 二、传输层的安全性 在Internet应用编程序中，通常使用广义的进程间通信(IPC)机制来与不同层次的安全协议打交道。比较流行的两个IPC编程界面是BSD Sockets和传输层界面(TLI)，在Unix系统V命令里可以找到。 在Internet中提供安全服务的首先一个想法便是强化它的IPC界面，如BSD Sockets等，具体做法包括双端实体的认证，数据加密密钥的交换等。Netscape通信公司遵循了这个思路，制定了建立在可*的传输服务(如TCP/IP所提供)基础上的安全套接层协议(SSL)。SSL版本3(SSL v3)于1995年12月制定。它主要包含以下两个协议： SSL记录协议 它涉及应用程序提供的信息的分段、压缩、数据认证和加密。SSL v3提供对数据认证用的MD5和SHA以及数据加密用的R4和DES等的支持，用来对数据进行认证和加密的密钥可以通过SSL的握手协议来协商。 SSL握手协议 用来交换版本号、加密算法、(相互)身份认证并交换密钥。SSL v3 提供对Deffie-Hellman密钥交换算法、基于RSA的密钥交换机制和另一种实现在 Fortezza chip 上的密钥交换机制的支持。 Netscape通信公司已经向公众推出了SSL的参考实现(称为SSLref)。另一免费的SSL实现叫做SSLeay。SSLref和SSLeay均可给任何TCP/IP应用提供SSL功能。Internet号码分配当局(IANA)已经为具备SSL功能的应用分配了固定端口号，例如，带SSL的 HTTP(https)被分配的端口号为443，带SSL的SMTP(ssmtp)被分配的端口号为465，带SSL的NNTP(snntp)被分配的端口号为563。 微软推出了SSL2的改

进版本称为PCT(私人通信技术)。至少从它使用的记录格式来看，SSL和PCT是十分相似的。它们的主要差别是它们在版本号字段的最显著位(The Most Significant Bit)上的取值有所不同:SSL该位取0，PCT该位取1。这样区分之后，就可以对这两个协议都给以支持。 1996年4月，IETF授权一个传输层安全(TLS)工作组着手制定一个传输层安全协议(TLSP)，以便作为标准提案向IESG正式提交。TLSP将会在许多地方酷似SSL。 前面已介绍Internet层安全机制的主要优点是它的透明性，即安全服务的提供不要求应用层做任何改变。这对传输层来说是做不到的。原则上，任何TCP/IP应用，只要应用传输层安全协议，比如说SSL或PCT，就必定要进行若干修改以增加相应的功能，并使用(稍微)不同的IPC界面。于是，传输层安全机制的主要缺点就是要对传输层IPC界面和应用程序两端都进行修改。可是，比起Internet层和应用层的安全机制来，这里的修改还是相当小的。另一个缺点是，基于UDP的通信很难在传输层建立起安全机制来。同网络层安全机制相比，传输层安全机制的主要优点是它提供基于进程对进程的(而不是主机对主机的)安全服务。这一成就如果再加上应用级的安全服务，就可以再向前跨越一大步了。 