NCRE——三级信息安全技术电子教案

（2025年版）

# 第一章 信息安全保障概述

## 导入语

本章概述了信息安全保障的相关内容：

“信息安全保障背景”——介绍了信息技术发展的各个阶段及其对社会产生的影响；

“信息安全保障基础”——讲述了信息安全发展阶段以及信息安全的含义、问题根源及其在社会中的地位和作用；

“信息安全保障体系”——讲解了信息安全保障基本体系框架，并详细阐述了典型的P2DR安全模型和IATF框架的基本原理；

“信息安全保障基本实践”——讲述了国内外实践概况和信息安全保障的基本工作内容。

## 考核目标

⚫ 了解信息技术发展各个阶段的概况及其对社会、科技、人类生活所产生的影响；了解信息安全发展的各个阶段及其主要特征。

⚫ 理解信息安全的含义、问题根源及其在国家和信息社会中的地位和作用。

⚫ 理解信息安全保障体系；理解P2DR模型的基本原理及其数学表达公式的含义；理解IATF纵深防御思想及其对信息系统技术四个方面的安全需求划分。

⚫ 了解国内外信息安全保障工作概况；理解信息安全保障工作的各部分内容及其主要原则。

## 1 . 1 信息安全保障背景

### 1.1.1 信息技术及其发展阶段

人类社会的发展与进步是由社会生产力决定。当今社会，科学技术作为第一生产力的作用日益凸显，信息技术作为现代先进科学技术体系中的前导要素，其所引发的社会信息化迅速地改变着社会的面貌、改变者人们的生产方式和生活方式，并对社会运行方式产生着巨大的影响。

**什么是“信息技术”？**

笼统地讲，信息技术是能够延伸或扩展人的信息能力的手段和方法。本书中信息技术是指，在计算机技术和通信技术的支持下，用于获取、传输、处理、存储、显示和应用文字、数值、图像、视频、音频等信息，并且包括提供设备和信息服务的方法和设备的总称。

信息技术包括生产和应用两个方面。

• 信息技术的生产主要体现在信息技术产业，包括计算机软硬件、电信设备、微电子生产等；

• 信息技术的应用则是体现在信息技术的扩散上，包括信息服务、管理信息系统等。

在信息技术系统中，微电子技术、通信技术、计算机技术和网络技术可以称为信息技术的核心，它们的发展进程体现了信息技术的发展过程。

信息技术的产生与发展，大致经历了如下三个阶段：

第一阶段，电讯技术的发明（电报电话、收音机、电视机）

第二阶段，计算机技术的发展（图灵机理论、冯诺依曼体系结构、集成电路、大规模集成电路计算机）

第三阶段，互联网的使用（ARPAnet、TCP/IP协议、因特网）

### 1.1.2 信息技术的影响

信息技术的飞速发展，对人类社会产生了重要影响，其主流是积极的，但也客观存在一些负面影响。

**信息技术的积极影响：**

（1）对社会发展的影响。科学技术是第一生产力，如今信息技术已经成为科学技术前沿，人类社会正在从工业社会步入信息社会。

（2）对科技进步的影响。信息技术促进了新技术的变革，极大地推动了科学技术的发展。

（3）对人类生活的影响。信息技术的广泛应用，促进了人们工作效率和生活质量的提高，人们的工作方式和学习方式也正发生转变。足不出户可知天下事，人不离家照样能办事。

**信息技术的消极影响：**

（1）信息泛滥。一方面是信息急剧增长，另一方面是人们消耗了大量的时间却找不到有用的信息，信息的增长速度超出了人们的承受能力，导致信息泛滥的出现。

（2）信息污染。一些错误信息、虚假信息、污秽信息等混杂在各种信息资源中，使人们对错难分，真假难辨，人们如果不加分析，便容易上当受骗，受其毒害。

（3）信息犯罪。随着信息技术应用的普及，人们对信息技术的依赖程度越来越高，信息安全已成为日益突出的问题。一些不法分子利用信息技术手段及信息系统本身的安全漏洞进行犯罪活动，如信息窃取、信息欺诈、信息攻击和破坏等，严重地危害着正常的社会秩序。

## 1.2 信息安全保障基础

### 1.2.1 信息安全发展阶段

（1）通信保密阶段；

（2）计算机安全阶段；

（3）信息安全保障阶段。

1.2 信息安全保障基础

1. **通信保密阶段**

当代信息安全学起源于20世纪40年代的通信保密。这一时期，人们主要关注信息在通信过程中的安全性问题，即“机密性”。

1949年香农发表的《保密系统的通信理论》，首先用信息论的观点对信息保密问题作了全面论述。

2. **计算机安全阶段**。20世纪60年代和70年代，计算机安全的概念开始逐步得到推行。

1965年美国率先提出了计算机安全（COMPUSEC）。此时计算机主要用于军方，1969年的Ware报告初步地提出了计算机安全及其评估问题。

20世纪70年代是计算机安全的奠基时代。

20世纪80年代的一个标志性特征是计算机安全的标准化工作。

3. **信息安全保障阶段**。20世纪90年代以后，开始倡导信息保障（Information Assurance，IA）

主要关注“预警、保护、检测、响应、恢复、反击”整个过程，信息安全保障强调保护、检测、反应和恢复这四种能力，围绕人员、技术和管理这三个层面，以支持机构的任务和职能为目标，注重体系建设，强化组织与协调功能。

### 1.2.2 信息安全的含义

信息安全是一个广泛而抽象的概念。信息安全关注信息本身的安全，其任务是保护信息资产，防止偶然的或未经授权者对信息的恶意泄露、修改和破坏而导致的信息不可靠或无法处理等，使得在最大限度利用信息的同时不会导致损失或损失最小。

从信息安全的发展历程可以看出，信息安全在不同的发展阶段具有不同的内涵。在不同信息应用领域，存在的安全问题也不同；所站的角度不同，对信息安全的理解也不尽相同。

1.2 信息安全保障基础

从信息网络系统看，现代信息安全主要包含：

（一）**运行系统的安全**，包括严格而科学的管理，如对信息网络系统的组织管理、监督检查；规章制度的建立、落实与完善；管理人员的责任心、预见性、警惕性等；法律、政策的保护，如用户是否有合法权利，政策是否允许等；物理控制安全，如机房加锁、线路安全、环境适宜等；硬件运行安全；操作系统安全，如数据文件是否保护等；灾害、故障恢复；死锁的避免和解除；防止电磁信息泄漏等。

（二）**系统信息的安全**，包括用户口令鉴别；用户存取权限控制；数据存取权限、方式控制；审计跟踪；数据加密等。

信息安全的基本属性，主要包括：

① **完整性**：是指信息在存储和传输过程中保持未经授权不能改变的特性；

② **机密性**：是指信息不被泄露给未经授权者的特性；

③ **可用性**：是指信息可被授权者访问并按需求使用的特性；

④ **可控制性**：是指对信息的传播和内容具有控制能力的特性

⑤ **不可否认性**：也称不可抵赖性，即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。

信息信息安全的任务就是实现上述的安全属性，而攻击者则是想尽一切办法破坏上述信息安全属性。

整体上说，现代的信息安全是物理安全、网络安全、数据安全、信息内容安全、信息基础设施安全与公共、国家信息安全的总和，是一个多层次、多因素、多目标的复合系统。

### 1.2.3 信息系统面临的安全风险

随着信息网络系统的迅速发展和全面普及，人与计算机的关系发生了质的变化，人类社会与计算机和网络组成了一个巨大系统，出现了一个全新的世界——网络社会。网络社会的信息安全不仅涉及到个人权益、企业生存、金融风险防范、社会稳定和国家安全，甚至关系到环境安全、生态安全和人类安全。信息信息系统面临的主要安全威胁有：

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 信息泄露 | 9 | 恶意代码 |
| 2 | 破坏信息的完整性 | 10 | 假冒和欺诈 |
| 3 | 拒绝服务 | 11 | 抵赖 |
| 4 | 非授权访问 | 12 | 重放攻击 |
| 5 | 授权侵犯 | 13 | 陷阱门 |
| 6 | 业务流分析 | 14 | 媒体废弃 |
| 7 | 窃听 | 15 | 人员不慎 |
| 8 | 物理侵入 | 16 | 物理侵入 |

### 1.2.4 信息安全问题产生根源

信息系统的安全风险隐患来源于信息系统自身存在的脆弱性和信息系统面临的各种安全威胁。

（1）**信息安全内因：信息系统的复杂性**

信息系统（Information System）是由人、计算机及其他外围设备组成的，用于信息收集、传递、存储、加工、维护和使用的系统。信息系统本身是脆弱的，主要的原因有：

‒ 组成网络的通信和信息系统的自身缺陷。

‒ 互联网的开放性。

（2）**信息安全的外因：人为的和环境的威胁**

‒ 人为原因。很多系统内部和外部的攻击者非法入侵和破坏系统、窃取信息。

‒ 自然环境的原因。信息系统都是在一定的自然环境下运行的，自然灾害对信息系统的威胁是多方面的。

### 1.2.5 信息安全的地位和作用

在当今的信息时代和网络社会中，信息安全具有头等重要的地位，它是一切安全的重中之重和先中之先，是社会发展的首要条件，是民族振兴的根本保障，是21世纪各国努力争夺的制高点。

⚫ 信息安全是网络时代国家生存和民族振兴的根本保障

⚫ 信息安全是信息社会健康发展和信息革命成功的关键因素

⚫ 信息安全是网络时代人类生存和文明发展的基本条件

### 1.2.6 信息安全技术

现有的信息安全技术可以归纳为5类：

（1）核心基础安全技术（主要包括密码技术）；

（2）安全基础设施技术（标识与认证技术、授权与访问控制技术等）；

（3）基础设施安全技术（主机系统安全技术、网络系统安全技术等）；

（4）应用安全技术（网络与系统安全攻击技术、网络与系统安全防护与响应技术、安全审计与责任认定技术、恶意代码检测与防范技术等）；

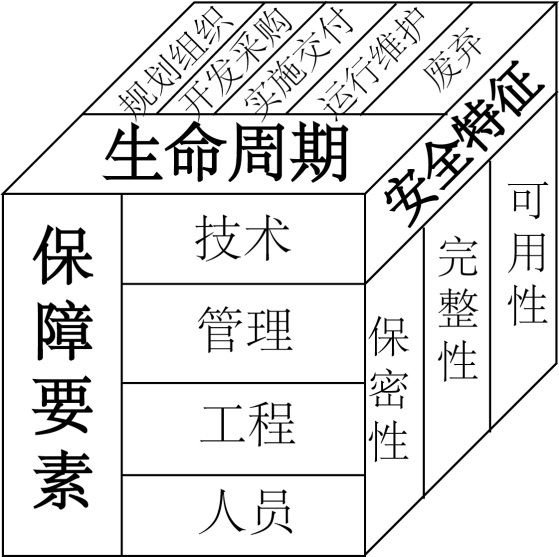
（5）支撑安全技术（信息安全测评技术、信息安全管理技术等）。

## 1. 3信息安全保障体系

### 1.3.1 信息安全保障体系框架

信息系统安全保障是在信息系统的整个生命周期中，通过分析信息系统的风险，制定并执行相应的安全保障策略，从技术、管理、工程和人员等方面提出安全保障要求，确保信息系统的机密性、完整性和可用性，降低安全风险到可接受的程度，从而保障信息系统能够实现组织机构的使命。

信息安全保障体系框架如图所示。



### 1.3.1 信息安全保障体系框架

信息系统安全保障涵盖以下几个方面：

（1）**生命周期**

信息系统安全保障应贯穿信息系统的整个生命周期，包括规划组织、开发采购、实施交付、运行维护和废弃5个阶段，以获得信息系统安全保障能力的持续性。

（2）**保障要素**

信息系统安全保障不仅涉及安全技术，还应综合考虑安全管理、安全工程和人员安全等，以全面保障信息系统安全。

（3）**安全特征**

信息系统安全保障是基于过程的保障。通过风险识别、风险分析、风险评估、风险控制等风险管理活动，降低信息系统的风险，从而实现信息系统机密性、完整性和可用性的安全保障。

### 1.3.2 信息系统安全模型与技术框架

#### 1. P2DR安全模型

P2DR模型是美国ISS公司提出的动态网络安全体系的代表模型，也是动态安全模型的雏形（如图所示），其包括四个主要部分：策略（Policy）、防护（Protection）、检测（Detection）和响应（Response）。



P2DR模型是在整体安全策略的控制和指导下，在综合运用防护工具（如防火墙、操作系统身份认证、加密技术等）的同时，利用检测工具（如漏洞评估工具、入侵检测系统等）了解和评估系统的安全状态，通过适当的反应将系统调整到“最安全”和“风险最低”的状态。防护、检测和响应组成了一个完整的、动态的安全循环，在安全策略的指导下保证信息系统的安全。

P2DR模型认为与信息安全相关的所有活动，不管是攻击行为、防护行为、检测行为和响应行为等，都要消耗时间。因此可以用时间来衡量一个体系的安全性和安全能力。

P2DR模型可以用下面典型的数学公式来表达安全的要求：

其中：系统为了保护安全目标设置各种保护后的防护时间；

：从入侵者发动入侵开始，系统检测到入侵行为所花费的时间；

：从发现入侵行为开始，到系统能够做出足够的响应，将系统调整到正常状态的时间。

针对需要保护的安全目标，如果上述数学公式满足防护时间大于检测时间加上响应时间，也就是在入侵者危害安全目标之前就能被检测到并及时处理。

式（2）的前提是假设防护时间为0。其中:

：从入侵者发动入侵开始，系统检测到入侵行为所花费的时间；

：从发现入侵行为开始，到系统能够做出足够的响应，将系统调整到正常状态的时间；

：安全目标系统的暴露时间，即Dt与Rt的和。

可见，针对于需要保护的安全目标， 越小系统就越安全。

通过公式(1)和公式(2)的描述，实际上给出了一个全新的安全定义：“及时的检测和响应就是安全”、“及时的检测和恢复就是安全”。而且，这样的定义为安全问题的解决给出了明确的方向：提高系统的防护时间，降低检测时间 和响应时间 。

然而，P2DR模型也存在一个明显的弱点，就是忽略了内在的变化因素。例如人员的流动、人员的素质和策略贯彻等不稳定性等。实际上，安全问题牵涉面广，除了涉及到防护、检测和响应，系统本身安全“免疫力”的增强、系统和整个网络的优化，以及人员这个系统中最重要角色的素质提升，都是该安全模型没有考虑到的问题。

#### 2. 信息保障技术框架

《信息保障技术框架》（Information Assurance Technical Framework，IATF）是由美国国家安全局（NSA）制定的描述信息保障的指导性文件。我国国家973计划项目“信息与网络安全体系研究”课题组在2002年将IATF 3.0版引进国内后，IATF开始对我国信息安全工作的发展和信息安全保障体系的建设起到了重要的参考和指导作用。

IATF提出的信息保障的核心思想是纵深防御战略（Defense in Depth）。所谓纵深防御战略就是采用一个多层次的、纵深的安全措施来保障用户信息及信息系统的安全。在纵深防御战略中，人员、技术和操作是三个主要核心因素，要保障信息及信息系统的安全，三者缺一不可。

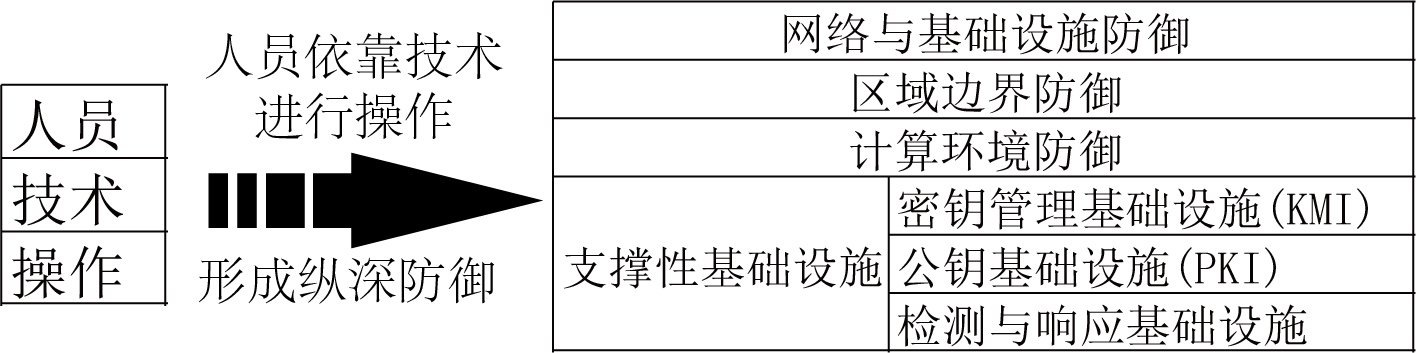
##### （1）IATF的三个核心要素

IATF提出了三个主要核心要素：人员、技术和操作。如表所示。

|  |  |  |
| --- | --- | --- |
| 人员 | 技术 | 操作 |
| 培训 | 纵深防御技术框架域 | 分析 |
| 意识 | 安全标准 | 监视 |
| 物理安全 | 获得 IA/TA | 入侵检测 |
| 人员安全 | 风险分析 | 警告 |
| 系统安全管理 | 证书与信任 | 恢复 |

下图描述了纵深防3御战略的三个主要层面：人员、技术和操作。

在这个战略的三个主要层面中，IATF强调技术并提供一个框架以进行多层保护，以此来防范面向信息系统的威胁。该方法使能够攻破一层或一类保护的攻击行为无法破坏整个信息基础设施。



##### （2）IATF的四个技术框架焦点域

IATF将信息系统的信息保障技术层面划分成了四个技术框架焦点域，并在每个焦点域范围内，IATF都描述了其特有的安全需求和相应的可供选择的技术措施：

①保护本地计算环境；

②保护区域边界；

③保护网络及基础设施；

④保护支撑性基础设施；

## 1. 4信息安全保障基本实践

### 1.4.1 国内外信息安全保障工作概况

随着冷战的结束和信息全球化步伐的加快，世界各国尤其是美、俄等国政府高度重视国家信息保障工作，并先后调整了国家安全战略，使信息保障在国家安全战略中的地位开始上升，已成为国家安

全战略中“不可分割的重要组成部分”。

美国：

美国信息安全保障体系建设比较完善：

‒ 《保护美国关键基础设施》总统令（PDD63）（ 1998.5.22）；

‒ 《信息保障技术框架》（IATF），IATF 3.1版（ 2002.9）；

‒ 信息保障训令8500.1（ 2002.10.24）和8500.2（ 2003.2.6）；

‒ 《国土安全国家战略》（ 2002.7.16），《保护网络空间的国家战略》（ 2003.2.14）；

‒ 《国防战略报告》（ 2005.3）。

俄罗斯：

‒ 《联邦信息化和信息保护法》（1995）；

‒ 《俄罗斯国家安全构思》（1997）；

‒ 《国家信息安全学说》（2000；

俄罗斯的安全部门使用了一个名为“操作与调查程序系统”（ SORM2 ）的网络监视系统对互联网信息进行监视。俄罗斯此举的目的之一是为了对抗美国国家安全局，因为美国国家安全局早就实现了对全球通信的监视。

日本：

‒ 日本强调，“信息安全保障是日本安全保障体系的核心” ；

‒ 《21世纪信息通信构想》（1999）、《信息通信产业技术战略》（1999）；

‒ 2000年3月，修改了《21世纪信息通讯技术研究开发基本计划》（1996）；

‒ 《信息通信网络安全可靠性基础》（2000.6.8）；

‒ 《IT安全政策指南》（2000.12）；

‒ 在内阁秘书处成立信息安全措施促进办公室（2000.2）；

‒ 决定成立三个重要机构（2000.2.29）：综合安全保障阁僚会议、IT安全专家委员会和内阁办公室下的IT安全分局；

日本政府还采取多种政策措施提高产业竞争能力，如宣布放宽企业向国外提供网络密码技术的出口限制（2000.6.23）；成立密码技术评价委员会（2000.4）；开始实行“安全测评认证制度”（2001.4）。

韩国：

韩国韩国政府投入了大量的资金用于发展国内信息安全技术工程。如：韩国情报通信部发表了“信息安全技术开发5年计划”，计划投资2777亿元以产、学、研等形式共同开发国内信息安全核心技术。韩国情报通信部还决定投资巨资开发下一代能动型网络信息保护系统。具体开发课题包括：安全引擎及安全节点系统开发、入侵忍耐型安全网络技术的开发和用户中心的各个安全级别的服务技术开发。

中国：

我国的信息安全保障体系建设始于2003年9月，中央颁布的《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发27号文件），提出要在5年内建设中国信息安全保障体系。

2006 年上半年，公安部会同国务院信息办在全国范围内开展了等级保护基础调查。2006年下半年，在13个省区市和3个部委联合开展了等级保护试点工作。2007年7月20日，“全国重要信息系统安全等级保护定级工作电视电话会议”召开，标志着信息安全等级保护工作在全国范围内的开展与实施。

2006年9月，科技部的《国家科技支撑计划“十一五”发展纲要》提出科技“支撑发展”的重要思想，

初步形成国家技术自主创新支撑体系，提高我国信息产业核心技术自主开发能力和整体水平，初步建立有中国特色的信息安全保障体系。

为了适应信息安全和网络安全的发展形势，我国政府也制定了一系列基本的管理办法。其中包括：《中华人民共和国计算机安全保护条例》、《中华人民共和国商用密码管理条例》、《中华人民共和国计算机信息网络国际联网管理暂行办法》、《关于对国际联网的计算机信息系统进行备案工作的通知》、《计算机信息网络国际联网安全保护管理办法》等；

在刑法修正案中，增加了有关计算机犯罪的条款。

在国家技术监督局和其它主管部门的指导下，信息安全与网络安全技术和产品标准也陆续出台，安全产品检测认证机构相继成立。成立了全国信息技术标准化技术委员会信息技术安全分技术委员会。经国家技术监督局和公安部授权，成立了公安部计算机信息系统安全产品质量监督检验中心。

这些都说明了国家信息安全保障发展的大环境已经日臻完善。

**我国信息安全保障的国家战略目标**是：保证国民经济基础设施的信息安全，抵御有关国家、地区、集团可能对我实施的信息战的威胁，打击国内外的高技术犯罪，保障国家安全、社会稳定和经济发展。

**信息安全战略防御的重点任务**是：保障国民经济中的国家关键基础设施，包括金融、银行、税收、能源生产储备、粮油生产储备、水电气供应、交通运输、邮电通信、广播电视、商业贸易等的安全。

### 1.4.2 信息安全保障工作的内容

信息系统安全保障工作基本内容包括：

➢ 确定安全需求；

➢ 设计和实施安全方案；

➢ 信息安全评测；

➢ 信息安全监控与维护。

#### 1. 确定安全需求

依据信息安全保障体系的结构框架进行安全需求分析。信息安全保障体系的管理体系需要建立健全的信息安全相关的法律法规和规章制度，并进行相关培训，包括法律法规、规章制度、岗位职责、操作规范、专业技术等知识，以提高相关人员的安全意识、安全技能、业务素质等方面的水平。信息安全保障体系的组织体系需要建立健全的，由决策、管理和执行三层组成的安全机构，合理设置安全岗位，完善安全相关人员的人事管理，明确安全职责，实行安全监督，保证安全运行。

信息安全保障体系的技术体系依据信息安全的三维结构和P2DR 模型进行安全需求分析。首先，对三维结构中的各系统单元（即物理平台、系统平台、通信平台、网络平台和应用平台）以及安全管理面临的安全风险进行识别和分析。然后，按照P2DR模型分别从策略、防护、检测和响应四个方面提出控制风险的要求（即安全需求）。

#### 2. 设计和实施安全方案

信息安全方案是信息安全保障实施的基础，安全方案的设计与实施是以安全需求

分析为依据的。安全方案的制定需要遵循以下原则：

① 综合性、整体性原则；

② 需求、风险、代价平衡的原则；

③ 标准性原则；

④ 一致性原则；

⑤ 分步实施原则；

⑥ 易操作性原则；

⑦ 多重保护原则。

#### 3. 信息安全评测

信息安全评测能够从风险管理角度，运用科学的方法和手段，系统地分析信息系统所面临的威胁及其存在的脆弱性；评估安全事件一旦发生可能造成的危害程度；提出有针对性的抵御威胁的防护对策和整改措施；为防范和化解信息安全风险，将风险控制在可接受的水平，从而最大限度地为保障信息安全提供科学依据。

信息安全风险评估通常采用如下评估方式：①配置核查；②工具测试；③专家访谈；④资料审阅；⑤专家评议。

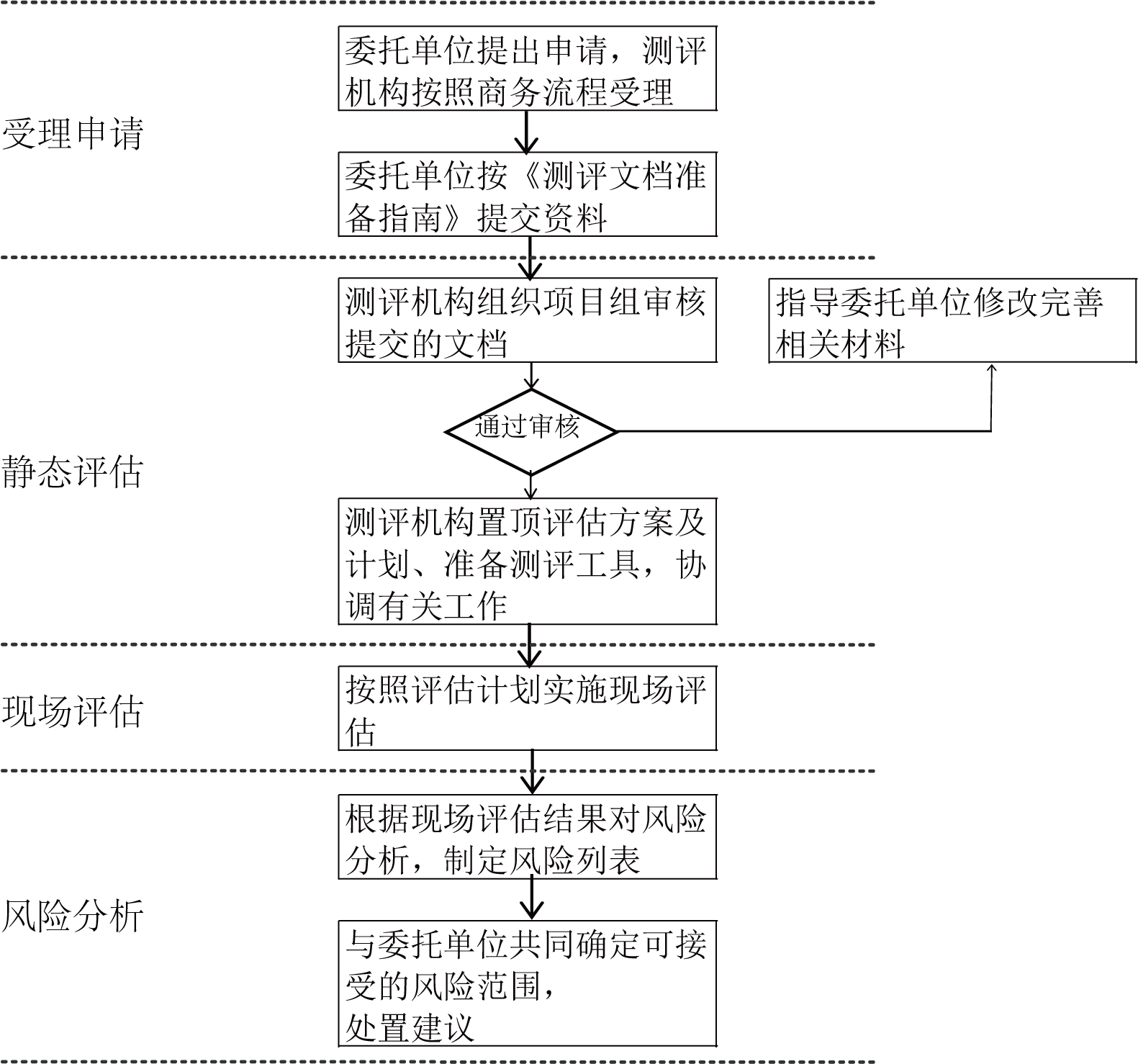
通常情况下，在评估信息系统存在的高中低风险的数量、可能性、影响时，主要从安全技术和安全管理两个角度评估：

（1）安全技术：

①物理安全；②网络层安全；③主机系统层安全；④应用层安全；⑤数据安全。

（2）安全管理方面：

①安全管理组织机构；②安全管理制度;③人员安全管理;④系统建设管理;⑤系统运维管理。信息安全风险评估流程如图所示：



#### 4. 实施信息安全监控

信息安全监控是指对信息系统的黑客入侵、网站挂马等行为进行安全监控，经过内部分析提交重大安全隐患分析报告和安全态势分析报告，以便在系统生命周期中持续提高信息系统安全保障能力。监控内容通常包括：门户网站是否受到黑客威胁，网站是否被挂马，网络流量是否异常，网络中病毒泛滥趋势，以及网络中是否存在入侵事件等。

信息安全监控方式包括两种：

①现场监控：由测评人员根据监控模版内容获取并分析信息系统关键设备当时的安全信息。

②非现场监控：由资深评测人员采用日志分析工具对被监控系统的各种日志进行综合分析。

## 小结

作为现代先进科学技术体系中的前导要素，信息技术所引发的社会信息化能够改变社会的面貌，改变人们的生产方式和生活方式，并对社会运行方式产生巨大影响。信息技术的发展可分为三个阶段：电讯技术的发明；计算机技术的发展和互联网的使用。信息技术的飞速发展，对人类社会产生重大影响，其主流是积极的，但一些负面影响也客观存在。为了限制其中的负面影响对社会稳定和国家安全的危害，必须采取措施确保信息安全。

经过通信保密、计算机安全和信息安全保障这三个阶段的发展和完善，现代信息安全是物理安全、网络安全、数据安全、信息内容安全和信息基础设施安全的总和，是一个多层次、多因素、多目标的复合系统。信息安全致力于保护信息的完整性、机密性、可用性、可控制性以及不可否认性，已成为网络时代国家生存、民族振兴、社会稳定的根本保障。

信息系统安全保障是指在信息系统的整个生命周期中通过对信息系统的风险分析，制定相应的安全保障策略，从技术、管理、工程和人员等方面提出安全保障要求，确保信息系统的机密性、完整性和可用性，将安全风险降低到可接受的程度，从而保障信息系统能够实现组织机构的使命。

典型的信息系统安全模型和框架是P2DR模型和IATF。其中，P2DR模型利用时间来衡量攻击、防护、检测和响应行为，进而通过适当的反应将系统调整到最安全和风险最低的状态。IATF将信息系统的信息保障技术层面划分成了4个技术框架焦点域：本地计算环境、区域边界、网络及基础设施和支撑性基础设施，并基于纵深防御的思想，以人员、技术和操作作为3个主要核心因素，以保障信息及信息系统的安全。

随着信息全球化的发展，信息保障在国家安全战略中的地位逐渐上升，已成为国家安全战略中“不可分割的重要组成部分”。我国从2003年9月颁布的《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发27号文件）开始，提出要在5年内建设中国信息安全保障体系。信息系统安全保障工作基本内容包括：确定安全需求、设计和实施安全方案、进行信息安全评估和实施信息安全监控。

# 第二章 信息安全基础技术与原理

## 考核目标

• 理解密码编码学和密码分析学的概念，掌握密码体制的分类，了解密码破解的典型方式。理解对 称加密算法的特点，了解DES、AES、IDEA三种典型对称加密算法的工作原理；理解非对称密 码算法的功能和特点，掌握RSA公钥密码体制，包括RSA的算法描述、RSA的实现、RSA的安 全性、RSA在应用中的问题，了解其它非对称密码算法ELGamal、ECC的特点；理解哈希（Hash） 函数的作用了解MD5算法、SHA1算法的工作原理；掌握数字签名的原理和应用，了解美国数 字签名标准；了解密钥管理的概念，理解密钥的产生及分配，了解密钥的存储、更换和注销等。

• 了解消息认证和身份认证的作用，掌握消息认证的常用手段，理解身份认证的认证手段及认证协 议。

• 了解访问控制的基本概念，理解访问控制模型的分类，理解自主访问控制的含义，了解访问矩阵 模型，理解访问矩阵模型的实现（访问控制列表、权能列表），理解基于角色的访问控制模型（RBAC） 的特点和优势，理解强制访问控制的分类和含义，了解典型强制访问控制模型：Bell Lapudula模 型Biba模型、Chinese Wall模型和ClarkWilson模型，理解集中访问控制的基本概念及其实现 （RADIUS、TACACS、TACACS+和Diameter等），理解非集中访问控制的基本概念及其实现（域 等）。

• 了解安全审计的基本概念，理解安全审计的作用和目标，了解审计系统的组成结构，了解常用安 全监控技术，掌握内容审计系统模型以及网络不良信息内容监控方法。

## 2.1 密码技术

密码学（Cryptology）是一门古老的科学。大概自人类社会出现战争便产生了密码，成为实现秘密通讯的主要手段，一般用于信息通信传输过程中的保密和存储中的保密，并逐渐形成一门独立的学科。在密码学形成和发展的历程中，科学技术的发展和战争的刺激都起了积极的推动作用。电子计算机一出现便被用于密码破译。1949年香农（Shannon）发表了《保密系统的通信理论》的著名论文，把密码学置于坚实的数学基础之上，标志着密码学作为一门学科的形成。1976年Diffie和Hellman提出公开密钥密码，从此开创了一个密码新时代。1977年，美国联邦政府颁布数据加密标准（DES，Data Encryption Standard），这是密码史上的一个创举。1994年美国联邦政府颁布数字签名标准（DSS，Digital Signature Standard），2001年美国联邦政府颁布高级加密标准（AES，Advanced Encryption Standard），这些都是密码发展史上一个个重要的里程碑。

### 2.1.1 对称密码与非对称密码

#### 1. 基本概念及分类

密码技术的基本思想是伪装信息，所谓伪装就是对数据进行一组可逆的数学变换。伪装前的原始数据称为明文（Plaintext），而伪装后的消息称为密文（Ciphertext）。伪装的数据变换过程称为加密（Encryption），相反的，将密文还原成明文的过程称为解密（Decryption）。

研究各种加密方案的学科称为密码编码学（Cryptography），而加密方案则称为密码体制（Cryptosystem）或密码（Cipher）。研究破译密码获得消息的学科称为密码分析学（Cryptanalysis）。密码编码学和密码分析学统称密码学（Cryptology）。

一个密码系统（即密码体制），通常由五部分组成：

**消息空间**：所有可能明文的有限集称为明文空间，通常用表示；

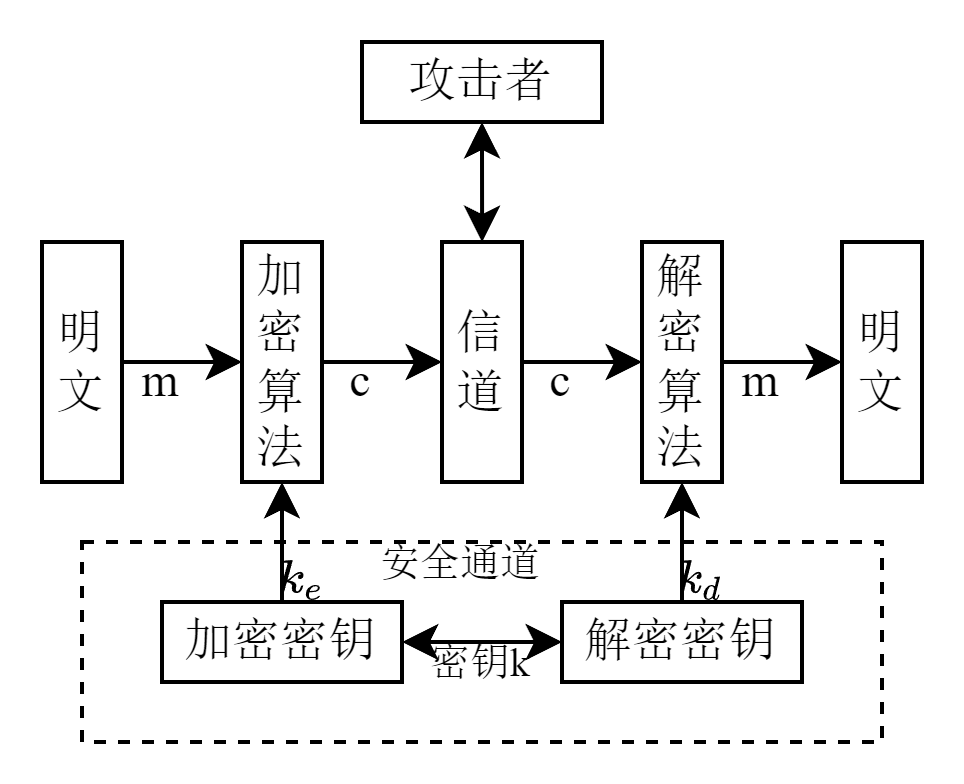
**密文空间**：所有可能密文的有限集称为密文空间，通常用表示；

**密钥空间**：一切可能的密钥构成的有限集称为密钥空间，通常用表示；

**加密算法**：加密算法是基于密钥将明文变换为密文的变换函数，相应的变换过程称为加密，通常用表示，即，也可表示为。

**解密算法**：解密算法是基于密钥将密文恢复为明文的变换函数，相应的变换过程称为解密，通常用表示，即，也可表示为。

对于有实用意义的密码体制而言，总是要求它满足：，即用加密算法得到的密文总是能用一定的解密算法恢复出原始的明文来。加密和解密算法的操作通常都是在一组密钥的控制下进行的，分别称为加密密钥（Encryption Key) 和解密密钥（Decryption Key），加密密钥通常用来表示，解密密钥通常用来表示。



根据密钥的数量，可以将密码体制分为两类：**对称密钥密码体制和非对称密钥密码体制**。

如果一个密码体制的，即发送方和接收方双方使用的密钥相同，则称为对称密钥密码体制；相反地，如果，即发送方和接收方双方使用的密钥不相同，则称为非对称密钥密码体制。

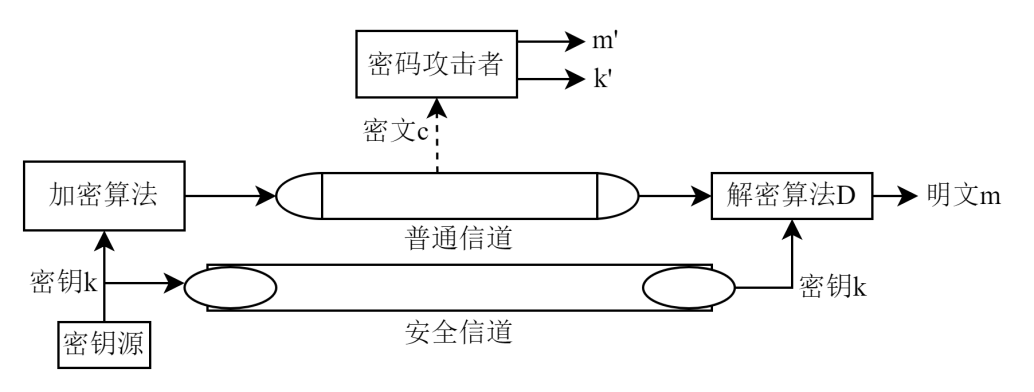
在非对称密钥体制中，由于在计算上不能由推出，这样将公开也不会损害的安全，于是可以将公开，因此，这种密码体制又被称为公开密钥密码体制。公开密钥密码体制的概念，由Diffie和Hellman于1976年提出，它的出现是密码史上的一个里程碑。

#### 2. 对称密钥体制

对称密钥密码体制也称为单密钥密码体制或传统密码体制，基本特征是发送方和接收方共享相同的密钥，即加密密钥与解密密钥相同。

##### （1）对称密钥体制

对称密码体制的基本元素包括原始的明文、加密算法、解密算法、密钥、密文及攻击者，如图所示。加密算法E根据输入的明文和密钥生成密文，即。拥有密钥的接收方接收到密文之后，可以使用解密算法恢复明文，即。



密码学设计中应遵循一个公开设计的原则，即密钥体制的安全应依赖于对密钥的保密，而不应依赖于对算法的保密。只有在算法公开的条件下依然可以保证密码的安全才是可取的。因此，上图所示的对称密码体制中，加密算法和解密算法是允许公开的，但是密钥必须妥善保管。

对称密码的优点在于加解密处理速度快、保密度高等。而缺点同样明显，突出表现在如下两个方面：

① 密钥管理和分发复杂、代价高。

密钥是保密通信安全的关键，发送方必须安全、妥善地把密钥护送到接收方，不能泄露其内容，如何才能把密钥安全地送到收信方，是对称密码算法的突出问题。

对称密码算法的密钥分发过程十分复杂，所花代价高；多人通信时密钥组合的数量会出现爆炸性膨胀，使密钥分发更加复杂化，N个人进行两两通信，总共需要的密钥数为N(N1)/2个。

② 数字签名困难。

除了密钥管理与分发问题，对称密码算法还存在数字签名困难问题（通信双方拥有同样的消息，接收方可以伪造签名，发送方也可以否认发送过某消息）。

##### （2）对称密钥分类

对称密钥体制，根据对明文的加密方式的不同而分为两类：分组密码（Block cipher）和序列密码（Stream cipher）。分组密码，也被称为分块密码，是将明文消息编码表示后的位（Bit）或字符序列，按指定的分组长度划分成多个分组（Block）后，每个分组分别在密钥的控制下变换成等长的输出。常见的分组密码算法主要有DES、IDEA、AES等。

序列密码，也被称为流密码，是将明文和密钥都划分为位或字符的序列，并且对明文序列中的每一位或字符都用密钥序列中的对应分量来加密。公开的序列密码算法主要有RC4、SEAL等。分组密码每一次加密一个明文分组，而序列密码每一次加密一位或者一个字符，两种密码在计算机系统中都有广泛的应用。

##### （3）传统的加密方法

传统对称密码加密时所使用的两个技巧是：代换和置换。

① **代换法**

代换法是将明文字母替换成其它字母、数字或符号的方法。如果将明文看作是二进制序列的话，那么代换就是用密文位串来代换明文位串。已知最早的代换密码是由Julius Caesar发明的Caesar密码。它非常简单，就是对字母表中的每个字母，用其之后的第k个字母来代换。例如，k取值为3，将用每个字母后的第3个字母来代换，加密结果如下：

明文： meet me after the toga party → 密文： phhw ph diwhu wkh wrjd souwb

对于Caesar密码而言，其密钥个数与字母表集合大小有关，容易遭受穷举攻击，攻击者只需要简单地测试所有可能的密钥就能完成破译。

**单表代换密码**

单表代换密码允许任意代换，使得密钥空间急剧增大。如果密文行是26个字母的任意置换，那么就有26！或大于4×1026种可能的密钥，足以抵抗穷举攻击了。

**多表代换**

单表代换的改进方法是在明文消息中采用不同的单表代换，即多表代换密码。多表代换密码有以下特征：一是采用相关的单表代换规则集；二是由密钥决定给定变换的具体规则。此类算法中最著名、最简单的是Vigenère密码。它的代换规则集由26个类似Caesar密码的代换表组成，其中每一个代换表是对明文字母表移位0到25次后得到的代换单表。每个密码代换表由一个密钥字母来表示，这个

密钥字母就是用来代换明文字母a的那个字母。

② **置换法**

另外一种传统的加密方法是置换，置换密码是通过置换而形成新的排列。最简单的例子就是栅栏技术，按照对角线的顺序写入明文，而按行的顺序读出作为密文。例如，用深度为2的栅栏技术加密消息“meet me afterthe toga party”，可写为：

m e m a t r h t g p r y

e t e f e t e o a a t

加密后的信息是mematrhtgpryetefeteoaat。

多步置换密码相对来讲要安全得多。这种复杂的置换是不容易构造出来的，可以采用之前置换的算法再反复加密几次，将会隐藏更多的字母频率特征，破坏原有的规律性，增加破解的难度。

##### （4）安全性

如果密码分析者能够根据密文c确定出明文m或密钥k，或者能够根据明文—密文对确定出密钥k，则我们说这个密码是可破译的。攻击密码体制一般有两种方法：

**① 穷举攻击法**：指攻击者对一条密文尝试所有可能的密钥，直到有一个合法的密钥能将密文恢复为明文。平均而言，获得成功至少要尝试所有可能密钥的一半。

**② 密码分析学**：密码分析学的攻击依赖于算法的性质和明文的一般特征或某些明文密文对。这种形式的攻击企图利用算法的特征来推导出特别的明文或使用的密钥。如果这种攻击能成功地推导出密钥，那么影响将是灾难性的，将会危及所有未来和过去使用该密钥加密的消息的安全。穷举攻击是对任何密码都普遍适用的攻击办法，抵抗穷举攻击的方法是增大密钥量，即保证有足够大的密钥空间，进而增加穷举攻击所需的时间代价。表给出了不同密钥空间所耗用的时间。

|  |  |  |  |
| --- | --- | --- | --- |
| 密钥大小（位） | 密钥个数 | 每微秒执行一次加密所需的时间 | 每微秒执行100万次加密所需的时间 |
| 32 | 232=4.3×109 | 35.8分 | 2.15毫秒 |
| 56 | 264=7.2×1016 | 1142年 | 10.01小时 |
| 128 | 2128=3.4×1036 | 5.4×1024年 | 5.4×1018年 |
| 168 | 2168=3.7×1050 | 5.9×1036年 | 5.9×1030年 |
| 26个字符的排列组合 | 26！=4×1026 | 6.4×1012年 | 6.4×106年 |

如果密钥的二进制位数是l，那么密钥空间大小（即密钥个数）为2l。如表2.2所示，对于密钥长度为128位及以上的密钥空间，穷举攻击方法就不再有效。因此，密码分析者必须依赖于对密文本身的分析，而这一般要运用到各种统计方法。

密码的设计应当遵循公开设计原则，即密钥体制的安全应依赖于对密钥的保密，而不应依赖于对算法的保密。只有在算法公开的条件下依然可以保证密码的安全才是可取的。

在假设密码分析者已知所用加密算法全部知识的情况下，根据密码分析者对明文、密文等数据资源的掌握程度，表2.3概括了密码分析学中几种典型的密码攻击。

|  |  |
| --- | --- |
| 攻击类型 | 密码分析者已知的信息 |
| 唯密文攻击​ | 加密算法、要解密的密文 |
| 已知明文攻击​ | 加密算法、要解密的密文  用（与待解的密文）同一密钥加密的一个或多个明密文对 |
| 选择明文攻击​ | 加密算法、要解密的密文  分析者任意选择的明文，用（与待解的密文）同一密钥加密的密文 |
| 选择密文攻击​ | 加密算法、要解密的密文  分析者有目的选择的一些密文，用（与待解的密文）同一密钥解密的对应明文 |

唯密文攻击是最容易防范的，因为攻击者拥有的信息量最少。

如果分析者能够通过某种方式，让发送方在发送的消息中插入一段他选择的信息，那么选择明文攻击就有可能实现。一个例子就是差分密码分析。一般说来，如果分析者有办法选择明文加密，那么他将故意选取那些最优可能恢复出密钥的数据。

加密算法一般要能抵抗选择明文攻击才认为是安全的。现代对称密码的研究始于20世纪70年代中期，而在90年代初提出了两种有效的对称密码的选择明文分析方法：差分分析和线性分析。差分密码分析法的基本思想是通过分析明文对的差值对密文对的差值的影响来恢复某些密钥比特。

差分密码分析是迄今已知的攻击迭代密码最有效的方法之一，它可以用来攻击任何由迭代一个固定的轮函数的结构的密码以及很多分组密码（包括DES）。虽然对16轮DES没有攻破，但是，如果迭代的轮数降低，则它可成功地被攻破。例如，8轮DES在PC机上只需要2分钟即可被攻破。

线性密码分析比差分密码分析更有效，其基本思想是通过寻找一个给定密码算法有效的线性近似表达式来破译密码系统。由于每个密码系统均为非线性系统，因此只能寻找线性近似表达式。随着对这两种分析方法的深入，人们更细致地从多个方面对密码的各个组件进行研究。在现有的对称密码算法中，所用的基本运算有异或、加、减、乘和查表等，在研究这些基本运算的差分性和非线性后，必须合理地安排这些基本运算，选择合适的参数，才能抵抗各种攻击。

##### （5）设计思想

上述分析方法都利用了这样一个事实：明文的结构和模式在加密之后仍然保存了下来，并能在密文中找到一些蛛丝马迹。攻击者可以根据明文、密文和密钥的统计规律来破译密码。因此，在设计密码的时候，如何破坏明文、密文和密钥之间的统计特性成为关键。

扩散（Diffusion）和混淆（Confusion）是对称密码设计的主要思想。

所谓扩散就是将每一位明文和密钥数字的影响扩散到尽可能多的密文数字中。在理想情况下，明文和密钥的每一位都影响密文的每一位。经由此种扩散作用，可以隐藏许多明文在统计上的特性，增加密码的安全。使用复杂的非线形代换算法可得到预期的混淆效果。

所谓混淆就是使密文和密钥之间的关系复杂化。密文和密钥之间的关系越复杂，使攻击者越难以从数学上描述或从统计上去分析，使得密文和明文之间、密文和密钥之间的统计相关性就越小，从而使统计分析的难度大大增加。

如何设计分组密码算法才能保证其实现足够的混淆和扩散？

乘积迭代的方法是达到扩散和混淆目的的常见方法，是Shannon在其1949的论文中提出的。所谓乘积密码就是采用m个函数（密码）的复合，其中每个可能是一个代换或置换。Shannon建议交替使用代换和置换两种方法，即他称之为混淆和扩散的过程，破坏对密码系统进行的

各种统计分析。

常见的乘积密码是迭代密码。典型的迭代密码定义了一个轮函数和一个密钥编排方案，对明文的加密将经过多轮迭代。这种思想在现代密码体制的设计中十分重要，深刻影响着数据加密标准DES高级数据加密标准AES的设计。

##### （6）数据加密标准DES

数据加密标准DES是在1970年代中期由美国IBM公司发展出来的，且被美国国家标准局（NIST，National Institute of Science and Technology）公布为数据加密标准的一种分组加密算法。

DES算法的分组大小为64位，所使用的加密或解密密钥也是64位大小，但因其中有8个位是用来做奇偶校验，所以64位中真正起密钥作用的只有56位。而DES加密与解密所用的算法除了子密钥的顺序不同之外，其它的部分则是完全相同的。

**1）Feistel网络**

DES密码结构基于一个称为Feistel网络的结构。Feistel网络（又称Feistel结构）是由Horst Feistel在设计Lucifer分组密码时发明的，并被DES、FEAL、Twofish、RC5等算法使用。

Feistel定义了一个迭代的分组密码算法，其本质是利用乘积密码顺序地执行多个基本密码系统，使得最后结果的密码强度高于每个基本密码系统产生的结果。

对一个分组长度为比特的轮Feistel型密码，每轮迭代执行的运算相同，而每轮的输入取决于前一轮的输出。以第轮为例，描述每轮迭代的运算过程如下：

① 将第轮的输出结果作为本轮输入（第一轮输入为原始分组），并将输入划分为左右长度相等的两部分，记作和分别为的左右比特。

② 将左右两部分交换位置，并将右半部分直接作为本轮输出的左半部分Li；同时，将右半部分和轮密钥作为轮函数的输入，将轮函数F的输出与左半部分进行逐位异或，得到的结果作为输出的右半部分Ri。如下所示：

Feistel网络的解密过程与加密过程完全一致，只是以相反的次数使用每轮的子密钥，这个特点使得基于Feistel网络设计的分组密码易于硬件实现。

**2）3DES算法**

DES现在已经不被视为一种安全的加密算法，攻击DES的最有效的办法是密钥穷举攻击，因为它使用的56位密钥过短。

1999年1月，distributed.net与电子前哨基金会合作，在22小时15分钟内即公开破解了一个DES密钥。为了提供实用所需的安全性，可以使用DES的派生算法3DES来进行加密，虽然3DES也存在理论上的攻击方法。在2001年，DES作为一个标准已经被高级加密标准AES所取代。

3DES算法顾名思义就是3次DES算法，其算法原理如下：

设和代表DES算法的加密和解密过程，代表DES算法使用的密钥，代表明文，代表密文，这样，

3DES加密过程为：

3DES解密过程为：

这里可以，但不能。如果相等的话就成了DES算法了。

##### （7）国际数据加密算法IDEA

IDEA是一种分组加密算法，由Lai及Massey在1990年所设计。其利用128位的密钥对64位的明文分组，经过连续加密产生64位的密文分组。

对任何对称加密算法的设计，混淆及扩散是两个最重要的安全特性。IDMA的混淆特性通过混合下述三种函数而达成：

① 以位为单位的异或，用⊕表示。

② 定义在模216(= mod 65536)的模加法运算，其操作数都可以表示16位整数，用+表示这个函数。

③ 定义在模216+1(= mod 65537)的模乘法运算。因为65537是一素数，所以对任何数（除0以外）的乘法逆元是存在的。值得一提的是，为了保证即使当“0”出现在16位的操作数也有乘法逆元存在，“0”被定义成216。用⊙表示这个函数。

以上三个函数，由于基于以下的非兼容性，可以充分发挥出混淆的特性：

① 三个函数中的任意两个函数，都无法满足分配律，例如对函数⊙及+，存在a, b, c∈F216，而且a+ (b⊙c)≠(a+ b)⊙(a+c)。

② 三个函数中的任意两个函数，都无法满足结合律，例如对函数+及⊕，存在a, b, c∈F216，而且a+ (b⊕c)≠(a+ b)⊕(a+c)。

在IDEA的设计中，使用了这三种函数的混合组合来打乱数据。攻击者无法用化简的方式来分析密文与明文及密钥之间的关系。

IDEA的扩散特性是建立在乘法/加法（MA）的基本结构上。图2.6表示MA的基本结构。该结构一共有4个16位的输入，两个16位的输出。其中的两个输入源于明文，另两个输入是子密钥，源于128位加密密钥。Lai经过分析验证，数据经过8轮的MA处理，可以得到完整的扩散特性。

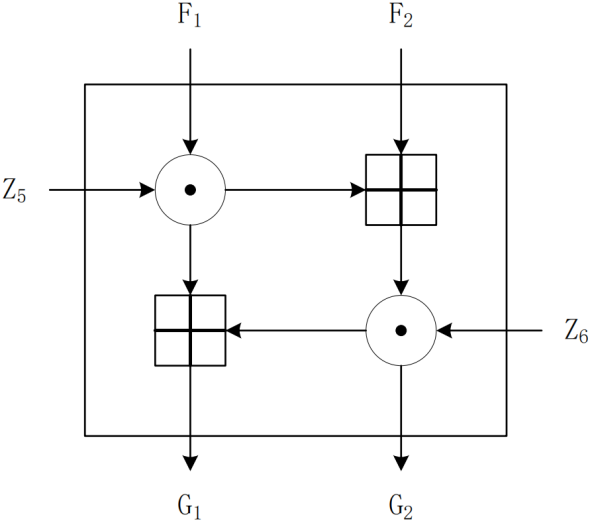


图2.6 MA运算器结构

安全性

目前，Eurocrypt'97会议上提出两种针对IDEA的攻击方法，但这两种攻击方法并未对IDEA的安全性构成威胁。就现在来看，应当说IDEA是非常安全的。

IDEA分组密码已在欧洲取得专利，而在美国的专利还悬而未决，不存在非商用所需的使用许可证费用问题。

##### （8）高级加密标准AES

高级加密标准AES，在密码学中又称Rijndael加密法，由美国国家标准与技术研究院于2001年11月26日发布于FIPS PUB 197，并在2002年5月26日成为有效的标准。这个标准用来替代原先的DES，已经被多方分析且广为全世界所使用，AES已然成为对称密钥加密中最流行的算法之一。

