第 1 章　引　　论

1.1　信息安全问题的提出

20 世纪 60 年代以前，信息安全是指通信保密，采用的保障措施就是加密和基于计算机规则的访问控制，这个时期被称为通信保密时代。到了 20 世纪 90 年代，明确提出信息安全就是要保证信息的保密性、完整性和可用性，这个时期被称为信息安全时代。

信息安全时代的时代标志是 1977 年美国国家标准局公布的国家数据加密标准和 1983 年美国国防部公布的可信计算机系统评价准则。从 20 世纪 90 年代后期到现在，信息安全在原来的概念上增加了信息和系统的可控性、信息行为的不可否认性要求，同时，人们也开始认识到安全的概念已经不再局限于信息的保护，而需要对整个信息和信息系统的保护和防御，包括对信息的保护、检测、反应和恢复能力等。于是出现了信息安全保障的概念：为了保障信息安全，除了要进行信息的安全保护，还应该重视提高安全预警能力、系统的入侵检测能力、系统的事件反应能力和系统遭到入侵引起破坏的快速恢复能力。区别于传统的加密、身份认证、访问控制、防火墙、安全路由等技术，信息安全保障强调信息系统整个生命周期的防御和恢复，同时安全问题的出现和解决方案也超越了纯技术范畴。由此形成了包括预警、保护、检测、响应和恢复五个环节的信息保障概念，即信息保障的 WPDRR 模型，如图 1-1 所示。美国国家安全局制定的《信息保障技术框架》则是这个时代的一个典型标志。

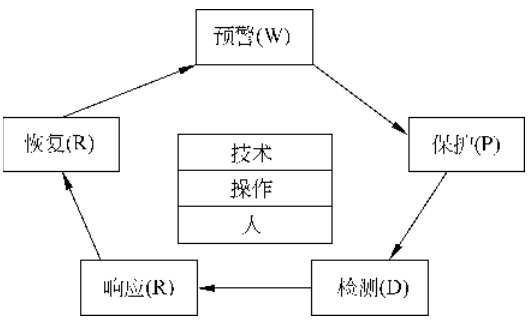

图 1-1　信息保障的 WPDRR 模型

信息安全保障的基本思想是深层防御战略。深层防御战略就是采用一个层次化的、多样性的安全措施来保障用户信息及信息系统的安全，在深层防御战略中，人、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，三者不可缺少；深层防御战略为在主机、网络、系统边界和支撑性基础设施等多个网络环节之中如何实现预警、保护、检测、反应和恢复这五个安全内容。

深层防御战略的含义是试图全面覆盖一个层次化的、多样性的安全保障框架。深层防御战略的核心目标就是在攻击者破坏了某个保护机制的情况下，其他保护机制依然能够提供附加的保护。深层防御战略的主要内容如下。

1. 主机及其计算环境

在主机及其计算环境中，安全保护对象包括服务器、客户机及其操作系统和应用系统。这些应用能够提供包括信息访问、存储、传输、录入等在内的多种服务。

根据信息保障技术框架对主机及其计算环境中的安全采用信息保障技术，确保用户信息在进入、离开或驻留客户机与服务器时具有保密性、完整性和可用性。客户机是作为终端用户工作站的附带外设的台式机与笔记本计算机，服务器则包括应用程序、网络、Web、文件与通信服务器。运行于客户机与服务器的应用程序包括安全邮件与 Web 浏览、文件传输、数据库、病毒、审计以及基于主机的入侵检测等应用程序。

对主机及其计算环境保护的目的如下所述：

(1) 建立防止有恶意的内部人员攻击的首道防线。

(2) 防止外部人员穿越系统保护边界并进行攻击的最后防线。

2. 操作系统

操作系统管理对内存、磁盘、数据端口和其他硬件资源的访问，同时操作系统也提供若干种基本的机制和能力来支持信息系统和应用程序的安全，如身份鉴别、访问控制、审计等。

目前主流的操作系统有 UNIX、Linux 和 Windows NT。这些操作系统都存在许多安全弱点，甚至包括结构上的安全隐患，如超级管理员/系统管理员的不受控制的权限、缓冲区溢出攻击、病毒感染等。操作系统的安全是上层应用安全的基础。提高操作系统本身的安全等级尤为重要，要对以下内容进行加强：

(1) 身份鉴别机制：实施认证方法，如口令、数字证书等。

(2) 访问控制机制：实施细粒度的用户访问控制、细化访问权限等。

(3) 数据保密性：对关键信息、数据要严加保密。

(4) 完整性：防止数据系统被恶意代码(如病毒)破坏，对关键信息进行数字签名技术保护。

(5) 系统的可用性：不能访问的数据等于不存在，不能工作的业务进程也毫无用处。因此操作系统要加强应对攻击的能力，如防病毒、防缓冲区溢出攻击等。

(6) 审计：审计是一种有效的保护措施，可以在一定程度上阻止对信息系统的威胁，并在系统检测、故障恢复方面发挥重要作用。

3. 基于主机的监视技术

基于主机的监视技术包括：检测并根除病毒等恶意软件；检测系统配置的改变；审计、审计消除与审计报告的生成。监视工具包括用户运行的反病毒软件等工具与系统管

理员运行的工具。例如，管理员为证实已经修补了系统漏洞、检测用户密码和监视用户访问权限而使用网络或基于主机的扫描工具。

4. 网络传输设施

网络是为用户数据流和用户的信息获取提供的一个传输机制。网络和支撑它的基础设施必须防止服务攻击。网络支持三种不同的数据流：用户、控制和管理。

(1) 传送用户数据流是建设网络的根本目的。网络通过物理或逻辑方式负责分隔用户数据流，如数据专线、VPN 等。网络也可能为用户提供保密性服务，如 IPSec 等。

(2) 控制数据流是为建立用户连接而必须在网络组件之间传送的控制信息。控制数据流是由一个信令协议提供的，如 7 号信令系统(SS7)，包括编址、路由信息和信令。其中路由信息决定用户信息流动的路径，信令控制用户的连接，而编址则是网络上设备的标识和最终寻找的根据，因此必须对网络中的控制信息加以保护。

(3) 管理数据流是用来配置网络元素或获取一个网络元素的信息。管理协议包括简单的网络管理协议(SNMP)、公共管理信息协议、超文本传输协议(HTTP)、rlogin 和 Telnet 命令行接口等。保护网络管理数据就是保障网络元素不被未授权用户更改。如果网络元素被非法通过管理手段破坏，那么攻击者就可以任意修改网络元素的配置和工作模式，网络的安全就得不到保障。

保护网络的技术有如下几种：

(1) 防火墙。

(2) 网络检测，包括入侵检测、漏洞扫描、病毒检测。

(3) 数据加密。

(4) 强认证功能。

(5) 数据完整性保护。

(6) 网络流量控制。

(7) 冗余、备份技术。

5. 应用程序

应用程序是运行于主机并可能涉及部分操作系统功能的软件。应用程序的安全是个很重要的问题，其解决方案必须有针对性，要依赖于具体的应用程序。对应用程序安全的考虑是：对于通用应用，如消息传递、文件保护、软硬件交付等，制定通用技术要求；对于特定的复杂应用，可分解为通用应用，同时考虑互操作性问题。

