HZ BOOKS

Configuring Windows 2000 Server Security

Windows 技术丛书

Windows

2000

(美) Thomas W. Shinder 等著

王永良 夏雨 张治 等译

Server

配置 Windows 2000 Server 安全

机械工业出版社 China Machine Press

SYNGRESS

Windows 技术丛书

配置 Windows 2000 Server 安全

（美） Thomas W. Shinder 等著

王永良 夏 雨 张 治 等译

机械工业出版社
China Machine Press

本书全面细致地介绍了 Windows 2000 Server 在控制系统安全方面的功能。内容包括：Windows 2000 Server 移植方法，检测默认的访问控制设置，Windows 2000 操作系统中全新的安全特性，快速实现 Windows 2000 安全的方案。本书的作者都是研究 Windows 2000 Server 的专家，专门针对 Windows 2000 Server 的系统安全进行了深入细致的描述。本书对 IT 经理和系统管理员在实现 Windows 2000 环境中的安全性具有重要指导作用。

本书版权登记号：图字：01-2000-1920

图书在版编目（CIP）数据

配置 Windows 2000 Server 安全/（美）顺德（Shinder，T.W.）等著；王永良等译．-北京：机械工业出版社，2001.9
（Windows 技术丛书）
书名原文：Configuring Windows 2000 Server Security
ISBN 7-111-09284-8

Ⅰ.配… Ⅱ.①顺… ②王… Ⅲ.服务器－操作系统（软件），Windows 2000 Server Ⅳ.TP316.86

中国版本图馆 CIP 数据核字（2001）第 055717 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：刘卫宏　张鸿斌
北京市密云县印刷厂印刷・新华书店北京发行所发行
2001 年 9 月第 1 版第 1 次印刷
787mm×1092mm1/16・13 印张
印数：0 001-5 000 册
定价：26.00 元

译 者 序

在当今的计算机网络应用中，安全是最重要的因素。随着公众上网人员的增多，电子商务的迅猛发展，各个组织必须使用不同的方法来保护自己的网络不被入侵，保证数据不被窃取。需要保护的数据有很多，例如：自己的数据（如新产品信息），合作伙伴的数据（如保密协议），客户的数据（如信用卡信息）等。因此，Windows 2000 Server 强大的安全保护功能显得格外重要。

Windows 2000 Server 的功能十分强大，它增强了 Windows 的网络安全性，几乎包含了目前计算机网络（尤其是 Internet）的所有新技术，其优秀的性能越来越受到广大企业和用户的青睐。本书全面细致地介绍了 Windows 2000 Server 在控制系统安全方面的功能，在 Windows 2000 Server 的系统安全方面进行了深入细致的描述。

本书共分十章，第 1 章讨论 Windows 2000 Server 移植方法，第 2 章讨论检测默认的访问控制设置，第 3 章到第 9 章详细说明了 Windows 2000 Server 操作系统中全新的安全特性，第 10 章提供了一个快速实现 Windows 2000 Server 安全的方案。

本书的主要读者对象为 IT 人员和系统管理员。对于那些想了解 Windows 2000 Server 全新安全特性的人员也是很好的参考书。

参加本书翻译工作的成员有：王永良、夏雨、张治、沈国鹏、秦玉洁、张伟、曹迎槐、买建英等人，全书由李蕾、冯燕奎、夏雨负责审校。参加本书部分翻译和校对工作的人还有田宝水、张义，王佳星、边洪元、薛峰、童建国、许刚、辛生发、张鲁垣、吕彦州等同志，参加文字录入工作的有孙标、鲍华、张有中、彭一庆、李英、王和菊、刘有章、张和、陶玉、李金根、张健英、周学冠、刘倚等。

由于时间有限，尽管我们付出了极大的努力，也难免有不当之处，恳请广大读者批评指正。

2001 年 1 月

前　言

安全对于计算机网络来说是很重要的。然而，在最近几年中，随着公众上网人员的增多，各个组织机构纷纷把私有的网络连进 Internet，并且电子商务迅猛发展，网络的景观大大改变了。各个组织必须使用不同的方法来保护自己的网络不被入侵，保证数据不被窃取，例如自己的数据（如新产品信息）；合作伙伴的数据（如保密协议）；客户的数据（如信用卡信息）等。