严格地说，AES和Rijndael加密法并不完全一样（虽然在实际应用中两者可以互换），因为Rijndael加密法可以支持更大范围的分组和密钥长度：AES的分组长度固定为128 比特，密钥长度则可以是128，192或256比特；而Rijndael使用的密钥和分组长度可以是32位的整数倍，以128位为下限，256比特为上限。

**1）SP网络**

不同于它的前任标准DES，AES算法在整体结构上（如图2.8所示）采用的是代换—置换SP网络（Substitutionpermutation Network）组成的圈函数，多圈迭代，而非Feistel网络结构。

SP网络（又称SP结构）是Feistel网络的一种扩展，其结构清晰。S一般称为混淆层，主要起到混淆作用；P一般称为扩散层，主要起到扩散作用。SP网络与Feistel网络相比，可以得到更快速的扩散，不过SP网络的加解密通常不相似。两者最大的区别在于：SP网络每轮改变整个数据分组，而

Feistel网络每轮只改变输入分组的一半。

#### 3．分组密码工作模式

即使有了安全的分组密码算法，也需要采用适当的工作模式来隐蔽明文的统计特性、数据的格式等，以提高整体的安全性，降低删除、重放、插入和伪造成功的机会。

分组密码的工作模式是一个算法，它刻画了如何利用分组密码提供信息安全服务。主要有五种工作模式，它们分别是电子密码本ECB（Electronic Codebook Mode）模式、密码分组链CBC（Cipher Block Chaining Mode）模式、密码反馈CFB（Cipher Feedback Mode）模式、输出反馈OFB（Output Feedback Mode）模式、计数CTR（Counter Mode）模式。

**（1）电子密码本模式**

直接利用分组密码对明文的各分组进行加密。设明文，相应的密文，其中：

电子密码本是分组密码的基本工作模式。

ECB的一个缺点是要求数据的长度为分组密码长度的整数倍，否则最后一个数据块将是短块，这时需要特殊处理。

ECB的另一缺点是容易暴露明文的数据模式。

ECB容易遭受重放攻击。攻击者通过重放，可以在不知道密钥情况下修改被加密过的消息，用这种办法欺骗接收者。例如在实际应用中，不同的消息可能会有一些比特序列是相同的（消息头），攻击者重放消息头，修改消息体以欺骗接收者。

**（2）密码分组链模式**

明文要与前面的密文进行异或运算然后被加密，从而形成密文链。密码分组链模式的运行原理如图2.11所示。每一分组的加密都依赖于所有前面的分组。在处理第一个明文分组时，与一个初始向量（IV，Initialization Vector）组进行异或运算。IV不需要保密，它可以明文形式与密文一起传送。

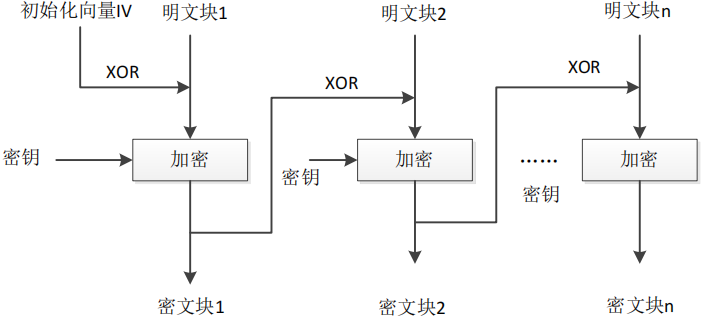


图2.11 密码分组链模式

输出反馈模式的工作原理如图2.12所示。其中，R为级寄存器，E为分组密码，如DES、IDEA、AES等强密码，I0为寄存器R的初始状态并称为种子，K为密钥。

分组密码E把寄存器R的状态内容作为明文，并加密成密文。E输出的密文又反馈到寄存器R，用作下一次加密的输入。E输出的密文的最右位（为了提高速度可输出最右边的8位）作为密钥序列输出，与明文异或实现序列加密。

这种工作模式将一个分组密码转换为一个序列密码，具有普通序列密码的优缺点，如没有错误传播、适合加密冗余度较大的数据、语音和图像数据，但对密文的篡改难以检测。

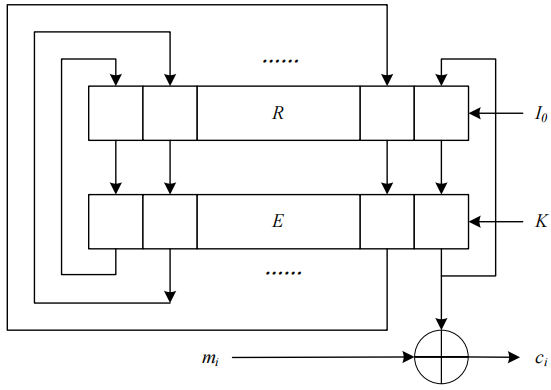


图2.12 输出反馈模式的工作原理

**（4）密码反馈模式**

密文反馈模式的工作原理与输出反馈的工作原理基本相同，所不同的仅仅是反馈到寄存器R的不是E输出的最右位，而是异或加密之后的。

**（5）计数模式**

计数模式使用一个计数ctr（也是一个初始向量），工作过程如图2.13所示，加解密运算如下：

注意该模式不需要计算Ek的逆。该模式的优点是可以并行、可以预处理、可证明其安全性至少与CBC一样好、加密与解密仅涉及密码算法的加密等。

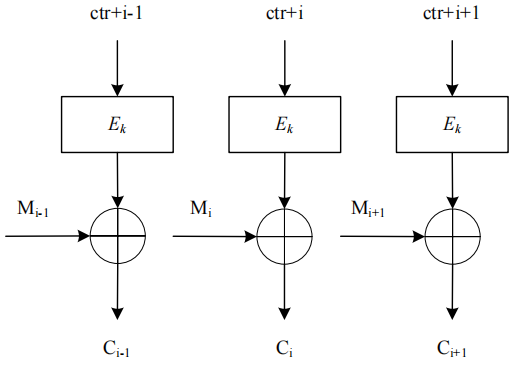


图2.13 计数模式

#### 4．非对称密码

对称加密最大的缺点在于其密钥管理困难，因为通信的双方必须首先预约相同的密钥后才能进行加密，而且在网络环境下，为了安全，密钥应当经常更换，在用户越多的情况下，密钥的数量及管理难度相应增加。此外，对称加密不易实现数字签名，也限制了它的应用范围。

1976年Diffie和Hellman第一次提出了公开密钥密码的概念，开创了一个密码新时代。

##### （1）基本概念

**1）基本思想**

公开密钥密码，也就是非对称密码体制，基本思想是将对称密码的密钥一份为二，分为加密密钥和解密密钥，用加密密钥控制加密，用解密密钥控制解密，而且由计算复杂性确保由加密密钥在计算上不能推出解密密钥。这样，即使是将公开也不会暴露，也不会损害密码的安全。于是便可将公开，而只对保密。由于是公开的，只有是保密的，所以便从根本上克服了传统密码在密钥分配上的困难。

因此，公开密钥密钥体制中，一个用户有两个密钥，即公钥和私钥，加解密的过程如下：

① 如果要给一个拥有公钥的用户发送信息，则可以用其公钥执行加密算法，以加密明文得到密文。

② 用户收到密文之后，用自己的私钥执行解密算法以恢复明文m：。可见，加密算法和解密算法是可逆运算，即：，不过加解密过程使用的密钥不同，不同于对称加密无论是加密还是解密均使用相同的密钥。

注意：也可以表达为。

**2）数字签名的应用**

在非对称密码中，还有一个重要的特性，也就是加密和解密运算具有可交换性，即：

这个特性使得非对称密码可应用到数字签名中。一个拥有公钥和私钥的用户，实现数字签名的过程如下：

拥有公钥的可以用其私钥执行解密算法，以产生信息的签名信息。

要验证一个签名信息sig是否某用户的签名时，只需要用该用户的公钥Ke执行如下校验过程计算出校验值m’：，如果，那么验证成功，否则失败。

**3）安全性**

在安全性方面，非对称密码通常依赖于某个难解的数学难题。也就是说，基于难解问题设计密码是非对称密码设计的主要思想。

设求解的问题规模（如输入变量的个数或输入长度）为，若对于所有的n和所有长度为n的输入，计算最多可用步完成，则称问题的计算复杂度为。若f(n)为n的多项式，则称其为多项式复杂度。

粗略的说，计算机可以在多项式时间复杂度内解决的问题称为P（Polynomial，多项式）类问题，计算机在多项式时间复杂度内不可以解决的问题称为NP（NonDeterministic Polynomial，非确定多项式）类问题。NP类问题是一类困难的问题，其中一类最困难的问题称为NP完全问题，简称为NPC问题。

设计一个安全密码本质上要寻找一个难解的问题，这一设计思想揭示了密码的安全性与计算复杂性之间的相互依赖关系。非对称密码，即公开密钥密码，开拓了直接利用NPC问题设计密码的技术路线。

现在主要流行的非对称密码包括RSA、ElGamal、椭圆曲线密码（ECC，Elliptic Curves Cryptography）等。RSA基于大合数因式分解难的问题设计；ElGamal 基于离散对数求解困难的问题设计；而ECC基于椭圆曲线离散对数求解困难的问题设计。

4）优缺点

如上面提到的基本思想及其在数字签名的应用，公开密钥密码的优点在于从根本上克服了对称密码密钥分配上的困难，且易于实现数字签名。然而，由于公开密钥密码通常依赖于某个难解的问题设计，虽然安全性高，但降低了加解密效率，是公开密钥密码一大缺点。

在应用中，通常采用对称密码体制实现数据加密、公钥密码体制实现密钥管理的混合加密机制。

##### （2）RSA算法

1978年美国麻省理工学院的三名密码学者Rivest、Shamir和Adleman提出了一种基于大合数因式分解困难性的公开密钥密码，简称为RSA密码。RSA密码既可用于加密，又可用于数字签名，安全、易懂，已成为目前应用最广泛的公开密钥密码。

**1）RSA算法**

RSA算法基于一个十分简单的数论事实：将两个大素数相乘十分容易，但想要对其乘积进行因式分解却极其困难，因此可以将乘积公开作为加密密钥。

具体算法描述如下：

① 随机选择两个大素数和，和都保密；

② 计算，将公开；

③ 计算，保密；

④ 随机选取一个正整数，且与互素，将公开；和就构成了用户的公钥；

① 根据（≡表示模同余运算），计算出，保密；和构成了用户的私钥；

① 加密运算：；

② 解密运算：。

由以上算法可见，RSA密码的公开加密密钥，而保密的解密密钥。

说明，算法中的是一个数论函数，称为欧拉函数。表示在比n小的正整数中与互素的数的个数。例如，，因为在1、2、3、4、5中与6互素的数只有1和5两个数。若和是素数，且，则。

通过RSA加解密运算可以看出，加密和解密运算具有可交换性：

因此，RSA密码可同时确保数据的秘密性和数据的真实性。

**2）安全性**

密码分析者攻击RSA密码的一种可能的途径是截获密文C，从中求出明文M。他们知道：

因此n是公开的，要从C中求出明文M，必须先求出d，而d是保密的。但他们知道，e是公开的，要从中求出d，必须先求出φ(n)，而φ(n)是保密的。但他们知道： 。要从n求出p和q，只有对n进行因式分解。

由此可见，只要能对n进行因式分解，便可攻破RSA算法。虽然大合数因式分解是十分困难的，但是随着科学技术的发展，人们对于大合数因式分解的能力在不断的提高。1994年，成功分解了129位的大合数；1996年又破译了RSA130；1999年又破译了RSA140。现在，科学家们正向512位的RSA，即RSA154发起冲击。

因此，要应用RSA密码，应当采用足够大的整数n。普遍认为，n至少应取1024位，最好是2048位。除了通过因式分解攻击RSA外，还有一些攻击方法，但是还不能构成有效威胁。因此，完全可以认为，只要合理的选择参数，正确的使用，RSA就是安全的。

**3）RSA参数选择**

为了确保RSA密码的安全，必须认真选择RSA的密码参数。

1）p和q要足够大,只有p和q足够大，n=pq才能足够大，才能对抗因式分解攻击。

2）p和q应为强素数

3）p和q的差要大，即要大。如果p和q的差很小，因为n=pq，所以可以估算(p+q)/2=n1/2。例如，设p=2，q=3，n=6，(p+q)/2=2.5，而n1/2=2.45，完全可以用n1/2来估算(p+q)/2。

又因为((p+q)/2)2n=((pq)/2)2，所以在估算出(p+q)/2的值后，便可计算出上式左边的值。因为，假设p和q的差很小，所以上式左边的值很小。预示可以通过实验得出(pq)/2，进而求出p和q。

4）p1的q1的最大公因子要小。设攻击者截获了某个密文攻击者进行迭代加密攻击即令i=2, 3, …，依次计算：，如果，则必有于是通过迭代加密获得明文，攻击成功。

5）e的选择。为了使加密速度快，根据“反复平方乘”算法，e的二进制表示中应当含有尽量少的1。一种方法是选择尽可能小的e或选择某些特殊的e。有学者建议取e=3，但e太小是不安全的。如果e太小，对于小的明文M，则有，加密运算未取模。于是直接对密文C开e次方，便可求出明文M。于是有学者建议取e=65537，其二进制表示中只有两个1，它比3更安全，而且加密速度也很快。

6）d的选择。与e的选择类似，为了使解密（数字签名）速度快，希望选用小的d，但是d太小也是不好的。当d小于n的1/4时，已有求出d的攻击方法。

7）不要许多用户共用一个模数n。多用户共用一个相同的模数n，各自选用不同的e和d，这样实现简单，但是不安全。设M为明文，用户A的加密密钥为eA，用户B的加密密钥为eB，他们使用同一个模数n。于是两个密文为：  
  
  
，假设攻击者截获了CA和CB，那么他就知道了CA、CB、eA、eB和n，于是可以利用Euclidean算法找出两个整数r和s，满足。r和s中必有一个为负数，否则此式不能成立，假设r是负数。仍然利用Euclidean算法找CA-1，于是。

**（3）ElGamal算法**

ElGamal密码是除了RSA密码之外最有代表性的公开密钥密码。RSA密码建立在大整数因式分解的困难性之上，而ElGamal密码建立在离散对数的困难性之上。大整数的因式分解和离散对数问题是目前公认的较好的单向函数，因而RSA密码和ElGamal密码是目前公认的安全的公开密钥密码。

**1）离散对数问题**

设p为素数，若存在一个正整数α，使得，关于模p互不同余，则称为模p的本原元。显而易见若α为模p的本原元，则对于一定存在一个正整数k，使得。

设p为素数，α为模p的本原元，α的幂乘运算为

则称X为以α为底的模p的对数。求解对数X的运算为

由于上述运算是定义在模p有限域上的，所以称为离散对数运算。

从X计算Y是容易的，至多需要次乘法运算。可是从Y计算X就困难的多，利用目前最好的算法，对于小心选择的p将至少需用次以上的运算，只要p足够大，求解离散对数问题是相当困难的。

这便是著名的离散对数问题。可见，离散对数问题具有较好的单向性。由于离散对数具有较好的单向性，所以离散对数问题在公钥密码学中得到广泛应用。除了ElGamal密码外，DiffieHellman密钥分配协议和美国数字签名标准算法DSA等也都是建立在离散对数问题之上的。

**2）ElGamal密码**

随机选择一个大素数p，且要求p1有大素数因子。再选择一个模p的本原元α，将p和α公开。

**密钥生成**

用户随机的选择一个整数d作为自己的秘钥，，计算，取y为自己的公钥。

**加密**

将明文消息加密成密文的过程如下：

① 随机选择一个整数k，。

② 计算

③ 取(C1, C2)作为密文

**解密**

将密文(C1, C2)解密的过程如下：

1. 计算
2. ② 计算

解密的可还原性可证明如下：因为，

故解密可还原。

**3）安全性**

由于ElGamal密码的安全性建立在GF(p)离散对数的困难性上，而且前尚无求解GF(p)离散对数的有效算法，所以在p足够大时ElGamal密码是安全的。

为了安全，p应该为150位以上的十进制数，而且p-1应有大素因子。此外，为了安全加密和签名所使用的k必须是一次性的。这是因为，如果使用的k不是一次性的，时间长了就可能被攻击者获得。又因y是公开密钥，攻击者就可以计算出U，进而利用Euclid算法求出U-1。又因为攻击者可以获得密文C2，因此可以通过计算U-1 C2得到明文M。另外，假设用同一个k加密两个不同的明文M和M’，相应的密文为(C1,C2) 和(C1’, C2’)。因为C2 / C2’ = C1 / C1’，如果攻击者知道M，则很容易求出M’。

**（4）椭圆曲线密码**

1985年，Koblitz和Miller在各自开发的新的公钥加密法中提出了使用椭圆曲线。 曲线是由如下的方程式定义的：

其中p为一个素数或2的幂（有时也称为椭圆曲线的秩），且。

表2.13列出了实现同等级别的安全性所需的密钥大小，从中可以看出，ECC比RSA更好。

|  |  |  |
| --- | --- | --- |
| 安全性 | RSA | ECC |
| 低 | 512 | 112 |
| 中 | 1024 | 161 |
| 高 | 3072 | 256 |
| 很高 | 15360 | 512 |

表2.13 同等安全级别所需密钥大小

### 2.1.2 哈希函数

哈希（hash）函数又称为散列函数、杂凑函数，它是一种单向密码体制，即它是一个从明文到密文的不可逆映射，只有加密过程，没有解密过程。

哈希函数可以将任意长度的输入经过变换后得到固定长度的输出。这 个 固 定 长度 的 输 出 称为 原 消 息 的“ 散 列 ” 或“ 消 息 摘要”（Message Digest）。哈希函数的数学表述为：

其中是哈希函数，是任意长度明文，是固定长度的哈希值。

理想的哈希函数对于不同的输入，获得的哈希值不同。如果存在x、x’两个不同的消息，存在，则称和是哈希函数H的一个碰撞。

哈希函数的这种单向的特性以及长度固定的特征使得它可以生成消息或者数据块的“消息摘要”（也称为散列值、哈希值），因此，在数据完整性和数字签名领域有着广泛的应用。

典型的哈希函数有两类：消息摘要算法MD5（Message DigestAlgorithm）和安全散列算法SHA（Secure Hash Algorithm）。

#### 1．哈希函数的性质

哈希算法有一些特点：

① 压缩。对于任意大小的输入x，哈希值H(x)的长度很小，实际应用中哈希函数H产生的哈希值是固定长度的。

② 易计算。对于任意给定的消息，容易计算其哈希值。

③ 单向性。对于给定的哈希值h，要找到m’使得H(m’) = h在计算上是不可行的，即求哈希函数的逆很困难。

④ 抗碰撞性。理想的哈希函数是无碰撞的，但实际算法设计中很难做到。因此有两种抗碰撞性：一种是弱抗碰撞性，即对于给定的消息x，要发现另一个消息y，满足H(x)= H(y)在计算上不可行；一

种是强抗碰撞性，即对任意一对不同的消息(x, y)，使得H(x)= H(y)在计算上不可行。

⑤ 高灵敏性。当一个输入位发生变化时，输出位将有一半以上会发生变化。

#### 2．哈希函数的应用

**消息认证**：在一个开放通信网络的环境中，信息面临的攻击包括窃听、伪

造、修改、插入、删除、否认等。因此，需要提供用来验证消息完整性的一

种机制或服务，即消息认证。这种服务的主要功能包括确保收到的消息确实

和发送的一样、确保消息的来源真实有效等，用于消息认证的最常见的密码

技术是基于哈希函数的消息认证码。

**数字签名**：由于非对称算法的运算速度较慢，所以在数字签名协议中，哈希函数扮演了一个重要的角色。对哈希，又称“消息摘要”进行数字签名，在统计上可以认为与对文件本身进行数字签名是等效的。

**口令的安全性**：由于哈希函数具有单向性的特征，在口令保护中应用非常广泛。通常，口令仅仅将其哈希值进行保存，进行口令校验的时候比对哈希值即可，即使攻击者获得了保存的哈希值，也无法计算出口令。

**数据完整性**：比较熟悉的校验算法有奇偶校验和循环冗余校验码（CRC，Cyclic Redundancy Check）校验，这两种校验并没有抗数据篡改的能力，它们一定程度上能检测并纠正数据传输中的信道误码，但却不能防止对数据的恶意破坏。哈希算法 “消息摘要”的特性，使它成为目前应用最广泛的一种数据完整性校验和算法。

#### 3．消息摘要算法

消息摘要算法MD5可以对任意长度的明文，产生128位的消息摘要。

MD5算法是按512位进行处理的，对于任意长度的消息将首先通过填充的办法使其成为512的倍数。首先，要对任意长度的信息进行填充，使信息的长度等于L\*512+448，即长度≡448 mod 512，填充的方法为在消息后面先添加一个位“1”，再依次添加位“0”，直到长度满足条件为止；然后，将原始消息的长度以64位表示，添加在最后面，使得信息长度恰好达到512位的倍数。

然后，MD5将填充后的消息以512位为单元分为L个分组，然后对每个分组进行处理。对每分组处理的时候，都执行4轮非常相似的运算，每一轮包括了16个类似的步骤。

**安全性**

对于攻击者而言，找到两个不同的明文却有相同的MD5明文摘要，至少需要264次运算。对于任意的明文摘要，要找到相对应的明文则需要2128次运算。虽然如此，已有一些攻击对MD5算法非常不利：

① Berson已经证明，对单轮的MD5算法，利用差分密码分析，可以在合理的时间内找出摘要相同的两条消息，这一结果对MD5的4轮运算中的每一轮都成立。但是Berson尚不能说明如何将这种攻击推广到具有4轮运算的MD5之上。

② Boer和Bosselaers说明了如何找到消息分组X和两个有关的链接变量使得它们产生相同的输出，也就是说，对一个512位的分组，MD5压缩函数对缓冲区ABCD的不同值产生相同的输出，称之为伪碰撞。目前尚无法用上述方法成功地攻击MD5算法。

③ Dobbertin提出的攻击对MD5最具威胁, 它可使MD5压缩函数产生碰撞。但到目前为止, 尚不能用Dobbertin提出的方法对使用初值的整个消息进行攻击。

④ 2004年，Xiaoyun Wang的算法在预定的时间内找到了MD5的一个碰撞。

4．安全散列算法

美国国家标准局NIST为配合数字签名标准，在1993年对外公布了安全散列算法（SHA，Secure Hash Algorithm）。SHA算法家族一共包含5个单向散列算法SHA-1、SHA-224、SHA-256、SHA-384和SHA-512。前三者适用于长度不超过264二进制位的消息，后两者适用于长度不超过2128二进制位的消息。

SHA对任意长度明文的预处理和MD5的过程是一样的，也即预处理完毕后的明文长度是512位的整数倍。SHA的输出是160位，分别存储于5个32位的记录单元中。

**与MD5的区别**

表2.18列出了MD5与SHA的比较差异之处。

① 安全性。SHA所产生的摘要较MD5长32位。若两种散列函数在结构上没有任何问题的话，SHA比MD5更安全。因为即使用“生日攻击法”伪造签名，要找到两个不同明文，但有相同摘要值的复杂度，在MD5中要264次运算，但在SHA中要280次运算。

② 速度。两种方法都是主要考虑以32位处理器为基础的系统结构。但SHA的运算步骤较MD5多了16个步骤。而且SHA记录单元的长度较MD5多了32位。因此若是以硬件来实现SHA，其速度大约较MD5慢了25%。

③ 简易性。两种方法都是相当的简单，在实现上不需要很复杂的程序或是大量的存储空间。然而总体上来讲，SHA对每一步骤的操作描述较MD5简单。

|  |  |  |
| --- | --- | --- |
| 差异处 | MD5 | SHA |
| 摘要长度 | 128 | 160位 |
| 运算步骤数目 | 64 | 80 |
| 基本逻辑函数数目 | 4 | 4 |
| 常数数目 | 64 | 4 |

表2.18 MD5与SHA的差异

### 2.1.3 数字签名

在人们的工作和生活中,许多事物的处理需要当事者签名。例如，政府部门的文件、命令、证书、商业的合同，财务的凭证等都需要当事者签名。签名起到确认、核准、生效和负责任等多重作用。

实际上，签名是证明当事者的身份和数据真实性的一种信息。既然签名是一种信息，因此签名可以用不同的形式来表示。在传统的以书面文件为基础的事物处理中，采用书面签名的形式、如手签、印章、手印等。书面签名得到司法部门的支持，具有一定的法律意义。在以计算机文件为基础的现代事物处理中，应采用电子形式的签名，即数字签名（Digital Signatuer）。

#### 1．概念

数字签名是一种以电子形式存在于数据信息之中的，或作为其附件或逻辑上与之有联系的数据，可用于辨别数据签署人的身份，并表明签署人对数据信息中包含的信息的认可的技术。

一种完善的数字签名机制应满足以下三个条件：

① 签名者事后不能抵赖自己的签名。

② 其它任何人不能伪造签名。

③ 如果当事人双方关于签名的真伪发生争执，能够在公正的仲裁者面前通过验证签名来确认其真伪。

数字签名通过密码技术实现，其安全性取决于密码体制的安全程度，因而可以获得比书面签名更高的安全性。虽然利用传统密码也可以实现数字签名，但是难于达到与书面签名一样的效果，因此不能使用。公开密钥密码不仅能够实现数字签名，而且安全方便。这是公开密钥密码深受欢迎的主要原因之一。自从公开密钥密码出现之后，数字签名技术日臻成熟，现已得到普遍应用。

目前主要是基于公钥密码体制的数字签名。包括普通数字签名和特殊数字签名。普通数字签名算法有RSA、ElGamal、椭圆曲线数字签名算法等。特殊数字签名有盲签名、代理签名、群签名、不可否认签名、具有消息恢复功能的签名等，它与具体应用环境密切相关。显然，数字签名的应用涉及到法律问题，1994年美国联邦政府制定了自己的数字签名标准DSS，1995年我国也制定了自己的数字签名标准（GB158511995）。

#### 2．工作原理

设用户A要向用户B发送文件M，数字签名主要研究解决这一过程中以下问题：

① A如何在文件M上签名？

② B如何验证A的签名的真伪？

③ A如何鉴别别人伪造自己的签名？

④ B如何阻止A签名后又抵赖？

一个数字签名体制都要包括两个过程：签名和验证签名。

设签名的算法为SIG，产生签名的密钥为K，被签名的数据为M，产生的签名信息为S，则有

设验证签名的算法为VER，用以对签名S进行验证，可鉴别S的真假。

即

##### （1）签名过程

A用自己保密的解密密钥KdA 对明文数据M进行签名：

SA 即为A对M的签名。如果不需要保密，则A直接将SA 发送给用户B。如果需要保密，则A查阅PKDB，查到B的公开的加密密钥KeB，并用KeB对SA 再加密，得到密文C，

最后，A把C发送给B，并将SA 或C留底。

##### （2）验证签名过程

B收到后，若不是保密通信，则首先查阅PKDB，查到A的公开的加密密钥KeA，然后用K\_{eA}对签名进行验证，

E( S\_A, K\_{eA})= E( D(M, K\_{dA}) , K\_{eA}) = M

若是保密通信，则B首先用自己的保密的解密密钥K\_{dB}对C解密，然后查阅PKDB，查到A的公开的加密密钥KeA，用KeA对签名进行验证，

验证签名的过程就是恢复明文的过程。如果能够恢复出正确的M，则说明SA 是A的签名，否则SA不是A的签名。

B将收到的SA 或者C留底。

B给A发回“收到M”的签名回执。

A收到回执后同样验证签名并留底。

因为只有A才拥有KdA，而且由于公开的KeA在计算上不能求出保密的解密密钥KdA。因此签名操作只有A才能进行，任何其它人都不能进行。所以，KdA就相当于A的印章或指纹，而SA 就是A对M的签名。对此A不能抵赖，任何其它人不能伪造。

事后如果A和B关于签名的真伪发生争执，则他们应向公证的仲裁者出示留底的签名数据，由仲裁者当从验证签名，解决纠纷。

##### （3）应用问题

对于上述签名通信，还有几个待解决的问题。第一，验证签名的过程就是恢复明文的过程。如果B能够恢复出明文M，那么B怎么判定恢复出的M是否正确的呢？第二，怎样阻止B或A用A以前发给B的签名数据，或用A发给其它人的签名数据来冒充当前A发给B的签名数据呢？仅仅

靠签名本身并不能解决这些问题。

对于这两个问题，只要合理实际明文的数据格式便可以解决。

一种可行的明文数据格式如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 发方标识符 | 收方标识符 | 报文序号 | 时间 | 数据正文 | 纠错码 |

形式上可将A发给B的第I份报文表示为：

进一步将附加包头数据记为

于是，A以<H，SIG( M, KdA) >为最终报文发给B，其中H为明文形式。由于以明文形式加入了发方标识符、收方标识符、时间等附加信息，就使得任何人一眼就可识破B或A用A以前发给B的签名报文，或用A发给其它人的签名报文来伪造冒充当前A发给B的签名报文的伪造或抵赖行为。其次，B收到A的签名报文后，只要用A的公开密钥验证签名并恢复出正确的附加信息 H = <A，B，I>，便可断定明文M是否正确，而附加H=<A，B，I>的正确与否B是知道的。设验证签名时恢

复出的附加信息为 H\* =<A\*，B\*，I\*>，而接收到的报头数据为H =<A，B，I>，当且仅当A\* = A 且B\* =B且I\* =I时我们认定恢复出正确的附加信息H = <A，B，I>。

注意，实际应用中为了缩短签名的长度、提高签名的速度，而且为了更安全，常对信息的摘要进行签名，这时M的哈希值代替M，而且数据格式也要结合实际认真设计。

#### 3. 美国数字签名标准

从1994年美国政府颁布了数字签名标准（DSS，Digital Signature Standard）以来，至今尚未发现DSS有明显缺陷。目前，DSS的应用已十分广泛，并被一些国际标准化组织采纳作为标准。2000年1月美国政府将RSA和椭圆曲线密码引入数字签名标准DSS，进一步丰富了DSS算法。

##### （1）算法参数

DSS的签名算法称为DSA（Digital Signature Algorithm），DSA使用以下参数：

① p为素数，要求2L-1<p<2L，其中512≤L≤1024 且L为64的倍数。即

② q为一个素数，它是（p1）的因子，2159<q<2160。

③ ，其中，且满足。

④ x 为一个随机数，0<x<q。

⑤ 。

⑥ k为一个随机数，0< k<g。

这里参数p，q，g可以公开，且可为一组用户共用。x和y分别为一个用户的私钥和公钥。所有这些参数可在一定时间内固定。参数x和k用于产生签名，必须保密。参数k必须对每一签名都重新产生，且每一签名使用不用的k。

##### （2）签名的产生

对数据M的签名为数r和s，分别如下计算产生：

其中k-1为k的乘法逆元素，即kk-1=1 mod q，且 0<k1<q。SHA是安全哈希函数，它将计算数据M的摘要SHA(M)，SHA(M)是一个160位的二进制数字串。

应该检验计算所得的r和s是否为零，若r = 0或s = 0，则重新产生k，并重新计算产生签名r和s。

最后，把签名r和s附近在数据M后面发给接收者：

|  |  |  |
| --- | --- | --- |
| M | r | s |

##### （3）验证签名

为了验证签名，要使用产生p，q，g，用户的公开密钥y和其标识符。

令MP、rP、sP分别为接收到的M、r和s。

① 先检验是否有，若其中之一不成立，则签名为假。

②计算：

若v=rP，则签名为真，否则签名为假或数据被篡改。

#### 4. 应用

**（1）鉴权**

公钥加密系统允许任何人在发送信息时使用公钥进行加密，数字签名能够让信息接收者确认发送者的身份。当然，接收者不可能百分之百确信发送者的真实身份，而只能在密码系统未被破译的情况下才有理由确信。

鉴权的重要性在财务数据上表现得尤为突出。举个例子，假设一家银行将指令由它的分行传输到它的中央管理系统，指令的格式是(a,b)，其中a是账户的账号，而b是账户的现有金额。这时一位远程客户可以先存入100元，观察传输的结果，然后接二连三的发送格式为(a,b)的指令。这种方法被称作重放攻击。

**（2）完整性**

传输数据的双方都希望确认消息未在传输的过程中被修改，即校验数据的完整性。加密使得第三方想要读取数据十分困难，然而第三方仍然能采取可行的方法在传输的过程中修改数据。一个通俗的例子就是同形攻击：回想一下，还是上面的那家银行从它的分行向它的中央管理系统发送格式为(a, b)的指令，其中a是账号，而b是账户中的金额。一个远程客户可以先存100元，然后拦截传输结果，再传输(a, b3)，这样他就立刻变成百万富翁了。

**（3）不可抵赖**

在密文背景下，抵赖这个词指的是不承认与消息有关的举动（即声称消息来自第三方）。消息的接收方可以通过数字签名来防止所有后续的抵赖行为，因为接收方可以通过出示签名给别人看来证明信息的来源。

### 2.1.4 密钥管理

无论是对称密码还是非对称密码，其安全性实际取决于对密钥的安全保护。在一个信息安全系统中，密码体制、密码算法可以公开，甚至如果所用的密码设备丢失，只要密钥没有被泄漏，保密信息仍是安全的。而密钥一旦丢失或出错，不但合法用户不能提取信息，而且非法用户也可能会窃取信息。因此，密钥管理成为信息安全系统中的一个关键问题。

#### 1．基本概念

现代密码学把数据加密保护的全部系于密钥之上，所以密钥的安全管理是保证密码系统安全性的关键因素。

密钥管理是指处理密钥自产生到最终销毁的有关问题的全过程，大体上讲，密钥管理包括密钥的生成、存储、分配、启用与停用、控制、更新、撤销与销毁等诸多方面，其中密钥的分配与存储最关键。

**（1）密钥的种类**

密钥种类很多，但主要有以下几种：

① 基本密钥或初始密钥

基本密钥是由用户选出或由系统分配给用户的可在较长时间（相对于会话密钥）内用户所专用的秘密密钥，又称用户密钥。基本密钥和会话密钥一起启动和控制由某种算法所构造的密钥产生器，以此产生用于加密数据的密钥流。

② 会话密钥

会话密钥是两个通信终端用户在一次交换数据时所采用的密钥，当用其保护传输数据时称为数据加密密钥，当用其保护文件时称为文件密钥。会话密钥可由通信双方预先约定，也可由系统动态地产生并赋予通信双方，它为通信双方专用，故又称为专用密钥。

③ 密钥加密密钥

密钥加密密钥（KEK，Key Encryption Key）是对传送的会话或文件密钥进行加密时采用的密钥，也称次主密钥。

④ 主机主密钥

主机主密钥是对密钥加密密钥进行加密的密钥，存于主机处理器中。此外还有用户密钥、族密钥和算法更换密钥等。

**（2）密钥生成**

不同种类的密钥，从安全角度有不同的要求，因此生成算法有所不同。

**（3）密钥存储**

将密钥保存到一个合适的载体上，如磁卡、智能IC卡、U盘等上面，使用时通过专用读取器输入终端设备。

**（4）密钥分配**

密钥分配是指密码系统中密钥的安全分发和传送过程，它要解决的问题就是将密钥安全地分配给保密通信的各方。目前有关密钥分配方案多种多样。

**（5）密钥替换与更新**

当密钥已泄漏、被破坏或将要过期时，就要产生新的密钥来替换或更新旧的密钥。

**（6）密钥撤销**

如果密钥丢失或其它原因在密钥未过期之前，需要将它从正常运行使用的集合中除去，称为密钥的撤销。

**（7）密钥销毁**

不用的旧密钥必须被销毁。

**（8）密钥有效期**

密钥有效期就是密钥的生命期，不同性质的密钥应根据其不同的使用目的有不同的有效期。一个密码应用系统，必须有一个策略能够检验密钥的有效期。

#### 2．密钥产生

密钥是数据保密的关键，应采用足够安全的方法来产生密钥。对密钥的一个基本要求是要具有良好的随机性，一个真正的随机序列是不可再现的，任何人都不能再次产生它，然而高效的产生高质量的真正随机序列，并不是容易的事。

对称密码的密钥本质上是一种随机数或随机序列，因此，密码产生本质上是产生具有良好密码学特性的随机数或随机序列，随机数的产生办法包括硬件和软件技术。

**（1）密钥产生的硬件技术**

噪声源技术是密钥产生的常用方法。因为噪声源具有产生二进制的随机序列或与之对应的随机数的功能，成为密钥产生设备的核心组件。随机数的产生常采用物理噪声源的方法。目前的物理噪声源主要包括基于力学的噪声源、基于电子学的噪声源以及基于混沌理论的密钥产生技术等。

① 基于力学噪声源的密钥产生技术

利用硬币、骰子等抛散落地的随机性产生密钥，这种方法效率低，而且随机性较差。

② 基于电子学噪声源的密钥产生技术

这种方法利用电子方法对噪声器件（如真空管、稳压二极管等）的噪声进行放大、整形处理后产生密钥随机序列。根据噪声迭代的原理将电子器件的内部噪声放大，形成频率随机变化的信号，在外界采样信号的控制下，对此信号进行采样锁存，然后输出信号为 “0”、“1”随机的数字序列。

③ 基于混沌理论的密钥产生技术

在混沌现象中，只要初始条件稍有不同，其结果就大相径庭，难以预测。在有些情况下，反映这类现象的数学模型又是十分简单。因此利用混沌理论的方法，不仅可以产生噪声，而且噪声序列的随机性好，产生效率高。

**（2）密钥产生的软件技术**

X9.17（X9.171985金融机构密钥管理标准）标准定义了一种产生密钥的方法。

X9.17算法使用三重DES，目的是在系统中产生一个会话密钥或是伪随机数，其过程如下：

假设E\_k(x)表示用密钥k对比特串x进行的三重DES加密，V0是一个秘密的64位种子，T是一个时间标记。产生的随机密钥Ri可以通过下面的两个算式来计算：

对于128位和192位密钥，通过以上方法生成几个64位的密钥后，串接起来就可以。

**（3）公钥体制下的密钥产生**

不同于对称密钥，公开密钥密码通常建立在某一数学难题之上，不同的公开密钥密码依据的难题不同，其密钥产生的具体要求不同。

对于RSA密码而言，其公开密钥，而保密的解密密钥，其密钥的产生主要根据安全性和工作效率来合理的产生相关的密钥参数。

一般来说p和q越大越安全，但效率就越低。根据目前因式分解的能力，对于一般应用，p和q至少要有512位，以使n至少有1024位。而对于重要应用，p和q至少要有1024位，以使n至少有2048位。此外，还要求p和q要随机，p和q差要大，e的二进制位要有尽可能少的1等。

对于椭圆曲线密码而言，私钥定义为一个随机数，公钥定义为椭圆曲线上的一个点。椭圆曲线密码的公钥和私钥的生成不困难，困难的是其系统参数的选取，也就是椭圆曲线的选取。

一般认为，目前椭圆曲线的参数n和p的规模应大于160位。参数越大越安全，但曲线选择越困难，资源的消耗也越多。

**（4）针对不同密钥类型的产生方法**

在大型计算机密码系统中，常采用主密钥、二级密钥和初级密钥三种不同等级的密钥，针对不同的密钥应采取的方法也不同。对于主密钥而言，通常应采用高质量的真正随机序列，而对于初级密钥，只要采用足够随机的伪随机序列就够了。

**1）主密钥的产生**

主密钥是控制产生其它加密密钥的密钥，而且长时间保持不变，因此它的安全是至关重要的。这类密钥通常要用诸如掷硬币、骰子，从随机数表中选数等随机方式产生，以保证密钥的随机性，避免可预测性。

**2）加密密钥的产生**

加密密钥可以由机器自动产生，也可以由密钥操作员选定。密钥加密密钥构成的密钥表存储在主机中的辅助存储器中，只有密钥产生器才能对此表进行增加、修改、删除和更换密钥，其副本则以秘密方式送给相应的终端或主机。

**3）会话密钥的产生**

会话密钥可在密钥加密密钥作用下通过某种加密算法动态地产生，比如用密钥加密密钥控制DES算法产生。

#### 3．密钥分配

密钥分配是密钥管理系统中最为复杂的问题，根据不同的用户要求和网络系统的大小，有不同的解决方法。

依据分配手段，密钥分配可分为人工分发（物理分发）与密钥交换协议动态分发两种。

从密钥属性上看，又分为秘密密钥分配与公开密钥分配两种。

从密钥分配技术来说，有基于对称密码体制的密钥分配与基于公钥密码体制的密钥分配。

从密钥信息的交换方式来说，可以分为人工密钥分发、基于中心的密钥分发和基于认证的密钥分发。

**（1）人工密钥分发**

在很多情况下，用人工的方式给每个用户发送一次密钥。然后，后面的加密信息用这个密钥加密后，再进行传送，这时，用人工方式传送的第一个密钥叫做密钥加密密钥。

然而，人工分配不适应现代计算机网络发展的要求。但是，对于主密钥而言，一般采用人工分配的方式，由专职密钥分配人员分配并由专职安装人员妥善安装。

**（2）基于中心的密钥分发**

基于中心的密钥分发利用可信任的第三方，进行密钥分发，实质上是利用公开密钥密码体制分配传统密码的密钥。

可信第三方可以在其中扮演两种角色：

① 密钥分发中心（KDC，Key Distribution Center）；

② 密钥转换中心（KTC，Key Translation Center）。

基于中心的密钥分发的优势在于，如果用户知道自己的私钥和KDC的公钥，就可以通过密钥分发中心获取他将要进行通信的他方的公钥，从而建立正确的保密通信。

基于中心的密钥分发有两种模型：拉模型和推模型。

在Kerberos中，如果主体Alice和Bob通信时需要一个密钥，那么，Alice需要在通信之前先从KDC获得一个密钥。这种模式又称为拉模式（Pull Model），如图2.21所示。

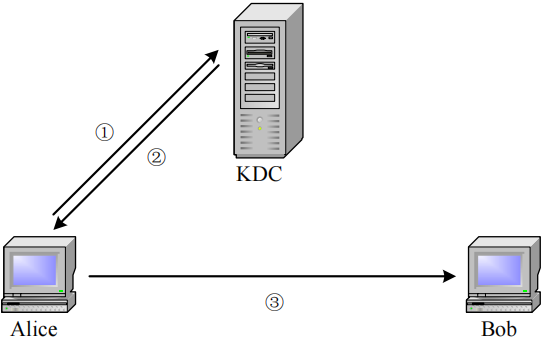


图2.21 拉模型示意

美国金融机构密钥管理标准（ANSI X9.17）要求通信方Alice首先要和Bob建立联系，然后，让Bob从KDC取得密钥。这种模式称为推模式（Push Model），表示是由Alice推动Bob去和KDC联系取得密钥。如图2.22所示。

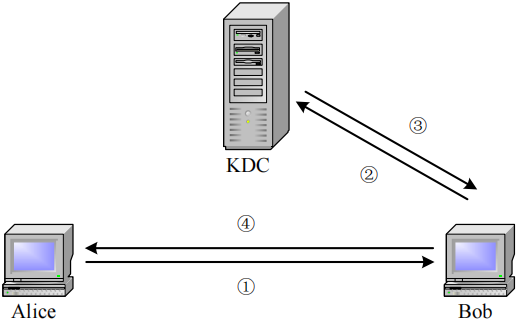


图2.22 推模型示意

在安全性方面，两种模型没有优劣之分，至于要实现哪种模型要看具体的环境而定。在Kerberos实现认证管理的本地网络环境中，把获得密钥的任务交给大量的客户端，这样可以减轻服务器的负担。而在使用X9.17设计的广域网环境中，采用由服务器去获得密钥的方案会好一些，因为服务器一般和KDC放在一起，而客户端通常和KDC离的很远。

**（3）密钥交换协议**

最典型的密钥交换协议是DiffieHellman算法。

DiffieHellman算法是第一个实用的在非保护信道中创建共享密钥方法，本身是一个匿名（无认证）的密钥交换协议，已成为很多认证协议的基础。

在DiffieHellman算法中，有两个全局公开的参数，分别为一个素数q和一个整数g，g是q的一个原根。

首先，Alice随机选取a，计算出A=ga mod p；Bob随机选取b，计算出B=gb mod p。

然后，Alice和Bob交换A和B。

此时，Alice和Bob就分别计算出共享的密钥 = 了：

应当注意到，Diffie Hellman密钥交换协议不支持对所建立的密钥的认证。处于两个通信参与者Alice和Bob之间的一个恶意的攻击者Mallary可以主动操纵协议运行过程的信息并成功实施所谓的中间人攻击（Maninthemiddle Attack）。因此，为了能够真正在两个通信参与者Alice和Bob之间协商一个密钥，就必须确保他们在协议运行过程中收到的信息来自真实的对方。

**（4）公开密钥分配**

公开密钥分配有如下几种方法：

① 公开发布

公开发布是指用户将自己的公钥发给每一其它用户，或向某一团体广播。

优点：简单。

缺点：任何人都可以伪造这种公开发布。

② 公用目录

公用目录表是指建立一个公用的公钥动态目录表，公用目录的建立、维护及公钥的分发由某个可信的实体或组织承担。

优点：比公开发布的安全性更高。

缺点：公钥目录表可能被伪造，也易受到对手窜扰。

③ 公钥授权

类似公用目录表，假定有一个公钥管理机构负责建立、维护通信各方公钥的动态目录表。此外，每个用户都可靠的知道管理机构的公开密钥，并且只有管理机构知道相应的秘密密钥。

公钥管理机构分配公钥如图2.23（根据教材自行解读）：

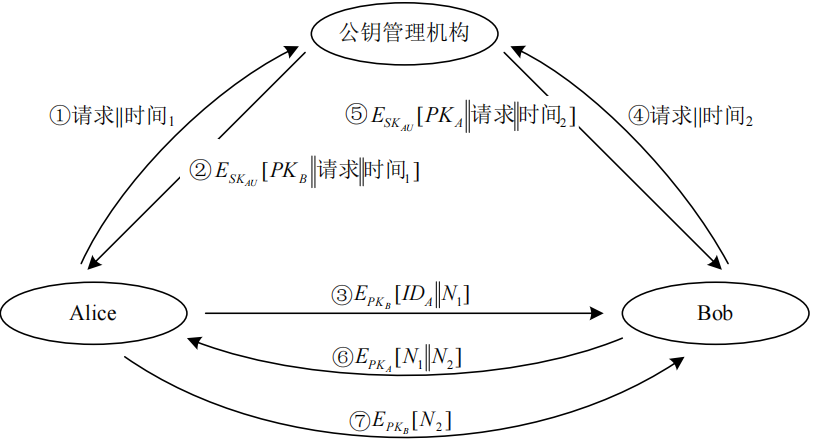


图2.23 公钥管理机构分配

优点：比前两种方法具有更高的安全性。

缺点：由于用户想要与他人联系都要求助公钥管理机构分配公钥，这样公钥管理机构可能成为系统的瓶颈，另外维护的公钥目录表也可能被对手窜扰。

④ 公钥证书

公钥证书方式是指用户通过公钥证书交换自己的公钥而无须与公钥管 理 机 构 联 系 ， 公 钥 证 书 由 证 书 管 理 机 构 （ CA ， Certification Authority）为用户建立。用户可将自己的公开钥通过公钥证书发给另一用户，接收方可用CA的公钥对证书加以验证。

优点：克服了公钥管理机构模式的不足。

基于公钥证书的密钥分发方法是目前广泛流行的密钥分发机制。

#### 4．密钥存储

由于密码机制的安全性主要依赖于密钥，因此密钥需要妥善保存。

（1）公钥存储

公钥通常被分发或提供给其它用户，但还必须通过中央权威机构（通常是证书管理机构CA）认证以便证明它属于密钥对的拥有者

（2）私钥存储

无论对称加密体制，还是非对称加密，用户的私钥都需要妥善保存。私钥管理是公钥系统安全中薄弱的环节。私钥存储方案有如下几种：

① 用口令加密后存放在本地软盘或硬盘

利用口令保护私钥非常简洁，但是用户使用时需要插入软盘或者利用存放在硬盘的文件，限制了用户的灵活性。而且存放的文件容易被复制，虽然经过口令加密，但是存在离线口令猜测攻击漏洞。这种方法适合于机器和用户固定的办公环境。

② 存放在网络目录服务器中

将用户的私钥集中存放在特殊的服务器中，用户可以通过一定的安全协议使用口令来获得自己的私钥和修改自己的私钥和口令，这种方式称为私钥存储服务（PKSS，Private Key Storage Service）。

优点在于由专职系统管理人员和专门的服务器对用户私钥进行集中存储和管理，用户必须通过相应的安全协议证实自己的身份后才能获得加密后的私钥，用户可以不限定在固定的某台机器上，减轻了第一种方法中密钥分散管理带来的不便和负担。

缺点在于容易遭到口令猜测攻击。

③ 智能卡存储

智能卡（Smart Cards）同普通信用卡的大小差不多，提供了抗修改能力，用于保护其中的用户证书和私钥。利用智能卡来存放用户的私钥比使用口令方式有更高的安全性。采用智能卡进行认证时，需要特殊的硬件读卡器，目前还难以全面推广。

④ USB Key存储

USB Key又称为电子钥匙，外形与普通的U盘类似。目前作为数字签名载体的智能卡及读卡器逐渐开始被USB Key产品所替代，后者除能实现智能卡的所有功能外，还利用USB技术将智能卡、读卡器的功能集于一身。USB Key内置CPU，可使得用户的私钥不出卡，所有的运算均在硬件内完成，从根本上保证了用户的私钥的安全，杜绝了用户密钥被截取的可能性。USB Key非常方便随身携带，并且密钥和证书不可导出，USB Key的硬件不可复制，更显安全可靠。由于使用计算机的USB端口，不需要专门的读取设备，不仅如此，USB Key的热插拔、易携带的特点也成为其迅速占领市场的重要因素。

#### 5．密钥更换与撤销

（1）密钥更换

密钥的使用是有寿命的，一旦密钥有效期到期，就必须消除原密钥存储区，或者使用随机产生的噪音重写。为了保证加密设备能连续工作，也可以在新密钥生成后，旧密钥仍保持一段时间，以防止密钥更换期间出现不能解密的问题。

密钥的更换，可以采用批密钥的方式，即一次注入多个密钥，在更换时可以按照一个密钥生效，另一个密钥废除的形式进行。替代的次序可以采用密钥的序号，如果批密钥的生成与废除是顺序的，则序数低于正在使用的密钥的所有密钥都已过期，相应的存储区清零。

（2）密钥吊销

密钥的寿命不是无限的。由于会话密钥只能存在于一个会话中，所以在会话结束时，这个密钥会被删除，不需要吊销它。一些密钥可能需要在给定的时间段内有效，一般来说，公钥对的有效期为一年到两年。有效的公钥会给出失效日期，在这个日期之后，读到该证书的系统不会认为它是有效的，因此不需要吊销已经失效的证书。不过，此类密钥可能丢失或者被攻击。在发生这种情况时，密钥的拥有者必须将密钥不再有效并且不应该继续使用这一情况通知其它用户。

## 2.2 认证技术

在网络通信环境中，可能有下述攻击：

① 泄密：将消息透露给没有合法密钥的任何人或程序。

② 传输分析：分析通信双方的通信模式。在面向连接的应用中，确定连接的频率和持续时间；在面向连接或无连接的环境中，确定双方的消息数量和长度。

③ 伪装：欺诈源向网络中插入一条伪造的消息。

④ 内容修改：对消息内容的修改，包括插入、删除、转换和修改。

⑤ 顺序修改：对通信双方消息顺序的修改，包括插入、删除和重新排序。

⑥ 计时修改：对消息的延时和重放。

⑦ 发送方否认：发送方否认发送过某消息。

⑧ 接收方否认：接收方否认接收到某消息。

对付前两种攻击的方法输入消息保密性范畴，在前面密码技术部分已经介绍了消息加密的方法；对付第3种到第6种攻击的方法一般称为消息认证。对付第7种攻击的方法属于数字签名。一般而言，数字签名方法也能够抗第3种到第6种中的某些或全部攻击。**对付第8种攻击需要使用数字签名和为抗此种攻击而设计的协议**。

### 2.2.1 消息认证

消息认证是验证所收到的消息确实来自真正的发送方，并且未被篡改的过程。

任何消息认证或数字签名方法在功能上基本可看作有两层。下层中一定有某种产生认证码的函数，认证码是一个用来认证消息的值；上层协议中将该函数作为原语使接收方可以验证消息的真实性。

产生认证码的函数类型，通常有三类：

① 消息加密：整个消息的密文作为认证码。

② 消息认证码（MAC，Message Authentication Code）：它利用密钥对消息产生定长的值，并以该值作为认证码。

③ 哈希函数：它将任意长的消息映射为定长的哈希值，并以该哈希值作为认证码。

#### 1．消息加密

消息加密本身提供了一种认证手段。在这种方法中，整个消息的密文作为认证码。

**（1）对称加密**

在传统密码中，如果发送方Alice要发送报文给接收方Bob，则Alice用他们共享的密钥K对发送的消息m加密后发送给Bob：

由于只有Alice和Bob知道密钥K，那么其它任何人均不能恢复出报文明文，因此，加密过程为消息提供了保密性。此外，Bob外只有Alice拥有密钥K，也就是只有Alice可产生Bob能解密的报文，所以Bob可相信该报文发自Alice，因此，加密过程提供了消息源的认证。因为攻击者不知道密钥K，所以也就不知如何改变密文中的信息位使得在明文中产生预期的改变。因此，若Bob可以恢复出明文，则Bob可以认为消息m中的每一位都未被改变。

由此可见，传统密码既可提供保密性又可提供认证。

但是给定解密算法D和密钥K，接收方可对接收到的密文c执行解密运算从而产生输出m’= DK( c )。因此要求接收方能对解密所得明文的合法性进行判别，但是这十分困难。例如，若明文是二进制文件，则很难确定解密后的报文是否是真实的明文。因此攻击者可以冒充合法用户来发布任何报文，从而造成干扰和破坏。

解决上述问题的方法之一是，在每个消息m后附加错误检测码，也称帧校验序列（FCS, Frame Check Sequence）或校验和：

若Alice要发送消息m给Bob，则将F( m )附于消息m之后：

发送方Alice把消息m和FCS一起加密后发送给Bob。接收方Bob解密出其收到的消息和附加的FCS，并用相同的函数F重新计算FCS。若计算得到的FCS和收到的FCS相等，则Bob认为报文是真实的。

