

<<信息系统安全风险估计与控制理论>>

图书基本信息

书名：<<信息系统安全风险估计与控制理论>>

13位ISBN编号：9787030310491

10位ISBN编号：7030310497

出版时间：2011-6

出版时间：科学出版社

作者：王祯学 等著

页数：171

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>

## <<信息系统安全风险估计与控制理论>>

### 内容概要

《信息系统安全风险估计与控制理论》将信息论、系统论、控制论以及博弈论的基本思想和方法综合应用于研究信息系统安全风险的识别与分析、评估与控制、信息对抗等问题上，从跨学科研究的角度出发，采用定性分析和定量分析相结合的方法，得到一系列新的理论研究成果，对信息安全的学科建设和工程实践都很有学术参考价值。

《信息系统安全风险估计与控制理论》可以作为高等院校信息安全、计算机应用、网络通信、电子工程等专业高年级大学生和研究生的教材，也可供广大科技工作者参考。

书籍目录

序

前言

第1章 绪论

1.1 引言

1.2 信息与信息系统

1.2.1 信息的基本概念

1.2.2 系统的基本概念

1.2.3 信息系统的基本概念

1.2.4 开放互联网络环境下的信息系统

1.3 信息系统的安全风险

1.3.1 风险的基本概念与定义

1.3.2 信息系统的风险

1.3.3 信息系统的安全属性

1.4 安全风险的分析与评估

1.4.1 风险要素关系

1.4.2 风险分析与评估的主要内容

1.5 风险评估与风险控制

1.5.1 风险评估与控制模型

1.5.2 风险评估与控制的系统理论方法

第2章 信息系统资源分布模型及基于信息资产的风险识别与分析

2.1 引言

2.2 信息系统资源分布模型

2.2.1 信息系统构成要素

2.2.2 基于信息流保护的资源分布模型

2.3 信息系统风险识别过程

2.3.1 风险识别的含义

2.3.2 风险识别过程活动

2.4 信息系统的资产识别

2.4.1 资产分类及其位置分布

2.4.2 资产安全属性赋值

2.4.3 资产重要性等级

2.5 信息系统的威胁识别

2.5.1 威胁分类

2.5.2 威胁赋值

2.6 信息系统的脆弱性识别

2.6.1 脆弱性识别内容

2.6.2 脆弱性赋值

2.6.3 已有安全措施确认

2.7 信息系统的风险分析

2.7.1 风险计算方法

2.7.2 风险结果判定

第3章 基于安全风险的信息系统数学描述与结构分析

3.1 引言

3.2 信息系统安全风险的状态空间描述

3.2.1 信息系统的描述变量

# <<信息系统安全风险估计与控制理论>>

- 3.2.2 基于空间坐标系的状态模型
- 3.2.3 基于时间坐标系的状态模型
- 3.2.4 随机扰动情况下的状态模型
- 3.3 基于拓扑结构的信息系统数学描述
  - 3.3.1 拓扑结构图与拓扑结构矩阵
  - 3.3.2 拓扑结构矩阵逻辑算法
- 3.4 信息系统的可控性与可观测性
  - 3.4.1 可控性分析
  - 3.4.2 可观测性分析
- 第4章 信息系统安全风险的状态重构与动态估计
  - 4.1 引言
  - 4.2 风险状态观测器及其存在条件
    - 4.2.1 风险状态重构及观测器构造
    - 4.2.2 状态观测器存在条件
  - 4.3 风险状态观测器设计问题
    - 4.3.1 全维状态观测器设计
    - 4.3.2 最小维状态观测器设计
  - 4.4 随机干扰情况下的安全风险状态估计
    - 4.4.1 基于Kalman滤波的安全风险状态估计
    - 4.4.2 线性时不变系统情形
- 第5章 信息系统安全风险的静态综合评估与风险熵判别方法
  - 5.1 引言
  - 5.2 确定性情况下的安全风险静态综合评估
    - 5.2.1 各资产要素风险对风险域的影响
    - 5.2.2 风险关联与风险合理性系数
    - 5.2.3 基本风险集与风险评估准则
    - 5.2.4 静态综合评估算法步骤
  - 5.3 风险评估中的概率模型与风险熵判别方法
    - 5.3.1 信息资产安全风险的概率模型
    - 5.3.2 风险熵：信息系统安全风险递增规律
    - 5.3.3 几条重要结论
- 第6章 信息系统安全风险的动态综合评估与最大熵判别准则
  - 6.1 引言
  - 6.2 基于安全属性的信息系统风险概率模型及基本特征
    - 6.2.1 基于安全属性的信息系统安全风险概率描述
    - 6.2.2 安全风险概率的理论分布
  - 6.3 基于信息资产的动态评估模型与最大熵判别准则
    - 6.3.1 信息资产安全风险的动态概率描述
    - 6.3.2 安全熵：信息系统安全性递减规律
    - 6.3.3 最大熵判别准则
- 第7章 信息系统安全风险的状态控制
  - 7.1 引言
  - 7.2 最优化与极大值原理
    - 7.2.1 最优化的基本概念
    - 7.2.2 最优控制问题的数学描述
    - 7.2.3 极大值原理的叙述
  - 7.3 基于线性二次模型的信息系统风险控制

