

<<访问控制与加密>>

图书基本信息

书名：<<访问控制与加密>>

13位ISBN编号：9787111391289

10位ISBN编号：7111391284

出版时间：2012-8

出版时间：机械工业出版社

作者：李双

页数：165

字数：149000

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>

<<访问控制与加密>>

内容概要

本书内容包括为三部分。

第一部分为第1章，介绍密码学的相关概念和知识。

第二部分为第2章~第5章，介绍了访问控制技术，包括自主访问控制、强制访问控制、基于角色的访问控制、基于对象的访问控制和基于任务的访问控制。

特别对基于对象的访问控制展开讨论，提出了一种扩展的基于角色的访问控制模型，并谈论了实现细节。

第三部分对应书中第6章和第7章，讲述可搜索加密方案的背景、相关知识和现状，并提出了基于属性的可搜索加密方案。

本书可供从事信息安全专业的科技人员、硕士和博士研究生参考，也可供高等院校相关专业的师生阅读。

<<访问控制与加密>>

书籍目录

前言

第1章 密码学基础

1.1 密码学简介

1.2 私钥密码体制

1.2.1 流密码

1.2.2 分组密码

1.2.3 DES

1.2.4 AES

1.3 Hash函数

1.3.1 Hash函数与数据完整性

1.3.2 Hash函数的安全性

1.4 公钥密码体制

1.4.1 RSA密码体制

1.4.2 ElGamal密码体制

1.4.3 椭圆曲线ElGamal型的密码体制

1.5 密码分析

第2章 访问控制技术

2.1 访问控制模型

2.1.1 DAC

2.1.2 MAC

2.1.3 RBAC

2.1.4 OBAC

2.1.5 TBAC

2.2 访问控制的安全策略

2.2.1 基于身份的安全策略

2.2.2 基于规则的安全策略

2.3 访问控制实现机制

2.3.1 访问控制列表

2.3.2 访问控制矩阵

2.3.3 访问控制能力列表

2.3.4 访问控制安全标签列表

2.4 访问控制的安全级别

2.5 访问控制中的授权

2.5.1 信任模型

2.5.2 信任管理系统

2.6 访问控制与审计

第3章 RBAC 2001建议标准的参考模型

3.1 核心RBAC

3.2 层次RBAC

3.3 有约束的RBAC

3.3.1 SSD

3.3.2 DSD

3.4 功能规范

3.4.1 核心RBAC功能规范

3.4.2 层次RBAC功能规范

<<访问控制与加密>>

- 3.4.3 SSD关系功能规范
- 3.4.4 DSD关系功能规范
- 3.5 功能规范包
- 3.6 结论
- 第4章 一种更灵活的RBAC模型
 - 4.1 具有清晰权限的RBAC
 - 4.1.1 相斥运算
 - 4.1.2 可继承运算
 - 4.1.3 私有化运算
 - 4.1.4 可代理运算
 - 4.2 可代理的RBAC
 - 4.2.1 可代理RBAC0模型
 - 4.2.2 可代理RBAC1模型
 - 4.3 具有条件约束的RBAC
 - 4.3.1 RBAC前置条件模型
 - 4.3.2 RBAC过程条件模型
 - 4.4 ERBAC模型的分析和应用
 - 4.4.1 ERBAC模型的优势
 - 4.4.2 ERBAC模型的新应用
- 第5章 RBAC的实现
 - 5.1 用户 - 角色委派
 - 5.2 权限授予
 - 5.2.1 多级安全性政策模型 (Bell和LaPadula)
 - 5.2.2 基于角色的多级安全性政策模型 (RBMLS)
 - 5.2.3 安全政策实施准则
 - 5.3 实现方案
 - 5.3.1 实现机制
 - 5.3.2 相关技术
 - 5.3.3 具体实现细节
- 第6章 关键词可搜索公钥加密技术
 - 6.1 双线性对与计算性假设
 - 6.1.1 双线性对运算
 - 6.1.2 计算性假设
 - 6.2 可搜索加密体制的研究现状以及发展趋势
 - 6.3 相关加密体制
 - 6.3.1 基于身份的加密体制 (IBE)
 - 6.3.2 可搜索加密体制 (PEKS)
 - 6.3.3 基于属性的加密体制 (ABE)
 - 6.3.4 几种加密体制的联系
- 第7章 基于属性的可搜索加密方案
 - 7.1 相关知识
 - 7.1.1 可证明安全性理论
 - 7.1.2 访问结构
 - 7.2 基于属性的可搜索加密方案 (ATT PEKS) 的定义
 - 7.3 攻击游戏
 - 7.4 基于属性的可搜索加密方案 (ATT PEKS) 构造
 - 7.4.1 ATT PEKS算法构造

<<访问控制与加密>>

7.4.2 ATT PEKS的计算一致性

7.4.3 ATT PEKS复杂度分析

7.5 安全性分析

附录数学基础

参考文献

<<访问控制与加密>>

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>