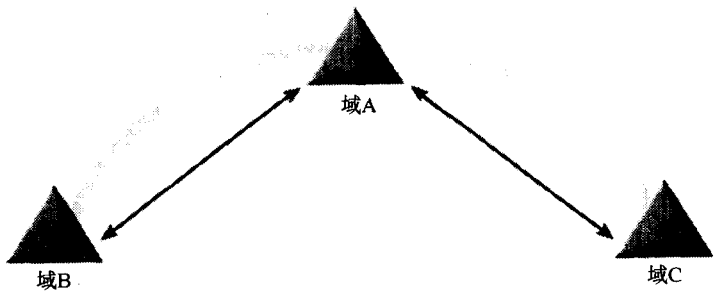


图1-1 Windows信任关系

1.2.2 Kerberos

Kerberos验证协议是20世纪80年代在麻省理工学院作为Athena工程的一部分发展而来的。

Athena工程检验了分布式网络的设计、实现和管理。Kerberos在许多UNIX平台上都已实现，并且在Kerberos协议中放置了分布式计算环境（DCE）安全服务。最新的Kerberos v5协议也已经在许多不同的平台上实现，并用来在分布式网络中提供一个单一的验证服务。IETF(Internet工程任务组)已经在RFC 1510中采纳了Kerberos v5。Kerberos在Windows 2000中的实现也遵守协议的这一最新版本，并采用通用安全服务KRB5令牌格式，以提供与不仅限于Windows 2000操作系统的互操作性。运行非Windows 2000操作系统的客户因此也可以成功地请求并使用来自Windows 2000网络验证服务（密钥分配中心，KDC）的服务票据（service ticket）。运行Windows 2000 Professional的桌上型电脑为使用UNIX KDC也可以配置Kerberos。用户可以使用在UNIX KDC中定义的帐户来登录计算机。Windows 95、Windows 98和Windows NT 4.0客户通过升级都可以支持Kerberos登录验证。

Kerberos验证协议定义了客户、资源和KDC之间的安全交互。在Windows 2000中，KDC是作为每个DC上的验证服务来实现的。通过把活动目录当作用户（主体）和工作组的帐户数据库，Windows 2000域变成了Kerberos领域的一个等价物。为了提供验证和访问控制，Kerberos协议完全集成到了Winlogon单一登录（sign-on）体系结构之中。在Windows 2000中，Kerberos v5是默认的也是主要的网络验证协议。如果是用口令登录域帐户，Windows 2000就会使用Kerberos进行验证。作为另一种选择，如果用户是用智能卡进行登录，那么就使用带证书的Kerberos验证。由Kerberos KDC Service负责为客户/服务相互验证生成会话密钥和授予服务票据。关于Kerberos KDC Service的深入讨论，请参阅第3章，“Windows 2000安全模型与子系统”。

Kerberos协议还支持“模拟”（impersonation）的概念，这样就允许客户连接到一个服务，然后该服务在与另一服务连接时模拟成该客户。同样地，如有需要，第二个服务也可以模拟该客户。这就在多层客户/服务应用体系结构中提供了一个更为健壮和更具伸缩性的验证模型。

虽然Kerberos协议是默认的网络验证协议，你也可以使用安全套接字层/传输层安全（SSL/TLS）验证。Windows NTLM验证也是为了与Windows NT 4.0的兼容性而保留了下来。

1.2.3 公钥密码系统

由于网络的开发是为了向包括供应商、合作伙伴和客户在内的内联网、Internet和外联网（extranet）提供商业服务，所以网络用户数量急剧增长。当网络在物理上和逻辑功能上变得越来越大时，非授权用户获取对数据访问权限的潜在机会也在增大。要在这种组织上安全地分配和管理用户证书，就需要一个经周密计划的公钥基础结构（PKI）。PKI是由数字证书和证书颁发机构（CA）组成的一个系统，证书颁发机构使用公钥密码手段对电子事务处理所涉及双方的有效性进行检查和验证。

1. Windows 2000 PKI

Windows 2000引入了建立全面基于标准的PKI所必需的工具。这一基础设施的核心是Microsoft Certificate Services（证书服务），它允许部署一个或多个企业级的证书颁发机构（CA）来支持组织的商业需求。通过管理X.509公钥证书的颁发与吊销，CA使组织能建立和确保证书持有者的身份。Certificate Services以用目录服务来发布关于证书服务信息的方式集成到了活动目录之中，这些信息包括用户证书的位置和证书吊销列表（CRL）。

