局域网络环境安全保密系统的设计与实现

陈　妍　李增智　（西安交通大学电信学院）

摘要：作者参加了国家863 CIMS重点应用工厂－济南第一机床厂网络安全保密系统的设计和开发工作，本文对该系统的设计原理及实现方法作了详细的阐述。

一、原理与方法

1.网络安全服务

网络的安全从层次上包括应用与数据安全性、系统安全性、网络传输安全性、访问控制安全性和物理安全性。为实现这些安全性，现在已提出了一系列的安全服务，主要有以下几类：

(1)实体保护服务

①实体鉴别。对互相通信的两实体进行鉴别，防止实体的冒充行为。

②数据来源鉴别。这种服务使数据的接收方能确认一个接收到的数据单元是从认定的发送方传来的。

(2)抗否认服务。这种服务使曾经交换过数据、文电、信息的收发方，事后都不能否认参加过这种交换。

(3)通信保护服务

①数据保密。这种服务保证实体间通信数据的保密性，使其不能被非授权地修改。

②完整性保护。这种服务要保证系统资源(数据、程序)的完整性、正确性、时效性和源发性。

(4)资源保护服务。这种服务主要指访问控制服务。它防止通过网络非授权地使用某些网络资源和非网络资源。

此外，还有审计服务，授权服务等。一个安全的计算机网络，在完成正常的数据通信功能外，还必须提供上面所列举的安全服务。

2.两种主要的加密算法

加密和解密是实现网络安全服务最主要的安全机制。实体保护，通信保护，抗否认服务等都离不开加密和解密。加密算法可分为两大类：对称密码体制(或传统方式)和不对称密码体制(或公开密码体制)。前者以DES算法为代表，后者较著名的有RSA算法。

(1)DES算法。DES算法是美国国家标准局(NBS)于1977年1月采纳的一种算法，后被采纳作为美国的商用加密算法。作为对称加密算法，它的加密密钥和解密密钥相同，是秘密的，解密过程是加密过程的逆过程。

DES算法输入的是二进制64位分组和64位长密钥，输出是64位密文，实际密钥长度为56位，密钥量为2^{56}。加密过程是在密钥控制下，对64位的输入明文进行16轮的移位和替换处理。移位和替换函数是精心选择的，消除数据的顺序性和统计性，使破译难于进行。

DES算法的优点在于速度快、开销小、易于实现、安全性高。但由于加密和解密两者使用同一密钥，一个结点的不安全势必影响另一结点的安全性，而且对于N个结点的网络需N(N－1)/2对密钥，密钥存储空间大，也不利于网络的扩充。上述弱点，在非对称秘密系统中得到了很好的解决。

(2)RSA算法。RSA算法是非对称算法，是1978年美国MIT的Rlberst、Shamir和Ademan三人正式提出的。RSA算法利用寻找大的素数在计算上比较容易，但要将一个数分解为两个素数因子的乘积在计算上却非常难这一特点，作为这种体制的理论基础。

作为非对称秘密体制，RSA算法的加密密钥与解密密钥不同，加密密钥公开而解密密钥保密，因而从根本上解决了传统密码体制在密钥分配上的困难。对于N个结点的系统，只需要N对密钥，大大缩小了密钥空间，并且每个结点只需要保存自己秘密的密钥，提高了密钥的安全性，从而提高了整个网络系统的安全性。而且网络的扩充也简单得多。但由于RSA算法比较复杂，加、解密速度慢，且带来许多额外开销。因此，在本系统的设计中，将DES算法与RSA算法相结合，如通信保密、报文鉴别、文件保密等采用DES算法，而数字签名和密钥管理采用RSA算法，以达到最佳的安全保密效果。

二、系统功能与实现

1.密钥管理

一个安全保密系统运行实现效率的高低与密钥管理

是密切相关的，而且对于 DES 和 RSA 密码体制丢失了

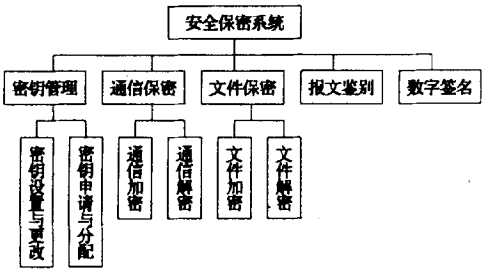


图 1　系统功能结构

密钥，整个安全保密系统便成为虚有。密钥管理包括密钥的产生、分配和安装三个主要部分。本系统密钥管理选择了 RSA 算法与 DES 算法相结合的综合密码体制。密钥分配中心(KDC)首先用 RSA 算法为每个用户分配一对密钥，用户保存好自己的秘密密钥，而公开密钥则以电话簿的方式公开。对于通信会话密钥，当链路会话时创建，随着会话的结束而废弃，因而更换频繁，为提高速度采用 DES 算法。若终端 A 要向终端 B 发送数据，其具体过程如下：

