Atitit 信息安全体系 资料书籍表

[1. 《信息安全原理与技术 2](#_Toc10970)

[1.1. 第2章 工具箱： 鉴别、 访问控制与加密 2](#_Toc28619)

[1.2. 第3章 程序和编程 漏洞 木马 病毒 3](#_Toc25509)

[1.3. Web和用户 4](#_Toc22017)

[1.4. 第5章 操作系统 安全性 4](#_Toc4960)

[1.5. 第6章 网络安全 通信 ddos 6.7 防火墙 6.8 入侵检测和防御系统 加密 5](#_Toc25436)

[1.6. 第7章 数据库存储安全 7.3 可靠性和完整性 7.4 数据库泄露 7.5 数据挖掘和大数据 6](#_Toc19153)

[1.7. 第8章 云计算安全 8.3 云安全工具与技术 8.4 云认证管理 OAuth等 7](#_Toc32554)

[1.8. 第9章 计算机中的隐私保护安全 9.4 数据挖掘 8](#_Toc3874)

[1.8.1. 9.4 数据挖掘 9.5 网站上的隐私 9.6 电子邮件安全性 8](#_Toc20641)

[1.8.2. 9.7 对新技术的影响 RFID VoIP与Skype 云端的隐私 9](#_Toc3744)

[1.9. 安全管理和事件 10](#_Toc2328)

[1.9.1. 10.1 安全计划 10](#_Toc2177)

[1.9.2. 10.3 事件处理 10](#_Toc22855)

[1.9.3. 10.4 风险分析 10](#_Toc26534)

[1.9.4. 10.5 处理灾难 10](#_Toc12647)

[1.10. 第11章 法律和道德问题 11](#_Toc20668)

[2. 信息安全技术 12](#_Toc11106)

[2.1. 第3章 密码技术  12](#_Toc9776)

[2.2. 第4章 标识与认证技术  13](#_Toc14198)

[2.3. 第5章 授权与访问控制技术  13](#_Toc22722)

[2.4. 第6章 信息隐藏技术  13](#_Toc9975)

[2.5. 第7章 网络与系统攻击技术  14](#_Toc20930)

[2.6. 第8章 网络与系统安全防护及应急响应技术  14](#_Toc19984)

[2.7. 第9章 安全审计与责任认定技术  14](#_Toc27716)

[2.8. 第10章 主机系统安全技术  14](#_Toc31933)

[2.9. 第12章 恶意代码检测与防范技术  15](#_Toc23748)

[2.10. 第13章 内容安全技术  15](#_Toc20556)

[2.11. 第14章 信息安全测评技术  16](#_Toc8975)

[2.12. 第15章 信息安全管理技术  16](#_Toc10788)

# 《信息安全原理与技术

目 录  
第1章 介绍  
1.1 什么是计算机安全  
1.1.1 资源的价值  
1.1.2 脆弱点—威胁—控制的范式  
1.2 威胁  
1.2.1 机密性  
1.2.2 完整性  
1.2.3 可用性  
1.2.4 威胁的类型  
1.2.5 攻击者类型  
1.3 危害  
1.3.1 风险及常识  
1.3.2 方法—时机—动机  
1.4 脆弱点  
1.5 控制  
1.6 总结  
1.7 下一步是什么  
1.8 习题

## 第2章 工具箱： 鉴别、 访问控制与加密

2.1 身份鉴别

2.1.1 识别与身份鉴别  
2.1.2 基于短语和事实的鉴别： 用户已知的事情  
2.1.3 基于生物特征鉴别技术的鉴别： 用户的一些特征  
2.1.4 基于令牌的身份鉴别： 你拥有的东西  
2.1.5 联合身份管理机制  
2.1.6 多因素鉴别  
2.1.7 安全鉴别  
2.2 访问控制  
2.2.1 访问策略  
2.2.2 实施访问控制  
2.2.3 面向程序的访问控制  
2.2.4 基于角色的访问控制  
2.3 密码编码学  
2.3.1 加密技术解决的问题  
2.3.2 术语  
2.3.3 DES： 数据加密标准  
2.3.4 高级加密标准  
2.3.5 公开密钥密码体制  
2.3.6 从公钥加密到密钥分配  
2.3.7 检错码（error detecting codes）  
2.3.8 信任度  
2.3.9 证书： 可信的身份信息与公钥  
2.3.10 数字签名： 整合  
2.4 习题