6. 网络边界

网络边界安全保护是指对进出网络边界的数据流进行有效地控制与监视的方法。有效地控制措施包括防火墙、边界护卫、虚拟专用网以及对于远程用户的识别与认证/访问控制。有效地监视机制包括基于网络的入侵检测系统、扫描器与局域网中的病毒检测器。网络边界采用的安全保护措施有如下几种：

(1) 防火墙。

(2) 物理隔离。

(3) 远程访问。

(4) 病毒/恶意代码防御。

(5) 入侵检测。

7. 支撑性基础设施

深层防御的一个基本原理是针对网络的入侵与攻击提供防范能力,并通过系统恢复有效地应对各种攻击。支撑性的基础设施是能够提供安全服务的一套相互关联的活动与基础设施。它所提供的安全服务用于实现框架式的技术解决方案并对其进行管理。目前的深层防御策略定义了两个支持性的基础设施。

(1) 私钥管理基础设施/公钥基础设施。用于产生、发布和管理密钥与证书等安全凭证。

(2) 检测与响应。用于预警、检测、识别可能的网络攻击、做出有效响应以及对攻击行为进行调查分析。

公钥基础设施技术发展迅速。快速建立一个大规模公钥基础设施应当采取如下策略,即建立一个数字标识符、篡改恢复、密钥恢复与归档等基本密码性能的简单基础设施。这样,政府部门、机构与公司便能够以此为基础建立具有访问控制等其他性能的基础设施。而此层面的检测和响应机制是建立在基于网络的检测和响应以及基于主机的检测和响应基础之上的,并构成一个层次化的报告和响应协调体系和机制。

坚持深层防御战略并不表明需要在网络体系结构的各个可能位置实现信息保障机制。信息安全保障是一个动态的概念,动态的概念体现在无论是在何种特定环境、特定时间下,深层防御战略都能通过在主要位置实现适当的保护级别,对各机构实现有效保护。

信息安全协议的建立和完善是安全保密系统走上规范化、标准化道路的基本因素。根据计算机专用网多年的经验,一个较为完善的信息安全保密系统至少要实现加密机制、验证机制和保护机制。目前,已经应用的协议有以下几种:

① 加密协议。有两个要素,一是能把保密数据转换成公开数据,在公用网中自由发送;二是能用于授权控制,无关人员无法解读。因此,数据要划分等级,算法也要划分等级,以适应多级控制的安全模式。

② 身份验证协议。这是上网的第一道关口,且与后续操作独立相关。因此,身份验证至少应包括验证协议和授权协议。人员要划分等级,不同等级具有不同的权限,以适应多级控制的安全模式。

③ 密钥管理协议。包括密钥的生成、分发、存储、保护、公证等协议,保证在开放环境中灵活地构造各种封闭环境。根据互联网的特点,密钥分粒度在网上要做到端级和个人级,在库中要做到字节级。

④ 数据验证协议。包括数据验证、数字签名。数字签名要同时具有端级签名和个人签名的功能。

⑤ 安全审计协议。包括与安全有关的事件,包括事件的探测、收集、控制,能进行事件责任的追查。

⑥ 防护协议。除防病毒卡、干扰仪、防泄射等物理性防护措施外,还对用于信息系统自身保护的数据(审计表等)和各种秘密参数(用户口令、密钥等)进行保护,以增强反入侵功能。

1.2 对信息的威胁和攻击的种类

1.2.1 信息泄漏

信息泄漏是偶然地或故意地获得(如侦收、截获、窃取或分析破译等)目标系统中的信息,特别是敏感信息,造成泄漏事件。这种威胁主要来自窃听、搭线和其他更加错综复杂的信息探测攻击。

1.2.2 信息破坏

信息破坏是指由于偶然事故或人为破坏,系统的信息被修改、删除、添加、伪造或非法复制,从而导致该信息的正确性、完整性和可用性受到破坏、修改或丢失。

1. 人为破坏的手段

(1) 利用系统本身的脆弱性。

(2) 滥用特权身份。

(3) 不合法的使用。

(4) 修改或非法复制系统中的数据。

2. 偶然事件的几种可能

(1) 硬、软件的故障引起安全策略失效。

(2) 工作人员的误操作使信息严重被破坏或工作人员无意地让别人看到了机密信息。

(3) 自然灾害的破坏。例如,洪水、地震、风暴、泥石流等使计算机系统受到严重破坏。

(4) 外界环境因素的突然变化。例如,高温或低温、各种污染破坏了空气洁净度,电源突然掉电或重系统信息出错、丢失或破坏。

1.2.3 计算机犯罪

20 世纪 40 年代以来,随着计算机首先在军事和科学工程领域的应用,计算机犯罪开始出现,美国学者埃德温·H.萨瑟兰开始分析和研究才智和现代技术工具的结合产生犯罪的可能性。他建议犯罪学家应将他们的注意力从传统犯罪转向利用技术和才智实施的犯罪。目前,计算机犯罪已成为现代社会一个严重的社会问题,对社会造成的危害也越来越严重,必须引起高度的重视。

1. 计算机犯罪的技术手段

计算机犯罪是利用暴力和非暴力手段,故意泄漏、窃取或破坏系统中的机密信息,危害系统实体和信息安全的不法行为。暴力手段是对计算机设备和设施进行物理破坏,例如,使用武器摧毁计算机设备,摧毁计算机中心建筑等。非暴力手段是利用计算机技术或其他技术进行犯罪活动,通常采用下列技术手段:

(1) 数据欺骗:非法篡改数据或输入假数据。

(2) 特洛伊木马术：非法装入秘密指令或程序，由计算机实施犯罪活动。

(3) 香肠术：利用计算机从金融信息系统中窃取存款，例如，窃取个人户头上的利息尾数以积少成多。

(4) 陷阱术：采用程序中为便于调试、修改或扩充功能而特设的断点，插入犯罪指令或在硬件中相应的地方增设供犯罪用的装置。总之，是利用计算机软、硬件的某些端点接口插入犯罪指令或装置。

(5) 逻辑炸弹：输入犯罪指令，以便在指定的时间或条件下，删除数据文件或破坏系统的功能。

(6) 寄生术：用某种方式紧跟享有特权的用户打入系统或在系统中装入“寄生虫”。

(7) 超级冲杀：用共享程序突破系统防护，进行非法存取或破坏数据及系统功能。

(8) 异步攻击：将犯罪指令掺杂在正常作业程序中，以获取数据文件。

(9) 废品利用：从废弃资料、磁盘、磁带中提取有用信息或进一步分析系统密码等。

(10) 伪造证件：伪造他人信用卡、磁卡、存折等。

2. 计算机犯罪的特点

(1) 作案手段智能化、隐蔽性强

大多数的计算机犯罪都是行为人经过狡诈而周密的安排，运用计算机专业知识从事的智力犯罪行为。进行这种犯罪行为时，犯罪分子只需要向计算机输入错误指令，篡改软件程序，作案时间短且对计算机硬件和信息载体不会造成任何损害，作案不留痕迹，使一般人很难觉察到计算机内部软件上发生的变化。

