第 1 章　网络安全概述

本章要点

随着计算机网络的发展，网络安全及其相关技术得到了前所未有的重视。本章的讲解将对本书后面章节的学习起到提纲挈领的作用。

本章的主要内容如下。

- 网络安全的现状。
- 针对校园网的攻击与防护。
- 校园网的安全管理。

1.1　为什么要重视网络安全

1.1.1　网络安全的现状

随着我国教育信息化的飞速发展，城域网和校园网的建设与应用得到了广泛的普及。然而，网络的信息安全问题不容乐观。我国校园网安全问题已经成为教育主管部门和各地学校管理者关心和研究的重要课题。

1．安全事件的发生呈上升趋势

据工业和信息化部网站统计，2018 年第一季度共监测网络安全威胁约 4541 万个，其中电信主管部门收集约 216 万个，基础电信企业监测约 1168 万个，网络安全专业机构监测约 6 万个，重点互联网企业和网络安全企业监测约 3151 万个。教育行业虽然不具有较高的商业价值，也不是网络攻击的主要目标，但是庞大的普通用户数量和相对较弱的安全防护意识，也导致了校园网内信息安全事件的频繁发生。

截至 2018 年上半年，各种网络钓鱼攻击增加了 74%，勒索软件攻击事件和商业电子邮件入侵（Business E-mail Compromise，BEC）事件也在逐步增多，这些都成为互联网安全的主要威胁，各种恶意软件通常在用户不知情的情况下把截获的用户信息发送给“信息收集者”，如盗取用户网络游戏的账号，并变卖玩家的装备，甚至是商业信息，这些都严重损害了使用者的利益。

各地中小型校园网虽然都会有一定的安全防护，但是学生的接入设备、共享 Wi-Fi 接入等终端并不在安全控制范围内，导致蠕虫病毒、间谍软件、网络钓鱼等各种恶意代码充斥在校园网中，严重影响了校园网的正常运行。

2．安全标准引用不及时

根据 BSI（British Standards Institution，英国标准协会）的统计，我国通过国际安全认证的企业和政府信息化职能部门相对较少，而引入某个管理标准进行管理的校园网就更少了。目前，校园网的网络结构没有统一的样式，安全产品和邮件服务器也应用着不同厂商的产品，网络管理员的维护技术和厂家的支持技术良莠不齐。

1.1.2　加强青少年的网络安全意识

有些青少年为了满足自己的好奇心，利用从网络上学来的入侵手段，非法获取别人的信息，恶意修改团体、学校甚至政府机关的网站，这些都触犯了我国的法律。需要指出的是，这类攻击

者号称黑客，其实他们只是网络攻击工具的使用者，简称 Tools User。

因此，我们应加强计算机安全教育，包括提高各级网络管理人员对网络重要性的认识和安全措施的掌握水平，向社会宣传计算机网络入侵的破坏性，尤其要加强拥有 Internet 访问能力的青少年的网络安全法律观念。

具体措施包括：以公益广告的形式向社会宣传计算机网络安全的重要性和法律含义；在校园网的主页以醒目的方式告诫有入侵倾向的网络用户；在注册校园网用户时，要求实名制；网络管理员在发现不明身份的用户时，应立即确定其身份，并对其发出警告，提前制止可能的网络犯罪；应该有专门的网络安全管理人员对校园网进行时段监控，并定期进行安全检查，同时应在网络中配置相关的安全检测工具。

切实加强网络的安全配置和管理，做到防患于未然，可以有效降低计算机网络受到攻击的频率，减少因受到攻击而产生的损失，增强校园网的安全性。

1.2 什么是攻击

仅在入侵行为已经完成，且入侵者已进入目标网络内的行为称为攻击。但关于攻击的定义更为积极的观点是，所有可能使一个网络受到破坏的行为都称为攻击，即从一个入侵者开始寻找目标机的那个时刻起，攻击就开始了。

通常，在正式攻击之前，攻击者先进行试探性攻击，目的是获取系统有用的信息，此时的攻击手段包括 Ping 扫描、端口扫描、账户扫描、DNS 转换、恶性的 IP Sniffer（通过技术手段非法获取 IP 包，以获得系统的重要信息）及特洛伊木马程序等。

1.2.1 收集信息的主要方式

经常使用的信息收集软件包括 NSS、Strobe、Netscan、SATAN（Security Administrator’s Tool for Auditing Network）、Jakal、FTPScan 及各种 Sniffer 软件。从广义上讲，特洛伊木马（Trojan）程序是收集信息攻击的重要手段。收集信息攻击有时是其他攻击手段的前奏。对于简单的端口扫描，敏锐的网络安全管理员往往可以从异常的日志记录中发现攻击者的企图。但是对隐秘的 Sniffer 软件和特洛伊木马程序来说，检测它们的存在是一件高级和困难的任务。

1．Sniffer

Sniffer 本来是用来诊断网络连接情况的，是带有很强 DeBug 功能的常用网络分析器，所以黑客利用它来截获用户口令等敏感信息，甚至还可以用它来攻击相邻的网络。