## 第3章 程序和编程 漏洞 木马 病毒

3.1 无意的（非恶意的）程序漏洞  
3.1.1 缓冲区溢出  
3.1.2 不完全验证  
3.1.3 检查时刻到使用时刻的错误  
3.1.4 未公开的访问点  
3.1.5 大小差一错误  
3.1.6 整型溢出  
3.1.7 未以空终止符结尾的字符串  
3.1.8 参数长度、 类型和数值  
3.1.9 不安全的通用程序  
3.1.10 竞态条件  
3.2 恶意的代码： 恶意软件  
3.2.1 恶意软件： 病毒、 木马和蠕虫  
3.2.2 技术细节： 恶意代码  
3.3 对策  
3.3.1 用户的对策  
3.3.2 开发者的对策  
3.3.3 专门的安全对策  
3.3.4 无效的对策  
3.4 小结  
3.5 习题

## Web和用户

1. 4.1 针对浏览器的攻击  
   4.1.1 针对浏览器的攻击类型  
   4.1.2 浏览器攻击如何成功： 识别失败与鉴别失败  
   4.2 针对用户的Web攻击  
   4.2.1 虚假或误导的内容  
   4.2.2 恶意的网页内容  
   4.2.3 防止恶意网页  
   4.3 获取用户或网站的数据  
   4.3.1 有数据的代码  
   4.3.2 网站数据： 用户的问题  
   4.3.3 挫败数据攻击  
   4.4 电子邮件攻击  
   4.4.1 虚假电子邮件  
   4.4.2 作为垃圾邮件的虚假电子邮件  
   4.4.3 假(错误的)电子邮件头数据  
   4.4.4 网络钓鱼  
   4.4.5 防止电子邮件攻击  
   4.5 小结  
   4.6 习题

## 第5章 操作系统 安全性

1. 5.1 操作系统的安全性  
   5.1.1 背景： 操作系统结构  
   5.1.2 普通操作系统的安全特性  
   5.1.3 历史回顾  
   5.1.4 受保护对象  
   5.1.5 实现安全功能的操作系统工具  
   5.2 安全操作系统的设计  
   5.2.1 简约设计  
   5.2.2 分层设计  
   5.2.3 内核化设计  
   5.2.4 引用监视器  
   5.2.5 正确性和完整性  
   5.2.6 安全设计原则  
   5.2.7 可信系统  
   5.2.8 可信系统的功能  
   5.2.9 可信系统的研究成果  
   5.3 rootkit  
   5.3.1 手机rootkit  
   5.3.2 rootkit躲避检测  
   5.3.3 rootkit未经检查的操作  
   5.3.4 索尼公司的XCP rootrootkit  
   5.3.5 TDSS rootkits  
   5.3.6 其他rootkits  
   5.4 小结  
   5.5 习题

## 第6章 网络安全 通信 ddos 6.7 防火墙 6.8 入侵检测和防御系统 加密

1. 6.1 网络的概念  
   6.1.1 背景： 网络传输介质  
   6.1.2 背景： 协议层  
   6.1.3 背景： 寻址和路由选择  
   6.2 网络通信的威胁  
   6.2.1 截取： 偷听与窃听  
   6.2.2 篡改、 伪造： 数据损坏  
   6.2.3 中断： 服务失效  
   6.2.4 端口扫描  
   6.2.5 脆弱点总结  
   6.3 无线网络安全  
   6.3.1 WiFi场景  
   6.3.2 无线网络中的脆弱点  
   6.3.3 故障的对策： WEP（等效于有线加密）  
   6.3.4 更强的协议族： WPA（WiFi保护访问）  
   6.4 拒绝服务  
   6.4.1 例子： 爱沙尼亚海量网络故障  
   6.4.2 服务是怎么被拒绝访问的  
   6.4.3 洪泛（flooding）攻击的细节  
   6.4.4 恶意代码导致的网络洪泛  
   6.4.5 资源消耗的网络洪泛  
   6.4.6 地址错误造成的拒绝服务  
   6.4.7 流量重定向  
   6.4.8 DNS攻击  
   6.4.9 利用已知的脆弱点  
   6.4.10 物理隔离  
   6.5 分布式拒绝服务  
   6.5.1 脚本拒绝服务攻击  
   6.5.2 Bots  
   6.5.3 僵尸网络  
   6.5.4 恶意自主的移动代理  
   6.5.5 自主移动防护代理  
   6.6 网络安全中的密码学  
   6.6.1 网络加密  
   6.6.2 浏览器加密  
   6.6.3 洋葱路由  
   6.6.4 IP安全协议套件（IPsec）  
   6.6.5 虚拟专用网络  
   6.6.6 系统架构  
   6.7 防火墙 6.8 入侵检测和防御系统  
     
