SSL 简介

SSL（Secure Socket Layer）即安全套接层，是由 Netscape 公司提出的一种基于 WEB 应用的安全协议。SSL 在传输层中对网络通信进行加密，其目的是为网络通信提供安全及数据完整性保障。

SSL 协议采用数据加密技术，确保数据在网络传输过程中不会被截取或者窃听。SSL 协议位于 TCP/IP 协议与应用层协议之间，并独立于应用层。在各应用层进行通信之前，SSL 协议就已完成数据加密算法、通信密钥的协商等工作，之后应用层所传输的数据就都会被加密。目前，SSL 协议已成为网络上保密通信的工业标准。

SSL 加密原理

在服务器与客户端进行通信时，服务器向客户端发送之前已经协商好的密钥，对传输过来的数据进行加密，之后通过解密来响应客户端发来的请求，这就是一个加密与解密的过程。目前常用的密钥算法有对称密钥算法、非对称密钥算法以及散列算法。对称密钥算法指加密与解密使用相同的密钥；非对称密钥算法指加密与解密使用不同的密钥；散列算法指通过某种公开的算法，使文件内容变成固定长度的值（散列值），这个过程可以使用密钥也可以不使用。密钥算法的加密位数越高，数据安全性就越好，目前市面上的主流加密位数已达到 256 位，而防解密已达到 2048 位。

SSL 工作原理

SSL 的工作原理主要由三个协议来完成：

1.握手协议（Handshake protocol）：握手协议是在应用程序的数据传输之前使用，是客户端和服务器用 SSL 连接通信时使用的第一个子协议，握手协议包涵了客户端与服务器之间的一系列消息。SSL 中最复杂的协议就是握手协议，该协议允许服务器和客户端相互验证，协商加密和 MAC 算法以及保密密钥，用来保护在 SSL 记录中发送的数据。

2.记录协议（Record protocol）：记录协议是在服务器与客户端握手成功后使用，即客户端与服务器鉴别对方和确定安全信息交换使用的算法后，进入 SSL 记录协议，记录协议向 SSL 连接提供两个服务：

保密性：使用握手协议定义的私密钥实现

完整性：握手协议定义了 MAC，用于保证消息完整性

3.警报协议（Alert protocol）：客户机和服务器出错时，一方会向另一方方发送警报消息。如果是致命错误，则算法立即关闭 SSL 连接，并删除之前相关的会话号、私密和公密。每个警报消息包涵 2 个字节。第 1 个字节表示错误类型，若是 1 则视为报警，若为 2 则视为致命错误；第 2 个字节代表具体错误类型。

SSL 证书

SSL 证书是一种包含 SSL 协议的证书，由数字证书提供商来提供。由于现今互联网的发展，SSL 证书已经不仅限于提供一份 SSL 协议，更多的是代表着一种互联网络的身份认证。现今 SSL 证书的类型非常多，服务功能越来越齐全，在

信任级别、核发时间等性能上也都有了很大提升。例如，一些 SSL 证书中增加了激活绿色地址栏功能，或者是提供域名验证揭露、企业名称验证揭露服务等。

证书类型

目前市面上比较常见的证书类型有以下几种：

- 普通 SSL 证书：提供常见、完备的 SSL 服务；
- 多域型 SSL 证书：提供完备的 SSL 服务，具有域名验证揭露的特点；
- 通配符 SSL 证书：提供完备的 SSL 服务，并能同时保护一个域名下多个的子域名；
- 安全站点型 SSL 证书：提供完备的 SSL 服务，增加激活绿色地址栏等功能；
- 快速型 SSL 证书：提供完备的 SSL 服务，能够实现快速核发。