检测 Sniffer 的存在是一个非常困难的任务，因为 Sniffer 本身只是被动地接收数据，而不发送任何数据包。

一般来讲，真正需要保密的只是一些关键数据，如用户名和口令等。因此，可以使用 IP 包级的加密技术，这样即使 Sniffer 得到数据包，也很难得到真正的数据信息。这样的工具包括 Secure Shell（SSH）及 F-SSH，尤其是 F-SSH 针对一般利用 TCP/IP 进行通信的公共传输提供了非常强大的、多级别的加密算法。另外，采用网络分段技术、减少信任关系等手段可以将 Sniffer 的危害控制在较小范围内。

2．特洛伊木马

RFC 1244 中给出了特洛伊木马程序的经典定义：“它提供了一些有用的或仅仅是有意思的功能。但是特洛伊木马程序通常会做一些用户不希望发生的事，诸如在用户不了解的情况下复制文件或窃取用户的密码、直接将重要资料转送出去和破坏系统等行为。”

很多情况下，特洛伊木马程序是在二进制代码中被发现的，它们大多无法直接阅读，并且可

以应用在很多系统平台上，它的传播方式和计算机病毒非常相似。从 Internet 上下载的软件（尤其是免费软件和共享软件）及从匿名服务器或 USERNET 新闻组中获得的程序等都有可能捆绑了特洛伊木马程序。因此，经常上网的用户自觉做到不轻易安装或使用来路不明的软件是十分必要的。2018 年 4 月份出现的木马病毒有 Ransom.Zenis 和 Backdoor.Teawhy 等。

检测一个特洛伊木马程序，需要深入了解有关操作系统的知识。用户可以通过检查文件的更改时间、文件长度、校验和等来判断文件是否进行过非预期的操作。另外，文件加密也是有效的检查特洛伊木马程序的方法。

1.2.2 攻击的主要手段

1．口令入侵

口令入侵包括两个层次的行为：一种是破解使用加密口令加密了的用户文件，对于这种破解，攻击者可以很轻松地完成任务，因为目标文件通常已经下载到攻击者本地的计算机上，受害者对此已经无能为力；另一种是破解目标计算机的系统口令，对于这种破解，攻击者需要小心处理，以免触动目标计算机的报警系统，因为通常情况下，在系统账号登录失败达到一定次数后，计算机通常会自动锁死，并触发一定的日志记录功能或进行报警（包括向系统管理员发送电子邮件进行通知）。

2．后门软件攻击

后门软件攻击是互联网上用得比较多的一种攻击手法。早期的 Back Orifice 2000、冰河等都是比较著名的后门软件，它们可以非法地取得用户计算机的超级管理员权限，并完全控制用户的计算机。这些后门软件一般分为服务器端和用户端两个部分，黑客进行攻击时，会使用用户端程序登录已安装好服务器端程序的计算机，这些服务器端程序都比较小，一般会被捆绑在某些软件上。另外，大部分后门软件的重生能力比较强，给用户的清理工作造成一定的困难。

目前最流行的是反弹端口的后门程序，这类后门程序不再区分客户端软件和服务器端软件，只需要安装在目标计算机上，使用的端口也是随机的，这对利用端口进行查毒的防护软件来说是一个很大的威胁。

3．监听法

这一部分的内容请参阅 1.2.1 节的“Sniffer”部分。

4．电子邮件技术

电子邮件（E-mail）是互联网上运用得十分广泛的一种通信方式。黑客可以使用一些电子邮件炸弹软件或 CGI 程序向目的电子邮箱发送大量内容重复、无用的垃圾电子邮件，使目的电子邮箱容量被占满，从而达到让其无法使用的目的。当垃圾电子邮件的发送流量特别大时，还有可能造成电子邮件系统对于正常的工作反应缓慢，甚至瘫痪的情况出现，这一点和本书后面要讲到的拒绝服务攻击（DDoS）比较相似。

电子邮件炸弹是一种简单有效的侵扰工具。它反复发送给目标接收者相同的信息，用这些垃圾信息填满用户的电子邮箱空间，如 bomb02.zip（Mail Bomber）软件（运行在 Windows 平台）和 EmailBomb 软件（运行在 UNIX 平台），它们的使用都非常简单。

同时，攻击者可以利用电子邮件列表，把攻击目标以电子邮件列表的方式注册到用户服务器的电子邮件列表中，或者直接通过用户的电子邮件列表发送垃圾电子邮件或带有计算机病毒的电子邮件。

对于遭受此类攻击的用户电子邮箱，可以使用一些垃圾电子邮件清除软件来解决，其中常见的有 Spam Eater、Spamkiller 等。Outlook 等软件也提供过滤功能，发现此类攻击后，将源目标地址放入拒绝接收列表中即可。

5．电子欺骗

电子欺骗（Spoofing Attack）包括两种攻击形式：一种是针对 HTTP、FTP、DNS 等协议的攻击，这种攻击可以窃取普通用户甚至超级用户的权限，任意修改信息内容，造成巨大危害；另一种攻击是 IP 欺骗，即攻击者伪造他人的 IP 地址，本质上就是让一台计算机来扮演另一台计算机，借以达到蒙混过关的目的。