   6.7.1 什么是防火墙  
   6.7.2 防火墙设计  
   6.7.3 防火墙的类型  
   6.7.4 个人防火墙  
   6.7.5 几种类型防火墙的比较  
   6.7.6 防火墙配置举例  
   6.7.7 网络地址转换（NAT）  
   6.7.8 数据丢失防护（Date Loss Prevention）  
   6.8 入侵检测和防御系统  
   6.8.1 IDS的种类  
   6.8.2 其他入侵检测技术  
   6.8.3 入侵防御系统  
   6.8.4 入侵响应  
   6.6.5 入侵检测系统的目标  
   6.8.6 IDS的能力和局限  
   6.9 网络管理  
   6.9.1 服务保障管理  
   6.9.2 安全信息和事件管理（SIEM）  
   6.10 小结  
   6.11 习题

## 第7章 数据库存储安全 7.3 可靠性和完整性 7.4 数据库泄露 7.5 数据挖掘和大数据

1. 7.1 数据库简介  
   7.1.1 数据库的概念  
   7.1.2 数据库的组成  
   7.1.3 数据库的优点  
   7.2 数据库的安全需求  
   7.2.1 数据库的完整性  
   7.2.2 元素的完整性  
   7.2.3 可审计性  
   7.2.4 访问控制  
   7.2.5 用户鉴别  
   7.2.6 可用性  
   7.2.7 完整性、 机密性和可用性  
   7.3 可靠性和完整性  
   7.3.1 操作系统提供的保护特性  
   7.3.2 两阶段更新  
   7.3.3 冗余/内在一致性  
   7.3.4 恢复  
   7.3.5 并发性/一致性  
   7.4 数据库泄露  
   7.4.1 敏感数据  
   7.4.2 泄露类型  
   7.4.3 防止泄露： 数据禁止和修改  
   7.4.4 安全性与精确度  
   7.5 数据挖掘和大数据  
   7.5.1 数据挖掘  
   7.5.2 大数据  
   7.6 小结  
   7.7 习题

## 第8章 云计算安全 8.3 云安全工具与技术 8.4 云认证管理 OAuth等

1. 8.1 云计算概念  
   8.1.1 服务模式  
   8.1.2 部署模式  
   8.2 迁移到云端  
   8.2.1 风险分析  
   8.2.2 评估云服务提供商  
   8.2.3 更换云服务提供商  
   8.2.4 作为安全控制的云  
   8.3 云安全工具与技术 8.4 云认证管理 OAuth等  
      
   8.3.1 云环境下的数据保护  
   8.3.2 云应用安全  
   8.3.3 日志与事件响应  
   8.4 云认证管理  
   8.4.1 安全断言标记语言  
   8.4.2 OAuth协议  
   8.4.3 OAuth用于认证  
   8.5 加固IaaS  
   8.5.1 公有IaaS与私有网络的安全性对比  
   8.6 小结  
   8.6.1 本领域的发展方向  
   8.6.2 更多参考  
   8.7 习题

## 第9章 计算机中的隐私保护安全 9.4 数据挖掘

1. 9.1 隐私的概念  
   9.1.1 信息隐私的各方面  
   9.1.2 与计算机相关的隐私问题  
   9.2 隐私的原理和政策  
   9.2.1 公平信息策略  
   9.2.2 美国的隐私法律  
   9.2.3 美国政府网站的控制  
   9.2.4 商业网站的控制  
   9.2.5 非美国的隐私原则  
   9.2.6 保护隐私的个人行为  
   9.2.7 政府和隐私  
   9.2.8 身份窃取  
   9.3 鉴别和隐私  
   9.3.1 鉴别意味着什么  
   9.3.2 结论

### 9.4 数据挖掘 9.5 网站上的隐私 9.6 电子邮件安全性

9.4.1 政府数据挖掘  
9.4.2 隐私保持的数据挖掘  
9.5 网站上的隐私 9.6 电子邮件安全性  
  
9.5.1 了解在线环境  
9.5.2 网上付款  
9.5.3 门户网站注册  
9.5.4 这是谁的网页  
9.5.5 冲浪要留心  
9.5.6 间谍软件  
9.5.7 网上购物  
9.6 电子邮件安全性  
9.6.1 电子邮件将发往何处， 谁能够访问它  
9.6.2 电子邮件的拦截  
9.6.3 监控电子邮件  
9.6.4 匿名、 假名、 消失的电子邮件  
9.6.5 欺骗和垃圾邮件  
9.6.6 小结

