目录

项目 1 计算机网络安全概述

项目导入

伴随计算机技术的提高和互联网的迅速扩张，个人隐私数据、重要企业资源、政府文件等，都存放在计算机系统上，通过网络互通。同时，易用型操作系统和开发环境普及，黑客技术在全球范围内共享、网络攻击变得越来越便利。安全成为网络必须面对的一个重大问题。

任务 1.1 网络安全基础

任务描述

计算机网络安全是全社会都关注并亟待解决的一个大问题：如何保护自己的网络及网络系统中数据不被破坏或丢失，如何保证数据在传输过程中不被破坏或丢失，如何保证数据在传输过程中的安全，如何避免数据被篡改以保持数据的真实性。本项目详细介绍了与计算机系统安全有关的一些基础知识，为后续进一步学习网络安全攻击与防范打下基础。

任务目标

1. 了解网络安全的定义。
2. 掌握安全的三要素。
3. 了解风险及其相关概念。
4. 掌握常见的网络攻击方式与防范方法。

相关知识

1. 网络安全

网络安全目前使用最多的一种定义是：保护网络系统的软硬件及其中的数据，不因偶然或者恶意的原因遭受破坏、更改与泄露，网络系统能连续、可靠、正常地运行，提供的网络服务不中断。网络安全从其本质上来讲是信息安全的子集，从广义来说，是一种涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

2. 安全的平衡性

CIW（Certified Internet Webmaster）认为，安全的关键原则是：使用有效的，但是并

笔记

不会给那些真正想要获取信息的合法使用者增加负担的方案。

然而，要寻找出一条实际能满足此原则的途径是比较困难的，需要在系统安全性及其使用效果之间寻求平衡。使用过于复杂的安全技术会导致合法使用者厌烦，从而采取规避措施。考虑安全政策给合法使用者带来的影响，在很多情况下如果使用者感受到的不方便大于所带来的安全性的提高，则说明采用的安全策略实际上降低了网络的可用性。

安全可以降低效率但绝不能影响使用效果，因此需要寻找使用者能够方便访问网络资源和系统安全最优化之间的平衡点。

3. 安全的相对性

网络连通就意味着被攻击的危险，允许合法的使用者访问计算机或网络就存在着被误用或者滥用的危险。只有计算机与网络无连接并且被锁在一个安全的地方，再把钥匙销毁，才是真正绝对安全的计算机。尽管这种方法使得计算机得到很好的安全保护，但也使得它毫无用处。所以在现实生活中，没有绝对的安全，只有相对的安全。

安全策略是在保证可用性的情况下使安全风险带来的损害最小化。

4. 网络安全的三要素

谈到网络安全时，我们必须强调网络安全所追求的目标为 CIA 三要素：保密性、完整性和可用性。

安全评价标准（Security Evaluation Criteria），是网络安全的基本要素和网络安全建设所应遵循的基本原则。

（1）保密性（Confidentiality）：确保信息在存储、使用、传输过程中不会泄露给非授权用户或实体。

（2）完整性（Integrity）：确保信息在存储、使用、传输过程中不会被非授权用户篡改，同时还要防止授权用户对系统及信息进行不恰当的篡改，保持信息内、外部的一致性。

（3）可用性（Availability）：确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息及资源。

不同的机构和组织，因为其需求不同，对 CIA 三要素的侧重也会不同，如果企业最关心的是对私密信息的保护，就会特别强调保密性原则；如果组织最关心的是随时随地向客户提供正确的信息，那就会突出完整性和可用性的要求。

除了 CIA，信息安全还有一些其他原则，包括可追溯性（Accountability）、抗抵赖性（Non-repudiation）、真实性（Authenticity）、可控性（Controllable）等，这些都是对 CIA 原则的细化、补充或加强。

与 CIA 三元组相反的有一个 DAD 三元组的概念，即泄露（Disclosure）、篡改（Alteration）和破坏（Destruction），实际上 DAD 就是网络安全面临的最普遍的三类风险，是网络安全实践活动最终应该解决的问题。

5. 安全风险与威胁

信息安全本质上就是风险管理的工作，安全风险与威胁不可能完全避免，所以安全的关键在于如何控制、化解和规避风险。要了解什么是安全风险与威胁，我们必须首先了解“资产”这个概念。

1）资产

资产就是对组织有价值的任何东西，而与信息系统相关的有价值资产是信息安全的关注点。资产分为有形资产和无形资产。

笔记

（1）有形资产。有形资产是主要的保护对象，也是产生风险的主要来源，常见类型包括以下两种。

①物理资产：存储设备、服务器、计算机、网络设备、投影仪、应用软件、电话、传真机等。

②数据资产：财务数据、客户信息、雇员信息、网络拓扑图、战略规划、知识产权、隐私信息、培训资料、产品文档、技术白皮书等。

（2）无形资产。无形资产是难以定量的，不仅很难评估其价值，且会不可预料地产生严重风险，例如负面影响及客户口碑等。

2）资产识别

资产识别是风险评估和管理的第一步，资产识别的关键在于确定资产的价值。参考国际标准 ISO/IEC 17799，在确定资产价值时需要明确以下几点：

（1）资产清单。资产清单可帮助确保有效的资产保护，编制一份完整的资产清单是风险管理的一个重要的先决条件。组织要能够确定其资产、资产的相对价值和这些资产的重要性。根据该信息，组织可以提供与资产价值及其重要性相符的安全保护等级。应当为每个信息系统的重要资产都建立并保有一份资产清单。对于每种资产，都要清楚地确认其所有权和安全等级划分，资产目前所处位置（当需要恢复损失和毁坏的信息时，这点就非常重要）都应当得到批准并记录在案。

（2）资产价值。无论是有形还是无形资产都具有价值。确定资产的货币价值是安全风险管理的一个重要组成部分。因为组织管理层会根据资产的价值来决定应该花费多少时间与金钱保护资产的安全。为了向资产指定价值，需计算下列三个主要因素：一是对于组织该资产所具有的总价值；二是资产损失对财务的直接影响；三是损失该资产的间接业务影响。

（3）资产分类。应当将资产进行合理分类，指出其安全保护的需要、优先级和保护程度。资产的类别有助于安全风险整体影响的定义，它们能够帮助组织首先着重于对最关键的资产进行保护。

（4）资产负责人。组织内资产会与很多人相关，包括资产创建人、购买人、所有人、使用人、传递人，但最重要是确定资产的负责人。即资产指定的所有权人应当承担一定的责任，例如对公司发放给个人的工作用笔记本电脑通常会确定一个资产责任人，该笔记本电脑的转移、修理、报废都由该资产责任人负责。

3）风险

风险是特定的威胁利用资产的脆弱性造成对资产的一种潜在伤害，风险严重程度与资产价值的损害程度及威胁发生的频率成正比。

（1）风险分类。不同分类原则可以定义不同的风险，一般认为风险可分为固有风险、控制风险和残余风险。

①固有风险：指在没有任何控制措施下自身发生错误的风险。它是事物的本身特性，由意外驱动而发生的不可避免的风险。例如安装木门的房间比安装防盗门的房间更容易被盗。

②控制风险：指在控制制度下，仍无法预防、及时发现或纠正错误的风险。通常是由组织的管理层定义或控制的。例如在研发区域设置门岗以防止内部信息泄露，但仍然可能有部分内部信息通过其他方式被带出。

③残余风险：指采取安全措施对风险进行处理，提高了信息安全保障能力后仍然可能存在的风险。残余风险的来源有两个方面：一部分来自安全措施无效，在以后需要继续控

提示

任何信息系统都会有安全风险，所谓安全的信息系统，实质是指信息系统在实施了风险评估并做出风险处理后，残余风险可被接受的信息系统。

制这部分风险；另一部分则是在综合考虑了安全的成本与资产价值后，有意没有去控制的风险，这部分风险是可以被接受的。

（2）风险处理。由于风险是一种客观存在，它的存在与客观环境及一定的时空条件有关，是不以人的意志为转移的。因此风险不能完全消除，但可以降低、转移、接受。风险处理是一种系统化方法，《中华人民共和国国家标准——信息安全风险管理指南》指出可通过以下方式处理。

①风险避免：不介入风险，通过消除风险的原因或后果来规避风险，如关闭计算机上不提供服务的端口。

②风险降低：通过实现安全措施来降低风险，从而将脆弱性被威胁源利用后可能带来的不利影响最小化，如通过网络安全技术和控制对策来降低风险。

③风险转移：通过使用其他措施来补偿损失，如购买保险。

④风险接受：接受潜在的风险并继续运行信息系统，不对风险进行处理和控制，如在不安全的计算机上存放重要数据。

4）威胁

《中华人民共和国国家标准——信息安全风险管理指南》认为，威胁是一种对组织及其资产构成潜在破坏的可能性因素，是客观存在的。威胁会导致个人或者组织的资产损失，它可以是一个或者多个漏洞的组合。

威胁代理是利用系统漏洞的实体，它能够具备或者假装具备能力去导致、创建、传播以及支持威胁。如威胁是带病毒的文件，而威胁代理是有人打开了这个带病毒的文件。

威胁需要查看以往的安全事件记录情况，根据入侵检测情况和专家经验对信息系统存在的威胁进行识别，分析可能的威胁源、威胁动机和目的以及威胁源具备的能力情况，确定系统可能遭受的威胁。

（1）造成威胁的因素可以分为以下两种。

①人为因素：恶意或无意。

②环境因素：自然界不可抗因素和其他物理因素。

（2）从技术上分析，网络安全威胁的来源有以下几种。

①外部渗入者：未被授权使用计算机的人，如恶意黑客。

②内部渗入者：被授权使用计算机，但不能访问某些数据、程序或资源的人，包括冒名顶替（使用别人的用户名和口令进行操作）、隐蔽用户（逃避审计和访问控制的用户）。如窃取公司机密的内部员工。

③滥用职权者：被授权使用计算机和访问系统资源，但却访问或操作超出授权范围以外的数据。如误操作的雇员、驻场合作方。

（3）威胁直接作用于资产，造成潜在的危险和灾难，最终会增加资产损失的可能性，因此威胁会衍生出各种攻击方式。威胁通常分为有意威胁和偶然威胁，它们都会导致资产的破坏、暴露、篡改和中断。

①有意威胁：黑客、商业间谍、前任雇员等带有明确目的性造成的损失。

②偶然威胁：包括自然环境，如火灾、洪水、地震、海啸等；人类环境，如电力中断、烟雾、爆炸等意外发生的不可抗威胁，也包括系统设备错误、误操作、意外事件等。

5）漏洞

在信息安全管理中我们通常叫漏洞、弱点为脆弱性。广义的漏洞包括系统可能被威胁

利用的，在管理和技术方面的脆弱性情况。

笔记

《中华人民共和国国家标准——信息安全风险管理指南》对脆弱性的定义是：脆弱性是对一个或多个资产弱点的总称。弱点是资产本身存在的，如果没有相应的威胁发生，单纯的弱点本身不会对资产造成损害。而且如果系统足够强健，再严重的威胁也不会导致严重安全事件，即威胁总是要利用资产的弱点才可能造成危害。

威胁发生是由于信息资源存在脆弱性，脆弱性是信息资源的固有特性，其可以被威胁利用造成损害。

简言之，威胁就是攻破和损坏系统的潜在途径；而漏洞是在攻破系统过程中被利用的属性。理解威胁并最大限度地减少漏洞是任何组织信息安全管理的重要组成部分。

漏洞的特点有如下几个：

（1）不正确的、没有效率的或没有正确实施的安全措施本身就可能是一个漏洞。

（2）风险评估在完成威胁识别和价值计算后，就会围绕漏洞进行具体的分析和寻找缓解的方式。

（3）漏洞广泛出现在各种资产中，也囊括了管理制度，因此它是信息资源的固有特性。

（4）漏洞与威胁是概念上的互补，漏洞通常因被威胁利用而暴露，但不一定造成威胁。

（5）资产的脆弱性具有隐蔽性，有些漏洞只有在一定条件和环境下才能显现，这也是漏洞识别中最为困难的部分。

（6）漏洞识别将针对每一项需要保护的资产，找出可能被威胁利用的弱点，并对脆弱性的严重程度进行评估。这些数据应来自资产的所有者、使用者以及相关业务领域的专家和软硬件方面的专业人员。

漏洞分类主要依据系统的运行，从技术本身到配置维护再到管理控制进行分类。这是最符合信息安全管理体系要求的。依此，可以将漏洞分为技术漏洞、配置漏洞、管理漏洞三类。

6）风险评估技术

风险评估是风险管理的一种技术手段，根据当前信息安全的要求，风险评估不仅反映技术风险，还需要反映组织的运营风险、管理风险、法律风险等。风险评估已经成为一门涉及组织发展方方面面的、综合的、定量的以及定性的分析技术。

