SSL协议

SSL(Secure Sockets Layer 安全套接层),及其继任者传输层安全（Transport Layer Security，TLS）是为网络通信提供安全及数据完整性的一种安全协议。TLS与SSL在传输层对网络连接进行加密。

SSL和TLS的历史：

- 1990年，Netscape公司提出SSL，使得通信在WWW的环境下能够安全进行。
- 1994年，Netscape公司发布了SSL v2，SSL越来越流行并成为一个真正的标准。
- 1995年，Netscape公司发布SSL V3版本
- 1996年，Internet工程任务组IETF建立了传输层安全工作组，致力于SSL协议标准化
- 1999年，标准协议TLS作为RFC 2246被公布。总体上和SSL V3类似
- 现今TLS有两个新变体是无线TLS(WTLS)和数据报TLS(DTLS)

SSL VPN的工作原理：

1、SSL VPN用处：

- SSL VPN主要提供基于Web应用程序的安全访问
- SSL VPN操作在OSI的会话层
- Cisco将SSL VPN称为Web VPN

2、SSL VPN客户端模式：

- 无客户端：用户只是借助Web浏览器即可实现登录访问，但仅限于可以依赖浏览器的流量
- 瘦客户端：用户通过SSL下载Java或Active软件以实现部分非Web流量的传输
- 胖客户端：用户通过SSL动态下载客户端软件，类似于网络层VPN

3、SSL VPN的验证方式：数字证书和用户名密码

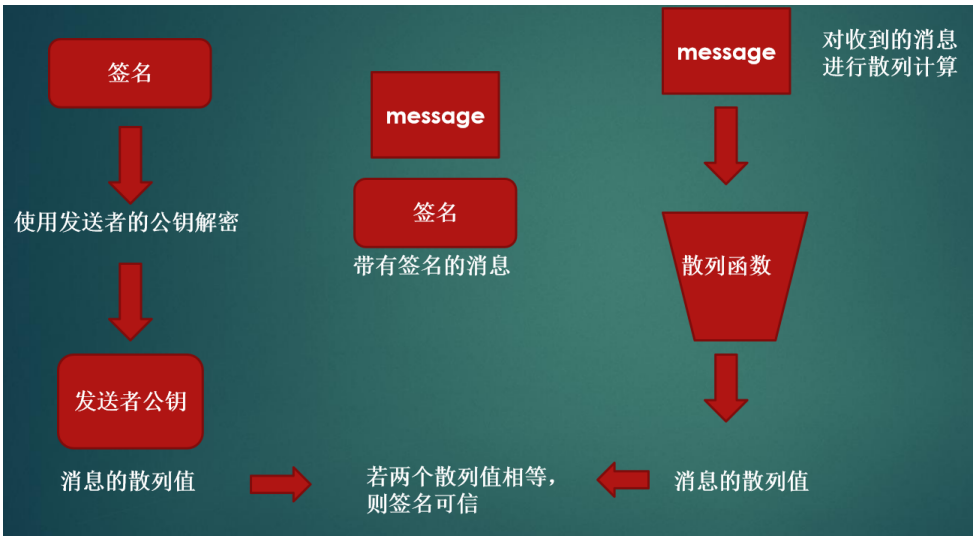
4、SSL VPN的加密：通过SSL协议实现

5、SSL VPN的内容控制：根据不同的用户来开放不同的应用程序从而对用户的访问进行控制

数字签名：

数字签名是指使用发送者的私钥加密消息散列值行为，其输出结果即被称为数字签名。当接收者收到带有相应签名的消息时需要进行两步运算：使用发送者的公钥解密收到的签名以获得散列值，再计算收到消息的散列值。对比两次计算的输出结果，若结果相同，那么接

收者就能证实此签名是可信的。常用的数字签名算法包括基于MD5和SHA-1的RSA及基于SHA-1的DSS。数字签名的验证过程如下图所示：



公钥基础结构PKI(Public Key Infrastructure)

公钥基础设施(PKI)是一个利用非对称加密算法原理和技术实现并提供安全服务的具有通用性的技术规范和标准。是管理非对称加密算法的密钥和确认信息。整合数字证书、公钥加密技术和CA的系统。其结合了软件、加密技术和组织需要进行非对称加密算法的服务。PKI技术是信息安全技术的核心。也是电子商务的关键和基础技术。

