# 计算机网络系统的安全保密方法

中国电子设备系统工程公司研究所　　陈爱民

**摘要**：本文主要对网络系统应考虑的保密问题进行了阐述，并就网络系统的加密方式、加密方法、密钥的和访问控制等技术谈了一些看法。

## 一、概　述

一般来说，对于一个的网络系统，除采取必要的行政管理手段外，主要采取加密、访问控制、审计跟踪等技术。这些技术措施在 ISO／7498-2 中都提出了一些具体的要求。但这是一种理想的模式，因为并不是所有的网络系统都必须采取所有这些措施。例如对网络系统的加密，也不是在网络体系结构的每个层次(OSI 开放系统互连共分七层)都采取加密措施，这里有以下几方面的因素：

1.在每个层次都实施加密技术，势必增加系统开销，影响计算机处理效率。

2.目前使用的网络系统大都是计算机生产厂家的成品，而这些网络产品一般没有按照 OSI 开放系统互连模型的层次设计，因此，要在原有系统加入安全功能并非一件容易的事情。

3.按用户要求，一般也不需要每层都采取加密措施。例如，为了保护通信的正文，在表示层或应用层对数据加密即可；若要对网络口令、控制信息等进行保护，并防止业务流分析，则必须在物理层进行加密才能达到目的；若用户要求只对源节点到目标节点之间传输的信息进行保护，则在运输层增加加密措施即可。因此，可根据不同的用户要求，采用不同的加密方式。

对于访问控制和安全管理也是一样，不同的系统、不同的应用环境、不同的地点、不同的保护等级，采取的保护措施也各有不同。但只要各种保护措施能相互协调，互为补充，是可以达到对抗各种威胁的目的的。同时就网络系统的安全保密问题，对于一般的用户，它也有共同的地方，一般应从以下几个方面考虑：

1.实体安全。采用各种物理手段防火、防盗、防水等；建立各项规章制度，防止信息丢失或意外事故发生；采用防辐射技术，防止计算机设备本身的信息泄露。

2.人员管理。在计算机中，对于工作人员的管理是一个重要的问题，许多计算机系统的威胁来自人的因素。

3.信息加密。根据不同的应用环境，对传输和存储信息进行加密保护。

4.密钥管理。“一切秘密寓于密钥之中”，这说明密钥在信息保护中所处的地位是非常重要的，密钥管理的不好，再强的保密方法也无济于世。

5.访问控制。实施访问控制与验证技术，防止非法用户闯入网络系统、并非法获取用户信息和网络资源。

6.身份鉴别。采用鉴别和签名技术，防止对数据的非法修改和服务拒绝等。

7.安全审计。采用审计跟踪技术，对危害网络安全的事件进行审计。

## 二、网络系统的加密方式

对于一般的用户，通常采用在应用层(表示层或运输层)和物理层加密的方法就可达到保密的目的。下面简要介绍一下这几种方式。

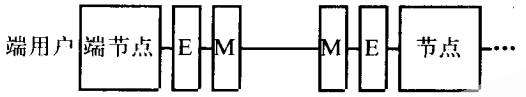
**1.物理层加密**

随着信息社会的不断发展，提供对计算机设备的远程访问的网络不断被开发，并被重要单位或公司广泛采用。因而，使计算机窃贼攻击的目标集中到了网络系统，而新技术发展使得有些类型的攻击变的极为容易，如计算机窃贼可轻而易举地监视卫星、有线和无线通信信道，得到有用信息。为此，在物理层采取加密措施是十分必

要的。

物理层加密是对相邻网络节点(节点或端节点)之间在线路上传输的数据进行保护。对于这种保护,加解密是在被置于两个网络节点(或端节点)之间的通信线路上(即位于通信线路两端)的两个保密设备中实现的。这两个保密设备被放在它们各自的节点(DTE)及相应的调制解调器(DCE)之间,并使用相同的密钥,如图 1 所示。

采用物理层(加密装置)加密,即可对选择明文加密,也可采用全信息流加密。




注:E:加解密装置 M:调制解调器

图 1 物理层加密方式

**2.运输层加密**

运输层加密是对源节点到目标节点间传输的数据进行保护,如图 2 所示。在每对节点间采用共用一个密钥的方法对数据加密。它与物理层加密的主要区别是数据通过中间节点时,仍以密的形式出现,只有到达目标节点时才还原成明文。这种方法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。