信息安全风险评估是指对信息系统及其处理的传输和存储信息的保密性、完整性和可用性等安全属性进行科学识别和评价的过程。风险评估是运用技术方法与手段对风险进行分析、评估确定风险结果并提出相应风险处理意见的过程。风险评估的方法分为定性的风险评估、定量的风险评估以及综合风险评估（结合定性与定量的方法）。

（1）定性的风险评估。在评估风险时，评估分析人员根据经验与业内实践为风险的各个要素进行大小、高低的定性分级。

定性分析方法是目前采用最为广泛的一种方法，它与定量风险分析的区别在于不需要对资产及各相关要素分配确定的数值，通常通过问卷、面谈及研讨会的形式进行投资收集和风险分析，它往往带有一定的主观性，需要凭借专业咨询人员的经验和直觉，或者业界的标准和惯例，为风险各相关要素（资产价值、威胁、脆弱性等）的大小或高低程度定性分级，如分为“高”“中”“低”三级。通过这样的方法，对风险的各分析要素赋值后，可以定性区分这些风险的严重等级，避免了复杂的赋值过程，简单又易操作。

（2）定量的风险评估。评估风险是明确分析风险几个要素的客观数字值，使得定量的

笔记

风险评估更具客观性，如用直接或者间接的商业价值来衡量资产的价值。

定量分析法，就是对风险的程度用直观的数据表示出来，主要思路是对构成风险的各个要素和潜在损失的程度赋予数值或货币金额度量风险的所有要素（资产价值、弱点级别、脆弱性级别等）都被赋值，计算资产暴露程度、控制成本以及在风险管理流程中确定的所有其他值时，尽量只有相同的客观性，这样风险分析的整个过程和结果都可以被量化。

任务实施

从理论上讲，通过定量分析可以对安全风险进行准确的评价与衡量。但是，使用定量分析的方法需要同各相关人员交流以了解并掌握其业务流程，这需要耗费大量的成本、大量的人力资源和时间来完成其全部周期，经常会出现员工对如何计算具体数值发生争论的情形，导致项目进展缓慢。从实际使用情况来看，单纯采用定量分析的案例并不多见。在风险评估过程中结合定性与定量对风险的赋值方式，综合使用对风险进行评估。

1. 风险评估分析方法

当前最常用的风险评估分析方法一般都是定量和定性的混合方法，对两者可以明确赋予数值的要素直接赋予数值，对难以赋值的要素使用定性方法，这样不仅更清晰地分析了单位资产的风险情况，也极大简化了分析的过程，加快了分析进度。

选择风险分析的方法和判断标准，应考虑组织特点，区别组织的关注点，灵活制订风险分析过程和分析方法。

通用的风险评估步骤如下：

步骤 1：识别资产。

步骤 2：识别漏洞与威胁。

步骤 3：分析可能性与影响。

步骤 4：确定风险。

步骤 5：编写风险评估报告。

尽管风险定量计算分析是非常困难的，但是毫无疑问，风险的定量是风险管理的核心，也是方法论发展的目标。

2. 风险后期处理

（1）在明确资产、威胁、漏洞的同时，还需要对风险进行分级，组织必须决定可以接受的风险。

（2）组织需要评估现有的控制措施。这些控制包括行为、设备程序、技术等。

（3）最终完成风险的处置，接受残余风险。

图 1-1 详细描述了风险、资产、脆弱性、威胁等各个因素的关系。

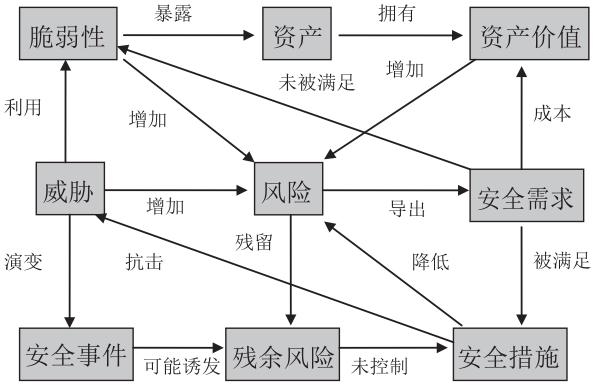


图 1-1　风险关系图

知识拓展

笔记

对常见的网络攻击手段进行分类，可以分为数据嗅探、非法使用、信息篡改、拒绝服务、社会工程、BUG 与恶意代码。

1. 数据嗅探

数据嗅探是了解目标网络各种信息的首要技术，通过数据报文、端口、服务、IP 地址等各种关键信息的扫描获得信息，并以此准备网络攻击。

嗅探技术是黑客和网络管理员最常用的工具和技术：

（1）抓取报文（抓包）。抓包即通过网络监听非法获取用户信息，如明文传输的用户名、密码。这类方法有一定的局限性，但危害性极大。监听者往往采用中途截击的方法来获取用户账户和密码。抓包实际上是在以太网卡处于混杂状态下通过专门的软件实现对数据包的获取过程，通常需要与端口镜像、HUB、分光器、TAP（Test Access Point）等紧密配合。常见的抓包工具有开源的 Wireshark（原 Ethereal）（见图 1–2）、Wildpackets 的 Omnipeek 等。

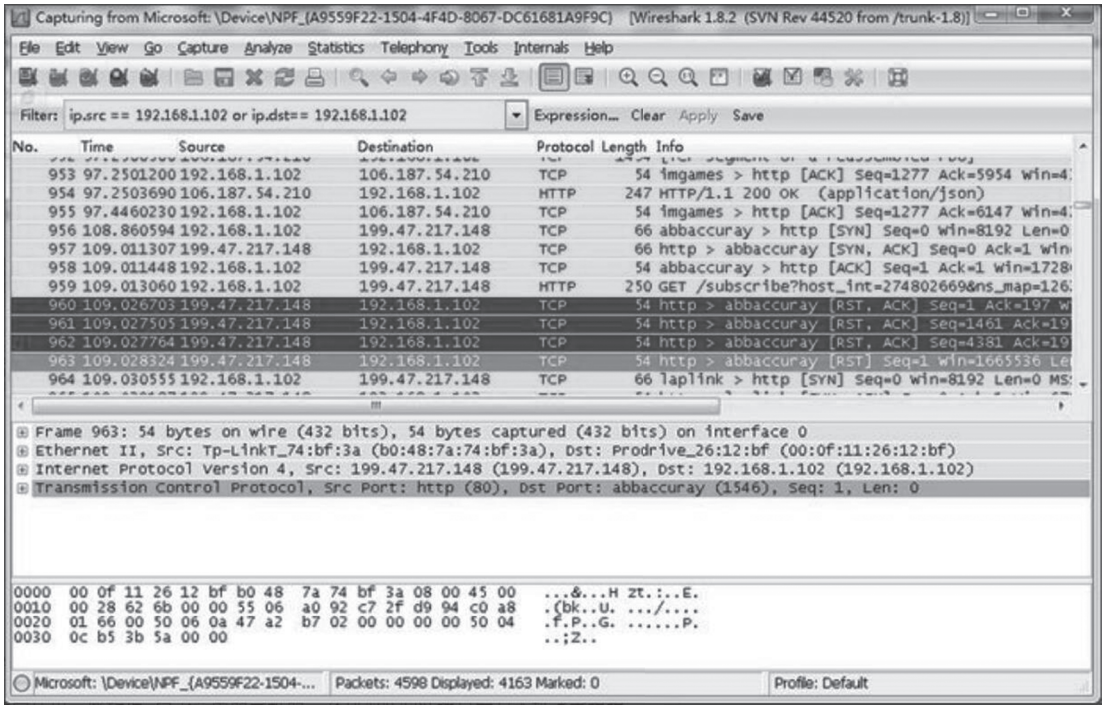


图 1–2　Wireshark 的操作界面

（2）扫描。扫描即通过发送报文探测网络中各种主机和服务的状态，准确了解网络中的资产和系统漏洞。一般分为端口扫描和漏洞扫描。

端口扫描通常使用一些软件，向大范围的主机的一系列 TCP/UDP 端口发起连接请求，根据应答报文判断主机是否使用这些端口提供服务。端口扫描仅能对接收数据进行分析，帮助发现目标主机的某些内在的弱点，而不能直接侵入目标系统。漏洞扫描主要包括以下两种方法：一是先使用端口扫描软件查看目标主机开启的端口，然后查看已有漏洞库是否有与该端口相关联的漏洞。二是模拟各种黑客攻击方法，对目标主机进行各种漏洞攻击，如测试是否有 IE 缓冲区溢出、弱势口令等，如攻击成功，则表明目标主机系统存在安全漏洞。

常见的这类工具有开源的远程扫描工具 NMAP、漏洞扫描工具 Nessus（见图 1–3）以

笔记

及一些商用软件，如 GFI LanGuard、Retina、CoreImpact、QualyGuard 等。

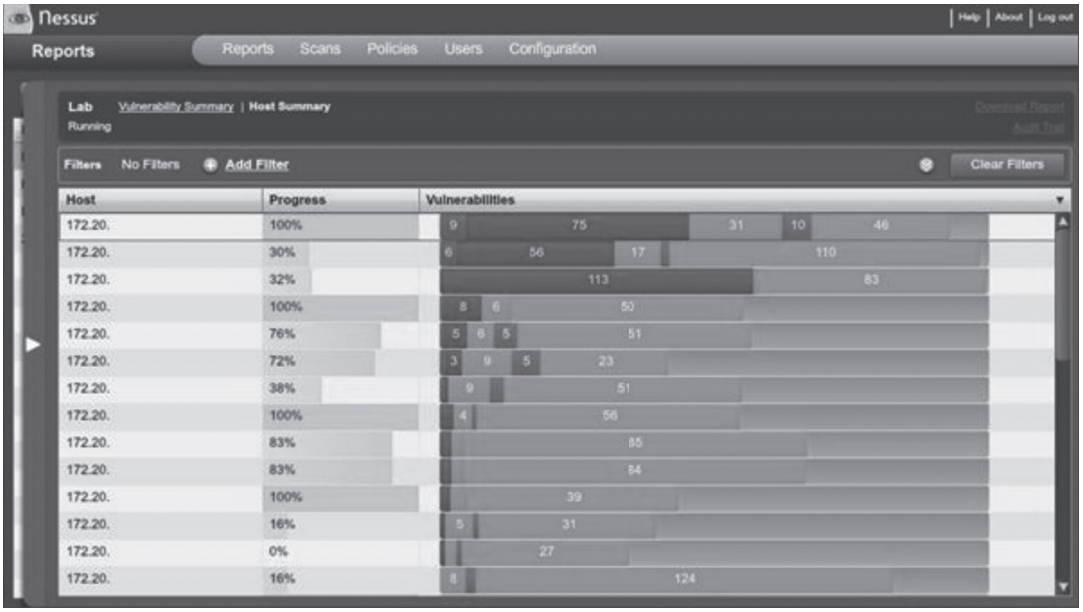


图 1-3　Nessus 运行界面

（3）操作系统标识。要想了解操作系统间处理 TCP/IP 协议的差异，需要向这些系统的 IP 端口发送各种特殊的包。通过 Banner Grabbing 获取操作系统的各种信息，根据这些系统对包的回应的差别，推断操作系统的种类。

例如开源工具 NMAP 中就包含有 350 种以上协议，如 SMTP、FTP、HTTP 等的约 3000 条模式匹配。

（4）电磁捕捉。电磁捕捉即通过捕捉屏幕、网线发出的电磁波，还原信息的嗅探手段，常用于攻击军事机构。

2. 非法使用

无论有意或者无意避开系统访问控制机制，对网络设备及资源进行非正常使用或擅自扩大权限，越权访问信息，都是非法使用的形式。

3. 信息篡改

信息篡改是指通过删除、修改、插入或重发某些重要信息等非法手段来获取对数据的使用权。

典型的数据篡改都发生在 Man-in-Middle 的情形下：

（1）Packet Replay（报文重放）：一种 Packet Injection 的方式，即捕捉到一个包后，向网络发回。通过所捕捉到的 login 信息，更改内容后重新发回，以获得控制权。

（2）Session Hijacking（会话劫持）：攻击者通过 Sniffing 或者 Brute force 等手段获得验证的 Token 进而劫持一个连接；让合法登录者误以为自己处于安全的操作状态，骗取登录者泄露自己的登录信息。

