Web安全

郑燕飞

主要内容

- Web安全
  - SSL
  - SET

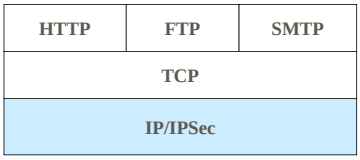
Web安全性问题

- Web是一个运行于internet和TCP/IP intranet 之上的基本的client/server应用。
- Web安全性涉及前面讨论的所有计算机与网络的安全性内容。同时还具有新的挑战。

基于Web信息流的安全方法

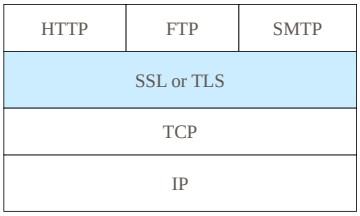
- 网络层——IP 安全性(IPSec)
- 传输层—— SSL / TLS
- 应用层——S/MIME,PGP,SET,Kerberos

(a) Network Level



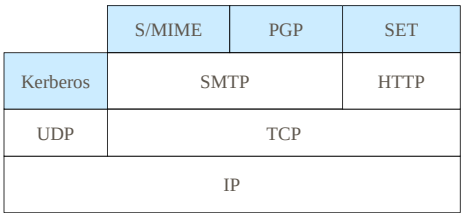
•IPSec的 好处在于对于最终用户和应用程序来说是透明的，并且提供了通用的解决方法。
•进而，IPSec包括了过虑功能，只有选择过的通信量才需要承担IPSec处理负担。

(b) Transport Level



SSL（TLS）作为基本协议族的一个部分提供，对应用程序透明。或是将SSL嵌入专门软件中。

(c) Application Level



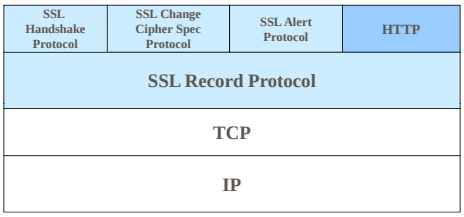
为特定应用程序的专门需要定制服务，如SET。

SSL -Secure Socket Layer

- Netscape开发。V3作为RFC发布。后IETF建立一个TLS工作小组，作为Internet Standard。TLS的第一个版本可以看作是SSLv3.1。

SSL体系结构

- SSL被设计用来使用TCP提供一个可靠的端到端安全服务。SSL是个两层协议：
  - SSL Record Protocol为更高层提供基本安全服务。特别是HTTP，它提供了Web的client/server交互的传输服务，可以构造在SSL之上。
  - SSL Handshake Protocol, SSLChange Cipher Spec Protocol, SSL Alert Protocol是SSL的高层协议，用于管理SSL交换。



SSL Protocol Stack

SSL的两个重要概念

- SSL连接（connection)
  - 一个连接是一个提供一种合适类型服务的传输（OSI分层的定义）。
  - SSL的连接是点对点的关系。
  - 连接是暂时的，每一个连接和一个会话关联。
- SSL会话（session）
  - 一个SSL会话是在客户与服务器之间的一个关联。会话由Handshake Protocol创建。会话定义了一组可供多个连接共享的加密安全参数，被多个连接共享。
  - 会话用以避免为每一个连接提供新的安全参数所需昂贵的谈判代价。

会话状态

- Session identifier: 服务器选择的一个任意字节序列，用以标识一个活动的或可激活的会话状态。
- Peer Certificate: 一个X.509.v3证书。可为空。
- Compression method: 加密前进行数据压缩的算法。
- Cipher spec: 指明数据体加密的算法（无，或DES等）以及散列算法（如MD5或SHA-1）用以计算MAC。还包括其它参数，如散列长度。
- Master secret: 48位秘密，在client与server之间共享。
- Is resumable:一个标志，指明该会话是否能用于产生一个新连接。

连接状态中的参数

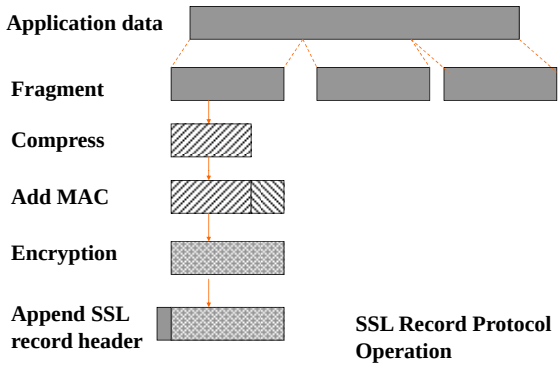
- Server and client random: server 和 client 为每一个连接所选择的字节序列。
- Server write MAC secret: 一个密钥，用来对server 送出的数据进行MAC操作。
- Client write MAC secret: 一个密钥，用来对client送出的数据进行MAC操作。
- Server write key: 用于server 进行数据加密，client进行数据解密的对称保密密钥；

连接状态中的参数

- Client wite key:用于client 进行数据加密，server进行数据解密的对称保密密钥；
- Initialization vectors: 当数据加密采用CBC方式时，每一个密钥保持一个IV。该字段首先由SSL Handshake Protocol，以后保留每次最后的密文数据块作为IV。
- Sequence number: 每一方为每一个连接的数据发送与接收维护单独的顺序号。当一方发送或接收一个改变的cipher spec message时，序号置为0, 最大$2^{64}-1$。

SSL Record Protocol

- SSL Record Protocol为SSL连接提供两种服务
  - 保密性。Handshake Protocol定义一个共享的保密密钥用于对SSL有效负载加密。
  - 消息完整性。Handshake Protocol定义一个共享的保密密钥用于形成MAC。