(1) 终端 A 向 KDC 申请工作密钥；

(2) KDC 为 A 产生一个工作密钥；

(3) KDC 用终端 A 的公开密钥加密工作密钥后传送给 A；

(4) 终端 A 用自己的秘密密钥解密工作密钥后，用此密钥加密报文，并发送给 B。

2.通信保密

在网络中通信保密有三种方式：链路加密，结点加密和端对端加密。在这三种方式中，无论从成本、灵活性还是从保密性来看，端对端加密都是最具吸引力的。因此本系统采用端对端加密。端对端加密就是在发送结点加密数据，在接收结点解密数据，而在中间结点数据永不以明文出现。如图 2 所示。

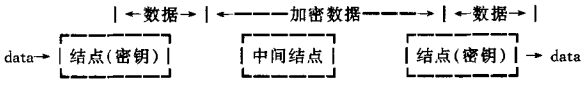
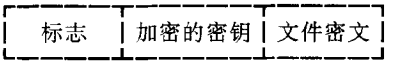


图 2　端－端加密

3.文件保密

文件是网络中的重要资源，系统已采用了口令、访问控制等安全措施，但其抗渗透性不强，容易被伪造、假冒，而使非法用户侵入文件系统，文件加密正是针对这种攻击采取的保护，即使非法用户获得了文件，也不解其义。本系统采用的加密后的文件格式为：



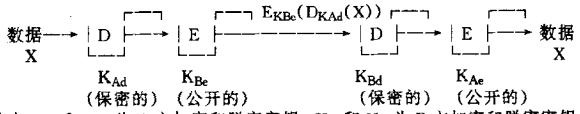
其中：标志和密钥由文件主的公开密钥进行加密，标志指出文件是已加密的文件。只有文件主可以用自己的秘密密钥得到工作密钥，而后看到文件原文，而其他用户则不可以。

4.报文鉴别

报文鉴别是良好数据保密的一部分，能提供对传输报文数据的有效性及完整性验证。它允许每一个通信者验证收报文的来源、内容、时间性和规定的目的地址。本系统采用具有错误传播特性的加密方法 — 分组链接技术来加密报文，即明文 X(i)块中每一位是密文块 Y(1)至 Y(i)中每一位的函数，仅仅由于一个密文比特的差错，就可以造成在被还原的明文中，每个后继比特的差错，也就是利用码间相关性来检测报文的真实性。我们采用明文与密文反馈结合的分组链接技术，在一次操作中可以达到保密和鉴定两个目的，其加解密算法仍是采用 DES 算法，但要求有初始化向量 Z，而且将其附加到明文块的末尾。通过判断作为 X(n+1)与 Z 是否相等，决定是否接收报文还是拒绝报文。

5.数字签名

在局域网络环境中，各部门负责人经常要签署决定或文件，因此在实现生产管理自动化中，也就需要解决与书写签名有对等功能的数字签名问题。数字签名可以采用 DES 体制或 RSA 体制，对于 DES 体制需要复杂的协议，并需要第三方仲裁服务。而公开密钥算法得到的数字签名是通用的、一般的或通用的签名，因为它能为任何存取发方公开密钥的人所证实，因此我们在系统中采用 RSA 体制。为达到只有合法发方才能通过所持有的密钥对数据解密，我们将数据保密通信和数字签名合为一体，利用乘法运算的可交换性，即 $D_{sk}(E_{pk}(X)) = E_{pk}(D_{sk}(X)) = (X)$(模 r)，$D_{sk}$是用公开密钥解密，$E_{pk}$是用公开密钥加密，若通信双方为 A、B，它的原理如图 3 所示：



其中：K_{Ae}和 K_{Ad}为 A 方加密和脱密密钥，K_{Bd}和 K_{Be}为 B 方加密和脱密密钥。

图 3　数字签名