（3）篡改审计数据：删除、修改、权限改变、使审计的抗抵赖性失效。审计数据是监控和事后报告网络应用情况的重要数据，如果对审计信息进行篡改无疑会造成责任难以追溯。通常篡改审计数据的方式有截取审计日志和未授权进入数据库两种。

（4）主页篡改：攻击者可以利用漏洞进入 Web 网站数据库或者在 HTML 页面植入恶意代码，导致主页被篡改。当下未经授权对 Web 服务器进行攻击并涂改默认主页的攻击

活动越来越多，许多企业、政府和公司都遭受过类似的攻击。

4. 拒绝服务

DoS（Denial of Service）攻击，即拒绝服务攻击。DoS 攻击是网络上一种简单但十分有效的破坏性攻击手段，通过发送大量攻击报文导致网络资源和带宽被消耗，从而达到阻止合法用户对资源的访问。分布式拒绝服务（Distrubute Denial of Service，DDoS）攻击是 DoS 的升级版，它采用的是多对一的攻击方式，攻击原理与 DoS 一样。

（1）主要攻占目的。它不以获取资源为目的，而以破坏资源为目的。普通攻击都是欺骗被攻击主机，以获取被攻击主机的信任进而获取希望得到的信息。拒绝服务攻击不会欺骗被攻击主机，而是让被攻击主机不会为任何它信任的主机提供服务。

（2）主要攻击特点。不断对网络服务系统进行干扰，改变其正常的作业流程。执行无关程序使系统响应减慢甚至瘫痪、影响用户的正常使用，使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。但由于它利用了协议本身的弱点，因此无法完全预防。

（3）拒绝服务攻击原理。攻击者向被攻击服务器发送某项服务的请求，服务器将根据攻击者所发出报文中携带的信息给攻占行发送回复信息并等待攻击者确认。攻击者可通过各种手段（如伪造源地址）故意响应该回复的信息，那么服务器就会一直等不到回传的消息，分配给这次请求的资源就始终不会被释放。攻击者会不断传送新的一批请求，在这种反复发送请求的情况下，服务器资源最终会被耗尽。

DoS 伴随 Internet 公众服务的增加，也不断演变出各种攻击手段，令服务提供者防不胜防。现在常见的 DoS 攻击有 SYN Flooding、DNS poison、Land 攻击、CC 攻击、ping of death 等。这些攻击的共同点就是将攻击目标的资源耗尽，导致其无法提供正常服务。

5. 社会工程

人的因素是信息安全链条中最薄弱的一环。社会工程就是利用人的弱点（信任），通过欺骗手段而获得计算机系统信息的一种攻击手段，其特点如下：

（1）攻击者伪装成受信任的个体或者组织。

（2）实施简单，直接威胁信息安全。

（3）攻击技术容易复制而且扩展范围广、速度快。

6. BUG 与恶意代码

BUG 是一个程序（代码）的漏洞，它会产生一个隐藏的通道，很多情况下一个运行在服务器的操作系统或程序都会出现这些问题，攻击者经常研究并充分利用它们。以下是两种常见的 BUG：

（1）后门（Backdoor）。后门是一个在操作系统上或程序上未被记录的通道，它是程序设计人员为了便于快速进行产品支持有意在系统或程序中留下的入口。

（2）缓冲区溢出（Buffer Overflow）。利用缓冲区溢出攻击，可以导致程序运行失败、系统宕机、重新启动等后果。更为严重的是，可以利用它执行非授权指令，甚至可以取得系统特权，进而进行各种非法操作。

技能拓展

1. 缓解数据嗅探的威胁

（1）验证。身份验证是安全的第一道防线，因此强认证避免了非法用户进入网络进行数据嗅探的行为。强认证技术具备几个重要特点：①采用强密钥技术；②密钥不容易被复

笔记

提示

常见的攻击形式有：phishing（网络钓鱼）、E-mail 诈骗、电话访问、信任关系利用（Trust Exploitation）、物理攻击。

笔记

制；③密钥验证机制严密；④多因素验证；⑤抗重放攻击。

（2）改变网络结构。由于网络嗅探需要几个必要条件，如在同一冲突域、网络流量重定向到某个区域。因此如果能够合理规划网络环境中数据流的方向和接口，那么就延缓了攻击者嗅探网络关键数据流的效率。

（3）反嗅探工具。通过部署一些软件，利用网卡的混杂方式探测数据的技术。最广泛的是 Sentinel，其中 Sentinel 支持三种远程混杂探测模式：ARP 测试、Etherping 测试、DNS 测试。

① ARP 测试是发送一个 ARP 请求报文（其中的目的地址为伪造的）给需要探测的“目标”，如果“目标”网卡处于混杂模式，就会对这个 ARP 请求做出回应，而正常的网卡会丢弃这个 ARP 请求报文。

② Etherping 测试就是发送一个经过特别改造过的 ICMP Echo 报文（目标 MAC 地址是伪造的）给“被探测的目标”，处于混杂模式的目标可能会对这个报文做出反应。而正常网卡会丢弃这个报文。

③ DNS 测试就是发送伪造的主机信息，同时检测 DNS 请求报文来查看目标是否在请求解析这些不存在的主机。

除了以上方法还有一种方法也经常用于混杂模式探测，即反应时间测量，就是发送大量干扰伪造的报文给目标地址，如果目标网卡处于混杂模式，就会一一处理这些干扰报文，在发送干扰报文的同时 ping 目标，观察返回的时间间隔，来判断目标网卡是否处于混杂模式。

（4）加密。利用数据嗅探技术可以获取到对自己有用的数据，因此在无法完全杜绝嗅探攻击的情况下，最简单也是最有效的办法就是对数据加密。可以采用两种方法对数据进行加密，即数据通道加密（IPSEC）、数据文件加密（对称和非对称加密）。

2. 缓解非法使用的威胁

（1）过滤。使用访问控制技术可以对非法 IP 进行严格的控制，这是已经非常普及的控制方法，根据数据流的方向，防火墙等边界网关设备可以对由外到内的数据包进行过滤，也可以对由内至外的数据包进行过滤。当对由内至外的数据包进行过滤时，边界网关设备可对该数据包的源地址进行检查，如果该源地址不属于本地局域网，则将此报文过滤掉，不允许该报文离开。这种方法可以保证本地局域网无法发出 IP 地址欺骗攻击。如果每一个旧 IP 或局域网的网关都对出去的 IP 数据包进行 IP 源地址的检验和过滤，则 IP 地址欺骗攻击将没有用武之地。

（2）验证。采用非 IP 地址的方式强验证是防止基于非 IP 欺骗的最有效的技术，结合应用权限控制，还可以为溯源提供依据。常见技术和方法有双向验证（CHAP）、动态口令（One-time Passwords，OTP）、数字证书、令牌（Token）技术、验证码、Kerberos、生物识别等。

（3）加密。对于针对密码的攻击方式，只要加密算法足够“强壮”，同时采用强密码，任何攻击都是没有实效的。从理论上说，所有密文都是可以被破译的，但密码越长，加密算法越复杂，破译难度就越大。而每一段密文都是有时效性的，超出了这个时间段后，即使密文被破解成明文也没有意义了。

（4）关闭服务和端口。服务和端口在为用户提供支持平台和接口时，也成为攻击者的目标，因此关闭不需要的服务和端口是非常有必要的，如 25 端口（用于架设 SMTP 邮件服务器）、139 端口（用于提供 Windows 文件和打印共享）。许多木马程序可以通过 25 端

口监视计算机正在运行的窗口，而通过扫描目标计算机的 139 端口，攻击者可以尝试获取操作系统用户名、密码。

笔记

3. 缓解信息篡改攻击

信息篡改的本质是对信息进行修改，如果没有办法完全阻止信息在 Man-in-Middle 状态下被非法获取，最有效的方式还是通过各种加密算法，以确保其保密性、完整性和抗抵赖。常见的方法如下：

（1）明文加密：可以防止信息被破解。

（2）数据摘要：通过散列算法验证其未被修改，或者修改后能够被发现。

（3）数字签名。

4. 缓解 DoS 攻击

缓解 DoS 攻击的方式包括屏蔽 IP、流量控制、协议防范、侦测等。

5. 缓解社会工程攻击

对常用到的诱骗手段，如邮件、电话、网站链接等，可以采用相应的过滤技术。例如垃圾邮件可以采用黑白名单、贝叶斯算法、HASH 算法、关键字过滤、Sender ID 等技术来屏蔽；在电话欺骗中，应用反查技术验证和确认对方身份；针对网站链接，进行反钓鱼检测。

6. 缓解 BUG 和恶意代码攻击

BUG 和恶意代码的产生是无法控制的，我们只能采用措施防范 BUG 被利用或者恶意代码蔓延。主要有以下 4 种方法。

（1）补丁。补丁是伴随 BUG 和恶意代码出现的，它能及时解决系统的 BUG、清除恶意代码。补丁的获取一般有两条路径：

①部署自动分发系统，如企业内部的补丁分发系统及防恶意代码服务器自动更新特征库，这种系统一般包含在终端安全软件中。

②手动更新，需要我们能够关注各个厂商和安全研究机构对当前 BUG 和恶意代码的通告，及时了解各种攻击的缓解办法。

（2）定时扫描。由于互联网和软件开放性技术的普及，恶意代码产生越来越快，隐藏越来越深，带来的伤害也越来越大，因此我们对于很多 BUG 和恶意代码程序会出现漏报、漏杀的情况，必须自动或手动定时扫描，以了解整个系统服务、端口、账户、进程等的运行状况。

（3）审计。审计并不能防止攻击，但是能够记录恶意代码感染的过程，以及系统出现问题的连续信息，可以为安全工程师进行事后分析和总结提供全面的数据依据。

（4）终端保护。传统的主机保护是独立的，没有联动，也没有形成自愈的结构，因此采用终端保护的策略以及技术将更为关注主机安全，是建立基于网络的安全免疫体系的重要技术手段。而采取终端保护，可以将不符合组织安全基线的终端单独隔离，避免单个终端的安全问题影响整个系统。

提示

加强安全意识和技术培训是缓解社会工程的最好方式。教育应该是自上而下的，这样才能从管理层开始重视信息安全，提高 IT 应用的责任感。

任务 1.2　网络安全技术原理

任务描述

互联网技术的不断发展和信息化水平的不断提高，给人们的生活带来了极大的便利，但同时黑客攻击和信息泄露问题也给人们带来了巨大的威胁，因此网络信息安全问题已引

笔记

起人们的普遍关注。将信息加密技术应用于信息安全领域，在数据传输前完成加密处理，给数据安全增加了一道屏障，即使数据被不法分子窃取，也不会造成机密信息的泄露。

目前，为保护国家安全和公民隐私，世界各发达国家都越来越重视信息加密技术在计算机网络通信领域的应用研究。针对日趋严重的网络安全问题，本项目将信息加密技术应用在网络通信中，信息加密技术应用于数据信息传输有助于提高计算机网络安全水平。通过任务实施带领大家学习如何在信息加密技术概念和基本原理的基础上，掌握 DES 算法、MD5 算法、RSA 算法等经典信息加密算法，以及基于信息加密技术在数据库加密、软件加密、电子商务、虚拟网等计算机网络安全方面的应用方法，对信息加密技术在计算机网络安全中的进一步应用可以起到一定的促进作用。

任务目标

1. 了解加密技术原理及应用。
2. 了解访问控制技术原理。
3. 了解深度检测技术原理及应用。
4. 了解入侵检测防御技术原理及发展方向。
5. 了解 VPN 技术。
6. 掌握应对内网威胁的解决方案。

相关知识

1. 加密技术

密码学是研究如何隐秘地传递信息的学科，在现代特别指对信息及其传输的数学式研究，常被认为是数学和计算机科学的分支，与信息论也密切相关，随着计算机网络和计算机通信技术的发展，计算机密码学得到前所未有的重视并迅速普及和发展起来。在国外，它已成为计算机安全主要的研究方向，也是计算机安全课程教学中的主要内容。

密码是实现秘密通信的重要手段，是隐藏语言、文字、图像的特殊符号。密码通信是指用特种符号按照通信双方约定的方法把信息的原形隐藏起来，不为第三者所识别的一种通信方式。在网络通信中，通常采用密码技术将需要传输的信息隐藏起来，再将隐藏后的信息传输出去，使信息在传输过程中即使被窃取或截获，窃取者也不能正常读取信息的内容，从而保证信息传输的安全。

加密就是利用密码学的方法（即加密算法），使用密钥将明文信息转换成密文，使得无密钥者不能识别信息的真实含义，同时也不能对信息进行篡改、伪造或破坏。在开放的网络环境中，加密对于通信安全是非常重要的。信息加密技术是计算机网络安全技术的基础，为实现信息的保密性、完整性、可用性以及抗抵赖性提供了丰富的技术手段，对计算机网络的安全具有重要意义。