几乎所有的电子欺骗都依赖目标网络的信任关系（计算机之间的互相信任）。入侵者可以使用扫描程序来判断远程计算机之间的信任关系。这种技术欺骗成功的案例较少，要求入侵者具备特殊的工具和技术（并且对非 UNIX 系统不起作用）。

6．拒绝服务

从网络攻击的各种方法和所产生的破坏情况来看，拒绝服务（Denial of Service，DoS）算是一种很简单但又很有效的进攻方式。它的目的是降低或中断用户服务器提供的访问能力，破坏组织的正常运行，最终它会使用户的 Internet 连接和网络系统部分或全部失效。DoS 的攻击方式有很多种，最基本的 DoS 攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务。

1.2.3 入侵的常用策略

1．利用系统文件攻击

这里以攻击 UNIX 系统为例，黑客可以通过 Telnet 指令操作得知 Sendmail 的版本号，从而结合已公布的资料了解操作系统会有哪些安全漏洞。禁止对可执行文件的访问虽不能防止黑客对它们的攻击，但至少可以使这种攻击变得更困难。

2．伪造信息攻击

黑客可以通过发送伪造的路由信息，构造系统源主机和目标主机的虚假路径，从而使流向目标主机的数据包均经过攻击者的系统主机。这样攻击者就有可能获得用户密码等敏感信息。

3．利用协议弱点攻击

IP 地址的源路径选项允许 IP 数据包选择一条捷径通往系统目的主机。假设攻击者试图连接到防火墙后面的主机 A 上，攻击者只需要在送出的请求报文中设置 IP 源路径选项，使报文有一个目的地址指向防火墙，而最终地址是主机 A。当报文到达防火墙时被允许通过，因为它指向防火墙而不是主机 A。防火墙的 IP 层处理该报文的源路径被改变，并被发送到内部网上，报文就这样到达了主机 A。

4．网络钓鱼

在被攻击主机上启动一个可执行程序或打开一个链接，该程序或链接显示一个伪造的登录界面。当用户在这个伪装的界面上输入登录信息（用户名、密码等）后，该程序将用户输入的信息传送到攻击者主机，然后关闭界面给出提示信息“系统故障”，要求用户重新登录或跳转到一个真实的界面上，此后才会出现真正的登录界面。

5．利用系统管理员失误的攻击

网络安全的重要因素之一就是人。网络安全中常说的一句话就是：“堡垒最容易从内部攻破。”人为的失误包括 Web 服务器系统的配置差错、普通用户使用权限扩大等，这些给黑客造成了可乘之机。黑客常利用系统管理员的失误收集用于攻击的信息。

6．利用 ICMP 报文攻击

黑客利用 ICMP 报文的重定向消息可以改变路由列表，路由器可以根据这些消息建议主机走另一条更好的路径。攻击者可以有效地利用重定向消息把连接转向一个不可信的主机或路径，或者使所有报文通过一个不可信主机来转发。

7．利用源路径选项弱点攻击

一个外部攻击者可以传送一个具有内部主机地址的源路径报文。服务器会相信这个报文并向攻击者发送回应报文。

8．“跳跃式”攻击

现在许多网点使用 UNIX 操作系统。黑客们会设法先登录到一台 UNIX 的主机上，通过该操作系统的漏洞来取得系统特权，然后以此为据点访问其余主机，这种攻击方式称为“跳跃式”（Island-Hopping）攻击。黑客们在到达目的主机之前往往会这样跳几次。即使被攻击网络发现了黑客是从何处向自己发起了攻击，管理人员也很难顺藤摸瓜找回去，而且黑客在取得某台主机的系统特权后，可以在退出时删掉系统日志，清除痕迹。攻击者只要能够登录到 UNIX 系统上，就能相对容易地成为超级用户，这使得“跳跃式”攻击同时成为黑客和安全专家们的关注点。

1.2.4 攻击对象排名

下面是网络中公布的容易成为攻击对象的排名。

（1）主机运行没有必要的服务。
（2）未打补丁的、过时的应用软件和硬件固件。
（3）信息泄露，通过服务如 Gopher、Finger、Telnet、SNMP、SMTP、Netstat 等。
（4）盗用信任关系，如 Rsh、Rlogin、Rexec。
（5）配置不当的防火墙或路由器 ACL（Access Control List，访问控制列表）。
（6）弱口令。
（7）配置不当的网络服务器。
（8）不合理的输入文件系统。
（9）配置不当或未打补丁的 Windows NT 系统。
（10）无担保的过程存取点，如远程存取服务器、Modem 池等。

由此可见，网络攻击绝大部分是针对弱口令、安全策略设置不当、开启不必要的服务等设置不当的服务器进行攻击的，归根到底是人的因素导致了网络安全事故的发生。

1.3 入侵层次分析

与攻击对象排名不同的是，入侵层次的划分主要是从引发的危险程度来进行分析的。下面就入侵层次的划分和相应的对策进行讨论。使用敏感层的概念来划分标志攻击技术如下所示。

（1）第一层：电子邮件炸弹攻击（E-mail Bomb）。
（2）第二层：简单服务拒绝攻击（DoS）。
（3）第三层：本地用户获得非授权读访问。
（4）第四层：本地用户获得非授权的文件写权限。
（5）第五层：远程用户获得非授权的账号。
（6）第六层：远程用户获得特权文件的读权限。
（7）第七层：远程用户获得特权文件的写权限。
（8）第八层：远程用户拥有根（Root）权限。

