信息安全作业 12

190110429-何为

1. HTTPS 是如何实现数据的安全性的?

答:

HTTPS 是以安全为目标的 HTTP 协议，在 HTTP 下加入了 SSL 协议。建立了一个信息安全通道，用来保证数据传输的安全。

主要方法: 客户端向服务器发送一个连接请求，然后双方协商一个 SSL 会话，并启动 SSL 连接，接着就可以在 SSL 的应用通道上传送 HTTPS 数据。HTTPS 使用与传统 HTTP 不同的端口，IANA 将 HTTPS 端口定为 443，以此来区分非安全 HTTP 的 80 端口，同时采用“https”来标识协议类型。

2. SET 协议要解决的主要问题有哪些?

答:

SET 协议要解决交易各环节中的安全问题，满足交易各方的安全需求。

(1) 防止数据被黑客或被内部人员窃取，保证交易信息在互联网上安全传输。
(2) 保证电子商务参与者信息的相互隔离。客户的资料加密或打包后通过商家到达银行，但是商家不能看到客户的账户和密码信息。
(3) 持卡人和商家相互认证，以确定通信双方的身份，由第三方机构负责为在线通信双方提供信用担保。
(4) 保证网上交易的实时性，使支付过程都是在线的。
(5) 要求软件遵循相同协议和报文格式，使不同厂家开发的软件具有兼容性和互操作功能。

3. SET 协议是如何保证商家、顾客和银行之间数据隐私的安全性的。

答:

SET 协议安全性主要依靠其采用的多种安全机制:

(1) 对称密钥密码：发送方使用接收方的公钥加密临时密钥，一般将这个被加密的秘钥称为电子信封。
(2) 公开密钥密码：接收方用其私钥解密出临时秘钥。
(3) 数字签名：双重签名。
(4) 消息摘要：DS（Dual Signature）技术将 OI 和 PI 这两部分的摘要信息绑定，确保电子交易的有效性和公正性。
(5) 电子信封：SET 协议使用电子信封来传递更新的密钥。
(6) 数字证书：CA 证书就是一份文档，它记录了用户的公开密钥和其他身份信息，证书均由一个权威的 CA 签发，如某金融机构的认证中心。
(7) 双重签名：分离 PI 与 OI，确保商家不知道顾客的支付卡信息，银行不知道顾客的订购细节。