在信息密码学中，加密技术有 4 个要素：明文（Plaintext）、密钥（Key）、加密算法（Encrypt）和密文（Ciphertext）。

加密算法的表达式为 C=En（K，P）。

密码技术可以看作是一个复杂的函数变换，其中 C 代表密文，即加密后得到的字符序列；P 代表明文即待加密的字符序列，K 表示密钥，En 表示加密算法，是秘密选定的一个字符序列。

笔记

信息数据加密实质上是对以符号为基础的数据进行移位和置换的变换算法。从技术的角度来看，加密就是基于数学方法的程序和保密的密钥对信息进行编码，把计算机数据变成一堆看似杂乱无章难以理解的字符串，也就是把明文变成密文的一门科学。密码学作为数学的一个分支，其主要内容包括如下。

（1）密码编码学：使消息保密的技术和科学，是网络安全应用的研究方向。

（2）密码分析学：破译密文的技术和科学，是密码算法发展的研究方向。

在密码学中，密钥是一个关键的要素，如何保证加密后的密文不被非法用户窃取，取决于密钥的强度。密钥的强度通常由以下 3 个因素决定。

（1）算法的强度：算法是用于加密和解密的数学函数，是将明文转换成密文的数学方法。应该尽量使用工业标准的算法，因为它们已经被加密学专家测试过无数次，任何一个新的或个体的算法将不被信任直到它被商业化应用认证为止。

（2）密钥：密钥是具有确定长度的数字单元。如果密钥受到损害，那么算法将没有任何作用。因此，数据的保密程度直接与密钥的保密程度相关。注意区分密钥和算法，算法不需要保密。

（3）密钥强度：就是密钥长度，我们用密钥的位数来衡量，在密钥的长度上加一位则相当于一把可能的密钥的总数乘以 2 倍。简单地说，1 个长度为 n 的密钥，其可能的组合个数为 2 的 n 次方。例如，1 个 64 位长度的密钥，就是 2^{64} 种不同的密钥。

密码学的一个原则是“一切秘密寓于密钥之中”，加密算法可以公开，密码设备可以丢失，如果密钥丢失则信息将被完全破译。因此在加密完成后，可以将密文通过不安全渠道送给通信对方，但只有拥有解密密钥的接收方可以对密文进行解密进而得到明文。因此，密钥的传递必须通过安全渠道。

理论上讲，任何密钥都能被破解，目前论证了只有 1 种密码算法是理论上不可解的，那就是 OTP。这种算法要求采用一个随机的进制序列作为密钥，与待加密的二进制序列进行按位异或运算，其中密钥的长度不小于待加密的进制序列的长度，每一个密钥只能使用一次。除此之外的其他算法都是理论上可解的，加密的程度只是延缓了破解的时间。当加密算法产生的密文满足下列条件之一或全部条件时，则称加密算法是计算安全的（computationa secure）：破解密文的代价超出被加密信息的价值；破解密文需要的时间超出信息的有用寿命。

2. 加密技术发展史

加密作为保障信息安全的一种方式，不是现代才有的，它产生的历史相当久远，可以追溯到人类尝试去学习如何通信的时候。他们试图去寻找办法确保他们的通信秘密。但是最先有意识地使用一些技术方法来加密信息的可能是公元 6 年前的古希腊人。他们使用的是一根叫 scytale 的棍子，送信人先绕棍子卷一张纸条，然后把要加密的信息写在上面，接着打开纸送给收信人。如果不知道棍子的宽度（这里作为密钥），那么就不可能解密信里面的内容。

大约在公元前 50 年，古罗马的统治者恺撒发明了一种战争时用于传递加密信息的方法，后来称为“恺撒密码”。它的原理就是：将 26 个字母按自然顺序排列，并且首尾相连，明文中的每个字母都在字母表上向后（或向前）按照一个固定数目偏移后替换成密文，例如 Huaweisymantec 通过向后偏移 3 个字母加密后就变成了 KxdzhlvBPdqwhf。

近期加密技术主要应用于军事领域，如美国独立战争、美国内战和两次世界大战。在

笔记

美国独立战争时期，曾经使用过一种“双轨”密码，就是先将明文写成双轨的形式，然后按行顺序书写，例如：Huaweisymantec，先用双列书写：

s n h l

e d e p

然后按行书写，加密后的密文就是：

s n h l e d e p

图 1–4　Enigma 密码机

在第一次世界大战中，德国人曾依靠字典编写密码，例如：10-4-2，就是某字典第 10 页，第 4 段的第 2 个单词。在第二次世界大战中，最广为人知的编码机器是德国人的 Enigma 二转轮密码机（见图 1–4）。此后，由于 Alan Turing 和 Ultra 计划以及其他人的努力，终于对德国人的密码进行了破解，由此人为扭转了第二次世界大战的格局。

20 世纪，美国人对计算机的研究就是为了破解德国人的密码，当时的人们并没有想到计算机给今天带来的信息革命。随着计算机的发展以及运算能力的增强，传统密码的破解变得十分简单；同时，随着计算机在商业、个人等领域的不断扩展，使得商业或个人对数据保护、数据传输的安全性、防止信息被泄露等方面越来越重视，正是因为这些原因大大促进了加密技术的发展。在此背景下，美国人提出了公钥加密体系，从而使加密技术进入一个全新的发展阶段。

3. 对称加密算法

对称加密算法也叫传统密码算法（又称秘密密钥算法或单钥算法），就是加密密钥能从解密密钥中推算出来的算法。

对称加密算法是应用较多的加密算法，技术成熟。在对称加密算法中，数据发送方将明文（原始数据）和加密密钥一起经过特殊加密算法处理后，使其变成密文发送出去。接收方收到密文后，若想解读原文，则需要使用发送方加密用的密钥及相同算法的逆算法对密文进行解密，才能使其恢复成可读明文。在对称加密算法中，密钥只有一个，这种密钥既用于加密，也用于解密，叫作秘密密钥（也称为对称密钥或会话密钥），这就要求解密方事先必须知道加密密钥。

对称密钥加密是加密大量数据的一种行之有效的方法。

对称密钥加密有许多种算法，但所有这些算法都有一个共同的目的，以可以还原的方式将明文转换为密文。密文使用加密密钥编码，这对于没有解密密钥的人来说是没有任何意义的。由于对称密钥加密在加密和解密时使用相同的密钥，所以这种加密过程的安全性取决于是否有未经授权的人获得了对称密钥。特别注意：使用对称密钥加密的通信双方在交换加密数据之前必须先安全地交换密钥。

1）对称密钥算法体系

前文中提到，衡量对称算法优劣的主要尺度是其密钥的长度，密钥越长，在找到解密数据所需的正确密钥之前必须测试的密钥数量就越多。需要测试的密钥越多，破解这种算法就越困难。有了好的加密算法和足够长的密钥，如果有人想在一段实际可行的时间内逆

转转换过程，从密文中计算出明文，从应用的角度来讲，这种做法是徒劳的。对称密钥算法体系包括：

（1）明文（Plaintext）：这是原始消息或数据，作为算法的输入。

（2）加密算法（Encryption Algorithm）：对明文进行各种替换和转换。

（3）秘密密钥（Secret Key）：其也是算法的输入。

（4）密文（Cipher Text）：这是产生的已被打乱的消息输出，它取决于明文和秘密密钥，对于一个给定的消息，两个不同的密钥会产生两个不同的密文。

（5）解密算法（Decryption algorithm）：本质上是加密算法的反向执行，它使用密文和统一密钥产生原始明文。对称加密算法如图 1–5 所示。

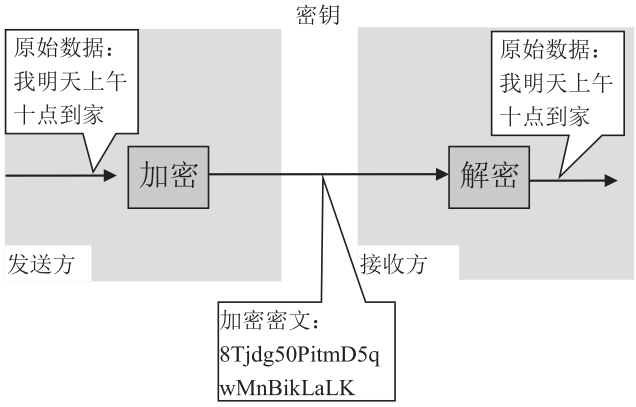


图 1–5　对称加密算法过程

对称加密算法过程用公式表示如下：

发送者用密钥 K 将明文 X 加密为 Y，这个过程表示为 Y=E[K，X]

接收者用密钥 K 将密文 Y 解密为 X，这个过程表示为 X=D[K，Y]，

对称加密的安全使用有以下 3 个要求：

（1）需要一个高强度加密算法。

（2）密钥要足够复杂。

（3）密钥的传递需要一个安全的方式。

2）对称算法

有很多特殊的数学算法来实现对称加密，具体包括以下两类算法：

（1）序列算法（Stream Algorithm），又称流加密算法，在算法过程中连续输入元素，一次产生一个输出元素。典型的流密码算法 2 次加密一个字节的明文，密钥输入到一个伪随机字节生成器，产生一个表面随机的字节流，称为密钥流。流加密算法一般用在数据通信信道、浏览器或网络链路上。

流加密算法的加密流程如图 1–6 所示。

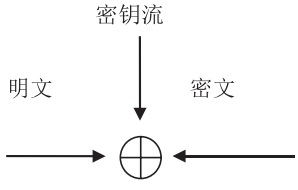


图 1–6　流加密算法示意图

笔记

常见的流加密算法是 RC4。RC4 是 Ron Rivest 在 1987 年为 RSA Security 公司设计的流加密算法。它是密钥大小可变的流密码，使用面向字节的操作，即实时地把信息加密成一个整体。

（2）分组算法（Block Algorithm），其输入为明文分组及密钥，明文被分为两半，这两半数据通过 n 轮处理后组合成密文分组，每轮的输入为上轮的输出；同时子密钥也是由密钥产生。典型分组长度是 64 位。

对称分组加密算法的具体操作取决于以下参数和设计属性。

①分组大小（Block Size）：在其他条件固定的情况下，越大的分组意味着越高的安全性，但降低了加密 / 解密的速率。典型的分组长度是 64 位。

②密钥大小（Key Size）：越长的密钥意味着越高的安全性，但会减小加密 / 解密的速率。普遍的密钥长度为 128 位。

③迭代轮数（Number of Rounds）：对称分组算法中单轮处理不能提供充分的安全性，多轮处理能提供更高的安全性。迭代轮数的典型值是 16。

④子密钥产生算法（Subkey Generation Algorithm）：子密钥产生算法的复杂度越高，密码被破译的难度就越大。

⑤轮函数（Round Function）：轮函数越复杂破译的难度就越大。

对称分组加密算法流程如图 1–7 所示。

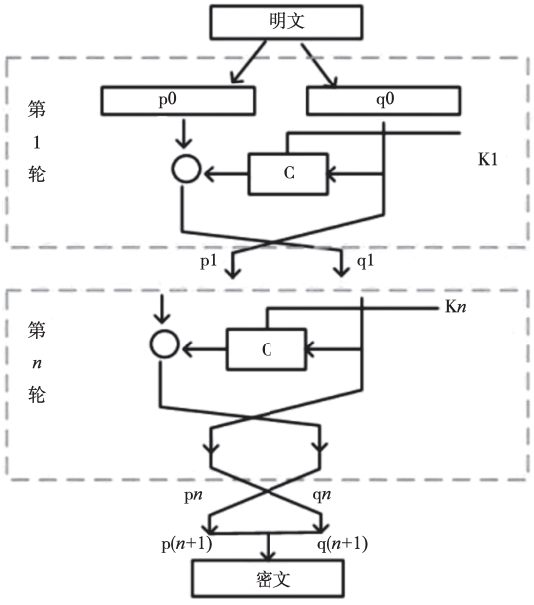


图 1–7　对称分组加密算法流程

常见的对称分组加密算法有 DES、3DES、AES 三种。

数据加密标准（Data Encryption Standard，DES）：DES 是第一个得到广泛应用的密钥算法，使用相同的密钥来加密和解密。DES 是一种分组加密算法，输入的明文为 64 位，密钥为 56 位，生成的密文为 64 位（把数据加密成 64 位的 block）。这种标准使用一种叫作 diffusion and confusion 的技术。每 64 位的数据被分成两半，并利用密钥对每一半进行运算（称作一次 round）。DES 运行 16 个 rounds，并对每个 round 运算所使用的密钥位数是不同的。DES 的优点是快速并易于实施。DES 提出并使用已超过 25 年，因此很多硬件和软件都使用