以上层次划分在所有的网络中几乎都一样，基本上可以作为网络安全工作的考核指标，也可作为网络安全配置的基线标准。其中，本地用户（Localuser）是一种相对概念，它是指能自由登录网络上的任何一台主机，并且在网络上的某台主机上拥有一个账户，在硬盘上拥有一个目录的任何一个用户。

我们应根据遭受攻击的不同层次，采取不同的对策。

第一层和第二层的攻击包括电子邮件炸弹攻击和服务拒绝攻击。电子邮件炸弹攻击还包括登记列表攻击。对付此类攻击的最好方法是对源地址进行分析，把攻击者使用的主机（网络）信息加入访问控制列表中。除使攻击者网络中所有的主机都不能对目标网络进行访问外，没有其他有效的方法可以防止这种攻击的出现。

此类型攻击的破坏性不大，但是发生的频率可能很高，因为入门者仅需具备有限的经验和专业知识就能进行此类型的攻击。

第三层至第五层的攻击包括本地用户获得非授权读访问、本地用户获得非授权的文件写权限和远程用户获得非授权的账户的攻击。

处于第三层和第五层的攻击的严重程度取决于对那些文件的读或写权限的非法获得。导致攻击的原因有可能是部分配置错误或在软件内固有的漏洞。对于前者，管理员应该注意经常使用安全工具查找一般的配置错误。后者的解决需要安全管理员花费大量的时间去跟踪了解最新的软件安全漏洞报告，下载补丁软件或联系供货商。管理员发现发起攻击的用户后，应该立即停止其访问权限，冻结其账户。

第六层的攻击包括远程用户获得特权文件的读权限攻击。处于第六层的攻击涉及远程用户如何获取访问内部文件的权利问题。其起因大多是服务器配置不当、CGI 程序的漏洞和溢出问题。关于这种攻击，通常对内部人员的防范技术水平要求更高。据统计，对信息系统的攻击主要来自内部，占 85%。因为内部人员对网络有更多了解，有更多的时间和机会来测试网络安全漏洞，并更容易逃避系统日志的监视。

第七层和第八层的攻击包括远程用户获得特权文件的写权限、远程用户拥有根（Root）权限的攻击。处于第七层和第八层的攻击只能利用那些不该出现却出现了的漏洞，只有这些漏洞存在，才可能出现这种致命的攻击。

出现第三、四、五层的攻击表明网络已经处于很不安全的状态，安全管理员应该立即采取有效措施，保护重要数据，进行日志记录和汇报，同时争取能够定位发起攻击的地点，具体步骤如下。

（1）将遭受攻击的网段分离出来，将此攻击范围限制在最小的范围内。

（2）记录当前时间，备份系统日志，检查并记录损失范围和程度。

（3）分析是否需要中断网络连接。

（4）让攻击行为继续进行，并对已被入侵的系统做备份，以便留下证据。

（5）将入侵的详细情况逐级向主管领导和有关主管部门汇报。如果系统受到严重破坏，影响网络业务功能，则应立即调用备件恢复系统。

（6）尽可能寻找攻击的源头。

总之，尽量不使系统退出服务，同时尽力寻找出入侵者，并通过法律手段迫使其停止攻击，才是最有效的防卫手段。

1.4 设置安全的网络环境

通常，操作系统在安装完毕后，很多安全设置默认都没有启用，需要系统管理员进行手工设置，以确保网络和服务的安全。

1.4.1 关于口令安全性

通过口令进行身份认证是目前实现计算机安全的主要手段之一。黑客攻击目标时也常常把破

译普通用户的口令作为攻击的开始，通常采用字典穷举法进行密码破解。在线的密码探测容易在主机日志上留下明显的攻击特征，因此，更多时候攻击者会利用其他手段去获得主机系统上的/etc/passwd 文件甚至/etc/shadow 文件，然后在本地对其进行字典攻击或暴力破解。攻击者并不需要所有人的口令，他们得到几个用户口令就能获取系统的控制权。

然而，有许多用户对自己的口令没有很好的安全意识，使用很容易被猜出的口令，如有些是系统或主机的名字，或者是常见名词，如 System、Manager、Admin 等。保持口令安全的一些要点如下。

（1）口令长度不要小于 6 位，应同时包含字母和数字，以及标点符号和控制字符。

（2）口令中不要使用常用单词（避免字典攻击）、英文简称、个人信息（如生日、名字、反向拼写的登录名、房间中可见的东西）、年份及机器中的命令等。

（3）不要将口令写下来。

（4）不要将口令存于计算机文件中。

（5）不要让别人知道。

（6）不要在不同系统上，特别是不同级别的用户上使用同一口令。

（7）为防止眼明手快的人窃取口令，在输入口令时应确认无人在身边。

（8）定期改变口令，至少每 6 个月要改变一次。

（9）在系统中安装对口令文件进行隐藏的程序或设置。

（10）在系统中配置对用户口令设置情况进行检测的程序，并强制用户定期改变口令。任何一个脆弱的用户口令，都会影响整个系统的安全。

最后，永远不要对自己的口令过于自信，也许就在无意当中泄露了口令。定期地改变口令，会使自己遭受黑客攻击的风险降到一定限度之内。一旦发现自己的口令不能进入计算机系统，应立即向系统管理员报告，由系统管理员来检查原因。