- PKI允许用户相互验证各自使用的、由认证中心颁发的数字证书
- X.509：关于PKI的ITU-T标准，定义了公钥证书的标准格式
- 公钥基础结构X.509(PKIX):IETF工作组，定义了数字证书的用途
- 公钥加密标准（PKCS）:由RSA实验室设计并公布的一组公钥加密标准。PKCS是PKI的加密基础。常见的几个标准如下：
    - PKCS1定义了RSA加密标准
    - PKCS7定义了加密消息语法标准，指定了在PKI下对消息的签名和加密。
    - PKCS10定义了证书请求标准，指定了发往认证中心的消息的格式，此消息用于请求带有密钥对的证书。

数字证书：

数字证书实质上是用户身份与其公钥的绑定。数字证书由第三方实体即认证中心（CA,certification authority）颁发，确保证书的可信性和真实性。CA负责验证用户身份、颁发证书、吊销证书和发布CRL。主要内容如下：

- 签名算法ID:指定签名算法（RSA或者DSS）
- 颁发者（CA）的X.509名称：CA服务器的身份

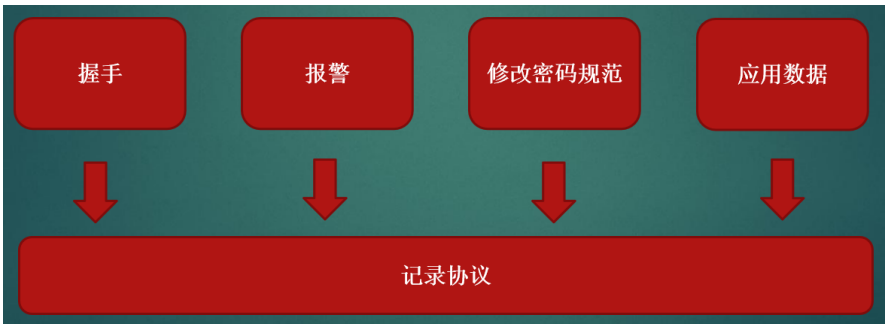
- 有效期：指定了证书的寿命
- 用户名称：包括带有X.509目录格式的用户身份。
- 用户公钥：包括与用户身份绑定的用户公钥。
- 扩展域：用户电子邮件地址或FQDN、证书吊销列表
- CA数字签名：CA服务器用CA私钥签名的散列值。

使用证书认证过程：

1. Alice首先请求根证书，即CA证书
2. CA服务器将自己的根证书回复给alice
3. alice产生一个证书请求，其中包括Alice的身份信息和公钥。Alice用CA根证书中的CA公钥签名此证书请求
4. CA服务器获得证书请求，验证Alice身份，并为Alice产生一个数字证书，将其身份与公钥绑定。这个身份证书由CA签名，提供了Alice的身份与CA身份之间的绑定。
5. CA服务器向Alice颁发证书
6. 当Alice获取证书，使用证书，将其呈递给Bob以传达信任
7. Bob将验证此数字签名，以确认Alice的证书，随后便对Alice的公钥建立信任。

SSL协议结构

SSL是一个分层协议，在最底层的是SSL记录协议。记录协议主要是一个封装协议，用于传输各种高层协议和应用数据。记录协议由4个上层客户端协议组成：握手协议、报警协议、修改密码规范协议和应用数据协议。