DES 算法。但是，密钥的传播和管理非常困难，因为 DES 依赖于单密钥模式。

三重数据加密标准（3DES，TripleDES）：DES 已经能够被现代的服务器暴力破解，因此不安全。TripleDES 使用了 168 位密钥解决了这个问题。这种情况下，信息先使用 56 位的密钥加密，然后使用另一个 56 位的密钥译码，最后再用原始的 56 位密钥加密，这样 3DES 使用了有效的 128 位长度的密钥。TripleDES 最大的优点就是可以使用已存在的软件和硬件，并且 DES 加密算法技术可以轻松地实施 TripleDES。

高级加密标准（Advanced Encwption Standard，AES）：相比较而言，DES 和 3DES 加密速度比较慢，因此 2001 年，NIST（National Institute for Standards Technology）发布了 AES，即 FIPS197。AES 采用 128 位的分组长度，支持长度为 128 位、192 位和 256 位的密钥长度，并可支持不同的平台。128 位的密钥长度能够提供足够的安全性，而且比更长的密钥需要较少的处理时间。到目前为止，AES 还没有出现任何致命缺陷。AES 取代 DES 和 3DES 以增强安全性和效率已是大势所趋。

3）对称密钥算法的优缺点

对称密钥的主要优点在于速度快，通常比非对称密钥快 100 倍以上，而且可以方便地通过硬件实现。其主要缺点在于密钥的管理复杂和缺乏抗抵赖性。由于每对通信者间都需要一个不同的密钥，n 个人通信需要 $n(n-1)/2$ 密钥；同时如何安全地传递密钥给信息接收方成为最大的问题；并且由于没有签名机制，因此也不能实现抗抵赖问题，即通信双方都可以否认发送或接收过的信息。

4. 非对称算法

非对称算法也叫公钥加密，其使用两个密钥：一个公钥和一个私钥，这两个密钥在数学上是相关的。在公钥加密中，公钥可在通信双方之间公开传递，或在公用储备库中发布，但相关的私钥是保密的。只有使用私钥才能解密用公钥加密的数据，相应地，使用私钥加密的数据只能用公钥解密。与对称密钥加密相似，公钥加密也有许多种算法。然而，对称密钥却完全不同，因此它们不可互换。而另一方面，不同公钥算法的工作方式数很容易相乘，而对得到的乘积反求其因子则很难。公钥算法的实际难度在于选择和生成私钥和公钥，下面是非对称算法如何生成私钥和公钥以及如何进行加密与解密的过程：

步骤 1：选择两个大素数 P、Q。

步骤 2：计算 N=P"Q。

步骤 3：选择两个公钥（加密密钥）E，使其不是（P–1）与（Q–1）的因子。

步骤 4：选择私钥（即解密密钥）D，满足下列条件：（D・E）mod（P–1）"（Q–1）=1。

步骤 5：加密时，从明文 PT 计算密文 CT 为：CT = PTEmoDN。

步骤 6：将密文 CT 发送给接收者。

步骤 7：解密时，从密文 CT 计算明文 PT 为：PT=CTDmoDN。

公钥算法的主要局限在于，这种加密形式的速度相对较低，实际上，通常仅在关键时刻才使用公钥算法，如在实体之间交换对称密钥时，或者在签署一封邮件的散列时（散列是通过应用一种单向数学函数获得的一个定长结果，对于数据而言，叫作散列算法）。

1）非对称密钥算法体系

非对称密钥算法体系包括以下内容：

（1）明文：它是可读的消息或数据，用作算法的输入。

（2）加密算法：加密算法对明文进行各种形式的变换。

笔记

（3）公钥和私钥：它们是被选择的对称密钥，如果一个密钥用于加密，则对另一个密钥当作解密。其中公钥是公开给其他人的，私钥只有自己知道。

（4）密文：它是输出的混乱的消息，取决于“明文和密钥”。对于给定的消息，两个不同的密钥将产生两个不同的密文。

（5）解密算法：该算法接受密文和匹配的密钥，并产生原始的明文。

2）非对称密钥原理

非对称加密算法原理如图 1–8 所示。

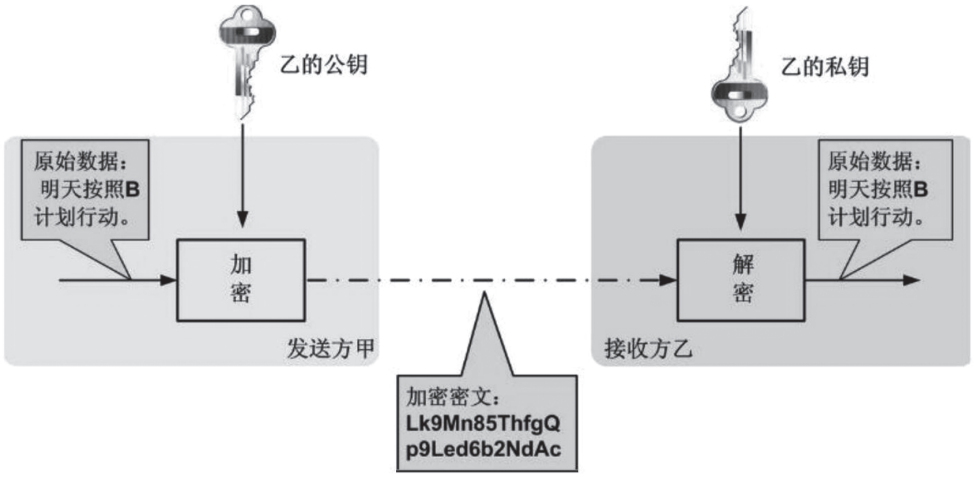


图 1–8　非对称加密算法原理

加密过程的基本步骤如下。

步骤 1：每个用户都生成一对密钥。

步骤 2 ：每个用户都把其中一个密钥放在一个公用的寄存器或者可访问的文件夹里，作为公钥剩下一个用户保存为私钥。每个用户都保存着别人的公钥。

步骤 3 ：如图 1–8 所示，如果甲要给接收者发送消息，则发送者在自己或者公共的公钥库里找出接收者的公钥 PU，用来将消息 X 转换为密文 Y，这个过程为 Y=E[PU，X]，然后将密文发送给接收者。

步骤 4 ：接收者收到密文 Y 后，用自己的私钥 PR 将接收到的密文 Y 解密为明文消息 X，这个过程表示为 X=D[PR，Y]，私钥只有接收者拥有，所以别人不能解密密文。

3）非对称密钥算法

非对称密钥算法有：RSA（Riveli Shamir Adlcman ）、DSA（Digital Signature Algorithm）、ECC（Elliptic Curve Cryptography）。

4）非对称密钥算法的优缺点

优点：可以公开加密密钥。为公钥加密提供了一种有效的方法，可用来把为大量数据执行对称加密时使用的秘密密钥发送给某人。

缺点：其主要局限就是速度。实际上。通常仅在关键时刻才使用公钥算法，如在实体之间交换对称密钥时，或在签署一封邮件的散列时。

对称和非对称密钥算法通常结合使用，用于密钥加密和数字签名，既实现安全需求又能优化性能。

5. 散列算法

散列算法又称哈希算法（HASH），就是把任意长度的输入（又叫作预映射，pre-

image），通过散列算法，变换成固定长度的输出，该输出就是散列值，或信息摘要（Hash-based Message Authentication Code，HMAC）。

笔记

哈希算法是一种压缩映射，通常 HASH 算法的输入空间远大于输出空间。数学公式为：

$$h = H(M)$$

其中，H( ) 代表单向散列函数，M 代表任意长度明文，H 代表固定长度散列值。

哈希加密并非用于加强信息的保密性，因为在 HASH 算法中，不同的输入可能会散列成相同的输出，要从散列值来唯一地确定输入值在理论上是不可能的。

1）散列算法加密原理

在通信的过程中，数据发送方通常对传输的数据进行 HASH 计算得到一个 HASH 值，并对该 HASH 值进行加密，将其与数据一同发送出去，接收方收到数据后对数据进行 HASH 计算，并比较收到的 HASH 值，如果相同则表示数据没有被损坏或被篡改。

哈希加密是通信的双方通过对比各自的哈希值，从而判断信息是否变更的方法，这可以运用在信息完整性的验证中。哈希加密的另外一种用途是签名文件。

2）散列算法举例

（1）信息 – 摘要算法（Message-Digestalgorithm 5，MD5）。MD5 是由 MD2、MD3、MD4 发展而来的一种单向函数算法（也就是 HASH 算法），可产生一个 128 位的散列值。它由 RSA 实验室的第一设计者 R.Rivest 于 20 世纪 90 年代初开发出来的。MD5 的最大作用在于，将不同格式的大容量文件信息在用数字签名软件签署私人密钥前“压缩”成一种保密的格式，关键之处在于这种“压缩”是不可逆的。MD5 设计经过优化用于 Intel 处理器。这种算法的基本原理已经泄露，这就是为什么它不太受欢迎的原因。

（2）SHA-1 算法。SHA-1 是流行的用于创建数字签名的单向散列算法。与 DSA 公钥算法相似，安全散列算法 1（SHA-1）也是由 NSA 和 NST 共同设计的，并由 NIST 将其收录到 FIPS 中，作为散列数据的标准。它可以将任意长度的字符串计算为 160 位的 HASH 值。SHA 在结构上类似于 MD4 和 MD5。尽管它比 MD5 的速度要慢 25%，但它更加安全。它产生的信息摘要比 MD5 要长 25%，因此对于预防攻击来说是更有效的。不过鉴于 SHA-1 的漏洞也已被发现，因此现已逐步推广更安全的 SHA-224、SHA-256、SHA-384 和 SHA-512。

任务实施

1. 加密技术的应用

数字签名（Digital Signature）在 ISO 7498-2 标准中定义为：“附加在数据单元上的一些数据，或是对数据单元所做的密码变换，这种数据和变换允许数据单元的接收者用以确认单元来源和数据单元的完整性，并保护数据，防止被伪造。”简单来说，数字签名主要的功能是：保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生。

基于公钥密码体制和私钥密码体制都可以获得数字签名，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、Fiat-Shamir Guillou-Quisquarter Schnorr Ong-SchnolT-Shamir 数字签名算法，Des/DSA、椭圆曲线数字签名算法和有限自动机数字签名算法等。特殊数字签名有盲签名、代理签名、群签名、不可否认签名、公平盲签名、门限签名、具有消息恢复功能的签名等。数字签名技术是公钥密码体制的典型应用。数字签名的应用过程是，数据源发送方使用自

笔记

己的私钥对数据校验和或其他与数据内容有关的变量进行加密处理，完成对数据的合法“签名”，数据接收方则利用对方的公钥来解读收到的“数字签名”，并将解读结果用于对数据完整性的检验，以确认签名的合法性。数字签名技术是在网络系统虚拟环境中确认身份的重要技术，完全可以代替现实过程中的“亲笔签字”，在技术和法律上有保证。在数字签名应用中，发送者的公钥可以很方便地得到，但其私钥则需要严格保密。

我们将公钥与散列算法结合可以实现一种数据交换协议，使得收发数据的双方能够满足两个条件：

（1）接收方能够鉴别发送方所宣称的身份。

（2）发送方事后不能否认他发送过数据这一事实。

数字签名可用作数据完整性检查并提供拥有私钥的凭据。签署和验证数据的步骤如下：

（1）发送者将一种散列算法应用于数据，并生成 1 个散列值。

（2）发送者使用私钥将散列值转换为数字签名。

（3）发送者将数据、签名发给接收者。

（4）接收者使用发送者的公钥对数字进行解密。

（5）发送者将该列算法应用于接收到的数据，并生成一个散列值。

（6）比较发送者发送的散列值与新生成的散列值是否相同。

（7）散列值相同则表示该消息来自发送者，并且消息未被篡改。

数字签名的原理如图 1–9 所示。

图 1–9　数字签名原理

数字签名能够实现：

（1）接收者能够核实发送者对报文的签名。

（2）发送者事后不能抵赖对报文的签名。

（3）任何人不能伪造对报文的签名。

（4）保证数据的完整性，防止截获者在文件中加入其他信息。

（5）对数据和信息的来源进行保证，以保证发件人的身份。

（6）数字签名有一定的处理速度，能够满足所有的应用需求。

其实公私密钥对的用法可以归纳为一句话：对于发送方来说，公钥用于加密，私钥用于签名，对用户而言这一过程是透明的。

笔记

2. 数字证书

随着网络上商业应用迅速发展，如网上银行、支付宝等电子商务应用对网络安全和网络信赖的要求越来越高。电子交易行为随处所见，为了确保交易的顺利进行，必须在互联网中建立并维护一种可以信任的环境和机制。为了应对这种对安全的需求，世界各国对其进行了多年的研究，初步形成了一套完整的 Internet 安全解决方案，即目前被广泛采用的公钥基础设施技术（Public Key Infrastructure，PKI），如图 1–10 所示。

