第1章 绪 论

1.1 信息安全

信息安全是一个综合性的交叉学科，它涉及数学、密码学、计算机、通信、控制、人工智能、安全工程、人文科学、法律等诸多学科。近15年来，计算机、通信和网络技术的快速发展大大促进了对信息进行获取、处理、储存、传输等操作方面的能力，同时也拓宽了信息应用的范围。

当今，互联网已广泛普及到个人、社会、政治、军事等领域。通过各种通信网络、计算机，或其他通信终端对信息进行获取、处理、存储、传输等操作，信息随时都可能受到非授权的访问、篡改或破坏，也可能被阻截、替换而导致无法正确读取。

对信息所进行的各种非授权的操作是对信息进行有意的破坏，如网络黑客的攻击和病毒感染。而对信息的各种误操作或程序出错，则可导致信息的无意破坏。

1.1.1 信息安全的目的

信息安全的内容十分丰富，随着计算机网络的广泛应用，在近15年来得到了快速发展。国际上已经把信息安全的概念扩展为信息保障(information assurance，IA)，即信息的保护(protect)、检测(detect)和恢复(restore)。信息保护的目标，也就是信息安全的目的，主要是指保护信息的机密性(confidentiality)、完整性(integrity)、不可抵赖性(non-repudiation)，以及可用性(availability)。也可以简单地说，信息安全的目的就是要保障网络环境下数字信

息的有效性。

机密性是对抗敌手被动攻击，保证信息不泄露给未经授权的主体(个人、组织或系统)。完整性是对抗敌手主动攻击，防止信息被未经授权的主体篡改。防抵赖性是指主体无法在事后否认曾经对信息进行发送、接收等操作。可用性是保证信息及信息系统确实可随时为经授权的主体所用(对信息进行访问或操作)而不受到干扰或阻碍。

1.1.2 信息安全中攻击的基本类别

在网络环境下，按攻击者对信息所采用的攻击手段，攻击主要可分为非授权访问、假冒和拒绝服务 3 种。从攻击是否对数据的正常使用产生影响来看，可把攻击分为主动攻击(active attack)和被动攻击(passive attack)两种。

1. 非授权访问

非授权访问是指未经授权的主体获得了访问网络资源的机会，并有可能篡改信息资源。这种访问通常是通过在不安全信道上截取正在传输的信息或者利用技术及产品中固有的弱点来实现的。

防止非授权访问的最佳方法是采用加密和识别技术对信息进行加密和鉴别编码，使攻击者无法窃听和篡改在不安全信道上传输的信息。

2. 假冒

假冒是指通过出示伪造的凭证来冒充别的主体的能力。非授权访问通常是假冒的基础，同时又是假冒的目的，二者有很密切的联系。它们的差别是，假冒通过欺骗对方获得授权，而非授权访问则绕过授权机制对信息进行访问。

假冒攻击可分为重放、伪造和代替 3 种。重放攻击是先把消息记录下来，然后再发送出去，利用身份验证机制或协议中的漏洞

进行欺骗；伪造攻击是指提供冒充主体身份的信息，以获得对系统及其服务的访问权力；代替攻击则通过分析截获的消息，构造一种难以辨别真伪的身份信息取代原来的消息，破坏正常的访问行为。利用加密、数字签名技术，可以在一定程度上阻止假冒攻击的发生。

3. 拒绝服务

拒绝服务(denial of service，DoS)是指通过对网络或服务基础设施的摧毁、非法占用等手段，使系统永久或暂时不可用。例如摧毁计算机硬盘、切断物理连接和耗尽所有可用内存。

DoS 攻击经常是由于网络协议本身存在的安全漏洞和软件实现中考虑不周共同引起的。为软件安装补丁可以避免某些 DoS 攻击。例如，许多软件开发商都为他们的 IP 应用添加了补丁程序，从而防止入侵者利用 IP 重装配错误的问题。只有少数 DoS 攻击不可避免，但仍然可以限制其影响范围。

