第 18 章思考题和补充习题

1、何谓安全攻击（security attack）？安全攻击有哪些种类？对安全攻击的防卫方法有哪些？
2、对安全机制和安全服务给予简单描述。
3、报文的保密性和报文的完整性有何不同？保密性和完整性能否只要其中的一个而不要另一个？
4、拒绝服务（DOS—Denial Of Service） 和分布式拒绝服务（DDOS—Distributed DOS）这两种攻击是怎样产生的？
5、对加密/解密技术的种类进行归纳？
6、公开密钥加密技术中，同一对密钥既可用于报文加密，又可用于报文鉴别，此话对吗？
7、能否举一个实际的 RSA 加密和解密的例子？
8、有兴趣的话，请证明 RSA 密码体制的解密公式 $M=C^d \bmod n$ 。
9、RSA 加密能否被认为是保证安全的？
10、报文摘要并不对传送的报文进行加密。这怎么能算是一种网络安全的措施？不管在什么情况下永远将报文进行加密不是更好一些吗？
11、按网络分层体系结构概述 IP 网络的安全性。
12、相对于应用层而言，比较网际互联层安全机制和传输层安全机制的优缺点。
13、简述防火墙的类型。
14、什么是堡垒主机？堡垒主机有几种？屏蔽主机防火墙和屏蔽子网防火墙有何区别？
15、在防火墙技术中，分组过滤器工作在哪一个层次？
16、试破译下面的密文诗。加密采用替代密码，使得 26 个字母（从 a 到 z）中的每一个用其他某个字母替代（注意，不是按序替代）。密文中无标点符号。空格未加密。

kfd ktbd fzm eubd kfd pzyiom mztx ku kzyg ur bzha kfthcm ur mfudm zhx
mftnm zhx mdzythc pzq ur ezsszcdm zhx gthcm zhx pfa kfd mdz tm sutythc
fuk zhx prfdkfdi ntcm fzld pthcm sok pzck z stk kfd uamkdim eitdx sdruid
pd fzld uoi efzk rui mubd ur om zid uok ur sidzkf zhx zyy ur om zid rzk
hu foiia mztx kfd ezindhkdi kfda kfzhgdx ftb boef rui kfzk

17、下面一段密文本来是连续的字串，只是为了便于阅读将它分成每五个一组。明文是一般计算机教科书中的一段话，因此也许有“ computer ”这个字出现。加密采用的是置换密码，明文中无空格，无标点符号。试破译之。

aauan cvlre rurnn dltme aeepb ytust iceat npmey iicgo gorch srsoc nntii
imiha oofpa gsivt tpsit lbolr otoex

18、常规密钥体制与公开密钥体制的特点各如何？各有何优缺点？
19、链路加密与端到端加密各有何特点？各用在什么场合？
20、采用 DES 加密算法和加密分组链接的方法。在传输过程中，某一个密文分组 C_i 中的一个 0 变成了 1。试问：在对应的明文中会出现多少个错误？
21、在上题中，若不是一个 0 变成了 1 而是在 C_i 中多出了一个 0。试分析明文中会出现什么
22、使用 RSA 公开密钥体制进行加密。设 a=1，b=2，等等。

（a）若 p=7 而 q=11，试列出 5 个有效的 e。
（b）若 p=13，q=31，而 e=7，问 d 是多少？
（c）若 p=5，q=11，而 d=27，试求 e，并将“ abcdefghij ”进行加密。

第 18 章思考题和补充习题参考答案

1、何谓安全攻击（security attack）？安全攻击有哪些种类？对安全攻击的防卫方法有哪些？

解答

安全攻击是指危及某个机构所拥有信息之安全的任何行为。

主要的安全攻击种类分为中断（interruption）、截获（interception）、篡改（modification）和伪造（fabrication）。中断危及到信息的可用性（availability），如使信息系统失效或资源耗尽而拒绝服务，信息系统的文件因感染病毒而被破坏等；截获危及信息的保密性（confidentiality），如分析通信线路或设施上的通信量，泄露报文内容等；篡改危急信息的完整性（integrity），如未经授权对报文内容进行非法修改；伪造危及信息的真实性（authenticity），如伪装成另一个网络实体获取某些额外特权，或者截获一个合法的报文然后重新传输以达到非法侵入的信息系统或获取未经授权访问的信息等目的。截获并不侵入信息系统，只在信息传输途中进行攻击，因此称为被动攻击（passive attack），其它攻击种类则归属于主动攻击（active attack）一类。

对安全攻击的防卫可以采用加密技术、安全策略以及物理的、软件或硬件的控制方法来实现。

2、对安全机制和安全服务给予简单描述。

解答

安全机制用于检测、防范安全攻击以及能够从遭受的攻击状态下恢复。安全服务利用一种或多种安全机制，提高信息系统以及信息传送中的安全性。

3、报文的保密性和报文的完整性有何不同？保密性和完整性能否只要其中的一个而不要另一个？

解答

报文的保密性和完整性是完全不同的概念。

保密性的特点是：即使加密后的报文被攻击者截获了，攻击者也无法了解报文的内容。

完整性的特点是：接收者收到报文后，知道报文没有被篡改。

保密性和完整性都很重要。

有保密性而没有完整性的例子：接收者收到一份可能遭到攻击的加密报文“ 明日 6 时发起进攻 ”。攻击者破译不了被截获的报文，但随意更改了一些比特（攻击者也不知道更改后的密文将会使解码后得出的明文变成什么样子）。接收者收到的还是密文。他认为别人不会知道密文的内容，于是用密钥将收到的密文进行解码，但得到的明文已经不再是原来的明文了。原来的明文是 “ 明日 8 时发起进攻 ”，现在却提前了 2 小时。当然也可能将被篡改的密文解码后变得看不懂意思的明文，在这种情况下也许还不致产生有危害的后果。