### 9.7 对新技术的影响 RFID VoIP与Skype 云端的隐私

9.7.1 RFID  
9.7.2 电子投票选举  
9.7.3 VoIP与Skype  
9.7.4 云端的隐私  
9.7.5 有关新技术的结论  
9.8 领域前沿  
9.9 小结  
9.10 习题

## 安全管理和事件

### 10.1 安全计划

### 10.3 事件处理

### 10.4 风险分析

### 10.5 处理灾难

1. 10.1 安全计划  
   10.1.1 组织和安全计划  
   10.1.2 安全计划的内容  
   10.1.3 安全计划编制组成员  
   10.1.4 安全计划的承诺  
   10.2 业务持续计划  
   10.2.1 评估业务影响  
   10.2.2 发展战略  
   10.2.3 开发计划  
   10.3 事件处理  
   10.3.1 事故响应计划  
   10.3.2 应急小组  
   10.4 风险分析  
   10.4.1 风险的性质  
   10.4.2 风险分析的步骤  
   10.4.3 赞成和反对风险分析的理由  
   10.5 处理灾难  
   10.5.1 自然灾难  
   10.5.2 停电  
   10.5.3 人为破坏  
   10.5.4 敏感信息截取  
   10.5.5 意外事故处理计划  
   10.5.6 物理安全的回顾  
   10.6 小结  
   10.7 习题

## 第11章 法律和道德问题

1. 11.1 程序和数据的保护  
   11.1.1 版权  
   11.1.2 专利  
   11.1.3 商业秘密  
   11.1.4 特殊情况  
   11.2 信息和法律  
   11.2.1 作为对象的信息  
   11.2.2 与信息相关的法律问题  
   11.2.3 法律制度  
   11.2.4 计算机产品保护的小结  
   11.3 雇员和雇主权利  
   11.3.1 产品所有权  
   11.3.2 雇佣合同  
   11.4 软件故障的补救  
   11.4.1 销售正确的软件  
   11.4.2 报告软件错误  
   11.5 计算机犯罪  
   11.5.1 为什么要有计算机犯罪的单独类型  
   11.5.2 为什么计算机犯罪很难定义  
   11.5.3 为什么对计算机犯罪难以起诉  
   11.5.4 法令实例  
   11.5.5 国际范围  
   11.5.6 为什么破获计算机犯罪困难重重  
   11.5.7 什么样的计算机犯罪没有讨论  
   11.5.8 计算机安全法律问题的小结  
   11.6 计算机安全中的道德问题  
   11.6.1 法律与道德之间的区别  
   11.6.2 对道德的研究  
   11.6.3 道德推理法  
   11.7 道德的案例分析  
   11.7.1 案例1： 计算机服务的使用  
   11.7.2 案例2： 隐私权  
   11.7.3 案例3： 拒绝服务  
   11.7.4 案例4： 程序的所有权  
   11.7.5 案例5： 专有资源  
   11.7.6 1

# 信息安全技术

1. 绪论   
   　1.1 什么是信息安全   
   　1.2 信息安全发展历程   
   　1.3 信息安全威胁   
   　1.4 信息安全技术体系   
   　1.5 信息安全模型   
   　1.6 小结与后记   
   　论述与思考   
   第2章 信息安全保障技术框架   
   　2.1 深度防御策略   
   　2.2 信息保障框架域   
   　2.2.1 框架域1——保护网络与基础设施   
   　2.2.2 框架域2——保护区域边界和外部连接   
   　2.2.3 框架域3——保护计算环境   
   　2.2.4 框架域4——支持性基础设施   
   　2.3 信息系统安全工程   
   　2.3.1 产生背景   
   　2.3.2 信息系统安全工程与通用系统工程的联系   
   　2.3.3 阶段1——发掘信息保护需求   
   　2.3.4 阶段2——定义信息保护系统   
   　2.3.5 阶段3——设计信息保护系统   
   　2.3.6 阶段4——实施信息保护系统   
   　2.3.7 阶段5——评估信息保护的有效性   
   　2.4 小结与后记   
   　论述与思考