4. 主动攻击与被动攻击

主动攻击是指篡改信息的攻击。主动攻击通过对信息的修改或对网络设施的更改，产生实时的破坏，如修改别人的网页，有选择地删除、添加、伪造和复制信息。主动攻击可危害到信息的完整性和可用性。它以各种方式，造成信息破坏。主动攻击容易发现。

被动攻击是指对信息的保密性进行攻击。被动攻击一般是通过隐蔽的措施窃取机密数据而不对其进行修改，如破译别人的密码系统。被动攻击具有潜在的危害性，难以觉察。两类攻击在网络环境与单机环境中又有不同的表现。

在网络环境中，主动攻击可表现为：篡改(插入、删除、代替)、伪造、时间攻击(重放、延迟)等；而被动攻击则表现为：窃听、流量分析等。

在单机环境中，主动攻击可表现为：病毒、Trojan 木马、非授

权访问、拒绝服务、破坏系统、篡改数据等；而被动攻击则表现为：偷阅、泄露、推断等。

1.1.3 信息安全的基本模型

信息安全的基本模型是指保密通信模型。该模型一般由至少两个主体(通信双方)、一个可信第三方、攻击者、信道、加密算法，以及有关通信协议诸要素所组成，如图 1.1 所示。

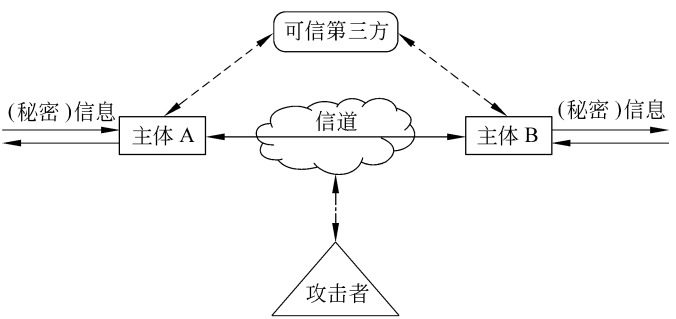

图 1.1 信息安全的基本模型

通信主体又称为用户，可为个人、某个组织或某个系统。主体 A 可作为发送者将消息加密后直接发送给作为消息接收者的主体 B，也可通过可信第三方将消息发送给主体 B，反之亦然；可信第三方是指通信双方都信赖的某主体，其作用是向通信双方发布秘密信息、分发密钥、身份识别，或在通信双方发生争议时进行仲裁；攻击者指信息的窃取者或破坏者；信道在这里可指任何公开的通信线路或网络；加密算法用于伪装或隐藏在信道上传送的信息；通信协议是指使得各通信主体能够使用加密算法以及共享密钥等秘密信息，以获得安全服务所必须执行的若干项规定。

1.1.4 信息安全研究的基本内容

信息安全的基本内容就是研究信息和承载信息的系统的事先保护,以免信息受到各种攻击的破坏。如果不能保证信息防护措施的有效性,则对攻击事件快速响应(如发现攻击行为后,切断网络连接)和对攻击造成的灾难的恢复(如对数据进行备份恢复)将是重要的补救措施,它们是近年来兴起并得到快速发展的课题。

信息安全的研究内容大致可分为基础理论研究、应用技术研究以及安全管理研究。基础研究包括密码理论研究与安全理论研究。

安全理论主要是研究在单机或网络环境下信息保护的基本理论,主要有身份识别、访问控制、安全协议等。

应用技术研究,即安全技术研究,重点是研究在单机或网络环境下信息保护的应用技术,主要有防火墙技术、入侵检测技术和漏洞扫描技术等。

安全管理研究主要包括安全标准、安全策略、安全审计、安全测评等方面的研究。在信息安全领域有一个较普遍的观点:信息安全三分靠技术,七分靠管理。所以,安全管理研究也是非常重要的一个研究内容。

1.2 密 码 学

密码学是研究信息及信息系统安全传统的科学,它起源于保密通信技术。密码学又分为密码编码学(cryptography)与密码分析学(cryptanalysis)。研究如何对信息编码,以实现信息及通信保密的科学称为密码编码学;研究如何破解或攻击加密信息的科学称为密码分析学。