在过去，只有研究人员和科学家使用 ARPANET，与之形成鲜明对比的是，现在公共访问 Internet 的现象巨增，因此网上也出现了许多“Script Kiddies”，这些“Script Kiddies”可以非常容易地获取他们想要搜寻的黑客工具，因为这些工具在一些地下网站可以自由地获取，因此他们不必对编程语言和 UNIX 有深层次的了解，可以直接利用黑客软件闯入某个组织的网络。

面对这些黑客带来的威胁，IT 人员（Mananger）以及系统管理员（Administrator）能做些什么呢？为了确保安全的管理而将所有的连接断开？对于一个机构来说，网络对其目标的实现有着战略性的意义；在某些情况下，还能帮助维护其竞争优势。那么必须更改现有的操作系统吗？大可不必，尽管每个操作系统都声称自己拥有多么高的完备性，但总是或多或少地存在一些安全漏洞。唯一安全的办法是把计算机锁在一个没有窗户的房间里，不开机、不上网！IT 人员和系统管理员必须保证他们所采取的预防措施能保障网络安全。

在 Windows 2000 Server 强有力安全性的保护之下，组织和管理网络及其安全变得更加容易了；Windows 2000 Server 极大地增强了基于 Windows 的网络安全性。但这还只是一个阶段性的进步。举个例子来说，用于定义文件加密系统钥匙的大小必须随着技术的发展而增大，这对于由文件加密系统保护的信息的完整性是十分重要的。虽然各个组织已经把 Windows 2000 Server 扩展到了企业层次，难道这就意味着安全吗？不！网络策划者和 IT 经理必须正确积极地使用 Windows 2000 Server，才可以为他们组织的特定目的的实现提供安全标准。这种实现必须是经过慎重考虑的，这也就是网络安全计划非常重要的原因。在这里我不能更多地强调网络安全计划的重要性，但是可以想像 Windows 2000 Server 也有可能受到来自某些机构的压力，这些机构没有花费足够的时间去制定一个网络安全计划就仓促地付诸实践，从而表现出对 Windows 2000 Server 的不满。

组织结构

本书第 1 章讨论 Windows 2000 Server 移植方法；在第 2 章讨论检测默认的访问控制设置；第 3 章到第 9 章详细地说明了 Windows 2000 操作系统中全新的安全特性；第 10 章提供了一个快速实现 Windows 2000 安全的方案。

第 1 章为 Windows 2000 Server 的安全特性提供了一个简要的描述，测试了 Windows 2000 Server 的安全性，同时对升级和移植也进行了充分考虑，最后对网络安全计划作了一番讨论。

第 2 章讨论了在 Windows 2000 Server 安装过程中配置的有关文件系统和注册表的访问控制设置，还讨论了默认的用户权限以及不同的内置组成员。

第 3 章介绍了 Kerberos 协议和在 Windows 2000 Server 中使用 Kerberos 协议的细节。

第 4 章讨论了 Windows 2000 的分布式安全服务。包括活动目录及其安全，多重安全协议，企业的 Internet 单独注册以及远程合作伙伴的商业访问。

第 5 章深入探讨 Windows 2000 中使用的安全设置工具集。包括设置安全特性，分析安全性，组策略的综合以及工具的使用。

第 6 章讨论文件加密系统。由使用 EFS 开始，然后到用户操作，最后深入地讨论 EFS 框架组成。

第 7 章有关 IPSec 的讨论。包括网络攻击方法简介、IPSec 框架，最后以组织所在机构的 Windows IPSec 作为总结。本章还包含了一个实践中的例子。

第 8 章深入地讨论了 Windows 2000 中智能卡的使用，包括交互操作性、基于组件的智能卡以及增强的解决方案。

第 9 章首先讨论了公钥基础结构的概念，然后讨论了一个 Windows 2000 公钥基础结构的组件，包括证书的颁发，激活域客户以及公钥安全策略。本章以一个实际应用和为 Windows 2000 PKI 准备的指令集作为结束。

第 10 章提供了一个 Windows 2000 安全的快速方案以及需要了解的原因。本章包含了 Windows NT 安全的历史回顾以及 Windows 2000 中重要的特性以及设计更改的信息。