有完整性而没有保密性的例子是对明文加上保证其完整性的措施。接收者收到明文后，就可以相信这就是发送者发送的、没有被篡改的报文。这个报文可以让所有的人都知道（不保密），但必须肯定这个报文没有被人篡改过。

可见保密性并不是永远都需要的，但完整性往往总是需要的。这样的例子很多。大家都知道，人民日报所登载的新闻对全世界的所有人都是公开的，没有什么秘密可言。但报纸上的新闻必须保证其完整性（读者不会怀疑报纸的印刷单位擅自改动了新闻的内容）。如果新闻被恶意地篡改了就会产生极其严重的后果。现在有些情况不允许使用电子邮件（例如导师给某个学校发送为某学生写的正式推荐信），并不是因为推荐信有多大的机密，而是因为普通的电子邮件没有使用数字签名，它不能证明对方收到的电子邮件的确是某个导师写的并且

没有被篡改过。而从邮局寄送的、写在纸上的、有导师亲笔签名的推荐信则是可信赖的。

以上这些都说明了保密性和完整性不是一个概念。

总之，保密性是防止报文被攻击者窃取，而完整性是防止报文被篡改。

4、拒绝服务（DOS—Denial Of Service） 和分布式拒绝服务（DDOS—Distributed DOS）这两种攻击是怎样产生的？

解答

DOS 是中断攻击类型的典型例子，可以由以下几种方式产生（往往使用虚假的 IP 地址）：

(1) 向一个特定服务器非常快地发送大量任意的分组，使得该服务器过载因而无法正常工作。

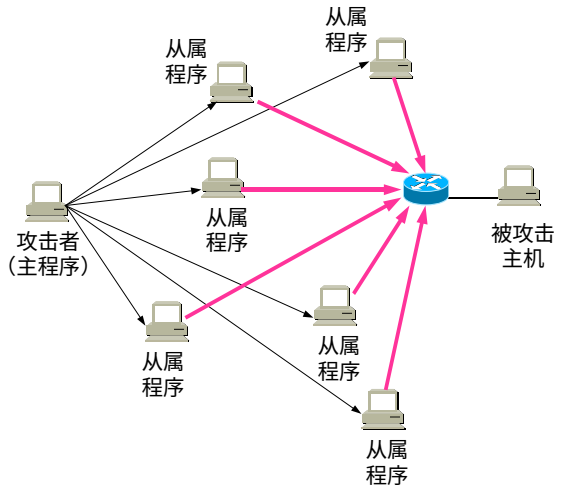
(2) 向一个特定服务器发送大量的 TCP SYN 报文段（即建立 TCP 连接的三次握手中的第一个报文段）。服务器还误以为是正常的因特网用户的请求，于是就响应这个请求，并分配了数据结构和状态。但攻击者不再发送后面的报文段，因而永远不能够完成 TCP 连接的建立。这样可以浪费和耗尽服务器的大量资源。这种攻击方式又称为 SYN flooding（意思是使用同步标志进行洪泛）。

(3) 重复地和一个特定服务器建立 TCP 连接，然后发送大量无用的报文段。

(4) 将 IP 数据报分片后向特定服务器发送，但留一些数据报片不发送。这就使得目的主机永远无法组装成完整的数据报，一直等待着，浪费了资源。

(5) 向许多网络发送 ICMP 回送请求报文（就是使用应用层的 PING 程序），结果使许多主机都向攻击者返回 ICMP 回送回答报文。无用的、过量的 ICMP 报文使网络的通信量急剧增加，甚至使网络瘫痪。这种攻击方式被称为 smurf 攻击。Smurf 是能够对网络自动发送这种 ICMP 报文攻击的程序名。

DDOS 的特点就是攻击者先设法得到因特网上的大量主机的用户账号。然后攻击者设法秘密地在这些主机上安装从属程序(slave program)，如图所示。



当攻击者发起攻击时，所有从属程序在攻击者的主程序(master program)的控制下，在同一时刻向被攻击主机发起拒绝服务攻击 DOS。这种经过协调的攻击攻击具有很大的破坏性，可以使被攻击的主机迅速瘫痪。

在 2000 年 2 月美国的一些著名网站（如 eBay, Yahoo,和 CNN 等）就是遭受到这种分布式拒绝服务的攻击。

拒绝服务和分布式拒绝服务都是很难防止的。使用分组过滤器并不能阻止这种攻击，因为攻击者的 IP 地址是事先不知道的。当主机收到许多攻击的数据报时，很难区分开哪些是

好的数据报，而哪些是坏的数据报。例如，当服务器收到请求建立 TCP 连接的 SYN 报文时，很难区分这是真的请求建立 TCP 连接，还是恶意消耗服务器资源的连接请求。当攻击者使用 IP 地址欺骗时，要确定攻击者真正的 IP 地址也是很难的。

5、对加密/解密技术的种类进行归纳？

解答

加密和解密技术分为传统的和公开密钥两大类，传统加密技术的加密和解密使用相同的密钥，所以又称为对称加密技术。而公开密钥技术的加密和解密分别使用不同的密钥，故谓非对称加密技术。

传统加密技术分为字符级加密和比特级加密两个层次。我们课上讲到的恺撒算法和行置换算法分别代表了字符级加密技术的替代方法和置换两种方法。比特级加密技术可使用替代（S 盒子）、置换（P 盒子）、乘积（P 盒子和 S 盒子的组合）、异或、循环移位等多种变换方法，典型代表是 DES 算法，比 DES 的安全性更高的比特级还有 TDEA、IDEA、AES 等。