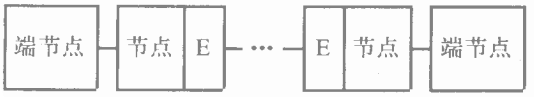



图 2 运输层加密方式

**3.应用层(端—端用户间)加密**

应用层加密是对源端用户到目的用户的数据提供连续的保护,因此也称为端—端用户加密,如图 3 所示。它与运输层加密的主要区别是:运输层加密只提供源节点到目的节点的保护,而端—端用户加密是提供源端用户与目的端用户的保护。

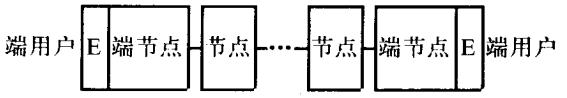



图 3 应用层加密方式

在物理层加密的情况下,用户通常不知道报文已接受加密保护,即对用户是透明的。对于端—端用户加密,若加密功能经由系统服务自动提供,那么,对于用户也是透明的,但若由用户请求专门的加密技术,其使用就不是透明的了。

支持透明的端—端用户加密要有一个系统服务,这个系统服务要为用户间提供对传输的报文进行加解密时需要的密钥和加解密功能(也可全部由保密装置实现)。若加解密功能由用户选择,则密钥可由系统提供,也可由用户自己提供。

另外,这种加密形式与物理层加密形式不同的是:在被传输的信息进入通信网之前对其加密,并在信息离开网络之后始终处于加密状态,直到目标用户。采用这种方式时,不用担心信息在传输过程中被窃取,同时也不必对通信系统操作人员提出特别的要求,因为他们不直接访问网络系统中的任何信息。但这种加密方式还是存在一些问题,因为供网络确定报文目的地的编址信息和一些必要的网络控制信息是以明的形式出现在信道上的,所以网络操作人员或其他任何企图借助网络通信链路截取信息者,都能够得到网络中正在传输的信息,这一点关系到信息流的分析问题。另外,路由口令等在传输过程中也是明的,如果被人截取,对网络系统会造成很大威胁。因此,对于政府和军事方面(如有关军事态势和财政问题等)的重要信息,除采用端—端用户加密外,还必须结合物理层加密措施,以防止外部人员搭线或无线截取信息的威胁,这样才能保证整个网络系统的安全。

## 三、网络加密的一般方法

目前实现网络保密一般采用硬件,软、硬件结合或软件对信息进行加密的方式。软件加密在应用层(或表示层)使用,对存储文件和数据库等加密。这种方法,成本低,使用灵活,但要解决加密软件的保护和密钥的管理问题,因为若软件或密钥被人窃取或暴露,就等于把秘密信息送给了敌对者。对于纯硬件实现的保密装置随着电子技术的发展已很少使用。而最常使用的是软、硬件结合的方式。因为它造价相对较低,使用灵活,应用广泛,既可用于线路加密,也可做为用户保密装置使用,而且保密装置本身的保密性也可以做的很好。这种保密装置的构造如图 4 所示:

I/O 部分负责明文接收、密文的输出或密文接收、

明文输出等工作；

随机数产生器主要产生加解密所用的密码序列参数，它被加入到密码算法中去；

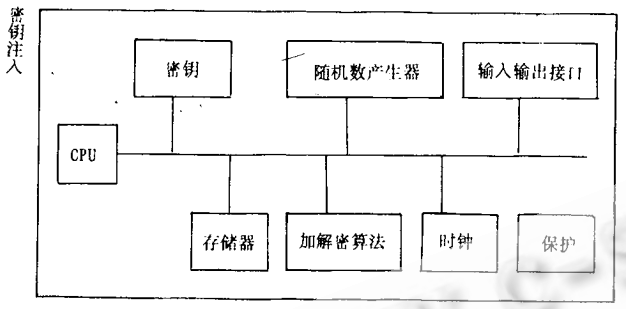



图 4　保密装置构造

密钥部分主要是保存主密钥(或基本密钥)，在多用户情况下，也可能是一个密钥表，若采用对称密钥密码算法，则收、发双方应当相同；

处理器是保密装置的心脏，它控制信息的收发，进行资源管理、信息加解密等工作；

存储器用于保存信息和相应的参数等；

物理保护主要是指外围的保护如加密码锁等，还有密钥的保护、消毁，在应急情况下的密钥清除等措施。

目前有些保密机生产厂家(如 AT&T)都把保密算法做成的专门芯片，通过处理器控制既可实现信息加密，而且速度快，保密性好。

另外，这种保密装置用做线路保密时，用串行口与计算机相连，而另一串口与调制解调器连接。加密方式一般采用序列加密，当接收到计算机内送来的字符(一个或多个)时就对此加密，然后发往线路，经过保密机时没有太多的时间延迟。