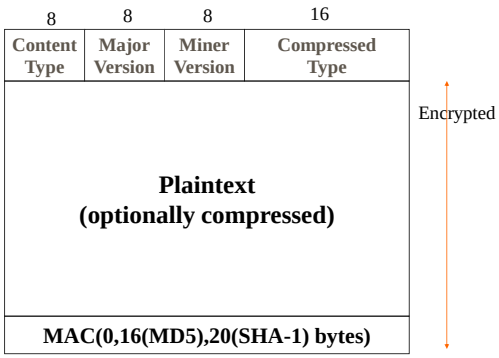
SSL Record Protocol Operation

MAC的计算过程

- hash(MAC_write_seret||pad_2||hash(MAC_write_secret||pad_1||seq_num||SSLCompressed.type||SSLCompressed.length||SSLCompressed.fragment)

可供选择的加密算法：

Block Cipher		Stream Cipher	
IDEA	128	RC-40	40
RC2-40	40	RC4-128	128
DES-40	40		
DES	56		
3DES	168		
Fortezza	80		



SSL Record Format

(a) Change Cipher Spec Protocol

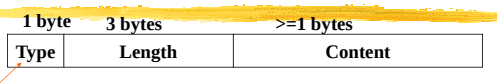
1 byte

一字节值为1，用以将挂起状态转至当前状态，导致当前加密处理包用于该连接。

(b) Alert Protocol

2字节，
Level = 1(warning),
2(fatal), SSL将立即关闭本连接，本会话的其它连接可以继续，但不能创建新连接。
Alert = 具体警告编码；如：(均为fatal的警告内容)
unexpected_message
bad_record_mac

(c) Handshake Protocol

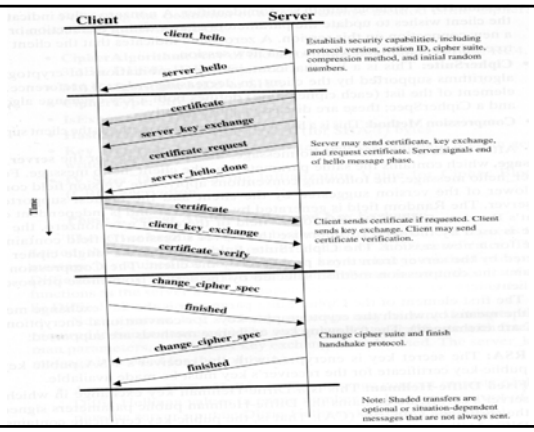


10 种类型的消息

Message Type	Parameters
hello_request	null
client_hello	version,random,session id,cipher suite,compression method
server_hello	version,random,session id,cipher suite,compression method
certificate	chain of X.509v3 certificates
server_key_exchange	parameters,signature
certificate_request	type,authorities
server_done	null
certificate_verify	signature
client_key_exchange	parameters,signature
finished	hash value

建立逻辑链接的四个阶段

- 建立安全能力
- 服务认证和密钥交换
- 客户认证和密钥交换
- 结束



安全电子交易（SET）

- SET是开放的，用于保护Internet上信用卡消费的加密和安全规范。
- SET本身不是一个支付系统，而是一个安全协议和格式的集合，使得用户能以安全的方式将已经存在的信用卡支付基础设施配置在开放网络上。

SET提供三种服务：

- 在交易涉及的各方之间提供安全的通信信道。
- 通过使用X.509数字证书提供信任。
- 保证机密性，因为信息只是在必要的时候、必要的地方才对交易各方可用。

SET的规范

- 商业描述
- 程序员指南
- 形式化的协议定义

SET的商业需求

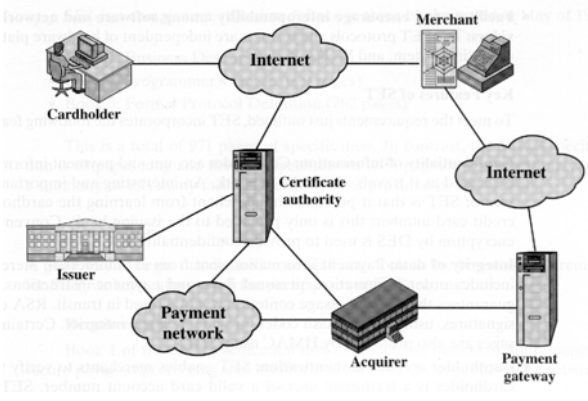
- 对支付和定购信息提供机密性
- 保证所有数据传输的完整性
- 对卡的用户进行认证
- 对商家是否合法提供鉴别认证
- 保证使用最好的安全策略和系统设计
- 协议不依赖也不阻止传输层安全机制
- 方便和鼓励软件和网络提供者之间的互操作性

SET的关键特征

- 信息的保密性
- 数据的完整性
- 卡用户的帐户鉴别
- 商人的鉴别

SET的参与者

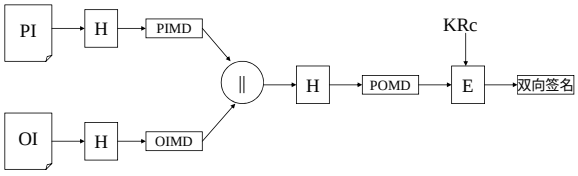
- 卡用户：消费者
- 商人：供货商
- 发行人：金融机构，银行
- 获得者：与商人之间建立一个帐户并处理支付卡的授权和支付的金融机构（商人要使用多个银行的服务，但只需与获得者联系）
- 支付网关：实现核准与支付功能
- 证书管理机构（CA）



一个交易所要求的事件序列

- 消费者开通帐号
- 消费者收到证书
- 商人拥有自己的证书
- 消费者提出一项定购
- 商人被验证
- 发送定购和支付信息
- 商人请求支付认可
- 商人确认该定购
- 商人提供服务或订货， 请求支付

双向签名



END!