传统的加密技术主要用于对报文内容加密，也能起一定报文鉴别作用。公开密钥加密技术也可用于报文内容加密，更广泛的应用是报文鉴别（包括数字签名）和密钥的发布和交换方面。Diffie-Hellman 算法是最早发布的公开密钥算法，在密钥交换应用中至今仍发挥着重要作用。目前更广泛采用的公开密钥算法是 RSA 算法。

6、公开密钥加密技术中，同一对密钥既可用于报文加密，又可用于报文鉴别，此话对吗？

解答

此话正确。但注意的是，此对密钥在两种应用中用法不同。

使用公开密钥对报文加密时，报文发送方使用接收方的公开密钥加密，而接收方的解密密钥是秘密的，只有接收者才知道，因此只有接收者自己才能对报文解密。

使用公开密钥实现报文鉴别时，报文发送方使用自己的保密的私钥加密，而报文接收方使用发送方的公开密钥解密，用谁的公钥能正确解密报文内容，就证明报文是谁发送的，是无法抵赖的，相当于一种是数字签名。但报文内容并不保密，因为凡持有发送者公钥的接收者都可对报文内容正确解密。

7、能否举一个实际的 RSA 加密和解密的例子？

解答

不行。我们知道，在 RSA 公开密钥密码体制中，加密密钥和解密密钥中都有一个大整数 n，而 n 为两个大素数 p 和 q 的乘积（素数 p 和 q 一般为 100 位以上的十进数）。因此加密和解密的运算需要非常大的运算量。

我们可以用一个能说明 RSA 工作原理的小例子使读者体会一下 RSA 计算量有多大。

假定选择 $p = 5, q = 7$。（显然这样小的素数是根本不能用于实用的 RSA 的加密计算中。）

这时，计算出 $n = pq = 5 \times 7 = 35$。

算出 $\phi(n) = (p - 1)(q - 1) = 24$。

从[0, 23]中选择一个与 24 互素的数 e。现在我们选 $e = 5$。

然后根据教材第 531 页 RSA 算法，有

$$ed = 5d = 1 \bmod 24$$

找出 $d = 29$, 因为 $ed = 5 \times 29 = 145 = 6 \times 24 + 1 = 1 \bmod 24$。

这样，公开密钥 PK = $(e, n) = \{5, 35\}$, 而秘密密钥 SK = $\{29, 35\}$。

明文必须能够用小于 n 的数来表示。现在 $n = 35$。因此每一个英文字母可以用 1 至 26 的数字来表示。

假定明文是英文字母 o，它是第 15 个字母。因此明文 X = 15。

加密后得到的密文 $Y = X^e \bmod n = 15^5 \bmod 35 = 759375 \bmod 35$

$$= (21696 \times 35 + 15) \bmod 35 = 15。$$

以上的计算还是很简单的。现在看一下解密的过程。

在用秘密密钥 SK = {29, 35}进行解密时，先计算 $Y^d = 15^{29}$。这个数的计算已经需要不少时间了。它等于 1278340394885893911123275756835937 5。进行模 35 运算，得出 $15^{29} \bmod 35 = 15$，而第 15 个英文字母就是 o。原来发送的明文就是这个字母。

从以上例子可以体会到使用的 RSA 加密算法的计算量是很大的。

8、有兴趣的话，请证明 RSA 密码体制的解密公式 $M=C^d \bmod n$ 。

解答

现在回顾一下 RSA 公开密钥密码体制的要点。

① 秘密选择两个大素数 p 和 q，计算出 $n = pq$。明文 $X < n$。

② 计算 $\phi(n) = (p - 1)(q - 1)$。

③ 公开选择整数 e。$1 < e < \phi(n)$。e 与 $\phi(n)$互素。

④ 秘密计算 d，使得 $ed = 1 \bmod \phi(n)$。

⑤ 得出公开密钥（即加密密钥）PK = {e, n}，秘密密钥（即解密密钥）SK = {d, n}。

⑥ 明文 M 加密后得到密文 $C = M^e \bmod n$。

⑦ 密文 C 解密后还原出明文 $M = C^d \bmod n$。

下面就来证明上面的解密公式（参考《RSA 公开密钥算法相关数论基本知识》一文）。

$C^d \bmod n = (M^e \bmod n)^d \bmod n = M^{ed} \bmod n$

但 $ed = 1 \bmod \phi(n)$ 表示 $ed = k\phi(n) + 1$，这里 k 任意整数。因此现在的问题就是要证明

$$M^{ed} \bmod n = M^{k\phi(n) + 1} \bmod n \text{ 是否等于 } M \bmod n。$$

根据欧拉定理的一个推论，就可很容易地证明上式。这个推论是这样的：给定两个素数 p 和 q，以及整数 $n = pq$ 和 m，其中 $0 < m < n$，则下列关系成立：

$$m^{k\phi(n) + 1} = m^{(p - 1)(q - 1) + 1} \equiv m \bmod n \qquad (1)$$

下面就来证明公式(1)。

根据欧拉定理的公式 $a^{\phi(n) + 1} \equiv a \bmod n$（由费马定理和欧拉函数推得），如果 m 和 n 互素，则等式(1)显然成立。

但如果 m 和 n 不是互素，则下面我们也可以证明等式(1)仍然成立。

当 m 和 n 不是互素时，m 和 n 一定有公因子。由于 $n = pq$ 且 p 和 q 都是素数，因此当 m 和 n 不是互素时，我们一定有下面的结论：或者 m 是 p 的倍数，或者 m 是 q 的倍数。

下面我们不妨先假定 m 是 p 的倍数，因此可记为 $m = kp$，这里 k 是某个正整数。在这种情况下，m 和 q 一定是互素的。因为如果不是这样，那么 m 一定是 q 的倍数（如果 m 是 q 的倍数，那么 m 就同时是 p 和 q 的倍数，这就和 $m < n = pq$ 的假定不符）。因此我们得出以下结论：如果 m 和 n 不是互素，若假定 m 是 p 的倍数，则 m 和 q 一定是互素的。