**（2）非对称加密**

若利用公钥加密，则可提供认证和签名：  
  
 因为接收方Bob可能用发送方的公钥恢复出和，并将计算得出的与恢复出的比较。若相等，则Bob认为报文是真实的。

另外，Alice可以通过其私钥对报文签名，任何人均可用Alice的公钥恢复出报文，对报文进行验证，具体实现方法详见数字签名部分。

#### 2．消息认证码

消息认证码（MAC，Message Authentication Code）是一种认证技术，它利用密钥来生成一个固定长度的数据块，并将该数据块附加在消息之后。

假定通信双方共享密钥*K*。若发送方Alice向接收方Bob发送消息m，则Alice先使用消息认证码计算函数C计算MAC：

并将消息m和MAC发送给接收方：

接收方Bob收到消息后，用相同的密钥K进行相同的计算得出新的MAC，并将其与接收到的MAC进行比较。若二者相等则

① 接收方可以相信消息未被修改。如果攻击者改变了消息，因为已假定攻击者不知道密钥，所以他不知道如何对MAC做相应修改，这将使接收方计算出的MAC不等于接收到的MAC。

② 接收方可以相信消息来自特定的发送方。因为其它各方均不知道密钥，因此他们不能产生具有 正确MAC的报文。

③ 如果消息中加入序列号（如HDLC、X.25和TCP中使用的序列号），由于攻击者无法成功地修改序列号，因此接收方可以相信报文顺序是正常的。

**（1）保密性**

在上述方法中，消息是以明文形式传送的所以该方法可以提供认证，但不能提供保密性。若要获得保密性，可使用下面两种方法。

一种是在使用MAC算法之后对报文加密：

因为只有Alice和Bob共享K2，所以该方法可提供认证；因为只有Alice和Bob共享K1，所以该方法可以提供保密性。

另一种是在使用MAC算法之前对消息加密来获得保密性：

上述两种方法都需要两个独立的密钥，并且收发双方共享这两个密钥。第一种是先将消息作为输入，计算MAC，并将MAC附加在消息后，然后对整个信息加密形成待发送的信息块；第二种是先将消息加密，让后将此密文作为输入，计算MAC，并将MAC附加在密文之后形成待发送的信息块。通常使用的第一种方法，即将MAC直接附加于明文之后。

**（2）安全性**

从理论上讲，对不同的m产生的消息认证码MAC也不同，因为若，而，则攻击者可将m1篡改为m2，而接收方不能发现。换言之，函数C应与m的每一个位相关。否则若函数C与m中某位无关，则攻击者可篡改该位而不会被发现。但是要使函数C具备上述性质，将要求报文认证码MAC至少和消息m一样长，这是不现实的。因此，实际应用时要求函数C具有以下性质：

① 对已知和，结构满足的消息在计算上是不可行的；

② 应是均匀分布的，即对任何随机选择的报文和，的概率是，其中n是MAC的位数；

③ 设和的某个已知的变换，即，如f逆转的一位或者多位，那么的概率是。

性质①是为了阻止攻击者构造出与给定的MAC匹配的新消息。性质②是为了阻止基于选择明文的穷举攻击，也就是说，攻击者可以访问MAC函数，对报文产生MAC，这样攻击者就可以对各种消息计算MAC，直至找到与给定的MAC相同的报文为止。如果MAC函数具有均匀分布的特征，那么用穷举方法平均需要步才能找到具有给定MAC的消息。性质③要求认证算法对消息各部分的依赖应该是相同的，否则，攻击者在已知和时，可以对的某些已知的“弱点”处进行修改，然后计算MAC，这样有可能更早得出具有给定的MAC的新消息。

值得注意的是，MAC算法不要求可逆性，而加密算法必须是可逆的；一般而言，MAC函数是多对一函数，其定义域由任意长的消息组成，而值域由所有可能的MAC和密钥组成，因此，MAC函数与加密函数相比，要更不易被攻破；由于收发双发共享密钥，因此MAC不能提供数字签名功能。**（3）MAC算法示例**

基于DES的MAC算法是使用最广泛的MAC算法之一，可以满足上面提出的要求。首先，它将需认证的数据分成大小为64位的分组D1|| D2||…|| DN，若最后分组不足64位，则在其后填0直至成为64位的分组。然后，它基于密文反馈连接（CBC）的分组密码工作模式，计算得到认证码。

#### 3．哈希函数

单向哈希函数是消息认证码的一种变形。与消息认证码一样，哈希函数的输入是可变大小的消息m，输出是固定大小的哈希值H(m)。与MAC不同的是，哈希值并不使用密钥，它仅是输入消息的函数。哈希值也称为散列值，或消息摘要。哈希值是所有消息位的函数，它具有错误检测能力，即改变消息的任何一位或多位，都会导致哈希值的改变。

将哈希函数用于消息认证有如下几种方法：

① 用对称密码对消息及附加在其后的哈希值加密。

② 用对称密码仅对哈希值加密。对那些不要求保密性的应用，这种方法会减少处理代价。

③ 用公钥密码和发送方的私钥仅对哈希值加密。同②一样，这种方法可提供认证；由于只有发送方可以产生加密后的哈希值，所以这种方法也提供了数字签名。

④ 若既希望保证保密性又希望有数字签名，则先用发送方的私钥对哈希值加密，再用对称密码中的密钥对消息和上述加密结构进行加密。这种技术比较常用。

### 2.2.2 身份认证

为了保护网络资源及落实安全政策，需要提供可追究责任的机制。这里涉及到三个概念：认证、授权及审计。

① 认证（Authentication）：在做任何动作之前必须要有方法来识别动作执行者的真实身份。认证又称为鉴别、确认。身份认证通过标识和鉴别用户的身份，防止攻击者假冒合法用户获取访问权限。

② 授权（Authorization）：授权是指当用户身份被确认合法后，赋予该用户进行文件和数据等操作的权限。这种权限包括读、写、执行及从属权等。

③ 审计（Auditing）：每一个人都应该为自己所做的操作负责，所以在做完事情之后都要留下记录，以便核查责任。

#### 1．认证手段

身份认证的基本手段包括静态密码方式、动态口令认证、USBKEY认证以及生物识别技术等。**（1）静态密码方式**

静态密码方式是指以用户名及密码认证的方式，优点是无论使用还是部署都非常简单，是最常用的身份认证方法。但是，由于密码是静态的数据，在验证过程中需要在计算机内存中和传输过程可能会被木马程序或网络中截获。

因此，静态密码机制是一种不安全的身份认证方式。

**（2）动态口令认证**

动态口令是应用最广的一种身份识别方式，基于动态口令认证的方式主要有动态短信密码和动态口令牌（卡）两种方式，口令一次一密，大大提高了安全性。

① 短信密码以手机短信形式请求包含6位随机数的动态密码，身份认证系统以短信形式发送随机的6位密码到客户的手机上。客户在登录或者交易认证时候输入此动态密码，从而确保系统身份认证的安全性。

② 动态口令牌是客户手持用来生成动态密码的终端，主流的是基于时间同步方式的，每60秒变换一次动态口令，口令一次有效，它产生6位动态数字进行一次一密的方式认证。

①由于它使用起来非常便捷，85%以上的世界500强企业运用它保护登录安全，广泛应用在VPN、网上银行、电子政务、电子商务等领域。优点：采用一次一密的方法，不能由产生的内容去预测出下一次的内容。缺点：如果客户端硬件与服务器端程序的时间或次数不能保持良好的同步，就可能发生合法用户无法登录的问题，这使得用户的使用非常不方便。

**（3）USB Key认证**

基于USB Key的身份认证方式是近几年发展起来的一种方便、安全的身份认证技术。它采用软硬件相结合、一次一密的强双因子认证模式，很好地解决了安全性与易用性之间的矛盾。USB Key是一种USB接口的硬件设备，它内置单片机或智能卡芯片，可以存储用户的密钥或数字证书，利用USB Key内置的密码算法实现对用户身份的认证。

基于USB Key的身份认证系统主要有两种认证模式：

① 挑战/应答模式：每次认证时认证服务器端都给客户端发送一个不同的“挑战”字串，客户端程序收到这个“挑战”字串后，做出相应的“应答”。

② 基于PKI体系的认证模式：随着PKI技术日趋成熟，许多应用中开始使用数字证书进行身份认证与数字加密。数字证书是由权威公正的第三方机构即CA中心签发的，以数字证书为核心的加密技术，可以对网络上传输的信息进行加密和解密、数字签名和签名验证，确保网上传递信息的机密性、完整性，以及交易实体身份的真实性，签名信息的不可否认性，从而保障网络应用的安全性。

**（4）生物识别技术**

生物识别技术是指通过可测量的生物信息和行为等特征进行身份认证的一种技术。认证系统测量的生物特征一般是用户唯一生理特征或行为方式。优点：使用者几乎不可能被仿冒。缺点：较昂贵；不够稳定（辩识失败率高）。

#### 2．认证协议

**（1）基于口令的认证协议**

口令是双方预先约定的秘密数据，它用来验证用户知道什么。口令验证的安全性虽然不如其它几种方法，但是口令验证简单易行，因此口令验证是目前应用最为广泛的身份认证方法之一。

在计算机系统中，操作系统、网络、数据库，都采用了口令验证。

在一些简单的系统中，用户的口令以口令表的形式存储。当用户要访问系统时，系统要求用户提供其口令，系统将用户提供的口令与口令表中存储的相应用户的口令进行比较。若相等则确认用户身份有效，否则确认用户身份无效，拒绝访问。

但是，在上述口令验证机制中，存在下列一些问题：

① 攻击者可能从口令表中获取用户口令。因为用户的口令以明文形式存储在系统中，系统管理员可以获得所有口令，攻击者也可利用系统的漏洞来获得他人的口令。

② 攻击者可能在传输线路上截获用户口令。因为用户的口令在用户终端到系统的线路上以明文形式传输，所以攻击者可在传输线路上截获用户口令。

③ 用户和系统的地位不平等。这里只有系统强制性地验证用户的身份，而用户无法验证系统的身份。下面给出几种改进的口令验证机制。

**1）利用单向函数加密口令**

在这种验证机制中，用户的口令在系统中始终以使用单向函数加密后的密文形式存储，并且从该密文恢复出口令的明文在计算上是不可行的。也就是说，口令一旦加密，将永远不可能以明文形式在任何地方出现。用户访问系统时提供其口令，系统对该口令用单向函数加密，并与储存的密文相比较。若相等，则确认用户身份有效，否则确认用户身份无效。

**2）一次性口令**

为了安全，口令应当能够更换，而且口令的使用周期越短对安全越有利，最好是一个口令只使用一次，即一次性口令。

实现一次性口令的方法很多。

利用DES等强密码算法可以实现一次性口令：系统产生一个随机数r，并对其加密得到，并将提供给用户，用户计算，并将计算值回送给系统。同时系统计算。系统将用户返回的值与系统自己计算的值进行比较。若两者相等，则系统认为用户的身份为真。这种方法中，系统和用户必须持有相同的密钥。动态口令认证手段本质上也采用了一次性口令。

**（2）基于对称密码的认证**

典型的基于对称密码的身份认证协议是1978年提出的Needham Schroeder认证协议。

需要建立一个称为鉴别服务器的可信权威机构（密钥分发中心KDC），拥有每个用户的秘密密钥。若用户Alice欲与用户Bob通信，则用户Alice向鉴别服务器申请会话密钥。在会话密钥的分配过程中，双方身份得以鉴别。

具体认证过程需要5个步骤，如图2.25所示：其中KDC是密钥分发中心，用、表示认证过程中用到的两个一次性随机数，用和分别表示Alice和KDC、Bob和KDC之间共享的保密密钥，用表示由KDC分发的A与B的会话密钥，用表示使用密钥X加密。

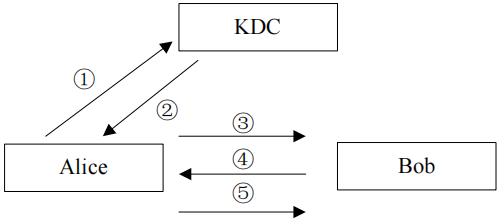


图2.25 NeedhamSchroeder认证过程

整个认证过程详细描述如下：

① Alice告诉KDC，Alice想与Bob通信，明文消息中包含一个大的随机数ra。即：

② KDC发送一个使用Alice和KDC之间共享的密钥加密的消息，消息包括由KDC分发的Alice与B的会话密钥Ks，Alice的随机数ra，Bob的名字，一个只有Bob能看懂的许可证。Alice的随机数保证了该消息是新的而不是攻击者重放的，Bob的名字保证了第一条明文消息中的Bob未被更改，许可证使用Bob和KDC之间共享的密钥加密。即：

③ Alice将许可证发给Bob。即：

④ Bob解密许可证获得会话密钥，然后产生随机数，Bob向Alice发送消息。即：

⑤ Alice向Bob发送消息EKs (rb 1)以证明是真正的Alice与Bob通信。即：

以上完成了双向认证，并同时实现了秘密通信。这个认证过程容易遭受重放攻击。假定攻击方已经掌握Alice和Bob之间通信的一个旧的会话密钥（如经过蛮力攻击等），则入侵者可以在第3步冒充Alice利用老的会话密钥欺骗Bob。除非Bob记住所有以前使用的与Alice通信的会话密钥，否则Bob无法判断这是一个重放攻击。

Needham和Schroeder于1987年发表了一个协议修正了这个漏洞。DenningSacco协议使用时间戳修正这个漏洞。Gavin Lowe 1997年给出的基于DenningSacco协议的改进版本，通过在第2步和第3步中使用时间戳来达到了抵抗重放攻击的目的。

**（3）基于公钥密码的认证**

这里分为两种情况。

情况一：假定双方已经知道对方的公开密钥。

ISO/IEC 97983单向认证的基本步骤如下：

① 首先Alice发送给Bob一个随机数，即：Alice → Bob ：

② 然后，Bob产生一个随机数，并将自己的证书、以及使用私钥对随机数签名的信息发送给Alice，用表示用Bob的私钥产生数字签名，即：  
如果需要双向认证，需要第三步：

③ Alice将自己的证书Certa以及使用私钥签名的信息发送给Bob，用Signa表示用Alice的私钥产生数字签名，即：

情况二：假定双方都不知道对方的公开密钥。这时需要一个可信的第三方T保存公开密钥库。DenningSacco认证协议如下：

① 首先，Alice向可信第三方发送他将要通信的对象，即：

② 然后，第三方T将用其私钥签名的Bob的公钥K\_b、用其私钥签名的Alice的公钥K\_a发送给Alice。即：  
可以用第三方的公钥来校验有关Alice的公钥的签名，如果正确，则说明得到的是Bob的公钥。

③ Alice生成一个随机的会话密钥K，用自己的私钥对K和一个时间标记进行签名后，用Bob的公钥进行对该签名加密，并将收到的第三方的对两者公钥的签名，也一起发送给Bob，即：

这样，Bob用私钥解密Alice发来的消息，然后用A的公钥验证签名，以确信时间标记仍有效。然后基于会话密钥K，安全地通信。

但该协议是有缺陷的。在和Alice一起完成协议后，Bob能够伪装是Alice。其步骤是：

①

②

③ 此时，Bob将从Alice那里接收到的会话密钥K和时间标记的签名用Clark的公钥加密，并将Alice与Clark的经过第三方T签名的公钥发送给C，即：  
这样，Bob就成功地欺骗了Clark。在时间标记截止前，Bob可以欺骗任何人。这个问题容易解决。解决方法为在第③步的加密消息内加上名字，即：  
因为这一步清楚地表明是Alice和Bob在通信，所以现在Bob就不可能对Clark重放旧消息。

## 2.3 访问控制技术

在计算机系统中，认证、访问控制（Access Control）和审计共同建立了保护系统安全的基础，如图2.26所示。认证是用户进入系统的第一道防线，访问控制是在鉴别用户的合法身份后，控制用户对数据信息的访问，它是通过引用监控器实施这种访问控制的。

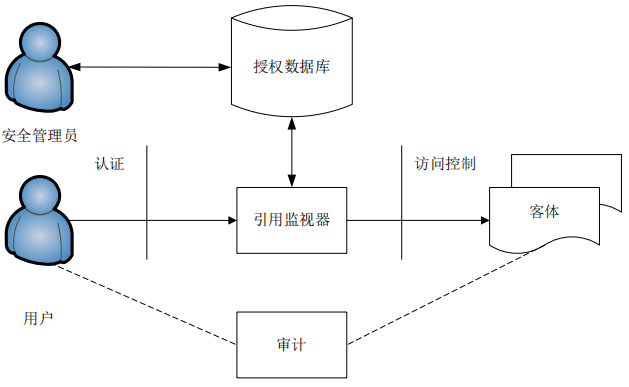


图2.26 访问控制与其它安全服务关系模型

区别认证和访问控制是非常重要的。在通过引用监控器进行访问控制时，总是假定用户的身份已经被确认，而且访问控制在很大程度上依赖用户身份的正确鉴别和引用监控器的正确控制。同时要认识到，访问控制不能作为一个完整的策略来解决系统安全，它必须要结合审计而实行。审计主要关注系统所有用户的请求和活动的事后分析。

访问控制是在身份认证的基础上，依据授权对提出的资源访问请求加以控制。访问控制是一种安全手段，能够控制用户和系统与其它的系统和资源进行通信和交互，也能够保护系统和资源免受未经授权的访问，并为成功认证的用户授权不同的访问等级。

在访问控制的环境中，正确地理解主体和客体的概念是非常重要的。访问是在主体和客体之间的一种信息的传输。

主体是一个主动的实体，它提供对客体中的对象或数据的访问要求。主体可以是能够访问信息的用户、程序、进程。当程序访问文件时，程序是主体而文件是客体。

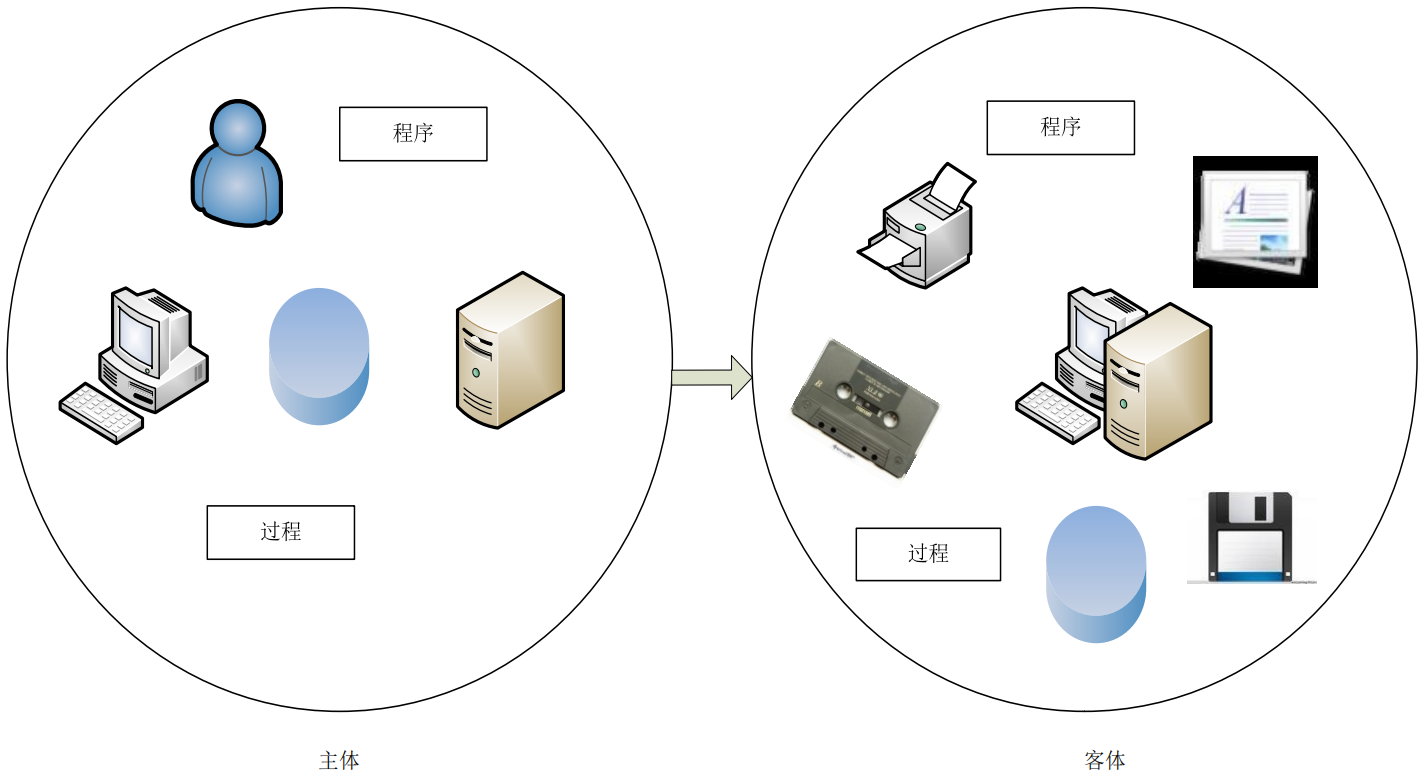
客体是含有被访问信息的被动实体。客体可以是一台计算机、一个数据库、一个文件、一个计算机程序、目录，甚至可以是一个数据库中的一个表中的一个数据区。当你在数据库中查询信息的时候，你就是一个主动实体，而数据库就是一个被动实体。图2.27给出了主体和客体的关系。

图2.27主体是访问客体的主动实体；客体是被访问的被动实体

访问控制包含的范围很广，它涵盖了几种不同的机制。因为它是防范计算机系统和资源被未授权访问的第一道防线，所以其地位非常重要。提示用户输入用户名和密码才能使用该计算机的过程，就是一种访问控制。一旦用户登录之后访问文件，文件应该有一个包含能够访问它的用户和组的列表，如果用户不在这个列表上面，那么用户的访问就要求被拒绝。用户的访问权限主要基于其身份和访问等级。访问控制给予组织控制、限制、监控以及保护资源的可用性、完整性和机密性等能力。

### 2.3.1 访问控制模型

#### 1．分类

访问控制模型是一种从访问控制的角度出发，描述安全系统并建立安全模型的方法。它主要描述了主体访问客体的一种框架，通过访问控制技术和安全机制来实现模型的规则和目标。

可信计算机系统评估准则（TCSEC）提出了访问控制在计算机安全系统中的重要作用。TCSEC要达到的一个主要目标就是：阻止非授权用户对敏感信息的访问。访问控制在准则中被分为两类：自主访问控制（DAC，Discretionary Access Control）和强制访问控制（MAC，Mandatory Access Control）。该标准将计算机系统的安全程度从高到低划分为A1、B3、B2、B1、C2、C1、D七个等级，每一等级对访问控制都提出了不同的要求。例如，Ｃ级要求至少具有自主型的访问控制；Ｂ级以上要求具有强制型的访问控制手段。我国也于1999年颁布了计算机信息系统安全保护等级划分准则这一国家标准。

最近几年，基于角色的访问控制（RBAC，Rolebased AccessControl）正得到广泛的研究与应用，目前已提出的主要RBAC模型有美国国家标准与技术局NIST的RBAC模型。具体分类如图2.28所示：

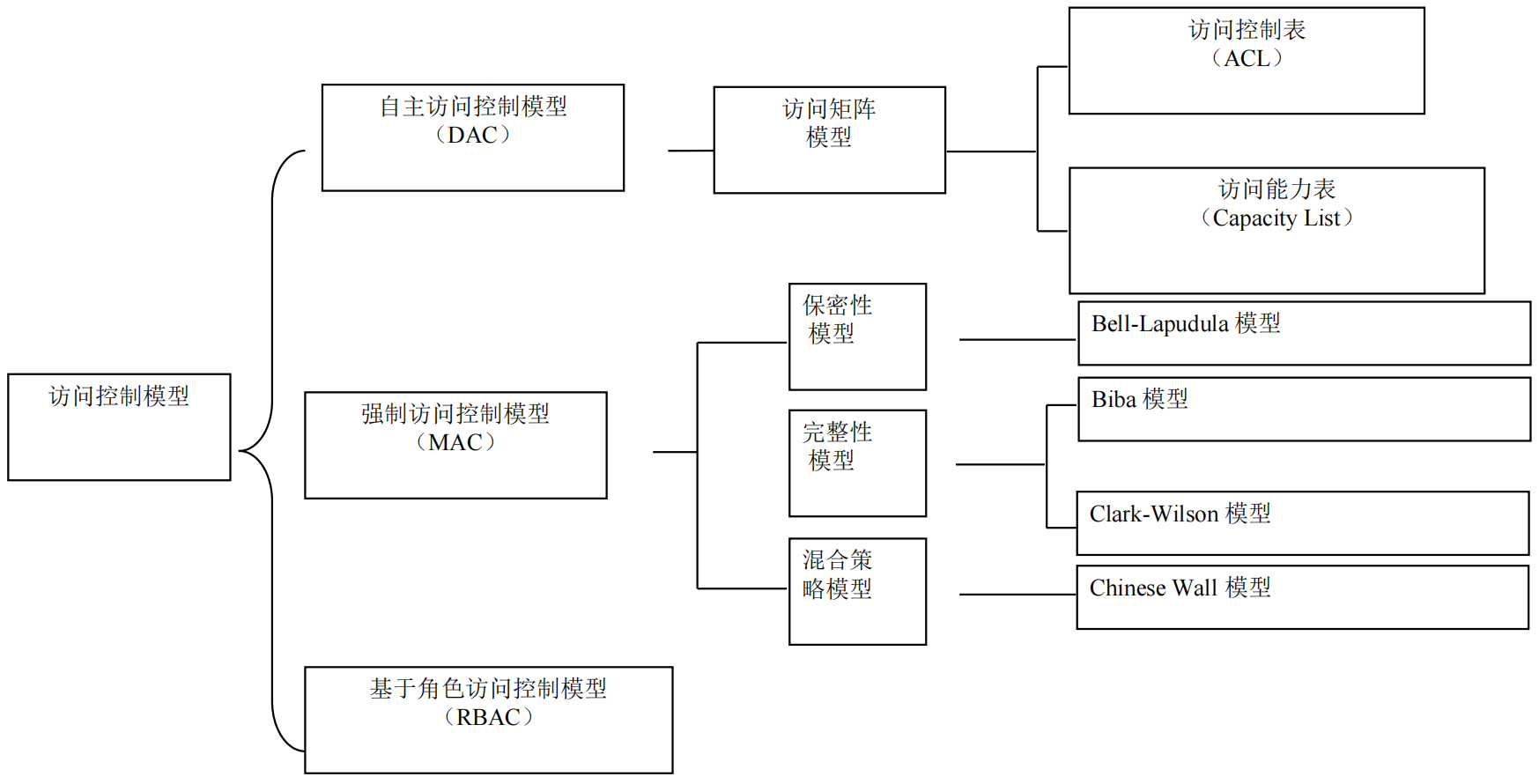


图2.28 访问控制模型分类

#### 2．自主访问控制

自主访问控制DAC模型是根据自主访问控制策略建立的一种模型，允许合法用户以用户或用户组的身份访问策略规定的客体，同时阻止非授权用户访问客体，某些用户还可以自主地把自己所拥有的客体的访问权限授予其它用户。

自主访问控制又称为任意访问控制。Linux\Unix、Windows操作系统都提供自主访问控制的功能。在实现上，首先要对用户的身份进行鉴别，然后就可以按照访问控制列表所赋予用户的权限允许和限制用户使用客体的资源。主体控制权限的修改通常由特权用户或是特权用户（管理员）组实现。（1）访问控制矩阵任何访问控制策略最终可以被模型化为访问矩阵形式，行对应于用户，列对应于目标，矩阵中每一元素表示相应的用户对目标的访问许可。如表2.19所示

|  |  |  |  |
| --- | --- | --- | --- |
|  | 目标X | 目标Y | 目标Z |
| 用户A | 读取、修改、管理 |  | 读取、修改、管理 |
| 用户B |  | 读取、修改、管理 |  |
| 用户C1 | 读取 | 读取、修改 |  |
| 用户C2 | 读取 | 读取、修改 |  |

为了实现完备的自主访问控制系统，由访问控制矩阵提供的信息必须以某种形式存放在系统中。访问矩阵中的每行表示一个主体，每一列则表示一个受保护的客体，而矩阵中的元素，则表示主体可以对客体的访问模式。

**（2）访问能力表和访问控制表**

目前，在系统中访问控制矩阵本身，都不是完整地存储起来，因为矩阵中的许多元素常常为空。空元素将会造成存储空间的浪费，而且查找某个元素会耗费很多时间。实际上常常是基于矩阵的行或列来表达访问控制信息。

基于矩阵的行的访问控制信息表示是访问能力表（CL, CapacityList），即每个主体都附加一个该主体可访问的客体的明细表。

基于矩阵的列的访问控制信息表示的是访问控制表（ACL, AccessControl List），即每个客体附加一个它可以访问的主体的明细表。

自主访问控制模型的实现机制就是通过访问控制矩阵实施，而具体的实现办法则是通过访问能力表或访问控制表来限定哪些主体针对哪些客体可以执行什么操作。

访问能力表和访问控制表的对比如表2.20所示。

|  |  |  |
| --- | --- | --- |
| 对比项 | ACL（访问控制列表） | CL（能力表） |
| 保存位置​ | 客体（如文件、资源） | 主体（如用户、进程） |
| 浏览访问权限​ | 容易（直接查看客体的ACL即可） | 困难（需要汇总所有主体的CL） |
| 访问权限传递​ | 困难（需要修改客体的ACL） | 容易（主体可直接将自己的能力传递） |
| 访问权限回收​ | 容易（在客体的ACL中统一修改即可） | 困难（需要定位并修改所有相关主体的CL） |
| 使用（适用系统） | 集中式系统 | 分布式系统 |

表2.20 访问能力表和访问控制表对比

多数集中式操作系统中使用访问控制表或者类似方式实施访问控制。由于分布式系统中很难确定给定客体的潜在主体集，在现代OS中CL也得到广泛应用。

**（3）优缺点**

优点：根据主体的身份和访问权限进行决策；具有某种访问能力的主体能够自主地将访问权的某个子集授予其它主体；灵活性高，被大量采用。

缺点：信息在传递过程中其访问权限关系会被改变。

（4）应用实例

在商业环境中，经常会遇到自主访问控制机制，由于它易于扩展和理解。大多数系统仅基于自主访问控制机制来实现访问控制，如主流操作系统、防火墙等。

举一个更具体的例子：假设某所大学使用计算机系统进行学生信息的管理。教务处在系统中建立了一张表，存入了每个学生的有关信息，如姓名、年龄、年级、专业、系别、成绩、受过哪些奖励和处分等。教务处不允许每个学生都能看到所有这些信息，他可能按这样一个原则来控制：

① 每个学生可以看到自己的有关信息，但不允许看别人的；

② 每个班的老师可以随时查看自己班的学生的有关信息，但不能查看其它班学生的信息；

③ 并且教务处可限制教务处以外的所有用户不得修改这些信息，也不能插入和删除表中的信息，这些信息的拥有者是教务处。

教务处可按照上述原则对系统中的用户（该大学的所有老师和学生）进行授权。于是其它用户只能根据教务处的授权来对这张表进行访问。根据教务处的授权规则，计算机中相应存放有一张表（授权表），将教务处的授权情况记录下来，以后当任何用户对教务处的数据要进行访问时，系统首先查这张表，检查教务处是否对他进行了授权，如果有授权，计算机就执行其操作；若没有，则拒绝执行。3．强制访问控制

强制访问控制（MAC，Mandatory Access Control）是“强加”给访问主体的，即系统强制主体服从访问控制政策。强制访问控制的主要特征是对所有主体及其所控制的客体（例如：进程、文件、段、设备）实施强制访问控制。

**（1）安全标签**

强制访问控制对访问主体和受控对象标识两个安全标签：一个是具有偏序关系的安全等级标签；另一个是非等级分类标签。它们是实施强制访问控制的依据。系统通过比较主体和客体的安全标签来决定一个主体是否能够访问某个客体。用户的程序不能改变他自己及任何其它客体的安全标签，只有管理员才能够确定用户和组的访问权限。

安全标签是限制和附属在主体或客体上的一组安全属性信息。安全标签的含义比能力更为广泛和严格，因为它实际上还建立了一个严格的安全等级集合。

访问控制标签列表（ACSLL，Access Control Security Labels Lists）是限定一个用户对一个客体目标访问的安全属性集合。访问控制标签列表的实现示例如图2.29所示，左侧为用户对应的安全级别，右侧为文件系统对应的安全级别。假设请求访问的用户A的安全级别为S，那么A请求访问文件2时，由于S<TS，访问会被拒绝；当用户A请求访问文件N时候，因为S>C，所以允许访问。

安全标签能对敏感信息加以区分，这样就可以对用户和客体资源强制执行安全策略，因此，强制访问控制经常会用到这种实现机制。

|  |  |  |  |
| --- | --- | --- | --- |
| 用户 | 用户安全级别 | 文件 | 文件安全级别 |
| A | S | 1 | S |
| B | C | 2 | TS |
| ... | ... | ... | ... |
| X | TS | N | C |

图2.29 访问控制标签列表的实现示例

**（2）强制访问策略**

强制访问策略将每个主体与客体赋予一个访问级别，如，最高秘密级（Top Secret），秘密级（Secret），机密级（Confidential）及无级别级（Unclassified），定义其级别为T>S>C>U。用一个例子来说明强制访问控制规则的应用，如WEB服务以“秘密级”的安全级别运行。假如WEB服务器被攻击，攻击者在目标系统中以“秘密级”的安全级别进行操作，他将不能访问系统中安全级为“最高秘密级”的数据。

强制访问控制系统根据主体和客体的敏感标记来决定访问模式，访问模式包括：

◼ 向下读（rd，read down）：主体安全级别高于客体信息资源的安全级别时允许的读操作；

◼ 向上读（ru，read up）：主体安全级别低于客体信息资源的安全级别时允许的读操作；

◼ 向下写（wd，write down）：主体安全级别高于客体信息资源的安全级别时允许执行的写操 作；向上写（wu，write up）：主体安全级别低于客体信息资源的安全级别时允许执行的写操 作。

由于MAC通过分级的安全标签实现了信息的单向流通，因此它一直被军方采用，其中最著名的是BellLaPadula模型和Biba模型：Bell LaPadula模型具有只允许向下读、向上写的特点，可以有效地防止机密信息向下级泄露；Biba模型则具有不允许向下读、向上写的特点，可以有效地保护数据的完整性。

**（3）BellLaPadula模型**

BellLapadula安全模型（也称为BLP模型）利用“不上读/不下写”的原则来保证数据的保密性。以信息的敏感度作为安全等级的划分标准，主体和客体用户被划分为以下安全等级：公开(Unclassified)、秘密(Confidential)、机密(Secret)、绝密(Top Secret)，安全等级依次增高。BLP模型不允许低安全等级的用户读高敏感度的信息，也不允许高敏感度的信息写入低敏感度区域，禁止信息从高级别流向低级别。强制访问控制通过这种梯度安全标签实现信息的单向流通，这种方法一般应用于军事用途。



图2.30 BellLapadula安全模型

例如，见图2.30。假如一个用户，他的安全级别为“秘密”，想要访问安全级别为“公开”的文档，他将能够成功读取该文件，但不能写入；而安全级别为“秘密”的用户访问安全级别为“高密”的文档，则会读取失败，但能够写入。这样，文档的保密性就得到了保障。

**（4）Biba模型**

由于BLP模型存在不保护信息的完整性和可用性、不涉及访问控制等缺点，1977年Biba模型作为BLP模型的补充而提出。它针对的是信息的完整性保护，主要用于非军用领域。它和BLP模型相类似，也使用了和BLP模型相似的安全等级划分方式，只不过Biba模型的划分标准是信息对象的完整性，主体和客体用户被划分为以下完整性级别：重要（Important）、很重要（VeryImportant）、极重要（Crucial），完整性级别依次增高。

Biba模型利用“不下读/不上写”的原则来保证数据的完整性。在实际应用中，完整性保护主要是为了避免应用程序修改某些重要的系统程序或系统数据库。

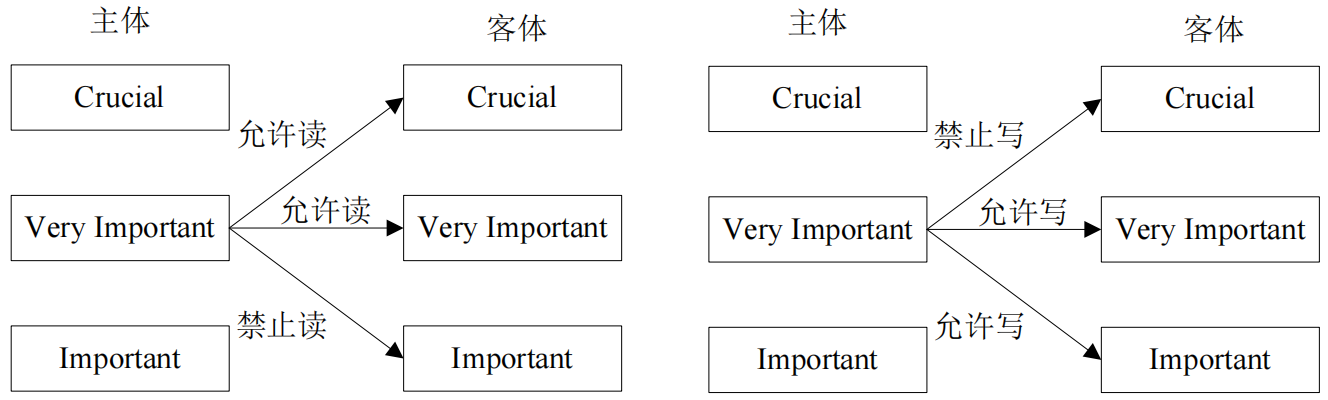


图2.31 Biba安全模型

例如，如图2.31所示，一个安全级别为“很重要”的用户要访问级别为“重要”的文档，他将被允许写入该文档，而不能读取。如果他试图访问“极重要”的文档，那么，读取操作将被允许，而写入操作将被拒绝。这样，就使资源的完整性得到了保障。

因此，只有用户的安全级别高于资源的安全级别时可对资源进行写操作，相反地，只有用户的安全级别低于资源的安全级别时可读取该资源。简而言之，信息在系统中只能自上而下进行流动。

**（5）Chinese Wall模型**

Chinese Wall模型是应用在多边安全系统中的安全模型（也就是多个组织间的访问控制系统），应用在可能存在利益冲突的组织中。最初是为投资银行设计的，但也可应用在其它相似的场合。

Chinese Wall安全策略的基础是客户访问的信息不会与目前他们可支配的信息产生冲突。在投资银行中，一个银行会同时拥有多个互为竞争者的客户，一个银行家可能为一个客户工作，但他可以访问所有客户的信息。因此，应当制止该银行家访问其它客户的数据。

Chinese Wall安全模型的两个主要属性：

① 用户必须选择一个他可以访问的区域；

② 用户必须自动拒绝来自其它与用户所选区域的利益冲突区域的访问。

这种模型同时包括了DAC和MAC的属性：银行家可以选择为谁工作（DAC），但是一旦选定，他就只能为该客户工作（MAC）。Chinese Wall安全模型在网络安全体系中应用的一个典型的例子是位于防火墙内部的一台服务器，连接着内部与外部网络。假如策略禁止经由此服务器转发数据，该服务器将暴露于外部网络（也就是说，该服务器仅能与外部网络通讯，而不能与内部网络通讯）。

#### 4．基于角色的访问控制模型

**（1）基本定义**

基于角色的访问控制（RBAC，Rolebased Access）模型的要素包括用户、角色、许可等基本定义。

用户是一个可以独立访问计算机系统中的数据或者用数据表示的其它资源的主体。

角色是指一个组织或任务中的工作或者位置，它代表了一种权利、资格和责任。

许可（特权）是允许对一个或多个客体执行的操作。

用户、角色、许可的关系如图2.32所示：一个用户可经授权而拥有多个角色，一个角色可由多个用户构成；每个角色可拥有多种许可，每个许可也可授权给多个不同的角色；每个操作可施加于多个客体（受控对象），每个客体也可以接受多个操作。

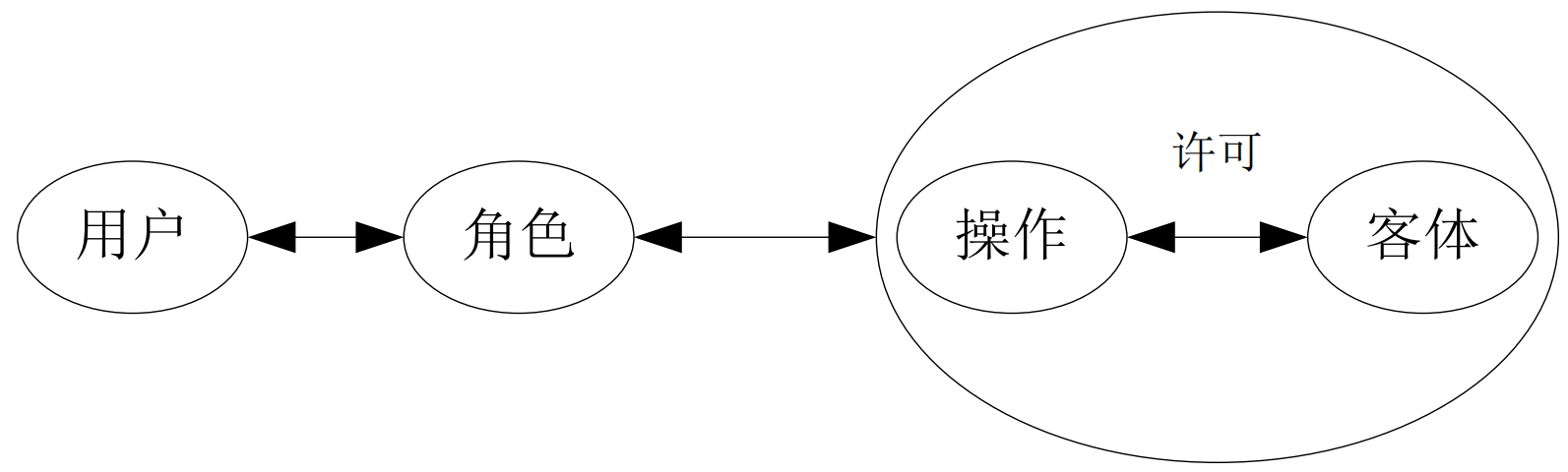


图2.32 用户、角色、许可的关系

**（2）基本思想**

RBAC模型的基本思想是将访问许可权分配给一定的角色，用户通过饰演不同的角色获得角色所拥有的访问许可权。这是因为在很多实际应用中，用户并不是可以访问的客体信息资源的所有者（这些信息属于企业或公司）。这样的话，访问控制应该基于员工的职务而不是基于员工在哪个组或谁是信息的所有者，即访问控制是由各个用户在部门中所担任的角色来确定的，例如，一个学校可以有教工、老师、学生和其它管理人员等角色。

角色可以看作是一组操作的集合，不同的角色具有不同的操作集，这些操作集由系统管理员分配给角色。

根据上面描述的自主访问控制的应用实例，我们假设Tch1、Tch2、Tch3、…、Tchi代表教师，Stud1、Stud 2、Stud3、…、Studj代表学生，Mng1、Mng2、Mng3、…、Mngk代表教务处管理人员。定义教师角色并赋予权限TchMN={查询成绩、上传所教课程的成绩}；定义学生角色并赋予权限StudMN={查询成绩、反映意见}；定义教务管理人员角色并赋予权限MngMN={查询、修改成绩、打印成绩清单}。那么，依据角色的不同，每个主体只能执行角色定义的访问功能。

用户在一定的部门中具有一定的角色，其所执行的操作与其所扮演的角色的职能相匹配，这正是基于角色的访问控制（RBAC）的根本特征，即：依据RBAC策略，系统定义了各种角色，每种角色可以完成一定的职能，不同的用户根据其职能和责任被赋予相应的角色，一旦某个用户成为某角色的成员，则此用户可以完成该角色所具有的职能。

系统管理员负责授予用户各种角色的成员资格或撤消某用户具有的某个角色。例如学校新进一名教师Tchx，那么系统管理员只需将Tchx添加到教师这一角色的成员中即可，而无需对访问控制列表做改动。

同一个用户可以是多个角色的成员，即同一个用户可以扮演多种角色，比如一个用户可以是老师，同时也可以作为进修的学生。同样，一个角色可以拥有多个用户成员，这与现实是一致的，一个人可以在同一部门中担任多种职务，而且担任相同职务的可能不止一人。因此RBAC提供了一种描述用户和权限之间的多对多关系，角色可以划分成不同的等级，通过角色等级关系来反映一个组织的职权和责任关系，这种关系具有反身性、传递性和非对称性特点，通过继承行为形成了一个偏序关系，比如MngMN>TchMN>Stud MN。

**（3）特点**

相比较而言，RBAC是实施面向企业的安全策略的一种有效的访问控制方式，其具有灵活性、方便性和安全性的特点，目前在大型数据库系统的权限管理中得到普遍应用。

角色由系统管理员定义，角色成员的增减也只能由系统管理员来执行，即只有系统管理员有权定义和分配角色。用户与客体无直接联系，他只有通过角色才享有该角色所对应的权限，从而访问相应的客体。因此用户不能自主地将访问权限授给别的用户，这是RBAC与DAC的根本区别所在。

RBAC与MAC的区别在于：MAC是基于多级安全需求的，而RBAC则不是。

### 2.3.2 访问控制技术

访问控制的管理方法可以分为两类：一类是集中式访问控制（Centralized Access Control），一类是分布式访问控制，即非集中式访问控制（Decentralized/Distributed Access Control）。

#### 1．集中访问控制

自网络诞生以来，认证、授权和审计（AAA，Authentication Authorization-Accounting）管理就成为其运营的基础。网络中各类资源的使用，需要由认证、授权和审计进行管理。而AAA的发展与变迁自始至终都吸引着运营商的目光。对于一个商业系统来说，鉴别是至关重要的，只有确认了用户的身份，才能知道所提供的服务应该向谁收费，同时也能防止非法用户（黑客）对网络进行破坏。在确认用户身份后，根据用户开户时所申请的服务类别，系统可以授予客户相应的权限。最后，在用户使用系统资源时，需要有相应的设备来统计用户所对资源的占用情况，据此向客户收取相应的费用。

远程用户访问网络资源的AAA过程见图2.33所示，如下：

① 远程用户给网络接入服务器（NAS，Network Access Server）发送自己的用户名和密码。

② NAS接收用户提供的用户名和密码信息，并将信息转交给验证服务器。

③ 验证服务器通过用户的身份验证后，将用户可用的网络连接参数（带宽、可用时长等）、用户授权和协议信息返回给NAS。

④ NAS确认并向用户提供连接服务，并将此连接写入验证服务器的日志中。

集中式的AAA管理协议包括拨号用户远程认证服务RADIUS、终端访问控制器访问控制系统TACACS、Diameter等。

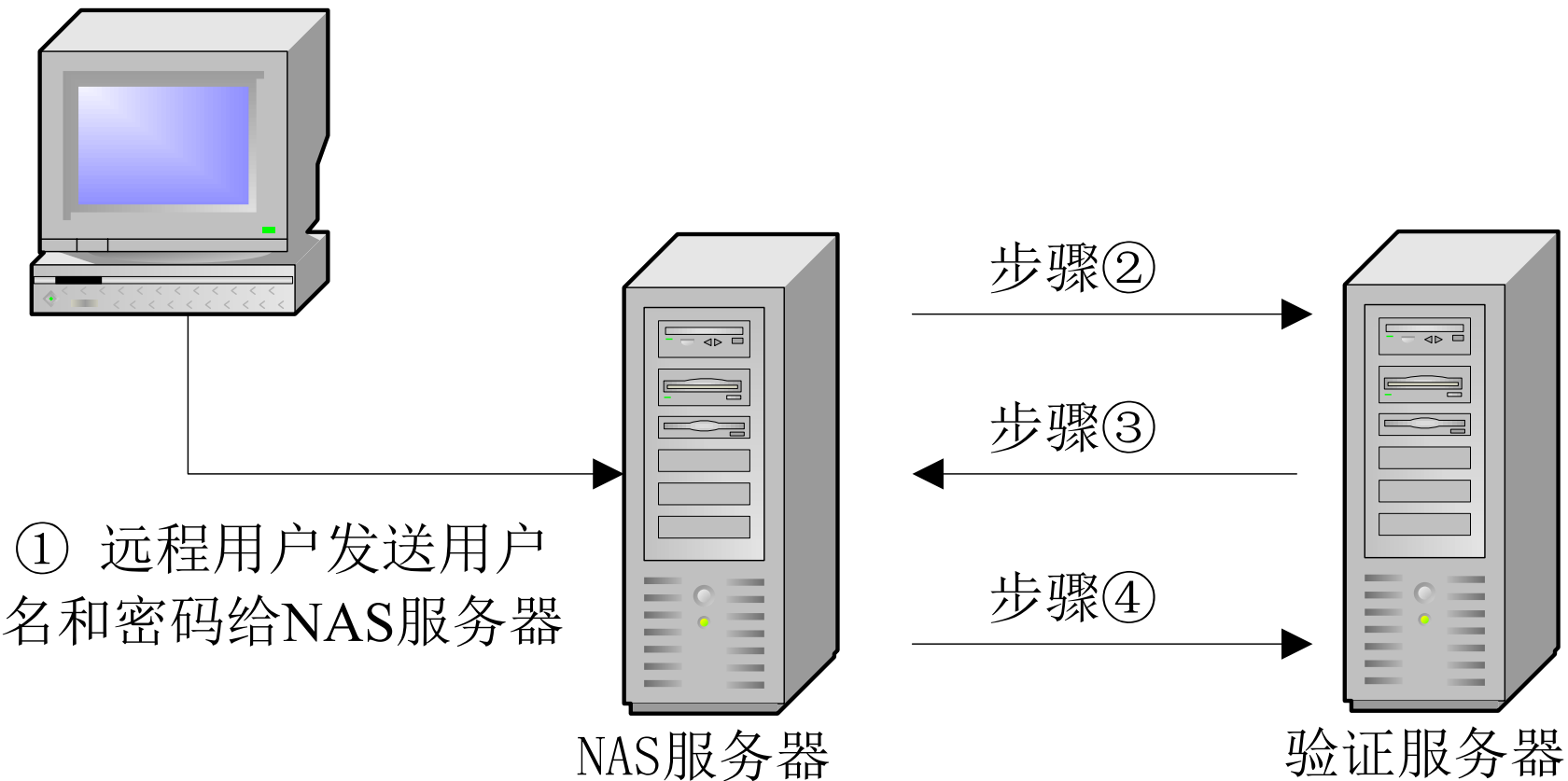


图2.33 AAA服务的示意图NAS服务器

**（1）RADIUS协议**

拨号用户远程认证服务（RADIUS，Remote Authentication DialIn User System）是一个网络协议，提供集中式AAA管理。

RADIUS协议最初由Livingston公司提出，为拨号用户进行认证和审计，经多次改进，形成了一项通用的认证审计协议。RADIUS协议具有广泛的适应性，支持绝大多数网络，因此互联网服务供应商和企业远程接入互联网或内部网络都将RADIUS作为主要的AAA管理方法。支持的设备除了主机以外还包括如调制解调器、DSL线路、无线接入点、虚拟专用网VPN、交换机或路由器的网络端口等。

RADIUS 是一个客户端/服务器协议，它运行在应用层，使用UDP协议，RADIUS的身份认证和授权使用1812端口，而审计使用1813端口。

RADIUS服务器通常是运行在专门用于进行RADIUS验证的服务器（可以是Unix主机或Windows NT主机）之上的一个后台进程。RADIUS客户端最初是一个网络接入服务器NAS，现在任何运行RADIUS客户端软件的计算机都可以成为RADIUS的客户端，可以是一台web服务器，也可以是远程连接服务器，或者是一个路由器或交换机，也能够是一个无线接入点。特别需要注意的是，RADIUS客户端并不一定安装在最终用户的主机中，而是主要安装在直接为用户提供服务的各类服务器（如VPN服务器）中。因此对于RADIUS的身份验证和授权过程而言，相当于RADIUS服务器取代了提供服务的主机本身的身份验证和授权功能。

RADIUS有三个最主要的功能：

① 对需要访问网络的用户或设备进行身份验证。

② 对通过身份验证的用户或设备授予访问资源的权限。

③ 对已经授权的访问进行审计。

1**）身份验证和授权**

RADIUS协议允许RADIUS服务器支持多种用户的身份验证方法，这取决于RADIUS服务器和客户端的约定。RADIUS身份验证的起点是用户计算机发送访问请求到网络接入服务器NAS。因此，NAS根据用户的请求，使用RADIUS客户端发送“访问—请求”（AccessRequest）消息到RADIUS服务器，该消息中一般包含了用户的用户名与密码等身份验证信息。RADIUS服务器根据这个“访问—请求”消息就可以从用户身份数据库中查找相应的信息，并将身份验证结果以消息的形式发送给RADIUS客户端。RADIUS服务器进行身份验证过程中，除了使用一些常规的身份验证方法以外，还可选择其它相关附加信息——如用户的网络IP地址或电话号码等，协助进行验证。早期RADIUS服务器将用户身份信息存放在本地文件中，而现代的RADIUS服务器除了本地文件以外，还可以用关系型数据库、Kerberos、LDAP或Active Directory来进行用户的身份验证。

2）RADIUS的特点

RADIUS协议的优点是简单明确，可扩充，因此得到了广泛应用，包括普通电话上网、ADSL上网、小区宽带上网、IP电话、基于拨号用 户 的 虚 拟 专 用 拨 号 网 业 务 （ VPDN ， Virtual Private DialupNetworks）、移动电话预付费等业务。最近IEEE提出了802.1x标准，这是一种基于端口的标准，用于对无线网络的接入认证，在认证时也采用RADIUS协议。但是由于协议本身的缺陷，比如基于UDP的传输、简单的丢包机制、没有关于重传的规定和集中式审计服务，都使得它需要进一步改进。

**（2）TACACS协议**

终端访问控制器访问控制系统（TACACS，Terminal Access ControllerAccess Control System），对于Unix网络来说是一个比较老的基于UDP的认证协议，它允许远程访问服务器传送用户登录密码给认证服务器，认证服务器决定该用户是否可以登录系统。

TACACS 经 历 了 三 代 ： TACACS 、 扩 展 TACACS （ XTACACS ） 和TACACS+。TACACS将认证和授权过程结合起来，而XTACACS将认证、授权和审计功能分开，TACACS+是一种采用扩展的双重用户认证的XTACACS。TACACS使用固定的密码进行认证，而TACACS+允许用户使用动态密码，这样可以提供更强大的保护。