读者对象

本书主要的读者对象为 IT 人员和系统管理员。他们一般都需要对 Windows 2000 环境中的安全性负责。当然，本书对于那些想了解 Windows 2000 Server 全新安全特性的人员也是很好的参考书。那些想要快速理解本书中包含信息的读者可以先阅读第 10 章。

本书英文原书书名：Configuring Windows 2000 Server Security
原书书号：ISBN 1-928994-02-4
相关网址：Solutions@Syngress.com

作者介绍

Stace Cunningham（CCNA，MCSE，CLSE，COS/2E，CLSI，COS/2I，CLSA，MCPS，A+）是微软公司在 Biloxi 的系统工程师兼 SDC 顾问。他曾经是设计和实现一个由 12 000 个结点组成的企业网络的主力。在美国空军服役期间，曾担任网络安全指挥官和计算机系统安全指挥官。他也是技术手册“Windows NT Security Step by Step”的积极投稿者。自从微软发布了 Windows 2000 Beta1 版以来，Stace 就开始使用 Windows 2000，并且对该系统提供的新的安全特性感到高兴。

Stace 曾经以技术撰稿人的身份参与了 IIS3.0 的测试、SMS1.1 的测试、Proxy Server 1.0 的测试、Exchange Server 5.0 和 5.5 的测试、Proxy Server 2.0 的测试、IIS4.0 的测试、IEAK 的测试以及 Windows 95 修订版的测试。另外，他还与人合著了 16 本由微软出版社、Osborne/McGraw-Hill 和 Syngress Media 出版的书，同时还担任了一些由微软出版社、Osborne/McGraw-Hill 和 Syngress Media 出版的书籍的技术评论员。

他的妻子 Martha 和女儿 Marissa 非常支持他将很多时间花在家里的计算机网络上。没有她们的爱和支持，他就不能达到为自己设立的目标。

Debra Littlejohn Shinder（MCSE，MCP+I，MCT）是在 Dallas Country Community College District 的 Eastfield College 的 AATP 任教的讲师。她从 1992 年开始执教。她是德克萨斯 Seagoville 和 Sunnyvale 两个城市的 Webmaster，同时还是家庭网站 www. shinder. net 的 Webmaster。她和她的丈夫 Thomas W. Shinder 博士为 Dallas 地区的组织提供顾问和技术支持。她同时还是女儿 Kristen 和儿子 Kris 引以为荣的妈妈，Kristen 现在在美国驻意大利海军服役，Kris 夺得了高中的象棋冠军。Deb 写了许多有关她生活的事情，在技术领域和非技术领域发表了许多文章。您可以通过 deb@shinder. net 与她联系。

Thomas W. Shinder，M. D.（MCSE，MCP+I，MCT）是 Dallas-Ft. Worth Metropkx 公司的技术培训者兼顾问。他曾担任一些主要的公司诸如 Xerox、Lucent Technologies 和 FINA Oil 公司的顾问，帮助它们开发和实现基于 IP 的通信策略。Dr. Shinder 曾在芝加哥的 Illinois 大学的医学院上学，并在波兰的 Oregon Health Sciences Center 接受过泌尿学的培训。他对研究神经元间通信的强烈爱好和他对互联网络的兴趣使他取下了诊所的招牌，而致力于系统工程。Tom 与他妻子 Deb Shinder 热情地工作，为基于 Windows NT/2000 平台的中小型商业系统提供一流的有效使用资金的解决方案。

Brian M. Collins（MCNE，CNI，MCSE，MCT，CTT）是 NetWork Appliance（NASDAQ：NTAP）公司的技术培训员，该公司是 Network Attached Storage 的主要提供者，Brian 还是他自己的公司 Collins Network Engineering 的培训员和顾问。Brian 是一个有着 18 年经验的技术老手，他曾经担任网络工程师、培训员、软件开发人员和政府顾问，为 500 个公

司的和小商业带来了利润。他的爱好有步行、高尔夫以及操作系统。Brian 住在加利福尼亚州的 Boulder Creek 的红木森林，距离加州的硅谷 30 英里远。

