第7章 操作系统的安全性

随着信息技术应用的不断深入，系统安全性显得尤为重要。本章介绍了系统安全性的含义，影响系统安全性的主要因素以及相关的实现系统安全性的基本策略。

教学要求

- 理解系统安全性含义
- 了解影响系统安全性的主要因素
- 了解实现系统安全性的基本策略
- 了解Windows 2000/XP的安全策略

教学内容

7.1 系统安全性概述

7.1.1 安全性概述

安全性是指防范与保护计算机系统及其信息资源，使其在使用过程中免受人为的蓄意攻击、失误与自然危害等带来的损坏、窃取、篡改或泄密。

7.1.1 安全性概述（续）

安全性内容包括：

- 物理安全
- 逻辑安全
- 安全管理

7.1.1 安全性概述（续）

逻辑安全则是指系统中信息资源的安全，它又包括以下4个方面：

(1) 保密性(Secrecy)

(2) 完整性(Integrity)

(3) 可用性(Availability)

(4)真实性(Authenticity)

7.1.2 影响系统安全的因素

1、自然因素

- 自然灾害
- 软、硬件故障

7.1.2 影响系统安全的因素（续）

2、人为因素

- 发生人为失误
- 病毒破坏

  包括：蠕虫、木马、恶意脚本代码等
- 黑客入侵

7.1.3 操作系统的安全机制

1、隔离机制

- **状态隔离**

  通过对处理机设置不同的工作状态或模式来保护系统程序或用户程序不受到其他程序的干扰和破坏。

1、隔离机制（续）

- 空间隔离

  为每个进程分配不同的地址空间实现，即实现对内存区域的保护。

2、分级安全机制

- 系统级安全管理

  注册与登录机制：用户认证策略

- 用户级安全管理

  防范系统内部人员非法存取未经许可的文件信息。

- 文件级安全管理

  控制文件被访问的权限

7.2 实现系统安全性的策略

- 身份鉴别策略
- 文件保护策略
- 内存保护策略
- 恶意代码防御策略

7.2 安全性策略（续）

7.2.1 身份鉴别策略

1．账号-口令的身份鉴别

2．物理标志的身份鉴别

3．公开密钥的身份鉴别

7.2 安全性策略（续）

7.2.2 文件保护策略

- 口令
- 加密
- 存取控制表
- 存取控制矩阵

1、口令

访问文件时需输入口令，口令正确才能访问

【优点】：简便，节省空间

【缺点】：

- 可靠性差：口令易被窃取
- 存取控制不易改变
- 保护级别少

2、加密

文件用密文的形式保存

【优点】：保密性强，节省存储空间

【缺点】：花费大量的编码和译码时间，从而增加了系统的开销。

3、存取控制矩阵

文件 / 用户	ALPHA	BETA	REPORT	SQRT		
张三	RWX	---	R-X	---		
李四	R-X	---	RWX	R-X	…	
王五	---	RWX	R-X	R-X		
赵六	---	---	---	RWX		
.	.					

存取控制矩阵

存取控制矩阵在概念上是简单清楚的，但实现上却有困难。当一个系统用户数和文件数很大时，二维矩阵要占很大的存储空间，验证过程也费时。

4、存取控制表

按用户对文件的访问权限的差别对用户进行分类，它把用户分成三类：文件主、同组用户和其它用户，每类用户的存取权限为可读(R)、可写(W)、可执行(E)以及它们的组合。

存取控制表

文件名：FILE1			
用户组	文件主	同组用户	其他用户
访问权限	R W E	R	R

7.2.3 内存保护策略

- 界址与界限保护
- 分段保护

7.2.4 恶意代码防御策略

层层设防：入侵－>潜伏－>传染－>激活

1、杜绝传染渠道

- 网络（浏览网页、下载、E-mail等）
- 软盘、U盘、光盘

7.2.4 恶意代码防御策略（续）

2、定期使用杀毒软件

McAfee、诺顿、卡巴斯基、**360**等杀毒软件

3、安装防火墙

360安全卫士、天网防火墙

7.2.4 恶意代码防御策略（续）

4、系统安全设置

- 取消所有共享
- 禁用**Guest**账户
- 更改**Administrator**账号名
- 取消不必要的系统服务
- 定期升级系统

7.3 Linux的安全性

7.3.1 Linux的安全措施

1、标识与鉴别
2、存取控制
3、加密与审计
4、入侵检测
5、备份与恢复

7.3.2 Linux的安全漏洞

1、权限提升类漏洞
2、拒绝服务类漏洞
3、整数溢出漏洞
4、IP地址欺骗类漏洞

7.4 Windows 2000/XP的安全策略

7.4.1 Windows安全模型

1. 用户身份验证
2. 基于对象的访问控制
3. 活动目录
4. 其他安全机制

7.4.2 Windows的注册表

- 注册表(registry)，它实际上是一个存放系统配置信息的巨大树状分层数据库。
- Windows 2000/XP的注册表由两个文件组成： System.dat 和 User.dat 。 其 中 ， System.dat为系统配置注册表文件，它存放了一般硬件与软件的设置；User.dat为用户平台配置注册表文件，它存放各个用户特定的一些设置。

7.4.3 Windows的组策略

- 组策略是Windows 2000/XP中的一项方便修改注册表中配置的重要安全策略。它通过将系统重要的配置功能汇集成各种配置模块，供管理人员直接使用，从而达到方便管理计算机的目的。因此，采用组策略，远比手工修改注册表方便、灵活，功能也更加强大。

7.4.3 Windows的组策略（续）

- Windows 2000/XP组策略是从Windows 9X/NT的“系统策略”发展而来，具有更多的管理模板和更灵活的设置对象功能。使用组策略很简单，只需选择【开始】|【运行】菜单，然后在文本框中输入**gpedit.msc**命令，即可进入组策略界面。