Microsoft Certificate Services为支持证书服务的不同用法提供了一个可伸缩的CA层次模型。在最简单的形式下，CA层次可以只由一个CA组成。但是大型组织一般都会部署由明确定义了证书路径的多个CA组成的PKI。位于层次结构顶层根节点上的CA可以存在于该组织之外，也可以由第三方提供。但是，并不需要所有CA都共享同一个顶层根CA。

Certificate Services的一个独立组件是certification Web enrollment pages（证书Web注册页），它让需要证书的用户可以用Web浏览器进行申请。这种基于Web的界面是可定制的，允许一个组织根据其特殊需要来修改界面。

可以用Windows 2000组策略对象（GPO）来向计算机自动分配证书、建立证书信任清单和确定普遍受到信任的证书颁发机构。GPO也控制对EFS基于证书的恢复策略的管理。

一旦组织能够管理数字证书，那么就有一套增强的安全选项可用于处理下列技术：电子邮件、安全Web通信、经数字签名的软件、EFS、IPsec以及智能卡安全。

2. 安全电子邮件

标准的Internet电子邮件并不安全。它是以明文形式在开放的网络上进行发送的。电子邮件的这一根本特性增加了一种风险，非授权者甚至不用进入你所在组织的许可范围就可以监视你的邮件，而你的邮件中也许含有机密信息或个人隐私信息。

警告 认识到你所在组织电子通信的性质是十分重要的。有多少雇员把他们的办公电子邮件发送到了个人Internet邮件帐户？又有多少人因疏忽大意而把私人电子邮件发送到了错误的地址？电子邮件也容易受到模拟的影响。任何人都可以通过使用现有工具仿造出电子邮件的源IP地址和邮件报头，从而模拟成邮件报文的发送方。

针对潜在的弱点，IETF的安全多用途Internet邮件扩展（S/MIME）工作组已经开发出了开放的S/MIME标准。该标准允许电子邮件的数字签名和加密。在任何采用了S/MIME的平台上进行操作的客户，无论由什么服务器处理消息，都可以相互发送安全的电子邮件，因为所有的加密功能都在邮件客户方执行。大多数主要的邮件客户销售商（包括微软公司）都支持S/MIME。S/MIME安全电子邮件采用了工业标准X.509数字证书和公钥技术，可以向发送方保证只有计划中的接收方才能阅读加密邮件的内容，并同时向接收方保证报文的真实性。每个邮件客户必须要有一个有效的证书，安全电子邮件才能正确地发挥作用。

最佳操作 你可以用Microsoft Certificate Service来颁发能够在Microsoft Outlook 98/2000等兼容S/MIME的安全邮件客户应用程序中工作的安全邮件证书。Web enrollment page（Web注册页）也可以帮助用户对安全邮件证书提出请求和接收。

3. 安全Web通信

所有应用了TCP/IP上的超文本传输协议（HTTP）、Telnet和文件传输协议（FTP）基于Web的通信都是不安全的，因为所有信息都是以明文发送的。机密信息和敏感信息都容易被截取和阅读。天生缺少加密，再加上使用标准HTTP时缺少Web服务器的验证，这就为引入欺诈性Web服务器提供了方便。这种服务器可以尝试被动地从客户获取信息，也可以尝试主动地向客户引入恶意软件。

许多现存的安全通信标准都使用了公钥技术。最流行的两个这种协议，安全套接字层（SSL）

3.0和开放传输层安全（TSL，基于SSL），被企业用来为Web上的保密通信提供安全通道。对准许出口的加密强度的限制条件，是在客户与服务器协商好所用加密强度之后，在任何事务处理的初始阶段进行处理的。服务器应该选择客户与服务器都能支持的最大加密强度。因此，仅当客户与服务器都支持具有出口限制的高强度密码时，才能达到最高级别的安全性。

在需要高强度加密技术的场合（例如为了保护金融业务）都已经采用了特定用途的密码协议（在当前密码出口规则允许的情况下），例如安全电子传输（SET）协议和服务器网关加密（SGC，亦作服务器选通密码技术）协议。微软的Internet Information Server（Internet信息服务器，IIS）支持SGC协议，Internet Explorer 5（Internet资源管理器，IE 5，应用了微软电子钱包技术）支持SET协议。为了能够与其他第三方产品一起使用IE和IIS，可以使用Microsoft Certificate Services来颁发客户和服务器验证证书。用户验证证书也可以用来控制对IIS资源的访问。IIS在证书的基础上验证用户，然后把证书映射到用户帐户。这种映射可以在一对一或一对多的基础上完成。在一对多的情况下，映射是在特定CA颁发的证书与单独一个用户帐户之间进行的。当某股东的雇员需要访问基于Web的股票管理应用时，这种一对多的映射就可能是很好的。该股东用他自己的CA来向该雇员发布验证证书。与其把独立证书映射到Web服务器上的特定用户帐户，还不如决定把所有由该股东的CA所颁发的有效证书都映射到单独一个用户帐户上。

