网络中的安全、付费和保密

田波　（上海财政税务局信息中心　200002）

计算机网络本身的特性使得如窃听、信息修改、冒名访问等威胁可以来自系统的各个方面，例如用户的计算机、服务提供者的系统或网络中的任何一个节点。随着商务活动中网络应用的推广，不同集团之间直接通过网络进行商务活动也会越来越频繁，因此有必要研究如何使商家与客户之间通过网络传输的信息得到安全的保障，促进网络应用的发展。

1. **加密方式及策略**

为网络数据传输提供保密性的最佳方式是采用加密，由于对传输的数据进行加密解密操作，保障了数据不被窃听者剽窃。另外加密还能够使数据保持完整性，由于加密使传输的数据按一定方式进行改变并加上相应的标志信息，避免不了知道密码者对加密数据的修改。

加密方式主要有对称加密和非对称加密两种。对称加密系统是加密方与解密方必须使用同一把密钥，这就要求每一对用户之间都有不同于其他的密钥，每个服务提供者需要给所有潜在的客户准备一把密钥。这个限制可以采用非对称解密方式或通过一个相互信任的中介者产生新的密钥和一对互不相知的私有密钥进行数据加密，这种方式的主要优点是只需为每个用户和服务提供者分发一把密钥，数据的保密性也不由公用密钥提供，使得密钥的分发容易的多。非对称加密非常适用于存储和转发应用，例如电子邮件和信息分发应用。但是该方式的主要缺点是它的性能不高，从现有的非对称加密系统来看，它们明显比相应的对称加密系统缓慢。正是由于性能问题，非对称加密很少单独使用，它通常用来对对称密钥和校验单进行加密。这一技术被用在保护电子信件的系统中，例如保密增强信件（Privacy Ehanced mail－PEM）、顶好保密（Pretty Good Privacy－PGP）以及 3W 协议的安全版如安全 HTTP（SHTTP）和安全套接层（Secure Sockets Layer－SSL）。

基于口令的身份鉴定是传统系统中通常采用的方式，但由于通过网络传送的口令可能被窃取并用来冒充用户，因此基于口令的方式在计算机网络中并不适合。为了解决这一问题，可以不通过网络传输口令，而采用身份鉴定协议来证明对口令的了解。在这方面 Kerberos 协议是比较典型的解决方案，Kerberos 身份鉴定协议基于对称加密方式，其协议如图 1 所示。

当客户希望同服务提供方通信时，它先同 Kerberos 身份鉴定服务方联系并把它的名字、希望联系的服务提

供方的名字以及一些其他信息传送给身份鉴定服务方。Kerberos 身份鉴定服务方随机地生成一个暂时密钥并将之加密连同一个包含客户名和暂时密钥的票据返回给客户方。客户将票据连同加密的时戳送给服务提供者，服务提供者将票据解密并使用暂时密钥解密时戳，如果时戳是最近的，服务器认为消息是由知道暂时密钥者发来，从而能够对客户身份进行鉴定。

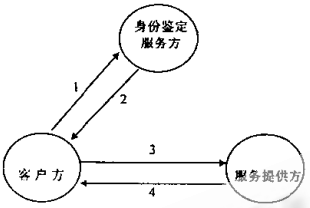

图 1　基于 Kerberos 身份鉴定协议

加密和鉴定技术已经发展了多年，然而我们的网络仍然并不安全。这主要是因为这些技术的推广还需要支持它们的基础设施的推广（例如受人信任的第三方鉴定服务方和鉴定授权）以及技术与应用的集成。

授权是确定用户是否可以执行某一特定操作的过程。现有的系统大都基于服务器本地的信息。这些信息以与文件或目录相关联的存取控制表的形式出现。现在有不少研究是针对分布式授权服务，分布式授权服务对电子贸易是极其重要的，因为这种服务为授权信息提供更好的管理并通过计算机和应用支持授权信息的共享。例如，服务提供者可以使某组中的成员获得一项服务；而在没有分布式授权服务的情况下，每个服务提供者都必须保持各自的组成员列表，而且在一组当中增删一个成员需要对所有服务提供者进行刷新。

在当前的 Internet 付费机制当中大致可以分为以下三种类型：电子货币系统，信用记帐系统和支持安全信用卡号码表示的系统。电子货币虽然具有方便、匿名等优点，但采用电子货币机制的最大缺点是它需要为以往的事务准备大型的数据库。支持信用记帐模式的付费服务系统往往要倚重前面所述的授权服务，在当前的 Internet 上有不少这一类的付费模式采用的授权服务都是 Kerberos 或是基于 Kerberos 的协议。这种付费模式对于一些小额付费方式的系统是非常适用的，例如某人可以用几便士去查询一些数据或存取个人的文档。安全信用卡付费模式在当今应用较广，一些知名的网络服务商如 Netscape、Mosaic 等都采用这一方式，这种方式可以用两种方法：一是客户的信用卡号采用非对称加密分发的密钥进行加密，从而保证只有商家才能读取；二是采用可靠的第三方付费过程服务保证交易的保密性。显然信用卡付费方式具有简单可靠的优点，但由于该方式牵涉到比较复杂的金融手续，故不太适用于小额付费场合。

2. 实施中的问题

前面是从技术的角度介绍和分析了当前网络中的安全、保密和付费问题及通常应采取的策略。尽管大量的技术提出并被了解，但却很难使技术得到有效的推广应用。因此为了实施这些技术，还需要在实施方面提供保障和研究。首先应使鉴定、授权、付费等服务具有可伸缩性即单个的网络范围的保密、安全、付费等服务可以方便的拓展到更大的整个网络范围。其次应为各类服务提供相应的基础设施，例如保障注册用户及他们的密钥，要有值得信赖的服务提供商。另外在实施推广当中还需要将安全服务同应用及操作系统实现集成，由于安全服务可以集成到多个协议层次上，因此现在主要有将安全服务集成到 IP 层或应用层两种。虽然集成到应用层比较复杂，难度也较大，但从今后的应用扩展的方便性来看应当是发展的重点。

Internet 在商业贸易中的应用日益广泛，由传统商业贸易方式存在的问题同样在网络中存在，因此从技术上及非技术方面如何提高网络的安全保密性、付费的方便可靠性并推广实施就成为 Internet 应用推广及商务贸易和人际交流发展的关键。在这方面，我认为单纯靠一两个方面的措施是很难解决的，应当将一些技术上的实施同立法、社会人员协同等非网络本身技术方面综合考虑，以促进 Internet 在现代及未来社会中的应用服务。

参考文献

[1] Clifford A. Lynch" Networks Information Resource Discovery: An Overview of Current Issues" IEEE Journal on selected areas in communications. Vol. 13. No. 8. Oct 1995

[2] 马鸿飞 《INTERNET 资源与使用》西安电子科技大学出版社 1995

（来稿时间：1997 年 8 月）