

<<数据恢复原理与实践>>

图书基本信息

书名：<<数据恢复原理与实践>>

13位ISBN编号：9787118073140

10位ISBN编号：7118073148

出版时间：2011-5

出版时间：国防工业

作者：李晓中//乔晗//马鑫//常涛

页数：320

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<数据恢复原理与实践>>

内容概要

《数据恢复原理与实践》主要对常见的WINDOWS文件系统进行了详细的分析和介绍，在此基础上对当前的一些常用数据恢复技术进行了详细的介绍。

内容包括：数据恢复技术综述；硬盘基础知识；WINDOWS文件系统；数据恢复技术基础；文档的数据恢复；密码修复；系统的修复；数据安全与数据备份等。

《数据恢复原理与实践》适合于计算机用户、各种文件系统应用人员、数据恢复技术人员、操作系统开发人员、数据恢复编程人员、电子取证工作者、数据安全研究人员、系统管理员及数据安全存储与灾难恢复爱好者、学生阅读和使用，也可作为高等院校相关专业的教材或教学参考书。

<<数据恢复原理与实践>>

书籍目录

第1章 数据恢复技术综述1.1 数据存储技术1.1.1 数据的定义1.1.2 数据的存储介质1.2 数据存储安全1.2.1 影响数据存储安全的因素1.2.2 数据保护方式介绍1.3 数据恢复技术1.3.1 什么是数据恢复1.3.2 数据的可恢复性1.3.3 数据恢复的范围1.3.4 数据恢复技术展望第2章 硬盘基础知识2.1 硬盘的物理结构与组成2.2 硬盘逻辑结构2.2.1 磁道2.2.2 柱面2.2.3 扇区2.3 常用的硬盘接口标准2.3.1 IDE2.3.2 SCSI2.3.3 Serial ATA2.3.4 USB2.3.5 Fibre Channel2.4 硬盘的主要技术指标2.4.1 容量2.4.2 转速2.4.3 缓存2.4.4 平均寻道时间2.4.5 传输速率2.5 硬盘的工作原理2.6 硬盘的主要技术2.7 硬盘的品牌2.8 硬盘缺陷与故障2.8.1 硬盘缺陷的分类2.8.2 厂家处理硬盘缺陷的方式2.8.3 硬盘缺陷的处理2.8.4 坏扇区的修复原理第3章 Windows文件系统3.1 文件系统概述3.2 FAT文件系统3.2.1 硬盘组织结构3.2.2 FAT文件系统结构3.2.3 主引导扇区3.2.4 分区引导扇区3.2.5 FAT类型识别3.2.6 FAT表结构3.2.7 目录结构3.2.8 长文件名3.3 NTFS文件系统3.3.1 NTFS文件系统基础3.3.2 NTFS的DBR3.3.3 NTFS文件空间分配3.3.4 NTFS元文件3.3.5 常驻属性与非常驻属性3.3.6 MFT文件记录结构分析3.3.7 sBoot元文件介绍3.3.8 NTFS索引与目录第4章 数据恢复技术基础4.1 数据恢复的定义4.2 数据恢复的原理4.2.1 分区4.2.2 Format的使用4.2.3 文件分配表4.2.4 Fdisk的使用4.2.5 文件的读取与写入4.2.6 格式化与删除4.2.7 覆盖4.2.8 硬件故障数据恢复4.2.9 磁盘阵列RAID数据恢复4.3 数据恢复的基本方法4.3.1 故障表现4.3.2 数据丢失后的注意事项4.3.3 数据恢复需要的技能4.3.4 数据恢复的一般原则4.3.5 自己恢复——数据恢复原理方法4.4 硬盘一般性故障的检测4.4.1 MHDD的使用.....第5章 数据恢复必备的相关软件第6章 系统分区的修复第7章 数据的恢复第8章 文档修复第9章 密码修复第10章 数据安全与数据备份

<<数据恢复原理与实践>>

章节摘录

版权页：插图：1.2 数据存储安全数据的存储安全有两方面的含义，一个是指逻辑上的安全，例如防止病毒的侵人与破坏、防止黑客的入侵等；另一个是指物理上的安全，比如人为的操作错误或不可预见的灾难。

逻辑上的安全需要系统的安全防护，而物理上的安全需要数据存储备份和容灾的保护。

1.2.1 影响数据存储安全的因素影响数据存储安全的因素大体上可以分为以下情况：1.网络安全与网络架构安全该指标主要是指各种企业在建设其网络时要考虑到的一些因素。

主要包括：网络入侵检测与分析、VPN、无线安全等。

2.应用安全主要是指在计算机产品的应用中会遇到的几种不同类型的欺骗攻击，攻击者可能会利用伪造的IP数据包源、电子邮件或者网站等来欺骗受害者接收恶意数据。

从历史上看，这种欺骗攻击开始流行于20世纪90年代。

主要包括：Email安全、Web安全、SOA与Web服务安全、数据库安全、IM安全、软件开发的安全。

3.信息安全信息安全包括的范围很大，这里主要指在网络环境下应用计算机时的信息安全。

包括计算机安全操作系统、各种安全协议、安全机制（数字签名、信息认证、数据加密等），其中任何一个安全的漏洞便可以威胁全局安全。

现在流行的信息安全技术包括：防网络钓鱼（Phishing）技术、防病毒/蠕虫/恶意软件、木马/间谍软件、Rootkit、身份窃取/数据泄露、Web威胁、反垃圾邮件、黑客攻防、新兴信息安全威胁、系统平台安全技术。

4.操作系统安全操作系统是控制其他程序运行，管理系统资源并为用户提供操作界面的系统软件的集合。

操作系统的主要功能是资源管理、程序控制和人机交互等。

计算机系统的资源可分为设备资源和信息资源两大类。

设备资源指的是组成计算机的硬件设备，如中央处理器、主存储器、磁盘存储器、打印机、磁带存储器、显示器、键盘输入设备和鼠标等。

信息资源指的是存放于计算机内的各种数据，如文件、程序库、知识库、系统软件和应用软件等。

任何一个操作系统都存在着一些安全漏洞，这也是我们不断安装补丁的原因。

在这里操作系统的安全主要指信息资源，包括数据存储安全、漏洞管理、虚拟化安全管理。

5.身份识别管理安全身份识别主要指我们在计算机应用中，机器、网络的各种对用户或个人的识别管理。

身份识别技术采用密码技术（尤其是公钥密码技术）设计出安全性高的协议。

我们最熟悉的口令是应用最广的一种身份识别方式，一般是长度为5~8的字符串，由数字、字母、特殊字符、控制字符等组成。

<<数据恢复原理与实践>>

编辑推荐

《数据恢复原理与实践》是由国防工业出版社出版的。

<<数据恢复原理与实践>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>