NT Network Security

Windows NT网络的安全性

Matthew Strebe
〔美〕 Charles Perkins 著
Michael G. Moncur

严程 张芳兰 田立生 译

杨为理 审校

電子工業出版社
Publishing House of Electronics Industry

内 容 提 要

本书全面而系统地介绍了计算机网络，特别是Windows NT网络安全领域的知识，包括对人为安全性、用户安全性、客户机安全性、服务器安全性及物理安全性、数据安全性与组网和远程访问安全性等诸多方面都作了简明扼要的论述，并提供了丰富的实用安全工具及实例分析与应用经验。

本书适合于从事计算机与综合信息网络工程和应用方面的技术人员作为学习参考书。

书　　名：**Windows NT网络的安全性**

著　　者：〔美〕Matthew Strebe　Charles Perkins　Michael G. Moncur

译　　者：严程　张芳兰　田立生

审　　校：杨为理

责任编辑：章为华

印 刷 者：北京天竺颖华印刷厂

装 订 者：三河金马印装有限公司

出版发行：电子工业出版社出版、发行

北京市海淀区万寿路173信箱　邮编：100036　发行部电话：68279077

北京市海淀区万寿路甲15号南小楼一层　邮编：100036　发行部电话：68215345

URL:http://www.phei.com.cn

经　　销：各地新华书店经销

开　　本：787×1092 1/16　印张：26.75　字数：700千字

版　　次：1999年1月第1版　1999年1月第1次印刷

书　　号：ISBN 7-5053-4374-2/TP・2010

定　　价：45.00元

著作权合同登记号　图字：01-98-0477

致　谢

我的妻子很贤惠，她耐心地等待了几年，使我完满地写成此书，继续正常的生活，她的支持给我极大的力量。衷心感谢我的两位最亲密的老朋友Mike Moncur和Charles Perkins，没有他们的帮助，这本书不可能这么快就得以出版。Sybex出版公司的工作人员为此书付出的努力甚至比作者还大。此外，还应感谢Neil、Maureen、Guy、Shelby、Vivian和Jim等人（及Rodnay Zaks，他的著作是我拥有的第一本计算机书，而且至今仍在使用），也许应当由他们来写这方面的书籍。我的家人给予我很大的支持，特别是Roy和Carol、Lee和Donna、Terry和Sharee。还应感谢我的兄弟姐妹们：Daan与Fukiko、Rachel与Kerry、Ruth与James、Chris与Phyllis、Jacqui与Bob、Duane、Gretchen与Paul、Susan与Jimm、Victor、Doug与Colleen、Margaret与Richard、David与Debbie、Don与Christine、Sharon与Ken、Linda、Scott与LeAnn、Dennis、William与Kori、Rachelle、Brent及LoraLee等。

感谢Mike，并感谢我的家人和朋友，他们为我提供了安静的环境、使我保持旺盛的精力投入写作。感谢Sybex出版公司的人们，他们一如既往，热情鼓励我写这本书，特别是Henry J. Tillman。

感谢Matthew和Charles对我写此书的帮助并为我提供参与此项工作的机会。也应感谢Sybex出版公司的工作人员，帮助我出版此书，特别是Neil Edde、Maureen Adams和Shelby Zimmerman。还要感谢Kate Kaminski、Eryn Osterhaus、Andrew Benzie、Molly Sharp和Dale Wright，他们为此书的出版作了大量的工作，包括设计和制作插页、封面、装饰图及CD-ROM等。由于编辑Vivian Perry的帮助，使本书的叙述更加清晰与确切。技术评论者Jim Polizzi提出了许多宝贵的意见和建议。我要再一次感谢我的妻子Laura及我的家人：爸爸、妈妈与Kristen、Matt、Mel、Ian。尤其要感谢我的祖母和外祖母Alice Moncur、Edna Tippets对我的爱和支持。也要向我的所有朋友致谢：Matt和Christy、Chuck、Cory和Kathleen、Dylan与Joan、Robert、Curt、James及Henry。

引　言

在各种规模的网络中，Windows NT业已成为一种最流行的网络操作系统。网络管理员最关心的问题之一是网络安全。

本书全面介绍了Windows NT网络的安全性问题，从基本的注册或登录安全到因特网（Internet）安全与防火墙（firewall），也包括了一般的安全论题（如加密技术）和人为安全性问题。

本书的读者和对象

此书是为网络管理人员而编写的，他们或许正工作于Windows NT网络，或许计划在某个时期使用Windows NT系统。本书的目的不是要写一本Windows NT的安全性指南，而是想对Windows NT网络的各个安全方面作概括性介绍。