# <<信息系统安全风险估计与控制理论>>

- 7.3.1 离散线性二次问题
- 7.3.2 离散线性二次问题的解及控制算法步骤
- 7.3.3 离散线性二次问题再解
- 7.4 基于概率模型的信息系统风险控制
  - 7.4.1 面向信息资产的风险控制模型及控制算法
  - 7.4.2 信息系统的安全熵及控制效能综合评价
- 7.5 基于Logistic模型的信息系统攻防控制
  - 7.5.1 攻防控制的含义与内涵
  - 7.5.2 围绕信息资产的动态竞争模型
  - 7.5.3 攻防控制模型及控制算法
  - 7.5.4 信息系统的状态熵及攻防控制效能综合评价
- 7.6 信息系统的风险控制与耗费成本
  - 7.6.1 关系方程
  - 7.6.2 风险控制方案的选择
  - 7.6.3 耗费成本增量的分配
- 第8章 基于博弈论的信息系统攻防控制
  - 8.1 引言
  - 8.2 博弈问题的基本要素与分类
    - 8.2.1 博弈问题的基本要素
    - 8.2.2 博弈问题的分类
  - 8.3 信息系统攻防博弈模型
    - 8.3.1 攻防博弈的基本要素
    - 8.3.2 攻防博弈的模型结构
    - 8.3.3 攻防博弈问题的数学描述
  - 8.4 基于矩阵博弈的信息系统攻防控制
    - 8.4.1 攻防控制中的矩阵博弈模型
    - 8.4.2 攻防策略的分类与量化
    - 8.4.3 基于矩阵博弈的攻防控制算法
    - 8.4.4 实例仿真与分析
  - 8.5 基于Nash均衡的信息系统攻防博弈
    - 8.5.1 一般和非合作博弈攻防控制模型及控制算法
    - 8.5.2 攻防控制中的双矩阵博弈与纯策略Nash均衡
    - 8.5.3 双矩阵博弈中的混合策略Nash均衡
- 参考文献
- 附录A 攻防最优混合策略的线性规划问题求解
  - A1 攻击方最优混合策略的线性规划问题求解
  - A2 防御方最优混合策略的线性规划问题求解
- 后记

## 章节摘录

版权页：插图：系统一词是人们所熟知的，它是一个广义的概念，有各种不同的定义方法，本书从系统的基本特征出发，给出一个直观的定义。

定义1.1系统是特定命题和制束条件下有组织体制的通称。

注意上述定义中的“特定命题”、“制束条件”、“有组织体制”几个关键词。

所谓特定命题，是指为了达到某些特定的目的而确定的研究对象；所谓制束条件，是指组成系统的各元素（元部件）之间互有关联，并按一定的规则相互连接；所谓有组织体制，是指组成系统的各单元之间的关系要服从整体的要求，各单元与系统之间的关系也要服从整体的要求，以整体的观念来协调系统的诸单元。

可见，能够称之为系统的研究对象至少必须具备以下基本特征：（1）目的性。

例如，研究开放互连网络环境下的信息系统，目的是什么呢？

首先当然是信息通信和信息共享，这就是命题，也就是目的。

在这个命题下去研究信息系统的通信性能和互联互通规则，如网络传输延迟、路由选择的转发指数、网络容量、网络协议等。

其次是在保证信息通信和信息共享的同时，还必须保证信息的安全。

在信息通信和信息共享的过程中保证信息安全，这也是命题，也是目的。

从这个命题去研究信息系统的安全风险特性，如信息资产的脆弱性和可能受到的威胁以及由此引发的安全事件发生的可能性和安全事件造成的损失等。

（2）相关性。

组成系统的各元素（元部件）之间要相互联系，相互作用；互联要按一定的规则，即受到一定的约束。

显然，信息系统必须由客体（计算机网络）、主体（管理者和使用者）和运行环境（客体和主体共存的物理空间、逻辑空间及保障条件）三大要素按事先设计好的网络拓扑结构图和管理规则连接组成。若只有以上三大要素而不按网络拓扑结构图和管理规则连接，或者缺少其中必需要素而添上别的要素，都构不成信息系统。

（3）整体性。

无论是选择各元素（元部件）的参数，还是协调各单元之间的关系以及各单元和整体之间的关系，都要从整体的观念出发，服从整体的要求。

（4）相对性。

通常，人们把系统看成是比元部件更复杂、规模更大的组成体，但这是不确切的。

因为实际上很难从复杂程度和规模的大小来确切区分什么是元部件，什么是系统。

例如，一个双稳态触发器，作为记忆和信息处理系统，它由两只晶体管和几只电阻、电容构成；但在一个运算或控制系统里，这个双稳态触发器就退居为一个逻辑单元，这个运算或控制系统在一台复杂的计算机中只能算一个部件。

在一个规模不大的局域网系统中，一台计算机只能算一个设备单元。

所以系统的概念具有明显的相对性，与我们要讨论的命题和要达到的目的紧密相关，而不是从简单或复杂程度来区分什么是元部件，什么是系统。

此外，系统具有输出某种产物或信息的功能，但它不能无中生有。

也就是说，对输出必须要有输入经过处理才能得到。

输出是处理的结果，代表系统的目的；处理是输入变成输出的一种加工，由系统本身担任。

编辑推荐

《信息系统安全风险估计与控制理论》是由科学出版社出版的。

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>