TACACS+和RADIUS在现有网络里已经取代了早期的协议。TACACS+使用传输控制协议（TCP），而RADIUS使用用户数据报协议（UDP）。一些管理员推荐使用 TACACS+ 协议，因为 TCP 更可靠些。RADIUS 从用户角度结合了认证和授权，而 TACACS+ 分离了这两个操作。

|  |  |  |
| --- | --- | --- |
| 对比项 | RADIUS | TACACS+ |
| 包传输​ | UDP | TCP |
| 包加密​ | 仅加密在客户端和服务器之间传送的密码 | 加密客户端与服务器之间的所有流量 |
| AAA支持​ | 组合认证与授权服务 | 使用AAA体系结构，分隔认证、授权和审计 |
| 多协议支持​ | 在PPP连接上工作 | 支持其它协议，如AppleTalk、NetBIOS和IPX |
| 响应​ | 在认证时使用适用于所有AAA活动的单质响应 | 对每一个AAA进程使用多质响应：每个AAA活动必须进行认证 |

表2.21 TACACS+和RADIUS的区别

如果进行简单的用户名/密码认证，且用户只需要一个接受或拒绝即可获得访 问 （ 如 在 互 联 网 服 务 提 供 商 ISP 中 ） ， RADIUS 就 是 合 适 的 协 议 。TACACS+更适于需要更加复杂的认证步骤，并对更加复杂的授权活动实施更严格的控制的环境。表2.21 TACACS+和RADIUS的区别RADIUS TACACS+包传输 UDP TCP包加密 仅加密在RADIUS客户端和服务器之间传送的密码 加密客户端服务器之间的所有流量AAA支持 组合认证与授权服务 使用AAA体系结构，分隔认证、授权和审计多协议支持 在PPP连接上工作 支持其它协议，如AppleTalk、NetBIOS和IPX响应 在认证时使用适用于所有AAA活动的单质响应 对每一个AAA进程使用多质响应：每个AAA活动必须进行认证如果进行简单的用户名/密码认证，且用户只需要一个接受或拒绝即可获得访 问 （ 如 在 互 联 网 服 务 提 供 商 ISP 中 ） ， RADIUS 就 是 合 适 的 协 议 。TACACS+更适于需要更加复杂的认证步骤，并对更加复杂的授权活动实施更严格的控制的环境。（3）Diameter协议随着新的接入技术的引入（如无线接入、DSL、移动IP和以太网）和接入网络的快速扩容，越来越复杂的路由器和接入服务器大量投入使用，对AAA协议提出了新的要求，使得传统的RADIUS结构的缺点日益明显。目前，3G网络正逐步向全IP网络演进，不仅在核心网络使用支持IP的网络实体，在接入网络也使用基于IP的技术，而且移动终端也成为可激活的IP客户端。在这样的网络中，移动IP将被广泛使用。支持移动IP的终端可以在注册的家乡网络中移动，或漫游到其它运营商的网络。当终端要接入到网络，并使用运营商提供的各项业务时，就需要严格的AAA过程。AAA服务器要对移动终端进行认证，授权允许用户使用的业务，并收集用户使用资源的情况，以产生审计信息，这就需要采用新一代的AAA协议——Diameter。Diameter协议是RADIUS协议的升级版本，Internet工程任务组（IETF，Internet Engineering Task Force）的AAA工作组同意将Diameter协议作为下一代的AAA协议标准。Diameter协议支持移动IP、NAS请求和移动代理的认证、授权和审计工作，协议的实现和RADIUS类似，但是采用TCP协议，支持分布式审计，克服了RADIUS的许多缺点，是最适合未来移动通信系统的AAA协议。1）Diameter和RADIUS的区别AAA协议Diameter和RADIUS的不同，包括如下几个方面：① 模式：RADIUS固有的客户端/服务器模式限制了它的进一步发展；Diameter采用了端到端模式，任何一端都可以发送消息以发起审计等功能或中断连接。② 传输机制：RADIUS运行在UDP协议上，并且没有定义重传机制；而Diameter运行在可靠的传输协议TCP、SCTP之上。③ 失败恢复机制：RADIUS协议不支持失败恢复机制；而Diameter支持应用层确认，并且定义了失败恢复算法和相关的状态机，能够立即检测出传输错误。④ 服务器初始化消息：由于在RADIUS中服务器不能主动发起消息，只有客户能发出重认证请求，所以服务器不能根据需要重新认证；而Diameter指定了两种消息类型，重认证请求和重认证应答消息，使得服务器可以随时根据需要主动发起重认证。⑤ 认证和授权：RADIUS中认证与授权必须成对出现；Diameter支持认证和授权分离，重授权可以随时根据需求进行。⑥ 安全机制：RADIUS仅仅在应用层上定义了一定的安全机制，但没有涉及到数据的机密性；Diameter要求必须支持IPsec以保证数据的机密性和完整性。2．非集中访问控制分布式访问控制需要解决跨域访问的问题。域是指一个信任范围，或者是共享共同安全策略的主体和客体的集合。通常，每个域的访问控制与其它域保持独立。如果要实现跨域访问，必须建立信任关系，使得用户可以从一个域访问另一个域中的资源。这种信任关系可以是单向的，也可以是双向的。目前广泛使用的三种分布式访问控制方法为：单点登录（SSO，Single Sign On）、Kerberos协议和SESAME。（1）单点登录在日常的工作中，常常会遇到这样的情况：需要访问多个不同的计算机系统或应用程序，才能获取完成某项特定工作所需的所有条件。在涉及的不同计算机系统和应用程序较多的情况下，记住对应的用户名和密码成为一项不容易的任务，许多用户为了简化这一流程，往往会使用简单的密码，或将密码写在纸上，从而对系统的安全留下了不小的隐患。为了降低和消除这一隐患，安全厂商推出了单点登录技术。单点登录技术将不同的系统和应用程序所需的访问控制功能抽离出来，用户在使用时只需要在统一的单点登录方案下进行一次验证，便可以访问到自己所需的网络、信息和其它资源。由于应用单点登录技术之后，用户在IT环境中使用的用户名密码对和需要进行的验证次数大为减少，用户可以使用较为复杂的密码，在某种程度上提升了IT环境的安全性，也简化了用户的访问控制难度。现在可以从越来越多的场合看到单点登录技术的使用，如Hotmail、yahoo、163等知名网站上使用的通行证技术，开源社区中的OpenID等。1）单点登录的优缺点单点登录的优点如下：① 提供一个更为有效的用户登录流程，用户只需输入一次用户名和密码，就能访问到多个该用户所需要的资源，降低了用户名密码的记忆难度并减少了用户验证所需的时间。② 由于用户要记忆的密码数目减少，用户可以使用更为复杂、更难破解的密码，从而提升IT环境的安全性。③ 消除了多个系统中的用户密码进行同步时的风险。④ 用户账户超时和登录尝试能够更密切地和登录入口相结合。⑤ 简化了管理员的账户管理流程，管理员只需要进行一次操作就可以完成用户账户的添加、修改、禁用和删除等操作。但单点登录技术也有其与生俱来的缺点，就是：① 当用户的用户名和密码被入侵者窃取的时候，入侵者能够访问到该用户所授权的所有系统和资源，这种危害在管理员密码被入侵者窃取的时候尤其明显。② 在部署单点登录技术时必须严格遵守企业的安全策略，并细致地分配用户权限，否则很容易造成用户权限过大等问题。③ 使用单点登录技术后，企业要部署不支持该方案的计算机系统或应用程序会遇到相当多的问题。为了降低和消除单点登录技术密码失窃导致的风险，企业在使用时还可以使用双因素或者多因素验证方法来增强单点登录技术的安全性。对于移动用户多的应用场景，企业还可以使用一次性加密的加密算法来保证用户密码传输时的安全性。（2）Kerberos协议Kerberos可能是至今为止使用最为广泛的身份验证协议，它在上个世纪80年代由麻省理工学院设计并在雅典娜计划中使用，适用于大规模的异构网络中。Kerberos协议设计的核心是，在用户的验证过程中引入一个可信的第三方，即Kerberos验证服务器，它通常也称为密钥分发服务器，负责执行用户和服务的安全验证。Kerberos协议在网络上传输的数据都是用DES加密方法进行处理。Kerberos除了提供验证服务外，还能够提供网络信息的保密性和完整性保障。在一个封闭的小型网络，所有的节点都有一个组织所拥有并维护的情况下，使用Kerberos并不是部署验证服务的必然选项。但在一个开放的，分布式的网络环境中，尤其是有许多异构系统，用户必须向每个要访问的服务器或服务提供凭证的情况下，使用Kerberos协议能够有效的简化网络的验证过程。Kerberos服务可以采取多个服务器的分布式部署方式，以冗余的方式来保证Kerberos验证服务不成为网络的单点故障。Kerberos服务通过核对用户及其要使用的服务之间的授权状态，来确定用户是否能访问服务，核对通过后，Kerberos会为用户提供访问服务所需的“票据”，票据有使用时限并保存在用户系统的缓存中。2）Kerberos特点Kerberos服务的可靠程度取决于用户如何部署Kerberos，Kerberos需要在整个网络中进行时间同步，如果用户减小授权票据的存活时间，将可以降低入侵者通过替换票据获取访问权限的风险。此外，由于Kerberos服务中的KDC保存了所有客户端的访问密钥，因此，KDC需要在物理和网络安全上进行双重的加固，以保证整个网络的安全。Kerberos优点有：① 单点登录，只要用户拿到了TGT并且该TGT没有过期，就可以使用该TGT通过TGS完成到任一个服务器的认证而不必重新输入密码。② 与授权机制相结合。③ 支持双向的身份认证。④ 通过交换“跨域密钥”实现分布式网络环境下的认证。Kerberos缺点有：① AS和TGS是集中式管理，容易形成瓶颈，系统的性能和安全也严重依赖于AS和TGS的性能和安全。② 时钟同步问题。③ 身份认证采用的是对称加密机制，随用户数量增加，密钥管理较复杂。（3）SESAMESESAME是多厂商环境下的欧洲安全系统的缩写，是一个由欧盟委员会资助的研究项目。SESAME技术能够提供单点登录功能和分布式的访问控制，所有在网络上传输的数据都可以使用对称和非对称加密方法进行处理。SESAME的认证过程类似于Kerberos，实际上SESAME也能够使用Kerberos第5版协议。2.4 审计和监控技术在计算机系统中，认证、访问控制和审计共同建立了保护系统安全的基础，安全审计是对认证和访问控制的有效补充。安全审计对用户使用何种信息资源、使用时间，以及如何使用（执行何种操作）进行记录并检查。审计和监控的联合，能够再现原有的使用场景、发现操作时的问题，对于追查责任和恢复数据非常必要。2.4 审计和监控技术2.4.1 审计和监控基础日志就是记录的事件或统计数据，这些事件或统计数据能提供关于系统使用及性能方面的信息。审计就是对日志记录的分析，并以清晰的、能理解的方式表述系统信息。审计使得系统分析员可以评审资源的使用模式，以便评价保护机制的有效性。安全审计在系统安全保护方面，具有重要的作用。通过安全审计，能记录系统被访问的过程以及系统保护机制的运行状态，发现试图绕过保护机制的行为，及时发现用户身份的变化，报告并阻碍绕过保护机制的行为并记录相关过程，为灾难恢复提供信息等。安全审计的目标有两个：（1）必须提供足够的信息使得安全人员能够将问题限制于局部，而信息量不足以以此为基础进行攻击。（2）优化审计记录的内容，审计分析机制应可以对一些特定资源辨认正常的行为。审计是通过对所关心的事件进行记录和分析来实现的，因此一个审计系统通常由三部分组成：日志记录器、分析器、通告器，分别用于收集数据、分析数据及通报结果。（1）日志记录器日志机制可以把信息记录成二进制形式或可读的形式。系统会提供一个日志浏览工具。用户能使用工具检查原始数据或用文本处理工具来编辑数据。2.4 审计和监控技术1）日志的内容在理想的情况下，日志应该记录每一个可能的事件，以便分析发生的所有事件，并恢复任何时刻进行的历史情况。然而，这样做显然是不现实的，因为要记录每一个数据包、每一条命令和每一次存取操作，需要的存储量将远远大于业务系统，并且将严重影响系统的性能。因此，日志的内容应该是有选择的。一般情况下，日志记录的内容应该满足以下原则：日志应该记录任何必要的事件，以检测已知的攻击模式；日志应该记录任何必要的事件，以检测异常的攻击模式；日志应该记录关于记录系统连续可靠工作的信息。通常，对于一个事件，日志应包括事件发生的日期和时间、引发事件的用户（地址）、事件和源和目的的位置、事件类型、事件成败等。2）安全审计的记录机制不同的系统可采用不同的机制记录日志。日志的记录可能由操作系统完成，也可以由应用系统或其它专用记录系统完成。但是，大部分情况都可用系统调用Syslog来记录日志。2.4 审计和监控技术（2）分析器分析器以日志作为输入，然后分析日志数据。分析的结果可能会改变正在记录的数据，也可能只是检测一些事件或问题。通过对日志进行分析，发现所需事件信息和规律是安全审计的根本目的。因此，审计分析十分重要。日志分析就是在日志中寻找模式，主要内容如下：① 潜在侵害分析。日志分析应能用一些规则去监控审计事件，并根据规则发现潜在的入侵。这种规则可以是由已定义的可审计事件的子集所指示的潜在安全攻击的积累或组合，或者其它规则。② 基于异常检测的轮廓。日志分析应确定用户正常行为的轮廓，当日志中的事件违反正常访问行为的轮廓，或超出正常轮廓一定的门限时，能指出将要发生的威胁。③ 简单攻击探测。日志分析应对重大威胁事件的特征有明确的描述，当这些攻击现象出现时，能及时指出。④ 复杂攻击探测。要求高的日志分析系统还应能检测到多步入侵序列，当攻击序列出现时，能预测其发生的步骤。（3）通告器分析器把分析结果传送到通告器，通告器把审计结果通知系统管理员和其它实体，这些实体可能执行一些操作来响应通告结果。2.4 审计和监控技术2.4.2 审计和监控技术安全监控通过实时监控网络或主机活动，监视分析用户和系统的行为，审计系统配置和漏洞，评估敏感系统和数据的完整性，识别攻击行为，对异常行为进行统计和跟踪，识别违反安全法规的行为，使用诱骗服务器记录黑客行为等功能，使管理员有效地监视、控制和评估网络或主机系统。安全监控的对象按照不同标准可以划分成不同的分类，将主要从恶意行为监控和内容监控两方面进行介绍。1．恶意行为监控恶意行为审计与监控主要监测针对网络中针对服务器的恶意行为，包括恶意的攻击行为和入侵行为。恶意的攻击行为，如拒绝服务攻击、网络病毒等等，这些行为旨在消耗服务器资源，影响服务器的正常运作，甚至服务器所在网络的瘫痪；恶意的入侵行为，会导致服务器敏感信息泄露，入侵者更是可以为所欲为，肆意破坏服务器。为了减轻网络恶意行为对互联网基础设施和重要应用系统的危害，必须对网络威胁进行监控和追踪。恶意行为的监控方式主要分为两类：主机监测和网络监测。主机监测是在用户主机上安装反病毒软件和基于主机的入侵检测软件，对入侵主机的已知恶意代码进行检测和告警。它能够提供详细的入侵信息，但如果主机上不安装入侵检测软件，则无法监测到任何入侵活动，因此该方式的监测规模取决于安装入侵检测软件的主机数目，可监测的地址空间规模有限。2.4 审计和监控技术网络监测中最常用的技术是在活动网络中被动监听网络流量，利用检测算法识别网络入侵行为。监测活动网络虽然扩大了监测范围，但区分活动网络中的“善意”和恶意流量却变得非常困难，致使检测结果中存在着大量虚警。第二种网络监测技术是在未使用IP地址空间内被动收集数据。通常采用发布全球路由公告的方式，将发往未使用地址空间的分组包全部路由至特定网络流量收集设施。与基于主机的监测技术相比，这种技术能够扩大监测地址空间规模，但无法获取有关特定安全事件的详细信息；与应用于活动网络的网络监测技术相比，由于黑洞地址空间中不存在合法主机，因此到达该空间的任何流量均可看作是恶意或网络误配流量，从而降低了检测虚警。但这种集中收集恶意流量的监测方式割裂了恶意流量与原有活动网络流量之间的关联，适于观测大规模地址空间上的恶意行为分布，而不适于监测特定活动网络中发生的恶意威胁。第三种网络监测技术是将未使用地址空间伪装成活动网络空间，通过与入侵者的主动交互获取入侵详细信息，如蜜罐技术（HoneynetProject，相关软件有honeyd等）。与以上两种网络监测技术相比，这种技术可以应用于活动网络并模拟活动主机的主动交互功能，能够有效分离出活动网络中的恶意流量，监测到与活动主机相关联的网络入侵行为，从而达到保护监测网络的目的。该技术可通过模拟服务来获取入侵事件的具体信息，通过在一台物理主机上虚拟网络和不同操作系统的主机来扩大监测地址空间，从而可在监测规模和监测细节间取得折衷，因此这种网络监测技术已成为目前网络安全领域的新兴技术。2.4 审计和监控技术蜜网是在蜜罐技术上逐渐发展起来的一个新的概念，又可称为诱捕网络。蜜网技术实质上还是一类研究型的高交互蜜罐技术。其主要目的是收集黑客的攻击信息。但与传统的蜜罐技术的差异在于，蜜网构成了一个黑客诱捕网络体系架构，在这个架构中，可以包含一个或多个蜜罐，同时保证网络的高度可控性，以及提供多种工具以方便对攻击信息的采集和分析。蜜罐系统没有任何的业务活动，因此蜜罐系统中发生的任何行为都是恶意的。通过实时监控蜜罐系统文件系统的变化，从而发现和捕获恶意代码样本。恶意代码诱捕系统由高交互蜜罐、低交互蜜罐和主机行为监视模块三大部分组成，其中高交互蜜罐和低交互蜜罐配合完成“诱”的功能，主机行为监视模块在“诱”的平台上完成“捕”的操作。高交互蜜罐指的是用做攻击诱捕的有真实操作系统的虚拟机系统，可以收集到丰富的主机响应信息。为了使“诱”更有效果，蜜罐系统的操作系统包括常用的Windows版本和Linux版本，提供常见服务例如web服务、ftp服务等，同时有意遗留部分漏洞不打补丁。低交互蜜罐是用通过脚本或其它形式程序虚拟部分操作系统及服务行为，同时模拟系统服务漏洞，达到攻击诱捕的目的。2.4 审计和监控技术主机行为监视模块，装在高交互蜜罐系统上，捕获系统网络连接变化、文件系统变化、系统服务变化、进程变化等操作系统主机行为信息，生成主机监视日志，同时通过文件系统变化情况提炼恶意样本文件。主机行为监视模块应具备隐秘性，不为攻击者所发现。互联网上传播的恶意代码攻击高交互式蜜罐系统上存有安全漏洞的网络服务，并感染蜜罐系统，在大多数情况下，恶意代码样本将会被传播并保存在蜜罐主机的文件系统中，监控组件将通过截获文件系统调用，实时捕获新建的或修改的恶意代码样本文件。2．网络信息内容审计网络内容安全问题主要表现在对网络数据的攻击上，通常是为政治与社会稳定服务，防止造成社会不安定的信息向网络进行传播，主要是对特定信息的监测与阻断，主要作用于内容的机密性、真实性和可用性三个属性。信息内容安全的问题主要表现在有害信息利用互联网所提供的自由流动的环境肆意扩散，其信息内容或者像脚本病毒那样给接收的信息系统带来破坏性的后果，或者像垃圾邮件那样给人们带来烦恼，或者像谣言那样给社会大众带来困惑，从而成为社会不稳定因素。网络信息内容审计是指通过采取一定的技术手段，监管网络中不良文本、图片、视频等各类信息的传播行为，以保证网络所传播的各类信息内容的健康性、合法性，提供干净的网络信息环境。2.4 审计和监控技术网络信息内容审计侧重于理解网络所传播的信息内容，判断信息内容的性质，并根据相关的安全策略，对非法、不良等各类网络信息进行有效控制和管理，是网络安全中保障信息资源安全性的重要组成部分。1996年英国颁布《三R互联网安全规则》，旨在消除网络上的色情内容；美国出台《儿童在线保护法》、《电子通信隐私法》等法规加强对网络言论的规范和保护；我国在2000年9月颁布了《互联网信息服务管理办法》等多个涉及互联网的法律文件，对非法网络信息内容做出了明确的规定。（1）审计与监控方法内容监控的主要方法为网络舆情分析。舆情是指在一定的社会空间内，围绕中介性社会事件的发生、发展和变化，民众对社会管理者产生和持有的社会政治态度。它是较多群众关于社会中各种现象、问题所表达的信念、态度、意见和情绪等等表现的总和。网络舆情形成迅速，对社会影响巨大，不仅需要各级党政干部密切关注，也需要社会各界高度重视。由于网络信息量十分巨大，仅依靠人工的方法难以应对网络海量信息的收集和处理，需要加强相关信息技术的研究，即网络舆情分析技术。网络舆情分析从互联网这个巨大的数据来源中获取信息，萃取为针对特定社会公共事务的情况概览，为公共事务管理者提供决策参考，及时应对网络舆情，由被动防堵，化为主动梳理、引导。2.4 审计和监控技术网络舆情分析系统应该具备以下三个部分：首先是舆情分析引擎。这是舆情分析系统的核心功能，包括：① 热点话题、敏感话题识别，可以根据新闻出处权威度、评论数量、发言时间密集程度等参数，识别出给定时间段内的热门话题。利用关键字布控和语义分析，识别敏感话题。② 倾向性分析，对于每个话题，对每个发信人发表的文章的观点、倾向性进行分析与统计。③ 主题跟踪，分析新发表文章、帖子的话题是否与已有主题相同。④ 自动摘要，对各类主题，各类倾向能够形成自动摘要。⑤ 趋势分析，分析某个主题在不同的时间段内，人们所关注的程度。⑥突发事件分析，对突发事件进行跨时间、跨空间综合分析，获知事件发生的全貌并预测事件发展的趋势。⑦ 报警系统，对突发事件、涉及内容安全的敏感话题及时发现并报警。⑧ 统计报告，根据舆情分析引擎处理后的结果库生成报告，用户可通过浏览器浏览，提供信息检索功能，根据指定条件对热点话题、倾向性进行查询，并浏览信息的具体内容，提供决策支持。 其次是自动信息采集功能。现有的信息采集技术主要是通过网络页面之间的链接关系，从网上自动获取页面信息，并且随着链接不断向整个网络扩展。目前，一些搜索引擎使用这项技术对全球范围内的网页进行检索。舆情监控系统应能根据用户信息需求，设定主题目标，使用人工参预和自动信息采集结合的方法完成信息收集任务。2.4 审计和监控技术第三是数据清理功能。对收集到的信息进行预处理，如格式转换、数据清理，数据统计。对于新闻评论，需要滤除无关信息，保存新闻的标题、出处、发布时间、内容、点击次数、评论人、评论内容、评论数量等。对于论坛BBS，需要记录帖子的标题、发言人、发布时间、内容、回帖内容、回帖数量等，最后形成格式化信息。条件允许时，可直接针对服务器的数据库进行操作。舆情分析系统的核心技术在于舆情分析引擎，涉及的最主要的技术包括文本分类、聚类、观点倾向性识别、主题检测与跟踪、自动摘要等计算机文本信息内容识别技术，这些技术一向是国内外信息工作者关注的领域。（2）网络信息内容审计系统模型网络信息内容审计系统包括对网络信息报文格式的完整性与合法性进行形式化审查及对报文类型与内容审查两部分，主要在应用层对信息内容进行审计分析，发现可疑行为，并对这些行为采取相应的措施，如记录、报警和阻断等，实现对网络信息内容的检测与控制。网络信息内容审计涉及的技术，主要有两类：① 网络信息内容的获取技术（也称为嗅探技术），主要研究如何在大规模网络环境中快速获取各种协议的信息内容；② 网络内容还原分析技术，主要是将获取的数据包还原，并分析其中的信息内容。根据具体需求和资源限制，可以将内容审计系统分为流水线模型和分段模型两种过程模型：2.4 审计和监控技术① 流水线模型是一种可使两个或多个操作在执行时发生重叠的技术。在流水线操作中，一个任务被分解为多个子任务。在执行时，多个子任务相互重叠。根据处理流量不同，流水线处理过程中各个时期的延时均不相同，但应保证延时的平均值不会随时间的推移而增大。因此，流水线处理要求各个部分处理速度基本相同。② 分段式处理模型的基本思想是先收集某个网段一定时间内的数据，然后进行离线式分析。此模型分为实时处理和离线处理两部分。包捕获以前的部分设计为实时处理部分，协议分析还原部分设计为离线处理部分。与流水线模型相比，分段式处理模型的瓶颈在于其包捕获处理能力，仅能对部分时间段内的高速流量进行处理。（3）不良信息内容监控方法对于网络中不良信息监控的方法，主要包括：① 网址过滤技术，即通过封锁网址来达到控制访问的目的，这种方法实现简单，在明确判定网站性质时有较好的控制效果。但这种方法需要定期搜索更新不良信息网站地址，具有滞后性，不能适应动态变化。② 网页内容过滤技术，通过在网页文字中搜索设定的关键字来判断是否有不良信息。由于文本内容审计的局限性，当网络中不包含敏感文字时，会造成不良站点被漏过以及合法站点被屏蔽等。2.4 审计和监控技术③ 图像内容过滤方式，即利用图像识别技术来判断网页中是否含有不良图像。由于不良网站中通常存在大量不良图片，这种技术已经成为研究热点。网址过滤技术和网页内容过滤技术自身具有一定的局限性，对不良信息识别方面准确率不够高。在网络不良信息的传播中，不良图像、视频较之文本信息，其危害性更为严重。所以，对网络中的不良图片及视频等进行分析具有更现实的意义。2.5 小结1. 密码技术根据密钥的数量，可以将密码体制分为两类：对称密钥密码体制和非对称密钥密码体制。对称加密的优点在于加密速度快，最大缺点在于其密钥管理困难。非对称密码体制，也称为公开密钥密码，从根本上克服了对称密码密钥分配上的困难，且易于实现数字签名，而典型缺点在于加解密效率较低。因此，在应用中通常采用对称密码体制实现数据加密、采用公钥密码体制实现密钥管理的混合加密机制。对称密钥体制根据对明文的加密方式的不同而分为两类：分组密码和序列密码。分组密码主要有五种工作模式，分别是电子密码本模式、密码分组链模式、密码反馈模式模式、输出反馈模式和计数模式。2.5 小结扩散和混淆是对称密码设计的主要思想，乘积迭代的方法是达到扩散和混淆目的的常见方法，DES算法所采用的Feistel网络和AES算法所采用的SP网络，是两类典型的迭代密码。基于难解问题设计密码是非对称密码设计的主要思想，其中RSA基于大合数因式分解难的问题设计、ElGamal 基于离散对数求解困难的问题设计、ECC则基于椭圆曲线离散对数求解困难的问题设计。虽然大合数因式分解十分困难，但随着科学技术发展，对于大合数因式分解的能力在不断的提高。因此，为了确保RSA密码的安全，必须认真选择RSA的密码参数。哈希函数又称为散列函数、杂凑函数，它是一种单向密码体制，即它是一个从明文到密文的不可逆映射，只有加密过程，没有解密过程。同时，哈希函数可以将任意长度的输入经过变换后得到固定长度的输出。单向及输出长度固定的特征使得哈希函数可以生成消息或者数据块的消息摘要，因此，在数据完整性和数字签名领域有着广泛的应用。典型的哈希函数有两类：消息摘要算法MD5和安全散列算法SHA，SHA比MD5更安全。数字签名是一种以电子形式存在于数据信息之中的，或作为其附件或逻辑上与之有联系的数据，可用于辨别数据签署人的身份，并表明签署人对数据信息中包含的信息的认可的技术。目前主要采用基于公钥密码体制的数字签名，包含两个过程：签名和验证签名。实际应用中为了缩短签名的长度、提高签名的速度，而且为了更安全，常对信息的摘要进行签名。2.5 小结密钥管理是指处理密钥自产生到最终销毁的有关问题的全过程，包括密钥的生成、存储、分配、启用与停用、控制、更新、撤销与销毁等诸多方面，其中密钥的分配与存储最关键。从密钥信息的交换方式来说，密钥分配可以分成三类：人工密钥分发、基于中心的密钥分发和基于认证的密钥分发。典型的密钥交换协议是DiffieHellman算法，它是第一个实用的在非保护信道中创建共享密钥方法，本身是一个匿名（无认证）的密钥交换协议，已成为很多认证协议的基础。2. 认证技术消息认证是验证所收到的消息确实来自真正的发送方，并且未被篡改的过程。常见的三类产生消息认证码的方法是消息加密、消息认证码和哈希函数。身份认证是对网络中的主体进行验证的过程，主要通过身份认证协议和认证系统软硬件进行实现，是许多应用系统中安全保护的第一道设防。身份认证协议分为：单向认证协议和双向认证协议，常用的认证协议则包括基于口令的认证协议、基于对称密码的认证和基于公钥密码的认证。2.5 小结3. 访问控制技术访问控制是在身份认证的基础上，依据授权对提出的资源访问请求加以控制。访问控制模型主要包括三类：自主访问控制、强制访问控制和基于角色的访问控制。自主访问控制的实现机制是通过访问控制矩阵实施，而具体的实现办法则是通过访问能力表或访问控制表来限定哪些主体针对哪些客体可以执行什么操作。强制访问控制强调主体服从访问控制政策，对访问主体和受控对象标识安全标签，系统通过比较主体和客体的安全标签来决定一个主体是否能够访问某个客体，两个典型的强制访问控制模型是BellLaPadula模型和Biba模型：BellLaPadula模型具有只允许向下读、向上写的特点，可以有效地防止机密信息向下级泄露；Biba模型则具有不允许向下读、向上写的特点，可以有效地保护数据的完整性。基于角色的访问控模型的基本思想是将访问许可权分配给一定的角色，用户通过饰演不同的角色获得角色所拥有的访问许可权。访问控制的管理方法可以分为两类：集中式访问控制和分布式访问控制。集中式的AAA管理协议包括拨号用户远程认证服务RADIUS、终端访问控制器访问控制系统TACACS、Diameter等。三种典型的分布式访问控制方法包括单点登录、Kerberos协议和SESAME。2.5 小结4. 审计与监控技术审计是通过对所关心的事件进行记录和分析来实现的，因此一个审计系统通常由三部分组成：日志记录器、分析器、通告器，分别用于收集数据、分析数据及通报结果。安全监控通过实时监控网络或主机活动，使管理员有效地监视、控制和评估网络或主机系统。恶意行为的监控方式主要分为两类：主机监测和网络监测。蜜罐技术是一种网络监测技术，它将未使用地址空间伪装成活动网络空间，通过与入侵者的主动交互获取入侵详细信息，以达到对攻击活动进行监视、检测和分析的目的。网络信息内容监控的主要方法为网络舆情分析。2.5 小结习题1. 简述密码体制的构成。2. 简述分组密码与序列密码的区别。3. 简述对称密码和非对称密码体制的区别。4. 简述分组密码的工作模式。5. 什么是乘积密码，它的主要作用是什么？简述DES和AES所使用的两类乘积密码。6. 简述DES、AES、IDEA三种典型对称加密算法的工作原理；简述RSA算法的原理以及参数选择；简述ECC所依赖的数学难题。7. 设通信双方使用 RSA 加密体制，接收方的公开钥是(e, n) = (5, 35)，接收到的密文是c = 10，求明文m。2.5 小结习题8. 什么是HASH函数？对HASH函数的基本要求和安全性要求分别是什么？9. 简述MD5和SHA的工作原理及区别。10. 简述数字签名的作用，及数字签名体制的两个过程。数字签名要预先使用单向HASH函数进行处理的原因是什么？11. 简述在公钥体制下利用 DiffieHellman方法产生共享密钥的方法。12. 简述密钥分配的分类及各自的工作原理。13. 什么是消息认证？为什么要进行消息认证？14. 消息认证的方法有哪些？为什么人们一直用哈希函数而不是用对称密码来构造消息认证呢？15. 简述基于DES的消息认证码的生成算法。16. 简述身份认证的协议。17. 描述使用DES算法实现一次性口令的算法。18. 描述基于公钥密码的单向和双向身份认证的过程。2.5 小结习题19. 简述一下数字签名的产生和验证过程。20. 举例说明访问控制中主体和客体；简述访问控制模型的分类及其优缺点。21. 举例说明访问能力表和访问控制表的应用。22. 简述BellLaPadula模型和Biba模型的工作原理和区别。23. 简述RADIUS协议、TACACS协议以及Diameter的区别。24. 简述单点登录机制及其实现原理。25. 简述审计和监控的作用及审计系统的组成。26. 简述恶意行为审计与监控的实现方法及网络信息内容审计的方法。信息安全等级考试三级教材Nankai University刘哲理 13212115916信息安全等级考试三级教材第三章 系统安全考核目标了解操作系统体系架构、基本概念和基本元素，了解操作系统基本实现机制；了解Unix/Linux系统架构和关键系统组件，理解系统服务和系统进程，理解Unix/Linux系统启动过程，理解Unix/Linux系统安全实现，包括文件系统安全、账户安全、日志与审计等；了解Windows系统架构和关键系统组件，理解系统服务和系统进程，理解Windows系统启动过程，理解Windows系统安全实现，包括文件系统安全、身份认证与验证授权、账号安全、日志与审计等；了解可信计算技术的产生及发展，了解我国可信计算技术及其与TCG可信计算技术的区别。考核目标了解数据库概念，掌握结构化查询语言SQL，理解数据库安全概念，理解数据库安全功能，掌握数据库“视图”对于数据保密性的作用，理解“规则与默认”和“事务管理”对于数据完整性的作用；理解数据库威胁与防护，掌握数据库安全特性检查，了解数据库运行安全监控，了解数据库管理系统产品安全，了解数据库管理系统安全要求。3.1 操作系统安全3.1.1 操作系统安全基础1．操作系统基本概念一般情况下，我们不能直接操作裸机，必须通过一个叫做基本输入输出系统（BIOS，Basic Input/Output System）的软件系统，才能操作控制裸机，之所以这样称呼它，是因为它提供了最基本的计算机操作功能，如在屏幕上显示一点、接收一个键盘字符的输入等。3.1 操作系统安全在基本输入输出系统的外面是操作系统（OS，OperatingSystem），专门负责管理计算机各种资源，并提供操作电脑所需的工作界面。计算机主要由四部分组成，分别为硬件设备、基本输入输出系统、操作系统及应用程序。（1）操作系统基本概念操作系统是控制其它程序运行，管理系统资源并为用户提供操作界面的系统软件的集合。操作系统是计算机系统的内核与基石。（2）操作系统基本元素操作系统通过一些基本元素，在硬件支持的基础上来实现其功能。3.1 操作系统安全1）用户模式和内核模式现代 CPU通常运行在两种模式下：① 内核模式，在 Intel x86 系列中称为核心层（Ring 0）。② 用户模式，也称为用户层（Ring 3）。如果CPU处于内核模式，那么硬件将允许执行一些仅在内核模式下许可的特殊指令和操作。一般看来，操作系统应当运行在内核模式下，其它应用应当运行在用户模式下。显然，要使内核模式所提供的保护真正有效，那么普通指令就不能自由修改CPU的模式。在标准的模型中，将CPU模式从用户模式转到内核模式的唯一方法是触发一个特殊的硬件自陷，如① 中断，一些外部硬件引发的，如I/O或者时钟。② 异常，如除数为零、访问非法或者不属于该进程的内存。③ 显式地执行自陷指令。3.1 操作系统安全2）内存管理如果要避免用户进程相互影响，那么最好的方法是避免它们互相从对方的存储区域读写数据，同时还应当避免读写操作系统的内存区域，其中也包括操作系统代码。系统达到该目的方法是在CPU和系统其它部分之间的地址总线上嵌入内存管理单元 （MMU，Memory ManagementUnit) 。CPU 发射合适的地址，MMU 单元负责将逻辑地址转换成物理地址，操作系统使用特殊指令来建立和控制这种转换关系。MMU的转换机制也可以使我们能够标记某些内存区域仅是可读的（对用户代码而言），如果用户级的CPU试图发出一条写入该地址的指令，那么MMU将拒绝转换地址，同时将引发异常，从而进入内核级。3.1 操作系统安全与此类似，MMU可以避免用户代码读取不该访问的内存。内核创建仅由它自己才能查看的内存区域，并使用该片内存来存储用户进程维护数据、I/O缓冲等。然而，如何完成这一过程依赖于硬件体系结构和操作系统的设计选择。3）用户接口用户接口是为方便用户使用计算机资源所建立的用户和计算机之间的联系，主要有两类接口：作业级接口和程序级接口。作业级接口是操作系统为用户对作业运行全过程控制提供的功能，解决了用户如何将请求告诉计算机、接到请求后计算机如何服务的问题。从用户角度看，作业是用户要求计算机所做的工作的集合。从程序运行的角度看，作业由一些相对独立的顺序执行的步骤所组成，这些相对独立的执行步骤通常被称为作业步。3.1 操作系统安全从系统角度看，作业由一个完整的用户程序、数据和作业说明书三部分组成。程序是问题求解的算法描述；数据是程序加工的对象；作业说明书是告诉操作系统本作业的程序和数据按照什么样的数据要求使之执行。用户要求处理问题时，应首先用某种程序设计语言对要处理的问题编制源程序，再准备好初始数据，然后把编制好的源程序和准备好的数据输入到计算机系统中，在操作系统的控制下，经过编译、装配、运行等加工步骤，就能得到处理结果。程序级接口是操作系统专门为用户程序设置的，它也是用户程序取得操作系统服务的唯一途径。程序接口通常由各种各样的系统调用所组成。不同的系统所提供的系统调用命令不同，从功能上大致可以划分为三类：一般设备输入输出的系统调用、磁盘的输入输出及磁盘文件管理的系统调用、其它系统调用。3.1 操作系统安全4）系统调用在操作系统的内核中设置了一组用于实现各种特定系统功能的子程序（过程），并将它们提供给应用程序调用。这样，在编程过程中，需要系统完成特定的功能时，可以通过调用系统中特定的子程序完成，这就是系统调用。当用户代码需要请求操作系统提供的服务时，通常采用系统调用的方法来完成这一过程：用户代码将在约定的地方（如CPU寄存器）存储一个值，该值能够代表它所请求的服务。如果服务需要参数，则用户代码采用同样的方法将其存放在约定的地址。然后用户代码发出一条自陷指令。与其它类型的中断相同，系统做出响应，保存用户进程的状态，记录程序计数器、其它硬件寄存器、进程栈以及其它进程数据。硬件切换到内核模式，执行系统调用处理程序，该函数通常需要查找服务表以便于找到所请求服务的处理子过程入口。上述整个过程称为上下文切换。一旦所请求的服务完成，就恢复用户进程的状态，控制重新交给进程。3.1 操作系统安全2．操作系统的功能操作系统有如下基本功能：①资源管理：系统的设备资源和信息资源都是操作系统根据用户需求按一定的策略来进行分配和调度的，包括处理器管理、存储管理、设备管理、文件系统管理。②用户接口：提供人机交互操作的用户接口，为不同用户提供操作界面，实现对系统资源的控制。③进程管理：通过对CPU每个执行周期的分片，实现不同进程的调度，从而实现多任务。④内存管理：管理和规划主机内存的使用，为其它模块提供接口。操作系统的功能模块，一般以进程的方式在后台运行，以启动服务的方式对用户提供访问接口。以下仅介绍一下进程管理和文件系统管理。3.1 操作系统安全（1）进程管理进程就是为了实现多任务而提出的概念，其实它还有更细的管理单位——线程。目前的操作系统都通过多程序和多任务来有效的利用CPU时间，提高调度和的运行速度。进程管理实质上是对处理机执行“时间”的管理，将CPU真正合理地分配给每个任务，以达到多程序和多任务并发的目的。1）概念从程序运行角度来看，程序是在计算机上运行的一组指令及指令参数的集合，指令按照既定的逻辑控制计算机运行；进程是程序运行的一个实例，是运行着的程序；线程是为了节省资源而可以在同一个进程中共享资源的一个执行单位。3.1 操作系统安全从资源的组织和执行角度来看，进程是用于组织资源的最小单位，进程将相关的资源组织在一起，这些资源包括：内存地址空间、程序、数据等，将这些以进程的形式组织起来可以使得操作系统管理这些资源更为容易；而线程是安排CPU执行的最小单位，是每一个进程中执行的一条线。线程虽然共享进程中的大多数资源，但线程也需要自己的一些资源，比如：用于标识下一条执行指令的程序计数器、一些容纳局部变量的寄存器以及用于表示执行历史的栈。2）实现进程管理就是通过中断实现的。用于进程管理的定时器产生中断，则系统暂停当前代码执行，进入进程管理程序；而进程管理程序则分析当前各进程的优先级和等待顺序，选择合适的进程，将CPU的时间片交给它。3.1 操作系统安全（2）文件系统管理文件是存储在外存上具有标识名的一组相关字符流或记录的集合。文件系统是操作系统负责存取和管理文件的一组软件及所需数据结构，是用户与外存之间的接口。文件系统在操作系统存在的时候就已经存在，操作系统程序自身也是保存在文件系统之中，所以在安装系统之前总是会先将存储盘格式化成某种文件系统格式。准确地来说，文件系统是一种数据链表，用来描述磁盘上的信息结构（创建日期、修改日期、文件作者、读写属性等），并支持磁盘文件的取出和写回，如新建、修改、复制、剪切、粘贴、删除等。一旦这种表被破坏，即使磁盘中的数据不被破坏，也无法被读取出来。3.1 操作系统安全3．基本安全实现机制（1）CPU模式和保护环操作系统使用保护环机制来确保进程不会在彼此之间或对系统的重要组件造成负面影响。保护环对工作在环内的进程能够访问什么、能够执行什么命令提出了严格的界线和定义。在内环中执行的进程比在外环中执行的进程有更高的权限，这是因为内环只允许最可信的组件和进程在其中执行。虽然操作系统在保护环上的数量有所不同，但是在内环中执行的进程往往处于内核模式，在外环中工作的进程则处于用户模式。3.1 操作系统安全图3.3保护环结构（进程运行所在的环编号越小，进程的可信度越高） 0环 操作系统 内核 文件系统驱动程序 1环操作系统3环2环 操作系统实用程序文字处理器 Web浏览器图片编辑器 数据库3.1 操作系统安全保护环支持多任务操作系统所要求的可用性、完整性和机密性要求。如图3.3，最常见的保护环结构提供4个保护环：① 0环 操作系统内核② 1环 操作系统的其它部分③ 2环 I/O驱动程序和实用工具④ 3环 应用程序和用户活动这些保护环在主体和客体之间提供了一个中间层，当一个主体试图访问一个客体时，可以用它来进行访问控制。环决定对敏感系统资源的访问级别。环号越低，赋予运行在该环内的进程的权限就越大。每个主体和客体都分配有一个编号（03），这个编号取决于操作系统赋予它的信任级别。3环中的主体不能直接访问1环中的客体，但1环中的主体能直接访问3环中的客体。所有实体只能访问它所在环的客体，不能直接与外环的客体通信。当一个应用程序需要访问不允许它直接访问的环中的组件时，它要向操作系统发出请求，要求执行必要的任务。这一请求通过系统调用来处理，此时操作系统可以执行不允许在用户模式下执行的指令。请求被提交给一个操作系统服务来完成，这个服务在更高权限下运行，能够执行更加敏感的任务。3.1 操作系统安全当操作系统为0环和1环执行指令时，它在管理员模式或内核模式下运行。当操作系统为3环中的应用程序和进程执行指令时，它在用户模式下运行。用户模式为在其中运行的应用程序提供一个更加限制性的环境，这反过来又保护系统不会受到行为不端程序的伤害。注意：现在的许多操作系统并不经常使用第二保护环，有的甚至根本不用。（2）进程隔离进程隔离是指系统对同时执行的进程进行隔离，防止进程之间的互相影响，这个功能在现代操作系统中是一个基本功能。进程隔离是为保护操作系统中进程互不干扰而设计的一组不同硬件和软件的技术，是操作系统在安全性方面的主要贡献之一。为了避免进程A写入进程B的情况发生，进程隔离使用虚拟地址空间达到该目的。进程隔离要求不同的进程拥有不同的虚拟地址，即进程A的虚拟地址和进程B的虚拟地址不同，这样通过内存管理禁止一个进程读写其它进程的内存，就防止了进程A将数据信息写入进程B。3.1 操作系统安全3.1.2 操作系统安全实践1．Unix/Linux系统概述Unix是一个交互式的多用户、多任务的操作系统。（1）系统架构和关键系统组件Unix系统可分为三个层次：硬件层、内核层和用户层。（2）系统启动过程以下以Linux为例，来说明Unix/Linux系统的启动过程。第一步 加载BIOS当打开计算机电源，Intel CPU在实模式下自检，开始执行物理地址0xFFFF0处的代码，加载BIOS信息。BIOS信息包含了CPU的相关信息、设备启动顺序信息、硬盘信息、内存信息、时钟信息等。第二步 读取主引导记录硬盘上第0磁道第一个扇区被称为MBR（Master Boot Record），即主引导记录，它的大小是512字节，存放了预启动信息、分区表信息。系统找到BIOS所指定的硬盘的MBR后，就会将其复制到0x7c00地址所在的物理内存中。其实被复制到物理内存的内容就是引导程序（BootLoader）。3.1 操作系统安全第三步 加载引导程序引导程序是在操作系统内核运行之前运行的一段小程序。通过这段小程序，我们可以初始化硬件设备、建立内存空间的映射图，从而将系统的软硬件环境带到一个合适的状态，以便为最终调用操作系统内核做好一切准备。引导程序有若干种，其中Grub、Lilo和spfdisk是常见的Loader。Lilo是一个在系统启动时运行的程序，它允许选择用于引导计算机的操作系统。可以用Lilo引导几个不同的操作系统，如Linux和MSDOS。用Lilo可以定义一个默认的要引导的操作系统和一个引导该操作系统的延迟时间。Grub是一个多操作系统启动程序，是多启动规范的实现，它允许用户可以在计算机内同时拥有多个操作系统，并在计算机启动时选择希望运行的操作系统。Grub可用于选择操作系统分区上的不同内核，也可用于向这些内核传递启动参数。系统读取内存中的Grub配置信息（一般为menu.lst或grub.lst），并依照此配置信息来启动不同的操作系统。3.1 操作系统安全第四步 加载内核根据Grub设定的内核映像所在路径，系统读取内存映像，并进行解压缩操作。此时，屏幕一般会输出“Uncompressing Linux”的提示。当解压缩内核完成后，屏幕输出“OK, booting the kernel”。系统将解压后的内核放置在内存之中，并调用start\_kernel()函数来启动一系列的初始化函数并初始化各种设备，完成Linux核心环境的建立。至此，Linux内核已经建立起来了，基于Linux的程序应该可以正常运行了。第五步 执行init进程所谓的init进程，它是一个由内核启动的用户级进程。加载内核之后，就通过启动一个用户级程序init的方式，完成引导进程，所以init始终是第一个进程（其进程编号始终为1）。Init进程的位置是/sbin/init，它会读取/etc/inittab文件，并依据此文件来进行初始化工作。最后，执行/bin/login程序，进入登录状态。3.1 操作系统安全（3）系统服务和进程1）守护进程守护进程是脱离于终端并且在后台运行的进程。它是一个生存期较长的进程，通常独立于控制终端并且周期性地执行某种任务或等待处理某些发生的事件。守护进程常常在系统引导装入时启动，在系统关闭时终止。Unix/Linux系统有很多守护进程，大多数服务都是通过守护进程实现的，同时，守护进程还能完成许多系统任务，如作业规划进程crond、打印进程lqd等（这里的结尾字母d是Daemon的意思）。在Unix/Linux中，每一个系统与用户进行交流的界面称为终端，每一个从此终端开始运行的进程都会依附于这个终端，这个终端就称为这些进程的控制终端。当控制终端被关闭时，相应的进程都会自动关闭。但是守护进程却能够突破这种限制，它从被执行开始运转，直到整个系统关闭时才退出。如果想让某个进程不因为用户或终端或其它变化而受到影响，那么就必须把这个进程变成一个守护进程。3.1 操作系统安全2）启动与关闭服务在Unix/Linux中，服务就是运行在网络服务器上监听用户请求的进程，服务是通过端口号来区分的。在大多数Unix/Linux机器上的/etc/services中可以找到常用的一部分服务，包括：ftp 21/tcp、telnet 23/tcp、smtp 25/tcp等。在Unix/Linux系统中, 服务是通过inetd进程或启动脚本来启动。通过inetd 来启动的服务可以通过在/etc/inetd.conf文件中注释来禁用；通过启动脚本启动的服务可以通过改变脚本名称的方式禁用。3）inetd 进程Inetd是Unix最重要的网络服务进程，是监视一些网络请求的守护进程，通过一个集中的配置文件（inetd.conf）来管理大多数入网连接，根据网络请求调用相应的服务进程来处理连接请求。使用 inetd 来运行那些负载不重的服务有助于降低系统负载，避免出现可能有几十种服务都运行在内存中准备被使用的情况。它们都列在inetd的配置文件/etc/inetd.conf中。而代替它们的是inetd监听着进入的连接。这样只需要有一个进程在内存中就可以了。3.1 操作系统安全经典的inetd守护程序已经存在很久了，有几种替换inetd的功能的方法，但是最灵活、最简便的方法是xinetd。xinetd已经取代了inetd，并且提供了访问控制、加强的日志和资源管理功能，已经成了新版Unix/Linux系统的Internet标准超级守护进程。2．Unix/Linux系统安全做为一个强大的多用户、多任务操作系统，因为安全可靠、高效强大的特点，Unix/Linux系统在服务器领域得到了广泛应用，而其安全性一直是用户关心的主要问题。下面从文件系统安全、账户安全、日志和审计方面介绍Unix/Linux系统的基础安全机制。（1）文件系统安全文件系统安全是Unix/Linux系统安全的核心。Unix/Linux文件系统控制谁能访问信息以及他们能做些什么。即使外层账号安全被突破，攻击者也很难击败文件系统根据文件拥有权和权限精心设置的防御措施。3.1 操作系统安全1）文件系统基础文件系统安全如此重要的一个原因是在Unix/Linux中，所有的事物都是文件。用户数据的集合是文件，目录是文件，进程是文件，命令是文件，甚至网络连接也是文件。Unix/Linux中的部分文件类型如下：① 正规文件—ASCII文本文件、二进制数据文件、二进制可执行文件等。② 目录—包括一组其它文件的二进制文件。③ 特殊文件—包括通常能在/dev目录下找到的设备文件，对硬件驱动器等进行信息编码。④ 链接—硬链接，把两个或更多处于同一存储位置的文件名连接起来；软链接（符号链），指向其它文件。⑤ Sockets—进程间通信时使用的特殊文件。这些不同类型的文件以一个分层的树结构进行组织，以一个叫“root”的目录为起始位置（用“/”表示），如图3.5所示。3.1 操作系统安全图3.5 Linux/Unix文件层次结构boot user lib proc bin home dev etc var lib bin man tmp lib log run spool tmp linux ljw ftp3.1 操作系统安全树中的所有东西统称为“文件系统”。虽然任何特定的Unix系统实际都由许多基于磁盘和网络的文件系统组合而成，但它为用户只提供一个树。树中的每项都由若干属性来描述，包括一个或多个名字、拥有者、分组、一组权限、长度和其它。这些属性大多数保存在磁盘中一个称为“i节点（inode）”的数据结构中。一个文件系统中的每个i节点有一个唯一的数字，每个文件有不同的i节点。i节点关注Unix文件系统中所有的文件活动。Unix文件系统安全就是基于i节点中三段关键信息：① UID：文件拥有者。② GID：文件所在分组。③ 模式：文件的权限设置。i节点中还包括其它信息：① 文件大小：以字节为单位。② 文件类型：文件、目录、链接等。③ ctime：i节点上次修改的时间。④ mtime：文件上次修改的时间。⑤ atime：文件上次访问的时间。⑥ nlink：硬链接的数目。3.1 操作系统安全提示：当攻击者窜改文件时，他们经常因修改i节点设置而留下一个足印。该足印有时能用来作为搜索攻击者的证据，即使他们试图掩盖痕迹。2）目录结构具体的目录结构如表3.1所示：3）文件权限文件权限是Unix文件系统安全的关键。Unix是一个多用户系统，甚至在只有一个用户登录时它也要正常运行。Unix文件系统中的每个文件属于一个用户和一个分组。通常，一个文件属于创建它的用户以及该用户的基本分组。每个文件和目录有三组权限与之相关：一组为文件的拥有者，一组为文件所属分组的成员，一组为其它所有用户（通常用“the world”或“others”指代）。每组权限有三个权限标志位来控制以下权限：① 可读（r）—如果被设置，则文件或目录可读。② 可写（w）—如果被设置，文件或目录可以被写入或修改。③ 可执行（x）—如果被设置，文件或目录可以被执行和搜索。3.1 操作系统安全表3.1 UNIX目录结构目录 内容/bin 用户命令的可执行文件（二进制）/dev 特殊设备文件/etc 系统执行文件，配置文件，管理文件：Red Hat Linux中为配置文件保留（非二进制）/home 用户起始目录（/u, /users, /Users是可选择的）/lib 引导系统以及在root文件系统中运行命令所需的共享库文件/lost+found 与特定文件系统断开连接的丢失文件/mnt 临时安装的文件系统（如CDROM等）/proc 一个伪文件系统，用来作为到内核数据结构或正在运行的进程的接口（多调试很有用）/sbin 为只被root使用的可执行文件以及那些只需要引导或安装/usr的文件保留/tmp 临时文件/usr 为用户和系统命令使用的可执行文件，头文件，共享库，帮助文件，本地程序/var 用于电子邮件、打印、cron等的文件，统计文件，日志文件3.1 操作系统安全这9位合起来被称为“模式位（mode bits）”。模式位通常用一列十个字符来表示，每个字符表示一个模式设置，还有一位指明文件类型。ls l命令可以查看Unix文件权限，如下所示：$ ls –lrw 1 jrandom hackers 2967 Aug 30 1994 privatedrwxrx 2 jrandom hackers 96 Mar 2 09:47 backupsrwrwrw 3 jrandom albion 15 Apr 14 1998 mbox例如，最后一行的rwrwrw以“”开始，表示mbox是一个正规文件。拥有者、分组和其它用户有相同级别的权限（rw），表示任何人可以对该文件进行读或写。第二行是一个目录（以“d”指明），其拥有者有读、写和执行/搜索权限（rwx），分组有读和执行/搜索权但不能写（rx），其它用户什么权限都没有（）。权限模式位如图 3.6描述。3.1 操作系统安全图3.6 权限模式位rwx rx rx 文件大小文件类型 其他人权限（o） 链接数所有者ID所有组ID vi Sep 15 21:21 437428 root 1 root文件拥有组权限（g） 文件拥有者权限（u）最后一次修改时间 文件名3.1 操作系统安全文件类型可以为p、d、l、s、c、b和：p表示命名管道文件、d表示目录文件、l表示符号连接文件、表示普通文件、s表示socket文件、c表示字符设备文件、b表示块设备文件。4）权限位的八进制数表示权限位还可以用一个八进制数来表示。把9个模式位分为三组，每组三位：一位为拥有者，一位为分组，一位为其它用户。然后加上表3. 2所示的数值。例如，为一个文件的拥有者授予可读和可写权限，给分组和其它用户只有可读权限，则权限位为“rwrr—”。