D. Lynn White（MCPS，MCSE，MCT，MCP + I）是 Independent Network Consulatants 公司的主席。在编程和网络方面拥有 14 年的工作经验，已经成为大型机环境中的系统管理者并且是一家过程控制公司的高级软件工程师。在网络领域和计算机相关技术领域是专业的技术作家、编辑和顾问。12 年来，无论在美国国内还是在国外，Lynn 已经发表了关于大型机、微软官方培训课程和其他网络课程的大量著作。

Garrick Olsen（A + ，Network + ，MCP + I，MCSE + I，CNE）现在担任 Alaska Anchorage 的 MicroAge 公司的网络技术人员。若有问题或建议可以通过 golsen@gci．net 发送给他。

目　录

第 1 章　Windows 2000 Server 安全的移植

本章解决的问题：

- Windows 2000 Server 安全特性概述
- Windows 2000 Server 安全白皮书

1.1　Windows 2000 Server 安全特性概述

为什么必须对网络安全特性有所了解呢？有几个原因。第一，必须确保只有经过授权的用户才可以访问网络。如果没有这一层的保障，那么任何人都可以访问网络资源，一些重要的数据就有可能会被窃取。第二，即使网络使用了安全登录，仍需要一种机制来防止没必要的访问。例如，市场部的职员没有必要访问工薪部的数据。这两种机制可以帮助保护网络资源避免被破坏或非授权访问。随着网络的进一步发展，各种机构更加依赖于网络安全，这就必须实施额外的保护，以确保网络的完整性。

随着 Windows 2000 Server 的发布，Microsoft 网络操作系统的安全性大大的提高了。从该版本的改进可以看出来，即使象 Microsoft 的这种软件巨人也十分重视安全性。这些新的特性包括：

- 授权内部用户和外部用户的多种方法。
- 使用加密保护存储在磁盘上的数据。
- 使用加密保护数据在网络之上传输。
- 对象各属性的访问控制。
- 验证用户安全证书的智能卡。
- 域间信任关系。
- 公钥基础结构（PKI）。

1.2　Windows 2000 Server 安全白皮书

Windows 2000 Server 的安全性超过了所有网络操作系统以前的版本。在今天这种多变的环境中，网络操作系统可以提供的安全特性越多，使用它的机构就会得到更多的好处。因为各机构非常依赖于他们的信息系统。

1.2.1　为什么 Windows 2000 要改进安全性

随着越来越多的机构使用 Windows 操作系统进行事务处理，Windows 2000 Server 对安全性的改善就显得十分必要了。一个操作系统在行业中使用的越为广泛，那么受到攻击的可能性就越大。随着 Windows NT 在工业中应用的推广，它的弱点也就更多地暴露在攻击之

下。LOpnt Heavy Industries 曾经演示了攻击局域网管理器（LM）时 Windows NT 的密码加密系统是如何的脆弱。当某一个用户登录时，因为局域网管理器默认发送重述信息密码很容易被破解。幸亏 LOpnt Heavy Industries 及时发现了 Windows NT 上的这个漏洞！Microsoft 发布了一个服务补丁包来修正 NT 中的这个漏洞。在 Windows 2000 Server 中，它用 Kerberos V5 为所有基于 Windows 2000 域控制器的网络替换了原来默认的身份验证。

1.2.2 Windows 2000 Server 安全特性与早期版本的不同之处

Windows 2000 Server 安全性的增强的一个方面就是 Windows 2000 Server 支持两种身份验证协议：Kerberos V5 和 NTLM（NT 局域网管理器）。Kerberos V5 是 Windows 2000 域默认的身份验证方法。提供 NTLM 是为了向下兼容 Windows NT 4.0 和更早的操作系统以及所有 Windows 2000 网络上的其他计算机（见第 3 章，“Kerberos Server 身份验证”）。

另一个安全增强方面是文件加密系统（EFS）。EFS 允许用户对系统中的文件进行加密-解密，对文件提供了比只用 NTFS 更高的保护（见第 6 章，“Windows 2000 的文件加密系统”）。

包含在 Windows 2000 Server 中的 IPSec 增强了数据在网络传输时对完整性和保密性的保护。显而易见，今天的网络不仅仅包含企业内部的网络，还包含有分支机构以及差旅人员远程访问，当然还有 Internet（见第 7 章，“Windows 2000 Server 的 IP Security”）。

