1. Web (World Wide Web万维网)

\*基本结构：

开放式的客户/服务器结构：

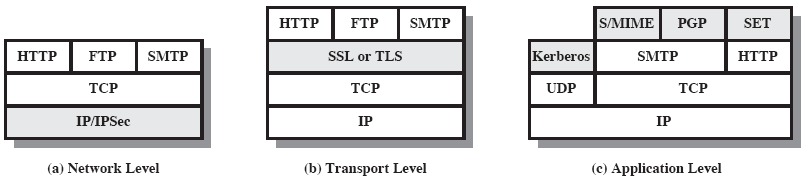
a.Web服务器（服务器端）b.Web浏览器（客户端）c.传输协议（HTTP协议）

\*Web安全方案：

（1）网络层安全：IPSec

（2）传输层安全：SSL/TLS

（3）应用层安全：SET/SHTTP



1. 安全套接层SSL

\*主要功能：

(1)建立一个信息安全通道，来保证数据传输的安全；

(2)确认网站的真实性。

\*工作过程：

(1)第一阶段：发起阶段

(2)第二阶段：服务器认证和密钥交换

(3)第三阶段：客户端认证和密钥交换

(4)第四阶段：结束阶段

\*SSL提供的面向连接的安全性具有以下三个基本性质：

(1)连接是秘密的。

(2)连接是可认证的。

(3)连接是可靠的。

\*解决的问题:

(1)客户对服务器的身份认证。

(2)服务器对客户的身份认证。

(3)建立服务器与客户之间安全的数据通道。

(4)用户和服务器的合法性认证。

(5)传输数据的机密性。

(6)传输数据的完整性。

\*使用的安全机制:

(1)加密机制

(2)数据签名机制

(3)数据完整性机制

(4)交换鉴别机制

(5)公证机制

1. 传输层安全TLS

\*具体目标:解决两个通信实体之间的数据的保密性和完整性等，总体目标是为了在Internet上统一SSL标准。

#在协议构成方面TLS几乎与SSL协议一样，主要分为TLS记录协议和TLS握手协议。

4.HTTPS

\*概述：用于安全的HTTP数据传输,是HTTP的安全版。即HTTP下加入SSL层， HTTPS的安全基础是SSL，因此加密的详细内容就需要SSL。

\*主要作用：

(1)建立一个信息安全通道，来保证数据传输的安全；

(2)确认网站的真实性。

\*解决问题：

(1)信任主机的问题

(2)通讯过程中的数据的泄密和被篡改

\*缺点：效率低

\*HTTP与HTTPS的区别：

(1)HTTPS协议需要到ca申请证书，一般免费证书很少，需要交费。

(2)HTTP(超文本传输协议)信息是明文传输，HTTPS 则是具有安全性的SSL加密传输协议。

(3)HTTP和HTTPS使用的是完全不同的连接方式，用的端口也不一样，前者是80，后者是443。

(4)HTTP的连接很简单，是无状态的；HTTPS协议是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议，比HTTP协议安全。