将该权限位用八进制数表示如下：mode = owner(read) + owner(write) + group(read) + world(read)mode = 400 + 200 + 40 + 4mode = 644在表3.3中把一些绝对模式和等价的符号方式进行了比较。3.1 操作系统安全表3.2 八进制权限值权限 拥有者 分组 其它用户可读 400 40 4可写 200 20 2可执行 100 10 1无 0 0 03.1 操作系统安全表3.3 绝对模式与符号模式绝对模式 符号模式777 rwxrwxrwx755 rwxrxrx750 rwxrx700 rwx666 rwrwrw644 rwr—r640 rwr600 rw444 rrr400 r3.1 操作系统安全5）设置SUID和SGIDUnix中的SUID（Set User ID）与SGID（Set Group ID）设置了用户id和分组id属性，允许用户以特殊权利来运行程序，这种程序执行时具有文件所有者的权限和文件所在组的权限。如果一个文件被设置了SUID或SGID位，会分别表现在所有者或同组用户权限的可执行位上。例如：① rwsrxrx 表示SUID和所有者权限中可执行位被设置② rwsrr 表示SUID被设置，但所有者权限中可执行位没有被设置③ rwxrsrx 表示SGID和同组用户权限中可执行位被设置④ rwrsr 表示SGID被设置，但同组用户权限中可执行位没有被设置其实在Unix的实现中，文件权限用12个二进制位表示，如果该位置上的值是1，表示有相应的权限：11 10 9 8 7 6 5 4 3 2 1 0S G T r w x r w x r w x第11位为SUID位，第10位为SGID位，第9位为sticky位，第80位对应于上面的三组rwx位。rwsrxrx的值为： 1 0 0 1 1 1 1 0 1 1 0 1rwrSr的值为： 0 1 0 1 1 0 1 0 0 1 0 03.1 操作系统安全SUID程序是为了使普通用户完成一些普通用户权限不能完成的事而设置的。比如每个用户都允许修改自己的密码，但是修改密码时又需要root权限，所以修改密码的程序需要以管理员权限来运行。6）查看Unix文件权限ls l 命令可以来显示文件名与特性。7）Unix文件权限修改命令用户可以使用chmod命令来改变文件的权限设置。Chmod命令只能由文件拥有者或root运行。Chmod命令有两个变元：perm是为文件设置的权限；files是文件的名字。权限变元可以指明为绝对或符号模式。使用绝对模式，命令“Chmod 666 myfiles”表示将文件myfiles的权限设为rwrwrw。符号方式说起来稍微有些复杂，但也许更容易使用。其变元由3部分组成：who op permission这里：3.1 操作系统安全① who是一个用户（u）、分组（g）、其它（0）或者所有（a或ugo） 。② op是＋、－或＝之一。“＋”使得选择的权限添加到文件已存权限中，“－”把其删除，“＝”使文件只能拥有这些权限。③ permission是可读（r）、可写（w）和可执行（x），setuserid或set groupid（s），或粘位（t）的任一组合。如果who被去掉，则假设是“a”。如果要给文件foo的分组以读权限，则使用如下命令：$ chmod g+r foo与chmod相关的是chown（改变拥有权）和chgrp（改变分组）。这些命令的格式为：chown user myfilechown命令可以一次性改变拥有者和分组：chown user.group myfile（有些系统使用“:”作为分界符）。8）创建文件的默认权限创建一个文件总是有一个默认权限的，那么这个权限是怎么来的呢？这就是umask干的事情。umask设置了用户创建文件的默认权限。umask命令的一般格式：umask [选项] [权限值]。3.1 操作系统安全（2）账号安全管理1）passwd文件通常在Linux系统中，用户的关键信息被存放在系统的/etc/passwd文件中，系统的每一个合法用户账号对应于该文件中的一行记录。这行记录定义了每个用户账号的属性。超级用户root或某些高级用户可以使用系统命令passwd来更改系统中所有用户的口令，普通用户也可以在登录系统后使用passwd命令来更改自己的口令。现在的Unix/Linux系统中，口令不再直接保存在passwd文件中，通常将passwd文件中的口令字段使用一个“x”来代替，将/etc/shadow作为真正的口令文件，用于保存包括个人口令在内的数据。当然shadow文件是不能被普通用户读取的，只有超级用户才有权读取。此外，需要注意的是，如果passwd字段中的第一个字符是“\*”的话，那么，就表示该账号被查封了，系统不允许持有该账号的用户登录。当编辑/etc/passwd文件来建立一个新账号时，应在密码字段放一个“\*”，（一些伪用户，例如daemon也如此）以避免用户未经权而使用该账号，直到为此新建账号设置了真实密码。3.1 操作系统安全如果要禁用账号，在/etc/passwd文件中用户名前加一个“#”即可。相反，把“#”去掉即可取消限制。需要注意的是，系统管理员通常没有必要直接修改passwd文件，Linux提供一些账号管理工具帮助系统管理员来创建和维护用户账号。2）伪用户账号系统中有一类用户称为伪用户，这些用户在/etc/passwd文件中也占有一条记录，但是不能登录，因为它们的登录shell为空。它们的存在主要是方便系统管理，满足相应的系统进程对文件属主的要求。3）root账户的管理在Unix\Linux系统中，root账号是一个超级用户账户，可以对系统进行任何操作。Unix\Linux超级用户账户可以不止一个。在Unix系统中，只要将用户的UID和GID设置为0就可以将其变成超级用户，但并不是所有的超级用户都能很容易的登录到Unix系统中，这是因为，Unix系统使用了可插入认证模块PAM进行认证登录，PAM要求超级用户只能在指定的终端上进行访问，以确保系统的安全性。Root用户账户也是有密码的，这个密码可以对那些通过控制台访问系统的用户进行控制，即使是使用su命令的用户也不例外。3.1 操作系统安全在使用root账户的时候，要注意以下事项：① 除非必要，避免以超级用户登录。② 严格限制root只能在某一个终端登陆，远程用户可以使用/bin/su l来成为root。③ 不要随意把root shell留在终端上。④ 若某人确实需要以root来运行命令，则考虑安装sudo这样的工具，它能使普通用户以root来运行个人命令并维护日志。⑤ 不要把当前目录(“. /”)和普通用户的bin目录放在root账号的环境变量PATH中。⑥ 永远不以root运行其它用户或不熟悉的程序。（3）日志与审计审计可以提供一种追踪用户活动的方法，使得系统管理员可以知道系统的日常活动、及时了解和处理安全事件，而且审计是一种在安全事件发生后可以提供法律证据的机制。因此，启用审计非常有必要。在Unix\Linux中, 主要的审计工具是 syslogd守护进程。通过配置这个后台进程程序，可以提供各种水平的系统审计和指定输出目录。3.1 操作系统安全1）日志系统Unix系统中，主要分为以下3种形式的日志系统：① 记录连接时间的日志系统中多个进程运行时，把记录写入到/var/log/wtmp和/var/run/utmp，这两个文件的更新由login等进程完成，以便于管理员跟踪谁在何时登录了系统。② 进程统计进程的执行和终止，都将被记录到统计文件pacct和acct中。进程统计由系统内核执行，目的是为系统中的基本服务提供命令使用情况统计。③ 错误日志由syslog执行各种系统守护进程、用户程序和内核通过syslog向文件/var/log/messages报告值得注意的事件。2）连接时间日志有关当前登录用户的信息记录在文件/var/run/utmp中，登录进入和退出纪录在文件/var/log/wtmp中，数据交换、关机和重起也记录在wtmp文件中，所有的纪录都包含时间戳。3.1 操作系统安全Login等程序更新wtmp和utmp文件，使系统管理员能够跟踪谁在何时登录到系统。最后一次登录文件可以用lastlog命令查看，它根据UID排序显示登录名、端口号和上次登录时间。如果一个用户从未登录过，lastlog显示\*\*Never logged\*\*。wtmp和utmp文件都是二进制文件，它们不能被诸如tail命令剪贴或合并（使用cat命令）。用户需要使用who、w、users、last和ac来使用这两个文件包含的信息。① who命令Who命令查询utmp文件并报告当前登录的每个用户。Who的缺省输出包括用户名、终端类型、登录日期及远程主机。② w命令w命令查询utmp文件并显示当前系统中每个用户和它所运行的进程信息。③ users命令users命令用单独的一行打印出当前登录的用户，每个显示的用户名对应一个登录会话。如果一个用户有不止一个登录会话，那他的用户名将显示相同的次数。$ usersalice carol dave bob3.1 操作系统安全④ last命令last命令往回搜索wtmp来显示自从文件第一次创建以来登录过的用户。如果指明了用户，那么last只报告该用户的近期活动。⑤ ac命令ac命令根据当前的/var/log/wtmp文件中的登录进入和退出来报告用户连结的时间（小时）。“d”标志产生每天的总的连接时间，“p”标志报告每个用户的总的连接时间，如果不使用标志，则报告总的时间。$ actotal 136.253）进程统计日志当一个进程终止时，为每个进程往进程统计文件pacct或acct中写一个纪录。进程统计的目的是为系统中的基本服务提供命令使用统计。4）错误日志由syslogd执行。各种系统守护进程、用户程序和内核通过syslog向文件/var/log/messages报告值得注意的事件。另外有许多Unix程序创建日志。像HTTP和FTP这样提供网络服务的服务器也保持详细的日志。3.1 操作系统安全5）本地日志记录方式Syslog 设 备 依 据 两 个 重 要 的 文 件 ： /etc/syslogd （ 守 护 进 程 ） 和/etc/syslog.conf（配置文件），习惯上，多数syslog信息被写到/var/log目录下的信息文件中（messages.\*）。Syslog.conf文件指明syslogd程序纪录日志的行为，该程序在启动时查询配置文件。6）远程日志记录方式因为syslog daemon的默认配置是拒绝接收来自网络上的信息，我们必须使它能够接收来自网络上的信息。3．Windows系统概述作为一个实际应用中的操作系统，Windows没有单纯地使用某一种体系结构，它的设计融合了分层操作系统和客户/服务器（微内核）操作系统的特点。（1）系统架构为了防止用户应用程序访问或更改重要的操作系统数据，计算机的处理器支持两种模式：用户模式和内核模式。3.1 操作系统安全用户应用程序代码在用户模式下运行，操作系统代码（如系统服务和设备驱动程序）在内核模式下运行。内核模式是处理器的一种执行模式，它允许访问所有的系统内存和所有的CPU指令。操作系统软件的特权级别高于应用程序软件，这样，处理器就为操作系统的设计者提供了一个必要的基础，保证了应用程序的不当行为在总体上不会破坏系统的稳定性。表3.9列出了Windows操作系统核心组件的文件名。（2）系统服务和进程1）Windows系统基本进程根据系统进程的重要程度可以分为最基本的系统进程和附加进程。基本的系统进程是系统运行的必备条件，只有这些进程处于活动状态，系统才能正常运行；而附加进程则不是必需的，可以按需建立或结束。表3.10列出了Windows系统中最基本的9个进程，通常情况这些进程是不应被终止的。3.1 操作系统安全表3.9 Windows操作系统核心组件文件名 组件Ntoskrnl.exe 执行体和内核Ntkrnlpa.exe 执行体和内核，支持物理地址扩展，使得系统可寻址多达64GB物理内存Hal.dll 硬件抽象层Win32k.sys Windows子系统的内核模式部分Ntdll.dll 内部支持函数，以及执行体函数的系统服务分发存根（stub）Kernel32.dll, Advapi32.dll,User32.dll, Gdi32.dll Windows的核心系统DLL3.1 操作系统安全表3.9 Windows操作系统核心组件序号 进程项 描 述1 csrss.execsrss.exe是微软客户端/服务端运行时的子系统，该进程管理Windows图形相关任务。正常的进程应该是储存在%systemdrive%\system32\文件夹下。2 explorer.exeexplorer.exe是Windows程序管理器或者Windows资源管理器，它用于管理Windows图形壳，包括开始菜单、任务栏、桌面和文件管理。删除该程序会导致Windows图形界面无法适用。正常的进程应该是储存在系统目录下。3 lsass.exelsass.exe是一个关于微软安全机制的系统进程，主要处理一些特殊的安全机制和登录策略。正常的进程应该是储存在%systemdrive%\system32\文件夹下。4 services.exeservices.exe是微软Windows操作系统的一部分，用于管理启动和停止服务。该进程也会处理在计算机启动和关机时运行的服务 。 这 个 程 序 对 系 统 的 正 常 运 行 是 非 常 重 要 的 。 正 常 的 进 程 应 该 是 储 存 在%systemdrive%\system32\文件夹下。5 smss.exesmss.exe是一个会话管理子系统，负责启动用户会话。正常的进程应该是储存在%systemdrive%\system32\文件夹下。6 svchost.exesvchost.exe是一个属于微软Windows操作系统的系统程序，用于执行DLL文件。正常的进程应该是储存在%systemdrive%\system32\文件夹下。7 system idle process这个进程是作为单线程运行在每个处理器上，并在系统不处理其它线程的时候分派处理器的时间, 它专门负责收集处理器的空闲时间，它占用的CPU或内存越大，表示系统目前可分配的CPU或内存资源越多。8 spoolsv.exe 将文件加载到内存中以便迟后打印。9 winlogon.exewinlogon.exe是Windows域登录管理器。它用于处理登录和退出系统过程，在系统中的作用是非常重要的。正常的进程应该是储存在%systemdrive%\system32\文件夹下。表3.10 最基本的Windows系统进程3.1 操作系统安全2）进程安全管理进程的管理有以下几种方法：① 任务管理器Windows任务管理器是系统自带的一个很方便的软件，它能提供系统正在运行的程序和进程的相关信息，可以实现监视计算机性能、查看网络状态、终止已停止响应的程序等功能。② Msinfo32Msinfo32是Windows提供查看系统信息的工具，可以显示本地计算上硬件、系统组件和软件环境的完整视图。通过Msinfo32提供的系统信息，能够查看当前运行的程序及加载的模块。点击“开始” “运行”在运行框里输入 “ msinfo32” 打 开 “ 系 统 信 息 ” 窗 口 。 依 次 点 击 “ 软 件 环境” “正在运行任务”可以查看到进程的详细信息，比如进程路径、文件创建日期启动时间等等。③ DOS命令行管理进程常用的DOS命令见表3.11：3.1 操作系统安全表3.11 管理进程常用DOS命令指令名 说明tasklist命令 查看进程命令，并能查看进程同服务的关系taskkill命令 终止进程命令netstat命令 可以用来查看进程，并能查看进程发起程序ntsd命令 可以用来终止进程3.1 操作系统安全3）系统服务服务是一种在系统后台运行的应用程序类型，又称为Windows本机应用程序编程接口，它由执行体为用户模式和内核模式的程序提供的系统服务集。① 服务控制管理器管理系统服务最常使用的方法是Windows系统自带的服务控制管理器。通常可以通过“开始”→“管理工具”→“服务”打开，或在运行栏输入命令“services.msc”进入服务管理器。在服务的属性面板，可以通过更改服务的启动类型来依据自己的需要启动、关闭或禁用服务。切换到具体服务的属性面板的“常规”页面，“服务名称”是指服务的简称，并且也是在注册表中显示的名称，“显示名称”是指在服务配置面板中每项服务的显示名称，“描述”是对此服务的简单解释，还有“可执行文件路径”。“启动类型”是整个服务配置管理的核心。对于任意一个服务，通常都有3种不同的启动类型：Automatic（自动）、Manual（手动）和Disabled（禁止），只要从下拉菜单中选择就可以随意更改服务的启动类型。3.1 操作系统安全② net start/stop命令Net start/stop命令可以启动或关闭一项服务，还可以直接使用不带任何参数的net start命令查看当前已经启动的服务列表。命令行格式：net start/stop [service]③ sc命令从Windows XP开始，自带的DOS工具中加入了一个sc.exe（ServiceControl）的文件，可以对服务的启动类型以及服务的启动或者关闭进行操作，通常可以利用DOS的批处理优势，可以将服务设置自动化、批量化。命令行格式：SC [Servername] command Servicename [Optionname= Optionvalues]4．Windows系统安全（1）Windows安全子系统对于Windows安全子系统而言，包括以下部分：winlogon、图形化标识和验证GINA、本地安全认证、安全支持提供者的接口、认证包、安全支持提供者、网络登陆服务、安全账号管理者。3.1 操作系统安全① winlogon 和GINAWinlogon调用GINA DLL，并监视安全认证序列。 而GINA DLL提供一个交互式的界面为用户登陆提供认证请求。GINA DLL被设计成一个独立的模块，当然我们也可以用一个更加强有力的认证方式（指纹、视网膜）替换内置的GINA DLL。Winlogon 在 注 册 表 中 查 找 “ \HKLM\Software\Microsoft\WindowsNT\CurrentVersion \Winlogon”，如果存在GinaDLL键， winlogon将使用这个DLL，如果不存在该键Winlogon将使用默认值msgina.dll。② 本地安全认证本地安全认证（LSA，Local Security Authority）是安全子系统的核心，它的作用就是加载认证包，管理域间的信任关系。③ 安全支持提供者的接口微软的安全支持提供者的接口（SSPI，Security Support Provide Interface）提供一些安全服务的API，为应用程序和服务提供请求安全的认证连接的方法。3.1 操作系统安全④ 认证包认证包可以为真实用户提供认证。通过GINA DLL的可信认证后，认证包返回用户的SIDs给LSA，然后将其放在用户的访问令牌中。⑤ 安全支持提供者安全支持提供者实现一些附加的安全机制，安装时以驱动的形式安装。默认情况下有Msnsspc.dll（微软网络挑战/反应认证模块）、Msapsspc.dll（分布式密码认证挑战/反应模块）、Schannel.dll（证书模块）三种。⑥ 网络登陆服务网络登陆服务必须在通过认证后建立一个安全的通道。要实现这个目标，必须通过安全通道与域中的域控制器建立连接，然后，再通过安全的通道传递用户的口令，在域的域控制器上响应请求后，重新取回用户的SIDs和用户权限。⑦ 安全账号管理器安全账号管理器（SAM，Security Account Manager）是用来保存用户账号和口令的数据库。保存了注册表中\HKLM\Security\Sam中的一部分内容。不同的域有不同的Sam，在域复制的过程中，Sam包将会被拷贝。3.1 操作系统安全Windows对用户账户的安全管理使用了安全账号管理器机制，安全账号管理器对账号的管理是通过安全标识进行的，安全标识在账号创建时就同时创建，一旦账号被删除，安全标识也同时被删除。安全标识是唯一的，即使是相同的用户名，在每次创建时获得的安全标识都时完全不同的。因此，一旦某个账号被删除，它的安全标识就不再存在了，即使用相同的用户名重建账号，也会被赋予不同的安全标识，不会保留原来的权限。SAM 构 成 Windows 注 册 表 里 五 大 分 支 之 一 ， 保存在%systemroot%\system32\config\sam里；在Windows域控制器上，账户和口令字密文保存在活动目录（AD，Active Directory）里，对应文件是：%systemroot%\ntds\ntds.dit。安全账号管理器的具体表现就是 %SystemRoot%\system32\config\sam文件，该文件是 Windows的用户账户数据库，多数Windows系统的所有用户的登录名及口令等相关信息都会保存在这个文件中。Windows中用文件保存账号信息，不过如果我们用编辑器打开这些sam文件，除了乱码什么也看不到。因为Windows系统中将这些资料全部进行了加密处理，一般的编辑器是无法直接读取这些信息的。3.1 操作系统安全注册表 HKEY\_LOCAL\_MACHINE\SAM\SAM 、HKEY\_LOCAL\_MACHINE\SECURITY\ SAM保存的就是SAM文件的内容，在正常设置下仅对system是可读写的。在Windows NT里，口令字密文保存在SAM文件里。NT4SP3以后，微软又对保存在SAM文件里口令字密文增加了一层加密保护机制，这就是SYSKEY机制。可以在“开始”→“运行”键入“SYSKEY”命令，得到如图3.10所示窗口，可以手动激活SYSKEY机制：（2）登录验证当用户登录Windows时，Windows用两种过程验证本地登录。Windows尝试使用Kerberos作为基本验证方式，如果找不到密钥分发中心KDC服务，会使用Windows NT LanManager（NTLM）安全机制来验证在本地SAM中的用户。本地登录验证过程如下：① 输入用户名及密码然后按回车键，GINA会收集这些信息。② GINA传送这些安全信息给LSA来进行验证。③ LSA传送这些信息给SSPI。SSPI是一个与Kerberos和NTLM通讯的接口服务。3.1 操作系统安全图3.10 手动激活SYSKEY窗口3.1 操作系统安全① SSPI传送用户名及密码给Kerberos SSP。Kerberos SSP检查目的机器是本机还是域名。如果是本机，Kerberos返回错误消息给SSPI。如果找不到KDC，机器生成一个用户不可见的内部错误。② 这个内部错误促发SSPI通知GINA。GINA再次传送这些安全信息给LSA。LSA再次传送这些安全信息给SSPI。③ SSPI传送用户名及密码给NTLM driver。NTLM driver用Netlogon服务和本地SAM来验证用户。（3）用户权利与权限网络安全性依赖于给用户或者组所授予的能力，包括：权限、权利和共享。权限是指可以授予用户或组的文件系统能力，有了相应的用户权限，账户才有权去进行特定的操作。有两类用户权限，分别为登陆权限和操作权限。登录权限是指账户在通过身份验证之前所具备的权限，而操作权限是指账户在通过身份验证之后所具备的权限。权利是指在系统上完成特定动作的授权，一般由系统指定给内置组，但也可以由管理员将其扩大到组和用户上。共享是指用户可以通过网络使用的文件夹。3.1 操作系统安全1）用户权利权利适用于对整个系统范围内的对象和任务的操作，通常是用来授权用户执行某些系统任务。当用户登录到一个具有某种权利的账号时，该用户就可以执行与该权利相关的任务。2）用户权限权限适用于对特定对象如目录和文件（只适用于NTFS卷）的操作，指定允许哪些用户可以使用这些对象，以及如何使用（如把某个目录的访问权限授予指定的用户）。权限分为目录权限和文件权限，每一个权级别都确定了一个执行特定的任 务 组 合 的 能 力 ， 这 些 任 务 是 ： Read(R) 、 Execute(X) 、 Write(W) 、Delete(D)、Set Permission(P)和Take Ownership(O)。表3.12、3.13、3.14显示了这些任务是如何与各种权限级别相关联的。3）共享权限共享只适用于文件夹（目录），如果文件夹不是共享的，那么在网络上就不会有用户看到它，也就更不能访问。网络上的绝大多数服务器主要用于存放可被网络用户访问的文件和目录，要使网络用户可以访问在NT Server服务器上的文件和目录，必须首先对它建立共享。3.1 操作系统安全表3.13 文件权限权限级别 RXWDPO 允许的用户操作NoAccess 用户不能访问该目录List RX 可以查看目录中的子目录和文件名，也可以进入其子目录Read RX 具有List权限，用户可以读取目录中的文件和运行目录中的应用程序Add XW 用户可以添加文件和子目录Add and Read RXW 具有Read和Add的权限Change RXWD 有Add和Read的权限，另外还可以修改文件的内容，删除文件和子目录Full control RXWDPO 有Change的权限，另外用户可以更改权限和获取目录的所有权权限级别 RXWDPO 允许的用户操作NoAccess 用户不能访问该文件Read RX 用户可以读取该文件，如果是应用程序可以运行Change RXWD 有Read的权限，还可以修改和删除文件Full control RXWDPO 包含Change的权限，还可以更改权限和获取文件的所有权表3.12 目录权限3.1 操作系统安全共享权限建立了通过网络对共享目录访问的最高级别。下表列出从最大限制到最小限制的共享权限。权限级别 允许的用户操作NoAccess 禁止对目录和其中的文件及子目录进行访问但允许查看文件名和子目录名，改变共享Read 目录的子目录，还允许查看文件的数据和运行应用程序Change具有Read权限中允许的操作，另外允许往目录中添加文件和子目录，修改数据，删除文件和子目录Full control 有Change权限中允许的操作，另外允许更改权限和获取所有权（只适用于NTFS卷）表3.14 共享权限3.1 操作系统安全（4）日志与审计Windows有三种类型的事件日志：① 系统日志。跟踪各种各样的系统事件，比如跟踪系统启动过程中的事件或者硬件和控制器的故障。② 应用程序日志。跟踪应用程序关联的事件，比如应用程序产生的象装载DLL（动态链接库）失败的信息将出现在日志中。③ 安全日志。跟踪事件如登录上网、下网、改变访问权限以及系统启动和关闭。注意：安全日志的默认状态是关闭的。1）修改日志文件存放目录Windows日志文件默认路径是“%SYSTEMROOT%\system32\config”，LOG 文 件 在 注 册 表 的 位 置 是 ：“ HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Eventlog”，可以通过修改注册表来改变它的存储目录，来增强对日志的保护。点击“开始”→“运行”，在对话框中输入“Regedit”，回车后弹出注册表编辑器 ， 依 次 展 开“ HKEY\_LOCAL\_MACHINE/SYSTEM/CurrentControlSet/Services/Eventlog”后，下面的Application、Security、System几个子项分别对应应用程序日志、安全日志、系统日志。3.1 操作系统安全2）设置文件访问权限修改了日志文件的存放目录后，日志还是可以被清空的，下面通过修改日志文件访问权限，防止这种事情发生，前提是Windows系统要采用NTFS文件系统格式。右键点击D盘的CCE目录，选择“属性”，切换到“安全”标签页后，首先取消“允许将来自父系的可继承权限传播给该对象”选项勾选。接着在账号列表框中选中“Everyone”账号，只给它赋予“读取”权限；然后点击“添加”按钮，将“System”账号添加到账号列表框中，赋予除“完全控制”和“修改”以外的所有权限，最后点击“确定”按钮。这样当用户清除Windows日志时，就会弹出错误对话框。（5）安全策略Windows的安全策略主要包括：密码策略、锁定策略、审核策略、用户权利指派、安全选项、装载自定义安全模板、软件限制策略等。下面分别讨论各种策略的使用方法。1）密码策略打开“控制面板”→“管理工具”→“本地安全策略”→“安全设置”→“账户策略”→“密码策略”。有两个选项值得注意：3.1 操作系统安全① 密码必须符合复杂性要求。为了避免通过字典攻击来破解SAM数据库，Windows提供了一种强大的密码过滤器以加强复杂密码策略。复杂密码必须至少有6个字符，不能包括用户名或用户全名，且必须包含大写字母、小写字母、阿拉伯数字、特殊字符和标点符号中的三种。② 密码最长存留期。在默认情况下密码有效期为42天。2）锁定策略为了防止网络黑客在网络上猜出用户的密码，可以在连续多次无效登录之后对用户账号实行锁定策略。打开“本地安全策略”→“安全设置”→“账户锁定策略”，查看选项：① 复位账户锁定计数器：将锁定阈值归零的时间间隔。② 账户锁定时间：账户从被锁定到解锁的时间间隔。③ 账户锁定阈值：在账户锁定之前，允许的无效登录的次数。3）审核策咯无论Unix还是Windows系统，审核策略都是网络安全的核心策略之一。在Windows系统中，任何涉及安全对象的活动都应该受到审核。3.1 操作系统安全打开“本地安全策略”→“安全设置”→“本地策略”→“审核策略”，可以看到能够被审核的事件有策略更改、登录事件、对象访问、过程追踪、目录服务访问（仅限于Windows的域控制器）、特权使用、系统事件、账户登录事件、账户管理等。其中“登录事件”与“账户登录事件”是不同的，前者记录网络登录和注销网络访问事件，而后者记录本地登录与注销事件。审核报告将被写入安全日志中，可以使用“事件查看器”来查看。安全日志SecEvent. Evt位于\Windows\System32\Config目录中。日志大小默认为512KB，如果需要修改日志的设置可右键单击“安全日志”对象并从弹出的菜单中选择“属性”，进行设置。4）用户权力指派在该安全策略中，安全组定义了从建立页面文件到登录服务器控制台的各种权力。用户和组通过被添加到相应的安全组而得到这些系统权限。5）安全选项安全选项包括了一些与安全性有关的独立的注册表项，这些项目与用户无关，它们只影响常规的系统操作。如果修改了安全选项策略，在命令行提示符下，运行“Secedit”→“RefreshpolicyMachine\_policy”命令则无需重新启动计算机，即可直接刷新策略。3.1 操作系统安全6）装载自定义安全模板除了系统定义的各种安全设置外，Windows还提供了“安全模板”来初始化系统安全配置。安全模板就是对整个系统安全属性的一个配置文件。系统管理员可以生成一个能够反映实际需要的安全模板，并把它应用于本地计算机或把它输入到活动目录的一个组策略对象。当新的模板被加入到一个组策略中后，所有受它影响的计算机都会接收模板的设置。模板文件是基于文本的文件。可从微软管理控制台的“安全模板”管理单元或通过使用“记事本”等文本编辑器来更改模板文件。安全模板文件中的某些部分（如[文件安全]和[注册表项]）包含特定的访问控制列表ACL。这些ACL是由安全描述符定义语言定义的文本字符串。（6）Windows加密文件系统Windows强大的加密系统能够给磁盘、文件夹、文件加上一层安全保护。加密文件系统提供一种核心文件加密技术，该技术用于在NTFS文件系统卷上存储已加密文件。一旦加密了文件或文件夹，你就可以象使用其它文件和文件夹一样使用它们。对加密该文件的用户，加密是透明的。这表明不必在使用前解密已加密的文件。你可以象平时那样打开和更改文件。但是，试图访问已加密文件或文件夹的入侵者将被禁止这些操作。如果入侵者试图打开、复制、移动或重新命名已加密文件或文件夹，将收到拒绝访问的消息。3.1 操作系统安全5．可信计算技术由防火墙、入侵监测和病毒防范为主要构成的传统信息安全系统，是以防外为重点；从组成信息系统的服务器、网络、终端三个层面上看, 把过多的注意力放在对服务器和网络设备的保护上，而忽略了对终端的保护。因此，导致当前普通计算机的资源可以较容易地被攻击程序占用，这些计算设备在用户认证、操作检查、访问控制、网络连接等方面设置的安全措施经常被攻击者绕过。只有从信息系统的硬件和软件的底层采取安全措施，从芯片、主板等硬件和BIOS、操作系统等底层软件综合采取措施，才能有效地提高其安全性。正是基于这一思想催生了可信计算的迅速发展。（1）可信计算的发展1）国外进展1983年美国国防部制定了世界上第一个《可信计算机系统评价准则》，准则中第一次提出可信计算机（trusted computer）和可信计算基（TCB，trusted computing base）的概念，并把TCB作为系统安全的基础。之后，美 国 国 防 部 又 相 继 推 出 了 可 信 网 络 解 释 （ TNI ， trusted networkinterpretation）和可信数据库解释（TDI，trusted database interpretation）。从而，形成了最早的一套可信计算技术文件。3.1 操作系统安全1999年10月，由几大IT巨头Compaq 、HP 、IBM 、Intel 和Microsoft 牵头组织了可信计算平台联盟（TCPA，Trusted Computing Platform Alliance)，成员达190 家。TCPA的成立，标志着可信计算高级阶段形成。2003年3月TCPA 改组为“可信计算组织”（TCG，Trusted Computing Group)，标志着可信计算技术和应用领域的进一步扩大。TCPA和TCG的出现形成了可信计算的新高潮。TCG是一个非盈利组织，旨在研究制定可信计算的工业标准。目前，TCG已经制定了一系列的可信计算技术规范，如可信PC、可信平台模块（TPM，Trusted Platform Module）、可信软件栈（TSS，TrustedSoftware Stack）、可信网络连接（TNC，Trusted Network Connection）、可信手机模块等规范，而且不断地对这些技术规范进行修改完善和版本升级。 TCG倡导的可信计算已逐步由理论逐步转化为产业，转入到实质性的实现阶段。3.1 操作系统安全2）国内进展2000年6月武汉瑞达公司和武汉大学合作，开始研制安全计算机。2004年10月在解放军密码管理委员会的支持下，在武汉大学召开了第一届中国可信计算与信息安全学术会议。2005年联想集团的“恒智”芯片和可信计算机相继研制成功。同年，兆日公司的TPM芯片研制成功。这些产品都相继通过国家密码管理委员会的鉴定和认可。2006年11月3日，可信计算密码专项组在国家密码管理局的支持下正式组建。22007年在国家信息安全标准委员会的主持下，我国开始制定一系列的可信计算标准，包括芯片、主板、软件、可信网络连接等标准。2008年中国可信计算联盟成立。2009年瑞达公司的“可信计算机密码模块安全芯片”通过国家密码管理局的认证，基于这一新芯片的可信计算机也推出上市。至此，中国的可信计算事业进入了蓬勃发展的阶段。我国的可信计算技术与产品得到了国际同行的高度评价，我国已经站在国际可信计算领域的前列。3.1 操作系统安全（2）可信计算概述1）可信的定义目前，关于可信尚未形成统一的定义，主要有以下几种说法。可信计算组织TCG用实体行为的预期性来定义可信：一个实体是可信的，如果它的行为总是以预期的方式，达到预期的目标。ISO/IEC 15408标准将可信定义为：参与计算的组件，操作或过程在任意的条件下是可预测的，并能够抵御病毒和物理干扰。所谓可信是指计算机系统所提供的服务是可以论证其是可信赖的。这就是指从用户角度看，计算机系统所提供的服务是可信赖的，而且这种可信赖是可论证的。我们给出自己的观点：可信≈安全+可靠。可信计算系统是能够提供系统的可靠性、可用性、信息和行为安全性的计算机系统。2）信任的属性信任是一种二元关系。它可以是一对一、一对多（个体对群体）、多对一（群体对个体）或多对多（群体对群体）的。3.1 操作系统安全信任具有二重性，既具有主观性又具有客观性。信任不一定具有对称性，即A信任B不一定就有B信任A。信任可度量，即信任的程度可划分等级。信任可传递，但不绝对，而且在传播过程中有损失。信任具有动态性，即信任与环境和时间因素相关。3）信任的获得方法信任的获得方法主要有直接和间接两种方法。设A和B以前有过交往，则A对B的可信度可以通常考察B以往的表现来确定。我们称这种通过直接交往得到的信任值为直接信任值。设A和B以前没有任何交往，这种情况下，A可以去询问一个与B比较熟悉的实体C来获得B的信任值，并且要求实体C与B有过直接的交往经验。我们称之为间接信任值，或者说是C向A的推荐信任值。有时还可能出现多级推荐的情况，这时便产生了信任链。4）信任根和信任链可信计算指一个可信的组件，操作或过程的行为在任意操作条件下是可预测的，并能很好地抵抗不良代码和一定的物理干扰造成的破坏。可信计算主要思路是在计算机硬件平台上引入安全芯片架构，通过提供的安全特性来提高终端系统的安全性。3.1 操作系统安全可信计算的基本思想是在计算机系统中首先构建一个信任根，再建立一条信任链，从信任根开始到硬件平台，到操作系统，再到应用，一级认证一级，一级信任一级，把这种信任扩展到整个计算机系统，从而确保整个计算机系统的可信。因此，信任根和信任链是可信计算平台的最主要的关键技术之一。信任根是系统可信的基点。TCG定义可信计算平台的信任根包括三个根：可信测量根（RTM，root of trust for measurement）、可信存储根（RTS，root of trust for measurement）和可信报告根（RTR，root of trust formeasurement）。其中可信测量根RTM是一个软件模块，可信存储根RTS由可信平台模块TPM芯片和存储根密码SRK组成，可信报告根PTR由可信平台模块TPM芯片和根密钥EK组成。信任链把信任关系从信任根扩展到整个计算机系统。在TCG的可信PC技术规范中，具体给出了可信PC中的信任链，如图3.11所示。可以看出：这个信任链以BIOS Boot Block和TPM芯片为信任根，经过BIOS→OSloader→OS。沿着这个信任链，一级测量认证一级，一级信任一级，以确保整个平台的系统资源的完整性。3.1 操作系统安全图3.11 TCG的信任链MeasuringHardwareTPMOption ROMs New OS component BIOS boot block Memory BIOS OS OS Loader Application NetworkReporting Storing Logging Root of trust in integrity reporting Root of trust in integrity measurement3.1 操作系统安全（3）可信平台模块可信平台模块TPM是可信计算平台的信任根，是可信计算的关键技术之一。近年来，国内外在可信平台模块TPM方面都有许多重要的研究和发展。1）TCG可信平台模块基本结构TPM通常具有密码运算能力和存储能力，内部拥有受保护的安全存储单元，是一个含有密码运算部件和存储部件的小型片上系统。TPM向操作系统、TSS等提供诸多安全方面的支持，通过TPM的功能支持，可信计算平台能够提供各种安全服务，它可作为密码运算引擎，用于对外提供加、解密的密码运算服务，可存储敏感数据。TPM由CPU、存储器、I/O、密码运算器、随机数产生器和嵌入式操作系统等部件组成，它本身就是一个小的计算机系统，一般是一种片上系统SOC（System on Chip），而且它应当是物理可信和管理可信的。优缺点TCG的TPM设计在总体上是很成功的，它体现了TCG以硬件芯片增强计算平台安全的基本思想，为可信计算平台提供了信任根。TPM以密码技术支持了TCG的可信度量、存储、报告功能，为用户提供确保平台系统资源完整性、数据安全存储和平台远程证明。3.1 操作系统安全但是TCG的TPM设计明显存在一些不足，其原因可能是主要考虑了低成本以及希望回避对称密码在产品出口方面的政策障碍，包括：采用LPC总线与系统连接，不适合大数据量通信；缺少芯片本身物理安全方面的设计；可信测量根RTM是一个软件模块，存储在TPM之外，容易遭受恶意攻击；在密码配置方面存在一些不足，比如密钥种类多、授权协议复杂、TPM内部缺少对称密码等；TPM的设计主要面向PC平台的，对于服务器和嵌入式移动运算平台并不完全适合。随着可信计算技术的发展与应用，特别是在了解了中国的可信密码模块TCM技术发展后，TCG也逐渐认识到在TPM设计方面存在的不足。于是，TCG开始制定TPM的新规范，并命名为TPM.next。2）中国可信平台模块2003年瑞达公司与武汉大学合作研制出我国第一个TPM芯片J2810，该芯片在CPU的工作状态划分（系统态和用户态）、存储器的分区隔离保护和I/O端口设置等方面有自己的创新特色。可信密码模块2006年在国家密码管理局的主持下，我国制定了《可信计算平台密码技术方案》和《可信计算密码支撑平台功能与接口规范》两个规范。3.1 操作系统安全2007年，中兴集成电路公司研制出第一个符合我国标准的可信密码模块（TCM，Trust Cryptography Module）。 TCM与TPM相比，在设计上充分考虑了TPM存在的不足，在芯片本身物理安全方面、密码配置方面等都有明显提升。如图3.13所示，可信密码模块包括密码计算区、受保护存储区和主计算区，提供了多种密码算法，特别的是使用了自主密码算法：SM2、SM3、SMS4、RNG，其目标是建立计算平台安全信任基。其核心功能包括：度量平台完整性，建立平台免疫力；为平台身份提供唯一性表示；提供硬件级密码学计算与密钥保护。中国的TPCM针对TCG的TPM所存在的一些不足，我国正在研究制定我国自己的可信平台控制模块（TPCM，Ttrusted Platform Control Module）。与TCG TPM基本结构的一些区别，主要表现在TPCM新增了输入输出桥接单元、修改了密码算法引擎并采用了自主密码算法等。3.1 操作系统安全（4）可信计算平台TCG首先提出可信计算平台的概念，而且具体化到可信PC、可信服务器、可信PDA和可信手机，并制定了相应的技术规范。我国也在制定相应的技术规范。目前，国内外的可信计算PC平台都已经产业化，并走向实际应用。根据我们的实际测评，国内外的可信计算平台在标准符合性方面虽然还存在一些问题，但是在不断提高。1）TCG可信平台TCG可信计算系统结构可划分为三个层次，分别为可信平台模块TPM、可信软件栈TSS和可信平台应用软件。可信平台模块TPM是可信计算平台的信任根，是可信计算平台的关键组件。TSS位于TPM和可信平台应用软件之间，主要功能为负责对可信平台应用软件提供可信计算支持，包括提供对TPM的访问和操作、安全认证、密码操作调用和资源管理等。3.1 操作系统安全2）我国可信平台我国可信计算平台的层次结构同TCG可信平台一致，也分为三个层次：可信密码模块TCM、TCM服务模块TSM和安全应用。中国可信平台与TCG可信平台最根本的差异，是所使用的可信平台模块不同。TCG使用了TPM，而中国的可信平台基于可信密码模块TCM为核心，从3个维度构建平台的安全功能体系，包括：构建信任链确保平台的完整性、通过身份密钥和数字签名实现平台身份可信、通过“密封”和“绑定”确保平台数据安全。（5）可信网络连接1）TCG可信网络连接TNC在设计过程中，既要考虑架构的安全性，又要考虑与现有标准和技术的兼容性，在一定程度上进行了折中考虑，因此，TNC既具有一定的优点，也具有一定的局限性。2）中国的可信网络连接研究我国学者在分析了TNC的优缺点之后，结合中国的实际情况，对TNC进行了一些改进，形成了自己的可信网络连接架构。3.1 操作系统安全我国的可信网络架构采用了一种三元、三层、对等、集中管理的结构。通过引入一个策略管理器作为可信第三方，对访问请求者和访问控制器进行集中管理，网络访问控制层和可信平台评估层执行基于策略管理器为可信第三方的三元对等鉴别协议，实现访问请求者和访问控制器之间的双向用户身份认证和双向平台可信性评估。该架构采用国家自主知识产权的鉴别协议，将访问请求者和访问控制器作为对等实体，以策略管理器为可信第三方，既简化了身份管理、策略管理和证书管理机制，也保证了终端与网络的双向认证，具有很大的创新性。3.2 数据库安全3.2.1 数据库安全基础1．数据库概念本质上来讲，数据库（DB, Database）就是信息的集合。准确的说，数据库是一个长期存储在计算机内的、有组织的、有共享的、统一管理的数据集合。它是一个按数据结构来存储和管理数据的计算机软件系统。数据库的概念实际包括两层意思：① 数据库是一个实体，它是能够合理保管数据的“仓库”，用户在该“仓库”中存放要管理的事务数据，“数据”和“库”两个概念结合成为数据库。② 数据库是数据管理的新方法和技术，它能更合适的组织数据、更方便的维护数据、更严密的控制数据和更有效的利用数据。如何地组织和存储数据库中的数据，如何有效地获取和维护这些数据。完成这个任务的程序（软件）叫数据库管理系统（DBMS, DatabaseManagement System）。DBMS是位于用户应用软件与操作系统之间的数据管理软件。3.2 数据库安全数据库系统（DBS, Database System）由计算机硬件系统、数据库、数据库管理系统、应用软件、包括用户在内的各类人员构成。数据库通常分为层次式数据库、网络式数据库和关系式数据库三种。而不同的数据库是按不同的数据结构来联系和组织的。自20世纪80年代以来，作为商品推出的数据库管理系统几乎都是关系型的，如Oracle、DB2、Informix、Visual FoxPro、Mysql、Sqlserver等。由关系数据结构组成的数据库系统被称为关系数据库系统。关系式数据结构把一些复杂的数据结构归结为简单的二元关系（即二维表格形式）。例如某单位的职工关系就是一个二元关系。在关系数据库模型中，数据库为一些相互之间存在一定关联的表格的集合。一个表格是由若干的行（记录）来构成。字段是记录的一部分。同一个数据表中的记录在结构上是相同的，但所记录的数据库并不完全相同，每一条记录必须是可以辨认的。也就是说，每个表中都存在一个关键字来分辨不同的记录，关键字的值必须是唯一的。关系数据库系统中的所有数据以表格的方式来描述，每一个数据表又可以称之为关系。每个数据表包括了一组固定的属性（列）定义以及所录入的一条条记录（行）。3.2 数据库安全2．结构化查询语言结构化查询语言简称SQL（Structured Query Language），是一种数据库查询和程序设计语言，用于存取数据以及查询、更新和管理关系数据库系统。结构化查询语言是高级的非过程化编程语言，允许用户在高层数据结构上工作。它不要求用户指定对数据的存放方法，也不需要用户了解具体的数据存放方式，所以具有完全不同底层结构的不同数据库系统可以使用相同的结构化查询语言语言作为数据输入与管理的接口。结构化查询语言语句可以嵌套，这使它具有极大的灵活性和强大的功能。（1）基本表与视图基本表（Base Table）是本身独立存在的表，即实际存储在数据库中的表。视图（View）是从一个或几个基本表或几个视图导出来的表。视图本身并不独立存储数据，系统只保存视图的定义。从用户的观点出发，基本表和视图都是关系，使用SQL访问它们的方式一样。3.2 数据库安全（2）定义基本表定义基本表就是创建一个基本表，对表名（关系名称）以及它所包括的各个属性名及其数据类型做出具体规定。命令格式：CREATE TABLE 表名 （字段名1 类型（宽度，小数），字段名2 类型（宽度，小数），┄┄）命令功能：用于建立一个基本表。（3）修改、删除基本表修改、删除基本表的基本命令是ALERT和DROP。（4）插入数据命令格式：INSERT INTO 表名 [（字段名1,字段名2）┄┄] VALUES (表达式1,表达式2┄┄)命令功能：按给定的字段值在数据库的末尾追加一条新记录。3.2 数据库安全（5）SQL查询 SELECTSQL的查询可以很方便地从一个或多个表中检索数据，查询是高度非过程化的，用户只需要明确提出“要干什么”，而不需要指出“怎么去干”。SQL基本查询模块的结构：SELECT <表达式1>,<表达式2>┄<表达式n>；—查询目标FROM <关系1>,<关系2>,┄<关系m>； —查询的源（所有关系的关系名）WHERE <条件表达式> —查询目标必须满足的条件（选择运算）（6）SQL数据操纵命令1）更新数据命令命令格式：UPDATE <表名>;SET <更新表达式>;[WHERE <条件>]2）删除数据命令命令格式：DELETE;FROM <表名>;WHERE <条件>3.2 数据库安全3．数据库安全概念数据库的一大特点是数据可以共享，然而，数据共享必然带来数据库的安全性问题。数据库系统中的数据共享不能是无条件的共享，比如军事秘密、国家机密、新产品实验数据、市场需求分析、市场营销策略、销售计划、客户档案、医疗档案、银行储蓄数据等。数据库的安全性是指保护数据库，防止因用户非法使用数据库造成数据泄露、更改或破坏。数据库系统的安全保护措施是否有效是数据库系统主要的性能指标之一。安全性问题不是数据库系统所独有的，所有计算机系统都有这个问题，如操作系统、网络系统等。（1）非法使用数据库的情况非法使用数据库的情况很多，大致分为如下三类：① 用户编写一段合法的程序绕过DBMS及其授权机制，通过操作系统直接存取、修改或备份数据库中的数据。② 直接或编写应用程序执行非授权操作。③ 通过多次合法查询数据库从中推导出一些保密数据。例：某数据库应用系统禁止查询单个人的工资，但允许查任意一组人的平均工资。用户甲想了解张三的工资，于是他：首先查询包括张三在内的一组人的平均工资；然后查用自己替换张三后这组人的平均工资；从而推导出张三的工资。3.2 数据库安全（2）传统的数据库运行环境传统的数据库运行环境通常采用“客户—服务器”模式。每个客户端建立一个与数据库服务器的连接，以便于通过数据库访问数据。在传统数据库运行环境中，数据安全主要体现在防止未经授权的数据泄露和数据修改。相应的安全策略包括：认证、授权和审计。（3）统计数据库安全统计数据库安全的目标是允许用户查询聚集类型的信息（例如合计、平均值等），但是不允许查询单个记录信息。如下SQL查询是合法的：SELECT count(\*) FROM Patients;WHERE age=42 and sex=‘M’ and diagnostic=‘schizophrenia’然而如下SQL查询是非法的：SELECT name FROM Patients;WHERE age=42 and sex=‘M’ and diagnostic=‘schizophrenia’（4）现代数据库运行环境与传统数据库运行环境的区别在于，为了减少数据库服务器的访问瓶颈等问题，现代应用软件多数采用多层体系结构，通过设置中间层完成对数据库访问的封装。 在一个多层应用环境中，中间层通常负责鉴别客户层应用（用户认证）以及管理与数据库交互（数据库会话管理）。3.2 数据库安全中间层将使用通用的用户名和密码与数据库连接并进行身份验证。数据库服务器则使用中间层的通用用户名和密码，依据应用上下文对终端用户的权限进行管理。（5）计算机系统中的安全模型实际上，安全性问题并不是数据库系统所独有的，所有计算机系统都存在这个问题。在计算机系统中，安全措施是一级一级层层设置的，安全控制模型如图3.21所示：用户 DBMS 操作系统 数据库标识和鉴定 存取权限控制 OS安全保护 密文存储图3.21 安全控制模型3.2 数据库安全根据图3.21的安全模型，当用户进入计算机系统时，系统首先根据输入的用户标识进行身份的鉴定，只有合法的用户才允许进入系统。对己进入系统的用户，DBMS还要进行存取控制，只允许用户进行合法的操作。DBMS是建立在操作系统之上的，安全的操作系统是数据库安全的前提。操作系统应能保证数据库中的数据必须由DBMS访问，而不允许用户越过DBMS，直接通过操作系统访问。数据最后可以通过密文的形式存储到数据库中。（6）数据库安全有关的基本概念用户：数据库中的行动者。数据库用户分为最终用户、管理员、开发员、分析和设计员。数据库对象：是SQL安全性保护能够施加的项，如数据库表与视图、存储过程与函数、数据库表与视图中的列、行等。权限：允许用户对一个给定数据库对象执行的动作，如表对象的CREATE、SELECT、INSERT、UPDATE、DELETE等操作权限。授权：规定用户可对某个数据库对象执行的动作（如读、写、执行等）。3.2 数据库安全4．数据库安全功能数据库安全性控制的常用方法包括：用户标识和鉴定、存取控制、审计、数据加密等，下面将详细阐述。（1）用户标识和鉴定数据库系统是不允许一个未经授权的用户对数据库进行操作的。用户标识和鉴定是系统提供的最外层的安全保护措施。其方法是由系统提供一定的方法让用户标识自己的名字或身份，系统内部记录着所有合法用户的标识，每次用户要求进入系统时，由系统进行核实，通过鉴定后才提供机器的使用权。用户标识和鉴定的方法有多种，为了获得更强的安全性，往往多种方法并用。常用的方法有以下几种：① 用一个用户或用户标识符来标明用户身份，系统以此来鉴别用户的合法性。如果用户名或用户标识正确，则可进入下一步的核实；否则，该用户不能使用计算机。3.2 数据库安全① 用户标识符是用户公开的标识，它不足以成为鉴别用户身份的凭证。为了进一步核实用户身份，常采用用户名与口令相结合的方法，系统通过核对口令判别用户身份的真伪。系统有一张用户口令表，为每个用户保存一个记录，包括用户名和口令两部分数据。用户先输入用户名，然后系统要求用户输入口令。为了保密，用户在终端上输入的口令不显示在屏幕上。系统核对口令以鉴别用户身份。通过用户名和口令来鉴定用户的方法简单易行，但该方法在使用时，由于用户名和口令的产生和使用较简单，也容易被窃取，因此还可采用更复杂的方法。例如每个用户都预先约定好一个过程或者函数，鉴别用户身份时，系统提供一个随机数，用户根据自己预先约定的计算过程或者函数进行计算，系统根据计算结果辨别用户身份的合法性。