密码学是在编码与破译的矛盾斗争中逐步发展起来的,并随着计算机等先进科学技术的发展与应用,已成为一门综合性、交叉

性的学科。它与语言学、数学、电子学、信息论、计算机科学等有着广泛而密切的联系。

1.2.1 密码学发展简史

密码学的发展大致可分为 4 个阶段：第一个阶段是指第一次世界大战之前的古典密码术(手工操作密码)，它有几千年的历史；第二个阶段是指第一次世界大战爆发至第二次世界大战结束期间的机器密码时代；第三个阶段是以 C. E. Shannon 在 1949 年发表的文章“The Communication Theory of Secrecy Systems”为起点的传统密码学；第四个阶段是以 W. Diffie 和 M. E. Hellman 在 1976 年发表的文章“New Directions in Cryptography”为起点的现代公钥密码学。

1. 古典密码术

古典密码的特征主要是以纸和笔进行加密与解密操作的密码术时代，这时密码还远没有成为一门科学，仅仅是一门技艺或技术。古典密码的基本技巧都是较简单的代替、置换，或二者混合使用。

古典密码的历史最早可追溯到四千多年前雕刻在古埃及法老纪念碑上的奇特的象形文字。不过这些奇特的象形文字记录不可能是用于严格意义上保护秘密信息的，而更可能仅是为了神秘、娱乐等目的。

下面介绍一些比较典型的古典密码术的例子。

(1) Caesar 密码

Caesar 密码大约出现于公元前 100 年的高卢战争期间古罗马统治者 Julius Caesar 为了秘密传达战争计划或命令的通信中。Caesar 密码就是以 Julius Caesar 的名字命名的。Caesar 密码的规则是将明文信息中的每个字母，用它在字母表中位置的右边的第 k 个位置上的字母代替，从而获得它相应的密文。比如 $k=3$

时，明文字母与密文字母的对应关系可用置换表表示如下：

$$\begin{pmatrix} A\ B\ C\ D\ E\ F\ G\ H\ I\ J\ K\ L\ M\ N\ O\ P\ Q\ R\ S\ T\ U\ V\ W\ X\ Y\ Z \\ D\ E\ F\ G\ H\ I\ J\ K\ L\ M\ N\ O\ P\ Q\ R\ S\ T\ U\ V\ W\ X\ Y\ Z\ A\ B\ C \end{pmatrix}$$

于是对于明文信息 secret message，可得其相应的密文为 VHFUHW PHVVDJH。

在 Caesar 密码中，参数 k 就是密钥。如果 26 个字母用 0 至 25 的整数替代，即 0 替代 a，1 替代 b，……，24 替代 y，25 替代 z。那么，Caesar 加密运算其实就是计算同余式

$$c = m + k \bmod 26$$

其中 m 是明文字母对应的数，c 就是对应的密文字母代表的数，密钥 k 是 0 至 25 内的任何一个确定的数。

Caesar 密码属于单表代换密码。

(2) Vigenère 密码

Vigenère 密码是由法国密码学家、外交家 Blaise de Vigenère 在 1586 年提出的一种多表代换密码。其代换原则基于下列字母对应表，每行都对应于一个 Caesar 密码代换表，即第 $t(0 \leqslant t \leqslant 25)$ 行对应于密钥 $k=t$ 的 Caesar 密码代换表：

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I

K K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

每次在加密信息时，需要利用一个关键词，即密钥。具体地说，加密一条明文信息时，需对每一个明文字母，先从表的顶端找出明文字母所在的列，然后再从左边找出相应的密钥字母所在的行，那么对应该明文字母的密文字母就是表中此列与此行交叉位置上的字母。解密时，在最左边找出相应的密钥字母所在的行，然后沿着此行找出密文字母，那么密文字母所对应的最顶端的字母就是相应的明文字母。一般来说，使用的密钥比明文短，所以密钥一般是周期性地重复使用，即将加长到与明文相同的长度。