另外，有些计算机犯罪经过一段时间之后，犯罪行为才能发生作用而达到犯罪目的。如计算机逻辑炸弹，行为人可设计犯罪程序在数月甚至数年后才发生破坏作用。也就是行为时与结果时是分离的，这对作案人起了一定的掩护作用，使计算机犯罪手段更趋向于隐蔽。

(2) 犯罪侵害的目标较集中

就国内已经破获的计算机犯罪案件来看，作案人主要是为了非法占有财富和蓄意报复，因而目标主要集中在金融、证券、电信、大型公司等重要经济部门和单位，其中以金融、证券等部门尤为突出。

(3) 侦查取证困难，破案难度大，存在较高的犯罪黑数(dark figure of crime)

计算机犯罪数相当高，据统计，99%的计算机犯罪不能被人们发现。另外，在受理的这类案件中，侦察工作和犯罪证据的采集相当困难。

(4) 犯罪后果严重，社会危害性大

国际计算机安全专家认为，计算机犯罪社会危害性的大小取决于计算机信息系统的社会作用，取决于社会资产计算机化的程度和计算机普及应用的程度，其作用越大，计算机犯罪的社会危害性也越大。

3. 对计算机信息系统的违法犯罪行为及攻击的主要手段

(1) 窃听。

(2) 越权存取。

(3) 有害信息。
(4) 计算机病毒。
(5) 黑客。
(6) 因特网带来新的安全问题。

1.2.4 计算机病毒

随着因特网的发展,计算机病毒的发展主要表现在以下几个方面:
(1) 新病毒层出不穷,感染发作有增无减。
(2) 电子邮件已经取代磁盘成为病毒传播的主流途径。
(3) 传播速度大大加快,病毒已无国界。
(4) 病毒家族的种类越来越多。
(5) 病毒的破坏性不断增加。

1.3 密 码 学

随着计算机网络的普及,大量的数据通过网络传输到世界各地。但在具有重大的经济价值或关系国家机密等重要数据的传输过程中,任何一点泄露和差错都可能造成不可估量的损失。如何保证信息的机密性、真实性、不可否认性是密码学研究的热点问题。

密码技术是信息安全的保障及核心技术。计算机网络、通信技术的发展和信息时代的到来,给密码学提供了发展机遇,密码理论、密码技术、密码管理等研究与应用进入了一个新的时期。密码学是研究编制密码和破译密码的技术科学。研究密码变化的客观规律,应用于编制密码以保守通信秘密的内容,称为密码编码学;应用于破译密码以获取通信情报的内容称为破译学,也称为密码分析学,两者总称密码学。密码是通信双方按约定的法则进行信息特殊变换的一种重要保密手段。根据这些法则,变明文为密文称为加密变换;变密文为明文称为脱密变换。密码在早期仅对文字或数码进行加、脱密变换,随着通信技术的发展,对语音、图像、数据等都可实施加、脱密变换。密码学是对编码学和分析学这两门分支进行综合分析、系统研究的科学,是保护信息安全最主要的手段之一。密码学是在编码与破译的对弈中逐步发展起来的,并随着广泛的应用,已成为一门综合性的尖端技术科学。它与语言学、数学、电子学、声学、信息论、计算机科学等有着广泛而密切的联系。

进行明密变换的法则称为密码的体制。指示这种变换的参数称为密钥。它们是密码编制的重要组成部分。密码体制的基本类型可以分为四种。①错乱:按照规定的图形和线路,改变明文字母或数码等的位置成为密文。②代替:用一个或多个代替表将明文字母或数码等用密文代替。③密本:用预先编定的字母或数字密码组,代替一定的词组单词等变明文为密文。④加乱:用有限元素组成的一串序列作为乱数,按规定的算法,同明文序列相结合变成密文。上述四种密码体制,既可单独使用,也可混合使用,以编制出各种复杂度很高的实用密码。

20 世纪 70 年代以来,一些学者提出了公开密钥体制,即运用单向函数的数学原理,以实现加、脱密密钥的分离。加密密钥公开,脱密密钥保密。这种新的密码体制引起了密

码学界的重视。利用文字和密码的规律，在一定条件下，采取各种技术手段，通过对截取密文的分析，以求得明文，还原密码编制，即破译密码。破译不同强度的密码，对条件的要求也不相同，甚至很不相同。

现代密码技术已从传统的单纯保密功能发展成为一门具有加密与密码分析、数字签名、信息鉴别、身份认证、密钥管理、安全协议等多分支的综合学科。当前密码技术的研究领域非常广泛，主要涉及如下研究：

(1) 密码学的信息理论和计算机复杂性理论的研究，如密码中信息泄露的发现和利用、安全密码体制的准则和评测。

(2) 公开密钥密码理论的研究，寻找可构造的公开密钥算法，椭圆曲线公钥密码算法等密码算法的快速实现。

(3) 对称密码理论的研究，如对称密码的设计准则和评测等。

(4) 新型安全密码算法的研究，如量子密码、混沌密码理论、DNA 密码、信息隐藏技术等。

(5) 密码安全协议的研究，如数字签名、身份鉴别、数据完整性、密钥管理、秘密共享等设计理论和方法，虚拟专用网络技术，计算机网络通信安全技术等。

1.4 信息安全的重要性

(1) 由于因特网的开放性以及企业信息系统基本都采用开放性的系统平台，包括网络、操作系统和数据库系统等，系统的弱点成为更容易被攻击的环节。如通过因特网可以非常容易地获取各种黑客工具，这使得黑客进行攻击所需要的技能比以前降低，由此带来了更大的潜在黑客群体。

(2) 安全漏洞成倍地增长。例如，微软 2005 年为 IE 浏览器软件提供了 80 多个安全漏洞的补丁，然而，还有 30 多个 IE 浏览器软件的安全漏洞没有提供补丁。这些安全漏洞就能够让恶意的代码进入到企业的计算机或网络。

(3) 随着因特网的普及，一些日益增长的威胁包括伪装成可以合法下载的文件和广告软件。许多人从网上下载的文件以为是.jpeg 或.mpeg 图像文件，其实这些文件有可能包含特洛伊木马程序，允许文件的制作者无限制地访问计算机。广告软件虽然不破坏计算机，但是，这种软件可以侵犯隐私，这种软件常常是在用户下载其他软件时一同下载的。这种软件监视用户访问的每一个网页并且根据其兴趣爱好制作一个图表，这样就能提供适合的广告。

因此，一方面由于信息系统的开放性以及安全性不足，另一方面各种攻击手段和工具不断出现并且易于获得，并且企业网络面临的黑客攻击风险的发生概率与其业务性质有关，其应对措施必须是避免并在实际风险发生后要尽快尽量减少风险的破坏后果。因此，保障信息安全是十分重要的。