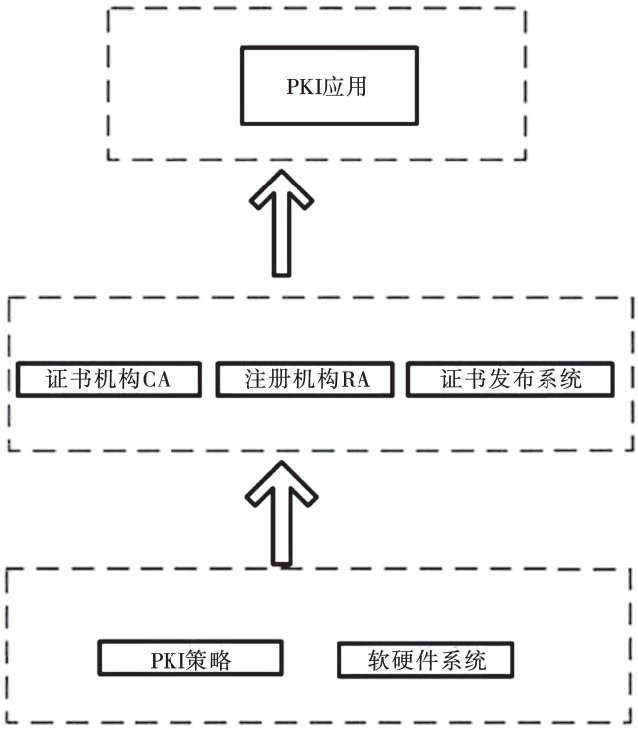


图 1–10　PKI 系统构成示意图

3. PKI 的应用

PKI 是一个用非对称密钥算法原理和技术来实现并提供安全服务的具有通用性的安全基础设施。实际上，PKI 在不同的场合代表不同的含义，一方面 PKI 是一系列提供安全基础框架的工具、技术、方法；另一方面它是公私密钥进行认证、加密的体系方法。PKI 支持在不安全的网络上传输安全信息，也支持在公司内网的私有网络上传输信息。不仅如此，PKI 还可以用来在用户方安全地传输密钥等。

一个典型的 PKI 系统包括 PKI 策略、软硬件系统、证书机构 CA、注册机构 RA、证书发布系统和 PKI 应用等。如图 1–11 至图 1–14 所示，分别为 PKI 系统中的 CA 级联结构示意图、CA 证书内容、查看本地证书及 CA 证书认证登录界面。

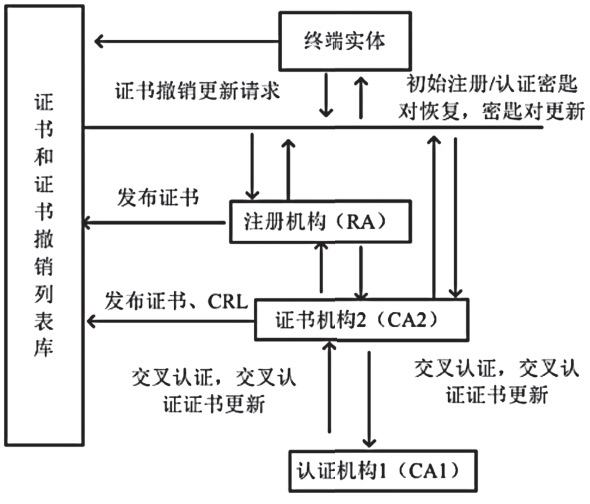


图 1–11　CA 级联结构示意图

证书版本格式	3
证书序列号	65436789
CA 签名算法标示	ShalRSA
签发 CA 名称	O=test, c=CN
证书有效期	2008-1-1 2009-12-31
证书持有者姓名	Cn=, O=test1, c=CN
证书公钥	ab78 3456 e3a2
证书扩展域…	keyusage=CHINA
CA 对证书的签名	0d27 29c4 052a

图 1–12　CA 证书示意图

笔记

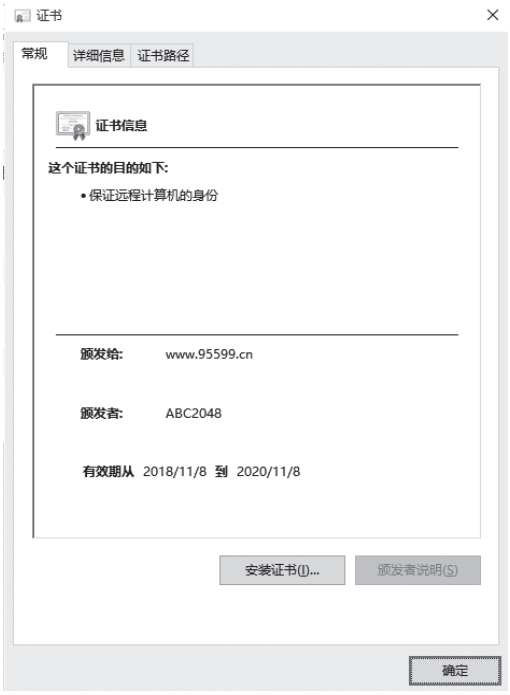


图 1-13　查看本地证书

图 1-14　CA 证书认证登录界面

知识拓展

1. 访问控制技术

访问控制是策略（Policy）和机制（Mecharism）的集合，它允许对限定资源的授权访同，它也可保护资源，防止那些无权访问资源的用户的恶意访问或偶然访问。

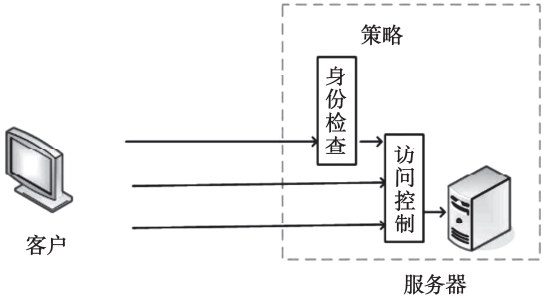


图 1-15　C/S 模式中的访问控制模型

C/S 客户 / 服务器访问控制模型如图 1-15 所示。

在图 1-15 中，把客户看成一个实体（实际上是一个人或者代表个人的应用操作），这个实体希望访问服务器的某种资源。访问主要包括读取数据、更改数据、运行程序、发起连接。资源可以是能够以某种方式（如读操作、写操作或者修改操作）对其进行操作的任何对象，也可以是那些被迫执行某种操作（如运行一个程序或者发送一个消息）的对象。总之，访问控制是为了限制访问主体（或称为发起者，是一个主动的实体，如用户、进程、服务等）、访问客体（需要保护的资源）的访问权限，从而使计算机系统在合法范围内使用。访问控制机制决定客户及代表一定客户利益的程序中能做什么，以及做到什么程度。

访问控制长信息安全保障机制的核心内容，是实现数据保密性和完整性机制的主要手段，是对信息系统资源进行保护的重要措施，也是计算机系统中最重要和最基础的安全机制。

访问控制系统涉及 3 个概念，即主体、客体和访问授权。

（1）主体：是一种可以使信息在客体之间流动的实体（如进程、作业、客户等）或能访问或使用客体的活动实体。

（2）客体：是一种能够从其他主体或客体接收信息的实体（文件、目录、数据块、记

录、程序、存储器段、网络节点等），既包含信息，又包含可以被访问的实体。

（3）访问授权：指客体对主体访问的允许，授权访问针对每一对主体和客体是给定的。对用户的访问授权是由系统的安全策略决定的，例如允许用户进行读 / 写操作。

在一个访问控制系统中，区别主体与客体很重要，主体和客体是可以互相转换的。首先，由主体向客体发起访问操作，该操作根据客体系统的授权被允许或拒绝。主体与客体的关系是相对的。

笔记

2. 访问控制策略

访问控制有三种策略：自主访问控制（Discreti onary Access Control，DAC）、强制访问控制（Mandatory Access Control，MAC）、基于角色的访问控制（Role-Based Access Control，RBAC）。各种访问控制策略之间并不相互排斥，现存计算机系统中通常都是多种访问控制策略并存，系统管理员能够对安全策略进行配置使其达到安全政策的要求。

1）自主访问控制（DAC）

自主访问控制，又称为随意访问控制，根据用户的身份及访问权限决定其访问操作，只要用户身份被确认后，即可根据访问控制表上赋予该用户的权限，进行限制性访问。在这种控制方法中，用户或应用可任意在系统中规定谁可以访问它们的资源，这样，用户或用户进程就可以有选择地与其他用户共享资源。自主访问控制是一种对单独用户执行访问控制的过程和措施。

由于 DAC 对用户提供灵活和易行的数据访问方式，能够适用于许多系统环境，所以 DAC 被大量采用，尤其在商业和工业环境的应用上。然而，DAC 提供的安全保护容易被非法用户绕过而获得访问。例如，若甲用户有文件 A 的访问权限，而乙用户没有文件 A 的访问权限，当甲用户获取 A 文件后再传送给乙用户，则乙用户也可以访问 A 文件。这是由于在自主访问控制策略中，当用户获得文件的访问权后，并没有限制其对该文件信息的操作，即并没有控制数据信息的转发。所以自主访问控制提供的安全性还相对较低，不能够对系统资源提供充分的保护，不能抵御类似特洛伊木马的攻击。

2）强制访问控制（MAC）

与自主访问控制相比，强制访问控制提供的访问控制机制无法被绕过。在强制访问控制中，每个用户及文件都被赋予一定的安全级别，用户不能改变自身或客体的安全级别，即不允许单个用户确定访问权限，只有系统管理员可以确定用户和资源组访问该文件。系统通过比较用户和其访问文件的安全级别来决定该用户是否可以访问。此外，强制访问控制不允许任何两个进程生成共享文件，从而防止进程通过共享文件将信息从一个进程传到另一个进程。强制访问控制可通过使用敏感标签对所有用户和资源强制执行安全策略，即实行强制访问控制。安全级别定义分为四级：绝密级（Top Secret）、秘密级（Secret）、机密级（Confidential）和无级别级（Unclassified），其中 T>S>C>U。

用户与访问的信息的读 / 写关系有四种，具体包括如下。

（1）下读（read down）：用户级别高于文件级别的读操作。

（2）上写（write up）：用户级别低于文件级别的写操作。

（3）下写（write down）：用户级别高于文件级别的写操作。

（4）上读（read up）：用户级别低于文件级别的读操作。

上述读 / 写方式都保证了信息流的单向性，显然上读—下写方式保证了数据的完整性，上写—下读方式则保证了信息的秘密性。

3）基于角色的访问控制（RBAC）

角色访问策略是根据用户在系统里表现的活动性质而定的，活动性质表明用户充当一

笔记

定的角色。

3. 访问控制机制

访问控制机制是为检测和防止系统中未经授权的访问，对资源进行保护所采取的软硬件措施和一系列管理措施等。访问控制一般是在操作系统的控制下，按照事先确定的规则决定是否允许主体访问客体，它贯穿于系统工作的全过程。访问控制矩阵（Access Control Matrix）是最初访问控制机制的概念模型，它利用二维矩阵规定了任意主体和任意客体间的访问权限。

访问控制矩阵中的行代表主体的访问权限属性，矩阵中的列代表客体的访问权限，矩阵中的每一格表示所在行的主体对所在列的客体的访问授权。

访问控制就是确保系统的操作是按照访问控制矩阵授权的访问来执行，它是通过引用监控器，来协调客体对主体的每次访问，这种方法清晰地实现了认证与访问控制的相互分离。

访问控制矩阵的形式如表 1-1 所示。

表 1-1　访问控制矩阵

用户	文件 A	文件 B	文件 C
用户甲	Own/R/W	R/W	R
用户乙	Rr	Own/R/W	
用户丙	R/W		Own/R/W

在较大的系统中，访问控制矩阵将变得非常大，而控制矩阵中的许多格可能都为空，造成很大的存储空间浪费，因此在实际应用时，访问控制很少利用矩阵方式实现。下面，我们将介绍在实际应用中访问控制的几种常用方法。