## 第3章 密码技术

1. 3.1 基本概念   
   　3.2 对称密码   
   　3.2.1 古典密码   
   　3.2.2 分组密码   
   　3.2.3 序列密码   
   　3.3 公钥密码   
   　3.4 杂凑函数和消息认证码   
   　3.5 数字签名   
   　3.6 密钥管理   
   　3.7 小结与后记   
   　论述与思考

## 第4章 标识与认证技术

1. 4.1 标识   
   　4.2 口令与挑战-响应技术   
   　4.3 在线认证服务技术   
   　4.4 公钥认证技术   
   　4.5 实体认证相关标准   
   　4.6 远程口令认证技术   
   　4.7 其他常用认证技术   
   　4.8 匿名认证技术   
   　4.9 PKI技术   
   　4.10 小结与后记   
   　论述与思考

## 第5章 授权与访问控制技术

1. 5.1 授权和访问控制策略的概念   
   　5.2 自主访问控制   
   　5.3 强制访问控制   
   　5.4 基于角色的访问控制   
   　5.5 基于属性的访问控制   
   　5.6 PMI技术   
   　5.7 小结与后记   
   　论述与思考

## 第6章 信息隐藏技术

1. 6.1 基本概念   
   　6.2 隐藏信息的基本方法   
   　6.3 数字水印   
   　6.4 数字隐写   
   　6.5 小结与后记   
   　论述与思考

## 第7章 网络与系统攻击技术

1. 7.1 典型攻击过程   
   　7.2 网络与系统调查   
   　7.3 口令攻击   
   　7.4 缓冲区溢出攻击   
   　7.5 拒绝服务攻击   
   　7.6 典型案例分析   
   　7.7 小结与后记   
   　论述与思考

## 第8章 网络与系统安全防护及应急响应技术

1. 8.1 防火墙技术   
   　8.2 入侵检测技术   
   　8.3 “蜜罐”技术   
   　8.4 应急响应技术   
   　8.5 小结与后记   
   　论述与思考

## 第9章 安全审计与责任认定技术

1. 9.1 审计系统   
   　9.2 事件分析与追踪   
   　9.3 数字取证   
   　9.4 数字指纹与追踪码   
   　9.5 小结与后记   
   　论述与思考

## 第10章 主机系统安全技术

1. 10.1 操作系统安全技术   
   　10.1.1 基本概念   
   　10.1.2 商业操作系统安全机制   
   　10.1.3 商业操作系统安全性的验证   
   　10.1.4 其他安全机制   
   　10.2 数据库安全技术   
   　10.2.1 安全数据库管理系统   
   　10.2.2 外包数据库安全   
   　10.2.3 云数据库/云存储安全   
   　10.3 可信计算技术   
   　10.4 小结与后记   
   　论述与思考   
   第11章 网络系统安全技术   
   　11.1 OSI安全体系结构   
   　11.2 SSL/TLS协议   
   　11.3 IPSec协议   
   　11.4 SET协议   
   　11.5 安全电子邮件   
   　11.5.1 PGP   
   　11.5.2 S/MIME   
   　11.6 小结与后记   
   　论述与思考

## 第12章 恶意代码检测与防范技术

1. 12.1 常见的恶意代码   
   　12.2 恶意代码机理   
   　12.3 恶意代码分析   
   　12.4 恶意代码检测   
   　12.5 恶意代码清除与预防   
   　12.6 小结与后记   
   　论述与思考

## 第13章 内容安全技术

1. 13.1 内容安全的概念   
   　13.2 文本过滤   
   　13.3 话题发现和跟踪   
   　13.4 内容安全分级监管   
   　13.5 多媒体内容安全技术简介   
   　13.6 小结与后记   
   　论述与思考

## 第14章 信息安全测评技术

1. 14.1 信息安全测评的发展   
   　14.2 信息安全验证与测试技术   
   　14.3 信息安全测试技术   
   　14.4 信息安全评估技术   
   　14.5 信息安全评估准则及其主要模型与方法   
   　14.6 小结与后记   
   　论述与思考

## 第15章 信息安全管理技术

1. 15.1 信息安全规划   
   　15.2 信息安全风险评估   
   　15.3 物理安全保障   
   　15.4 信息安全等级保护   
   　15.5 国际信息安全管理标准   
   　15.6 信息安全法规   
   　15.7 小结与后记   
   　论述与思考   
   附录 基础知识与综合习题   
   附录A 数论初步   
   附录B 代数系统与多项式   
   附录C 信号变换   
   附录D 综合习题   
   参考文献