系统管理员也应定期运行破译口令的工具，以尝试破译 shadow 文件，若有用户的口令密码被破译，则说明这些用户的密码设置得过于简单或有规律可循，应尽快通知他们及时更改密码，以防止黑客的入侵。

1.4.2 局域网安全

目前的局域网基本上采用以广播为技术基础的以太网，任何两个节点之间的通信数据包，不仅为这两个节点的网卡所接收，也同时为处在同一以太网内的任何一个节点的网卡所截取。因此，黑客只要接入以太网上的任意一个节点进行侦听，就可以捕获发生在这个以太网上的所有数据包，这就是以太网固有的安全隐患。

目前，Internet 上许多免费的黑客工具（如 SATAN、ISS、NETCAT 等）都把以太网侦听作为最基本的入侵手段。当前局域网安全的解决办法有以下几种。

1．网络分段

网络分段通常被认为是控制网络广播风暴的一种基本手段，但其实也是保证网络安全的一项重要措施。其目的就是将非法用户与敏感的网络资源相互隔离，从而防止可能的非法侦听。网络分段可分为物理分段和逻辑分段两种方式。

2．用交换式集线器代替共享式集线器

对局域网的中心交换机进行网络分段后，以太网侦听的危险仍然存在。这是因为网络最终用户的接入往往是通过分支集线器而不是中心交换机，而使用最广泛的分支集线器是共享式集线器，当用户与主机进行数据通信时，两台机器之间的数据包（单播包，Unicast Packet）还是会被同一台集线器上的其他用户所侦听。

因此，应该用交换式集线器代替共享式集线器，使单播包仅在两个节点之间传送，从而防止非法侦听。

3．划分 VLAN

为了克服以太网的广播问题，除上述方法外，还可以运用虚拟局域网（Virtual Local Area Network，VLAN）技术，将以太网通信变为点到点通信，防止大部分基于网络侦听技术的入侵。

目前的 VLAN 技术主要有基于交换机端口的 VLAN、基于节点 MAC 地址的 VLAN 和基于应用协议的 VLAN 三种。基于交换机端口的 VLAN 虽然稍欠灵活，但比较成熟，在实际应用中效果显著。基于节点 MAC 地址的 VLAN 为移动计算提供了可能性，但同时潜藏着遭受 MAC 欺诈攻击的危险。而基于应用协议的 VLAN，理论上非常理想，但实际应用尚不成熟。

在集中式网络环境下，通常将中心的所有主机系统集中到一个 VLAN 里，在这个 VLAN 里不允许有任何用户节点，从而较好地保护了敏感的主机资源。在分布式网络环境下，可以按机构或部门的设置来划分 VLAN。各部门内部的所有服务器和用户节点都在各自的 VLAN 内，互不侵扰。

VLAN 内部的连接采用交换机进行通信，而 VLAN 与 VLAN 之间的连接则采用路由器进行通信。目前，大多数交换机支持 RIP 和 OSPF 这两种国际标准的路由协议。如果有特殊需要，必须使用其他路由协议（如 Cisco 公司的 EIGRP 或支持 DECnet 的 IS-IS），则也可以用外接的多以太网口路由器来代替交换机，实现 VLAN 之间的路由功能。

无论是交换式集线器还是 VLAN 交换机，它们都需要以交换技术为核心。它们在控制广播、防止黑客进行侦听上非常有效，但同时也给一些基于广播原理的入侵监控技术和协议分析技术带来了麻烦。如果局域网内存在这样的入侵监控设备或协议分析设备，就必须选用特殊的带有 SPAN（Switch Port Analyzer）功能的交换机。这种交换机允许系统管理员将全部或某些交换端口的数据包映射到指定的端口上，提供给接在这一端口上的入侵监控设备或协议分析设备。

1.4.3 广域网安全

下面讨论广域网的安全问题，由于广域网大多采用公网来进行数据传输，所以信息在广域网上传输时被截取和利用的可能性就比在局域网上大得多。为了保护在广域网上发送和接收信息的安全，通常需要做到以下几点。

（1）除发送方和接收方外，其他人无法知悉（隐私性）。

（2）传输过程中不被篡改（真实性）。

（3）发送方能确认接收方不是假冒的（非伪装性）。

（4）发送方不能否认自己的发送行为（不可抵赖性）。

为了达到以上安全目的，广域网通常采用以下安全解决办法。

1．加密技术

加密型网络安全技术的基本思想是不依赖于网络中数据通道的安全性来实现网络系统的安全，而是通过对网络数据的加密来保障网络的安全可靠性。数据加密技术可以分为三类，即对称型加密、不对称型加密和不可逆加密。