4. 经数字签名的软件

针对病毒和Internet下载程序中恶意代码的威胁，微软开发了认证码（Authenticode）技术，该技术使得开发人员能够采用标准X.509证书对软件进行数字签名。一旦软件经过签名，任何修改都会使该数字签名无效。有效数字签名的存在能够确保用户既可以检验软件的出处，又能校验软件在签名后是否被修改。Windows 2000公钥组策略可以为代码签名配置你所在组织信任的特定CA。这样，来自由这些CA提供证书的发行商的软件，就可以自动下载而不需用户干预。还可以通过配置IE来防止用户下载和运行未签名软件。

5. 智能卡

含有一个微型集成电路的智能卡能防止窜改，并可用来存储用户的证书和公钥。受个人身份号码（PIN）的保护，智能卡为用户验证和认可提供了更强的安全性。因为加密操作独立于操作系统，所以它们不易受到对操作系统的攻击影响。有一种通用智能卡接口已经用于把加密智能卡集成为支持登录Windows 2000的智能卡的一部分。要使用该卡，用户必须把它插入到系统附带的智能卡阅读器中，然后根据提示，输入PIN码。因此，智能卡需要两个识别要素：拥有该卡并知道PIN码。Windows 2000通过使用点对点隧道协议（PPTP）的EAP-TLS扩展，支持用智能卡进行网络登录和远程访问验证。

说明 可以用Microsoft Certificate Service来颁发智能卡证书。

微软CryptoAPI为在应用中支持密码功能提供了一个体系结构。它把使用加密技术的应用与密码算法的实现分离开来。CryptoAPI体系结构是为支持可安装加密服务提供程序（CSP）而设计的。这些CSP可能是基于软件的，也可以利用硬件密码设备。通过CryptoAPI，在运行Windows NT和Windows 2000的工作站和服务器与运行Windows 95/98的工作站上，都统一提供了对基于公钥应用程序的支持。

1.2.4 组策略对象

在Windows NT 4.0中，System Policy Editor（系统策略编辑器）可以配置存储在Windows NT注册表数据库中的用户和计算机设置。在Windows 2000中，组策略对象（GPO）的概念代替了这一功能。组策略是用来为用户与计算机组集中定义系统设置和应用程序而设置的。这些设置包括软件策略、脚本（计算机启动关闭和用户登录注销）、用户文档与设置、应用程序的部署和安全设置。组策略由Active Directory Users And Computers（活动目录用户与计算机）管理工具定义为域或OU的一个属性。组策略定义了包含在组策略对象（GPO）中的信息。GPO关联到一个或多个活动目录对象，如站点、域和OU，并允许选择集中或者分散管理。分散管理由于管理员具有授予GPO控制权的能力而得到支持。默认情况下，GPO会影响其作用范围内的所有计算机和用户。但是通过采用对用户或计算机在Windows 2000安全组内成员身份的过滤（即系统访问控制列表，SACL），就可以改变这一点。ACL也用来控制授权访问Group Policy Editor（组策略编辑器）。

Group Policy Editor及其扩展可以让你为所管理的计算机和用户桌面配置定义组策略选项。用Group Policy Editor可以对下列内容进行设置：

- 软件策略（Software policy）。可以在桌上型电脑中用软件策略托管注册表设置，包括那些影响操作系统组件与应用的内容。
- 脚本（Script）。可以通过组策略来控制脚本，例如计算机的启动、关闭、登录、注销等。
- 软件管理选项（Software management option）。软件管理选项可以控制哪些应用程序对用户是可用的，以及哪些可以出现在桌面上。管理员可以通过这些选项为用户与计算机组安装、分配、发行、升级、维护和删除软件。
- 用户文档与设置（User documents and setting）。用户文档与设置可以向用户桌面中的特定文件夹增加文件、文件夹和快捷方式。特定文件夹位于\Documents And Settings文件夹的用户配置文件下。这些设置可以控制把用户的\My Documents文件夹重定向到某一网络位置。
- 安全设置（Security setting）。可以从一个安全模板中导入安全设置并自动采用。同样的模板可用Security Configuration Tool Set（安全配置工具集）来分析系统的当前安全配置。