(4) 不管公司内部连接的是至关重要的公司数据库，还是仅仅承担公司内部的电话呼叫与电子邮件的传输服务，保证网络上的信息安全都是非常重要的工作。如果一个公司通过 WAN 连接到网络上进行销售或采购时，每一分钟的掉线都将给公司带来成千上

万的损失。

(5) 网络存在的问题主要有以下三类：

① 机房安全。机房是网络设备运行的关键地，如果发生安全问题，如物理安全(火灾、雷击、盗贼等)、电气安全(停电、负载不均等)等情况，必定影响信息的安全。

② 病毒的侵入和黑客的攻击。网络开拓性的发展使病毒可能成为灾难。黑客对计算机网络构成的威胁大体可分为两种：对网络中信息的威胁；对网络中设备的威胁。以各种方式有选择地破坏信息的有效性和完整性；进行截获、窃取、破译，以获得重要机密信息。

③ 管理不健全而造成的安全漏洞。从广泛的网络安全意义范围来看，网络安全不仅仅是技术问题，更是一个管理问题。它包含管理机构、法律、技术、经济各方面。网络安全技术只是实现网络安全的工具。因此要解决网络安全问题，必须要有综合的解决方案。

1.5 信息安全的任务

信息安全任务包括可获得性、授权与密钥管理、身份识别与完整性。

1. 可获得性

网络中的结点具有可移动性，所以网络拓扑不固定更容易受到拒绝服务攻击。阻塞无线信道，或者发送虚假的路由信息，就可以达到破坏的目的。需要特别指出的是，现有的路由协议没有考虑安全机制，安全的路由协议必须能够处理网络拓扑的变化，并且可以删除恶意用户发送的虚假路由信息。可获得性的另一个威胁是能源消耗攻击，目前对能源消耗攻击还没有行之有效的办法。

2. 授权与密钥管理

授权与密钥管理也是个复杂问题，由于网络没有固定拓扑，无法确定业务授权中心。同时，如果网络中结点数目较多，并且移动性较强，就会造成认证机制相对复杂，这需要第三方介入。

3. 身份识别与完整性

由于无线信道的开放性，如果不对信道进行加密将使信息暴露给外部用户。但是如果没有完备的认证机制，就不能完成通信单元的身份识别，而信道的加密也变得毫无意义。所以，一旦建立完备的认证机制，身份识别与信道加密问题就会迎刃而解。信息的完整性的保护必须建立在对无线通信链路的防护基础之上，从某种意义上来说，信息的完整性同样建立在认证机制的基础上。

1.6 信息安全的对策与措施

1.6.1 信息安全的对策

基于信息保障深层防御战略思想，并结合长期的信息安全系统建设实践经验，将网络安全划分为三个模块来全面考虑：主机、网络传输设施和网络边界，并将预警、保护、检

测、反应和恢复这五个安全环节体现到具体的系统建设的部署之中。

1. 系统边界

网络边界是外部入侵的突破口，保护网络的边界就是限制或隔断了黑客从外部攻击的可能性。最容易理解的网络边界是本网络和其他网络的连接接口，包括因特网或其他企业网络。对企业内部来说，其任何一个应用也存在和其他应用系统的连接接口，如财务部门和技术部门之间，这种形式的边界也是网络安全要着重考虑的环节。

最常见的边界保护措施就是防火墙，防火墙确保内部网络与外部非信任公共网络的安全隔离。防火墙通过监测、限制、更改数据流，可以保护系统不受来自外部或其他部门的攻击。随着网络安全技术的整体发展和网络应用的不断变化，防火墙技术已经融入了许多增值功能，例如 VPN、入侵检测、病毒查杀等。

为了考虑在家用户、出差人员或远程办事机构人员访问内部网络系统的需求，传统的解决办法是在内部网络配置网络拨号服务器，上述人员可以通过拨号进入企业网络。但这会带来几个问题：①安全问题。拨号服务器本身就是一个网络隐通道，黑客可以通过一些攻击方法，如攻破并直接进入用户网络。②费用问题。拨号访问方式对于远程用户来说，其通信费用是不可忽视的。③传统的拨号访问性能也受到限制。由于虚拟企业专网系统采用各种信息加密技术和身份鉴别技术，为远程的信息访问提供了安全可靠的网络传输通道。④VPN 由于利用公网设施，因此还有价格低廉和性能好的优势。

对很多用户，如政务系统，对网络安全尤其重视，甚至要求业务网络和互联网完全隔离。但是其初始数据的采集和处理结果的反馈又可能要求通过互联网来实现，数据的审核则需要由处于内网中的工作人员来完成，这就产生了一个需求，如何在内外网物理隔离的条件下，将外网工作数据安全转移到内网。另外，许多与业务相关的来自外网的资料和文档也需要传入内网，供内网工作人员使用。因此，内外网之间的信息交流成为各政府部门需要迫切解决的问题。物理隔离系统从一定程度上满足了这种物理断接、逻辑连接的数据交换需求。

2. 网络系统

网络是用户业务和数据通信的传输纽带、桥梁，是连接主机（服务器）、用户工作站的唯一设施。网络的主要功能就是为用户业务和数据通信提供可靠的、满足传输服务质量的传输通道。网络可能受到资源滥用、管理失控、DOS 等攻击。因此对用户网络必须要能够进行安全监控，包括监视网络的安全生态，对网络攻击及时预警、报警、制止和记录。适当地部署入侵检测和漏洞扫描产品，可以让用户了解其网络的安全状况，并对黑客攻击进行有效检测和反应，尽量减少黑客攻击机会和攻击成功的可能性。

3. 主机

在网络系统中，主机（服务器）是网络的核心、数据的集中点和业务服务的提供者，因此主机是黑客的重点攻击对象，也是进行安全防护的重中之重。黑客攻击主机的目的有窃取用户数据信息、窃取系统控制权、中断/破坏系统服务，因此主机的安全包括操作系统和运行在其上的应用系统的安全以及存储在主机中数据的安全。为保护主机不遭受黑客攻击及减少黑客攻击的可能性，必须对主机进行安全加固。加固主机安全的方法有很多

种，如提高操作系统的安全等级、安全配置操作系统、安装最新补丁文件等，也有其他层面的配套安全保护措施，如主机防火墙、主机入侵检测、主机漏洞扫描等。

综上所述，在信息安全保障中，一定要坚持深层防御战略思想，采用层次性、多样化的安防手段，最大限度地保障用户信息及其系统安全。

1.6.2 信息安全的措施

1. 发展和使用信息加密技术

信息加密技术是确保计算机系统安全的重要技术措施之一，包括以下三个方面的内容：

(1) 文件加密技术

文件名加密只是利用文件名的屏幕显示形式，通过变换，使得实际注册的文件名与显示的不相符，或者根本不显示，难以读写。文件加密技术包括文件的加密及文件名加密。目前的加密方法有两种，一种是利用加密软件对文件单独进行加密和解密；另一种是把加密系统妥善地嵌入到文件访问机制中，并尽量减少加密和解密所需的时间，在文件存储时系统自动加密，而运行前，则自动解密。