在本书中，我们将认真分析Windows NT安全的长处和弱点，提供一些安全方面的建议，其范围包括从小公司所需的简单安全措施到大公司与政府机构所要求的复杂而完美的安全机制。

这本书对任何管理Windows NT网络的人，不管其经验和水平如何，都是有用的。然而在此我们仍作几点假设：

- 读者熟悉计算机的基础知识，对Windows NT或至少对Windows 95有一定程度的了解。本书不介绍Windows NT的安装、网络连接及完成其它基本任务方面的内容。
- 如果读者希望进行安全方面的实践或实现我们的建议，应能以管理者身份访问Windows NT网络。我们也介绍其它网络系统的某些问题，但Windows NT是本书的重点。

如何使用此书

本书的内容分别组织到二十二章和四个附录中，以安全性简介开始，逐章讲述其它更深入的问题。

第1章　为安全基础简介及在网络中应考虑的安全类型。

第2章　说明人为的安全性，即由用户的行为所引起的安全问题。

第3章　介绍各种加密方法及如何将其应用于网络安全规划中。

第4章　描述成功的安全管理所需要的技术与资源。

第5章　深入了解Windows NT的安全性模型及其组成部分。

第6章　说明如何建立、保存用户帐号和分配权限。

第7章　介绍系统的策略，用于控制对操作系统内各功能的访问。

第8章　说明如何利用文件系统的安全性来控制对文件和目录的访问。

第9章　介绍工作组和共享件，这是内建于Windows NT的两种简单、但不太安全的系统。

第10章 讨论域安全性和信任关系及较大型网络的Windows NT安全措施。

第11章 说明如何利用容错方法（如磁盘镜像与备份）防止意外的数据丢失。

第12章 讨论与远程访问服务（拨号访问Windows NT网络）有关的网络安全问题。

第13章 概述多厂家网络的安全问题，包括UNIX、NetWare和Macintosh的安全性

第14章 介绍因特网（Internet）、内联网（intranet）和外联网（extranet）及它们的安全性。

第15章 介绍TCP/IP协议簇及与其有关的安全风险。

第16章 研究某些可用于客户计算机与应用程序的安全方法。

第17章 介绍防火墙，它是用于控制局部网络与因特网间安全性的设备。

第18章 介绍Microsoft BackOffice的几个部分，如Internet Information Server等，并说明它们与安全性的关系。

第19章 探讨某些可被黑客利用的高层缺陷和安全漏洞及防止攻击的措施。

第20章 说明网络层和数据链路层存在的安全危险及如何防止它们。

第21章 介绍保证Windows NT服务器安全的各种方法。

第22章 说明与OSI模型物理层有关的安全问题。

附录A 提供某些典型的安全政策与原则。

附录B 给出一些安全工具或实用程序。

附录C 给出一些影响网络安全及有价值的联机资源。

附录D 列出常用词汇表。

虽然我们希望读者能够通读此书，但也可把它作为一般的参考书使用。例如，当你要建立用户帐号时，可阅读第6章；当你欲将网络连到因特网时，可阅读第14章、第17章。

在大多数章节中，包含三种有特色的插入段：

专用名词（terminology） 列出某些与本章有关的术语，其定义可参见本书后所附词汇表。

策略（policies） 为保证网络某些方面的安全，我们所提出的建议。

实际考察（reality check） 我们曾经遇到的一些现实的安全方面的趣事，这些故事告诉你在实际网络中会遇到的情况及应有的概念。

保持联系

有关网络安全领域的技术与应用处于迅速发展之中。为使读者能够获得最新的、确切的安全方面信息及更广泛的知识，本书的附录C列出一些联机资源，并提供Web页面，利用地址

```
http://www.starlingtech. com/ntsecurity/
```

可访问NT安全性页面。你也可通过电子邮件与我们联系，我们很乐意听到你对本书的评论意见及有关安全方面的趣事与故事。并将尽力回答你有关NT安全方面的问题。我们的电子邮件地址是

```
ntsecurity@starlingtech.com
```

目　录

引　言

在各种规模的网络中，Windows NT业已成为一种最流行的网络操作系统。网络管理员最关心的问题之一是网络安全。

本书全面介绍了Windows NT网络的安全性问题，从基本的注册或登录安全到因特网（Internet）安全与防火墙（firewall），也包括了一般的安全论题（如加密技术）和人为安全性问题。

本书的读者和对象

此书是为网络管理人员而编写的，他们或许正工作于Windows NT网络，或许计划在某个时期使用Windows NT系统。本书的目的不是要写一本Windows NT的安全性指南，而是想对Windows NT网络的各个安全方面作概括性介绍。