在 Active Directory 中的每一个对象能在十分细微的层次上拥有授权控制。这种属性层次的授权控制可以在活动目录的所有层次使用（见第 4 章，“使用 Windows 2000 分布式安全服务进行安全的网络通信”）。

Windows 2000 Server 支持智能卡以提供对客户身份验证以及 E-Mail 的额外保护。添加额外保护层的原因是假如有黑客想要入侵网络，那么他必须有智能卡以及个人标识号码（PIN）（见第 8 章，“智能卡”）。

可传递信任关系是 Kerberos V5 操作特性之一，可自动设定并维护。信任的传递依赖于 Kerberos V5。所以只能在基于 Windows 2000 Server 的域中起作用（见第 4 章）。

Windows 2000 Server 很大程度上依赖于公钥基础结构（PKI），PKI 由如下几个组件组成：公钥、密钥、证书以及证书颁发机构（CAs）（见第 9 章，“Windows 2000 公钥基础结构 PKI”）。

IT 专业人员参考——域用户管理器在什么地方

在 Active Directory 中，网络管理工具有一些变动。对于用户和组的管理有一些新的方法。每一个熟悉使用 Windows NT 4.0 以及老版本用户管理器的用户如今在 Windows 2000 域中管理对象时必须习惯于使用管理控制台（MMC）中管理单元——“Active Directory 的用户和计算机”这一工具。MMC 中嵌入了用于管理 Windows 2000 Server 环境的几种新工具，如服务质量控制以及分布式文件系统。MMC 中也包含了以前的工具，比如性能监视器和事件查看日志。表 1-1 列出了这些工具在 Windows NT 4.0 中和 Windows 2000 Server 中不同使用方法。

表 1-1　Windows NT 4.0 和 Windows 2000 Server 中使用的工具

Windows NT 4.0	Windows 2000 Server
域用户管理器	“Active Directory 的用户和计算机”用于修改用户账户。安全设置编辑器用于设置安全策略
系统策略编辑器	组策略的管理模板扩展用于基于注册表的策略配置
添加用户账号（管理向导）	“Active Directory 的用户和计算机”用于添加用户
组管理器（管理向导）	“Active Directory 的用户和计算机”用于添加组，组策略增强了策略集
服务管理器	由“Active Directory 的用户和计算机”代替

1.2.3　涉及的问题与限制

Windows 2000 Server 保持了对低版本 Windows NT 4.0、Windows 95、Windows 98 的兼容性，所以它也使用 NTLM 和 LM 身份验证登录。这就意味着强大的 Kerberos V5 身份验证还没有用于那些低版本的系统。在 Windows 2000 中 NTLM 和 LM 仍旧使用，使得那些低版本的系统用户的口令可以被认同。

Windows 2000 不支持在 Service Pack 4 for Windows NT 4.0 中发布的 NTLMV2。图 1-1 显示了一个捕获 Windows 98 客户登录到 Windows 2000 Server 域的数据包。Windows 98 机器正在发送广播 LM 1.0/2.0 登录请求。