(2) 存储介质加密技术

存储介质加密的主要目的在于防止非法复制。由于存储介质本身的某些特点，决定了存储介质加密的某种局限性。这类加密的原理很简单。把某些指纹性质的特征信息写入磁盘，作为密钥嵌入程序，可查验它的存在和正确性，使用普通磁盘驱动器能读出程序并运行，但不能写。当复制该盘时，指纹信息将被丢失，于是被查验为非法复制件；同时，密钥丢失，无法运行。

(3) 数据库加密方法

① 常见的加密方法。DES 分组加密类型的算法是数据库中加密数据的常用方法。对于数据之类加密，多采用分组密码的密本方式；对于记录、关系等较长数据的加密，多采用分组密码块键方式。密本方式是对定长的明文在固定长度的密钥的控制下加密后，得出密文的长度与原明文一样。所谓密码块键方式，则是把每次加密的输出反馈到输入，作用到下次要加密的明文上。于是每次的加密输出，不仅依赖于本次加密输入的明文，还与所有原先输入的明文有关。

② 子密钥数据库加密的秘密同态技术。中国剩余定理是子密钥数据库加密技术的数学基础。它是按记录对数据加密，按数据项(对关系数据而言)进行解答。需要其记录的某数据项时，就用该数据项的子密钥解密。

对数据项的访问，遵从最小授权原则，而不致泄露与授权无关的信息。利用读/写子密钥，还能较为方便地修改、更新数据库记录中的指定数据项，而无须把整个记录全部解密、修改后再重新加密。所谓秘密同态技术，是对加密的数据库无须解密就直接进行操作。这可避免大量繁琐的加密/解密操作，提高数据库的运行效率。但是，构造数据库的秘密同态是十分困难的，这种技术有无生命力，仍有待实践证明。

③ 数据库系统的密钥管理。对数据库而言，生存周期长的数据信息量大量存在，密钥也有多级。例如，用户级密钥、数据库级密钥、记录级密钥以及数据项级密钥等。各级

密钥的形式，具有生命周期相对较长的特点，要求数据库系统的密钥产生、更新和管理保护，应当适应下述特点：

- 为抵御密钥穷举搜索的攻击，产生重复密钥的概率要尽可能低。
- 谨防能从一个数据项的密钥推导出另一个数据项的密钥。这样，即使破译了某些数据项的密钥，也不会威胁到其他数据项的安全。
- 还得防止在已知部分明文或明文值的统计分布的情况下，从密文中破译为明文。

2. 采取技术防护措施

(1) 审计技术

审计技术使信息系统自动记录下网络中机器的使用时间、敏感操作和违纪操作等。审计为系统进行事故原因查询、定位，事故发生前的预测、报警以及为事故发生后的实时处理提供详细可靠的依据或支持。审计对用户的正常操作也有记载，因为往往有些正常操作(如修改数据等)恰恰是攻击系统的非法操作。

(2) 安全协议

整个网络系统的安全强度实际上取决于所使用的安全协议的安全性。安全协议的设计和改进有两种方式：①对现有网络协议(如 TCP/IP)进行修改和补充；②在网络应用层和传输层之间增加安全子层，如安全协议套接字层(SSL)，安全超文本传输协议(SHTTP)和专用通信协议(PCP)。安全协议实现身份鉴别、密钥分配、数据加密、防止信息重传和不可否认等安全机制。

(3) 访问控制技术

访问控制是保护系统资源不被未经授权或以未授权方式接入、使用、披露、修改、毁坏和发出指令等。访问控制技术还可以使系统管理员跟踪用户在网络中的活动，及时发现并拒绝黑客的入侵。访问控制采用最小特权原则：即在给用户分配权限时，根据每个用户的任务特点使其获得完成自身任务的最低权限，不给用户赋予其工作范围之外的任何权力。Kerberos 存取控制是访问控制技术的一个代表，它由数据库、验证服务器和票据授权服务器三部分组成。其中，数据库包括用户名称、口令和授权进行存取的区域，验证服务器验证要存取的人是否有此资格，票据授权服务器在验证之后发给票据允许用户进行存取。

3. 行政管理措施

除了从思想上提高对计算机网络安全重要性的认识和从技术上加强网络安全防范措施外，还必须有严格的行政管理措施。

(1) 加强对计算机的管理

对计算机的操作应建立严格的操作规程；对计算机要制订严格的管理制度；对重要的计算机中心要严加保卫，进出机房应有报告制度；重要的涉及国家机密的文件和信息的上传及下载都必须经有关保密部门的批准、审查。

(2) 对人员的管理

对计算机操作人员要经过考核，达到规定的技术要求；重要部门的计算机操作人员进入机房要有时间规定，不能随便进出；对核心部门的计算机操作人员要进行各方面的考核、审查；对计算机上出现的新问题、新情况要及时报告并采取紧急措施；要严厉打击

计算机犯罪行为并制定有效的网络安全法规。总之，只有从思想上、技术上以及行政管理上全面防护，才能保证计算机网络的安全。

1.7 小 结

信息化是目前国际社会发展的趋势，对经济、社会的发展都有重大意义。与此同时，由于计算机网络所具有的开放性和共享性，信息安全性也成为人们日益关注的问题。

本章从总体上概括了信息安全问题及保障信息安全的必要性。在深层防御战略中，主要内容是主机及计算环境的安全、操作系统的安全、应用程序的安全、基于主机的监视技术、网络传输设施、网络边界、支撑性基础设施。

确保网络系统的信息安全是网络安全的目标，对任何种类的网络系统而言，就是要阻止各种对信息的威胁和攻击的发生。这些威胁和攻击主要包括：信息泄漏、信息破坏、计算机犯罪、计算机病毒。本章简述了计算机病毒的起源、发展及其危害性，随着互联网的发展，病毒的发展主要表现在：新病毒层出不穷，感染发作有增无减；电子邮件已经取代磁盘成为病毒传播的主流途径；传播速度大大加快，病毒已无国界；病毒家族的种类越来越多；破坏性不断增加等方面。

密码技术是信息安全的保障及核心技术。计算机网络、通信技术的发展和信息时代的到来，给密码学提供了难得的发展机遇。密码学是研究编制密码和破译密码的技术科学。随着计算机网络不断渗透到各个领域，密码学的应用也随之扩大。数字签名、身份鉴别等都是由密码学派生出来的新技术和应用。

最后对信息安全的对策与措施进行了介绍，基于信息保障深层防御战略思想把信息安全的保护对象分为系统边界、网络系统和主机。通过对本章内容的学习，可对信息安全技术有一个总体的初步认识，为进一步学习信息安全技术打下坚实的基础。