计算机的GPO在系统启动时使用，而能影响用户的GPO则在用户登录时使用。这种使用仅在系统启动或者用户登录的过程中才会发生，而不是在一段时期内起作用。默认情况下，GPO每8小时就会重新使用一次（可配置为从7秒至45天之间的某个值）。

本地安全策略设置

管理员通过Control Panel（控制面板）中的Security Setting（安全设置），可以看到某特定系统正在实行的安全策略。“secpol” MMC 管理单元（Snap-In）允许管理员查看本地策略设置与生效的设置。当某个生效的设置是GPO作用的结果时，本地设置就不会起作用。当没有GPO强加的设置时，本地管理员才可以设置一个有效的本地策略，这样就允许域管理员能够集中定义某种安全策略选项，并在GPO的范围内统一采用。同时也允许本地管理员在每个独立的系统上设置其他安全策略选项。

1.2.5 IPsec协议

Windows 2000中包含有IETF（Internet 工程任务组）IP安全协议（IPsec）的实现。IPsec为高级网络安全提供了网络数据的验证、完整性和机密性。IPsec存在于传输层的下层，因此应用程序可以透明地继承其安全服务。IPsec也同样适用于保护在内联网各部分之间传输的敏感数据，例如在客户与特定应用服务器之间，或者是在不安全网络中组成虚拟专用网（VPN）的独立主机（或站点）之间。IPsec Policy Agent Service（IPsec策略代理服务）提供了IPsec工具，并负责管理IPsec策略、ISAKMP/Oakley（IKE）的启动和IPsec驱动程序。

由IETF为IP协议设计的Windows 2000 IPsec，采用了工业标准加密算法和验证技术。IPsec是一个开放的工业标准，由多个RFC定义。从事IPsec实现工作的多家公司依据标准测试了其互操作性，以确保与现有的IP加密技术相比，他们的产品能具有更强的互操作性。

按照IETF的定义，IPsec使用了一个IP验证报头（AH）和一个IP封装安全载荷（ESP）。AH可以提供完整性、源验证，可以防止采用算法重新计算出每个IP包的散列报文认证码（HMAC），即防重放。ESP通过采用DES-CBC算法提供机密性，以作为对验证与完整性的补充。Windows 2000 IPsec实现了Internet密钥交换（IKE）协议，可以自动管理完整性和加密密钥。管理员可以根据所要保护信息的敏感程度和相关网络的弱点选择AH或者ESP。当然，ESP加密需要相应的处理器系统开销。

Windows 2000 IPsec策略用IP Security Policy MMC Snap-In进行配置。用这个工具就可以集中设计IPsec策略，然后用活动目录中的OU把这些策略分配给独立计算机或者计算机组。IPsec策略是围绕协商策略和IP过滤器的概念而建立起来的。协商策略决定了你所要包括进去的安全服务，例如要求机密性的和不要求机密性的。ISAKMP/Oakley服务负责协商一个安全相关各方都能接受的策略。通过使用该服务，就可以为每个协商策略设置多个安全服务。过滤功能允许把协商策略用于不同的计算机。IP过滤器决定了能够执行什么操作、是基于单个的还是某个范围内的源与目标IP地址、协议类型，如果合适的话还可以决定单个IP数据报的IP协议端口。你可以定义一个IPsec策略来为一个数据报提供IPsec服务，可以允许它完整通过，也可以将其丢弃。

1.2.6 加密文件系统

通过采用公钥密码技术的磁盘数据加密，Windows 2000中的加密文件系统（EFS）可以保护用户系统中的文件和文件夹免遭非授权的访问。当Windows 2000不能用标准的NTFS ACL提供安全性的时候，这一层次的保护对防止访问敏感数据就是非常必要的。如果硬盘被盗并放入了另一个系统，或者原来的系统改从含有另一操作系统的软盘启动的时候，情况就更是如此。无需任何NTFS权限就可以访问NTFS格式卷中文件的工具，也同样适用于MS-DOS和UNIX操作系统。

数据加密带来了数据恢复的问题，因为对敏感数据执行加密的雇员有可能会跳槽，也有可能会丢失加密密钥。为了防止无法访问公司的数据，数据恢复计划对大多数业务环境来说都是至关重要的。