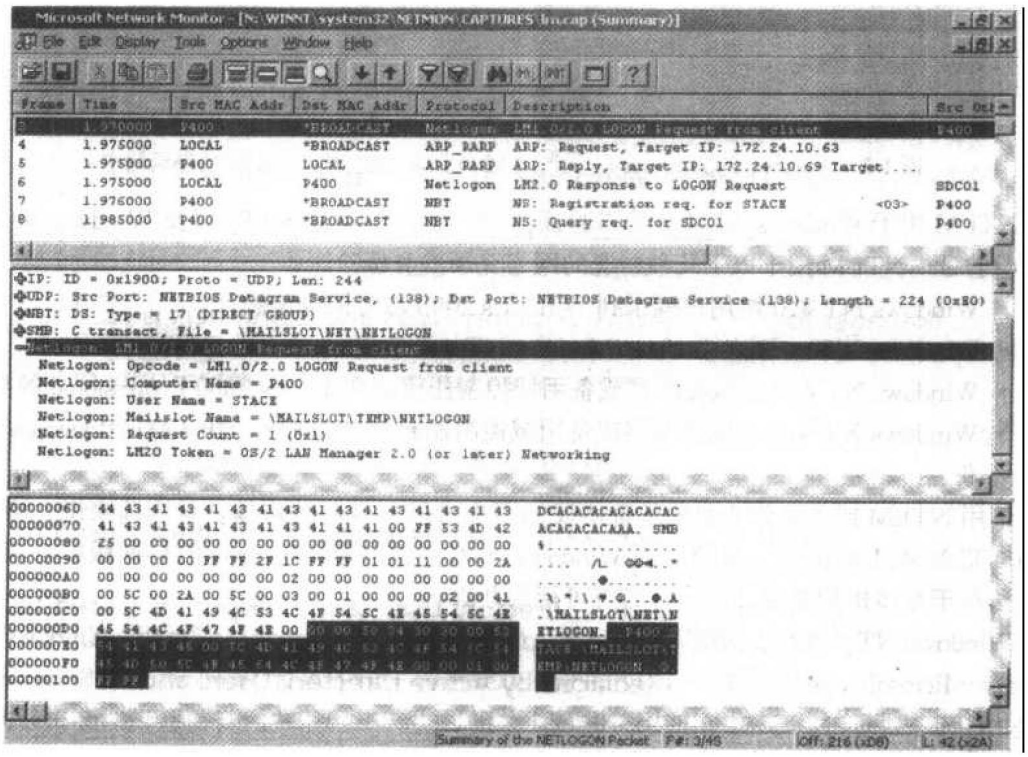

图 1-1　Windows 98 客户发送 LM 1.0/2.0 的登录请求

图 1-2 演示了 Windows 2000 Server 响应 Windows 98 客户机的请求。该 Windows 2000

Server 以一个 LM2.0 回应来响应该登录请求。

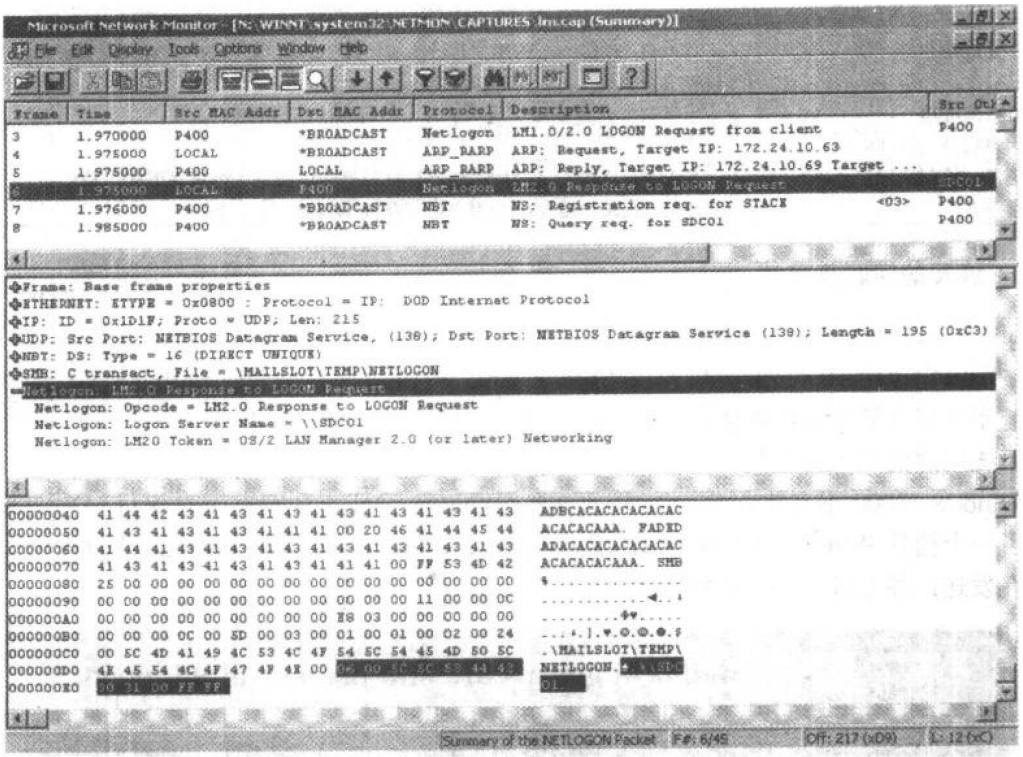

图 1-2 Windows 2000 Server 以一个 LM 2.0 回应响应 Windows 98 的登录请求

NTLM 用于 Windows NT 4.0 身份验证，LM 则用于 Windows 95 以及 Windwos 98 系统的身份验证。NTLM 用于以下几种情况的网络登录的身份验证：