1）访问控制表（Access Control List，ACL）

访问控制表是以文件为中心建立访问权限表，如图 1-16 所示。在访问控制表中记录了某文件被授权访问的用户名及访问权的隶属关系。通过查询访问控制表，能够很清晰、准确地查找出对于特定客体的授权访问，主体可以访问哪些客体并有什么访问权限。同样如果需要撤销针对特定客体的授权访问，只要把客体的访问控制表置为空即可。

由于访问控制表的简单、实用，虽然在查询特定能够访问的客体时，需要遍历查询所有客体的访问控制表，但它仍然是一种成熟且有效的访问控制实现方法，许多通用的操作系统都使用访问控制表来提供访问控制服务。

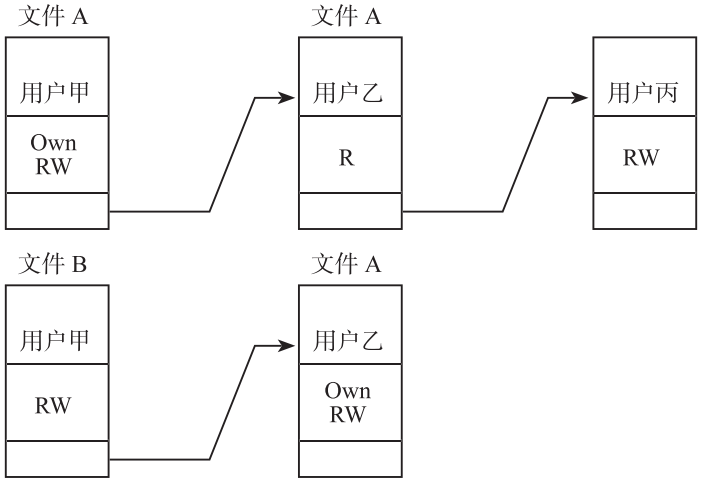


图 1-16　访问控制表

此处的访问控制表为访问控制技术中的模型，该模型在不同应用中有具体的实现方法。

2）能力关系表（Capabilities Lists）

能力关系表与 ACL 相反，是以用户为中心建立访问权限表，表中规定了该用户可访问的文件名及访问权限，利用能力关系表可以很方便查询两个主体的所有授权访问。相反，检索具有授权访问特定客体的所有主体，则需要遍历所有主体的能力关系表。

能力关系表如图 1–17 所示。

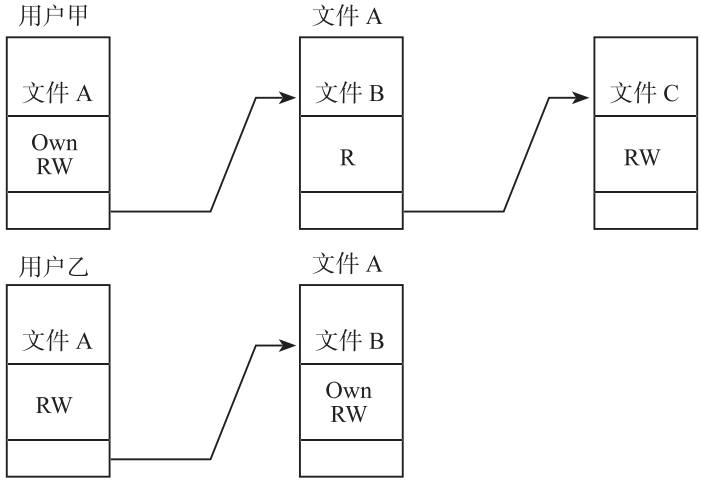


图 1–17　能力关系表

4. 深度报文检测技术

所谓深度报文检测技术（Deep Packet Inspection，DPI）是相对普通报文分析而言的一种新技术，普通报文检测仅分析 IP 包四层以下的内容。

针对不同的协议类型，识别技术一般可划分为以下三类：

（1）基于特征字的识别技术。

（2）基于应用层网关识别技术。

（3）基于行为模式识别技术。

行为模式识别技术通常用于那些无法由协议本身就能判定的业务。从 E-mail 的内容看，垃圾邮件（SPAM）业务流与普通邮件业务流没有区别，只有进一步分析才能识别出 SPAM 邮件。具体可通过发送邮件的速率、目的邮件地址数目、变化频率、源邮件地址数目、变化频率、邮件被拒绝的频率等参数，建立起行为识别模型，并以此分拣出垃圾邮件。

这一类识别技术分别适用于不同类型的协议，它们之间无法相互替代。综合运用这一种识别技术，即可高效、灵活地识别出网络上的各种应用。

DPI 的关键在于，它要不断地在格式不定的数据包中判断出各种特征字，实现这一过程搜索是否存在目标字符串的基础技术就是模式匹配（Pattern-Matching）。简单来说就是字符串匹配，即从数据中识别出业务类型后，高速转发这些业务数据流。从 DPI 的基本功能看，没有哪种器件能够兼顾识别和高速控制转发的双重要求。识别功能强调灵活性，主要 NP + 多核 CPU 很可能成为高端 DPI 的未来方向。采用多核 CPU 来实现，而控制转发强调高性能，NP 是最佳处理器。

5. 深度报文检测技术的应用

DPI 的主要应用包括如下几项。

（1）流量管理：控制 P2P 流量，防止这种“垃圾流量”占用太多带宽，从而影响其他

笔记

应用及网络资源使用的控制。

（2）安全：识别出并能抑制 DOS 攻击和其他恶意危害网络安全的行为。

（3）业务优化：个性业务和内容过滤。

（4）全局业务控制策略应用。

6. 入侵检测防御技术

1）异常检测模型（Anomaly Detection）

检测与可接受行为之间的偏差。如果可以定义每项可接受的行为，那么每项不可接受的行为就应该是入侵。总结正常操作应该具有的特征，当用户活动与正常行为有重大偏离时即被认为是入侵。这种检测模型漏报率低、误报率高。因为不需要对每种入侵行为进行定义，所以能有效检测未知的入侵。

2）误用检测模型（Misuse Detection）

检测与已知的不可接受行为之间的匹配程度。如果可以定义所有的不可接受行为，那么每种能够与之匹配的行为都会引起告警。收集非正常操作的行为特征，建立相关的特征库，当监测的用户或系统行为与库中的记录相匹配时，系统就认为这种行为是入侵。这种检测模型误报率低、漏报率高。对于已知的攻击，它可以详细、准确地报告出攻击类型，但是对未知攻击的检测却有限。

入侵检测过程分析分为三部分：信息收集、信息分析和结果处理。

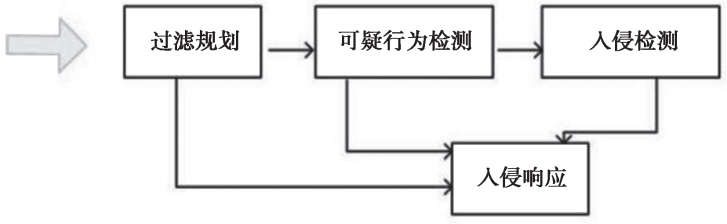
信息收集包括收集系统、网络、数据及用户活动的状态和行为。而且需要在计算机网络系统中的若干不同关键点（不同网段和不同主机）收集信息，这除了尽可能扩大检测范围的因素外，还有一个就是对来自不同源的信息进行特征分析之后比较得出问题所在。入侵检测收集的信息一般来自以下 3 个方面：

（1）系统和网络日志文件。

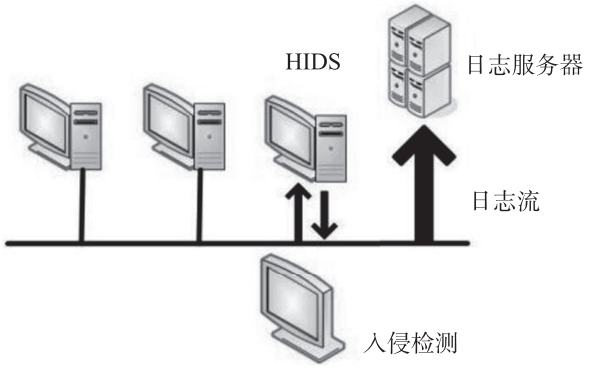
（2）非正常的目录和文件改变。

（3）非正常的程序执行。

网络结构及入侵检测相应流程如图 1–18 所示。

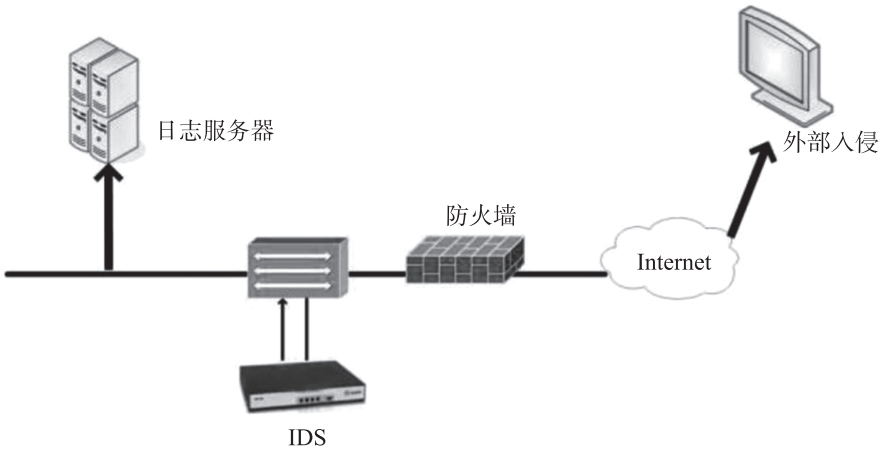


（a）

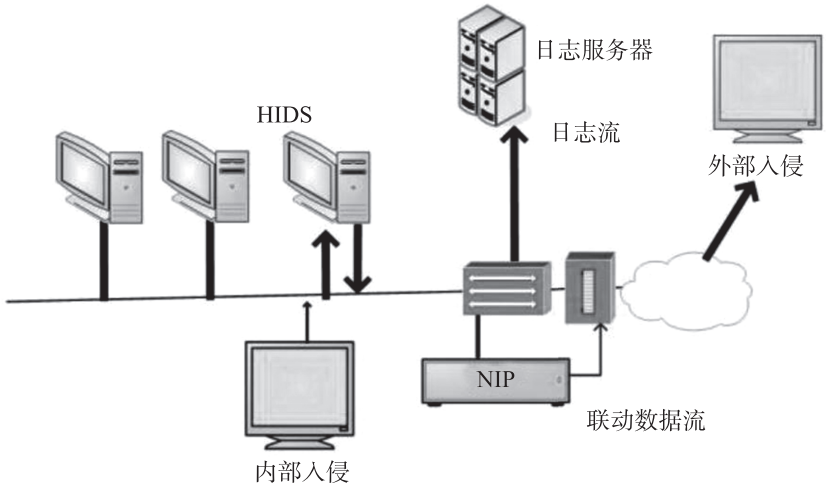


（b）

笔记



（c）



（d）

图 1-18　网络结构及入侵检测相应流程

7. 入侵防御技术

入侵防御技术（Intrusion Prevention System，IPS）检测是指针对检测到的网络中的攻击进行主动防御，在 IPS 设备上对攻击流进行处理。从对攻击流的识别技术来看，PS 和 IDS 采用相同的识别技术，IPS 设备接收数据流，以存储转发的方式来进行检测，如碎片重组、流重组、协议分析、状态检测等深度分析检测，对存在攻击的数据流进行实时处理。

典型的 IPS 网络结构如图 1-19 所示。

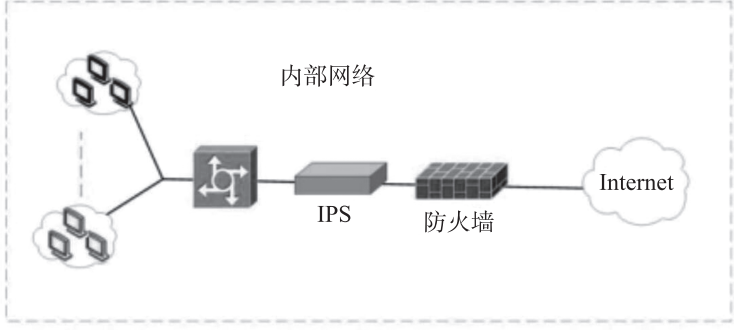


图 1-19　IPS 网络结构示意图

笔记

从图 1–19 可以看出，IPS 和 IDS 两者的部署方式不同，IDS 为旁挂方式，对网络也有比较大的影响。而 IPS 采用直路的方式，加入了单点故障，同时 IPS 设备的性能对网络影响比较小。