既然 m 和 q 互素，那么根据欧拉定理，我们有

$$m^{\phi(q)} \equiv 1 \bmod q$$

显然，将左端乘以任何整数次方的模 q 还是等于 1。因此

$$[m^{\phi(q)}]^{\phi(p)} \equiv 1 \bmod q$$

因为 $\phi(n) = \phi(pq) = \phi(p) \times \phi(q)$，所以上式变为

$$m^{\phi(n)} \equiv 1 \bmod q$$

可见存在某个整数 j 使得

$$m^{\phi(n)} = 1 + jq$$

将等式两端同乘以 $m = kp$，并考虑到 $n = pq$，得出

$$m^{\phi(n)+1} = kp + kpjq = m + kjn$$

取模 n，得出

$$[m^{\phi(n)+1}] \bmod n = [m + kjn] \bmod n = m \bmod n$$

因此

$$m^{\phi(n)+1} \equiv m \bmod n$$

这样就证明了公式(1)，因而也就证明了 RSA 的解密公式 $M = C^d \bmod n$。

9、RSA 加密能否被认为是保证安全的？

解答

RSA 之所以被认为是一种很好的加密体制，是因为当选择足够长的密钥时，在目前还**没有找出**一种能够对很大的整数快速地进行因子分解的算法。这里请注意，“ 在目前还没有找出 ” 并不等于说 “ 理论上已经证明不存在这样的算法 ”。如果在某一天有人能够研究出对很大的整数快速地进行因子分解的算法，那么 RSA 加密体制就不能再使用了。

10、报文摘要并不对传送的报文进行加密。这怎么能算是一种网络安全的措施？不管在什么情况下永远将报文进行加密不是更好一些吗？

解答

报文加密并非网络安全的全部内容。我们知道，使用 RSA 公开密钥体制进行加密时，往往需要花费很长的时间。当需要在网络上传送的报文并不要求保密但却不容许遭受篡改时，使用报文摘要就能够确保报文的完整性（因为这时仅仅对很短的报文摘要进行加密）。

11、按网络分层体系结构概述 IP 网络的安全性。

解答

TCP/IP 网络的网际互联层、传输层、应用层的安全性可以通过多种协议分别实现。

一、IP 层安全性

IETF 制定的网际互联安全协议 IPSEC 涉及 IP 安全协议 IPSP 和对应的 Internet 密钥管理协议 IKMP 两个方面。

IPSP 的主要目的是使需要安全措施的用户能够使用相应的加密安全体制。该体制分别扩展于 IPv4 中和包含在 IPv6 中。IPSP 规范包含鉴别首部 AH（Authentication Header）和封装安全有效负荷 ESP（Encapsulating Security Payload）。AH 提供 IP 分组的真实性和完整性，ESP 提供报文内容与受限通信流量的保密。AH 和 ESP 都支持两种使用方式：传输方式和隧道方式。传输方式只对 IP 数据报净负荷进行保护，隧道方式连同 IP 首部对整个 IP 数据报提供保护。

IPSP 用人工方式来分发密钥，而 IKMP 则实现密钥的自动交换，IPSEC 目前采纳的密钥交换几管理协议是 ISAKMP/OAKLEY 方案，即由美国国家安全署（NSA）提出的“ Internet 安全条例及密钥管理协议（ISAKMP）” 和 Hilarie Orman 提出的 “ OAKLEY 密钥决定协议 ” 结合而成。

二、传输层安全性

Netscape 公司提出的安全套接层协议 SSL 建立在如 TCP 协议所提供可靠传输服务的基

础上，提供两端实体的认证，数据加密密钥的交换等功能，旨在通过强化 Socket 等 IPC（进程间通信）接口在 Internet 中提供安全服务。Netscape 向公众发布的 SSL 参考实现 SSLref 和另一个免费的 SSL 实现 SSLeay 均可给任何 TCP/IP 应用提供 SSL 功能。Microsoft 公司也随 Windows 操作系统推出了 SSL2 的改进版本称为 PCT（私人通信技术）。

SSL 版本 3（SSL v3）于 1995 年 12 月制定。它主要包含 SSL 记录协议和 SSL 握手协议两个协议。SSL 记录协议涉及应用程序提供的信息的分段、压缩、数据认证和加密。SSL 握手协议用来交换版本号、加密算法、身份认证并交换密钥。SSL 提供了 SSL 服务器鉴别、SSL 客户鉴别、加密的 SSL 会话三方面功能。SSL 服务器鉴别允许客户证实服务器的身份，SSL 客户鉴别允许服务器证实客户的身份，加密的 SSL 会话功能可对窃听的攻击者进行检测，并要求客户和服务器交互的数据都在发送方加密，接收方解密。

IETF 基于 SSL v3 制定的一个传输层安全协议 TLSP 在许多地方酷似 SSL。

三、应用层安全性

在应用层提供安全服务的一种做法是对每个应用及应用协议分别进行修改。比如，在电子邮件的安全方面，IETF 规定了称为 PEM（私用强化邮件）的邮件安全建议标准，对为基于 SMTP 的电子邮件系统提供加密和鉴别等安全服务。PEM 依赖于公钥基础结构 PKI。PKI 按层次组织，自顶向下由 Internet 安全政策登记机构 IPRA、安全政策证书颁发机构 PCA、证书颁发机构 CA 三个层次构成。

PGP（Pretty Good Privacy）是 Zimmermann 开发的一个全面的电子邮件安全软件包，包括加密、鉴别、数字签名和压缩等技术。PGP 和 PEM 对每个报文的加密都采用一次一密，都提供了密钥管理机制，PEM 密钥管理机制比 PGP 更加完善。