EFS设计得非常好用，用户只需在Windows Explorer（Windows资源管理器）中从文件夹或文

件的Advanced（高级）属性中选择Encrypt Contents To Secure Data（把内容加密以保护数据），就可以加密单独一个文件或者一个文件夹（包括其当前和将来的内容）。如果一个文件夹被标记为encrypted（已加密），那么所有复制到该文件夹内或在该文件夹内创建的文件都会自动加密。另外，从一个已加密文件夹复制出去的文件仍然是已加密的，这就像那些用支持Windows 2000的备份程序打包的文件一样。但是复制到软盘或其他非NTFS卷的文件和文件夹都会失去加密特性。

EFS的初始发行版并不支持用户之间共享的文件，但是EFS体系结构的设计却使得在以后的发行版本中很容易就能实现这一功能。因此，当前的发行版本最适合保护手持移动系统上的敏感数据，或者只是单用户所需的数据。

这种保护是通过使用公钥密码并利用Windows 2000中的CryptoAPI体系结构来完成的。当启用了EFS时，文件是用一个随机生成的文件加密密钥（FEK）以一种快速对称加密算法进行加密的。EFS的初始发行版采用扩展的数据加密标准（DESX）作为加密算法。自动生成的文件加密密钥随后会用一个或多个公钥进行加密，包括用户的和密钥恢复代理的公钥。因为FEK完全依赖于用户的公钥－私钥对，所以恢复代理不用破坏用户的私钥就可以解密文件内容。EFS既支持对存储在本地驱动器中的文件进行加解密，也支持对存储在远程文件服务器中的文件进行加解密。EFS紧密集成到了NTFS中，提供了一个用户感觉不到读取加解密文件时与原来有何不同的高性能系统。

因为加密是在读写操作期间自动发生的，所以一个已加密的文件在发送给远程系统之前从磁盘读出的时候就被解密，然后在写入远程系统的磁盘时又被重新加密。因此，EFS并没有为传输中的数据提供保护。要想保护传输中的数据就必须使用IPsec等其他的网络安全协议。

可以在活动目录默认域策略（Active Directory Default Domain Policy）中定义你所在组织的Windows 2000 EFS恢复策略，并把该策略委托给域中的所有计算机。作为另一种选择，也可以定义一个涵盖独立OU的策略。默认情况下，由域管理员控制EFS恢复策略。他可以把控制权授予所指派的安全管理员。这就允许你的组织可以具有高级控制和灵活性，而无论是授权谁来恢复潜在敏感的已加密数据。EFS还支持使用多个恢复代理，允许在实现恢复过程时可以有一定的冗余度和灵活性。

更多信息 在家用环境中，当本地管理员第一次登录时，EFS自动产生一个恢复密钥，把本地管理员当作默认的恢复代理。

1.2.7 安全配置工具集

安全配置工具集（Security Configuration Tool Set）为基于Windows 2000系统的安全设置提供了单独的管理点。该工具集允许管理员：

- 在一台或多台基于Windows 2000的计算机上配置安全设置。
- 在一台或多台基于Windows 2000的计算机上执行安全分析。
- 把安全配置当作组策略的一部分来使用。

1. 可配置安全设置

由于Windows 2000中可配置安全参数的多样性，要按照所涉及的系统组件和可能要求变化

的级别来保护基于Windows 2000的网络，将是复杂而繁琐的。安全配置工具集允许在宏（macro）一级的配置，让管理员可以先在一个安全模板中定义大量的安全参数，然后让这些参数在域内自动实现。因此，安全配置工具集实现了特别注重系统安全特定方面的安全工具。该工具集含有下列组件：