举例：让用户记住一个表达式，如T=x+2y，系统告诉用户x=1, y=2，如果用户回答T=5，则证实了该用户的身份。当然，这是一个简单的例子，在实际使用的过程中，还可以设计复杂的表达式，以使安全性更好。系统每次提供不同的x、y值，其它人可能看到x、y值，但不能推算出确切的变换公式T。3.2 数据库安全（2）存取控制数据库安全性所关心的主要是DBMS的存取控制机制。数据库安全最重要的一点就是确保只授权给有资格的用户访问数据库的权限，同时令所有未被授权的人员无法接近数据，这主要通过数据库系统的存取控制机制实现。数据库系统提供了两种存取控制机制：自主存取控制方和强制存取控制，如下：① 在自主存取控制方法中，用户对于不同的数据库对象有不同的存取权限，不同的用户对同一对象也有不同的权限，而且用户还可将其拥有的存取权限转授给其它用户。因此，自主存取控制非常灵活。② 在强制存取控制中，每一个数据库对象被标以一定的密级，每一个用户也被授予某一个级别的许可证。对于任意一个对象，只有具有合法许可证的用户才可以存取。强制存取控制因此相对比较严格。1）自主存取控制方法用户权限是由两个要素组成的：数据库对象和操作类型。定义一个用户的存取权限就是要定义这个用户可以再哪些数据库对象上进行哪些类型的操作。在数据库系统中，定义存取权限称为授权。3.2 数据库安全在非关系系统中，用户只能对数据进行操作，存取控制的数据库对象也仅限于数据本身。关系数据库系统中存取控制的对象不仅有数据本身（基本表中的数据、属性列上的数据），还有数据库模式（包括数据库SCHEMA、基本表TABLE、视图VIEW和索引INDEX的创建）等。自主存取控制主要通过SQL的GRANT语句和REVOKE语句来实现。GRANT语句向用户授予权限，REVOKE语句收回授予的权限。① GRANT语句GRANT语句的一般格式为：GRANT <权限> [, <权限> ] …ON <对象类型> <对象名> [,<对象类型> <对象名> ] …TO <用户> [, <用户> ] …[ WITH GRANT OPTION ];其语义为：将对指定操作对象的指定操作权限授予指定的用户。发出该GRANT语句的可以是DBA，也可以是该数据库对象创建者（即属主Owner），也可以是已经拥有该权限的用户。接受权限的用户可以是一个或多个具体用户，也可以是PUBLIC，即全体用户。3.2 数据库安全如果指定了WITH GRANT OPTION子句，则获得某种权限的用户还可以把这种权限再授予其它的用户。如果没有指定WITH GRANT OPTION子句，则获得某种权限的用户只能使用该权限，不能传播该权限。例：把对Student表和Course表的全部操作权限授予用户U2和U3。GRANT ALL PRIVILEGESON TABLE Student, CourseTO U2, U3;② REVOKE语句授予的权限可以由DBA或其它授权者用REVOKE语句收回。REVOKE语句的一般格式为：REVOKE <权限> [, <权限> ] …ON <对象类型> <对象名> [,<对象类型> <对象名> ] …FROM <用户> [, <用户> ] …[ CASCADE | RESTRICT ];例：把用户U4修改学生学号的权限收回REVOKE UPDATE(Sno)ON TABLE StudentFROM U4;3.2 数据库安全③ 创建数据库模式的权限GRANT和REVOKE语句向用户授予或收回对数据的操作权限。对数据库模式的授权则由DBA在创建用户时实现。CREATE USER语句的一般格式如下：CREATE USER <username>[WITH] [ DBA | RESOURCE | CONNECT ];对CREATE USER语句说明如下：(a) 只有系统的超级用户才有权创建一个新的数据库用户。(b) 新创建的数据库用户有三种权限：DBA、RESOURCE、CONNECT。(c) CREATE USER命令中如果没有指定创建的新用户的权限，默认该用户拥有CONNECT权限。拥有CONNECT权限的用户不能创建新用户，不能创建模式，也不能创建基本表，只能登陆数据库。然后由DBA或其它用户授予他应有的权限，根据获得授权情况他可以对数据库对象进行权限范围内的操作。(d) 拥有RESOURCE权限的用户能创建基本表和视图，成为所创建对象的属主。但是不能创建模式，不能创建新的用户。数据库对象的属主可以使用GRANT语句把该对象上的存取权限授予其它用户。3.2 数据库安全(a) 拥有DBA权限的用户是系统中的超级用户，可以创建新的用户、创建模式、创建基本表和视图等；DBA拥有对所有数据库对象的存取权限，还可以把这些权限授予一般用户。④ 数据库角色数据库角色是被命名的一组与数据库操作相关的权限，角色是权限的集合。因此，可以为一组具有相同权限的用户创建一个角色，使用角色来管理数据库权限可以简化授权的过程。在SQL中首先用CREATE ROLE语句创建角色，然后用GRANT语句给角色授权。CREATE ROLE语句格式是：CREATE ROLE <角色名>将创建的角色授予其它的角色或用户的语句格式为：GRANT <角色1> [, <角色2> ] …TO <角色3> [, <用户1> ] …[ WITH ADMIN OPTION ];3.2 数据库安全对该语句说明如下：(a) 该语句把角色授予某用户，或授予另一个角色。这样，一个角色（例如角色3）所拥有的权限就是授予它的全部角色（例如角色1和角色2）所包含的权限的总和。(b) 授予者或者是角色的创建者，或者拥有在这个角色上的ADMINOPTION。(c) 如果指定了WITH ADMIN OPTION子句，则获得某种权限的角色或者用户还可以把这个权限再授予其它的角色。(d) 一个角色包含的权限包括直接授予这个角色的全部权限加上其它角色授予这个角色的全部权限。例：通过角色来实现将一组权限授予一个用户，步骤如下：首先，创建一个角色R1：CREATE ROLE R1;然后使用GRANT语句，使角色R1拥有Student表的SELECT、UPDATE、INSERT权限：GRANT SELECT, UPDATE, INSERTON TABLE StudentTO R1;3.2 数据库安全2）强制存取控制方法在强制存取控制MAC中，DBMS所管理的全部实体被分为主体和客体两大类。主体是系统中的活动实体，既包括DBMS所管理的实际用户，也包括代表用户的各进程。客体是系统中的被动实体，是受主体操纵的，包括文件、基本表、索引、视图等。对于主体和客体，DBMS为它们每个实例分配一个敏感度标记（Label）。敏感度标记被分为若干级别，例如绝密（TOP Secret）、机密（Secret）、可信（Confidential）、公开（Public）等。主体的敏感度标记称为许可证级别（Clearance Level），客体的敏感度标记称为密级（ClassificationLevel）。MAC机制就是通过对比主体的Label和客体的Label，最终确定主体是否能够存取客体。当某一用户（或某一主体）以标记Label注册入系统时，系统要求他对任何客体的存取必须遵循如下规则：① 仅当主体的许可证级别大于或等于客体的密级时，该主体才能读取相应的客体；② 仅当主体的许可证级别等于客体的密级时，该主体才能写相应的客体。可见，这两条规则禁止了拥有高许可证级别的主体更新低密级的数据对象，从而防止了敏感数据的泄漏。3.2 数据库安全强制存取控制MAC是对数据本身进行密级标记，无论数据如何复制，标记与数据是一个不可分的整体，只有符合密级标记要求的用户才可以操纵数据，从而提供了更高级别的安全性。（3）审计审计功能把用户对数据库的所有操作自动记录下来放入审计日志中。DBA可以利用审计跟踪的信息，重现导致数据库现有状况的一系列事件，找出非法存取数据的人、时间和内容等。审计通常是很费时间和空间的，所以DBMS往往都将其作为可选特征，允许DBA根据应用对安全性的要求，灵活打开或关闭审计功能。审计功能一般主要用于安全性要求较高的部门。审计一般可以分为用户级审计和系统级审计。用户级审计是任何用户都可设置的审计，主要是用户针对自己创建的数据库表或视图进行审计，记录所有用户对这些表或视图的一切成功和（或）不成功的访问要求以及各种类型的SQL操作。系统级审计只能由DBA设置，用以监测成功或失败的登陆请求、监测GRANT和REVOKE操作以及其它数据库级权限下的操作。3.2 数据库安全AUDIT语句用来设置审计功能，NOAUDIT语句取消审计功能。例：对修改SC表结构或修改SC表数据的操作进行审计AUDIT ALTER, UPDATEON SC;审计设置以及审计内容一般都存放在数据字典中。必须把审计开关打开（ 即 把 系 统 参 数 audit\_trail 设 为 true ） ， 才 可 以 在 系 统 表（SYS\_AUDITTRAIL）中查看审计信息。（4）数据加密前面介绍的几种数据库安全措施，都是防止从数据库系统窃取保密数据，不能防止通过不正常渠道非法访问数据。比如，偷取存储数据的磁盘，或在通信线路上窃取数据。为了防止这些窃密活动，比较好的办法是对数据加密。用密码体制来加密数据存储，由于存入时需加密、查询时需解密，会占用大量系统资源，降低了数据库的性能。因此数据加密功能通常允许用户自由选择，只对那些保密要求特别高的数据，如：财务数据、军事数据及国家机密等才值得采用此方法。3.2 数据库安全5．视图与数据保密性为不同的用户定义不同的视图，可以限制各个用户的访问范围。通过视图机制把要保密的数据对无权存取这些数据的用户隐藏起来，从而自动地对数据提供一定程度的安全保护。比如，如果限定USER1只能对计算机系的学生进行操作，一种方法是通过授权机制对USER1授权，另一种简单的方法就是定义一个“计算机系”的视图。但视图机制的安全保护功能太不精细，往往不能达到应用系统的要求，其主要功能在于提供了数据库的逻辑独立性。在实际应用中，通常将视图机制与授权机制结合起来使用，首先用视图机制屏蔽一部分保密数据，然后在视图上再进一步定义存取权限。例：建立计算机系学生的视图，把对该视图的SELECT权限授予王平，把该视图上的所有操作权限授予张明。3.2 数据库安全CREATE VIEW CS\_StudentASSELECT \*FROM StudentWHERE Sdept=’CS’;GRANT SELECTON CS\_StudentTO 王平;GRANT ALL PRIVILIGESON CS\_StudentTO 张明;3.2 数据库安全6．数据完整性数据库完整性就是确保数据库中的数据的一致性和正确性。数据库软件执行3种类型的完整性服务：语义完整性、参照完整性和实体完整性。语义完整性机制保证结构化规则和语义规则得到遵守。这些规则与以下因素有关：数据类型、逻辑值、唯一性约束以及可能负面影响到数据库结构的操作。如果所有外键参考现有的主键，则说明一个数据库具有参照完整性。应通过某种机制确保没有外键引用不存在的记录的主键，或者空值。实体完整性保证了元组由主键值唯一确定。为了保证实体完整性，每一个元组必须包含一个主键。数据库提供了约束、规则和默认、事务处理等功能以保证数据完整性。（1）约束设计表时需要识别列的有效值并决定如何强制实现列中数据的完整性。数据库提供多种强制数据完整性的机制，包括：PRIMARY KEY约束、FOREIGN KEY约束、UNIQUE约束、CHECK约束和NOT NULL。3.2 数据库安全6．数据完整性数据库完整性就是确保数据库中的数据的一致性和正确性。数据库软件执行3种类型的完整性服务：语义完整性、参照完整性和实体完整性。语义完整性机制保证结构化规则和语义规则得到遵守。这些规则与以下因素有关：数据类型、逻辑值、唯一性约束以及可能负面影响到数据库结构的操作。如果所有外键参考现有的主键，则说明一个数据库具有参照完整性。应通过某种机制确保没有外键引用不存在的记录的主键，或者空值。实体完整性保证了元组由主键值唯一确定。为了保证实体完整性，每一个元组必须包含一个主键。数据库提供了约束、规则和默认、事务处理等功能以保证数据完整性。（1）约束设计表时需要识别列的有效值并决定如何强制实现列中数据的完整性。数据库提供多种强制数据完整性的机制，包括：PRIMARY KEY约束、FOREIGN KEY约束、UNIQUE约束、CHECK约束和NOT NULL。3.2 数据库安全上述约束定义关于列中允许值的规则，是强制完整性的标准机制。使用约束优先于使用触发器、规则和默认值。查询优化器也使用约束定义生成高性能的查询执行计划。（2）默认值通过定义列的默认值或使用数据库的默认值对象绑定表的列，以确保在没有为某列指定数据时，来指定列的值。默认值可以是常量，也可以是表达式，还可以为NULL值。例如：将学生表的性别列设置默认值'女' 。默认值可以是任何取值为常量的对象。 （3）规则规则限制了可以存储在表中或者用户定义数据类型的值，它可以使用多种方式来完成对数据值的检验，可以使用函数返回验证信息，也可以使用关键字BETWEEN、LIKE和IN完成对输入数据的检查。（4）事务处理事务是单个的工作单元。如果某一事务成功，则在该事务中进行的所有数据更改均会提交，成为数据库中的永久组成部分。如果事务遇到错误且必须取消或回滚，则所有数据更改均被清除。3.2 数据库安全事务处理是一种机制，用来管理必须成批执行的SQL操作，以保证数据库不包含不完整的操作结果。利用事务处理，可以保证一组操作不会中途停止，它们或者作为整体执行，或者完全不执行，如果没有错误发生，整组语句提交给（写到）数据库。如果发生错误，则进行回退（撤销）以恢复数据库到某个已知且安全的状态。事务处理的术语① 事务（Transaction）指一组SQL语句；② 回退（Rollback）指撤销指定的SQL语句的过程；③ 提交（Commit）指将未存储的SQL语句结果写入数据库表；④ 保留点（Savepoint）指事务处理中设置的临时占位符，可以对它发布回退。可以回退的语句：事务管理用来管理INSERT、UPDATE和DELETE语句。不能回退SELECT语句，也不能回退CREATE语句和DROP语句。事务处理中可以使用这些语句，但是进行回退的时候，它们不撤销。保留点越多越好，因为保留点越多，就越能按照自己的意愿灵活地进行回退。每个事务均以 BEGIN TRANSACTION 语句显式开始，以 COMMIT 或ROLLBACK 语句显式结束。3.2 数据库安全3.2.3 数据库安全实践1．数据库威胁与防护（1）十大威胁企业的数据库体系结构会受到各种各样的威胁。对数据库结构威胁最严重的十种威胁包括：过度的特权滥用、合法的特权滥用、特权提升、平台漏洞、SQL注入、不健全的审计、拒绝服务攻击、数据库通信协议漏洞、不健全的认证、备份数据泄露。威胁1 过度的特权滥用当用户（或应用程序）被授予超出了其工作职能所需的数据库访问权限时，这些权限可能会被恶意滥用。例如，一个大学管理员在工作中只需要能够更改学生的联系信息，不过他可能会利用过高的数据库更新权限来更改分数。威胁2 合法的特权滥用用户还可能将合法的数据库权限用于未经授权的目的。假设一个恶意的医务人员拥有可以通过自定义Web应用程序查看单个患者病历的权限。通常情况下，该Web应用程序的结构限制用户只能查看单个患者的病史，即无法同时查看多个患者的病历并且不允许复制电子副本。3.2 数据库安全但是，恶意的医务人员可以通过使用其它客户端（如MSExcel）连接到数据库，来规避这些限制。通过使用MSExcel以及合法的登录凭据，该医务人员就可以检索和保存所有患者的病历。这种私自复制患者病历数据库的副本的做法不可能符合任何医疗组织的患者数据保护策略。要考虑两点风险。第一点是恶意的医务人员会将患者病历用于金钱交易。第二点可能更为常见，即员工由于疏忽将检索到的大量信息存储在自己的客户端计算机上，用于合法工作目的。一旦数据存在于终端计算机上，就可能成为特洛伊木马程序以及笔记本电脑盗窃等的攻击目标。威胁3 特权提升攻击者可以利用数据库平台软件的漏洞将普通用户的权限转换为管理员权限。漏洞可以在存储过程、内置函数、协议实现甚至是 SQL语句中找到。例如，一个金融机构的软件开发人员可以利用有漏洞的函数来获得数据库管理权限。使用管理权限，恶意的开发人员可以禁用审计机制、开设伪造的账户以及转账等。威胁4 平台漏洞底层操作系统中的漏洞和安装在数据库服务器上的其它服务中的漏洞可能导致未经授权的访问、数据破坏或拒绝服务。例如，“冲击波病毒”就是利用了Windows 2000的漏洞为拒绝服务攻击创造条件。3.2 数据库安全威胁5 SQL注入利用程序对用户输入数据的检查不足或程序自身对变量处理不当，把额外的SQL语句附加到中间层往后台数据库提交的语句中，轻则获得敏感信息，重则控制服务器。在SQL注入攻击中，入侵者通常将未经授权的数据库语句插入（或“注入”）到有漏洞的SQL数据信道中。通常情况下，攻击所针对的数据信道包括存储过程和Web应用程序输入参数。然后，这些注入的语句被传递到数据库中并在数据库中执行。使用SQL注入，攻击者可以不受限制地访问整个数据库。① 原因在应用程序中若有下列状况，则可能应用程序正暴露在SQL 注入的高风险情况下：⚫ 在应用程序中使用字符串联结方式组合SQL指令。⚫ 在应用程序连结数据库时使用权限过大的账户（例如很多开发人员都喜欢用sa（自带的最高权限的系统管理员账户）连接Microsoft SQLServer数据库）。⚫ 在数据库中开放了不必要但权力过大的功能⚫ 太过于信任用户所输入的数据，未限制输入的字符数，以及未对用户输入的数据做潜在指令的检查。3.2 数据库安全② 作用原理SQL命令对于传入的字符串参数是用单引号字符所包起来，但连续2个单引号字符，在SQL数据库中，则视为字符串中的一个单引号字符。SQL命令中，可以注入注解。连续2个减号字符——后的文字为注解，或“/\*”与“\*/”所包起来的文字为注解。因此，如果在组合SQL的命令字符串时，未针对单引号字符作取代处理的话，将导致该字符变量在填入命令字符串时，被恶意窜改原本的SQL语法的作用。③ 例子某个站点的登录验证的SQL查询代码为strSQL = "SELECT \* FROM users WHERE (name = '" + userName + "') and(pw = '"+ passWord +"');"恶意填入userName = "' OR '1'='1";与passWord = "' OR '1'='1";时，将导致原本的SQL字符串被填为3.2 数据库安全strSQL = "SELECT \* FROM users WHERE (name = '' OR '1'='1') and (pw ='' OR '1'='1');"也就是实际上运行的SQL命令会变成下面这样的strSQL = "SELECT \* FROM users;"因此达到无账号密码，亦可登录站点。所以SQL注入攻击被俗称为黑客的填空游戏。④ 危害可能造成的伤害包括：⚫ 数据表中的数据外泄，例如个人机密数据，账户数据，密码等。⚫ 数据结构被黑客探知，得以做进一步攻击（例如SELECT \* FROMsys.tables）。⚫ 数据库服务器被攻击，系统管理员账户被窜改（例如ALTER LOGIN saWITH PASSWORD='xxxxxx'）。⚫ 取得系统较高权限后，有可能得以在网页加入恶意链接。⚫ 经由数据库服务器提供的操作系统支持，让黑客得以修改或控制操作系统（例如xp\_cmdshell "net stop iisadmin"可停止服务器的IIS服务）。⚫ 破坏硬盘数据，瘫痪全系统（例如xp\_cmdshell "FORMAT C:"）。3.2 数据库安全⑤ 避免的方法⚫ 在设计应用程序时，完全使用参数化查询来设计数据访问功能。⚫ 在组合SQL字符串时，先针对所传入的参数作字符取代（将单引号字符取代为连续2个单引号字符）。⚫ 如果使用PHP开发网页程序的话，亦可打开PHP的魔术引号（Magicquote）功能（自动将所有的网页传入参数，将单引号字符取代为连续2个单引号字符）。⚫ 其它，使用其它更安全的方式连接SQL数据库。例如已修正过SQL注入问题的数据库连接组件，例如ASP.NET的SqlDataSource对象或是 LINQto SQL。⚫ 使用SQL防注入系统。威胁6 不健全的审计自动记录所有敏感的和/或异常的数据库事务应该是所有数据库部署基础的一部分。如果数据库审计策略不足，则组织将在很多级别上面临严重风险。3.2 数据库安全威胁7 拒绝服务拒绝服务是一个宽泛的攻击类别，在此攻击中正常用户对网络应用程序或数据的访问被拒绝。可以通过多种技巧为拒绝服务攻击创造条件，其中很多都与上文提到的漏洞有关。例如，可以利用数据库平台漏洞来制造拒绝服务攻击，从而使服务器崩溃。其它常见的拒绝服务攻击技巧包括数据破坏、网络泛洪和服务器资源过载（内存、CPU 等）。资源过载在数据库环境中尤为普遍。威胁8 数据库通信协议漏洞在所有数据库供应商的数据库通信协议中，发现了越来越多的安全漏洞。在两个最新的 IBMDB2 Fix Pack中，七个安全修复程序中有四个是针对协议漏洞1。同样地，最新的Oracle 季度补丁程序所修复的23个数据库漏洞中有11个与协议有关。针对这些漏洞的欺骗性活动包括未经授权的数据访问、数据破坏以及拒绝服务。例如，SQL Slammer2蠕虫就是利用了Microsoft SQL Server协议中的漏洞实施拒绝服务攻击。更糟糕的是，由于自身数据库审计机制不审计协议操作，所以在自身审计记录中不存在这些欺骗性活动的记录。3.2 数据库安全威胁9 不健全的认证薄弱的身份验证方案可以使攻击者窃取或以其它方法获得登录凭据，从而获取合法的数据库用户的身份。攻击者可以采取很多策略来获取凭据：① 暴力：攻击者不断地输入用户名/密码组合，直到找到可以登录的一组。暴力过程可能是靠猜测，也可能是系统地枚举可能的用户名/密码组合。通常，攻击者会使用自动化程序来加快暴力过程的速度。② 社会工程：在这个方案中，攻击者利用人天生容易相信别人的倾向来获取他人的信任，从而获得其登录凭据。例如，攻击者可能在电话中伪装成一名IT经理，以“系统维护”为由要求提供登录凭据。③ 直接窃取凭据：攻击者可能通过抄写即时贴上的内容或复制密码文件来窃取登录凭据。威胁10 备份数据暴露经常情况下，备份数据库存储介质对于攻击者是毫无防护措施的。因此，在若干起著名的安全破坏活动中，都是数据库备份磁带和硬盘被盗。防止备份数据暴露所有数据库备份都应加密。实际上，某些供应商已经建议在未来的DBMS产品中不应支持创建未加密的备份。3.2 数据库安全建议经常对联机的生产数据库信息进行加密，但是由于性能问题和密钥管理不善问题，这一加密方法通常是不现实的，并且一般被公认为是上文介绍的细化的权限控制的不理想的替代方法。（2）安全防护体系数据库的安全防护是多方位的，从部署数据库系统到运行期间，都需要围绕安全防护做完备的处理，才能确保数据库的安全性。一般来说，对于数据库的安全防护分为三个阶段：事前检查、事中监控和事后审计，如图3.23所示。事前检查是指采购及部署数据库阶段，对运行环境以及数据库本身安全特性进行检查，包括硬件环境与操作系统及数据库服务器的运行环境的安全检测、数据库漏洞检测两部分。事中监控是对数据库运行期间客户端与数据库交互行为的监控，包括身份认证、访问控制以及交互数据的检测等。事后审计是指对日志文件的审计，用于分析、跟踪发现问题。3.2 数据库安全硬件环境操作系统数据库服务器 数据文件 日志文件 配置文件应用服务器 应用程序运行环境安全检测数据库 漏洞检测 事前检查SQL 请求 返回结果 事中监控 访问监控 事后审计 日志文件图3.23 数据库安全防护体系3.2 数据库安全2．数据库安全特性检查数据库安全特性检查是对数据库的静态安全防护。静态安全防护是通过对数据库的各种安全特性配置进行扫描，从而发现其中的潜在安全风险。根据数据库安全体系结构及其安全机制、数据库安全特性检测的对象，认为数据库安全检测可分图3.24所示的三层实现。如图3.24所示，数据库安全检测具有三个不同的层次，按照检测的目的划分，由外及里，分别是：① 端口扫描：也称为服务发现，主要是对数据库的开放端口进行扫描，检查其中的安全缺陷，比如开放了多余的服务端口等。② 渗透测试：渗透测试是对数据库服务器进行黑盒式的安全检测，检测前不知道数据库内部的任何信息，完全根据对数据库外围的信息收集，来对数据库的安全进行测试，找到其中的安全隐患。渗透测试的对象主要是数据库的身份验证系统和服务监听系统。③ 内部安全检测：内部安全检测是深入数据库之内，对数据库内部的安全相关对象进行完整的扫描和检测，包括安全元数据、内部审计、安全配置检查、漏洞检测和版本补丁检测等。3.2 数据库安全图3.24 数据库安全特性检测三层模型数据库安全检测端口扫描（服务发现） 渗透测试 内部安全检测（安全元数 据、安全配置检查、漏洞检 查、版本补丁检测等） 数据库服务器数据库服务端口数据库服务以太网3.2 数据库安全按照上述的三层检测模型，能够对数据库安全进行较全面和完整的检测，发现其中的各种安全隐患和漏洞，为数据库管理员提供极具价值的信息，帮助其改进数据库的安全现状。（1）服务发现数据库都是通过开放一定的端口，来完成与客户端的通信和数据传输。对数据库的安全特性进行检测，绝大部分的检测内容都需要登录进入数据库内部进行。此外，数据库向外开放的端口，由于是通信和数据传输的唯一通道，因此也是安全入侵检测最好的实施点。鉴于以上原因，我们需要在检测前，对目标数据库的开放服务端口进行扫描和确定。1）发现数据库服务端口要发现目标数据库的开放服务端口，首先，我们无法借助任何的第三方数据库连接组件，因为这些连接组件本身就需要我们提供一个服务端口号。其次，我们的目标是发现并且确定目标机器上的数据库服务端口，不仅要发现一个可用的端口，而且要确认这个端口就是目标数据库的服务监听端口。发现一个端口是否可用，可以简单地ping这个端口，但是除此之外，还需要确认这个有效的端口是目标数据库的监听端口。3.2 数据库安全2）确认有效端口对端口进行确认的最好方法，就是发送有效的消息给端口，看端口是否能够返回带有特征值的数据包，根据这个特征值来断定端口是否是目标数据库的有效监听端口。因此，需要根据目标数据库的数据包格式，构造数据库通讯协议和监听端口直接通信。3）持续扫描对于目标IP范围内的服务器，应该提供持续扫描机制，使得可连续快速扫描一个IP范围、智能和自动化的确认端口。（2）渗透测试渗透测试是完全模拟黑客可能使用的攻击技术和漏洞发现技术，对目标系统的安全做深入的探测，发现系统最脆弱的环节。1）渗透测试原理渗透测试主要依据公共漏洞、已发现的安全漏洞及隐患漏洞，模拟入侵者的攻击方法对应用系统、服务器系统和网络设备进行非破坏性质的攻击性测试。3.2 数据库安全渗透测试利用各种安全扫描器对网站及相关服务器等设备进行非破坏性质的模拟入侵者攻击，目的是侵入系统并获取系统信息并将入侵的过程和细节总结编写成测试报告，由此确定存在的安全威胁，并能及时提醒安全管理员完善安全策略，降低安全风险。2）渗透测试方法人工渗透测试和工具扫描可以很好的互相补充。工具扫描具有很好的效率和速度，但是存在一定的误报率，不能发现高层次、复杂的安全问题；渗透测试对测试者的专业技能要求很高（渗透测试报告的价值直接依赖于测试者的专业技能），但是非常准确，可以发现逻辑性更强、更深层次的弱点。3）数据库渗透测试的主要内容针对数据库的渗透测试，主要包括以下三个方面：监听器安全特性分析、用户名和密码渗透、漏洞分析。① 监听器安全特性分析数据库的监听器通常是数据库对外通信的第一道大门，所有的初始化连接都是从监听器开始的。由于监听器具有十分重要的作用，因此对监听器的攻击和利用一直都是黑客专注的地方。3.2 数据库安全监听器本身具有许多与安全相关的特性，这些特性一旦被攻击者利用，就存在十分大的安全风险，此外在安全检测工具的服务发现功能中，也需要借助监听器的某些特性进行工作。监听器安全特性分析的主要目的是研究如何利用监听器得到监听器本身的一些安全信息，为安全检测工具提供信息基础。结合数据库监听器有关的协议分析，可以构造一些对监听器的命令数据包，然后根据监听器的返回消息，来确定监听器的这些安全参数。② 用户名和密码渗透用户名和密码是数据库安全检测中一项重要的检测内容。其中对数据库默认用户名和密码的检测、以及数据库中用户名和密码相同状况的检测，是最重要的两项检测手段，因为这关系到数据库的登录和验证安全。对默认用户名和密码的检测，采用的手段是连接尝试，这样做有一定的风险，可能会造成某些账户被锁定。但是在具体的检测环境中，可以根据实际情况予以进行。3.2 数据库安全对用户名和密码相同的检测，存在一些技术难点。在数据库中，通常用户名是以明文的方式存放的，但是密码却以哈希值的形式存储，因此知道密码的哈希值，也是不能够加以直接利用的，因为无法从哈希值还原到密码原文。但是如果我们能够知道所使用的哈希算法，我们就可以根据用户名和假定的和用户名相同的密码来构造这个哈希值，然后和数据库中的哈希值对比，如果相等，就说明用户名和密码是相同的。③ 漏洞分析在数据库内部，存在大量的内置函数和过程，这些函数和过程中，有的存在严重的安全漏洞，比如具有SQL注入缺陷和缓冲区溢出漏洞，这也是进行安全检测的对象所在。这些安全漏洞一个重要的特征就是，每个安全漏洞只存在于相应的某个具体版本，那么我们可以通过检测目标数据库的版本，然后根据版本所对应的漏洞，来确定某个漏洞是否存在。获取目标数据库的版本，可以通过查询数据库内部的一个版本表来进行。但是，在数据库安装上某个漏洞的安全补丁以后，某些时候数据库内部的版本表中的版本号不会随着更改，也就是说，根据版本号来判断某些安全漏洞，会存在误判的可能性。3.2 数据库安全（3）内部安全检测内部安全检测是深入数据库之内，对数据库内部的安全相关对象进行完整的扫描和检测，包括安全元数据、内部审计、安全配置检查、漏洞检测和版本补丁检测等等。（4）安全特性分析及检测工具数据库安全特性分析及其检测工具的开发在国外已经成为一个重要的研究方向，国内外成立了很多数据库安全漏洞和黑客网站，专门针对主流DBMS的脆弱性进行分析研究，大大促进了数据库安全技术的进步。从2006年1月开始，美国国家安全局资助斯丹福大学、Coverity和Symantec公司，用于查找开源项目中的缺陷，仅2006年就发现并修复了6000个漏洞，大约有700位开发人员注册以获得漏洞信息。我国在上世纪九十年代也开始关注可信 DBMS的研发，并取得可喜的成果。3.2 数据库安全3．数据库运行安全监控数据库安全特性检查只是检测数据库管理系统的安全配置是否存在安全隐患，但针对 SQL注入攻击、漏洞利用攻击、合法用户的非法使用等数据库内、外部的安全入侵需要通过对数据库用户活动的监控才能发现。数据库运行安全监控是对数据库的动态安全防护，动态数据库安全防护也称为数据库入侵检测防护。3.3 小结1. 操作系统安全内容小结操作系统是控制其它程序运行，管理系统资源并为用户提供操作界面的系统软件的集合。操作系统包括资源管理、用户接口、进程管理和内存管理等功能。操作系统的基本安全实现机制包括CPU模式和保护环、进程隔离和内存保护等。现代CPU通常运行在两种模式下：内核模式和用户模式。一般看来，操作系统运行在内核模式下，其它应用运行在用户模式下。Unix系统可分为三个层次：硬件层、内核层和用户层，关键系统组件包括内存管理系统、文件系统、进程间通信、进程调度系统和设备驱动程序。守护进程是脱离于终端并且在后台运行的进程。它是一个生存期较长的进程，通常独立于控制终端并且周期性地执行某种任务或等待处理某些发生的事件。Inetd是Unix最重要的网络服务进程，通过集中的配置文件inetd.conf来管理大多数入网连接，根据网络请求来调用相应的服务进程来处理连接请求，有助于降低系统负载。3.3 小结文件系统安全是Unix/Linux系统安全的核心。Unix文件系统安全基于i节点中三段关键信息：文件拥有者UID、文件所在分组GID和模式（文件的权限设置）。文件权限是Unix文件系统安全的关键，Unix使用权限模式位来表示一个文件的权限，提供了chmod等命令用于修改文件的权限。在Linux系统中，用户的关键信息被存放在系统的/etc/passwd文件中，可以使用系统命令passwd来更改系统中用户的口令，也可以通过一些账号管理工具来创建和维护用户账号。在Unix\Linux中, 主要的审计工具是 syslogd守护进程。通过配置这个后台进程程序，可以提供各种水平的系统审计和指定输出目录。Windows的设计融合了分层操作系统和客户/服务器（微内核）操作系统的特点。计算机的处理器支持两种模式：用户模式和内核模式。用户应用程序代码在用户模式下运行，操作系统代码在内核模式下运行。Windows的核心模式组件包括执行体、内核、硬件抽象层、设备驱动程序和图形引擎。基本的系统进程是系统运行的必备条件，只有这些进程处于活动状态，系 统 才 能 正 常 运 行 。 Windows 系 统 中 最 基 本 进 程 包 括 ： csrss.exe 、explorer.exe、lsass.exe、services.exe、smss.exe、svchost.exe、system idleprocess、spoolsv.exe和winlogon.exe。3.3 小结2. 数据库安全内容小结数据库是一个长期存储在计算机内的、有组织的、有共享的、统一管理的数据集合。数据库通常分为层次式数据库、网络式数据库和关系式数据库三种。自20世纪80年代以来，作为商品推出的数据库管理系统几乎都是关系型的。结构化查询语言是一种数据库查询和程序设计语言，用于存取数据以及查询、更新和管理关系数据库系统。数据库的安全性是指保护数据库，防止因用户非法使用数据库造成数据泄露、更改或破坏，数据库安全性控制的常用方法包括：用户标识和鉴定、存取控制、审计、数据加密等，此外，通过视图机制把要保密的数据对无权存取这些数据的用户隐藏起来，从而自动地对数据提供一定程度的安全保护。数据库完整性就是确保数据库中的数据的一致性和正确性，数据库提供了约束、规则和默认、事务处理等功能以保证数据完整性。3.3 小结企业的数据库体系结构会受到各种各样的威胁对数据库结构威胁最严重的十种威胁包括：过度的特权滥用、合法的特权滥用、特权提升、平台漏洞、SQL注入、不健全的审计、拒绝服务攻击、数据库通信协议漏洞、不健全的认证、备份数据泄露。数据库的安全防护是多方位的，一般来说，分为三个阶段：事前检查、事中监控和事后审计。数据库安全特性检查是对数据库的静态安全防护，安全检测具有三个不同的层次，包括端口扫描、渗透测试和内部安全检测。数据库运行安全监控是对数据库的动态安全防护，也称为数据库入侵检测防护，对数据库的安全防御主要是被集成在一般的入侵检测系统或者防火墙之中。习题1. CPU的两种模式是什么？如何切换模式？操作系统如何利用CPU模式和保护环来实现安全保护？2. 简述系统调用的实现。3. 进程管理如何实现的？4. 简述Unix系统的守护进程。5. Unix系统基于访问权限的文件保护是如何工作的？为了实现该策略，共需要多少个访问权限位？为什么？6. Unix系统passwd文件的作用是什么？如何删除一个用户？如何更改一个用户的口令？7. Unix/Linux系统中, 服务的启动方式和禁用方式是什么？8. 简述Unix系统的审计工具及其机制。9. 简述Windows操作系统的系统架构和关键系统组件。10. 简述Windows操作系统进程安全管理的方法。11. 简述Windows操作系统的启动过程。习题12. 某公司的一个部门需要设置一个Windows操作系统的共享文件夹，要求全公司都能读取该文件夹中的文件，但是不能对文件夹的内容进行任何修改，或向这个共享文件夹中添加新的文件或文件夹。只有本部门的成员才能具有对该文件夹内容进行修改的访问权限。为Everyone Group组设置该文件夹权限以实现这个目标的最好策略是什么？13. 什么是可信计算？其基本思想是什么？14. 简述TCG可信平台模块与中国可信密码模块的结构及优缺点。15. 什么是数据库的安全性？实现数据库安全性控制的常用方法和技术有哪些？16. 什么是数据库角色？如何利用数据库角色对用户授权？17. 什么是数据库审计？ 如何设置和取消审计功能？18. 视图机制有哪些优点？19. 数据库完整性约束条件可以分为哪几类？习题20. 设有如下两个关系模式：职工(职工号，名称，年龄，职务，工资，部门号)，其中职工号为主键。部门(部门号，名称，经理名，电话)，其中部门号为主键。试用SQL语言定义这两个关系模式，要求在模式中完成以下完整性约束条件的定义：(1) 定义每个模式的主键。(2) 定义参照完整性。(3) 定义职工年龄不得超过60岁21. 今有两个关系模式：职工（职工号，姓名，年龄，职务，工资，部门号）；部门（部门号，名称，经理名，地址，电话）。请用SQL的GRANT和REVOKE语句（加上视图机制），完成以下授权定义或存取控制功能。(1) 用户王明对两个表有SELECT权力。(2) 用户李勇对两个表有INSERT和DELETE 权力。习题(3) 用户刘星对职工表有SELECT权力，对工资字段具有更新权力。(4) 用户张新具有修改两个表的结构的权力。(5) 用户王明对两个表有的所有权力（读、写插、改、删除数据），并具有给其它用户授权的权力。(6) 用户杨兰具有从每个部门职工中SELECT最高工资，最低工资，平均工资的权力，她不能查看每个人的工资。22. 简述数据库安全防护的三个阶段。23. 试述数据库安全检测的三个层次及其内容。24. 说明事务处理中可以回退和不可以回退的语句各有哪些？25. 试述数据库中的访问控制机制。信息安全等级考试三级教材Nankai University刘哲理 13212115916第四章 网络安全网络安全一. 网络安全基础二. 网络安全威胁技术三. 网站安全防护技术4.1 网络安全基础TCP/IP协议架构网络协议4.1.1TCP/IP协议框架1.TCP/IP开放模型TCP/IP的体系结构中各层的功能如下：（1）物理和数据链路层（2）网络层（3）传输层（4）应用层4.1.1TCP/IP协议框架2.OSI/RM参考模型OSI/RM是国际标准化组织ISO（International Standard Organization）制定的标准化开放式计算机网络层次结构模型。和TCP/IP开发模型不同的是，OSI/RM参考模型定义了7个层次，从下到上依次是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。TCP/IP开放模型与OSI参考模型对比4.1.2 网络协议4.1.2.1 数据链路层协议4.1.2.2 网络层协议4.1.2.3 传输层协议4.1.2.4 应用层协议4.1.2.1 数据链路层协议1.ARP协议地址解析协议ARP（Address Resolution Protocol）能实现主机IP地址与MAC地址之间的映射。4.1.2.1数据链路层协议2. RARP协议RARP协议是用于MAC地址向IP地址转换的，与ARP的地址转换方向正好相反。4.1.2.2网络层协议1. IP协议IP协议是网络层的协议，它可实现跨越不同网络的主机间通信。（1）IP地址每台计算机或网络设备的网络接口都有一个IP地址。IP地址是一个32位的二进制数，为了方便记忆，也可将二进制数转换为点分十进制的IP地址。转换时，将32位IP地址每8位分成一组，每组的8位二进制数可用一个点分十进制数表示，并用小数点隔开。（2）IP地址分类IP地址共有5种类型，分别是A类、B类、C类、D类和E类，5类不同的IP地址格式如图413所示。 0 8 16 24 32 bits 类型A类B类C类D类E类网络号 0 主机号网络号 10 主机号网络号 110 主机号多播地址 1110保留使用 1111IP协议IP协议（3）其他IP地址一些用于企业内部网的IP地址，由于不会连接到互联网中，所以不会被互联网中的路由器转发，也不会和注册的IP地址发生冲突，这类IP地址称为私有IP地址。私有IP地址包括A、B和C三个类别的地址，其地址范围如下：A类：10.0.0.010.255.255.255 B类：172.16.0.0172.31.255.255C类：192.168.0.0192.168.255.255IP协议其他特殊的地址：网络地址：在A、B、C类地址中，主机号全为0的地址用来表示一个网络的本网络地址。直接广播地址：在A、B、C类地址中，主机号全为1的地址为直接广播地址。它用于表示特定网络的所有主机。受限广播地址：如果一个IP地址的32位全为1，即255.255.255.255，则这个地址表示当前网络的广播地址，不过这种数据包的广播只限于本地网络中。自环地址：IP地址为127.0.0.1，数据包将不会离开此设备，而是仍返回到软件中。（4）IP数据包格式在网络层中，IP数据包由头部和数据两部分组成，IPv4协议头部的格式、如图414所示。头部包括一个基本长度为20B的定长部分，和一个可选的变长选项部分，选项的最大长度为60B。图414 IPv4头部格式IP协议32 bits 版本 头部长度 服务类型 总长度 标识 标志 片偏移 寿命 协议 头部校验和 源IP地址 目的IP地址 选项（0或更多字节）4.1.2.2网络层协议2.ICMP协议在网络环境复杂的环境中，需要一套机制用于进行网络异常状态的监测和诊断。Internet控制报文协议（Internet Control Message Protocol，ICMP）的主要作用，是在TCP/IP网络中发送出错和控制消息，允许主机或网络设备报告差错或异常情况，从而提供了一个错误侦测与回馈机制。ICMP的功能主要包括差错报告和查询两种主要功能4.1.2.3传输层协议1.TCP协议TCP协议是应用广泛的一种面向连接的传输层协议，它提供了在复杂网络环境下的一种可靠的端到端传输功能。通过TCP协议传输数据之前，发送方主机和接收方主机首先要通过三次握手协商好数据传输机制，再建立起连接。当数据传输结束后，要断开此次连接。32 bits源端口 目的端口 序号确认号 TCP 头部长度 保留位 控制位URGACKPSHRSTSYNFIN 窗口大小校验和 紧急指针 选项（0或更多32位长的字） 数据（长度可变）（1）TCP数据包头部格式TCP协议TCP协议（2）TCP的三次握手发送SYN=1数据包, SEQ=XSYN/ACK=1, SEQ=Y,ACK=X＋1ACK=1, SEQ＝X＋1，ACK=Y+12.UDP协议UDP是一个无连接的传输层协议，源主机和目标主机不需要建立连接确认，就可以进行数据的封装和传输。UDP数据包格式较为简单，包括头部字段和数据字段两个部分，其中头部字段占8B，如图417所示。32 bits源端口 目的端口 UDP长度 UDP校验和 数据（长度可变）4.1.2.3传输层协议4.1.2.4 应用层协议1．HTTPHTTP（Hypertext Transfer Protocol）协议是超文本传输协议，它是Web服务的核心协议，在浏览器和Web服务器之间进行数据传输。它在传输层是基于TCP协议的，在80端口对外提供服务。4.1.2.4 应用层协议2．SMTP和POP3 SMTP（Simple Mail Transfer Protocol）协议是简单邮件传输协议，它的主要作用是将电子邮件发送到邮件服务器，属于电子邮件系统的重要协议。SMTP协议在传输层基于TCP协议，在25端口提供网络服务。POP3（Post Office Protocol 3）是邮局协议的第3个版本，定义了计算机连接到邮局服务器并下载电子邮局的规范。POP3可以使用户通过计算机从邮件服务器中下载邮件并存储在本地计算机中，同时可以删除保存在邮件服务器中的电子邮件。POP3协议是应用最广泛的邮件访问协议。4.1.2.4 应用层协议3.DNSDNS（Domain Name System）域名系统的主要功能，是将Internet中的域名转换成相应的IP地址。配置并支持DNS功能的服务器被称为DNS服务器。互联网中网络用户对Web服务器的访问，往往通过容易记忆的域名进行，而输入浏览器的域名地址，再通过计算机中的DNS客户端将域名转化为IP地址，从而使浏览器可以访问Web服务器的真实IP地址。4.2 网络安全威胁技术• 扫描技术• 网络嗅探• 网络协议欺骗• 诱骗式攻击• 软件漏洞攻击利用技术• 拒绝服务攻击• Web脚本攻击• 远程控制4.2.1扫描技术1. 互联网信息收集网络攻击者为了全面了解目标计算机的信息，事先通过多种手段收集其外围信息，以便为实施具体攻击寻找入手点。通过互联网进行信息收集在当前互联网非常发达的时代，成为一种必然和不可或缺的手段。4.2.1扫描技术2. IP地址扫描IP地址扫描主要在网络攻击的开始阶段，用于获取目标计算机及其外围网络使用的IP网段，以及对应网段中处于开机状态的计算机。4.2.1扫描技术3. 端口扫描一个开放的网络端口就是一条与计算机进行通信的虚拟信道，网络攻击者对网络端口的扫描可以得到目标计算机开放的网络服务程序，从而为后续的攻击确定好攻击的网络端口。端口扫描端口扫描的技术有多种，下面介绍常见的端口扫描技术。（1）TCP全连接扫描TCP全连接扫描方法是利用TCP的三次握手原理来探测目标主机的网络端口是否处于打开状态。源主机每次进行扫描时，都尝试与目标主机建立正常的TCP三次握手的全连接，如果能建立起三次握手，则说明三次握手所连接的目标主机的网络端口是打开的。端口扫描（2）TCP SYN扫描TCP SYN扫描也称为TCP的半连接扫描。它的原理是利用了TCP三次握手中的前两次握手，因为没有建立三次握手的全连接，只是利用了两次握手，所以称为半连接。首先，源主机向目标主机发送第一次握手的SYN数据包，如果远端目标主机的端口是开放的，目标主机则自动回应第二次握手的SYN和ACK标志位设为1的数据包。如果能收到目标主机返回的第二次握手的数据包，就可知目标主机的端口是开放的。端口扫描（3）TCP FIN扫描TCP FIN扫描是利用发送FIN标志位为1的数据包进行端口的扫描。首先，源主机向目标主机发送FIN标志位为1的数据包给目标主机，如果远端目标主机端口是开放的，则丢弃此包，不进行回应；如果远端目标主机端口是未开放，则返回一个RST标志位为1的数据包。端口扫描（4）UDP的ICMP端口不可达扫描这种扫描方法利用UDP协议向目标主机的UDP网络端口发送探测的数据包，由于UDP协议比TCP协议简单，所以打开的网络端口不会返回确认数据包，不过当源主机向目标主机的一个未打开UDP端口发送数据包时，目标主机会返回一个ICMP\_PORT\_UNREACHABLE错误，根据是否收到这个错误信息，就可以发现关闭的UDP端口。端口扫描（5）ICMP 扫描这种扫描方法利用ICMP协议的功能，向目标主机发送一个协议项存在错误的IP数据包，根据反馈的ICMP错误信息，判断目标主机使用的网络服务及使用的网络端口。端口扫描（6）乱序扫描和慢速扫描攻击者往往通过设置扫描软件，打乱扫描端口的顺序，并且降低端口的扫描速度，从而使端口扫描的数据包淹没在大量正常的网络数据包中，以隐藏端口扫描行为。端口扫描软件是黑客常用的工具，目前的扫描工具有很多种，例如Nmap、SuperScan、Netcat、Xport、PortScanner、Netscantools、Winscan等。4.2.1扫描技术4. 漏洞扫描漏洞扫描工具包括网络漏洞扫描工具和主机漏洞扫描工具。网络漏洞扫描工具主要通过网络扫描，针对网络设备的漏洞，以及对外提供网络服务的主机网络服务程序的漏洞进行检测。主机漏洞扫描工具主要针对本主机上安装的操作系统和应用软件系统的漏洞进行扫描，而不是进行网络的扫描。漏洞扫描（1）网络漏洞扫描网络漏洞扫描工具针对网络中的主机和网络设备，发送漏洞探测数据包进行漏洞的扫描。它主要利用模拟攻击技术扫描出具体的漏洞类型。网络漏洞扫描工具内部往往包含一个漏洞脚本库，漏洞脚本库中包含了大量漏洞的模拟攻击脚本或代码。漏洞扫描（2）主机漏洞扫描主机漏洞扫描工具扫描的原理是通过漏洞特征匹配技术和补丁安装信息的检测来进行操作系统和应用软件系统的漏洞检测。主机漏洞扫描工具对本机安装的操作系统和应用系统检测版本信息和补丁安装情况，根据自身数据库中保留的最新补丁信息进行比较，判定是否存在某些未打补丁的漏洞4.2.1扫描技术5.弱口令扫描目前很多主机和网络服务器都部署在网络中，需要通过用户名和口令才能进行远程登录。为了拿到相关服务器的用户名和口令，攻击者往往采用扫描技术来探测用户名和弱口令。对弱口令等登录信息的扫描，主要包括基于字典攻击的扫描技术和基于穷举攻击的扫描技术。（1）基于字典攻击的弱口令扫描技术基于字典攻击的弱口令扫描技术，需要事先构造常用口令的字典文件。常用口令的字典文件是用事先收集的常用来做口令的字符构造的文件。弱口令扫描（2）基于穷举攻击的弱口令扫描技术基于穷举攻击的弱口令扫描技术利用的是穷举的方法构造探测用的口令字典。其原理是把字母与数字进行组合，穷举出所有可能出现的组合，然后使用组合好的口令去进行口令扫描。4.2.1扫描技术6. 综合漏洞扫描综合漏洞扫描工具是一种自动检测系统和网络安全性弱点的工具，它集成了IP地址扫描、网络端口扫描、网漏洞扫描等多种扫描功能，使用者可以及时找出各系统的漏洞以及漏洞相关内容，不用每天关注各种系统发布的漏洞信息。网络攻击者利用综合漏洞扫描工具进行入侵的同时，对系统管理员来说，综合漏洞扫描工具是很好的管理帮手。4.2.1扫描技术7. 扫描的防范技术扫描往往是入侵的前奏，所以如何有效的保护计算机和网络，成为计算机安全维护和管理人员首要考虑的目标。从上面的介绍可知，众多扫描技术的原理都可以归纳为由源主机向目标主机发送各种扫描的数据包，并根据目标主机的反馈信息探测出其IP地址、网络端口、漏洞和弱口令等。4.2.2 网络嗅探1. 网络嗅探的原理网络嗅探技术是一种威胁性极大的非主动类信息获取攻击技术。对目标计算机的网络进行嗅探，可以通过Sniffer类的工具即网络嗅探器来完成。利用这种工具，可以监视网络的状态、数据流动情况以及网络上传输的信息。当信息以明文的形式在网络上传输时，便可以使用网络监听方式来进行数据包的嗅探和获取。将网络嗅探设备或网络嗅探主机的网络接口设置为监听模式，便可以将网上传输的信息截获。4.2.2 网络嗅探2. 网络嗅探的防范网络嗅探工具通过获取数据包中的明文数据来窃取敏感信息。为此，可通过使用对网络传输数据进行加密的软硬件工具或设备，实现对网络传输数据的加密，从而保护传输数据的安全性。4.2.3 网络协议欺骗1. IP地址欺骗IP地址欺骗是指网络攻击者伪冒第三方的IP地址，给目标主机发送包含伪造IP地址的数据包。由于TCP/IP协议中的IP协议缺乏对发送方的认证手段，因此，攻击者可以轻易构造虚假的IP地址，实时网络欺骗行为。4.2.3 网络协议欺骗2. ARP欺骗（1）ARP欺骗原理ARP欺骗的原理，就是恶意主机伪装并发送欺骗性的ARP数据包，致使其他主机收到欺骗性的ARP数据包后，更新其ARP缓存表，从而建立错误的IP与MAC地址的对应关系。ARP欺骗可以分为两种：一种是实施中间人欺骗，另一种是伪装成网关的欺骗。ARP 欺骗ARP的中间人欺骗攻击ARP的中间人欺骗攻击主要是在局域网环境内实施的。假设同一个局域网内有A、B、C三台计算机。它们的MAC地址分别为：A为MACA；B为MACB；C为MACC。A正常情况下与B进行直接的通信，而C想窃取A发给B的通信内容，为此C要通过实施中间人攻击实现上述目标。ARP 欺骗ARP的伪装网关欺骗攻击ARP病毒主机伪装成网关的欺骗攻击行为，主要是针对局域网内部主机与外网通信的情况。如果局域网内的主机C中了ARP病毒，C想截获A发出的消息内容，C就需要向A发送欺骗性的ARP包，声称网关的MAC地址改成C的MAC地址了，A将这个非正常的IP和MAC对应关系保存到本机的ARP缓存表后，后续A再给网关转发数据包时，查到的是对应的C的MAC地址，将数据包转发给了病毒主机C，为了不影响A主机正常连接外网，病毒主机C再将数据包转给真正的网关，最终也能实现A和外网的数据传输。ARP 欺骗（2）ARP欺骗的防范为了有效防范ARP欺骗，可以通过IDS、Antiarp或ARP防火墙等查找ARP欺骗的设备或工具检测网络内的ARP欺骗攻击，然后定位ARP病毒主机，再通过杀毒软件或手工分析清除ARP病毒。此外，还可以通过在局域网中进行MAC地址与IP地址的双向静态绑定，使ARP欺骗失效。4.2.3 网络协议欺骗3. TCP欺骗TCP欺骗是攻击者在伪造第三方IP的条件下，将伪造的数据加载到基于TCP协议传输的应用程序数据包中发送到目标主机，以实现使目标主机与第三方主机传输数据泄露或者造成数据被破坏。TCP欺骗攻击包括非盲攻击和盲攻击两种主要的欺骗手段。1）非盲攻击非盲攻击是在攻击者和目标主机在同一个网络时，可以通过网络嗅探工具获得目标主机的数据包，从而预测出TCP初始序列号的攻击方法。由于初始序列号可以通过网络嗅探获得，所以初始序列号的预测不是盲目的，因而得名。2.源IP=B，SYN 4.源IP=B，ACK 5.源IP=B，Z与A通信 ABZ 图426 CP非盲攻击流程TCP 欺骗3.SYN+ACK 1.用DoS攻击使B瘫痪TCP 欺骗2）盲攻击盲攻击发生在攻击者和目标主机不在同一个网络上的情况，由于两者不在同一个网络，所以攻击者无法使用网络嗅探工具捕获TCP数据包，因此无法获得目标主机的初始序列号，而只能预测或探测目标主机的初始序列号，因其存在盲目性，所以称为盲攻击。4.2.3 网络协议欺骗4. DNS欺骗DNS欺骗技术可分为基于DNS服务器的欺骗和基于用户计算机的欺骗。（1）基于DNS服务器的欺骗基于DNS服务器的欺骗技术欺骗的目标是DNS服务器。攻击者先向DNS服务器发送一个域名对应IP地址的查询请求，DNS服务器在没有此域名的条件下会向更高级别的DNS服务器上传查询请求。此时，攻击者可以伪造一个更高级别DNS服务器返回的DNS应答包给被他欺骗的DNS服务器，告知此DNS服务器要查询域名的IP地址，当有网络用户查询此域名时，就从缓存中找到这个虚假IP地址返回给用户，从而实现欺骗攻击。DNS 欺骗（2）基于用户计算机的DNS欺骗与基于DNS服务器的欺骗技术针对DNS服务器实施欺骗不同，基于用户计算机的DNS欺骗技术针对的是用户的计算机实施欺骗。4.2.4 诱骗式攻击诱骗式攻击是指通过伪造的或合成的具有较高迷惑性的信息，诱骗用户进行访问，从而诱发用户触发恶意代码，或者骗取被攻击者的敏感信息，达到攻击者入侵系统或获取敏感信息的目的。