S/MIME 是基于 RSA 密钥体制、在 Internet 电子邮件格式标准 MIME（Multipurpose Internet Mail Extension）上进行的安全扩充，功能与 PGP 类似。

IMAP 是一个比 POP3 复杂得多的 Internet 报文存取协议，它的鉴别和数据加密可依赖于 SSL 或 TSLP。

对于 Web 应用，企业集成技术公司设计的基于 SSL 传输层安全机制的 S-HTTP 是超文本传输协议 HTTP 的安全增强版本，提供了文件级的安全机制，因此每个文件都可以被设成私人/签字状态。用作加密及签名的算法可以由参与通信的收发双方协商。S-HTTP 提供了对多种单向散列函数、多种单钥体制和多种数字签名体制的支持，S-HTTP 和 SSL 是从不同角度提供 Web 的安全性的。S-HTTP 对单个文件作“私人/签字”之区分，而 SSL 则把参与通信的相应进程之间的数据通道按“私用”和“已认证”进行监管。Terisa 公司的 SecureWeb 工具软件包提供了对 SSL 和 S-HTTP 的全面支持。

另一个重要的应用是电子商务，尤其是信用卡交易。为使 Internet 上的信用卡交易安全起见，MasterCard 公司与 IBM，Netscape，GTE、Cybercash 一道制定了安全电子付费协议 SEPP；Visa 国际公司和 Micosoft 等公司一同制定了安全交易技术 STT 协议；同时，MasterCard、Visa 国际和 Microsoft 发布了相应的安全电子交易协议 SET，联手推出 Internet 上的安全信用卡交易服务，该机制有一个后台的证书颁发基础结构，提供对 X.509 证书的支持。

SET 的主要特点是：(1）专为与支付有关的报文进行加密；(2）涉及到顾客、商家和商业银行，三方之间敏感信息被加密；(3）要求三方都有证书，在交易中商家看不见顾客传送给商业银行的信用卡号码，这是 SET 最关键的特性。在一个 SET 交易中要用到三个软件：为顾客购物时提供信用卡及证书的存储与管理的浏览器钱包、实现商品交易的商家服务器、商业银行处理信用卡交易中授权和支付的支付网关。

12、相对于应用层而言，比较网际互联层安全机制和传输层安全机制的优缺点。

解答

网际互联层安全机制的主要优点是它的透明性，它提供的安全服务不要求应用层做任何改变。这对传输层来说是做不到的。原则上，任何 TCP/IP 应用程序只要基于传输层安全协议，就必定要进行若干修改以增加相应的功能，并使用稍许不同的 IPC 接口。

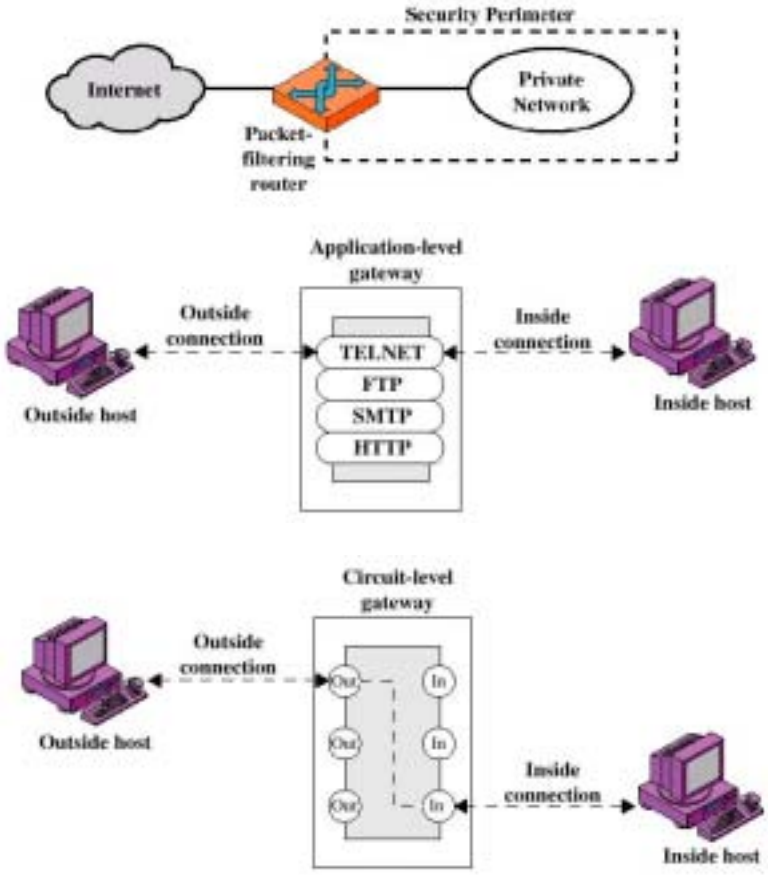
因此传输层安全机制的主要缺点就是要在传输层 IPC 接口和应用程序两端都进行修改。但比起网际互联层和应用层的安全机制来，传输层安全机制所需的修改还是相当小的。另一个缺点是，基于 UDP 的通信很难在传输层建立起安全机制来。

同网际互联层安全机制相比，传输层安全机制的主要优点是它提供基于进程对进程的安全服务，而不是象网际互联层安全机制那样提供主机对主机的安全服务。由此可以根据不同进程的需要，可以使用或不使用安全机制，可以提高网络的灵活性和传输效率。

13、简述防火墙的类型。

解答

防火墙主要有三种常见类型：分组过滤路由器（packet-filtering router）、应用级网关（application-level gateway）和电路级网关（circuit-level gateway）。



