计算机网络的安全技术与方法

李海泉 （西安石油学院计算机系 710061）

摘要：本文概要地说明了计算机网络安全所面临的威胁，重点阐述了网络的安全对策，网络中的数据加密技术和数据加密算法及其应用，可供有关方面及人员参考。

关键词：网络安全 网络加密技术 数据加密算法

一、网络安全所面临的威胁

计算机网络技术的发展使得计算机应用日益广泛深入，同时也使计算机系统的安全问题日益复杂和突出。一方面网络提供了资源共享性，提高了系统的可靠性，通过分散工作负荷提高了工作效率，并且还具有可扩充性。这些特点使得计算机网络深入经济、国防科技与文教等各个领域。另一方面正是这些特点，增加了网络安全的复杂性和脆弱性，资源共享和分布增加了网络受威胁和攻击的可能性。一个计算机网络进行通信时，一般要通过通信线路、调制解调器、网络接口、终端、交换器和处理机等部件。通信线路的安全令人担忧，通过通信线路和交换系统互连的网络是窃密者、非法分子威胁和攻击的重要目标。

对网络的威胁，主要有以下四个方面：

①网络部件的不安全因素；

②软件的不安全因素；

③工作人员的不安全因素；

④环境因素。

1.网络部件的不安全因素

(1)电磁泄漏。网络端口、传输线路和处理机都有可能因屏蔽不严或未屏蔽，造成电磁泄漏。目前大多数机房屏蔽和防辐射设施都不健全，通信线路也同样容易出现信息泄漏。

(2)搭线窃听。随着信息传递量的不断增加，传递数据的密级也在不断提高，犯罪分子为了获取大量情报，可能在监听通信线路，非法接收信息。

(3)非法终端。有可能在现有终端上并接一个终端，或合法用户从网上断开终端时，非法用户乘机接入并操纵该计算机通信接口，或由于某种原因使信息传到非法终端。

(4)非法入侵。非法分子通过技术渗透或利用电话线侵入网络，非法使用、破坏或获取数据及系统资源。目前的网络系统大都采用口令来防止非法访问，一旦口令被窃，很容易打入网络。

(5)通过电话线有预谋地注入非法信息，截获所传信息，再删除原有信息，注入非法信息再发出，使接收者收到错误信息。

(6)线路干扰。当公共载波转接设备陈旧和通信线路质量低劣时，会产生线路干扰，导致产生数据传输出错。调制解调器会随着传输速率的上升，错误迅速增加。

(7)意外原因。人为地对网络设备进行破坏；设备故障；处理非预期中断过程中，通信方式留在内存中未被保护的信息段；通信方式被意外弄错而传到别的终端上。

(8)病毒入侵。计算机病毒可以多种方式侵入计算机网络，并不断繁殖，然后扩散到网上的计算机来破坏系统。轻者使系统出错或处理能力下降，重者可使整个系统瘫痪或崩溃。

2.软件方面的不安全因素

(1)网络软件安全功能不健全或安装了特洛伊木马软件。

(2)应加安全措施的软件，可能未予标识和保护，要害的程序可能没有安全措施，使软件非法使用或破坏，或产生错误结果。

(3)未对用户进行分类和标识，使数据的存取未受限制和控制。

(4)不妥当的标定或资料，导致所修改的程序构成版本错，程序员没有保护程序变更的记录，没有做拷贝，未建立保存记录的业务。

(5)对软件更改的要求没有被充分理解，导致软件错误。

3.工作人员引起的不安全因素

(1)保密观念不强或不懂保密守则，随便泄漏机密；打印、复制机密文件；随机打印出系统保密字或向无关人员泄漏有关机密信息。

© 中国科学院软件研究所 http://www.c-s-a.org.cn

(2)业务不熟练,因操作失误,使文件出错或误发,或因未遵守操作规程而造成泄密。

(3)因规章制度不健全造成人为泄密事故。网络上的规章制度不严,对机密文件管理不善,各种文件存放混乱,违章操作造成不良后果。

(4)素质差,缺乏责任心,没有良好的工作态度,工作马马虎虎,或有意破坏网络系统和设备。

(5)熟悉系统的工作人员故意改动软件,或用非法手段访问系统,或通过窃取他人的口令和用户标识码来非法获取信息。

(6)担任系统操作的人员以超越权限的非法行为来获取或篡改信息。

(7)利用硬件的故障和软件的错误非法访问系统,或对系统的各部分进行破坏。

(8)利用窃取系统的磁盘、磁带或纸带等记录载体或利用废旧的打印纸、复写纸来窃取系统或用户的信息。

4.环境因素

除了上述因素之外,还有环境因素威胁着网络的安全,如地震、火灾、雷电、风灾、水灾等自然灾害,或温湿度冲击、空气洁净度变坏和掉电、停电或静电等工作环境因素的影响。

二、计算机网络的安全对策

针对网络的上述种种威胁,可采取如下的安全对策:

1.保密教育

对工作人员结合机房、硬件、软件、数据和网络等各个方面安全问题,进行安全教育,提高工作人员的保密观念和责任心;加强业务、技术的培训,提高操作技能;教育工作人员严格遵守操作规程和各项保密规定,防止人为事故的发生。

2.保护传输线路安全

对于传输线路,应有露天保护措施或埋于地下,并要求远离各种辐射源,以减少由于电磁干扰引起的数据错误;电缆铺设应当使用金属导管,以减少各种辐射引起的电磁泄漏和对发送线路的干扰。集中器和调制解调器应放置在受监视的地方,以防外连的企图;对连接要定期检查,以检测是否有搭线窃听、外连或破坏行为。

3.防入侵措施

应加强对文件处理的限制,控制重要文件的处理。利用报警系统检测违犯安全规程的行为,即对安全码的不正确使用或使用无效的安全码,对规定次数内不正确的安全码使用者,网络系统可采取行动锁住该终端并报警,以防止非法者突破安全码进行入侵系统。

4.网络加密

网络加密是网络中采用的最基本的安全技术。网络中的数据加密,除了选择加密算法和密钥外,主要问题是加密方式及实现加密的网络协议层和密钥的分配及管理。网络中的数据加密方式有链路加密、节点加密和端对端加密等方式。数据可以在OSI协议参考模型的多个层次上实现。

5.存取控制

访问控制是在由鉴别机制提供的信息基础上,对于个体或过程特权的获得与实现。鉴别是为存取控制提供支持的,是在对等实体被认证的基础上来限制任何非授权的资源存取。对于文件和数据库设置安全属性,对其共享的程序予以划分,通过存取矩阵来限制用户使用方式,如只读、只写、读/写、可修改、可执行等。数据库的存取控制,还可以分库、结构文件、记录和数据项四级进行。

6.鉴别机制

鉴别是为每一个通信方查明另一个实体身份和特权的过程。它是在对等实体间交换认证信息,以便检验和确认对等实体的合法性。它是取控制实现的先决条件。鉴别机制中采用报文鉴别,也可以采用数字签名或终端识别等多种方式。

报文鉴别是在通信双方建立通信联系之后,每个通信者对收到的信息进行验证,以保证所收到的信息的真实性的过程,也就是验证报文完整性。一旦这种鉴别信息被得知,并且它的准确性和完整性有保证,那么本地用户或系统就可做出适当的判断:什么样的数据可以发送到对方。

数字鉴名是一个密文收发双方签字和确认的过程。所用的签署信息是签名者所专有的、秘密和唯一的,而对接收方检验该签署所用的信息和程序则是公开的。签名只能由签名者的专用信息来产生。检验过程则是用公开程序和信息来确定签名是否用签名者的专用信息产生的。所以当出现纠纷时,仲裁者则可利用公开程序来证明签名者的唯一性。数字签名可以为实体认证,无连接完整性、源点鉴别、制止否认等服务提供支持。它也是数据完整性、公证和认证机制的基础。

终端识别技术是利用回收信息核对用户位置,识别用户身份的一种方式。回信核对装置还对用户的联机位置进行检查、核对。如果某人窃用得到的联机口令在非法地点联机,系统会立即切断联络,并对这一非法事件进行记录,将非法者的联机时间、地点等详细情况记录下

© 中国科学院软件研究所 http://www.c-s-a.org.cn

来，并打印出来，以便及时查处和制止非法犯罪行为。

7.路由选择机制

路由选择机制实际上就是流向控制。在一个大型网络系统中，选择安全通路是一个重要问题。这种选择，可以由用户提出申请，在自己的程序和数据前打上路由标志；也可以在网络安全控制机构检测出不安全路由后，通过动态调整路由表，限制某些不安全通路。

8.通信流控制

通信流分析是一种特殊的被动型攻击。其安全控制包括：(1)掩盖通信的频度；(2)掩盖报文的长度；(3)掩盖报文的形式；(4)掩盖报文的地址。具体方法是填充报文和改变传输路径。