IPS 与 IDS 的对比如表 1–2 所示。

表 1–2　IPS 与 IDS 的对比

对比方式	IDS	IPS
部署方式	旁路部署 工作无延时 不增加单点故障	直路部署 存储转发，增进网络延时 增加单点故障
阻断方式	使用 TCL RST 切断会话，只能针对 TCP 链接	实时防御，阻断攻击流量
对比方式	IDS	IPS
误报，漏报率	取决于检测手段和特征库	检测技术同 IDS，但深入检测会增加设备开销，降低设备性能
监控范围	支持全网监控	监控流经 IPS 的流量，需要在每个出口部署一台
价格	相对较低	比较高

8. 入侵检测防御系统的不足和未来发展趋势

入侵检测防御系统有如此重大的作用，但在国内的应用远远谈不到普及，一方面由于用户的认知程度较低，另一方面是由于入侵检测是技术门槛较高的技术，不是所有商家都有研发入侵检测产品的实力。

目前的入侵检测产品大多存在下面的弱点：

（1）误报和漏报的矛盾。入侵检测防御系统对网络上所有的数据进行分析，如果攻击者对系统进行攻击尝试，而系统相应服务开放，只是漏洞已经修补，那么这一次攻占是否需要报警，就是一个需要管理员判断的问题，因为这也代表了一种攻击的企图。但大量的报警事件会分散管理员的精力，反而无法对真正的攻击做出反应。与误报相对应的是漏报，随着攻击的方法不断更新，入侵检测防御系统是否能报出网络中所有的攻击也是个问题。

（2）隐私和安全的矛盾。入侵检测防御系统可以收到网络的所有数据，同时可以对其进行分析和记录，这对网络安全极其重要，但难免对用户的隐私构成一定威胁，这就要看具体的入侵检测产品是否能提供相应功能以供管理员取舍。

（3）海量信息与分析代价的矛盾。随着网络数据流量的不断增长，入侵检测防御产品能否高效处理网络中的数据也是衡量入侵检测防御产品的重要依据。

（4）功能性和可管理的矛盾。随着入侵检测防御产品功能的增加，可否在功能增加的同时不增大管理的难度。

为解决入侵检测防御系统的不足，更好地改善入侵检测防御系统，人们在完善原有技术的基础上，只在研究新的检测防御方法，如数据融合技术、智能技术以及免疫学原理的应用等。主要的发展方向可概括为以下几点：

（1）分布式入侵检测。传统的入侵检测防御技术一般只局限于单一的主机或网络框架，不能适应大型网络的监测，不同的入侵检测防御系统之间也不能协同工作。因此，必

须发展大规模的分布式入侵检测技术。

（2）实时入侵检测。大量高速网络的不断涌现，各种宽带接入手段层出不穷，如何实现高速网络下的实时入侵检测防御成为一个现实的问题。

（3）高集成。入侵检测防御系统与其他安全产品相结合，提供完整的网络安全保障，形成入侵检测、网络管理、网络监控。

笔记

9. VPN 技术

虚拟私有网（Virtual Private Network，VPN）是近年来随着 Internet 的广泛应用而迅速发展起来的一种新技术，用以实现在公用网络上构建私人专用网络。“虚拟”主要指这种网络是一种逻辑上的网络。VPN 通过一个公用网络建立一个虚拟的、安全的连接，是一条穿过公用网络的安全、稳定的隧道。通常，VPN 是对企业内部网的扩展，通过它可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。

伴随企业和公司的不断扩张，员工出差日趋频繁，驻外机构及客户群分布日益分散，合作伙伴日益增多，越来越多的现代企业迫切需要利用公共 Internet 资源来进行促销、销售、售后服务、培训、合作及其他咨询活动，这为 VPN 的应用奠定了广阔市场。

1）VPN 的要求

（1）安全性：VPN 主要是带给用户一种私人专用的感觉，因此建立在不安全、不可信任的公共数据网的首要任务是解决安全性问题。VPN 的安全性可通过隧道技术、加密和认证技术得到解决。

（2）管理问题：VPN 是公司对外的延伸，因此 VPN 要有一个固定管理方案以减轻管理、报告等方面的负担。管理平台要有一个定义安全策略的简单方法，将安全策略进行分布，并管理大量设备互操作。

（3）互操作：企业的 VPN 产品应该能够同其他厂家的产品进行互操作。这就要求所选择的 VPN 方案应该是基于工业标准和协议的。这些协议有 IPSec、点到点隧道协议（Point to Point Tunneling Protocol，PPTP）、第二层隧道协议（Layer 2 Tunneling Protocol，L2TP）等。

2）VPN 的特点

VPN 并不实际存在，而是利用现有公共网络，通过资源配置而成的虚拟网络，只是一种逻辑上的网络。即在一般情况下，VPN 资源不会被承载网络中的其他 VPN 或非该 VPN 用户的网络成员所使用；另一方面，VPN 提供足够安全性，确保 VPN 内部信息不受外部侵扰，如 VPN 内部的网络拓扑、路由计算、成员的加入与退出等，因此 VPN 技术就比各种普通的点对点的应用机制复杂得多。

3）VPN 的优势

在远端用户、驻外机构、合作伙伴、供应商与公司总部之间建立可靠的安全连接，保证数据传输的安全性。这一优势对于实现电子商务或金融网络与通信网络的融合将有重要的意义。

利用公共网络进行信息通信，一方面使企业以明显更低的成本连接远地办事机构、出差人员和业务伙伴；另一方面极大地提高了网络的资源利用率，有助于增加 ISP（Internet Service Provider）的收益。

笔记

只需要通过软件配置就可以增加、删除 VPN 用户，无须改动硬件设施，这使得 VPN 的应用具有很大灵活性。

支持驻外 VPN 用户在任何时间、任何地点的移动接入，这将满足不断增长的业务需求，构建具有服务质量保证的 VPN，提供不同等级的服务质量保证，通过收取不同的业务使用费用可获得更多的利润。

总之，基于公共网络的 VPN 通过隧道技术、数据加密技术，使得 VPN 用户能够降低成本、提高效率、增强安全性。VPN 产品从第一代 VPN 路由器、交换机、集中器，性能不断得到提高。在网络时代，企业发展取决于是否最大限度地利用网络。VPN 将是企业的最终选择。

10. 内网安全技术

所谓内网，是对应于外网而言的，又称作局域网、LAN 和私网。LAN 是指在小范围内的计算机互联网络。这个“小范围”可以是一家人、一所学校、一家企业或一个政府部门。内网上的每台电脑（或其他网络设备）内部分配得到的局域网中 IP 地址在不同的局域网内是可以重复的，不会相互影响。

所谓外网，通常又称为广域网、WAN、公网，就是我们通常所说的 Internet，它是一个遍及全世界的网络。外网上的每一台电脑（或其他网络设备）外网 IP 一般需要通过 ISP 交费后才能申请到，并且不能重复。

局域网内通过交换机将服务器和用户连接在一起，因此局域网内信息的传输速率比较高，同时局域网采用的技术比较简单，安全措施较少，同样也给病毒传播提供了有效的通道和为数据信息的安全埋下了隐患。从网络架构到终端设备、从网络技术到用户常识的角度来分析局域网所面临的威胁如下：

（1）网络及安全设计问题。

（2）非授权访问。

（3）系统和软件漏洞。

（4）病毒和恶意攻击。

（5）局域网用户安全意识不强。

由此可见，相比于外网安全，内网安全具有以下特点：

（1）要求建立两种更加全面、客观和严格的信任体系和安全体系。

（2）要求建立更加细粒度的安全控制措施，对计算机终端、服务器、网络和使用者都进行更加具有针对性的管理。

（3）对信息进行生命周期的完善管理。

技能拓展

以 SQL 蠕虫、“冲击波”、震荡波等病毒的连续性爆发为起点，到计算机文件泄密、硬件资产丢失、服务器系统瘫痪等诸多客户端安全事件在各地网络频繁发生，可见安全管理已迫在眉睫。在规划内网安全时需要从边界安全、业务安全、终端安全三方面来考虑，一个全系列的内网安全解决方案如图 1–20 所示。

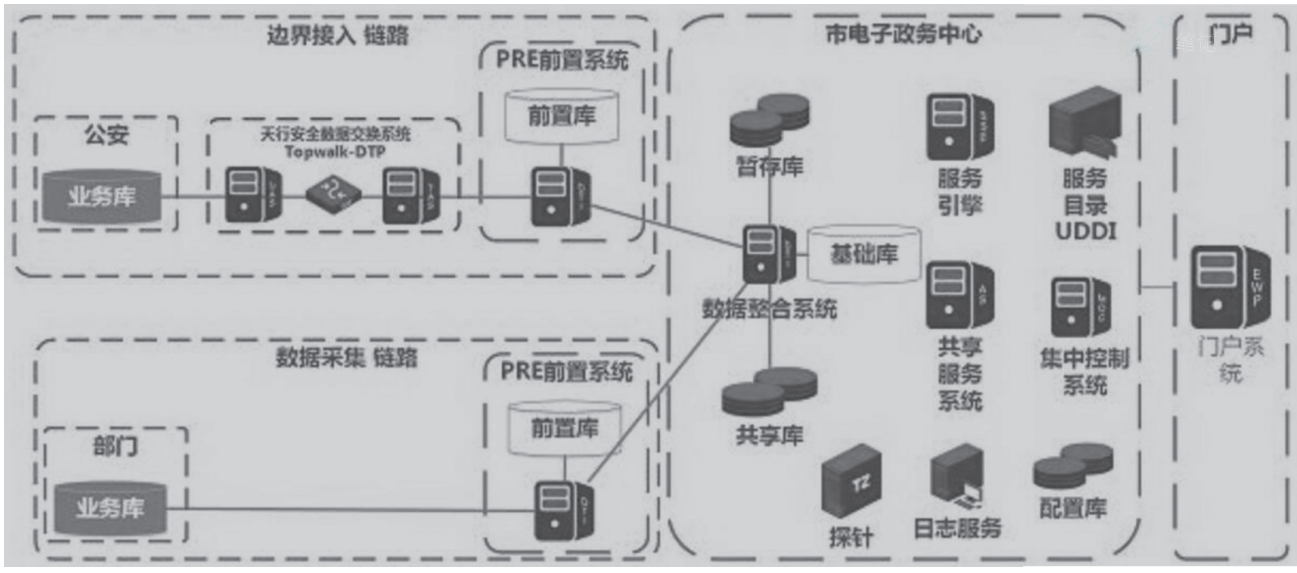


图 1-20　内网安全解决方案

1. 边界安全

边界防御可以抵御大部分外网攻击，而合理的网络架构是构建边界防御的前提条件。一个合理的网络架构首先应该考虑的是自身的业务、访问局域网的用户类型、局域网提供的业务类型等；另外需要进行风险评估，要明确企业自己的内网可能面临哪些风险，现有条件下对这些风险的承受程度如何。

企业应该在对于内网安全的投资和可接受的风险之间找一个平衡的位置，才能更好地规划内网安全。除了考虑业务系统重要程度和可接受的风险之外，另一个很重要的方面就是成本。

（1）在网络出口部署防火墙、入侵检测设备，降低外网对内网的安全威胁。

（2）部署 VPN，确保移动用户身份的合法性。

（3）在内部网络中，将不同业务类型的用户组划分在不同的 VLAN，在 VLAN 间访问进行策略限制。

2. 业务安全

在企业网络中存在的计费系统、V01P、带宽管理等类型的业务，如何保证不被非法使用保证企业收益至关重要；在 P2P、游戏、IM（Instance Message）等业务流行的网络环境中，如何保证带宽合理应用、员工高效率工作，也是企业领导关心的问题。针对业务安全的典型技术就是深度检测技术。

3. 终端安全

终端安全包含终端设备的安全和终端用户行为安全。企业可以通过以下方法来解决终端安全威胁：

1）完善的授权访问机制

非法访问、越权访问是企业面临的最重要的信息安全问题。完善的授权访问机制能够实现以下功能：

（1）隔离存在重大安全隐患的终端。

（2）进行用户身份认证，隔离未授权的外部用户，禁止授权用户越权访问。

笔记

（3）文档权限管理，包括文档加密、编辑权限管理。
（4）对终端移动存储设备进行管理。
（5）禁止未授权用户访问服务器。
（6）对网络访问提供审计。

2）完善的终端系统安全体系

（1）及时更新操作系统补丁。
（2）禁止终端安装非法软件。
（3）终端需要安装杀毒软件并及时更新病毒库。

3）完善的信息安全管理机制

（1）对敏感的用户行为进行监控。
（2）用户行为审计机制，对用户行为进行审计。
（3）加强信息安全学习，提高员工信息安全意识。