其中，不可逆加密算法不存在密钥保管和分发问题，适用于分布式网络系统，但是其加密计算量非常大，所以通常在数据量有限的情形下使用。计算机操作系统中的口令就是利用不可逆加密算法加密的。近年来，随着计算机系统性能的不断提高，不可逆加密算法的应用逐渐增加，常用的如 RSA 公司的 MD5 和美国国家标准局的 SHS。Cisco 路由器中有两种口令加密方式：Enable Secret 和 Enable Password。其中，Enable Secret 就采用了 MD5 不可逆加密算法，因而目前尚未发现除字典攻击法外的其他破解方法。而 Enable Password 则采用了非常脆弱的加密算法（简单地将口令与一个常数进行 XOR 与或运算），目前至少已有两种破解软件。因此，建议对重要数据不用 Enable Password 加密方式。

2．VPN 技术

VPN（Virtual Private Network，虚拟专网）技术的核心是隧道技术，将企业专网的数据加密封

装后，通过虚拟的公网隧道进行传输，从而防止敏感数据被窃。VPN 可以在 Internet、服务提供商的 IP、帧中继或 ATM 网上建立。企业通过公网建立 VPN，就如同通过自己的专用网建立内部网一样，享有较高的安全性、优先性、可靠性和可管理性，而其建立周期、投入资金和维护费用却大大降低，同时为移动办公提供了可能。因此，随着公网质量的不断提高，VPN 技术也得到了广泛的应用。

但应该指出的是，目前 VPN 技术具有许多核心协议，如 L2TP、IPSec 等，这使得不同的 VPN 服务提供商之间、VPN 设备之间的互操作性成为问题。因此，企业在 VPN 建网选型时，一定要慎重选择 VPN 服务提供商和 VPN 设备。

3．身份认证技术

对于从外部拨号访问总部内部网的用户，为了解决使用公共电话网进行数据传输所带来的风险，必须更加严格控制其安全性。一种常见的做法是采用身份认证技术，对拨号用户的身份进行验证并记录完备的登录日志。较常用的身份认证技术有 Cisco 公司提出的 TACACS+及业界标准 RADIUS。

1.4.4 制定安全策略

制定安全策略是非常有必要的，虽然没有绝对的把握阻止全部的入侵行为，但是一个好的安全策略至少可以减少入侵行为的发生次数，即使发生了入侵行为也可以最快地对其做出正确反应，最大限度地减少经济损失。

系统管理员在制定安全策略的具体内容时有如下几项安全原则。

1．最小权限（Least Privilege）

对于用户不需要使用的一些功能，不要赋予相应的权限。

2．多层防御

不能只依赖一种安全结构。例如，在增强服务器的安全策略的同时，也要注意防火墙等设备的升级和维护。

3．堵塞点（Choke Point）

尽量把攻击者引入一条死胡同，让系统记录下攻击者的所有操作。

4．考虑最薄弱的点（Weakest Link）

找出整个网络中最薄弱的地方，并采取相应的防范措施。

5．团队合作（Universal Participation）

大部分安全系统需要各个人员的配合，如果有一人疏忽或不配合，那么攻击者就有可能通过这台计算机，从内部来攻击其他的计算机。

6．保持简单（Simplicity）

尽量降低系统的复杂度，越复杂的系统越容易隐藏一些安全问题，建议不要在一台服务器上配置超过两种以上的应用。

1.5 安全操作系统简介

操作系统是信息系统安全的基础设施，在信息安全方面起着决定性的作用。信息系统安全在硬件方面关键是芯片，在软件方面关键是操作系统。我国目前正在进行芯片级的研发工作，本节主要讨论操作系统方面的安全问题。

没有操作系统的安全保障，其他的安全措施就无法发挥其应有的安全防范作用。例如，防火墙等安全产品，如果基于不安全的操作系统平台上，则其安全功能是可以被旁路屏蔽的。

此外，操作系统漏洞本身给网络信息安全带来了很大问题。用户不能幻想依靠防病毒产品彻底解决安全问题。实际上，要彻底解决计算机病毒入侵等安全问题还需要安全操作系统。

安全操作系统是根据国家标准，正式通过国家权威机构评测的操作系统。达到国标第三级以上的操作系统，才是真正意义上的安全操作系统。每种操作系统都有不同的安全级别，所以不能笼统比较操作系统的安全性。需要说明的是，并不是操作系统越安全越好，安全性和实用性是一对矛盾体。用户对安全性的需求不同，这需要在安全性和实用性之间找一个平衡点。对于普通用户和客户端，安全性要求不高，注重实用性；但对于安全性要求较高的用户和服务器，适宜采用适当级别的安全操作系统。

基于安全操作系统的重要性，我国要拥有自主知识产权的安全操作系统。从目前来看，Microsoft 公司统治桌面操作系统市场可能还有相当长的时期，而在 Windows 的基础上做它的安全操作系统版本也只能是 Microsoft 公司自己来做，别人很难做到。而从技术角度讲，在 Linux 开放源代码的基础上做安全性研究和实践，就不用把资源花费在非核心的安全技术上，且更容易一些。此外，源代码开放提供了很好的发展机遇，有利促进了软件产业的发展。