- Windows NT 4.0 域用户登录到 Windows 2000 域时的身份验证。
- Windows 2000 域控制器验证 Windows NT 4.0 Workstation 的身份。
- Windows NT 4.0 主域控制器或备用域控制器验证 Windows 2000 Professional 的身份。
- Windows NT 4.0 主域控制器或备用域控制器验证 Windows NT 4.0 Workstaion 的身份。

使用 NTLM 或 LM 作为身份验证协议的困难阶段不容易被跨越。就当前来说，要避免使用 NTLM 或 LM 的唯一途径是用 Windows 2000 系统替换 Windows 的早期版本。但是这种方法对于很多机构来说并非一件经济可行的办法。

Windows NT 3.51 有一些其他的问题，尽管可以将 Windows 3.51 升级到 Windows 2000 Server，Microsoft 却不赞同在一个 Windows 2000 Server 域中运行 Windows NT Server 3.51。这是由于 Windows NT 3.51 在使用登陆域之外的域进行组和用户的身份验证时会出现问题。

1.2.4 Windows 2000 Server 与早期 Windows 版本的相同之处

Windows 2000 Server 比早期的 Windows 版本多出了数百万行的代码，所以很难让人相

信和早期的版本有相同之处。由于 Windows 2000 Server 必须支持早期版本的用户，所以它的 NTLM 和早期的版本相同。

除了增加一个额外的组之外，全局组和本地组在 Windows 2000 Server 中依然存在。

内建的组，诸如 Backup operator、Account Operator、Server Operator、Print Operator 以及 Administrator 依然存在。新的 NTFS5 中依旧提供 NTFS 权限。

除上述之外，为了系统更加安全，这个全新的操作系统拥有许多更新的安全特性和功能，需要系统管理员进行学习。

1.2.5 升级/移植方面的考虑

从 Windows NT 4.0 升级/移植到 Windows 2000 Server 与从 Windows NT 3.51 升级/移植到 Windows NT 4.0 完全是两码事。Windows 2000 Server 包含了一些在 Windows NT 早期版本中没有的新的安全特性。因此在实现升级之前，必须考虑清楚从这种全新的操作系统中得到的利益的多少。

1.2.6 网络安全计划

在升级/移植到 Windows 2000 Server 之前需要考虑的安全项目便是开发一个网络安全计划。如果没有这个计划，将不能有效的利用 Windows 2000 Server 中的工具来构件一个安全网络。根据网络的大小，可能需要不止一个网络安全计划。分布在全球各地的不同机构可能需要不同的安全计划来满足不同的需要。小一点的机构可能只需要一个单独的计划。无论网络有多大，一个网络安全计划总是很重要的。Microsoft 建议网络安全计划至少应该包含以下几步：

- 安全组计略。
- 安全组策略。
- 网络登录与身份验证计略。
- 信息安全计略。

安全组计略用于规划三种类型组的使用：通用组，全局组和本地组。通用组是在 Windows NT 4.0 中未曾提供的新组，所以需要保证已经将它列入到计划考虑之中。当构建网络规划时，需要考虑如何使用存在的内建组以及明确需要创建什么样的组。

当为机构制定完必要的组计略之后，下一步需要完成的就是安全组策略。它包括：Active Diretory 对象、文件系统、注册表、系统服务、网络账户、本地计算机、事件日志以及受限组。组策略筛选器可以控制上述每一个项目。最好尽量精简组策略的数目，因为在计算机启动和用户登录时，它们会被下载到每一台计算机之上以及每一个用户的配置文件中（见第 5 章，“安全配置工具设置”）。

计划中的第三步是为机构计划必要的网络登录和身份验证计略。到底机构中用户使用的是 Kerberos 登录？NTLM 登录？智能卡登录？还是使用证书映射？根据机构网络的组成，Windows 2000 Server 既能够在混合模式（mixed model）下操作，也能够在本机模式（native model）下操作。而 NTLM 不能在本机模式下操作（见第 4 章）。