- Secedit.exe。可以使用命令行工具Secedit.exe来申请一个安全策略或者初始化一次分析。但是，需要用Security Configuration Manager（安全配置管理器）来显示结果。
- Security Configuration and Analysis（安全配置与分析）。Security Configuration and Analysis MMC Snap-In允许把Security Templates MMC Snap-In中定义的安全配置模板导入安全数据库（Local Computer Policy数据库或任何私有数据库）。通过导入配置就可以建立一个针对机器的安全数据库，然后就可以用于系统。另外，还可以对照数据库中保存的设置来分析系统，两者之间的差别会在图形用户界面（GUI）中显示出来。
- Security Configuration Service（安全配置服务）。Security Configuration Service是安全配置工具集的核心引擎。它可以在所有基于Windows 2000的计算机上运行，并负责工具集提供的所有安全配置和分析功能。
- Group Policy Editor的Security settings 扩展。作为Group Policy Editor（组策略编辑器）的一部分，管理员使用Security Configuration Tool Set把Security setting（安全设置）定义为GPO的一部分。GPO然后就可以分配给域、OU或者活动目录中的特定计算机。GPO可以周期性地重复使用，以保证系统能够连续实施给定的公司安全策略。存为模板的安全配置设置参数可以在Security Configuration Manager与Group Policy Editor之间导入和导出。
- Security Templates（安全模板）。MMC的Security Templates Snap-In允许管理员定义与计算机无关的安全配置（基于文本的.inf模板文件）。
- Setup Security。在Windows 2000操作系统的干净安装期间，安全配置服务执行随系统加载的预定义初始安全配置，创建一个初始安全数据库（即本地计算机策略数据库）。

Security Configuration MMC Snap-In允许管理员定义包括下列几方面内容的安全模板：

- 帐户策略。包括对口令策略、帐户封锁策略和只用于DC的Kerberos策略的安全设置。
- 目录对象。包括对活动目录对象的安全配置设置（只用于DC）。
- 事务日志。包括对事务日志的配置设置。
- 本地文件系统。包括对本地文件系统的访问控制设置。
- 本地策略。包括对审核策略、用户权限分配和计算机安全选项的安全设置。
- 注册表键。包括本地注册表键的访问控制设置和取值。
- 受限组。包括对所选组的组成员身份管理的安全设置，所选组可能会被视为是敏感的，如本地管理员和备份操作员。
- 系统服务。包括对所有本地和网络系统服务的安全启动设置。这一部分的这种设计使得独立软件销售商（ISV）能够对配置和特殊系统服务分析建立附件。

在目录、注册表和本地文件系统的情况下，安全模板保存了对基于对象描述符的安全设置，包括对象所有者、ACL和审核信息。

2. 默认安全设置

随着Windows 2000的发布，微软打算借此机会检查在考虑了授予三种主要用户组——Administrator（管理员）、Power User（高级用户）和User（一般用户）的访问权限与优先权之后的操作系统安全。微软试图根据其预期执行的功能与相应系统访问级别，来更清晰地定义这些工作组的作用。管理员被定义为具有下列功能：

- 安装操作系统。
- 安装服务包和补丁。
- 安装Windows升级。
- 更新操作系统。
- 修复操作系统。
- 在机器范围内配置操作系统的关键参数。

因此，Windows 2000中的默认权限并不限制管理员访问任何注册表和文件系统对象。管理员可以执行操作系统支持的所有功能。另外，管理员还可以为自己分配默认情况下并不具有的任何权力。

一般用户不应该能够损害操作系统和已安装应用的完整性。他们不能修改机器范围内的注册表设置、操作系统文件和程序文件，不能安装可供其他用户使用的程序，也不能运行其他用户安装的程序（这一限制是为了预防特洛伊木马）。但应该能够运行由管理员、高级用户和他们自己先前安装的任何应用程序。实际上，他们也许并不能运行传统的应用程序，因为那些应用程序在过去设计时并没有考虑操作安全性。

高级用户理论上应该能够执行除上面列出的管理员任务之外的任何任务。他们应该能够安装与卸载没有安装系统服务的应用程序。还应该能够定制系统范围内的资源（包括系统时间、显示设置、电源配置和打印机）。实际上，高级用户也许并不能安装传统的应用程序，因为那些应用程序在安装过程中会试图替换操作系统文件。

默认的访问控制设置也已经为Windows 2000进行了重要的检查，不再用Everyone和Authenticated User等工作组（其成员身份由操作系统自动配置）来分配权限（为了向下兼容，也有例外）。而只有其成员身份可由管理员控制的那些工作组才会被采用。

重新定义的默认访问控制设置（干净安装Windows 2000后就是可用的）提供了一个标准的Windows 2000安全环境。一旦使用了符合Windows 2000应用规范的应用程序，就不再需要让用户成为高级用户组的成员，从而进一步增强了安全性。

1.3 小结

本章介绍了Windows 2000分布式安全模型中较为重要的新增安全功能的部分内容。该安全功能由以前版本所不具有的增强安全性的许多方面组成，可以让Windows 2000成为广泛选用的最为安全的操作系统。只要正确使用和管理，Windows 2000就可以帮助改进现存网络与通信方面的安全处理和安全解决方案。