在用作用户保密时，一般用并行口与计算机连接。当保密机收到计算机发来一组信息后，保密装经过加密处理，再回送给计算机。当然，无论做为线路保密还是做为用户保密装置，在它与计算机交换信息或与另一端的保密装置通信时，也还要有一套保密协议(或约定)来保证信息的正确交换等。

## 四、密钥的管理

加密技术一般都是采用加密算法来实现的，而加密算法必须由密钥来控制，例如美国数据加密标准 DES。这个数据加密算法是在 56 比特密钥控制下，将 64 比特明文变换成为 64 比特的密文块。

那么，对密钥如何进行保密？如何既能互相通信，使应该得到明文的用户得到明文，而不该得到明文的人得不到有意义的明文呢？这个问题就是密钥管理研究的重要课题。这包括密钥的产生、注入、更换等一系列的环节。

当然对于应用对象不同，管理方式也不同，例如对于物理层加密，由于它只有相邻节点(或端节点)之间进行，与其他节点和端节点无关，因此，对于它的密钥管理比较简单。而对于运输层和表示层加密，管理起来就比较复杂。同时对于单节点(单域)构成的网络系统和多节点(多域)构成的分布式网络系统，在管理上就有很大区别。下面简要介绍一下端—端用户加密时密钥管理系统的设计。

**1.设计密钥管理系统时应考虑的问题**

在设计一个密钥管理系统时，首先要明确解决什么问题，有哪些因素需要考虑，这是设计好一个系统的前题。一般来说以下几个方面是必须要考虑的因素。

(1)系统对保密强度的要求。

(2)系统中那些地方需要密钥，这些密钥又是采用什么方法预置或装入保密组件的。

(3)多长时间更换一次密钥，即一个密钥规定的使用期限是多长。

(4)密钥在什么条件下产生。

(5)用什么方法来保护密钥和数据。

(6)系统的安全性与用户的承受能力

上述有些因素是非技术性的，如第三条，但它与系统的保密性密切相关。如果服务对象是商业界，它要求的保密强度就不是太高，密钥的使用期限就可以比较长一些；如果服务对象是政府或军事等重要部门，那么密钥的使用期限就相对较短。其它几项都属技术问题，只有对这些问题进行认真地考虑，才能设计出一个好的保密系统。

**2.密钥的种类和作用**

在一个网络系统中,为了保证信息和系统安全,一般需要下列几种密钥:

(1)数据加密密钥。在一个数据通信网中,假定一个主体(Object:它可以是应用程序或终端用户等)要通过网络与一个客体(Subject:它也是一个应用程序或一个终端用户)通信,为了保证数据的安全性,主体就需要采用一个特定的加密算法和密钥来对数据进行加密;而客体也必须采用相同的算法和密钥对已加密的数据进行解密。对数据加密的这种密钥一般定义为数据加密密钥(会话密钥)。

(2)基本密钥。为了提高系统的保密性,通常要求对数据加密的密钥只能在一次会话内有效,会话结束,数据加密密钥消失,这种密钥可以由主体通过乱码随机产生器产生,这就大大提高了保密性。但也存在一个问题,那就是主体随机产生的这个密钥(数据加密密钥)必须让客体知道,否则,客体就无法得到明文。让客体知道这个密钥的方法有两种,一种是通过秘密信道或信使送到客体手中,这种方法明然不适于现代电子通信;另一种方法(也是目前比较通用的方法)是通过通信网发送到客体。由于通过通信网不能以明的形式发送,因此就需要使用另一种密钥对其加密,把这种密钥叫做基本密钥。

(3)主密钥。在一个大的网络系统可能有上千个节点或端用户,若要实现全网互通,每个节点就要有与其它节点或端用户通信的基本密钥,这些基本密钥要形成一张表保存在节点(或端节点的保密装置)内,若以明的形式保存,有可能会被窃取。为了保证它的安全,通常还需要有一个密钥对基本密钥表进行加密保护。把这个密钥称为主密钥。

(4)其他密钥。在一个系统中,除了上述密钥外,还可能有通播密钥,共享密钥等,它们也都有各自的用途。

**3.密钥分配**

密钥分配是密钥管理系统最为复杂的问题,根据不同的用户要求和网络系统的大小(单域的还是多域的),有不同的解决方法。

方法一:在一个较小的网络中,一种最简单的方法是只使用一种密钥(即会话密钥)。由一专门机构生成好密钥后,将其发到各端用户,保存在保密装置内。在通信双方通信时,就直接使用这个会话密钥对信息加密。