习 题

1. 深层防御战略的定义及其主要内容是什么？
2. 深层防御战略包括哪些方面？
3. 计算机犯罪的定义及特点是什么？
4. 试分析计算机犯罪具有哪些特性。
5. 密码学的定义是什么？
6. 密码学的两个分支学科是什么？
7. 对于保障信息安全有哪些对策？
8. 为了保障信息安全可以采取多种技术防护措施，这些措施包括哪些？

第 2 章　信息安全基础

信息安全是指在给定的安全密级的条件下信息系统抵御意外事件或恶意行为的能力，这些事件和行为将危及所存储、处理、传输的数据安全以及经由这些系统所提供的服务的非否认性、完整性、机密性、可用性和可控性。

2.1　信息不安全因素

2.1.1　物理不安全因素

物理安全是信息安全的最基本保障，是物理层次上的安全保护。一方面，计算机系统和通信系统应该充分考虑到系统所受的安全威胁和相应的防护措施，提高系统的可靠性；另一方面，也应该通过安全意识的提高、安全制度的完善、安全操作的提倡等方式使用户和管理维护人员在系统和物理层次上实现信息的保护。

目前主要的物理不安全因素如下：

(1) 自然灾害(如雷电、地震、火灾、水灾等)，物理损坏(如硬盘物理损坏、设备意外损坏等)，设备故障(如意外断电，电磁干扰等)和意外事故。这类风险的特点是：突发性、自然因素性和非针对性。这种安全威胁只破坏信息的完整性和可用性(对信息的保密性无损害)；对该类威胁的防范一般是实施防护措施，建立数据备份和安全制度。

(2) 电磁泄漏(如侦听计算机操作过程)，产生信息泄漏，干扰他人，受他人干扰，乘机而入和痕迹泄露等，其特点是难以觉察性、人为实施的故意性、信息的无意泄露性，这种威胁只破坏信息的保密性(无损信息的完整性和可用性)。可以通过辐射防护、口令隐藏和销毁得以解决。

(3) 操作失误(如删除文件、格式化硬盘等)或意外疏漏(如系统崩溃等)。其特点是人为实施的无意性、非针对性。这种安全威胁只破坏信息的完整性和可用性(无损信息的保密性)，通常用状态检测、报警确认和应急恢复等方法处理。

(4) 计算机系统机房的环境安全。其特点是可控性强、损失大、可管理性强。解决方法是加强机房管理、运行管理、安全组织和人事管理。

2.1.2　网络不安全因素

计算机网络具有分布的广域性、体系结构的开放性、信息资源的共享性和通信信道的共用性等特点，基于这些特点，计算机网络存在很多严重的脆弱性。它们是信息安全的隐

患。问题严重，原因复杂，为攻击型的威胁提供了可乘之机，找到和确认这些脆弱性是至关重要的。影响计算机网络的因素很多，归结起来影响网络安全的因素主要有人为疏忽和人为恶意攻击、网络软件的漏洞、非授权访问、信息泄漏（或丢失）和破坏数据完整性。

（1）网络规模

网络安全的脆弱性和网络的规模有密切关系。网络规模越大，其安全的脆弱性越大。资源共享与网络安全是对矛盾，资源共享加强，不安全性就越加严重。

（2）网络物理环境

网络物理环境是指计算机设备防止自然灾害的保护，也包括一般的物理环境的保护，像机房的安全门、人员出入机房的规定等。物理环境安全保护的范围不仅包括计算机设备和传输线路，也包括一切可以移动的物品，如打印数据的打印纸和装有数据和程序的磁盘。网络物理环境存在脆弱性。

2.1.3　系统不安全因素

现在应用的大部分系统软件都有一定的漏洞，操作系统就是一个例子。操作系统是网络和应用程序之间接口的程序，是整个网络信息系统的核心，系统的安全性体现在整个操作系统中。对于一个设计不够安全的操作系统来说，应采用增加安全特性或打补丁的办法进行安全维护。下面列举一些这方面的例子：

- IIS ISM. dll 文件名截断漏洞、泄漏文件内容漏洞。
- Microsoft Windows 9X 共享密码校验漏洞。
- Microsoft IIS Unicode 解码目录遍历漏洞。
- Microsoft IIS CGI 文件名检查漏洞。
- Microsoft IIS 远东版泄漏文件内容漏洞。
- Microsoft IIS CGI 文件名错误解码漏洞。
- Microsoft FrontPage 2000 服务器扩展缓冲区溢出漏洞。
- Microsoft IIS ssinc. dll 缓冲区溢出漏洞。

由于系统中存在的这些漏洞，信息安全带来很大隐患，所以要加强系统建设，采取措施补救这些漏洞，消除隐患。

2.1.4　管理不安全因素

管理不安全因素主要有以下几个方面：

1. 管理不能做到多人负责

每一项与安全有关的活动都必须有两人或多人在场。这些人应是系统主管领导指派的，忠诚可靠，能胜任此项工作；他们应该签署工作情况记录以证明安全工作已得到保障。但现在普遍是一人负责制，给安全保障带来威胁。

2. 管理者任期太长

一般地来说，任何人最好不要长期担任与安全有关的职务，以免使他认为这个职务是专有的或永久性的。为了保证安全，工作人员应不定期地循环任职，强制实行休假制度，

并规定对工作人员进行轮流培训,以使任期有限制度切实可行。

3. 不能做到职责分离

在信息处理系统工作的人员普遍存在着打听、了解或参与职责以外的与安全有关的事情的现象。出于对安全的考虑,下面每组内的两项信息处理工作应当分开。

(1) 计算机操作与计算机编程。

(2) 机密资料的接收和传送。

(3) 安全管理和系统管理。

(4) 应用程序和系统程序的编制。

(5) 访问证件的管理与其他工作。

(6) 计算机操作与信息处理系统使用媒介的保管等。

2.2 信息攻击

根据信息攻击方式的不同,信息攻击可以分为以下 7 种:口令攻击、地址欺骗、连接盗用、业务否决、窃听、对于域名系统等基础设施的破坏和利用 Web 破坏数据库。

2.2.1 口令攻击

攻击者攻击目标时常常把破译用户的口令作为攻击的开始。只要攻击者能猜测或者确定用户的口令,就能获得机器或者网络的访问权,并能访问到用户能访问到的任何资源。如果这个用户有域管理员或根用户权限,则极其危险。

口令猜测前提是必须先得到该主机上的某个合法用户的账号,然后再进行合法用户口令的破译。获得普通用户账号的方法很多,主要有以下几种:

(1) 利用目标主机的 Finger 功能。当用 Finger 命令查询时,主机系统会将保存的用户资料(如用户名、登录时间等)显示在终端或计算机上。

(2) 利用目标主机的 X.500 服务。有些主机没有关闭 X.500 的目录查询服务,也给攻击者提供了获得信息的一条简易途径。

(3) 从电子邮件地址中收集。有些用户的电子邮件地址常会透露其在目标主机上的账号。

(4) 查看主机是否有习惯性的账号。有经验的用户都知道,很多系统会使用一些习惯性的账号,造成账号的泄露,这又有下述三种方法。

① 通过网络监听,非法得到用户口令,这类方法有一定的局限性,但危害性极大。采用中途截击的方法是获取用户账户和密码的一条有效途径。当前,很多协议根本就没有采用任何加密或身份认证技术,如在 Telnet、FTP、HTTP、SMTP 等传输协议中,用户账户和密码信息都是以明文格式传输的,此时若攻击者利用数据包截取工具便可很容易收集到账户和密码。还有一种中途截击攻击方法,它在与服务器完成三次握手建立连接之后,在通信过程中扮演第三者的角色,假冒服务器身份,再假冒向服务器发出恶意请求,其造成的后果不堪设想。另外,攻击者有时还会利用软件和硬件工具时刻监视系统主机的

工作，等待记录用户登录信息，从而取得用户密码；或者编制有缓冲区溢出错误的 SUID 程序来获得超级用户权限。

② 在获得用户的账号后（如电子邮件@前面的部分）利用一些专门的软件强行破解用户的密码。这种方法不受网段限制，但攻击者要有足够的耐心和时间。如采用字典穷举法来破解用户的密码。攻击者可以通过一些工具程序，自动从计算机字典中取出一个单词，作为用户的口令，再输入给远端的主机，申请进入系统；若口令错误，就按序取出下一个单词，进行下一个尝试，并一直循环下去，直到找到正确的口令或字典的单词试完为止。由于这个破译过程由计算机程序来自动完成，因而几个小时就可以把有十几万条记录的字典中的所有单词都测试一遍。

③ 利用系统管理员的失误。在现代的 UNIX 操作系统中，用户的基本信息存放在 password 文件中，而所有的口令则经过 DES 加密方法加密后，存放在一个叫 shadow 的文件中。黑客们获取口令文件后，就会使用专门的破解 DES 加密法的程序来破解口令。同时，由于操作系统都存在许多安全漏洞或一些设计缺陷，这些缺陷一旦被找出，黑客就可以长驱直入。例如，让 Windows 95/98 系统后门洞开的 BO 就是利用了 Windows 的基本设计缺陷放置特洛伊木马程序。特洛伊木马程序可以直接侵入用户的计算机并进行破坏，它常被伪装成工具程序或者游戏等，诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载，一旦用户打开了这些邮件的附件或者执行了这些程序之后，它们就会像古特洛伊人在敌人城外留下的藏满士兵的木马一样留在用户的计算机中，并在自己的计算机系统中隐藏一个可以在 Windows 启动时悄悄执行的程序。当连接到因特网上时，这个程序就会通知攻击者，来报告 IP 地址以及预先设定的端口。攻击者收到这些信息后，再利用这个潜伏在其中的程序，就可以任意地修改计算机的参数设定、复制文件、窥视整个硬盘中的内容等，从而达到控制计算机的目的。

2.2.2　地址欺骗

地址欺骗有三种基本形式：基本地址变化、使用源路由选择截取数据包、利用 UNIX 机器上的信任关系。

1. 基本地址变化

地址欺骗的最基本形式是搞清楚一个网络的配置，然后改变自己的 IP 地址，伪装成别人机器的 IP 地址。这样做将使所有被发送的数据包都带有假冒的源地址。这是非常低等级的技术，因为所有的应答都回到了被盗用了地址的机器上，而不是攻击者的机器。这被叫做盲目飞行攻击，或者叫做单向攻击。

这种攻击虽有一些限制，但就某一特定类型的拒绝服务攻击而言，只需要一个数据包去撞击机器，而且地址欺骗将让人们更难以找到攻击者的根源。对某些特定的攻击，如果系统收到了意想不到的数据包，说明对系统的攻击仍然在进行。而且因为 UDP 是无连接的，所以单独的 UDP 数据包会被发送到受害方的系统中。

2. 源路由攻击

地址欺骗的一个重要问题是被盗用的地址会收到返回的信息流，而攻击者从来不会

接收到它们。但是对于更高级的攻击，攻击者更愿意看到对话的双方。

为了获得从目的机器返回到源机器的流量，一个方法是攻击者插入到正常情况下流量经过的通路上。这是非常困难的，因为攻击者必须攻击受害网络上的一台机器，而且不存在任何保障措施让流量继续通过攻击者的机器。因特网采用动态路由，它每天、每小时，甚至每分钟都会有变化。有一种方法能够保证数据包会经过一条给定的路径，而且作为一次欺骗，保证它经过攻击者的机器。这样做需要使用源路由，它被包含在 TCP/IP 协议组中。源路由允许指定一条数据包必须经过的路径，它包括两种类型的源路。

(1) 宽松的源路由选择(LRS)

发送端指明了流量或者数据包必须经过的 IP 地址清单，但如果需要，也可以经过一些其他地址。换句话说，不用考虑数据包经过的确切地址，只要它经过这些地址就可以。

(2) 严格的源路由选择(SRS)

发送端指明 IP 数据包必须经过的确切地址。如果没有经过这一确切路径，数据包会被丢弃，并返回一个 ICMP 差错报文。换句话说，必须考虑数据包经过的确切路径，而且如果由于某种原因没有经过这条路径，这个数据包就不能被发送。

源站路由使用 IP 首部一个 39 个字节的源路由选项地址来工作。因为源站路由被放入了 IP 首部，所以对指定的 IP 地址数目会有限制。因为源路由选项字段是 39 个字节，其中 3 个字节是附加信息，那么剩下的 36 个字节是地址信息。每一个地址是 4 个字节，如果 36 除以 4，会有 9 个地址的空间。但情况不是那么简单，因为最后一个地址必须是目的地址，所以它只留下 8 个地址的空间。可知随着因特网的发展，会出现 IP 地址的数目大于 8 的情况。在这些情况下，就只能使用宽松的源站选路，因为如果不能找到确切的路径，那么严格的源路由选路就会丢弃那个数据包。

源路由的基本工作过程是：取出源站路由清单中第一个地址，使它成为目的地址。如果是严格的源路由选择，那么它必须是下一跳；如果不是，就将被丢弃。对于宽松的源路由选择，在数据包到达清单上指出的地址以前，经过多少跳是没有关系的。在到达目的地址后，它从清单中取出下一个地址，使它变为目的地址。接下来继续重复这个过程，直到找到目的地址或者数据包不能被路由为止。

需要指出的一点是如果发送端指定了到达目的地址的源路由，那么目的机器能够自动地使用源路由返回到发送端，这就是危险的原因，可能不知道有人正在使用它。可能回答一个数据包，而且如果发送端使用了源路由，就会在未知的情况下使用它。

攻击者使用假冒的地址向目的地发送数据包，但指定了宽松的源路由选择，并把他的 IP 地址填入地址清单中。那么，当接收端回应时，数据包返回到假冒的 IP 地址处，而不是前面它经过的攻击者的机器。攻击者没有盲目飞行，因为他能看到对话双方。