填充报文，包括增加伪报文或将所有报文都扩充到同样长度，并随机地选择通信对象，使网络中的数据流量比较平衡。为了掩盖报文地址，一般采用物理层的链路加密方式。而伪报文的发送则在网络高层协议中实现。为了掩盖报文的形式常采用带反馈的加密方式。

9.数据完整性

网络通信协议中一般都考虑了传输中的差错控制措施，但不能对付人为的破坏。网络中传输数据完整性控制包括：(1)数据来自正确的发送方而非假冒；(2)数据送到了正确的接收方，而无丢失或误送。(3)数据接收的内容与发送时一致。(4)数据接收的时序与发送时一致。(5)数据没有重复接收。保护数据完整性的措施是增加敌手所不能控制的冗余信息。

10.端口保护

远程终端和通信线路是安全的薄弱环节，尤其在利用电话拨号交换网的计算机网络中。因此，端口保护成为网络安全的一个重要问题。一种简单的保护方法是在不使用时拔下插头或关掉电源。不过这种方式对于拨号系统或联机系统是不可行的。因此，通常采用的方法是利用各种端口保护设备。

除此之外，还有安全检测、审查和跟踪等措施等。

三、计算机网络的加密技术

计算机网络的加密技术，是通过计算机网络中的加密机构，把网络中的各种原始的数字信息(明文)，按照某种特定的加密算法变换成与明文完全不同的数字信息，即密文的过程。计算机网络中的加密技术，主要采用链路加密、节点加密和端对端加密等三种方式。

1.链路加密

链路加密是目前最常用的加密方法，通常用硬件在网络层以下(1,2 层)的物理层实现。它用于保护通信节点间传输的数据。这种加密方式比较简单，实现起来比较容易，只要把一对密码设备安装在两个节点间的线路上，即把密码设备安装在节点和调制解调器之间，使用相同的密钥即可。用户没有选择的余地，也不需要了解加密技术的细节。一旦在一条线路上采用链路加密，往往需要在全网内都采用链路加密。图 1 是这种加密方式的原理图。

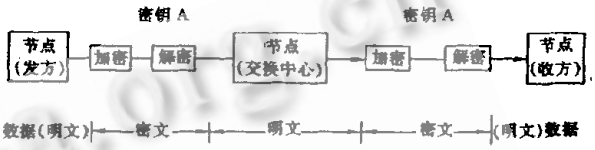

图 1　链路加密

链路加密方式对用户是透明的，即加密操作由网络自动进行，用户不能干预加密和解密过程。它主要用以对信道或链路中可能被截获的那一部分进行保护。这些链路主要包括专用线路、电话线、电缆、光缆、微波和卫星通道等。

链路加密按被传送的数字字符或位的同步方法的不同，分为异步通信加密和同步通信加密两种。而同步通信按字节同步，还是按位同步，又分为两种加密方式。

这种加密方式有两个缺点。一是全部报文都以明文形式通过各节点的计算机中央处理机。在这些节点上，数据容易受到非法存取的危害。二是由于每条链路都要有一对加密、解密设备和一个独立的密钥，因此成本较高。

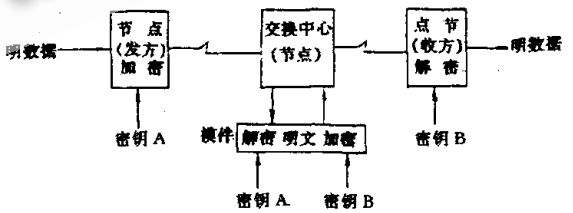

图 2

2.节点加密

节点加密是对链路加密的改进。其目的是克服链路加密在节点处易遭非法存取的缺点。在协议运输层上进行加密，是对源节点和目标节点之间传输的数据进行加

© 中国科学院软件研究所 http://www.c-s-a.org.cn

密保护。它与链路加密类似，只是加密算法要组合在依附于节点的加密模件中。其加密原理如图 2 所示。这种加密方式可提供用户节点间连续的安全服务，也可用于实现对等实体鉴别。

节点加密也是每条链路使用一个专用密钥，但一个密钥到另一个密钥的变换是在保密模件中进行的。这个模件设在节点中央处理装置中，可以起到一种外围设备的作用。所以明文数据不通过节点，而只存于保密模件中。要注意的是：对于相当多的电报数据，在路由选择信息时也要加密。这样，节点中央处理装置就能够恰当地选定数据的发送线路。