开放源代码对信息安全是非常有益的，但这并不意味着开放源码软件就是安全的。开放源码是保障信息安全一个非常有效的手段，但不是唯一的手段。一个软件不管是不是开放源代码，只有根据标准，通过信息技术安全性评估才能认为是否是安全的。

中国信息系统安全基础设施建设比较薄弱，尤其是安全操作系统，由于认识上的不足和没有明显的经济利益等因素，所以没有得到足够的重视和发展。

1.6 网络管理员的素质要求

下面简要介绍一下成为网络管理员所需要的基本素质，这里列举的内容不一定全面，但是希望能对打算成为网络管理员或将要毕业的工科同学有一定的指导作用。

（1）深入地了解过至少两种操作系统，主动学习 UNIX 操作系统。能够熟练配置主机的安全选项和设置，及时了解已公布的安全漏洞，并能够及时下载相应的补丁程序。

（2）对 TCP/IP 族有透彻的了解，这是任何一个合格的网络安全管理员的必备素质。不能停留在 Internet 基本构造等基础知识上，而且还必须能够根据侦测到的网络信息数据进行准确的分析，达到安全预警，有效制止攻击和发现攻击者等防御目的。

（3）精通 Linux 系统运维管理，能熟练使用 Python、Shell 编写自动化运维脚本，因为许多基本的安全工具是用这些语言的某一种编写的。网络安全管理员至少能正确地解释、编译和执行这些程序。

（4）精通 Zabbix、Nagios、Cacti 等监控平台，熟练掌握 LVS、Nginx、JBoss、Tomcat、Keepalived 的部署和调优工作，对日志具有一定的分析能力。

（5）熟练掌握英语读写能力，能阅读相关英文版安全文档。

（6）有丰富的系统故障排查和解决经验，以及突出的分析和解决问题的能力，并能进行技术方案的整合；有良好的沟通协调能力、学习能力；熟悉单位网络中的各种信息，如硬件信息（应识别其构造、制造商、工作模式及每台工作站、路由器、集线器、网卡的型号等）、网络正在使用的协议、网络规划（如工作站的数量、网段的划分、网络的扩展）及其他信息（如网络内部以前一直实施中的安全策略的概述，曾遭受过的安全攻击的历史记录等）。

1.7 校园网的安全

国内校园网的安全问题由来已久，由于意识与资金方面的原因，以及对技术的偏好和运营意识的不足，校园网普遍存在“重技术、轻安全、轻管理”的现象，常常只是在内部网与互联网之间放一个防火墙就万事大吉，有些学校甚至在没有任何防护措施下直接连接互联网，这就给计算机病毒、黑客提供了充分施展身手的空间，导致整个校园网处于危险之中。

校园网的安全威胁既有来自校内的，也有来自校外的，只有将技术和管理都重视起来，才能切实构筑一个安全的校园网。

1.7.1 校园网安全的特点

高等教育系统和科研机构是互联网诞生的摇篮，也是最早的应用环境。各国的高等教育系统都是较早建设和应用互联网技术的行业之一，中国的高校校园网一般最先应用最先进的网络技术，网络应用广泛，用户群密集而且活跃。然而，校园网由于自身的特点也是安全问题比较突出的地方，安全管理也更为复杂、困难。

与政府或企业网相比，高校校园网的以下特点导致安全管理非常复杂。

1．校园网的速度快和规模大

高校校园网是最早的宽带网络，普遍使用的以太网技术决定了校园网最初的带宽不低于100Mb/s，目前普遍使用千兆甚至万兆实现园区主干互联。校园网的用户群体一般较大，少则数千人，多则数万人。中国的高校学生一般是集中住宿制，因而用户群比较密集。正是由于高带宽和大用户量的特点，网络安全问题一般蔓延快，对整个校园网的影响比较严重。

2．校园网中的计算机系统管理比较复杂

校园网中的计算机系统的购置和管理情况非常复杂。例如，学生宿舍中的计算机一般是学生自己花钱购买、自己维护。这种情况下要求所有的端系统实施统一的安全政策（如安装防病毒软件、设置可靠的口令）是非常不现实的。由于没有统一的资产管理和设备管理，出现安全问题后通常无法分清责任。比较典型的现象是，用户的计算机接入校园网后感染计算机病毒，反过来这台感染了计算机病毒的计算机又影响了校园网的运行，于是出现了终端用户和网络管理员相互指责的现象。有些计算机甚至服务器系统建设完毕之后，出现无人管理被攻击者攻破作为攻击的跳板也无人觉察的现象。

3．活跃的用户群体

高等学校的学生通常是最活跃的网络用户，对网络新技术充满好奇，勇于尝试。有些学生会尝试使用网上学到的甚至自己研究的各种攻击技术，可能对网络造成一定的影响和破坏。

4．开放的网络环境

教学和科研的特点决定了校园网环境应该是开放的，管理也是较为宽松的。例如，企业网可以限制 Web 浏览和电子邮件的流量，甚至限制外部发起的连接进入防火墙，但是在校园网环境下，这些通常是行不通的，至少在校园网的主干不能实施过多的限制，否则一些新的应用、新的技术很难在校园网内部实施。