分组过滤路由器（简称分组过滤器）对进入的 IP 分组使用一组规则进行判别过滤，然后进行转发或丢弃分组。过滤规则基于 IP 首部中的源站和目的站 IP 地址、运输协议字段，以及 IP 数据字段中的 TCP 或 UDP 首部中的源进程和目的进程的端口号。

应用级网关也称代理服务器（proxy server），它担任应用级通信量的中继。用户使用应用程序与网关通信，网关询问用户打算访问的远程主机的名字，当用户回答并提供自己的合

法 ID 和鉴别信息（通常是用户名和口令）后，网关联系远程主机上的应用程序，在用户与与远程主机间建立起端到端 TCP 连接，并在两个端点间转发包含应用数据的报文段。应用级网关比分组过滤器更安全。

电路级网关可能是一个单独的系统，也可以应用级网关为特定应用程序实现的专门功能。电路级网关不允许建立端到端的 TCP 连接。相反，网关建立两个 TCP 连接，一个是网关本身和内部主机上的一个 TCP 用户之间，一个是在网关与外部主机上的一个 TCP 用户之间。一旦两个连接建立，网关从一个连接向另一个连接转发报文段，但不检查其内容。安全性体现在决定哪些连接是允许的。电路级网关比应用级网关更安全。典型的电路级网关应用是网管员信任内部用户的情况，网关可配置成在进入连接上支持应用级或代理服务，输出连接上支持电路级功能。

14、什么是堡垒主机？堡垒主机有几种？屏蔽主机防火墙和屏蔽子网防火墙有何区别？

解答

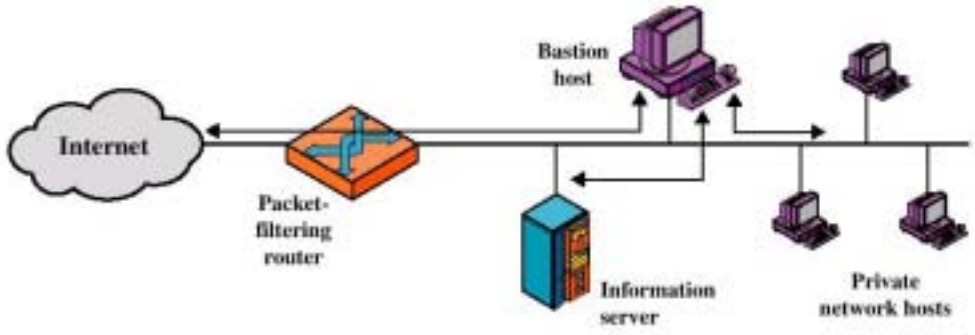


图 14（a）屏蔽主机防火墙系统（单穴堡垒主机）

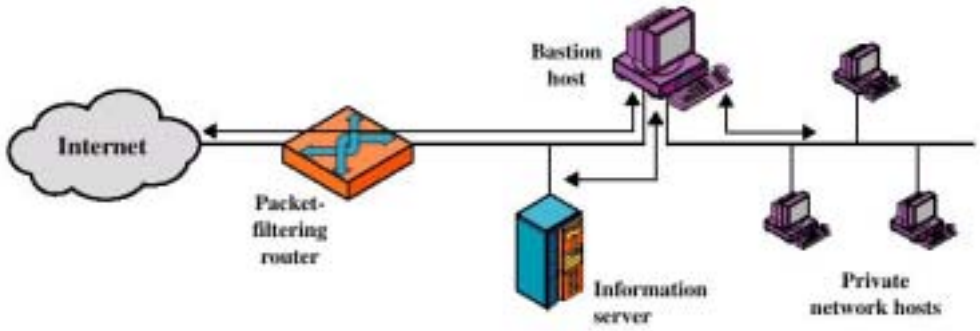


图 14（b）屏蔽主机防火墙系统（双穴堡垒主机）

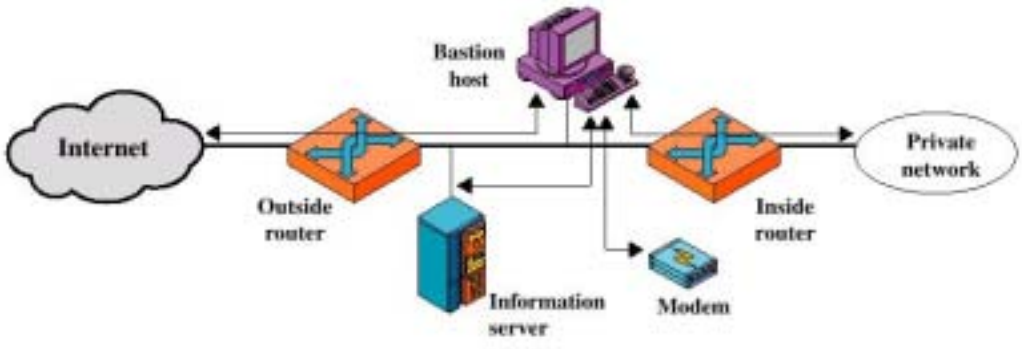


图 14（c）屏蔽子网防火墙系统

用作电路级和应用级网关的系统平台称为堡垒主机，是防火墙管理员标识的网络安全关键点。堡垒主机如果使用单个 IP 地址，称为单穴主机或单地址堡垒主机（single-homed bastion host），如果使用两个及两个以上 IP 地址，称为双穴（多穴）主机或多地址堡垒主机（dual-homed bastion host 或 multi-homed bastion host），双穴（多穴）主机一般使用两块（多块）网卡，在链路级将内外网隔开，比单穴主机方式安全。依靠堡垒主机隔离内外网络统的上述实现统称为屏蔽主机防火墙（screened host firewall）。如果在内网与堡垒主机之间增加一个路由器将内网与外网隔离，则称为屏蔽子网防火墙（screened subnet firewall）。此时由外网与堡垒主机之间连接的路由器可以是普通路由器（屏蔽主机防火墙方案的外网与堡垒主机之间需要分组过滤路由器），连接堡垒主机的内外网路由器之间（堡垒主机所在网段，通常 Web 服务器配置于此）戏称为“ 非军事区 ”。