3. 端对端加密

网络层以上的加密，通常称为端对端加密。端对端加密是面向网终高层主体进行加密，即在协议表示层上对传输的数据进行加密，而不对下层协议信息加密。协议信息以明文形式传输，用户数据在中间节点不需要解密。端对端加密一般由软件来完成。在网络高层进行加密，不需要考虑网络低层的线路、调制解调器、接口与传输码，但用户的联机自动加密软件必须与网络通信协议软件完全结合，而各厂家的通信协议软件往往又各不相同。因此，目前的端对端加密往往是采用脱机调用方式。端对端加密也可以用硬件来实现，不过该加密设备要么能识别特殊命令字，要么能识别低层协议信息，而仅对用户数据加密。硬件实现往往有很大的难度。在大型网络系统中，交换网络在多个发方和收方之间传输的时候，用端对端加密是比较合适的。端对端加密原理如图所示。

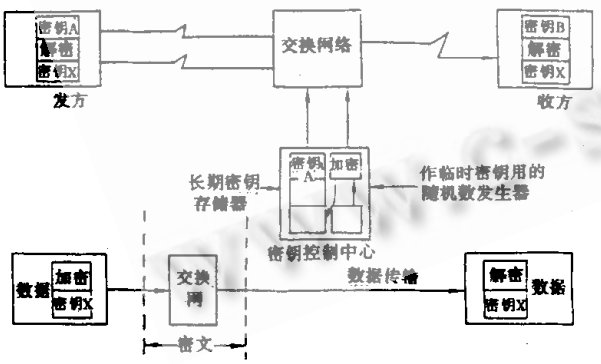

图 3　端对端加密

端对端加密具有链路加密和节点加密所不具有的优点。其一是成本低。由于端对端加密在中间任何节点上都不解密，即数据在到达目的地之前始终用密钥加密保护着，所以仅要求发送节点和最终的目标节点具有加密、解密设备。而链路加密则要求处理加密信息的每条链路均配有分立式密钥装置。其二，端对端加密比链路加密更安全。采用端对端加密，其控制中心的加密设备可对文件、通行字以及系统的常驻数据起到保护作用。由于端对端加密只是加密报文，数据报头仍需保持明文形式，所以数据容易为报务分析者所利用。对端对端加密来说，密钥数量大，因此其密钥管理是一个十分重要的问题。

四、网络中的数据加密算法

在计算机网络和数据通信中的数据加密，主要使用 DES 算法或 RSA 算法。

DES(Data Encryption Standard)算法由美国 IBM 公司 1973 年提出，1975 年 1 月 5 日被美国确定为统一数据加密标准。20 多年来得到了广泛应用。

该算法输入的是 64 比特的明文，在 64 比特的密钥控制下，通过初始换位 IP 变成 $T_0 = IP(T)$，再对 T_0 经过 16 次的加密变换，最后通过逆初始换位(也称为最后变换)，得到 64 位的密文。其密文的第一比特都是由明文的每一比特和密钥的每一比特联合确定的。其实现过程可分为加密处理、加密变换、子密钥生成和解密几个过程。它具有良好的保密性和抗分析破译性能，影响最大，应用最广。

RSA 算法是公开密钥密码体制中的一种比较成熟的加密算法，是 1976 年由 Diffie、Hellman 和 Merkle 等人提出来，1978 年由麻省理工学院 Rivest、Shamir 和 Adleman 等人研制出来。在公开密钥密码体制中，该算法的加密密钥和解密密钥互异、分离。加密密钥可以通过非保密通信向他人公开，使任何得到该加密密钥的用户能据此将明文信息加密成密文信息予以发送；而按特定要求选择的解密密钥则保持保密。

RSA 算法是建立在“大数分解和素数检测”的理论基础上的。两个大素数相乘在计算机是容易实现的，但将该乘积分解为两个大素数因子的计算量却相当巨大，大到甚至在计算机也不可能实现。素数检测就是判定一个给定的正整数是否为素数。该算法取用一个合数(该合数为两个素数的乘积)，而不是取用一个大素数作为其模数。其实现的步骤可分为：设计密钥，设计密文和恢复明文几个过程。RSA 算法具有一定的特定和优越性，但不能取代 DES 算法。它与 DES 并驾齐驱，互相促进。

(来稿时间：1997 年 6 月)

© 中国科学院软件研究所 http://www.c-s-a.org.cn