如果在一个网中只使用这一种密钥,在密钥更换时,必须在同一时间、在网内所有节点(或终端)上进行。密钥的这种设置,管理起来比较简单,但因为在某一段时间内,对网上传输的所有数据都采用同一密钥加密,保密性不好。

方法二:为了提高保密性,可以使用两种密钥:会话密钥和基本密钥。对于这种方法,进行数据通信的过程是:发送方在发送数据之前首先产生会话密钥,用基本密钥对其加密后,通过网络发送到接收方,接收方收到后用基本密钥对其解出,使用会话密钥,双方就可以开始通话了。

这种密钥的管理方法,每个用户必须要有与其他各用户通信的密钥,若有 N 个用户,则密钥数为 N(N-1)/2 个。显然,若该网络系统比较庞大时,产生、安装和管理这样大量的密钥的任务是非常困难的。因此,在较小的网络(单域的或单节点)系统中采用这种方法是可行的。在有许多节点和终端的情况下,考虑到节点的数据处理系统都具有数据处理和存储能力,可以通过把整个网络划分多个区域的方法,分区域管理,这样就可减少端点用户的密钥数量。

方法三:采用非对称密钥密码体制分配密钥。非对称密钥密码体制不仅可对数据进行加密、实现数字签名,也可用于对密钥的分配。

采用非对称密钥密码体制,每个用户都需要有一对密钥,这一对密钥分别表示为 DK 和 EK,DK 用于解密(也称秘密密钥),这个密钥只有该用户自己知道;EK 用于加密(也称公开密钥),全网各互通用户都应知道。如果用户 A 想与用户 D 通信,则用户 A 可用用户 D 的公开密钥对会话密钥进行加密,发送到用户 D;用户 D 用自己保存的密钥解密,就可得到需要的会话密钥。其它用户虽然也知道用户 D 的公开密钥,但不知道相应的秘密密钥,它就得不到相应的会话密钥。所以这种密钥分配方式可简化中间的加解密环节,使用方便。但由于它保密强度是建立在求解大合数因子难度上的,一旦在数学或计算机速度上有较大的突破,则保密强度就弱了。因此,在考虑采用这种分配方式时,首先考虑自己要求的保密强度如何。一般来说,应于商业等机密性不太高的地方是完全可以的。但如果把公开密钥的方法秘密使用,保密强度可大大提高。

## 五、网络系统的访问控制

为了保证网络系统的安全，拒绝非法用户使用系统资源，目前国际上比较流行的方法是采用委托监控器的概念。

如果一个网络用户（主体）要使用网络资源，进行联机访问，那么他必须通过委托监控器的检查。

委托监控器实施安全规则，根据监控器数据基本要求授权主体对客体的访问，必要时对违反系统要求的事件进行审计跟踪并告警。一般用户或进程必须通过监控器检查，核实后才能对客体进行访问。核实一般包括用户入网口令、节点名、用户识别码（UIC）、对文件的访问权限等。

监控数据基这义系统的安全要求，揭示主体（代表用户活动的）可以对这客体进行访问的范围，其中包括口令和访问控制表等。

口令是目前访问控制方面比较通用的方法，例如VAX／VMS操作系统就是采用的这种方法。当一个用户进入网络时，系统首先检查该用户是否在该系统注册，口令是否正确，如不正确拒绝进入网络。

如果要对文件进行访问，那么还要核对访问控制表，看该用户是否对该文件有访问权，如没有访问权而非法访问，要对该用户的活动进行记录，并在控制台告警。

由于口令由用户自己记忆，所以不能太长，一般应在6-8个字节内，这样，有些非法用户可能通过猜测和重试等方法进入系统。为了解决这个问题，在电子资金传送和一些重要的应用系统，采用一种个人识别号码（PIN）的卡，这种卡上有用户的姓名、密码等，一般人是很难分析出来的。在使用时，只要把这种卡插入一个专门装置内，由机器自动识别并确认后，才能进入系统。这种方法比口令要安全，但需要有专门装置，所以费用比较高。

另外，也有采用人体某些特征（如指纹、声音、照片等）来进行识别，但都需要专门的装置，因此只能用于一些重要的部门。

关于安全审计也是安全保密的一个重要部分，需要认真开发和使用。

**参考文献：**

*1.*陈爱民、于康友、管海明，计算机的与保密，电子工业出版社，*1992.9*。

*2.*全国计算机技术交流会论文集，*2---7*。

*3.*通信保，*1987—1991*。

*4.ISO / 7498-2, 1989*。

*5.Computers&security, 1985-1992*。

*6.Guide to VAX / VMS system security*。

*7.John M.Carroll, computer security, butter worths, 1987*。