15、在防火墙技术中，分组过滤器工作在哪一个层次？

解答

分组过滤器工作在网络层，但也可以把运输层包含进来。

大家知道，路由器工作在网络层。防火墙中使用的分组过滤器就是安装在路由器中的一种软件。从这个意义上讲，分组过滤器当然也应当是工作在网络层。而且，本来“ 分组 ”就是网络层的协议数据单元名称，分组过滤器根据所设置的规则和进入路由器的分组的 IP 地址（源地址或目的地址）决定对该分组是否进行阻拦。这样的分组过滤器当然是工作在网络层。

但是，为了增强分组过滤器的功能，一些分组过滤器不仅检查分组首部中的 IP 地址，而且进一步检查分组的数据内容，也就是说，检查运输层协议数据单元的首部。这主要是检查端口号。这样做的目的是可以进一步限制所通过的分组的服务类型。例如，阻拦所有从本单位发送出去的、向计算机 192.50.2.18 请求 FTP 服务的分组。由于 FTP 的熟知端口号是 21，因此只要在分组过滤器的阻拦规则中写上“ 禁止到目的地址为 192.50.2.18 且目的端口号为 21 的所有分组 ”即可。因此，这样的分组过滤器不仅工作在网络层，而且还工作在运输层。从严格的意义上讲，这样的路由器已经不是仅仅单纯工作在网络层了。

当然，像上面给出的规则，也可以由应用网关（即代理服务器）来实现。

16、试破译下面的密文诗。加密采用替代密码，使得 26 个字母（从 a 到 z）中的每一个用其他某个字母替代（注意，不是按序替代）。密文中无标点符号。空格未加密。

kfd ktbd fzm eubd kfd pzyiom mztx ku kzyg ur bzha kfthcm ur mfudm zhx
mftnm zhx mdzythc pzq ur ezsszcdm zhx gthcm zhx pfa kfd mdz tm sutythc
fuk zhx prfdkfdi ntcm fzld pthcm sok pzck z stk kfd uamkdim eitdx sdruid
pd fzld uoi efzk rui mubd ur om zid uok ur sidzkf zhx zyy ur om zid rzk
hu foiia mztx kfd ezindhkdi kfda kfzhgdx ftb boef rui kfzk

解答

单字母表是：

明文：a b c d e f g h i j k l m

密文：z s e x d r c f t g y b

明文：n o p q r s t u v w x y z

密文：h u n I m k o l p q a

根据该单字母表，可得到下列与本题中给出的单字母表密码对应的明文：

the time has come the walrus said to talk of many things

of shoes and ships and sealing wax of cabbages and kings
of why the sea is boiling hot and whether pigs have wings
but wait a bit the oysters cried before we have our chat
for some of us are out of breath and all of us are fat
no hurry said the carpenter they thanked him much for that

17、下面一段密文本来是连续的字串，只是为了便于阅读将它分成每五个一组。明文是一般计算机教科书中的一段话，因此也许有“ computer ”这个字出现。加密采用的是置换密码，明文中无空格，无标点符号。试破译之。

aauan cvlre rurnn dltme aeepb ytust iceat npmey iicgo gorch srsoc nntii
imiha oofpa gsivt tpsit lbolr otoex

解答

明文是“ a digital computer is a machine that can solve problems for people by carrying out instructions given to it ”

密钥 6 个字母，例如 ABCDE，明文按行书写，从第 1 列开始按列生成密文如下：

A	B	C	D	E	F
a	d	i	g	i	t
a	l	c	o	m	p
u	t	e	r	i	s
a	m	a	c	h	i
n	e	t	h	a	t
c	a	n	s	o	l
v	e	p	r	o	b
l	e	m	s	f	o
r	p	e	o	p	l
e	b	y	c	a	r
r	y	i	n	g	o
u	t	i	n	s	t
r	u	c	t	i	o
n	s	g	i	v	e
n	t	o	i	t	x

18、常规密钥体制与公开密钥体制的特点各如何？各有何优缺点？

解答

常规密钥体制的特点是加密密钥与解密密钥相同，加解密的双方使用相同的密钥。因此，在双方进行保密通信之前必须持有相同的密钥。而公开密钥体制的特点是加密密钥（即公开密钥）与解密密钥（即秘密密钥）不相同，解密密钥是保密的，但加密密钥、加密算法都是公开的，虽然解密密钥是由加密密钥决定的，但却不能根据加密密钥算出解密密钥。因此，在公开密钥体制下，通信双方持有不同的密钥的密钥。公开密钥算法有以下特点：

①用加密密钥 PK 对明文 X 加密后，再用解密密钥 SK 解密可得明文，即 $D_{SK}(E_{PK}(X))=X$，且加密和解密运算可以对调，即 $E_{PK}(D_{SK}(X))=X$；

②不能用加密密钥解密，即 $D_{PK}(E_{SK}(X))\neq X$；

③在计算机上可以容易地产生成对的 PK 和 SK；

④但从已知的 PK 不可能推导出 SK。

（2）常规密钥体制分序列密码和分组密码两种体制，序列密码体制的优点是保密性决定于密钥的随机性，如果密钥是真正的随机数，在理论上是不可破的，但所需密钥量大得惊人，实际上很难满足；分组密钥体制，将明文分成定长比特的数据组，一次变换一组，当给定一个密钥后，分组密码算法总是把明文分组变换成同样长度的密文组，分组密码的一个重要优点是不需要同步，在分组交换网中应用广泛。分组密码中最有名的是数据加密标准 DES。DES 的算法是公开的，其保密性仅取决于对密钥的保密性。