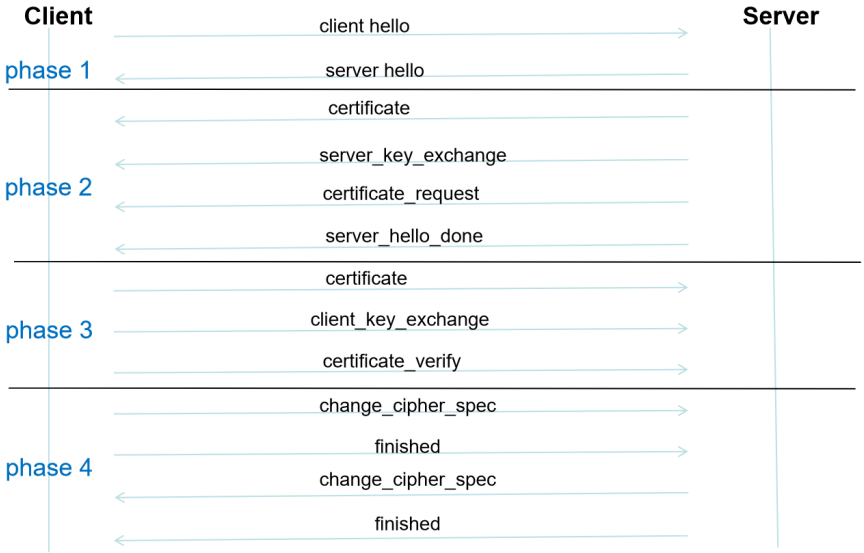
SSL 连接建立过程：

1、建立安全能力，包含协议版本，会话ID,加密套件列表、压缩方法以及初始随机数

2、服务器发送证书、密钥交换和请求证书以及服务信息结束消息

3、客户端发送证书（如果要求），客户端发送密钥交换，客户端发送证书验证消息

4、确认加密算法和密钥并完成握手协议



1、Hello阶段：

客户端和服务器建立一个逻辑连接并协商SSL会话基本的安全属性，如SSL协议版本和密码组。

客户端发起Client Hello消息：

- 协议版本
- 客户端随机数:用于计算主密钥
- 会话ID（可选）
- 客户端Cipher Suite:一个客户端支持的加密套件列表
- 压缩方法

服务器回应Server Hello消息，产生服务器随机数。

总之，经过Hello阶段后，客户端和服务器协商了安全参数，还产生了随后参与生成主密钥的必需品（客户端随机数和服务器随机数）。

2、验证和秘钥交换：

在这一阶段，客户端和服务器需要达成一个用于验证的共享密钥，称为预主密钥，这个预主密钥随后会变换成主密钥。

SSL v3和TLS支持的主要密钥交换方法：

- RSA:最常用的验证和密钥交换方法。在这个模式下，客户端产生一个随机密钥作为预主密钥，然后将其用服务器的RSA公钥加密，附在Client Key Exchange消息中发送给服务器。
- Diffie-Hellman：客户端和服务器执行DH交换，并将计算出的DH公共密钥作为预主密钥。

如果需要验证客户端，服务器将发送Certificate Request消息。客户端回应两个消息：Client Certificate和Certificate Verify。前者包含客户端证书，后者完成客户端验证工作。

3、密钥导出

主密钥从不交换，但也不是由客户端和服务器各自独立产生的。由主密钥产生的一些密钥用于消息加密和完整性验证。SSL客户端和服务器通过以下先前交换的数据来产生主密钥。

- 预主密钥
- 客户端随机数和服务器随机数

产生以下密钥：

- 客户端写密钥
- 服务器写密钥
- 客户端写MAC密钥
- 服务器写MAC密钥

4、完成握手

为了表示已准备好，客户端和服务器发送ChangeCipherSpec消息向对方表达已做好准备使用协商好的安全算法和密钥。

最后是Finished消息，此消息是由协商好的新安全算法和密钥保护的。主要是整个握手消息和主密钥的一个散列值，其消息的确认表明验证和密钥交换过程成功了。

这个阶段完成后，SSL客户端和服务器开始传送应用数据。

SSL VPN与IPSec VPN比较：

SSL VPN的优缺点：

- SSL VPN的无客户端、瘦客户端方式可以做到用户端无需安装任何软件
- 可以从任何地方安全的访问公司内部服务器
- 支持多种类型的浏览器
- 用户不需要进行特殊的培训
- SSL VPN可以和地址转换设备一起使用
- 可以对各种应用程序进行更加细致的控制

- SSL VPN为应用层内容加密，容易受到拒绝服务攻击
- SSL VPN对数据的验证功能，没有IPSec VPN使用HMAC验证效果好

特性	SSL VPN	IPSec VPN（Easy VPN）
连接	只支持远程访问	支持站点到站点和 远程访问（Easy VPN）
验证	进行证书验证	共享密钥、证书、RSA加密随机数
保护数据	只对TCP数据进行加密保护，容易受到攻击	使用隧道模式保护整个IP数据包； 使用传输模式保护用户数据
加密	一般浏览器支持RC4、DES、3DES等，而SSL/TLS还支持RC2、AES等加密算法	支持DES、3DES、AES等加密算法
消息完整性	SSL使用TCP序列号验证完整性	IPSec使用HMAC验证数据完整性
NAT	使用443端口，可以穿过一个NAT设备	需要使用NAT-T，增加复杂度
部署需求	无客户端不需要特殊部署，需要有Web浏览器；瘦客户端需要安装Java/AxtiveX的Web浏览；胖客户端需要从页面安装客户端	Ease VPN需要为每个客户端安装客户端软件。 站点到站点需要在双方设备进行相应的配置

课后习题：

1、数字证书主要包含哪些内容?

2、数字签名是怎样实现的?

3、简述SSL连接建立过程是怎样的?