3. 信任关系

在 UNIX 领域中，信任关系能够很容易得到。假如在主机 A 和 B 上各有一个账户，在使用当中会发现，在主机 A 上使用时需要输入在 A 上的相应账户，在主机 B 上使用时必须输入在 B 上的账户，主机 A 和 B 当作两个互不相关的用户，显然有些不便。为了减少这种不便，可以在主机 A 和主机 B 中建立起两个账户的相互信任关系。在主机 A 和主机 B 上 home 目录中创建.rhosts 文件。从主机 A 上，在 home 目录中输入“echo ‘B username’＞～/.rhosts”；

从主机 B 上，在 home 目录中输入“echo ‘A username’ >～/. rhosts”。至此，能毫无阻碍地使用任何以 r 开头的远程调用命令，如 rlogin、rcall、rsh 等，而不需要口令验证。这些命令将允许以地址为基础的验证，允许或者拒绝以 IP 地址为基础的存取服务，信任关系是基于 IP 地址的。rlogin 是一个简单的客户/服务器程序，它利用 TCP 传输。rlogin 允许用户从一台主机登录到另一台主机上，并且，如果目标主机信任它，rlogin 将允许在不应答口令的情况下使用目标主机上的资源。安全验证完全是基于源主机的 IP 地址。因此，根据以上所举的例子，能利用 rlogin 来从 B 远程登录到 A，而且不会被提示输入口令。

2.2.3　窃听

窃听是指攻击者通过对传输媒介的监听非法获取传输的信息，是对通信网络最常见的攻击方法。窃听的起源是偷听别人之间的谈话。随着科学技术的不断发展，窃听的含义早已超出隔墙偷听、截听电话的概念，它借助于技术设备和技术手段，不仅窃取语言信息，还窃取数据、文字、图像等信息。

这种威胁完全来源于无线链路的开放性，但是由于无线网络传输距离受到功率与信噪比的限制，窃听结点必须与源结点距离较近，所以与以太网、FDDI 等典型有线网络相比，更容易发现外部窃听结点。

现在的局域网大多是以太网，以太网以 CSMA/CD 的方式进行工作，在局域网内，数据的传送是以广播方式进行的，也就是人人都可以收到发向任何人的信息，只要把网卡模式设置成混合模式即可。即使不设网卡，也可以用一些监听软件将局域网内传送的数据包都收下来。如 IPMAN、NetXRay 等都可以从 Internet 下载得到，它们可以将局域网内传输的数据都记录下来，当然也可以通过加密来解决这个问题。

窃听技术是窃听行动所使用的窃听设备和窃听方法的总称，它不仅包括窃听器材，也包括窃听信号的传输、保密、处理，窃听器的安装、使用，以及与窃听相配合的信号截收等。

窃听技术的内涵非常广泛，特别是高档次的窃听设备或较大的窃听系统，应该包括信号的隐蔽、加密技术、工作方式的遥控、自动控制技术、信号调制、解调技术以及网络技术、信号处理、语言识别、微电子、光电子技术等现代科学技术的很多领域。这里，窃听技术主要是指获取信息的技术方法，也包括获取的信息的传递方法。

2.2.4　业务否决

业务否决是指入侵者通过某些手段使合法的网络实体无法获得其应有的网络服务。在蓝牙网络中，这种威胁包括阻止合法用户连接的建立，或者通过向网络或指定网络单元发送大量数据来破坏合法用户的正常通信。对于这种威胁，通常可采用认证机制和流量控制机制来防止。

2.2.5　链接盗用

链接盗用分为含蓄（隐蔽）的形式和明显（直接）的形式。企业通过站点来宣传自己的形象及产品，同时也可以和客户进行网上交易。可是，攻击者会把商品价格更改为比竞争

对手高，或把产品的价格涂改得一团糟。而那些直接的攻击者会把一张无聊的图片覆盖在页面上，或写上一些带有挑战性的言语。很显然，上面这些举动将给公司正常的业务带来严重的不良影响。

为了建立一个安全链接，Web 浏览器需要首先向 Web 服务器请求数字证书，数字证书提供了身份证明。浏览器在向 Web 服务器请求它的数字证书时，也同时发送了它所支持的加密算法列表。当服务器回送数字证书和它所选择的加密算法后，浏览器通过检查数字签名和确认 URL 是否与数字证明的公有名字域相匹配来验证数字证书。如果测试失败，浏览器将显示警告信息，其过程如图 2-1 所示。

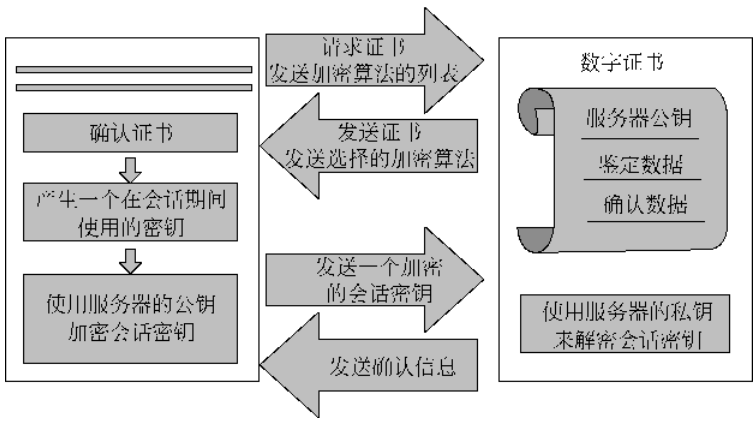

图 2-1 Web 服务器的鉴定

浏览器和服务器的通信使用对称加密，这就表明使用相同的密钥来进行加密和解密。当服务器的证书被证实后，浏览器将产生一个密钥，这个密钥需要通过一个安全的途径传递给服务器。一般使用双重加密技术来完成密钥的传递。浏览器使用服务器的公钥来加密密钥，然后把它传递给服务器。服务器使用它的私钥来解密密钥，然后向浏览器发送确认。上述过程表明对于一个加密链接，浏览器和服务器都拥有相同的密钥，使用相同的加密算法。它们后面的通信将使用这个加密的链接，浏览器会显示一个锁的图标，表示链接已建立。加密链接的证书如图 2-2 所示，站点访问者可以单击图标来检查服务器的证书，从而核实服务器的身份。

建立一个加密链接仅需要服务器获得权威机构颁发的证书。但是加密仅能阻止攻击者看到站点发送和接收的数据，并不能阻止攻击者伪造身份和对站点进行的恶意攻击。

2.2.6 对于域名系统等基础设施的破坏

1. 基本的网站欺骗

攻击者在注册一个域名时，抢先或特别设计注册一个非常类似的有欺骗性的站点。当一个用户浏览了这个地址，并与站点进行了一些信息交流，如填写了一些表单，站点给出一些响应的提示和回答，同时记录下用户的信息，并给这个用户一个 Cookie 数据，以便能随时跟踪这个用户。典型的例子是假冒金融机构，偷盗客户的信用卡信息。