常规密钥体制的缺点：

①由于通信双方必须有相同的密钥，这就存在密钥分配问题。虽然采用高度安全的密钥分配中心可以实现密钥分配自动化，但使网络成本增加，性能降低。

②如果两个未见面的人要进行通信，必须事先协商密钥。

③难以实现数字签名。

公开密钥体制相对于常规密钥体制有以下优点：

①对于一个常规密钥体制，每对用户间都需要一个互不相同的密钥。这样，n 个用户的系统将需要 $n\times(n-1)/2$ 个密钥。随着用户数的增加，密钥数将迅速增加，测定和分配如此多的密钥是一个难题。同时，由于用户不可能记住如此多的密钥，如何维护已经分配的密钥并保证其安全也是一个严重的问题。而公开密钥体制，每个用户只要两个密钥，一个加密密钥，一个解密密钥，任何用户都可以用 A 的加密密钥（因是公开的）加密给 A 用户的报文。根据公开密钥的特点①和②知，除用户 A 能解密外，其他用户无法将其解密出来，因此任何用户都可以给用户 A 发送一份秘密报文，且报文是受到保护的，可以防止窃听者阅读。

②公开密钥算法比常规密钥算法更容易实现数字签名。

公开密钥体制的缺点：

①在公开密钥体制中，每个用户只要具有其他用户的公开密钥，就可以实现安全通信。其实不然，由于密钥更换、增加和删除的频度很高，另外虽然公开密钥不需保密，但必须保证公开密钥的完整性，否则不能保证安全性，分配大量的公开密钥有保证其完整性是一项十分复杂的工作。

②公开密钥相当长，人工输入密钥相当麻烦且易出错。

因此，公开密钥体制仍需进行网内密钥分配。

19、链路加密与端到端加密各有何特点？各用在什么场合？

解答

（1）链路加密是对网络的每条通信链路上传输的数据进行加密，一般使用不同的加密密钥，但在结点中数据却以明文形式出现。因此，链路加密有以下特点：

①能防止各种形式的通信量分析。这里是因为整个 PDU 被加密，掩盖了源、目的结点的地址，当结点间保持连续的密文序列时，还掩盖了 PDU 的频度和长度。

②链路加密不需传输额外的数据，不会降低网络的有效带宽。

③由于相邻结点之间具有相同的密钥，因而密钥管理容易实现。

④链路加密的功能由通信子网提供，加密在 1 或 2 层实现，所以链路加密对用户是透明的。

⑤由于报文在各结点进行加密和解密，在结点内以明文形式出现，要求各结点必须是安全三，否则将威胁整个网络的安全。因此，仅采用链路加密在网络互联的情况下，不能实现安全通信。

⑥链路加密不适应广播网络，因为广播网络没有明确的链路存在，若将整个 PDU 加密，将无法确定接收者和发送者。

（2）端到端加密在源、目的结点对被传送的 PDU 进行加密和解密，具有如下特点：

①端到端加密的层次选择有一定的灵活性，容易适合不同用户的要求，不仅适用互联网环境，也可用于广播网。这是因端到端加密的范围在通信子网之外，要在运输层或其以上层次实现。

②为了保证中间结点正确选择路由，不能对 PDU 的控制信息加密，因而，端到端加密容易受到通信量分析的攻击。

③由于各结点必须持有与其他结点相同的密钥，端到端加密需要在全网范围内对密钥进行管理和分配。

20、采用 DES 加密算法和加密分组链接的方法。在传输过程中，某一个密文分组 C_i 中的一个 0 变成了 1。试问：在对应的明文中会出现多少个错误？

解答

在采用了加密分组链接的（CBC）方法的 DES 加密相当彻底地混合了一个分组中的位，因此在密文分组 C_i 中的单个位错将完全地破坏了明文分组 P_i。此时在第出 $i+1$ 个明文分组 P_{i+1} 中也将有一位错。然后，所有后随的明文分组都将是正确的。因此单个位错仅影响两个明文分组。

21、在上题中，若不是一个 0 变成了 1 而是在 C_i 中多出了一个 0。试分析明文中会出现什么样的错误？

解答

由于多出的“ 0 ”将变成密文分组 C_{i+1} 的第 1 位，现在从 P_{i+1} 开始的每一个明文分组都是错误的，因为对异或操作的所有输入（C_{i+1}，C_{i+12}，…）都将是错误的。显然成帧错误要比单个位翻转的错误严重得多。

22、使用 RSA 公开密钥体制进行加密。设 a=1，b=2，等等。

（a）若 p=7 而 q=11，试列出 5 个有效的 e。

（b）若 p=13，q=31，而 e=7，问 d 是多少？

（c）若 p=5，q=11，而 d=27，试求 e，并将“ abcdefghij ”进行加密。

解答

（a）p=7，q=11，z=（p－1）×（q－1）=6×10=60

因此，d 是一个与 60 互为质数的数，d 的 5 个可能的值是 7，11，13，17 和 19。

（b）p=13，q=31，d=7，z=12×30=360

∵e×d=1 mod z

∴7e=1 mod 360

那么 7e 可能是 361，721，1081，1441 等

用 7 去除这些数中的每一个，看哪一个可以被 7 整除。结果发现，721÷7=103

∵e=103

（c）p=5，q=11，d=27

z=4×10=40　　n=5×11=55　　27e=1 mod 40

27e 可能是 41，81，121 等

∵81 可以被 27 整除，∴e=81÷27=3

为加密 P，我们使用 $C=P^3 \bmod n=P^3 \bmod 55$。

对于 P=1 到 P=10（分别对应 abcdefghij）求得 C 分别等于 1，8，27，9，15，51，13，17，14 和 10。