4.2.4 诱骗式攻击1.网站挂马（1）网站挂马的概念及原理网站挂马是指网站中的网页被攻击者恶意修改后，添加了可以触发并下载恶意程序的链接以及恶意代码和脚本，当用户访问这些网站时，如果自身计算机的Web浏览器及插件中存在安全漏洞，这些安全漏洞就会被网页中的恶意代码和脚本进行利用攻击，最终在用户不知情的情况下，使用户自动访问网页中的恶意链接甚至自动下载木马病毒。网站挂马（2）网站挂马技术目前，网站挂马的主要技术手段有以下几种：a）框架挂马b）.js脚本挂马c）body挂马d）伪装欺骗挂马网站挂马（3）网站挂马的防范对于Web服务器，需要做好服务器的安全维护，防止攻击者的入侵，才能从根本上防止网站挂马的发生。Web服务器的防护措施包括：第一，要查找Web服务器的漏洞。第二，严格限制Web服务器网站文件夹的访问权限。第三，网站维护人员可通过部署Web防火墙、入侵防御系统、网站防篡改设备等防护产品防止攻击者的攻击。第四，定期对网页进行主动安全检测。第五，做好网站的定期备份。4.2.4 诱骗式攻击2.诱骗下载（1）诱骗下载概念及原理诱骗下载是指攻击者将木马病毒与图片、FLASH动画、文本文件、应用软件等多种格式的文件进行捆绑，将捆绑后的文件配以迷惑性或欺骗性的文件名在网络中发布散播，然后诱使用户点击下载。诱骗下载（2）诱骗下载的主要方式针对攻击者重点关注的多媒体类文件、网络游戏、应用软件、电子书文件以及P2P种子软件等几种文件类型，诱骗下载主要通过下面的几种方式实施。a）多媒体类文件下载b）网络游戏软件和插件下载c）热门应用软件下载d）电子书爱好者e）P2P种子文件诱骗下载（3）文件捆绑技术文件捆绑技术是将两个或两个以上的文件捆绑在一起成为一个可执行文件，在执行这个捆绑后的文件时，捆绑在里面的文件都会被执行。捆绑在一起的文件可以是相同的文件格式，也可以是不同的文件格式。目前流行的捆绑技术和方式主要有多文件捆绑、资源融合捆绑和漏洞利用捆绑三种情况。诱骗下载（4）诱骗下载的防范为了有效防范诱骗下载，需要用户提高自己的安全防范意识，不访问非官方网站，不从不正规网站下载文件，网络游戏使用正规厂商的游戏服务器，选择文本格式的电子书下载，不开启P2P的种子文件下载功能，下载的文件要先进行杀毒，并且用户自身计算机要安装杀毒软件，并及时升级操作系统补丁。4.2.4 诱骗式攻击3.钓鱼网站（1）钓鱼网站概念与原理钓鱼网站是一种被黑客实施网络欺诈的伪造网站。为了窃取用户的信息，攻击者或黑客团体自己会构建一个伪造网站去仿冒真实的网站，伪造网站与真实网站具有相似的域名，其网页页面也几乎与真实网站一模一样，因此这些伪造的网站被称为钓鱼网站钓鱼网站（2）钓鱼网站的防范a. 访问相关网站时，详细检查网站相关域名信息b. 针对大型电子商务网站或网银站点通过数字证书鉴别真伪c. 查询网站的ICP网站备案信息d. 安装安全防护工具4.2.4 诱骗式攻击4.社会工程诱骗式攻击的深层本质就是对社会工程学的实际应用。社会工程学，是针对受害者自身的好奇心、贪婪、心理弱点、本能反应等特点，而采取的欺骗、陷阱、伤害等危害手段，以取得利益回报的学问。社会工程学更是一门艺术，为了实现欺骗的目的，需要有灵活精密的构思，天衣无缝的计划，机智迅速的应变。4.2.5 软件攻击漏洞技术1. 软件漏洞的概念与分类软件漏洞是指计算机系统中的软件在具体的实现、运行、机制、策略上存在的缺陷或者脆弱点。软件漏洞一旦被攻击利用，最严重的情况下就可以获得计算机系统的额外权限，使攻击者能够在未授权的情况下对计算机系统的安全造成损坏，从而影响计算机系统中正常服务的运行。软件漏洞的分类（1）操作系统服务程序漏洞操作系统服务程序漏洞是针对操作系统平台中各项提供系统服务功能的模块中存在的漏洞。（2）文件处理软件漏洞Windows操作系统下的文件处理软件提供了非常丰富的选择，这类软件数量众多使用人数广泛，所暴露出的漏洞也非常多，严重威胁着这类软件使用用户的计算机安全。（3）浏览器软件漏洞针对浏览器软件漏洞的发起的攻击往往通过网络进行，不过不是采用攻击者通常的主动网络攻击技术，而是采用诱骗式被动网络攻击技术，网站挂马就是针对浏览器漏洞的一种主要攻击利用手段。（4）其他软件漏洞4.2.5 软件攻击漏洞技术2.软件漏洞的攻击利用技术（1）直接网络攻击直接网络攻击是攻击者直接通过网络即可对目标系统发起主动攻击。针对对外提供开放网络服务的操作系统服务程序漏洞，可通过直接网络攻击方式发起攻击。（2）诱骗式网络攻击对于没有开放网络端口不提供对外服务的文件处理软件漏洞、浏览器软件漏洞和其他软件漏洞，攻击者无法直接通过网络发起攻击。由于这些软件的漏洞只能在本地执行才能触发漏洞，所以攻击者只能采用诱骗的方法，才能诱使用户执行漏洞利用代码。4.2.5 软件攻击漏洞技术3.软件漏洞攻击的防范a）安装使用新版本的操作系统和软件b）访问正规网站，软件和文件从官方网站和门户网站下载c）不随意点击通过电子邮件或即时通信软件发来的文件d）安装杀毒软件和主动防御软件。4.2.6 拒绝服务攻击1.拒绝服务攻击概念拒绝服务攻击是指攻击者向目标计算机发出数量众多的攻击数据包，消耗目标计算机大量的网络带宽和计算机资源，使得目标计算机没有剩余带宽和资源给正常用户的服务请求提供响应的一种攻击方式。4.2.6 拒绝服务攻击2.DoS攻击原理DoS是拒绝服务（Denial of Service）的缩写。DoS攻击的攻击对象是目标主机，攻击的目的是使目标主机的网络带宽和资源耗尽，使其无法提供正常对外服务。（1）DoS攻击的实现方式DoS攻击的目的是使目标主机无法提供对外服务，一般可以通过三种方式实现。• 利用目标主机自身存在的拒绝服务型漏洞进行攻击。• 耗尽目标主机CPU和内存等计算机资源的攻击• 耗尽目标主机网络带宽攻击。DoS攻击（2）DoS攻击的分类a）IP层协议的攻击b）TCP协议的攻击c）UDP协议的攻击d）应用层协议的攻击4.2.6 拒绝服务攻击3.DDoS攻击原理DDoS是分布式拒绝服务（Distributed DoS）攻击的简称，它是在DoS攻击技术的基础上，由攻击者通过非法控制大量的第三方计算机辅助其进行攻击的一种攻击方式，DDoS可简单理解为多对一的攻击。4.2.6 拒绝服务攻击4.DoS/DDoS攻击的防御措施（1）静态和动态的DDoS过滤器（2）反欺骗技术（3）异常识别（4）协议分析（5）速率限制4.2.7 Web脚本攻击本节根据OWASP Top 10中囊括的Web脚本攻击技术，重点介绍针对Web服务器的注入攻击，以及针对Web客户端的跨站脚本攻击和跨站请求伪造攻击。1.注入攻击（1）注入攻击的概念和原理注入漏洞的基本原理是Web程序对用户输入请求中包含的非法数据检查过滤不严，使Web程序将用户的异常输入字符当作正常代码执行，从而使用户在未授权的情况下非法获取Web服务器的信息。注入攻击（2）SQL注入的原理SQL注入攻击的原理，是攻击者通过构造一小段SQL代码片段作为请求参数提交给Web应用程序，从而使这段SQL代码得到后台数据库程序的解释执行，使攻击者实现查询操作后台数据库的攻击意图。注入攻击（3）SQL注入攻击的步骤第一步，首先需要判断Web网站是否可以进行SQL注入。第二步：寻找SQL注入点。第三步：利用注入漏洞查询后台数据库并获取或猜解用户名和密码第四步：寻找Web管理后台入口，通过用户名密码登录。第五步：实现对网站的成功入侵和修改。注入攻击（4）注入攻击的防范第一，使用预编译语句第二，使用存储过程来验证用户的输入。第三，在数据类型、长度、格式和范围等方面对用户输入进行过滤。第四，使用数据库自带的安全参数。第五，按照最小权限原则设置数据库的连接权限。4.2.7 Web脚本攻击2.跨站脚本攻击（1）跨站脚本攻击的概念和原理XSS攻击是利用网站程序对Web页面中输入的数据过滤不严或未作过滤的漏洞，攻击者往Web页面里插入恶意脚本代码，当用户浏览此页面时，该用户的浏览器就会自动加载并执行页面中插入的恶意脚本代码，从而实现在用户浏览器中显示攻击者的恶意脚本、控制用户浏览器，或者窃取用户资料的目的。跨站脚本攻击（2）跨站脚本攻击的分类• 反射型XSS。反射型XSS攻击一般是向用户发送带有恶意攻击脚本的一个URL连接，诱骗用户去点击，当用户点击URL时，URL链接中嵌入的恶意脚本被浏览器解析执行，从而达到攻击受害用户的目的。• 存储型XSS。攻击者将恶意数据非法存储在Web服务器端的页面中，当用户访问Web服务器的特定页面时，嵌入在页面中的恶意代码被浏览器解析执行，从而导致跨站脚本攻击发生。• DOMbased XSS。DOMbased XSS是基于文档对象模型（DOM）的跨站脚本攻击，攻击者通过JavaScript脚本动态修改DOM结构，进而导致XSS漏洞。跨站脚本攻击（3）XSS攻击的流程和危害对于反射型的XSS，一般是攻击者将含有XSS攻击脚本的URL提交到博客或论坛上，诱骗用户点击URL链接实施攻击。而对于存储型XSS，由于攻击者直接将XSS代码写入到服务器的网页中，在用户正常浏览时会受到XSS攻击。跨站脚本漏洞本质上是获取了在客户端浏览器执行脚本的权限，因此，攻击者可以在客户端实现任意脚本可以实现的功能。此外，利用XSS攻击还可以通过编写恶意脚本，在受害用户打开自己的Web邮件时，按照恶意脚本包含的功能实现非法邮件操作。跨站脚本攻击（4）XSS的防范在理解了XSS漏洞的原理后，对其进行分析研究的基础上，可从以下几个方面进行有效防范。第一，给关键Cookie植入Httponly标识。第二，进行输入检查。第三，进行输出检查。4.2.7 Web脚本攻击3.跨站点请求伪造（1）跨站点请求伪造攻击的概念及原理跨站点请求伪造攻击属于伪造客户端请求的一种攻击方式，全称是Cross Site Request Forgery，简写为CSRF。CSRF攻击是让用户访问攻击者构造的网页，执行网页中的恶意脚本，伪造用户自己的请求，对用户自己有登录权限的网站空间实施攻击。（2）CSRF攻击的流程（3）CSRF攻击的防范4.2.8 远程控制1.木马木马是恶意程序中的一种，它是具有远程控制、信息偷取、隐蔽传输功能的恶意程序，它通过诱骗的方式安装，并在用户的计算机中通过隐藏运行以实现长时间控制用户计算机的目的。（1）木马的特点伪装性、隐藏性、窃密性、破坏性木马（2）木马技术的演变第一代木马出现在二十世纪八十年代，其技术特点主要是在UNIX环境中通过命令行界面实现远程控制。第二代木马出现在二十世纪九十年代，具备伪装和远程控制的功能，具有非常好的图形控制界面，可以进行密码窃取、远程控制等。第三代木马为了突破防火墙的拦截，在连接方式上比第二代木马进行了改进，通过端口反弹技术，实现从内网到外网的连接，可以穿透硬件防火墙。第四代木马通过线程插入技术隐藏在系统进程或者应用进程中，实现木马运行时没有进程，网络连接也隐藏在系统进程或应用进程中。第五代木马普遍采用了rootkit技术，通过rootkit技术实现木马运行时进程、文件、服务、端口等的隐藏，采用系统管理工具难以发现它的踪迹。（3）木马的连接方式a）木马最初的网络连接方法第一代和第二代木马采用的都是最初的网络连接方法，即由木马的客户端程序主动连接服务端程序。b）木马的反弹端口技术木马木马（4）木马的隐藏技术a）线程插入技术线程插入技术就是利用了线程之间运行的相对独立性，把木马程序做为一个线程，插入其他应用程序的地址空间。b）DLL动态劫持技术DLL劫持技术是一种让程序加载非系统目录下DLL的技术。攻击者精心构造一个与原DLL文件同名DLL文件，并保存在应用程序的目录下，就有机会让应用程序去加载这个新DLL文件并且不影响应用程序正常的运行。c）RootKit技术RootKit是一种内核隐藏技术，它使得恶意程序可以逃避操作系统标准管理程序的查找。4.2.8 远程控制2.Webshellwebshell以asp、php、aspx、jsp等网页文件的形式存在，攻击者利用Web网站的漏洞将这些网页文件非法上传到网站服务器的web目录中，然后通过浏览器访问这些网页文件，利用网页文件的命令行执行环境，获得对网站服务器一定的远程操作权限，以达到控制网站服务器的目的。4.3网络安全防护技术4.3.1 防火墙防火墙的概念防火墙位于可信和不可信网络之间，通过设置一系列安全规则对两个网络之间的通信数据包进行访问控制，检测网络交换的信息，防止对重要信息资源的非法存取和访问，以达到保护内部可信网络的目的。4.3网络安全防护技术图为防火墙的网络拓扑图。防火墙一般部署在网络边界，以对可信的内部网络和不可信的internet外网进行过滤和阻断。防火墙 Internet 防火墙网页篡改及防护2.防火墙的功能• 防火墙在内外网之间进行数据过滤• 对网络传输和访问的数据进行记录和审计• 防范内外网之间的异常网络攻击• 通过配置NAT提高网络地址转换功能4.3网络安全防护技术防火墙在内外网之间进行数据过滤防火墙部署在内外网之间的网络边界，管理员通过配置防火墙的访问控制规则，过滤内外网之间交换的数据包，只有符合安全规则的数据才能穿过防火墙，保障内网网络环境的安全。4.3网络安全防护技术对网络传输和访问的数据进行记录和审计 内网和外网之间的数据交换和传输都需经过防火墙，防火墙可对这些数据记录下来并保存在日志中，以供日后分析审计。同时，防火墙也能提供网络使用情况的统计数据。4.3网络安全防护技术防范内外网之间的异常网络攻击 防火墙可对网络中传输的数据包进行监测，阻塞内外网之间的网络攻击和异常网络行为，可通过防火墙获取分析网络异常行为的具体信息。4.3网络安全防护技术通过配置NAT提高网络地址转换功能防火墙部署在网络边界，可以作为部署网络地址转换NAT（Network Address Translator）的设备，通过NAT防火墙可以用来缓解地址空间短缺的问题。4.3网络安全防护技术3.防火墙的分类根据防火墙的组成、部署环境和重点防护功能的差别，防火墙又分为不同的类别。4.3网络安全防护技术防火墙组成形式软件防火墙硬件防火墙4.3网络安全防护技术防火墙组成形式软件防火墙（功能差别）✓企业级软件防火墙✓个人主机防火墙硬件防火墙（硬件平台）✓X86架构的防火墙✓ASIC架构的防火墙✓NP架构的防火墙4.3网络安全防护技术软件防火墙和硬件防火墙相比，软件防火墙需要安装在操作系统上，操作系统的漏洞可能导致软件防火墙本身遭受攻击，其安全性低于硬件防火墙。此外，由于受操作系统的限制，软件防火墙的性能远远不如硬件防火墙，并且安装配置复杂繁琐。因此，软件防火墙的应用范围从企业级软件防火墙逐渐收缩到个人主机防火墙，实现对个人计算机的防护。硬件防火墙中由于X86架构的网络防火墙性价比较高，在中小企业得到普遍应用。而采用ASIC和NP等专用芯片级网络处理器的网络防火墙，由于处理能力强，主要用在电信运营商等对网络带宽有较高要求的高端用户中。4.3网络安全防护技术4防火墙技术包过滤技术NAT技术应用级网关技术状态检测技术4.3网络安全防护技术包过滤技术包过滤是防火墙最基本的过滤技术，它对内外网之间传输的数据包按照某些特征事先设置一系列的安全规则（或称安全策略）进行过滤或筛选。包过滤防火墙检查每一条规则直至发现数据包中的信息与某规则相符，则允许或拒绝这个数据包穿过防火墙进行传输。如果没有一条规则能符合，防火墙就会使用默认规则，一般情况下，默认规则就是要求防火墙丢弃该包。4.3网络安全防护技术安全规则是根据数据包中的信息进行设置的，包括：✓ IP源地址✓ IP目标地址✓ 协议类型（TCP包、UDP包和ICMP包）✓ TCP或UDP包的目的端口、源端口✓ ICMP消息类型✓ TCP选项：SYN、ACK、FIN、RST等；✓ TCP包的序列号、IP校验和等✓ 数据包流向：in或out；✓ …….4.3网络安全防护技术当网络应用较多时配置复杂，容易因配置不当而带来很多的问题。并且，包过滤技术主要在网络层和传输层进行过滤拦截，对网络更高协议层的信息无理解能力，不能阻止应用层的攻击，不支持对用户的连接认证。此外，包过滤技术也不能防止IP地址欺骗。4.3网络安全防护技术包过滤防火墙的规则有优先顺序，每个过滤的数据包都按照规则的前后顺序依次匹配，最后一条规则是防火墙的默认规则。包过滤技术只需要对每个数据包与相应的安全规则进行比较，实现较为简单，速度快，设备投资费用低，安全策略灵活多样，并且对用户透明，因而得到了非常广泛的应用。虽然这种技术实现效率高。4.3网络安全防护技术动态检测技术状态检测技术也称为动态包过滤技术，它不像包过滤防火墙仅靠设置静态的包过滤规则来进行数据包的过滤拦截，而是增加了对数据包连接状态变化的额外考虑。它在防火墙的核心部分建立数据的连接状态表，将在内外网间传输的数据包以会话角度进行检测，利用状态表跟踪每一个会话状态，记录有用的信息以帮助识别不同的会话。4.3网络安全防护技术和包过滤防火墙相比，状态检测防火墙动态记录连接的各个状态，可以在连接终止后及时阻断后续连接，防止伪造流量通过，可有效阻止更多伪造网络地址的DoS攻击，而且不用为了大量的正常访问请求而长久的开放大量的端口。4.3网络安全防护技术状态检查防火墙也有其自身的局限性。首先，当其处理无连接状态的UDP、ICMP等协议时，则无法提供动态的连接状态检查。并且，当处理FTP等存在建立两个TCP连接的协议时，针对FTP的被动模式，要在连接状态表中允许相关联的两个连接；而在FTP的标准模式下，FTP客户端在内网，服务器端在外网，由于FTP的数据连接是从外网服务器连到内网客户端的一个变化的端口，为此状态防火墙需要打开整个端口范围才能允许第二个连接通过。此外，针对连接量非常大的网络，状态检测防火墙对每一个会话的记录、分析工作占用资源较多，可能会造成网络连接的迟滞现象。4.3网络安全防护技术地址翻译NAT技术目前合法的IPv4地址已经远远不够使用，许多单位内部使用的都是私有网段的IP地址，无法直接与外界相连。NAT（Network Address Translation）即网络地址翻译技术，它能够将单位内网使用的内部IP地址翻译为合法的公网IP，使内网使用内部IP的计算机无需变动，也能够与外网连接。4.3网络安全防护技术NAT根据映射方式不同而分为三种类型：静态NAT(Static NAT)、NAT池(Pooled NAT)、端口地址转换PAT（Port Address Translation）。4.3网络安全防护技术静态NAT• 在内部的IP地址与公有IP地址间建立一一对应的静态映射关系，对用户来说，既可拥有自己的公有地址，方便地跟外部通信，又可不必直接与外部网络相连，得到防火墙的保护。4.3网络安全防护技术NAT池• 采用动态地址池分配，管理员可以事先定义好一组可用的公网IP地址，当用户需要对外访问时，防火墙系统将会从这一组可用的公网IP地址中，动态抽取一个没有使用的IP地址给用户，使用户得到合法的IP地址与外部访问。当用户完成访问时，系统将回收这个IP地址，将它分配给另外一个用户使用。4.3网络安全防护技术端口地址转换PAT• 采用端口地址转换，管理员只需要设定一个或多个可以用作端口地址转换的公网IP地址，用户的访问将会映射到公网IP地址的一个端口上去，这使每个合法公网IP地址通过65535个端口映射到六万多台内网主机。4.3网络安全防护技术应用级网关应用级网关即代理服务器，代理服务器通常运行在两个网络之间，它为内部网的客户提供HTTP、FTP等某些特定的Internet服务。代理服务器相对于内部网的客户来说是一台服务器，而对于外界的服务器来说，它又相当于此Internet服务器的一台客户机。4.3网络安全防护技术应用级网关工作流程:当代理服务区接收到内部网的客户对某Internet站点的访问请求后，首先会检查该请求是否符合事先制订的安全规则，如果规则允许，代理服务器会将此请求发送给Internet站点，从Internet站点反馈回的响应信息再由代理服务器转发给内部网的客户。代理服务器会将内部网的客户和Internet隔离，从Internet中只能看到该代理服务器而无法获知任何的内部客户的资源。4.3网络安全防护技术三者不同点代理服务器和防火墙的包过滤技术、NAT技术不同之处在于，对于内外网转发的数据包，代理服务器在应用层对这些数据进行安全规则过滤，而包过滤技术、NAT技术主要在网络层和传输层进行过滤。由于代理服务器在应用层对不同的应用服务进行过滤，所以可以对常用的高层应用协议做更细的控制，如FTP的GET、PUT请求，HTTP的GET、POST、HEAD请求以及URL链接地址等具体信息进行安全规则匹配，因此实现了更多对数据传输内容方面的安全保障。4.3网络安全防护技术应用级网关缺点由于应用级网关不允许用户直接访问网络，因而将使效率降低，而且应用级网关需要对每一个特定的Internet服务安装相应的代理服务软件，内部网的客户要安装此软件的客户端软件，而且并非所有的Internet应用服务都可以使用代理服务器。4.3网络安全防护技术5.防火墙的体系结构双重宿主主机体系结构屏蔽主机体系结构屏蔽子网体系结构的防火墙。4.3网络安全防护技术双重宿主主机体系结构双重宿主主机体系结构是围绕双重宿主主机构筑的。双重宿主主机是一种防火墙，这种双重宿主主机防火墙至少有两个网络接口，分别连接着内部网络和外部网络，它位于内部网络和外部网络之间，然而它阻止了内外网络之间的IP通信，禁止从一个网络将IP数据包发往另一网络。4.3网络安全防护技术双重宿主主机体系结构双重宿主主机是隔开内外网络的唯一屏障，一旦它被入侵，内部网络便向入侵者敞开大门，这是它的缺点。所以为了保证内部网络的安全，双重宿主主机应具有强大的身份认证系统，才能增强阻止外部非法登录的可能性。4.3网络安全防护技术双重宿主主机体系结构双重宿主主机防火墙外部网… …内部网络4.3网络安全防护技术屏蔽主机体系结构屏蔽主机体系结构中防火墙由一台包过滤路由器和一台堡垒主机组成。4.3网络安全防护技术屏蔽主机体系结构屏蔽主机防火墙强迫所有外部网络到内部网络的连接通过此包过滤路由器和堡垒主机，而不会直接连接到内部网络，这提供了更高的安全性，因为它实现了网络层传输层安全（包过滤）和应用层安全（代理服务器）。4.3网络安全防护技术屏蔽子网体系结构屏蔽子网体系结构防火墙由两个包过滤路由器和一个堡垒主机构成，它是最安全的防火墙体系结构，能支持网络层、传输层和应用层的防护功能。4.3网络安全防护技术屏蔽子网体系结构添加了额外的一层保护体系——周边网络。周边网络是一个防护层，由于介于外网和内网中间，如果把外网认为是危险军事区，内网认为是安全区，则周边网络就相当于介于二者之间的缓冲区，又被称为非军事区DMZ(Demilitarized Zone)。DMZ是一个不同于外网或内网的特殊网络区域，DMZ内通常放置堡垒主机和对外开放的应用服务器，比如Web、Mail、FTP等。4.3网络安全防护技术屏蔽子网体系结构内部路由器保护内部网络不受外部网络和周边网络的侵害，它只允许内部网络向外访问堡垒主机，即把内部网络出站的数据包路由到堡垒主机，再通过堡垒主机上的代理服务器访问外网，外部路由器在由DMZ向外网的方向只接收由堡垒主机向外网的主动连接请求。堡垒主机位于周边网络，是整个防御体系的核心。堡垒主机运行应用级网关，例如运行各种代理服务程序。堡垒主机是最容易受侵袭的机器，如果堡垒主机被入侵，由于有内部路由器的保护，使得入侵者不能直接入侵内部网络。4.3网络安全防护技术6.防火墙的安全策略防火墙一般部署在内外网的网络边界，对进出内网的数据包进行规则匹配和过滤。硬件防火墙至少有两个网络接口，分别连接内外网。此外，硬件防火墙一般都支持网络接口的扩展，可以支持对DMZ网络的安全防护。因此，防火墙除了连接内外网的网络接口外，往往将第三个网络接口所连接的网络做为DMZ区域，连接web服务器、mail服务器等提高对外服务。4.3网络安全防护技术6.防火墙的安全策略DMZLANinternet防火墙4.3网络安全防护技术基本的访问控制策略内网可以访问外网内网可以访问DMZ外网不能访问内网外网可以访问DMZDMZ不能访问内网DMZ可以访问外网4.3网络安全防护技术7.防火墙的配置天融信公司的百兆硬件防火墙防火墙 Internet 内网 交换机FTP服务器 192.132.48.99 Web服务器 192.132.48.98 Mail服务器 192.132.48.100路由器 180.40.38.254DMZ内网口:eth0 192.132.91.25 外网口:eth1 180.40.38.20DMZ口:eth2 192.132.48.974.3网络安全防护技术8.防火墙不能防范的安全威胁不能防范内网之间的恶意攻击不能防范绕过防火墙通道上的攻击不能防范病毒和内部驱动的木马不能防备针对防火墙开放端口的攻击4.3网络安全防护技术入侵检测系统的概念入侵检测系统（Intrusion Detection System简称为IDS）工作在计算机网络系统中的关键节点上，通过实时地收集和分析计算机网络或系统中的信息，来检查是否出现违反安全策略的行为和是否存在入侵的迹象，进而达到提示入侵、预防攻击的目的。4.3网络安全防护技术入侵检测系统的概念防火墙 Internet IDS控制台交换机IDS探测器 IDS探测器Web服务器 Mail服务器路由器DMZ内网计算机交换机4.3网络安全防护技术IDS包括控制台和探测器两部分，其中探测器是前端采集数据的网络设备，连接交换机的网络端口，实行对交换机中传输数据的分析。IDS探测器一般要部署在计算机网络系统中的关键子网，实现对关键网络中传输数据的安全检测。IDS的控制台可以通过网络接收IDS探测器上传的检测数据，从而对计算机网络系统中的异常入侵事件进行全面管理和控制。4.3网络安全防护技术2.入侵检测系统的功能检测并记录计算机系统或网络中存在的活动和数据；检测黑客在攻击前的探测行为，预先给管理员发出警报；检测网络中入侵行为以及网络异常行为，并提供告警和响应；提供有关攻击的信息，帮助管理员诊断网络中存在的安全弱点；4.3网络安全防护技术3.入侵检测系统的分类根据数据采集方式的分类基于网络的入侵检测系统（NIDS，Netword based IDS）基于主机的入侵检测系统（HIDS，Host based IDS）根据检测原理的分类误用检测(Misuse Detection)的IDS基于异常检测(Anomal Detection)的IDS4.3网络安全防护技术4.入侵检测技术误用检测技术误用检测技术是指利用已知系统和应用软件的弱点攻击模式建立相关特征库，来检测入侵。异常检测技术异常检测技术根据检测异常行为和正常用户行为之间的差别来检测入侵。其他入侵检测技术4.3网络安全防护技术4.入侵检测技术误用检测技术 a）专家系统 b）模型推理 c）状态转换分析异常检测技术其他入侵检测技术4.3网络安全防护技术4.入侵检测技术误用检测技术异常检测技术a）统计分析b）神经网络其他入侵检测技术4.3网络安全防护技术4.入侵检测技术误用检测技术异常检测技术其他入侵检测技术a）模式匹配b）文件完整性检验c）数据挖掘d）计算机免疫方法4.3网络安全防护技术5.入侵检测体系结构入侵检测系统最基本的形式，包括基于网络的入侵检测系统NIDS和基于主机的入侵检测系统HIDS。NIDS和HIDS的检测范围有限，而针对大型网络，入侵检测体系结构包括集中式结构、分布式结构。4.3网络安全防护技术5.入侵检测体系结构（1）NIDS和HIDS（2）集中式结构（3）分布式结构4.3网络安全防护技术6.入侵检测系统的部署NIDS总的来说包括探测器和控制台两大部分。探测器是专用的硬件设备，负责网络数据流的捕获、分析检测和报警等功能。控制台是管理探测器的工具，它负责接收探测器的检测日志数据，并提供数据查询和报告生成等功能，一个控制台可以管理多个探测器。控制台可以分层部署，级连控制台实现了控制台之间的数据传输，保证了经过下级控制台过滤的信息可以及时准确的传输到上级控制台。4.3网络安全防护技术7.入侵检测系统的配置绿盟的冰之眼NIDS设备防火墙 InternetIDS控制台 192.168.1.2交换机eth1:192.168.1.99路由器IDS探测器内网计算机4.3网络安全防护技术8.入侵检测系统的不足首先，入侵检测系统旁路在网络上，当它检测出黑客入侵攻击并且报警时，攻击行为已到达目标并造成损失，而IDS 无法有效阻断攻击，比如蠕虫爆发造成企业网络瘫痪，IDS能报警，但不能防范这个问题。其次，对于蠕虫病毒传播、DDoS 攻击、缓冲区溢出攻击等混合威胁越来越多，传播速度加快，留给人们响应的时间越来越短，使用户来不及对入侵做出响应，最终往往造成企业网络瘫痪，IDS虽然能检测出来，但就是和防火墙联手也无法把攻击防御在企业网络之外。 总之，入侵检测系统侧重于对网络行为的检测监控，注重安全审计，适合用其了解网络安全状态，但在防御网络攻击方面，不能提供有效的帮助。4.3网络安全防护技术9.入侵防御系统基于目前网络安全形势的严峻态势，现有主流的安全防范设备中，防火墙对应用层攻击难以防范，而入侵检测系统只能对网络行为进行检测，因此，同时具有在应用层进行防护功能以及入侵检测功能的入侵防御系统IPS（Intrusion Prevention System）作为新一代安全防护产品应运而生。4.3网络安全防护技术（1）入侵防御系统的功能a）拦截恶意流量b）实现对传输内容的深度检测和安全防护c）对网络流量监测的同时进行过滤4.3网络安全防护技术（2）入侵防御系统的部署防火墙 Internet IPS控制台交换机IPSWeb服务器路由器 内网服务器交换机IPS4.3网络安全防护技术（2）入侵防御系统的部署a）内外网的网络边界b）DMZ与防火墙的边界c）内网核心交换机和防火墙中间d）内网关键服务器的外侧4.3网络安全防护技术（3）入侵防御系统的不足a）可能造成单点故障b）可能造成性能瓶颈c）漏报和误报的影响4.3网络安全防护技术4.3.3 PKIPKI的概念和组成PKI（Public Key Infrastructure）是一个用公钥密码学技术来实施和提供安全服务的安全基础设施，它是创建、管理、存储、分布、和作废数字证书的一系列软件、硬件、人员、策略、和过程的集合。PKI的核心是要解决信息网络空间中的信任问题4.3网络安全防护技术一个典型的PKI系统应该包括如下组件：✓安全策略✓证书认证机构CACA（Certificate Authority）系统是PKI的核执行机构，是PKI的主要组成部分。它的作用主要包括：验证用户身份并颁发证书确保用于证书签名的非对称密钥的安全管理证书信息资料4.3网络安全防护技术一个典型的PKI系统应该包括如下组件：✓安全策略✓证书认证机构CA✓注册机构RA✓证书分发系统CDS✓基于PKI的应用接口网页篡改及防护2.数字证书数字证书就是CA对用户进行身份验证后，签发的用于标志用户身份信息的一系列数据，用来在网络通讯中识别通讯各方的真实身份，它具有对用户身份标识的唯一性。数字证书主要用于在Internet上解决"我是谁"的问题4.3网络安全防护技术基于数字证书的信任链传递关系：通过真实的数字证书，从而相信网络用户身份的真实性，是通过信任链的传递关系来保证的。4.3网络安全防护技术基于数字证书的信任链传递关系：CA颁发证书之前，要对申请证书者的身份进行确认，只有经过身份核实的才签发证书。并且，证书中含有CA的数字签名，如果证书中的信息被篡改，可以通过CA公钥验证出来。那么，在可以信任CA的条件下，CA又信任证书拥有者，所以给证书拥有者颁发了数字证书，如果能验证数字证书是真实的没有被篡改过，则通过这个信任链的传递关系，就可以通过真实的数字证书，确认并相信在数字证书中证书拥有者的身份。4.3网络安全防护技术基于数字证书的安全机制：数字证书中包含CA为用户采用公钥密码体制生成的公钥，以及CA对数字证书的数字签名。CA利用非对称密码算法生成专属于该用户的公私钥对，公钥按照X.509等标准格式封装在数字证书中，私钥通过保存在安全的物理介质中下发给用户。数字证书可用于：发送安全电子邮件、访问安全站点、网上证券、网上招标采购、网上签约、网上办公、网上缴费、网上税务等网上安全电子事务处理和安全电子交易活动。4.3网络安全防护技术数字证书的存储格式：证书的版本号证书序列号签名算法证书签发机构名证书有效期证书持有者用户名证书用户公钥信息签发者唯一标识符证书持有者唯一标识符签名值图4329 X.509格式的数字证书结构4.3网络安全防护技术3.证书认证机构CA证书认证机构CA（Certification Authority）是PKI的核心部分，作为权威的、可信赖的、公正的第三方机构，专门负责为各种认证需求提供数字证书服务。一个典型的CA系统包括如下几个组成部分：CA服务器、证书注册机构RA、目录服务器、证书下载中心、OCSP服务器、密钥管理中心KMC4.3网络安全防护技术CA的组成部分4.3网络安全防护技术CA系统的主要功能颁发证书颁发证书的流程是，首先用户到CA的注册机构RA或通过web网站等提交证书申请。接着RA等机构对用户的信息进行审核，审核用户的关键信息和证书请求中是否一致，更高级别的证书需要CA进行审核。审核通过后，由CA产生对应的公私钥对并生成数字证书。数字证书由RA为此用户签发证书，证书可以灌制到硬件的证书介质中，发放给用户；或者将证书发布到LDAP服务器上，由用户下载并安装证书。证书介质目前多采用IC卡或USB接口的USBKEY。4.3网络安全防护技术CA系统的主要功能颁发证书废除证书废除证书的过程是，用户到RA申请废除证书，CA审核用户的身份后，将证书吊销，并将吊销的证书加入到证书黑名单CRL（Certificate Revocation List）中，CRL中包含了所有未到期的已被废除的证书信息。CA会临时或者定期签发证书黑名单CRL，并将更新的CRL通过目录服务器在线发布，供用户查询和下载。4.3网络安全防护技术CA系统的主要功能颁发证书废除证书证书的更新当用户的私钥被泄漏或证书的有效期快到时，如果用户希望继续使用证书，这时用户可以申请更新证书，以废除原来的证书，产生新的密钥对和新的证书。证书更新的操作步骤与申请颁发证书的类似。4.3网络安全防护技术CA系统的主要功能颁发证书废除证书证书的更新证书验证证书的验证包括对证书的下列三部分信息作确认：✓验证有效性✓验证可用性✓验证真实性4.3网络安全防护技术CA系统的主要功能颁发证书废除证书证书的更新证书验证管理密钥CA系统提供了基于密钥的管理功能，包括密钥的产生、密钥的备份和恢复，以及密钥的更新等。在一个CA系统中，密钥的备份和恢复也是密钥管理中的重要一环。当用户密钥不慎丢失或者被破坏时，CA可以为用户及时恢复密钥。4.3网络安全防护技术CA的安全运行要求CA运行的安全性从物理安全、网络安全、密码安全等多方面都有较高要求。物理安全从物理安全上的要求，包括CA机房建筑必须防火、防水、防震、防电磁辐射、防物理破坏和外人侵入。网络安全由于CA的部分服务器要与互联网相连，所以CA系统在网络安全防护上也要采取严密的措施以防止病毒、非授权访问和恶意攻击。此外，为了确保提供不中断服务，系统必须采取高冗余度的配置，包括要求部署灾难备份中心。4.3网络安全防护技术CA的安全运行要求CA运行的安全性从物理安全、网络安全、密码安全等多方面都有较高要求。密码安全按照信息产业部《电子认证服务管理办法》的规定，CA的密码方案必须经过国家密码管理局的审批认证，CA信息系统必须通过国家信息安全产品的评测认证，取得国家认可的资质，才能投入运营。4.3网络安全防护技术4信任模式由于国内外不同行业不同地域往往建设了不同的CA系统，它们各自颁发的数字证书只在本系统内有效，而不同的PKI系统在实际工作中有实现相互信任传递的需要。为此，PKI系统的多级信任模式被提出，并为解决这个问题提供了多种可选的模型。4.3网络安全防护技术（1）单CA信任模型单CA信任模型是最基本的信任模型。这种模型中的PKI体系只有一个CA，PKI的所有终端用户都信任这个CA。每个证书链都起始于该CA的公钥，该CA的公钥成为PKI体系中唯一的信任锚。单CA信任模型适合应用于规模不大的机构，但是不适用于拥有大量用户或不同类型用户的机构或行业。4.3网络安全防护技术（2）层次信任模型层次信任模型主要适用于有严格的级别划分的大型组织机构和行业领域。根CA 政策CA 政策CA 政策CA 运营CA 运营CA 运营CA 运营CA 运营CA 运营CA4.3网络安全防护技术（3）桥CA信任模型桥CA 根CA二级CA 二级CA 根CA二级CA 二级CA根CA桥CA信任模型具有良好的适应性，可支持多种不同类型的CA系统相互传递信任关系，这也是目前这种模型在国内外应用较广泛的原因。4.3.4 VPN1.VPN的概念VPN是利用开放网络的物理链路和专用的安全协议，实现逻辑上网络安全连接的技术。它在现有网络物理链路基础上，采用了专有的安全隧道协议，实现了数据的加密、完整性检验和用户的身份认证，从而在开放网络中建立了一条数据安全传输的通道。2.VPN的网络连接类型按照主机和网络连接类型的不同，VPN总体上可分为ClientLAN和LANLAN两种连接类型。（1）ClientLAN类型的VPNClientLAN类型的VPN也称为Acess VPN，即远程访问型VPN。它提供了一种安全的远程访问手段。VPN客户机和VPN服务器的计算机都安装VPN软件，双方在通过开放网络建立起正常网络连接后，通过VPN软件之间的安全连接实现网络传输的安全保密性。VPN客户机 VPN服务器 开放网络VPN连接图4334 ClientAN类型VPN4.3.4 VPN2）LANLAN类型的VPNLANLAN类型的VPN也称为网络到网关类型的VPN，它可以在不同局域网络之间建立安全的数据传输通道。这种类型的VPN通常采用VPN协议建立加密传输数据的安全隧道进行数据传输。VPN网关 VPN网关 VPN隧道图4335 LANLAN类型的VPNVPN的网络连接类型4.3.4 VPN3.VPN协议的分类（1）第二层隧道协议第二层隧道协议，即链路层隧道协议。它首先把各种网络层协议(如IP协议)封装到数据链路层协议PPP的数据帧中，再把整个PPP帧装入到隧道协议中。由于隧道协议封装的是数据链路层的数据包，即OSI开放系统互连模型中第二层的数据包，所以称之为第二层隧道协议，如PPTP，L2F，L2TP，它主要应用于基于远程电话拨号的internet远程访问。（2）介于二、三层之间的隧道协议MPLS VPN是一种基于MPLS(Multiprotocol Label Switching, 多协议标记交换)技术的IPVPN，是在网络路由和交换设备上应用MPLS技术，简化核心路由器的路由选择方式，利用结合传统路由技术的标记交换实现的IP虚拟专用网络。VPN的协议分类（3）第三层隧道协议第三层隧道协议，即网络层的隧道协议。它把第三层即网络层的各种协议直接封装到隧道协议中进行传输，由于被封装的是第三层的网络协议，所以称为第三层隧道协议。第三层隧道协议主要包括IPSec和GRE等隧道协议。IPSec(IP Security)协议是IETF IPSec工作组制定的一套保护IP通信安全的协议簇，是一个应用广泛、开放的VPN安全协议体系。GRE（Generic Routing Encapsulation）通用路由封装协议是一种将任意类型的网络层数据包封装入另外任意一种网络层数据包的协议。VPN的网络连接类型（4）传输层的SSL VPN协议SSL VPN采用标准的安全套接层协议SSL对传输中的数据包进行加密，从而在应用层保护了数据的安全性。SSL会话由两部分组成：连接和应用会话。在连接阶段，客户端与服务器交换证书并协商安全参数，客户端利用服务器证书，可生成主密钥，对后续通信进行加密。在应用会话阶段，客户端与服务器间可安全传输各类信息，如网上银行卡号密码等敏感或机密数据。SSL协议工作在TCP/IP和应用层之间，为应用层的访问连接提供认证、加密和防篡改功能。4.IPSec VPN的配置图4336 本地安全策略界面 图4337 “IPSECNEW”安全策略的属性界面4.3.4 VPN图4338 本地安全策略界面中新增的“IPSECNEW”安全策略图4339 管理IP筛选器列表和筛选器操作配置界面图4340 配置IPSec VPN的源IP地址 图4341 配置IPSec VPN的目标IP地址IPSEC VPN的配置IPSEC VPN的配置图4342 配置IPSec VPN要加密的协议 图4343 IP筛选器列表中配置完成的一个筛选器图4344 “管理IP筛选器列表和筛选器操作”配置界面 图4345 “管理筛选器操作”配置界面 IPSEC VPN的配置图4346 筛选器操作常规选项配置界面 图4347 IP流量安全界面IPSEC VPN的配置图4348 自定义安全方法设置界面 图4349 “管理IP筛选器列表和筛选器操作”配置界面IPSEC VPN的配置图4350 选择配置IPSec VPN的隧道模式或传输模式 图4351 IP筛选器列表选项界面IPSEC VPN的配置图4352 筛选器操作选项界面 图4353 身份验证方法界面IPSEC VPN的配置图4354 新增加的一条IP安全规则 图4355 点击分配将“策略已指派”由“否”变为“是IPSEC VPN的配置4.3.5 网络安全协议1.网络层安全协议IPSecIPSec（Internet Protocol Security），是由互联网工程任务组IETF（Internet Engineering Task Force）提供的用于保障Internet安全通信的一系列规范，为私有信息通过公用网提供安全保障。IPSec协议是一组开放协议的总称，它包括网络安全协议和密钥协商协议两部分。其中，网络安全协议包括认证协议头AH（Authentication Header）协议和安全载荷封装ESP（Encapsulating Security Payload）协议；密钥协商协议包括互联网密钥交换协议IKE(Internet Key Exchange)等。IPSEC（1）ESP协议ESP协议为基于IPSec的数据通信提供了安全加密、身份认证和数据完整性鉴别三种安全保护机制。根据ESP封装的内容不同，可将ESP分为两种模式：传输模式和隧道模式。IPSEC（2）认证协议头AHAH为IP数据包提供了数据完整性检验、数据源身份验证等服务功能，但不提供数据的加密保护，因而它不能提供加密的数据传输功能。两个应用最普遍的AH实施数据完整性检验的标准是MD5和SHA1。IPSEC（3）密钥协商协议IKE协议负责两个IPSec对等体之间协商相关安全参数，包括协商协议参数、交换公共密钥、对双方进行认证，以及在交换安全参数后对密钥的管理。一个完整的IPSec隧道建立过程如下：第一步，IPSec的一端收到另一端的IPSec数据流后，将产生IKE会话。第二步，IPSec两端使用IKE的主模式或者主动模式协商，交换IKE SA，建立安全通道。第三步，IPSec两端使用IKE的快速模式协商，交换IPSec SA，建立IPSec安全通道。第四步，上述协商完成并建立IPSec安全通道后，传输的数据采用ESP或者AH协议进行封装后就可以在加密的通道上传输了。4.3.5 网络安全协议2.传输层安全协议SSLSSL是Secure Sockets Layer（安全套接层）的简写，它是由Netscape公司开发的，用来解决点到点数据安全传输和传输双方身份认证的网络安全传输协议。它解决了TCP/IP协议的安全防护问题，为传输层之上的应用层提供了加密、身份认证和完整性验证的保护。当用户访问某些网站时发现使用的是https协议，就是通过SSL协议将HTTP数据包进行了安全保护后，在浏览器与Web网站之间建立了一个安全的连接。SSL（1）SSL协议的构成SSL协议包括两层协议：记录协议和握手协议。握手协议的作用是建立安全连接，在客户和服务器传送应用层数据之前，负责完成诸如加密算法和会话密钥的协商，以及通信双方身份验证等功能。SSL记录协议位于SSL握手协议的下层，它定义了传输格式。上层数据包括SSL握手协议建立安全连接时所需传送的数据，都通过SSL记录协议往下层进行传送。SSL（2）SSL协议的连接过程4.3.5 网络安全协议3.应用层安全协议（1）Kerberos协议简介Kerberos协议主要用于在分布式网络环境中，实现用户和服务器之间的安全身份认证。Kerberos V5协议的简要步骤如下。第1步，Client向AS申请进行身份验证；第2步，AS验证Client的身份后，向Client发放通过身份验证的票据。第3步，Client向TGS申请Server的访问权限；第4步，TGS验证Client有AS提供的通过身份验证票据后，向Client发放可以访问Server的票据。第5步，Client将TGS发放的访问Server的票据，访问应用服务器Server。第6步，这一步是否使用是可选的，由Server验证完Client访问Server的票据后，提供访问权限。KerborsKerberos服务器 AS TGSClient Server(2) (3) (4)(5)(6)应用层安全协议（2）SSH协议SSH是英文Secure Shell的简写形式， 通过使用SSH可以把所有传输的数据进行加密。SSH的加密通信通过以下五个阶段来实现：第一阶段：协商SSH版本第二阶段：协商产生会话密钥第三阶段：登录认证第四阶段: 处理会话请求第五阶段: 交互会话应用层安全协议（3）SHTTP协议SHTTP协议（Secure Hyper Text Transfer Protocal）是安全超文本传输协议，它可支持多种加密协议并提供灵活的编程环境，可对信息作多种方式的安全封装，封装内容可有加密、签名和基于报文鉴别码MAC的认证等，用于加密和签名的算法还可由通信双方协商。（4）S/MIME协议S/MIME（Secure Multipurpose Internet Mail Extensions）是安全多用途网际邮件扩充协议。它提供了针对电子邮件的数字签名和数据加密功能，以弥补SMTP和POP3协议在安全功能方面的不足。S/MIME版本3的一个值得注意的增强功能是“三层包装”。三层包装的S/MIME邮件是指经过签名、加密、再次签名的邮件。这个额外的加密层为邮件提供了更高一层的安全性。应用层安全协议（5）SET协议SET（Secure Electronic Transaction）协议是在开放网络环境中的卡支付安全协议，它采用公钥密码体制和X.509电子证书标准，通过相应软件、电子证书、数字签名和加密技术能在电子交易环节上提供更大的信任度、更完整的交易信息、更高的安全性和更少受欺诈的可能性。4.4 小结网络安全基础网络安全威胁技术网络安全防护技术4.4 小结1.网络安全基础TCP/IP开放模型定义了异构网络互联的通信协议规范，适用于在不同异构网络中或者在同一个局域网中实现不同计算机间的数据通信。TCP/IP的体系结构包括四层，从下往上依次为物理和数据链路层、网际层、传输层和应用层。链路层包含了ARP和RARP等协议。网络层包含了IP协议和ICMP协议等协议。传输层包含TCP和UDP两种主要协议。应用层包含的协议较多，例如HTTP、SMTP、POP3、DNS等都属于常用网络协议。4.4 小结2.网络安全威胁技术网络协议欺骗是网络攻击者利用IP、TCP、ARP、DNS自身在安全机制上的缺陷，实施的网络欺骗行为。诱骗式攻击包括网站挂马、诱骗下载、网站钓鱼、社会工程等几种主流的方式。拒绝服务攻击从原理上分为针对协议漏洞的攻击、消耗主机资源的攻击和消耗网络带宽的攻击。从攻击层次和协议上分，包括TCP洪水攻击、UDP洪水攻击、ICMP洪水攻击和应用层的洪水攻击。Web客户端的攻击技术包括基于客户端的攻击技术和基于服务器端的攻击技术。跨站脚本攻击、跨站请求伪造攻击属于基于客户端的攻击技术，SQL注入攻击属于基于服务器端的攻击技术。4.4 小结3.网络安全防护技术网络的安全防护技术包括防火墙、IDS/IPS、VPN、PKI和众多安全协议。防火墙位于可信和不可信网络之间，通过检测和过滤网络交换的信息，达到保护内部可信网络的目的。防火墙的主要技术包括包过滤技术、状态检测技术、NAT技术、代理服务器技术等。从防火墙配置的体系结构来划分，主要包括双重宿主主机体系结构、屏蔽主机体系结构和屏蔽子网体系结构。为了检测异常入侵行为，IDS从网络数据包和主机状态信息中采集数据。根据数据采集方式的不同，IDS可以分为基于网络的入侵检测系统和基于主机的入侵检测系统。根据IDS检测入侵行为的方式和原理的不同，可以分为基于误用检测的IDS和基于异常检测的IDS 。VPN实现了身份认证、加密传输和数据完整性验证功能，从而保证了数据传输的安全性。按照封装协议的层次划分，VPN协议主要包括第二层隧道协议、第三层隧道协议、介于二、三层之间的隧道协议，以及传输层的隧道协议。PKI的核心是要解决网络中的信任问题，确定网络空间中用户身份的唯一性、真实性和合法性。PKI通过发布数字证书解决了网络中用户身份的信任问题。PKI系统能够为用户生成并颁发数字证书。证书认证机构CA是PKI的核心部分。IPSec协议提供了网络层及网络层以上协议的安全防护。SSL协议支持应用层协议的安全传输。Kerberos协议实现了分布式网络环境中的安全认证。习题简述TCP/IP协议架构的层次结构和各层包含的主要协议？简述ARP协议欺骗的原理？简述ICMP协议的功能？简述TCP协议的三次握手过程？说明TCP全连接扫描、TCP SYN扫描和TCP FIN扫描的原理和不同之处？简述网络漏洞扫描和主机漏洞扫描的区别？介绍基于DNS服务器的欺骗技术原理？说明网站挂马的概念及原理？说明DoS攻击的三种实现方式？介绍SYNFlood攻击的原理？介绍ACKFlood攻击的原理?介绍应用层脚本洪水攻击的原理？习题举例说明SQL注入的原理？举例说明跨站脚本攻击的原理？解释说明跨站点请求伪造攻击的概念及原理？解释说明木马的端口反弹技术？说明防火墙的NAT原理？说明防火墙的包过滤技术和动态检测技术的区别？说明IDS和IPS功能的区别？说明防火墙和IPS功能的区别？介绍PKI中基于数字证书的信任链传递关系原理？介绍SSL协议的连接过程？Q & A谢谢！第五章：应用安全应用安全5.1软件漏洞5.2软件安全开发5.3软件安全检测5.4软件安全保护5.5恶意程序5.6 Web应用系统安全5.7小结5.1软件漏洞5.1.1软件漏洞的概念和特点软件漏洞的概念及产生原因软件漏洞的特点5.1.2软件漏洞的分类软件漏洞的分类和危险等级的划分5.1.3漏洞库5.1.4常见的软件漏洞5.1.5软件漏洞利用及其防护技术5.1.6软件漏洞的发展趋势5.1.1软件漏洞的概念和特点漏洞也称为脆弱性(Vulnerability)，是计算机系统的硬件、软件、协议在系统设计、具体实现、系统配置或安全策略上存在的缺陷。这些缺陷一旦发现并被恶意利用，就会使攻击者在未授权的情况下访问或破坏系统，从而影响计算机系统的正常运行甚至造成安全损害。软件漏洞专指计算机系统中的软件系统漏洞。5.1.1软件漏洞的概念和特点软件漏洞的种类较多，产生的原因也非常复杂，大体上可包括软件设计开发运行阶段的疏漏、软件技术和代码规模的快速发展、软件安全测试技术的滞后等三个方面的原因5.1.1软件漏洞的概念和特点软件漏洞对软件的安全运行影响很大，它主要具有以下几个方面的特点。（1）软件漏洞危害性大（2）软件漏洞影响广泛（3）软件漏洞存在的长久性（4）软件漏洞的隐蔽性5.1.2软件漏洞的分类（1）按照软件漏洞被攻击者利用的地点进行分类① 本地利用漏洞② 远程利用漏洞（2）根据漏洞形成原因分类① 输入验证错误漏洞② 缓冲区溢出漏洞③ 设计错误漏洞④意外情况处置错误漏洞5.1.2软件漏洞的分类（2）根据漏洞形成原因分类① 访问验证错误漏洞② 配置错误漏洞③ 竞争条件漏洞④ 环境错误漏洞⑤ 外部数据被异常执行漏洞（3）根据漏洞生命周期不同阶段的分类① 0day漏洞② 1day漏洞③ 已公开漏洞5.1.2软件漏洞的分类（4）按照软件漏洞对系统安全的直接威胁后果分类 普通用户访问权限漏洞 本地管理员权限漏洞 远程管理员权限漏洞 权限提升漏洞 本地拒绝服务漏洞 …5.1.2软件漏洞的分类软件漏洞的危险等级划分软件漏洞的危险等级划分是根据软件漏洞在破坏性、危害性、严重性方面造成的潜在威胁程度，以及漏洞被利用的可能性，对各种软件漏洞进行分级。5.1.2软件漏洞的分类第一级：紧急这是危险级别最高的等级，紧急级别漏洞的利用可以导致网络蠕虫和病毒在用户不知情的情况下在网络上任意传播和繁殖，或者导致执行远程恶意代码。微软公司安全公告的第一级定义为“严重”。第二级：重要对重要级别漏洞进行利用，包括导致执行远程恶意代码，或者导致权限提升。微软公司安全公告的第二级也定义为“重要”。5.1.2软件漏洞的分类第三级：中危对于中危级别漏洞，由于默认配置、审核或难以利用因素的影响，中危级别漏洞的利用效果显著降低。微软公司安全公告的第三级定义为“中等”。第四级：低危低危级别漏洞的利用难度非常大，微软公司安全公告的第四级定义为“警告”。5.1.3漏洞库为了应对软件漏洞的威胁，许多国家建立了针对漏洞的应急响应机构，他们是软件漏洞数据的主要提供者或者漏洞库的主要维护者，并且提供了高风险的漏洞警报和专家建议。另外，还有许多不同的国家官方组织、规模较大的企业和专门从事IT安全领域研究的机构和企业5.1.3漏洞库CVEBugTraqNVDCNNVDCNVD其他漏洞库：EDB漏洞库、微软安全公告板和微软安全建议、绿盟科技的中文安全漏洞库、启明星辰的中文安全公告库5.1.4常见的软件漏洞1.常见缓冲区溢出漏洞常见缓冲区溢出有栈溢出、堆溢出和单字节溢出2.格式化字符串漏洞3.整数溢出漏洞根据溢出原理的不同，整数溢出可以分为以下三类：存储溢出、运算溢出、符号问题5.1.4常见的软件漏洞4.数组越界漏洞（1）读取恶意构造的输入数据（2）用输入数据计算数组访问索引（3）对数组进行读/写操作5.写污点值到污点地址漏洞6.内存地址对象破坏性调用漏洞1.漏洞利用的概念和shellcode的编写（1）漏洞利用的基本概念（2）shellcode的概念栈溢出攻击时输入数据的组成（3）shellcode的编写5.1.5软件漏洞利用及其防护技术随机填充数据NOPNOP……NOPNOPShellcode 新的返回地址5.1.5软件漏洞利用及其防护技术2.漏洞利用技术（1）静态shellcode地址的利用技术（2）动态变化的shellcode地址的利用技术（3）heap spray技术3.软件漏洞利用的防护技术Windows操作系统中提供的主要几种软件漏洞利用的防范技术：GS、DEP、ASLR、safeSEH、SEHOP…5.1.6软件漏洞的发展趋势软件漏洞及其漏洞攻击利用技术在近几年内的发展趋势体现在以下几个方面。