5．有限的投入

校园网的建设和管理通常都轻视了网络安全，特别是管理和维护人员方面的投入明显不足。在中国大多数的校园网中，通常只有网络中心的少数工作人员负责网络安全，他们只能维护网络的正常运行，无暇顾及，也没有条件管理和维护数万台计算机的安全。因此，院、系一级的专职计算机系统管理员要加强对网络安全的防护工作，至少做好初级的网络防护工作。

6．盗版资源泛滥

由于缺乏版权意识，盗版软件、影视资源在校园网中被普遍使用，这些软件的传播一方面占用了大量的网络带宽，另一方面给网络安全带来了一定的隐患。例如，Microsoft 公司对盗版的操作系统的更新做了限制，安装盗版的计算机系统会留下大量的安全漏洞。另外，从网络上随意下载的软件中可能隐藏木马、后门等恶意代码，许多系统因此被攻击者入侵和利用。

1.7.2 校园网安全的隐患

随着校园网规模的不断扩大，网络安全事件的影响日益广泛，网络安全也越来越难以保障，仅仅靠少数几个网络管理员和几台防火墙是远远不够的，重要的是提高用户的整体安全意识。就长期而言，校园网中最突出的仍然是垃圾电子邮件、不规范的程序代码和内部安全三大问题。下面详细介绍这三大问题。

1．垃圾电子邮件

垃圾电子邮件大量产生的原因是，垃圾电子邮件的发送者可以利用“最小的成本”获得最大的利益，或者采取网络钓鱼的方式入侵计算机并获得被害者的敏感数据。校园网中巨大的用户数量及用户淡薄的防护意识都使其成为较严重的受害者之一。

除商业利益的驱使外，计算机病毒、蠕虫脚本的传播也是垃圾电子邮件产生的原因，垃圾电子邮件的泛滥使整个校园网的运行效率变得越来越低下。本书后面的章节会介绍一款校园网电子邮件系统。

2．不规范的程序代码

随着教育信息化的大力推进，教育信息网、学科资源网站、区域性的教育门户网站大量地建立起来。网站的开发大多是由在校的师生完成的，在建立网站的时候，开发者考虑最多的是内容的丰富性、宣传效应及访问量，而忽视了网站代码的安全性。

这是因为，随着 B/S 模式应用开发的发展，使用这种模式编写应用程序的程序员也越来越多，许多师生通过简单的学习和培训就可以利用 ASP.NET、PHP 等语言建立动态管理的网站，而非专业人员在设计中没有对网站的编写规范进行安全检查，不引用安全控件，造成注入式攻击，或者网站报错页面没有修改，导致攻击者故意输入错误参数，通过报错页面获得数据库的真实参数，从而导致网站受到攻击。

3．内部安全

教育网信息安全领域存在的另一个普遍性的问题就是“重外轻内”，用户将注意力集中于防范来自网络外部的恶意攻击，但是实际情况是，高校有很多学生的计算机相关技术水平非常高，甚至超乎管理人员的想象。在这种情况下，高校校园网如何能够保证网络的安全运行，同时又能提供丰富的网络资源，达到办公、教学及学生上网的多种需求成为一个难题。相比来自外部的攻击，来自局域网内的攻击更为可怕，威胁更大。由此可见，目前很多高校校园网的安全环境可以用“内外交困”来形容。

近年来，注重校园网内网安全的呼声越来越高。

1.7.3 校园网安全重点在管理

针对目前高校校园网安全现状，要想提高校园网的安全性，重点是提高和完善校园网的管理机制。校园网需要完善和补充的管理机制如下。

1．规范出口管理

实施校园网的整体安全架构，必须解决多出口的问题。对出口进行规范统一的管理，为校园网的安全提供最基础的保障。

2．配备完整系统的网络安全设备

在网内接口和网外接口处配置一定的网络安全设备就可防止大部分的攻击和破坏行为，一般包括防火墙、入侵检测系统、漏洞扫描系统、网络版的防病毒系统等。另外，通过配置安全产品可以实现对校园网进行系统的防护、预警和监控，对大量的非法访问和不健康信息起到有效的阻断作用，对网络的故障可以迅速定位并排除。

3．解决用户上网身份问题

建立全校统一的身份认证系统。校园网必须要解决用户上网身份问题，而身份认证系统是整个校园网安全体系的基础，否则即使发现了入侵行为，也无法确定肇事者。因此，只有建立了基于校园网的全校统一身份认证系统，才能彻底地解决用户上网身份问题，同时为校园信息化的各项应用系统提供安全可靠的保障。

4．严格规范上网行为

对上网行为进行集中监控和管理。上网用户不但要通过统一的校级身份认证系统确认，而且，合法用户上网的行为也要受到统一的监控，上网行为的日志要集中保存在中心服务器上，保证这个记录的法律性和准确性。

5．出台网络安全管理制度

网络安全的技术是多样化的，网络安全的现状还是“道高一尺，魔高一丈”，因此管理的工作就愈发重要和艰巨，必须要做到及时进行漏洞修补和定期巡检，以保证对网络的监控和管理。

习题

1．为什么需要网络安全？

2．如何具体配置一个安全的校园网？