在本书中，我们将认真分析Windows NT安全的长处和弱点，提供一些安全方面的建议，其范围包括从小公司所需的简单安全措施到大公司与政府机构所要求的复杂而完美的安全机制。

这本书对任何管理Windows NT网络的人，不管其经验和水平如何，都是有用的。然而在此我们仍作几点假设：

- 读者熟悉计算机的基础知识，对Windows NT或至少对Windows 95有一定程度的了解。本书不介绍Windows NT的安装、网络连接及完成其它基本任务方面的内容。
- 如果读者希望进行安全方面的实践或实现我们的建议，应能以管理者身份访问Windows NT网络。我们也介绍其它网络系统的某些问题，但Windows NT是本书的重点。

如何使用此书

本书的内容分别组织到二十二章和四个附录中，以安全性简介开始，逐章讲述其它更深入的问题。

第1章　为安全基础简介及在网络中应考虑的安全类型。

第2章　说明人为的安全性，即由用户的行为所引起的安全问题。

第3章　介绍各种加密方法及如何将其应用于网络安全规划中。

第4章　描述成功的安全管理所需要的技术与资源。

第5章　深入了解Windows NT的安全性模型及其组成部分。

第6章　说明如何建立、保存用户帐号和分配权限。

第7章　介绍系统的策略，用于控制对操作系统内各功能的访问。

第8章　说明如何利用文件系统的安全性来控制对文件和目录的访问。

第9章　介绍工作组和共享件，这是内建于Windows NT的两种简单、但不太安全的系统。

第10章 讨论域安全性和信任关系及较大型网络的Windows NT安全措施。

第11章 说明如何利用容错方法（如磁盘镜像与备份）防止意外的数据丢失。

第12章 讨论与远程访问服务（拨号访问Windows NT网络）有关的网络安全问题。

第13章 概述多厂家网络的安全问题，包括UNIX、NetWare和Macintosh的安全性

第14章 介绍因特网（Internet）、内联网（intranet）和外联网（extranet）及它们的安全性。

第15章 介绍TCP/IP协议簇及与其有关的安全风险。

第16章 研究某些可用于客户计算机与应用程序的安全方法。

第17章 介绍防火墙，它是用于控制局部网络与因特网间安全性的设备。

第18章 介绍Microsoft BackOffice的几个部分，如Internet Information Server等，并说明它们与安全性的关系。

第19章 探讨某些可被黑客利用的高层缺陷和安全漏洞及防止攻击的措施。

第20章 说明网络层和数据链路层存在的安全危险及如何防止它们。

第21章 介绍保证Windows NT服务器安全的各种方法。

第22章 说明与OSI模型物理层有关的安全问题。

附录A 提供某些典型的安全政策与原则。

附录B 给出一些安全工具或实用程序。

附录C 给出一些影响网络安全及有价值的联机资源。

附录D 列出常用词汇表。

虽然我们希望读者能够通读此书，但也可把它作为一般的参考书使用。例如，当你要建立用户帐号时，可阅读第6章；当你欲将网络连到因特网时，可阅读第14章、第17章。

在大多数章节中，包含三种有特色的插入段：

专用名词（terminology） 列出某些与本章有关的术语，其定义可参见本书后所附词汇表。

策略（policies） 为保证网络某些方面的安全，我们所提出的建议。

实际考察（reality check） 我们曾经遇到的一些现实的安全方面的趣事，这些故事告诉你在实际网络中会遇到的情况及应有的概念。

保持联系

有关网络安全领域的技术与应用处于迅速发展之中。为使读者能够获得最新的、确切的安全方面信息及更广泛的知识，本书的附录C列出一些联机资源，并提供Web页面，利用地址

```
http://www.starlingtech. com/ntsecurity/
```

可访问NT安全性页面。你也可通过电子邮件与我们联系，我们很乐意听到你对本书的评论意见及有关安全方面的趣事与故事。并将尽力回答你有关NT安全方面的问题。我们的电子邮件地址是

```
ntsecurity@starlingtech.com
```

目　录

第1章　安全性概念和术语

安全性是联网技术中最关键、最容易被忽视的问题之一。许多公司建立了庞大的网络，并且使用了多年，但是从未关心过它的安全性，直到某一天网络发生灾难性的瘫痪或是安全方面出现了漏洞、事故，才不得不关心并采取安全措施。本书将讨论安全性诸多方面的问题，以预防事故的发生。