第一，针对Web 应用的安全威胁越来越。第二，成熟商业软件的漏洞利用难度在增大。第三，信息化系统中的定制型软件应用系统的漏洞将逐渐增加。5.1.6软件漏洞的发展趋势软件漏洞及其漏洞攻击利用技术在近几年内的发展趋势体现在以下几个方面。第四，对已知漏洞的攻击利用仍然广泛存在。第五，对新兴计算机应用的漏洞攻击将成为未来攻击的重点，包括对云计算平台和云计算应用、移动互联网、物联网等。5.2软件安全开发5.2.1软件开发生命周期软件开发生命周期软件开发生命周期模型5.2.2软件安全开发建立安全威胁模型安全设计、安全编程、安全测试5.2.3软件安全开发生命周期5.2.1软件开发生命周期软件开发生命周期软件编码人员进行软件开发过程中，一般都会遵循相应的软件开发生命周期模型用于指导编码的整个过程。计算机软件产品从需求分析、设计、编码、测试、发布到维护，类似于经历一个生命的孕育、诞生、成长、成熟、衰亡的周期，一般称为软件开发生命周期。5.2.1软件开发生命周期一般的软件生命周期包含下面的六个阶段，问题定义、可行性分析、总体描述、系统设计、编码、调试和测试、验收与运行、维护升级到废弃等阶段5.2.1软件开发生命周期软件开发生命周期模型为了指导软件开发工作，在划分软件开发生命周期的基础上，进一步提出了一些软件开发全部过程、活动和任务的结构性指导框架，称为软件开发生命周期模型。软件开发生命周期模型包括瀑布模型、螺旋模型、迭代模型、快速原型模型等。5.2.1软件开发生命周期a)瀑布模型/改进的瀑布模型瀑布模型把软件开发的过程划分为需求>分析>设计>编码>测试等几个阶段进行，每一个阶段都明确定义了产出物和验证的准则。从而可以在每个阶段完成后组织相关的评审和验证，并且只有在前一个阶段的评审通过后才能够进入到下一个阶段。5.2.1软件开发生命周期b)螺旋模型螺旋模型总体上是遵从瀑布模型的，即总体上执行需求>架构>设计>开发>测试的路线，它将瀑布模型的多个阶段转化到多个迭代过程中,以减少项目的风险。每一次迭代都包含六个步骤:确定目标和替代方案，识别项目的风险，对技术方案进行评估，开发出本次迭代的交付物，并验证迭代产出的正确性，计划下一次迭代过程，提交下一次迭代的步骤和方案。5.2.1软件开发生命周期b)螺旋模型螺旋模型总体上是遵从瀑布模型的，即总体上执行需求>架构>设计>开发>测试的路线，它将瀑布模型的多个阶段转化到多个迭代过程中,以减少项目的风险。每一次迭代都包含六个步骤:确定目标和替代方案，识别项目的风险，对技术方案进行评估，开发出本次迭代的交付物，并验证迭代产出的正确性，计划下一次迭代过程，提交下一次迭代的步骤和方案。5.2.1软件开发生命周期c)迭代模型迭代式模型认为所有的软件开发阶段都可以包括多次迭代，每次迭代过程中要遵循需求>设计>开发的瀑布模型，每一次的迭代都会产生一个可以发布的产品，这个产品是最终产品的一个子集。5.2.1软件开发生命周期d)快速原型模型快速原型模型也称为敏捷开发，它是根据客户的需要在很短的时间内完成一个可以演示的软件产品，这个软件产品可以是只实现部分功能或者是最重要的功能，但是可以让用户直接看到一个直观的原型系统。5.2.2 软件安全开发软件安全开发技术主要包括以下四个方面： 建立安全威胁模型 安全设计 安全编程 安全测试5.2.2 软件安全开发建立安全威胁模型a)分析软件产品的安全环境b)分析软件产品可能遭受的威胁c)将所有威胁进行评估分析，并按照风险值进行排序，对风险较大的威胁要重点关注；d)考虑风险消减技术方案，应用于软件产品中，以缓解威胁；e)实施解决方案。5.2.2 软件安全开发g)代码重用性h)充分考虑软件运行环境i)选择安全的加密算法j)充分考虑不安全的条件k)失效防护a)最小权限原则b)开放设计原则c)全面防御原则d)权限分开原则e)最少公用原则f)心理接受性安全编程在软件设计初期，就需要按照以下安全设计的原则对软件的安全策略、安全环境、威胁解决方法进行全面考虑。5.2.2 软件安全开发安全测试一些通用的思路和方法：a)构造畸形数据包做测试b)对用户的输入进行全面检测c)验证输入输出的文件d)测试非正常的路径及其路径限制e)全面测试异常处理f )采用反汇编方式检测敏感信息5.2.3软件安全开发生命周期微软公司通过大量的开发实践，总结了一套完整的安全开发流程，将安全融入到了每个阶段，并且将安全的重视程度提高到了首要地位，它的实施为微软操作系统的安全性提供了保障。微软的软件安全开发生命周期模型共包括12个阶段5.2.3软件安全开发生命周期（1）第0阶段：准备阶段通过教育培训，培养开发团队员工的安全意识。（2）第1阶段：项目启动阶段在项目启动时，需要将项目涉及的安全问题都分析到位，以使软件产品更加安全可靠。（3）第2阶段：定义需要遵守的安全设计原则5.2.3软件安全开发生命周期安全设计的原则包括：简化原则，代码尽可能的简短精炼，则出错的几率就小；默认失效保护，对任何不符合条件的请求默认都拒绝。完全检查，对每一个访问受保护对象的行为都要进行检查公开原则，选取加密机制时尽可能选择经过公开验证过的密码算法；权限分离，不允许只经过单一条件就能通过验证的操作；最小特权，只给操作授予最小执行权限；5.2.3软件安全开发生命周期（4）第3阶段：产品风险评估在此阶段对所开发的产品进行风险评估，以确定开发的软件是否采用了有潜在风险的技术，或者是否有较大的隐私泄露危险性。（5）第4阶段：风险分析对于存在高风险的软件产品，有必要通过威胁建模开展深入的风险分析。（6）第5阶段：创建安全文档、安全配置工具在此阶段主要考虑的是为用户提供可操作的安全指南和安全配置工具。5.2.3软件安全开发生命周期（7）第6阶段：安全编码策略（8）第7阶段：安全测试策略安全测试不同于功能性测试，它可以协助开发团队发现可以被利用的高危漏洞。安全测试可以简单的理解为以攻击者的角度开展的测试，具体包括模糊测试（Fuzzing）、渗透测试、运行时验证测试、重新审核威胁模型、重新评估被攻击面。（9）第8阶段：开发团队自身进行的全面安全分析检测完成所有代码与功能开发后的一个阶段。5.2.3软件安全开发生命周期（10）第9阶段：最终安全评审在产品解决完成时，需要做一次最终的安全评审，以检查是否做好了提交给客户的准备。只有安全团队可以对软件产品进行最终评审。（11）第10阶段：组建安全响应团队制定安全响应计划（12）第11阶段：产品发布（13）第12阶段：安全响应执行5.3软件安全检测5.3.1软件静态安全检测技术软件源代码的静态安全检测技术可执行代码的静态安全检测技术5.3.2软件动态安全检测技术模糊测试智能模糊测试动态污点分析5.3.3软件动静结合安全检测技术5.3.1软件静态安全检测技术软件静态安全检测技术是针对未处于运行状态的软件所开展的安全分析测试技术。静态安全检测技术可以用于对软件源代码和可执行代码的检测。5.3.1软件静态安全检测技术1.软件源代码的静态安全检测技术由于源代码中的变量赋值明确，程序流程清晰，逻辑关系明了，采用静态安全检测技术更容易深入进行数据流的分析，并且可以全面地考虑执行路径的信息，能够更有效的发现漏洞。因此，静态安全检测技术是软件源代码的主要安全检测技术。静态安全分析技术主要优势是不需要构建代码运行环境，分析效率高，资源消耗低。虽然都存在较高的误报率，但仍然在很大程度上减少了人工分析的工作量。目前常用的静态安全检测技术包括词法分析、数据流分析、污点传播、符号执行、模型检查、定理证明等。5.3.1软件静态安全检测技术（1）词法分析词法分析通过对源代码进行基于文本或字符标识的匹配分析对比，以查找符合特定特征和词法规则的危险函数、API或简单语句组合。词法分析能够开展针对词法方面的快速检测，算法简单，检测性能较高，然而这种分析技术只能进行表面的词法检测，而不能进行语义方面的深层次分析，因此可以检测的安全缺陷和漏洞较少，会出现较高的漏报和误报，尤其对于高危漏洞无法进行有效检测。使用该技术的源代码安全检测工具包括Checkmarx和ITS4等。5.3.1软件静态安全检测技术（2）数据流分析通过分析软件代码中变量的取值变化和语句的执行情况来分析数据处理逻辑和程序的控制流关系，从而分析软件代码的潜在安全缺陷。将代码构造为抽象语法树或程序控制流图，接着追踪获取变量的变化信息，描述程序的运行行为，根据事先定义的安全规则检测出缺陷和漏洞。数据流分析适合检查因控制流信息非法操作而导致的安全问题，如内存访问越界、常数传播等。由于对于逻辑复杂的软件代码，检测的准确率较低，误报率较高。该方法具有较高的可行性，可实现针对大规模代码的快速分析，广泛应用于商业的源代码安全性分析工具中。例如，Coverity、Klockwork5.3.1软件静态安全检测技术（3）污点传播分析通过分析代码中输入数据对程序执行路径的影响，以发现不可信的输入数据导致的程序执行异常。首先对污点数据进行标记，静态跟踪程序代码中污点数据的传播路径，发现使用污点数据的不安全执行路径，进而分析出由于非法数据的使用而引发的输入异常类漏洞。较高的分析准确率，针对大规模代码时性能受影响。Pixy是使用该技术的典型工具5.3.1软件静态安全检测技术（4）符号执行在不实际执行程序的前提下，将程序的输入表示成符号，根据程序的执行流程和输入参数的赋值变化，把程序的输出表示成包含这些符号的逻辑或算术表达式的一种技术。通过符号执行获得程序输出和输入之间关系的算术表达式，可通过约束求解的方法获得能得出正常输出结果的输入值的范围。不能得到正常输出的输入值，或者输入值范围的边界点，则是触发程序输出异常结果的潜在输入点，也是进行安全性检测的重要检测区域。5.3.1软件静态安全检测技术符号执行有代价小，效率高的优点，然而由于程序执行的可能路径随着程序规模的增大呈指数级增长，从而导致符号执行技术在分析输入和输出之间关系时，存在一个路径状态空间的爆炸问题，路径爆炸问题在现有计算能力的条件下很难解决。由于符号执行技术进行路径敏感的遍历式检测，当程序执行路径的数量超过约束求解工具的求解能力时，符号执行技术将难以分析。使用了符号执行进行源码检测的工具有EXE、SAGE、SMART以及KLEE等。5.3.1软件静态安全检测技术（5）模型检验模型检验技术首先将软件构造为状态机或者有向图等抽象模型，并使用模态/时序逻辑公式等形式化的表达式来描述安全属性，然后对模型进行遍历以验证软件的这些安全属性是否满足。模型检验对于路径和状态的分析过程可以实现全自动化；但是由于穷举所有状态，所以存在计算能力受限的问题，在对大型复杂软件的漏洞挖掘方面仍处于探索阶段。对时序、路径等属性在边界处的近似处理难度也较大。微软公司的SLAM项目、伯克利大学的 MOPS工具等都是代表性工具。5.3.1软件静态安全检测技术（6）定理证明定理证明的方法通过将程序转换并表示为逻辑公式，然后使用公理和规则证明的方法，验证程序是否为一个合法的定理，从而发现其中无法证明的部分，从中发现安全缺陷。在静态分析技术中是最准确的，误报率较低。然而该技术抽象和转换工作需要人工干预，自动化程度不高，难以应用于新漏洞的检测，而且难以应用于大型程序分析。使用该技术的安全检测工具包括Saturn,ESC/JAVA等。5.3.1软件静态安全检测技术2.可执行代码的静态安全检测技术针对软件可执行代码的检测，只能对可执行代码反汇编后得到的汇编代码进行检测，而汇编代码中多是寄存器之间数值的操作，没有明确的语义信息，因此静态安全检测技术往往分析效率低下，误报率较高。可执行代码的静态安全检测技术可分为基于程序结构的安全检测技术和基于程序语义的安全检测技术。5.3.1软件静态安全检测技术（1）基于程序结构的安全检测技术基于程序结构的安全检测技术需要根据二进制可执行文件的格式特征，从二进制文件的头部、符号表以及调试信息中提取安全敏感信息，来分析文件中是否存在安全缺陷。由DataRescue公司开发的IDA Pro是一款备受业内人士青睐的的反汇编工具. Bugscam检测 工具能够基于IDA Pro对被测试程序进行安全 缺陷检测。5.3.1软件静态安全检测技术（2）基于程序语义的安全检测技术先对程序进行反汇编得到汇编代码，再将汇编代码转换为中间语言，在分析中间语言的基础上针对得到的部分语义信息进行缺陷和漏洞的检测。由于在不同的操作系统上，二进制可执行文件的格式不同，所以基于程序语义的分析方法得益其跨平台性而受到广泛的研究。UAFChecker检测工具采用了基于程序语义的安全检测技术，它能够对浏览器软件中常见的UseAfterFree漏洞进行静态检测。5.3.2软件动态安全检测技术软件动态安全检测技术是针对运行中的软件程序，通过构造非正常的输入来检测软件运行时是否出现故障或崩溃等非正常的输出，并通过检测软件运行中的内部状态信息来验证或者检测软件缺陷的过程，它的分析对象是可执行代码。动态安全检测技术是通过实际运行发现问题，所以检测出的安全缺陷和漏洞准确率非常高，误报率很低。目前，软件的动态安全检测技术主要包括模糊测试、智能模糊测试和动态污点跟踪等，下面进行具体介绍。5.3.2软件动态安全检测技术(1)模糊测试模糊测试(Fuzzing)是一种自动化或半自动化的安全漏洞检测技术，通过向目标软件输入大量的畸形数据并监测目标系统的异常来发现潜在的软件漏洞。通常的模糊测试过程基本都采用以下几个通用的步骤。(1)模糊测试5.3.2软件动态安全检测技术确定测试对象生成测试数据发送数据进行检测保存数据和异常信 息目标程序异常是 否图531 模糊测试流程5.3.2软件动态安全检测技术(2)智能模糊测试模糊测试方法是应用最普遍的动态安全检测方法，但由于模糊测试数据的生成具有随机性，缺乏对程序的理解，测试的性能不高，并且难以保证一定的覆盖率。为了解决这个问题，引入了基于符号执行等可进行程序理解的方法，在实现程序理解的基础上，有针对性的设计测试数据的生成，从而实现了比传统的随机模糊测试更高的效率，这种结合了程序理解和模糊测试的方法，称为智能模糊测试(smart Fuzzing)技术。5.3.2软件动态安全检测技术(2)智能模糊测试智能模糊测试具体的实现步骤如下。反汇编中间语言转换采用智能技术分析输入数据和执行路径的关系利用分析获得的输入数据集合，对执行路径集合进行测试5.3.2软件动态安全检测技术(3) 动态污点分析模糊测试技术侧重随机生成数据样本并测试，它不关注程序真实的执行过程。动态污点分析(dynamic taint analysis)技术则通过分析被测试程序内部指令真实的执行过程，追踪输入数据在程序内部的传递、处理流程，以检测输入数据是否存在涉及安全的敏感操作，从而分析出污点数据导致的潜在安全缺陷和漏洞。5.3.2软件动态安全检测技术(3) 动态污点分析动态污点分析关注所有来自程序外部的不可信污点数据在可执行程序中的传播过程，对所有的不可信污点数据都标记一个唯一的标签，然后跟踪这些标签在可执行程序中的传递过程。在跟踪这些过程时，不仅考虑二进制程序中的数据依赖关系，而且考虑不同变量之间的控制依赖关系。动态污点分析技术可以识别出输入文件中的哪些字节会影响二进制程序中涉及安全敏感操作的函数，从而发现可能触发安全缺陷和漏洞的污点数据。BitBlaze软件使用了该技术。5.3.2软件动态安全检测技术(3) 动态污点分析动态污点分析关注所有来自程序外部的不可信污点数据在可执行程序中的传播过程，对所有的不可信污点数据都标记一个唯一的标签，然后跟踪这些标签在可执行程序中的传递过程。在跟踪这些过程时，不仅考虑二进制程序中的数据依赖关系，而且考虑不同变量之间的控制依赖关系。动态污点分析技术可以识别出输入文件中的哪些字节会影响二进制程序中涉及安全敏感操作的函数，诸如内存分配函数、字符串函数和其它的一些函数，从而发现可能触发安全缺陷和漏洞的污点数据。5.3.3软件动静结合安全检测技术目前普遍应用的动静结合安全检测技术主要包括两种。第一种是先对源代码进行静态分析，发现潜在的漏洞，然后构造输入数据在程序动态运行时验证其真实性。这种方法没有更多地发挥动态分析的作用。第二种是对可执行代码进行反汇编，通过对汇编代码或者中间语言进行静态检测分析获取的信息指导动态漏洞分析。5.3.3软件动静结合安全检测技术目前普遍应用的动静结合安全检测技术主要包括两种。第一种是先对源代码进行静态分析，发现潜在的漏洞，然后构造输入数据在程序动态运行时验证其真实性。这种方法没有更多地发挥动态分析的作用。第二种是对可执行代码进行反汇编，通过对汇编代码或者中间语言进行静态检测分析获取的信息指导动态漏洞分析。5.4软件安全保护5.4.1软件安全保护的基本概念软件安全保护的概念软件安全保护的意义软件安全保护相关法案5.4.2基于软件技术的软件安全保护技术注册信息验证技术软件防篡改技术代码混淆技术… …5.4.3基于硬件介质的软件安全保护技术5.4.1软件安全保护的基本概念1．软件安全保护的概念软件安全保护技术是指通过技术手段对受保护文件以及其运行的环境添加防护和控制措施，使得受保护的软件在防护和控制范围内无法被逆向分析，从而在一定程度上防止软件被破解、篡改以及盗用版权。软件安全保护技术主要有软件水印、代码混淆、软件加密、功能限制等，主要实现降低代码的可读性和防止软件本身在运行时被调试等，主要应用在软件防盗版、防滥用、防篡改、防止信息获取等方面。5.4.1软件安全保护的基本概念2.软件安全保护的意义对于开发者或企业开发的应用软件，为了防止逆向分析，在软件产品上添加软件保护功能都是非常必要的。对于软件版权的保护是软件的一个基本需求，预防和阻止逆向分析人员进行逆向分析，是对应用软件进行保护的最有效方法。此外，某些软件开发平台上没有任何软件保护措施，逆向分析人员可以很容易地把程序转换回接近于源代码的表现形式，大多数基于非加密虚拟机的解释平台（如Java和.NET）就是这类开发平台，这些软件开发平台必须采用软件保护技术。5.4.1软件安全保护的基本概念2.软件安全保护的意义因此，进行软件安全保护可以有效的防止逆向分析人员对软件开发者的工作成果进行逆向分析。这种安全技术不仅可保护软件自身，同时也可以有效的保护软件的授权系统、防拷贝系统，以及其他正版软件防护系统发挥正常的功能。5.4.1软件安全保护的基本概念3.软件安全保护相关法案随着软件安全保护受到越来越多的重视，一些对应的保护法案也逐渐出现，即DMCA（Digital Millennium Copyright Act）。DMCA的核心思想是，版权保护技术本身是容易受到攻击的，必须通过立法的方式来保护这些技术。DMCA实际上只属于一种数字版权保护DRM（Digital Rights Management）的法案，它仅涉及到所有受数字权限管理系统保护的软件，对于其它大多数软件，则没有强制的法律效用。5.4.2基于软件技术的软件安全保护技术1.注册信息验证技术注册过程一般是用户把自己的个人或者单位信息提交给开发这款软件产品的公司，软件公司会根据用户提交的信息通过调用注册函数计算出序列码并返回给用户。用户得到这个序列码后，在进行软件注册时输入注册信息和注册码，由软件验证程序验证通过后，软件就会取消各种限制，这种注册加密方式实现简单，大多数软件都采用这种方式。5.4.2基于软件技术的软件安全保护技术2.软件防篡改技术软件防篡改技术主要是通过完整性检验来检测软件是否被攻击者篡改。软件的完整性检验主要通过验证软件的哈希值或者数字签名来判断。事先计算好的哈希值或数字签名隐藏在软件中，每次检测时重新计算哈希值并与原哈希值进行比较，或对数字签名进行验证。5.4.2基于软件技术的软件安全保护技术3.代码混淆技术代码混淆技术是在保持原有代码功能的基础上，通过代码变换等混淆手段实现降低代码的人工可读性，隐藏代码原始逻辑的一种技术。逆向人员在分析混淆后的代码时，会受到大量非相关信息干扰，从而大大增加代码逆向分析的难度。即使攻击者最后能破解这些经过混淆处理后的程序，但是也会让他们付出很高的时间代价。代码混淆技术可通过多种技术手段实现，包括词法转换、控制流转换、数据转换等。5.4.2基于软件技术的软件安全保护技术4.软件水印技术软件水印是一种软件产品版权保护技术，可以用来标识软件开发商、所有者、使用者等信息，通过水印中携带的版权保护信息和身份认证信息，可以鉴别出非法复制和盗用的软件产品。根据水印的加载位置，软件水印可以分为代码水印和数据水印。代码水印是将水印信息隐藏在程序的代码和指令部分。数据水印则是将水印信息隐藏在程序的头文件、字符串和调试信息等数据中。5.4.2基于软件技术的软件安全保护技术5.软件加壳技术软件加壳技术，也称为代码变形技术，可以实现对可执行文件的压缩或者加密，从而改变可执行文件中的代码表现形式，使逆向分析人员对存储在硬盘上的文件难以进行静态逆向分析，增加动态分析的难度。软件脱壳是将可执行文件进行解压缩或者解密，从而使可执行文件还原为可执行的正常状态。根据软件加壳的目的和作用，可分为两类。第一种是压缩保护壳，以减小软件体积和改变软件可执行代码的特征为目的，例如ASPacK、UPX 和PECompact 等。5.4.2基于软件技术的软件安全保护技术5.软件加壳技术第二种是加密保护壳，这种壳以保护软件为目的，根据用户输入的密码用相应的加密算法对原程序进行加密，如果破解者强行更改密码检测指令，因加密代码并未被解密还原，将导致程序的错误执行。例如 ASProtect、Armadillo、EXECryptor等。5.4.2基于软件技术的软件安全保护技术6.反调试反跟踪技术反调试技术往往是通过将一些与调试相关的API函数内嵌到软件源代码之中，检测是否有调试器驻留内存进行调试，如果检测到就认为被调试跟踪，对调试器设置断点以及单步跟踪的方式进行阻拦。此外，可将反调试技术与软件加壳技术、代码混淆等静态技术混合起来使用，加密后的软件会迫使逆向工作者在调试器中动态调试以进行破解，而进行过加密的反调试代码又可以有效的组织调试者使用调试工具，从而实现更安全的保护。5.4.3基于硬件介质的软件安全保护技术基于硬件介质的软件安全保护技术是利用计算机硬件或某些信息存储介质保存的认证和加密信息，实现对软件系统的安全加密保护。基于硬件介质的软件安全保护技术包括有加密狗、加密光盘、专用接口卡等。5.4.3基于硬件介质的软件安全保护技术1.加密狗加密狗是一种智能型加密工具，它是一个安装在并口、串口或者 USB口上的硬件设备，同时带有一套便于被开发者开发时使用的驱动程序接口和工具软件。当被加密狗保护的软件运行时，软件首先会搜索是否有连接在计算机上的加密狗硬件设备，接着向连接在计算机上的加密狗发出查询命令，加密狗收到查询后会进行响应，正确的响应会保证软件的正常运行。如果没有加密狗，软件没有得到响应数据，将终止运行。5.4.3基于硬件介质的软件安全保护技术2.光盘保护技术光盘保护技术将密钥或特定文件存储在光盘的轨道上，一般用户难以通过刻录光盘而得到这个密钥或者特定文件。一些采用光盘形式发行的应用程序或游戏等软件，在启动时往往通过判断光驱中的光盘是否存在密钥或者所需的特定文件，来实施对软件的保护。如果密钥或者特定文件不存在，则认为用户未得到正常授权，软件会终止运行。5.4.3基于硬件介质的软件安全保护技术3.专用的计算机接口卡首先，将软件的核心代码或主要模块采用加密方式写入到存储芯片中，并将芯片固化到该接口卡上，在计算机硬盘上只存储软件的引导部分。该软件启动后，需要将核心的运算传输到该接口卡进行处理，如果没有连接该硬件接口卡，就无法运行该软件。这种专用接口卡的方法对计算机系统资源的占有率较低，而且能够有效地防止各种调试跟踪手段和攻击工具对软件的破译，提供了很高的软件安全保护能力。然而，硬件方式成本较高，而且安装配置给用户增加了不便。5.5恶意程序5.5.1恶意程序的分类单一功能病毒木马,蠕虫,恶意脚本综合型病毒5.5.2 恶意程序的传播方式和破坏功能恶意程序的传播方法恶意程序的破坏功能5.5.3 恶意程序检测查杀技术5.5.1恶意程序的分类恶意程序是指恶意影响计算机操作系统、应用程序和数据的完整性、可用性、可控性和保密性的计算机程序。按传播方式，恶意程序可以分成以下几类：病毒，木马，蠕虫，恶意脚本、综合型病毒。恶意程序往往用来统称病毒、木马、蠕虫等恶意软件，有时广义的病毒概念等同于恶意程序的概念。5.5.1恶意程序的分类1.单一功能病毒计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或毁坏数据，影响计算机使用，并能够自我复制的一组计算机指令或者程序代码。计算机病毒具有很强的破坏性、传染性、隐藏性、寄生性、潜伏性和欺骗性，出现较早的单一功能的病毒包括以下几种。文件感染型病毒,宏病毒,引导型病毒,邮件型病毒.5.5.1恶意程序的分类2. 蠕虫蠕虫病毒一般有两部分组成：一个主程序和一个引导程序。主程序通过扫描技术自动搜集与当前被病毒感染计算机在一个网络中的其他机器，然后通过漏洞利用技术在远端计算机上将引导程序启动，从而将蠕虫病毒植入被感染的计算机中。蠕虫病毒在计算机普遍没有安装软件防火墙，并且操作系统没有补丁自动更新机制时，曾经大规模的流行，例如Blaster和SQL Slammer等。5.5.1恶意程序的分类3.恶意脚本恶意脚本通常是用脚本语言编写的恶意代码，它通过调用 Windows 系统中开放的对象、组件，在用户通过浏览器访问恶意的脚本代码时，可以直接对浏览器中的首页信息等进行修改和控制，甚至实施网站挂马、主页替换、跨站点脚本攻击等恶意操作。5.5.1恶意程序的分类4. 综合型病毒现在的病毒往往面临杀毒软件、主动防御软件、防火墙、入侵检测系统等查杀。为了在普遍应用安全防护产品的计算机中生存下来，并能实现有效的传播，往往病毒要具备多种感染传播功能才能实现，这种病毒即是综合型病毒。当前流行的病毒主要属于综合型病毒，通过网络挂马、移动存储介质、诱骗下载等途径传播。一旦感染则在操作系统中添加启动项实现自动启动，并通过链接攻击者接收指令实现下述功能：窃取信息、下载其它恶意程序、制造点击量、攻击其它计算机等。5.5.2 恶意程序的传播方式和破坏功能随着杀毒软件免费化的开展，杀毒软件的使用率逐渐提高，有效的遏制了病毒等恶意程序的传播。导致恶意程序传播途径和范围也在做相应的调整。随着网银、网购业务的大量开展，攻击者为了追求经济利益，针对这类网站进行攻击的定制病毒得到了快速发展，而病毒的大规模入侵情况在减少。调查发现，我国计算机病毒主要通过网站挂马、诱骗下载、电子邮件、移动存储介质和局域网内传播等途径进行扩散传播。5.5.1恶意程序的分类1.恶意程序的传播方法（1）网站挂马（2）诱骗下载（3）通过移动存储介质传播（4）通过电子邮件和即时通信软件传播（5）通过局域网传播5.5.2 恶意程序的传播方式和破坏功能1.恶意程序的传播方法（1）网站挂马（2）诱骗下载（3）通过移动存储介质传播（4）通过电子邮件和即时通信软件传播（5）通过局域网传播5.5.2 恶意程序的传播方式和破坏功能2.恶意程序的破坏功能（1）浏览器配置被修改（2）窃取用户密码账号等隐私信息（3）实现远程控制（4）破坏系统或网络的正常运行5.5.3 恶意程序检测查杀技术为了逃避杀毒软件等安全软件的查杀或防御功能，恶意程序采用了多种防杀或对抗技术来提升自身的生存能力。为此，检测或查杀恶意程序的手段或方法也在不断发展或提升，以适应新型恶意程序功能的变化。针对恶意程序检测或查杀的主要技术包括特征码查杀、启发式查杀、基于虚拟机技术的行为判定，以及主动防御等。5.5.3 恶意程序检测查杀技术1.特征码查杀技术依据恶意程序的特征码进行查杀是最基本的一种杀毒技术，目前大多数杀毒软件均采用此方法。它针对已知病毒木马等恶意程序进行分析，提取典型代码特征添加到特征库中，然后根据恶意程序的特征码对文件或内存进行扫描匹配，匹配成功则检测出相应特征码对应的恶意程序。征码查杀技术对恶意程序查杀有很高的准确性和可靠性。然而恶意程序为了躲避查杀，采用加密和变形等加壳技术，改变自身静态文件的特征码，使这种简单的特征码静态扫描方式失去作用。5.5.3 恶意程序检测查杀技术1.特征码查杀技术特征码的提取：第一种方法，提取恶意程序代码段中的特征码。第二种方法，通过特殊字符串提取特征码。第三种方法，提取通杀特征码。5.5.3 恶意程序检测查杀技术2.启发式查杀技术启发式查杀技术通过事先分析恶意程序执行指令的顺序、或者特定行为的组合情况等特征，建立检测的基准行为或指令的样本库，并以这些基于行为或指令的特征来检测并确定是否是恶意程序。由于恶意程序实施感染或破坏操作时，一般的行为都会有一定的特征，例如格式化硬盘、修改文件时间属性或大小属性等非正常文件读写、中断自身程序的运行、非正常进入系统内核层即Ring0层等。因而，可以通过检测程序实施的特定行为或多种行为的组合，来检测恶意程序。5.5.3 恶意程序检测查杀技术3.虚拟机查杀技术虚拟机查杀技术是在扫描恶意程序时，通过将恶意程序加载到虚拟机环境中运行，从而让恶意程序自动脱壳还原为原有状态，再进行检测查杀的技术。采用虚拟机技术查杀恶意程序时，需要执行一个虚拟环境，这将消耗较多的系统资源，可能引起性能的下降。而且，针对每个待检测的程序，虚拟环境只能在有限时间内进行检测，这样就给恶意程序通过自身添加干扰执行的代码，拖延脱壳的时间，从而实现和虚拟机杀毒技术的对抗。5.5.3 恶意程序检测查杀技术4.主动防御技术主动防御技术往往通过事先挂钩系统服务派发表SSDT中的多个API函数，例如进程创建、线程创建、DLL插入等系统函数，实现对恶意程序行为的全面监控。当恶意程序的行为符合事先设定的异常行为特征时，则对恶意程序进行拦截，并提示给用户，将是否终止的权利交给用户来决定。5.5.4 恶意程序的防范为了逃避杀毒软件的查杀，恶意程序不断提升技术实现与杀毒软件的对抗，不断开发具有新功能的变种程序。单纯依靠杀毒软件难以有效检测和防范大量新出现的恶意程序和新的变种。因此，在利用安全保护软件的基础上，针对恶意程序传播途径进行防护，最终做到防患于未然才是上策。而要做到防患于未然，需要从下面几点着手进行恶意程序的安全防护。5.5.4 恶意程序的防范（1）做好计算机自身的安全防护（2）防止网站浏览和访问造成的恶意程序入侵（3）防止因下载造成的恶意程序入侵（4）防止通讯类软件造成的恶意程序入侵（5）防止因移动存储介质造成的恶意程序入侵（6）防止基于局域网的恶意程序入侵5.6 Web应用系统安全5.6.1 Web安全威胁遭破坏的身份认证和会话管理不安全的直接对象引用安全配置错误不安全的加密存储… …5.6.2 Web安全防护客户端安全防护通信信道安全防护… …5.6.3 Web安全检测5.6.1 Web安全威胁在过去的十多年里，因特网在给人们带来革命性的信息沟通与协作平台的同时，各种恶意程序与黑客攻击也史无前例的增多，随着各种HTTP Web应用服务的普遍开展，再加上越来越多的服务朝向Web化的方向迈进，Web安全所面临的威胁也与日俱增。根据2010年OWASP发布的Web应用十大安全威胁排名，排在前十位的安全风险依次为：注入、跨站脚本、遭破坏的身份认证和会话管理、不安全的直接对象引用、伪造跨站请求、安全配置错误、不安全的加密存储、没有限制的URL访问、传输层保护不足和未验证的重定向和转发.5.6.1 Web安全威胁1.遭破坏的身份认证和会话管理“遭破坏的认证和会话管理”是指攻击者窃听了用户访问HTTP时的用户名和密码，或者是用户的会话，从而得到sessionID，进而冒充用户进行HTTP访问的过程。在用户登录时，在用户输入用户名和密码后一般通过POST的方法进行传输，可通过不安全的HTTP传递，也可通过加密的HTTPS传递。有些网站显示的是HTTPS，而事实上是用HTTP。检测是否使用HTTPS的最简单方法就是使用网络嗅探工具，SnifferPro或Ethereal来嗅探是否加密.5.6.1 Web安全威胁1.遭破坏的身份认证和会话管理假设登陆页面要求用户输入用户名和密码，然后有一个“提交”按钮，那么在WebScrab中可以得到如下的请求数据：POST http://www.example.com/login HTTP/1.1Host: www.example.comUserAgent: Mozilla/5.0 (Windows NT 5.2; rv:16) Gecko/20100101 Firefox/16.0Accept: text/xml,application/xml,application/xhtml+xmlAcceptLanguage: itit,it;q=0.8,enus;q=0.5,en;q=0.3AcceptEncoding: gzip,deflateAcceptCharset: ISO88591,utf8;q=0.7,\*;q=0.7KeepAlive: 300Connection: keepaliveReferer: http://www.example.com/index.jspCookie:JSESSIONID=LVrRRQQXgwyWpW7QMnS49vtW1rEdqn98CGlkP4jTvVCGdyPkmn3S!ContentType: application/xwwwformurlencodedContentlength: 64delegated\_service=218&User=test&Pass=test&Submit=SUBMIT5.6.1 Web安全威胁1.遭破坏的身份认证和会话管理假设登陆页面要求用户输入用户名和密码，然后有一个“提交”按钮，那么在WebScrab中可以得到如下的请求数据：POST http://www.example.com/login HTTP/1.1Host: www.example.comUserAgent: Mozilla/5.0 (Windows NT 5.2; rv:16) Gecko/20100101 Firefox/16.0Accept: text/xml,application/xml,application/xhtml+xmlAcceptLanguage: itit,it;q=0.8,enus;q=0.5,en;q=0.3AcceptEncoding: gzip,deflateAcceptCharset: ISO88591,utf8;q=0.7,\*;q=0.7KeepAlive: 300Connection: keepaliveReferer: http://www.example.com/index.jspCookie:JSESSIONID=LVrRRQQXgwyWpW7QMnS49vtW1rEdqn98CGlkP4jTvVCGdyPkmn3S!ContentType: application/xwwwformurlencodedContentlength: 64delegated\_service=218&User=test&Pass=test&Submit=SUBMIT在上面的数据中，可以看到，POST方法通过HTTP协议把数据发送到http://www.example.com/login，然而由于传送的数据没有进行加密，恶意用户通过监听网络就很容易得到用户名test和密码test。5.6.1 Web安全威胁1.遭破坏的身份认证和会话管理再看下一个用HTTPS协议的例子，请求的头数据如下：POST https://www.example.com:443/login.do HTTP/1.1Host: www.example.comUserAgent: Mozilla/5.0 (Windows NT 5.1; rv:16) Gecko/20100101 Firefox/16.0Accept: text/xml,application/xml,application/xhtml+xml,text/htmlAcceptLanguage: itit,it;q=0.8,enus;q=0.5,en;q=0.3AcceptEncoding: gzip,deflateAcceptCharset: ISO88591,utf8;q=0.7,\*;q=0.7KeepAlive: 300Connection: keepaliveReferer: http://www.example.com/homepage.doCookie: SERVTIMSESSIONID=s2JyLkvDJ9ZhX3yr5BJeRFLkdphH0QNSJ3VQB6pLhjkW6FContentType: application/xwwwformurlencodedContentlength: 45User=test&Pass=test&portal=ExamplePortal如上所示，请求通过HTTPS引向了https://www.example.com:443/login.do，如果看Referer的值，就发现是从HTTP http://www.example.com/homepage.do过来的。在这种情况下，浏览器窗口中并不会告知现在使用的安全连接，而事实上却是在使用HTTPS安全连接。在HTTPS协议下，上述协议的内容都是处于加密状态的，所以用户名和口令是无法看到的。上面的消息只是为了显示这个请求而进行了解析，实际内容是加密的。5.6.1 Web安全威胁2.不安全的直接对象引用不安全的直接对象引用就是指一个用户通过更改URL等操作可以成功访问到未被授权的内容。比如一个网站上的用户通过更改URL可以访问到其他用户的私密信息和数据等。String query=”SELECT \* FROM accts WHERE account=?”;PreparedStatement pstmt=connection.prepareStatement(query, ...);pstmt.setString(1,request.getParameter(“acct”));ResultSet results=pstmt.executeQuery();上面的代码中通过一个未被验证的用户账号来获取相关数据，在这样的情况下，攻击者可以通过在浏览器中简单修改“acct”参数的值发送到不同的用户账号来获取信息。因为代码并没有进行任何的验证，所以能够轻易的访问到其他用户的信息。5.6.1 Web安全威胁2.不安全的直接对象引用不安全的直接对象引用攻击，主要包含下面两个步骤。第一步，首先需要判断Web网站是否有泄漏直接对象引用给用户，如果在整个Web网站中未发现直接对象引用，则不存在此威胁。第二步，通过更改URL等操作，尝试访问非授权的数据，如果Web网站没有进行访问控制，即可获取Web网站非授权数据5.6.1 Web安全威胁2.不安全的直接对象引用为了防止不安全的对象引用，需要尽量避免将私密的对象引用直接暴露给用户。在向用户提供访问之前，一定要进行认证和审查，实行严格的访问控制。5.6.1 Web安全威胁3.安全配置错误安全配置错误是Web应用系统常见的安全问题，在Web应用的各个层次都有可能出现安全配置错误，比如操作系统、Web服务器、应用程序服务器、数据库、应用程序等。为了防止安全配置错误，首先，必须及时将各个软件更新到最新状态。其次，采用安全的系统框架，对Web系统的各个组件进行分离。最后，考虑定时对Web系统进行扫描，以发现可能存在的配置错误。归根到底就是尽可能的将Web应用系统的各个方面都做好安全配置。5.6.1 Web安全威胁4.不安全的加密存储所谓不安全的加密存储指的是Web应用系统没有对敏感性资料进行加密，或者采用的加密算法复杂度不高可以被轻易破解，或者加密所使用的密钥非常容易检测出来。归根到底就是所存储的内容能够轻易被攻击者解析从而产生安全威胁为了防止不安全的加密存储，对于所有的敏感性数据必须进行加密，且无法被轻易破解。保证加密密钥被妥善保管，攻击者不能轻易窃取，并准备密钥的定期更换。对于敏感存储内容必须进行严格的访问控制，只允许授权用户进行操作。5.6.1 Web安全威胁5.没有限制的URL访问通常URL访问限制主要是限制未授权用户访问某些链接，一般通过隐藏来实现保护这些链接。然而对于一个攻击者来说，在某些情况下有可能能够访问被隐藏了的链接，从而可以使用未被授权的功能。为了防止一些未经授权的URL访问，可以对每一个页面加上适当的授权认证机制。对于每一个URL链接必须要配置一定的防护措施，包括：对于要隐藏的链接必须能限制非授权用户的访问；加强基于用户或者角色的访问控制；禁止访问一些私密的页面类型5.6.1 Web安全威胁6.传输层保护不足Web应用系统一般部署在远端服务器上，客户端和服务器之间的请求和响应消息会在互联网上传输。攻击者利用嗅探方法就可以简单的截获网络上的数据，如果传输层上没有任何的保护措施，那么对于用户和Web应用系统都是非常危险的。为了实现对传输层的安全保护，可以将所有的敏感页面采用SSL技术加密传输，将未采用SSL的请求转向SSL页面。同时，后台或者其他链接也应该使用SSL或者其他加密技术。在使用SSL协议时，需要确保数字证书的有效性。5.6.1 Web安全威胁7.未验证的重定向及转发重定向就是将网络请求从一个网址转移到其他网址。在Web应用系统中，重定向是非常常见的，并且通常重定向所指向的目的是通过用户输入参数得到的。如果没有经过验证，攻击者就能够将其他用户引导到特定的站点。转发与重定向略有不同，但在Web系统中同样也非常常见。总的来说，未经过验证的重定向将可能使用户被引导到钓鱼网站或者挂马网站等恶意站点，而未经过验证的转发将可能导致用户绕过验证和授权机制。5.6.1 Web安全威胁7.未验证的重定向及转发示例1：应用程序的一个”redirect.jsp”页面有一个参数“url”。攻击者构造一个恶意的URL,可把用户重定向到一个恶意站点evil.com，如下所示。http://www.example.com/redirect.jsp?url=evil.com示例2：应用程序使用转发功能在网站的不同部分之间转发请求。为了实现这个功能，程序的一些页面使用参数来表明用户应该被重定向到什么地方。在这种情况下,攻击者就可以构造URL以成功绕过应用程序的访问控制功能，从而使攻击者可以获得在正常情况下无法获得的管理功能。http://www.example.com/boring.jsp?fwd=admin.jsp为了防范未验证的重定向及转发，需要考虑以下几点防范措施：尽量避免使用重定向和转发；使用重定向和转发要避免通过参数获得地址；如果必须使用目标地址，必须校验地址，并加强授权和认证。5.6.2 Web安全防护1.客户端安全防护Web客户端的防护是指浏览器的安全防护，主要是防止远程恶意代码执行。如果客户端浏览器存在未被修补的远程代码执行漏洞，在访问被挂马站点时，浏览器就会执行恶意代码，从而遭受攻击。对于Web客户端的防护措施，包括选择安全的、可信的浏览器，及时针对Web浏览器进行版本更新，并及时打补丁。2.通信信道安全防护针对于通信信道的安全防护主要是防止明文数据直接在网络中传输，HTTP协议在传输时，很容易通过嗅探工具截获数据，如果对安全性有较高要求，需要用HTTPS协议代替HTTP协议，它将利用SSL协议来保证数据传输的安全。由于SSL协议提供了安全认证、加密传输和数据完整性的检验，所以为Web客户端和服务器之间数据的安全传输提供了可靠的保障。5.6.2 Web安全防护3.服务器端安全防护在上一节中已经全面介绍了服务器端Web应用程序的各种安全威胁和防护措施。Web服务器端软件本身随着时间的推移，也会不断出现新的安全漏洞，及时做好版本升级更新就显得特别重要。必须及时的发现Web应用程序中可能存在的安全风险并予以修补，防止网站遭受恶意攻击。一旦遭到攻击，必须能够及时响应，修补漏洞，防止站点遭到恶意挂马等恶性攻击。5.6.3 Web安全检测1. 黑盒检测技术黑盒测试需要发送大量的请求，所以在检测的过程中，自动化检测工具是非常重要的，目前这种自动化的检测工具非常多的，比如IBM公司的AppScan，HP公司的WebInspect，OWASP项目组开发的ZAP,Web Vulnerability Scanner，以及国内的JSky、明鉴WEB应用弱点扫描器软件等。5.6.3 Web安全检测1. 黑盒检测技术5.6.3 Web安全检测2. 白盒检测技术白盒测试方法是针对Web系统的源代码进行全面的代码安全性分析和审查的方法，以全面检测分析Web应用程序的内部运作机制中存在的安全性问题。从理论上来说，通过代码审查几乎可以确定所有的安全威胁，然而对于一个完整的Web应用系统，其代码结构非常复杂，想要从中找出所有的安全威胁是非常困难。Fortify 、Coverity、Klockwork是典型的软件源代码安全测试工具。它们通过内置的分析引擎，从数据流、语义、结构、控制流、配置流等多个方面对应用软件的源代码进行静态分析并整理形成报告。5.7小结1.软件漏洞软件漏洞是计算机系统的硬件、软件、协议在系统设计、具体实现、系统配置或安全策略上存在的缺陷。漏洞的定义包含了三个要素，漏洞是计算机系统本身存在的缺陷；漏洞的存在和利用都有一定的环境要求；漏洞的存在本身是没有危害的，只有被攻击者恶意利用，才能给计算机系统带来威胁和损失。软件漏洞可以采用多种分类手段，软件漏洞的危险等级分为紧急、重要、中危、低危。国内外知名漏洞库包括CVE、BugTraq、NVD、CNNVD、CNVD、EDB等。常见的软件漏洞包括缓冲区溢出漏洞、格式化字符串漏洞、整数溢出漏洞、数组越界漏洞、写污点值到污点地址漏洞，以及内存地址对象破坏性调用漏洞。其中缓冲区溢出漏洞包括栈溢出漏洞、堆溢出漏洞和单字节溢出漏洞等三种典型的漏洞。根据软件漏洞具体条件，构造相应输入参数和shellcode代码，最终实现获得程序控制权的过程，就是漏洞利用。针对静态的shellcode地址、动态变化的shellcode地址分别采用不同的漏洞利用技术，此外堆漏洞的利用可采用heap spray技术。Windows操作系统为了防止漏洞利用，提供了GS、DEP、ASLR、safeSEH、SEHOP等漏洞利用防护技术。5.7小结2.软件安全开发软件编码人员进行软件开发过程中，一般都会遵循相应的软件开发生命周期模型用于指导编码的整个过程。软件开发生命周期包括了问题的定义与规划、需求分析、软件设计、程序编码、软件测试、运行维护等几个关键阶段。软件开发生命周期模型包括瀑布模型、螺旋模型、迭代模型、快速原型模型等几种主要模型。软件安全开发技术主要包括建立安全威胁模型、安全设计、安全编码和安全测试等几个方面。微软公司在软件安全开发技术等基础上，提出了软件安全开发生命周期的模型SDL，并通过12个阶段的划分，把安全的理念、管理和技术融入到整个软件开发生命周期中。5.7小结3.软件安全检测技术软件安全检测技术包括静态安全检测技术、动态安全检测技术以及动静结合的安全检测技术三大类。其中，目前常用的静态安全检测技术包括词法分析、数据流分析、污点传播、符号执行、模型检查、定理证明等。软件的动态安全检测技术主要包括模糊测试、智能模糊测试和动态污点跟踪等。4.软件安全保护技术软件安全保护技术是指通过技术手段对受保护文件及其运行的环境添加防护和控制措施，使得受保护的软件在防护和控制范围内无法被逆向分析，从而在一定程度上防止软件被破解、篡改以及盗用版权。软件安全保护技术主要有基于软件技术的安全保护技术和基于硬件介质的安全保护技术，基于软件技术的安全保护技术包括注册信息验证技术、软件防篡改、代码混淆、数字水印、软件加壳、反调试反跟踪技术等。加密狗是广泛应用的一种基于硬件介质的软件安全保护技术。5.7小结5.恶意程序恶意程序是指恶意影响计算机操作系统、应用程序和数据的完整性、可用性、可控性和保密性的计算机程序。按传播方式，恶意程序可以分成以下几类：单一功能病毒，木马，蠕虫，恶意脚本、综合型病毒。调查发现，恶意程序主要通过网站挂马、诱骗下载、电子邮件、移动存储介质和局域网内传播等途径进行扩散传播的。针对恶意程序检测或查杀的主要技术包括特征码查杀、启发式查杀、基于虚拟机技术的行为判定，以及主动防御技术等。恶意程序的防范主要针对其传播方式和传播途径，采用对应的防范手段进行防护。6.Web应用系统安全针对Web系统的主要安全威胁包括：注入、跨站脚本、遭破坏的身份认证和会话管理、不安全的直接对象引用、伪造跨站请求等。Web系统的安全防护分为客户端安全防护、网络通讯安全防护和服务器端安全防护。Web系统的安全检测技术包括黑盒检测和白盒检测两种主要的检测技术。5.8习题简述软件漏洞概念中包含的三个要素？简述软件漏洞的四个特点？按照软件漏洞被攻击者利用的地点进行分类，软件漏洞可以分为哪几类？根据漏洞生命周期不同阶段进行划分，软件漏洞可以分为哪几类？简述软件漏洞危险等级的划分？简单说明国内外知名漏洞库及其包含漏洞信息的特点。介绍缓冲区溢出的概念？说明操作系统的内存管理机制？介绍堆溢出和栈溢出的原理？介绍格式化字符串漏洞、整数溢出漏洞的原理？介绍数组越界漏洞、写污点值到污点地址漏洞，以及内存地址对象破坏性调用漏洞的原理？介绍漏洞利用的概念和shellcode的编写方法？针对静态的shellcode地址、动态变化的shellcode地址分别说明其漏洞利用技术的原理？5.8习题说明针对堆漏洞的heap spray漏洞利用技术？说明微软操作系统中几种常用的漏洞防护技术？说明软件开发生命周期的概念和阶段划分？介绍软件开发生命周期的几种模型？说明微软公司采用的软件安全开发生命周期模型12个阶段的内容？说明主要的软件静态和动态安全检测技术？详细介绍基于软件技术的软件安全保护技术？说明恶意程序主要的传播技术？说明恶意程序的4种检测技术？介绍10种常见的web安全威胁手段？Q & A谢谢！第6章 信息安全管理第 6 章 概述6.1 信息安全管理体系6.1.1 建立信息安全管理框架6.1.2 ISMS架构的具体实施6.1.3 信息安全管理体系审核6.1.4 信息安全管理体系评审6.1.5 信息安全管理体系认证第 6 章 概述（续）6.2 信息安全风险管理6.2.1 关于风险管理6.2.2 风险识别6.2.3 风险评估6.2.4 风险控制策略6.3 信息安全管理措施6.3.1 基本安全管理措施6.3.2 重要安全管理过程6.1.1 建立信息安全管理框架◼ 定义信息安全政策信息安全政策作为组织的信息安全的最高方针，必须形成书面文件，做到人手一份◼ 定义ISMS的范围① 组织现有部门② 处所③ 资产状况④所采用的技术◼ 进行信息安全风险评估（1）基本风险评估（2）详细风险评估6.1.2 ISMS架构的具体实施◼ 建立相关文档①信息安全方针的阐述；②控制目标与控制方式描述；③程序或其引用。◼ 文档的严格管理组织必须对各种文档实行严格的管理，并要结合业务和规模的变化，对文档进行有规律、周期性的回顾与修订。◼ 安全事件记录、回馈组织应建立记录（Records）控制程序，对证明符合特性的记录进行标识、维护、保留和处置方面的控制。6.1.3 信息安全管理体系审核◼ 体系审核的概念体系审核是为获得审核证据，对体系进行客观的评价，以确定满足审核准则的程度所进行的系统的、独立的并形成文件的检查。◼ 审核准备审核准备是体系审核工作的一个重要阶段，准备阶段工作做得越细致，现场审核就越深入。◼ 纠正措施纠正措施（Corrective Action）是为消除已发现的不符合或其他不期望情况的原因所采取的措施。◼ 审核实施审核组在完成了全部审核准备工作之后，就可按预先约定的日期和时间实施审核。实施审核的步骤6.1.4 信息安全管理体系评审◼ 信息安全管理体系评审程序（1）编制评审计划（2）准备评审资料（3）召开评审会议（4）评审报告分发与保存（5）评审后要求◼ 体系评审与持续改进经过分析造成不符合的原因，制定改进的纠正和预防措施，进而实施并验证纠正或预防措施的有效性。6.1.5 信息安全管理体系认证◼ 信息安全管理体系认证的目的◼ 组织进行信息安全管理体系认证的目的，一般包括以下几方面：（1）获得最佳的信息安全运行方式；（2）保证商业安全；（3）降低风险、避免损失；（4）保持核心竞争优势；（5）提高商业活动中的信誉；◼ 信息安全管理认证的依据与范围BS77992：1999标准构成了BS7799信息安全管理体系评估的基础，并用作正式认证计划的基础。BS77992：1999第二部分被分成独立的三个部分6.2.1 关于风险管理◼ 概念◼ 风险管理是指找出机构信息系统中的漏洞，采取适当的步骤，确保机构信息系统中所有组成部分的机密性、完整性和有效性。本章介绍各种控制方法，讨论这些控制方法的分类，理解控制过程及其细节。◼ 要熟悉机构的资产及漏洞，必须理解孙子所言的第二方面：知彼，这意味着识别、检查并熟悉机构面临的威胁。必须确定出对机构和机构信息资产的安全影响最直接的威胁。6.2.2 风险识别◼ 资产识别和评估◼ 信息资产分类◼ 信息资产评估◼ 安全调查◼ 分类数据的管理◼ 威胁识别和威胁评估◼ 漏洞识别6.2.3 风险评估◼ 风险评估概述◼ 风险=出现漏洞的可能性×信息资产的价值当前控制减轻的风险几率+对漏洞了解的不确定性。◼ 信息安全风险评估原则◼ 安全改进是一个连续的过程，信息安全风险评估的结果为连续的改进奠定了基础 。◼ 风险评估的过程◼ 成 果 用 途信息资产分类表 集合信息资产以及它们对机构的影响或价值权重标准分析表 为每项信息资产分配等级值或影响权重漏洞风险等级表 为每对无法控制的资产漏洞分配风险等级6.2.4 风险控制策略◼ 当机构管理人员发现信息安全威胁的风险产生了竞争劣势时，就通过信息技术和信息安全利益团体来控制风险，一旦该团体建立了漏洞等级表，就可以选择4项基本策略中的一项来控制这些漏洞产生的风险。这4个策略如下：◼ （1）采取安全措施，消除或者减少漏洞的不可控制的残留风险（避免）。◼ （2）将风险转移到其它区域，或者转移到外部（转移）。◼ （3）减少漏洞产生的影响（缓解）。◼ （4）了解产生的后果，并接受没有控制或者缓解的风险（接受）。6.3.1 基本安全管理措施◼ 安全策略◼ 人员安全管理◼ 安全组织机构◼ 资产管理◼ 物理与环境安全◼ 通信及操作管理◼ 访问控制6.3.2 重要安全管理过程◼ 系统获取、开发和维护◼ 系统开发的目的是创建一个具有特定功能和性能的系统，用于完成或辅助组织的某项业务，支持组织业务目标的实现。为了保证整个组织的信息系统安全，必须保证系统开发过程的安全，以及所开发系统的安全性。◼ 信息安全事件管理与应急响应◼ 管理者的一个重要任务是计划。IT和信息安全团体的管理者通常需要提供策略计划，以确保信息系统的持续可用。◼ 业务连续性管理与灾难恢复◼ 灾难恢复计划（DRP）是为灾难（自然或人为）做准备和从灾难中恢复的计划。应急计划小组必须区分灾难和事故，但在攻击发生前，这是不可能区分出来的。一个事件最初归类为事故，但后来常常判定为一个灾难。