例如，假设明文信息为

$$m = \text{Please keep this message in secret}$$

密钥为

computer

那么加密后的密文为

c = RZQPMX OVGD FWCL QVUGMVY BR JGQDTN

如果像上面一样将 26 个字母 A 至 Z 分别用 0 至 25 这 26 个数字代替，那么 Vigenère 密码的加密计算同样可用数学式子来表示。设 $m=m_1m_2\cdots m_t$（每个 m_i 代表一个字母）是明文，$k=k_1k_2\cdots k_t$（每个 k_i 代表一个字母）是密钥。加密后的密文为 $c=c_1c_2\cdots c_t$，则

$$c_i = m_i + k_i \bmod 26$$

这里作模运算时 m_i 与 k_i 分别取对应的数字。

所以 Vigenère 密码可以看成 Caesar 密码的推广。

(3) Playfair 密码

Playfair 密码是发明人 Charles Wheatstone 在 1854 年 3 月提出的，而后来才由他的朋友 Lyon Playfair 将此密码公诸于世，所以该密码就以 Playfair 命名。

在 Playfair 密码中，明文需按两个字母一组分成若干个加密单元，加密时是按单元进行的。所以，可以说是一个最初级的分组密码，也可以说是多字母代换密码。

明文的分组方式是：在将明文按字母对分组时，如出现两个相同字母，则在第一个字母后添加 X 构成一组，第二个相同字母与它后面的字母构成一组；如果一个字母与它前一组的最后一个字母相同，则在该字母前加上 X 构成一组；如果最后只剩下一个字母，则在其后添加 X 构成一组。例如：balloon 分组成 BA LX LO XO NX。当然，也可将 X 换成其他字母。

对明文进行加密前，先选定一个关键词或密钥，然后利用该密钥将 26 个英文字母排成一个没有重复字母的 5×5 的加密矩阵，并且将 j 换成 i。若同时出现 i 与 j，则去掉字母 Z。如密钥为 just 与 inject 时，得到的 5×5 加密矩阵分别为：

$$\begin{bmatrix} I & U & S & T & A \\ B & C & D & E & F \\ G & H & K & L & M \\ N & O & P & Q & R \\ V & W & X & Y & Z \end{bmatrix} \quad 与 \quad \begin{bmatrix} I & N & I & E & C \\ T & A & B & D & F \\ G & H & K & L & M \\ O & P & Q & R & S \\ U & V & W & X & Y \end{bmatrix}$$

Playfair 密码的加密规则为：设 m_1m_2 是一个明文字母组，加密后对应的密文字母组为 c_1c_2，则

① 如果 m_1 与 m_2 同在加密矩阵的同一行，那么 c_1 与 c_2 分别为紧靠 m_1 与 m_2 右端的字母。这里将加密矩阵的第一列看成是最后一列的右端。

② 如果 m_1 与 m_2 同在加密矩阵的同一列，那么 c_1 与 c_2 分别为紧靠 m_1 与 m_2 下方的字母。这里将加密矩阵的第一行看成是最后一行的下方。

③ 如果 m_1 与 m_2 不在加密矩阵的同行，也不在同列，那么 c_1 取为 m_1 所在行、m_2 所在列交叉处的字母，而 c_2 取为 m_2 所在行与 m_1 所在列交叉处的字母。

例如，设密钥为 cryptography，则 5×5 加密矩阵为

$$\begin{bmatrix} C & R & Y & P & T \\ O & G & A & H & B \\ D & E & F & I & K \\ L & M & N & Q & S \\ U & V & W & X & Z \end{bmatrix}$$

设需加密的明文为 m＝Hide the gold in the tree stump，则先对明文分组成：

HI DE TH EG OL DI NT HE TR EX ES TU MP

加密后的密文为 c＝IQ EF PB ME DU EK SY GI CY IV KM CZ QR。

(4) Hill 密码

Hill 密码是在 1929 年由 Lester S. Hill 发明的，其主要思想