本章将讨论安全性的基础知识和解决安全问题常用的方法。还将介绍公司应当建立的处理安全性的基本原则。最后简略谈谈Windows NT和其它常用操作系统的安全性，并作一比较。

安全性的定义

当你听到安全性（security）这一术语时，脑海里可能想到两个概念：保护和平安。网络安全性是为保护网络不受任何损害而采取的所有措施的总和，并且当正确实现这些措施时，就能使网络得到保护，使之免受侵害并保证网络的平静与安宁。为保护网络的安全，需要协同使用多种安全措施，从创建用户帐号到雇用忠诚的雇员值守锁在房间中的服务器，都要考虑到。

安全防范是一种每时每刻都不能松懈的工作。不能指望在安装Web服务器时采取一下安全措施，然后把服务器锁在安全室就万事无忧，也不能凭空以为操作系统或服务器运行软件都完美无缺，任何人都不能找出它的毛病和漏洞。必须始终留心操作系统和应用软件出现的新的安全性问题，不断完善和增加新的安全措施。以下几节将介绍网络安全性的基本类型。

注意： 本章介绍的安全类型不一定是网络安全性仅有的组成部分。事实上，有一些极为特殊的类型，内容极为复杂，足以写一本书。如下几节介绍的安全性基本类型，适用于大多数网络。

登录安全性

在安全的网络中，用户遇到的第一件事就是要回答用户名和口令。这是网络第一道关口上的保安措施，就好象大厦门口的电子锁或保安门卫。虽然这些措施不能完全防止出现问题，但是它确实能保证让你知道都是谁、何时在大厦（或网络）中，而且使那些未经授权的用户不能进入大厦（网络）。

不幸的是，没有任何登录安全系统是完美无缺的。有的用户常常选择容易被猜测出来的口令、或是把口令写在明显易见的位置，或是几个人共享一个口令。这样做都可能引起安全问题。可以使用Windows NT提供的一些方法，防止这类问题的发生。在第2章我们会讨论这些问题。

专用名词

- **帐号（account）**：为赋予用户访问网络（或某一计算机）的权利而建立的用户名和口令。除此之外，帐号还包括有关用户的其它信息，如所属用户组、用户可访问的目录和文件等。
- **黑客（hacker）**：闯入其无权访问的网络、窥探和扰乱网络正常工作的人。从在网上寻求刺激的未成年人到窃取情报的外国特务都是黑客。“黑客”一词原本是指计算机高手，但现在它广泛使用已失去原义，而具有贬义。
- **入侵者（intruder）**：这是一个通用词，指未经授权而企图登录进入系统的人。入侵者可能是黑客、合伙间谍、有不满情绪的前职员，或是忘了自己口令的普通职员。

文件系统安全性

用户登录网络的一个主要目的是访问服务器上的文件和目录。文件系统的安全性涉及到管理每个用户可以访问哪些文件。对于用户来说，每人都有一个具体的权限表，可以有权访问某些文件和目录。例如某一用户可能在某一目录内有完全访问权（读取、创建和删除文件等），而在另一目录中仅有只读的访问权。

在对网络上的文件采取安全措施时，要确保服务器上的文件和局部工作站上的文件两者都要考虑施以安全措施。这一点说起来容易，做起来很难。许多用户的操作系统，如DOS或Windows 95几乎没有安全功能。最好的办法是鼓励（或要求）用户把他们的文件保存在服务器中。

DOS、Windows 3.x、Windows 95和Windows NT都能使用FAT文件系统。从早期版本的DOS系统到如今，这个文件系统无多少变化，你可以料到它不很安全。虽然有一些办法可以提高FAT文件的安全性，但是最好的办法依然是采用更安全的文件系统。Windows NT支持NTFS（NT文件系统），它完全支持安全性。

提示：在第8章中将详细讨论文件系统安全性。

数据通信安全性

安全性的另一方面涉及到数据通信。通过网络传输的数据包含许多敏感的信息，例如绝密文件。除非工作站与服务器之间的通信业务是安全的，否则只保证文件系统安全是不顶用的。

监控网上的通信业务，就可以提高对未授权信息的访问机会，除非已对数据采取安全措施。除了要保护构成网络的设备和通信线路，使之免于非法访问外，还要对数据采取安全措施，例如加密（发端加密，收端解密，使非法截获信息者无法理解它们）。图1.1示出了安全通信系统的工作原理。

虽然在局域网内通信安全性是次要问题，但是在较大型的网络中它应是一个需要关心的问题。而当一个网络接入因特网（Internet）时，通信安全就成了关键问题。

提示：从第3章开始，本书中有几章都将较深入地讨论通信安全性问题。