SSL 及使用 OpenSSL 实现证书的签发和管理

王 娟,邱宏茂,盖 磊,王海军
(西北核技术研究所 数据处理研究室,陕西 西安 710024)

摘 要:WWW 服务器与浏览器之间的安全通信是 WEB 安全数据交换的基础。SSL 是基于 WEB 应用的安全协议,具有很强的实际安全性,它为 TCP/IP 连接提供数据加密、服务器认证、消息完整性以及可选的客户机认证。OpenSSL 是开源软件,提供了一个通用的高强度加密库,并在此基础上实现了 SSL2.0,SSL3.0,TLS1.0,分析了 SSL 协议规则,并简要介绍了 OpenSSL 软件包,同时就如何使用 OpenSSL 软件包实现证书的签发和管理进行了详细的探讨。实践证明,利用 OpenSSL 提供的库文件能很方便地对证书进行签发和管理,构建安全 WEB 服务器。

关键词:网络安全;安全套接字层;证书;OpenSSL
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1005-3751(2004)10-0138-03

SSL and Certificates Using OpenSSL

WANG Juan, QIU Hong-mao, GAI Lei, WANG Hai-jun
(Data Processing Laboratory of Northwest Institute of Nuclear Technology, Xi'an 710024, China)

Abstract: The secure communication between WWW server and browser is the basis of WEB data exchange. The SSL (Secure Socket Layer) protocol is a security protocol, which can provide data cryptograph, sever authentication, message integrity and optional client authentication. OpenSSL toolkit is open source software, which can implement SSL2.0, SSL3.0, TLS1.0. In this thesis, SSL protocol rule is analyzed and OpenSSL toolkit is introduced. Then, how to sign and manage certificate is introduced in this paper. The practice proves that is convenient to sign and manage certificates by using base documents provided by OpenSSL.

Key words: network security; SSL; certificate; openSSL

0 引 言

近年来,互联网络正以惊人的速度改变着人们的工作效率和工作方式,越来越多的个人和机构通过 Internet 发送电子邮件、互换资料及订购产品。但是 Internet 在改变人类许多行为的同时,也带来了许多安全上、管理上的问题,尤其在信息交换的过程中。因此,实现在用户浏览器与 WEB 服务器之间建立安全连接,在开放的互联网上显得尤其重要。

目前,在网络安全的各个领域中出现了许多协议,它们从不同层次、角度入手,以解决网络安全问题。SSL (Secure Socket Layer,安全套接层) 协议是目前国际上比较成熟的基于 WEB 应用的安全协议。它以多种密码技术为基础,使用公钥基础设施和 X.509 数字证书保护信息传输的机密性和完整性,在客户和服务器之间建立一个安全的网络通道,在该安全通道上,实现信息交换。

收稿日期:2004-02-30
基金项目:国防科研预先研究项目(413300305)
作者简介:王 娟(1973—),女,湖南娄底人,助理研究员,硕士,研究方向为信号处理、计算机应用。

1 SSL 安全协议

SSL 协议[1],即安全套接字层(Secure Socket Layer)协议,是 Netscape 公司于 1996 年推出的安全协议,它为网络应用层的通信提供了认证、数据保密和数据完整性的服务,较好地解决了 Internet 上数据安全传输的问题。SSL 的主要目的是为网络环境中两个通信应用进程之间提供一个安全通道。该协议共分为上、下两层。上层是握手协议,是在 Client 和 Server 之间交换消息以强化安全性的协议,Client 和 Server 在传送和接受数据前,可以鉴别相互的身份、协商加密算法和加密密钥。下层是 SSL 纪录协议,它的作用是对上层传来的数据加密后传输。

SSL 是一种介于可靠的传输协议(TCP/IP)和应用层(HTTP)之间的协议层,因此一个建立在 SSL 协议之上的应用协议能透明地传输数据。SSL 协议与应用层和传输层的关系如图 1 所示。

建立 SSL 连接通信连接,需要 WEB 服务器和浏览器都支持 SSL。SSL 的通信步骤如下:建立 TCP 连接;SSL 握手,建立 SSL 会话(Session);通过会话传送加密数据包;释放连接,会话过期。下面简要介绍 SSL 握手协议和 SSL 纪录协议。

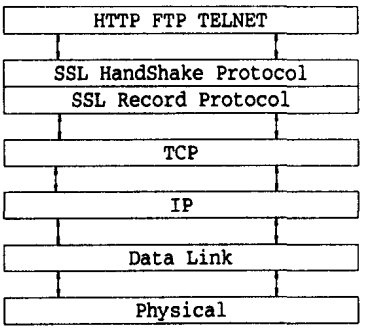
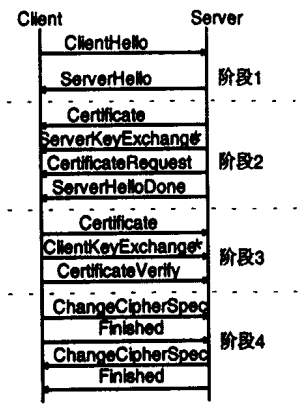


图 1　SSL 与 TCP/IP 的关系

1.1　SSL 握手协议

SSL 握手协议[2,3]维护 SSL 会话状态,为通信双方建立安全传输通道。当 SSL Client 和 Server 第一次开始通信时,双方通过握手协议,协商通信协议版本号、选择加密算法、互相认证身份,最后使用协商好的密钥交换算法产生一个只有双方知道的秘密信息,Client 和 Server 各自根据这个秘密信息产生数据加密算法和 HASH 算法的参数。会话过程如图 2 所示,可分为 4 个阶段。



* 为可选的消息

图 2　SSL 协议的握手会话

1) Hello 阶段。在该阶段,客户方先发出 ClientHello 消息,服务器方也发回一个 ServerHello 消息,Client 和 Server 通过这两条消息发起一次连接,并在协议版本号、密钥交换算法、数据加密算法和 HASH 算法上达成一致。

2) Hello 消息过后,Server 应发送服务器证书(包含了服务器公钥)和会话公钥,如果 Server 要验证 Client,则发送 CertificateRequest 消息。然后,Server 发送 ServerHelloDone 消息以表示 Hello 阶段完成。

3) Server 发证书交换要求时,Client 要返回证书或"没有证书"的提示,然后,Client 发出 Key 交换消息。

4) Finish 阶段,本阶段是 SSL 握手协议的最后部分。Client 与 Server 交换各自结束的消息。至此,握手全部完成,双方可以开始传输应用数据。

1.2　SSL 记录协议

SSL 记录协议用来在客户方和服务器方传输应用信息和 SSL 控制信息,限定了所有发送和接收的数据的打包。SSL 记录协议对上层传来的数据进行三步处理:

①由于应用协议使用的 PDU 和记录协议使用的 PDU 长度可能不一样,所以第一步要对应用数据进行重组。

②使用当前会话状态中的压缩方法对第一步的结果进行压缩;

③使用当前会话状态的加密算法对第二步的结果进行加密和 HASH 运算,算法使用的秘密在当前状态的连接状态变量中。

2　OpenSSL 概述

SSL 本身只是一个协议,要使用这个协议,还需要支持此协议的软件包。OpenSSL 提供了一个通用的高强度加密库,并在此基础上实现了 SSL2.0,SSL3.0,TLS 1.0[4]。OpenSSL 的密码库可以提供常用的对称密码算法,如:DES,DES3,IDEA,RC5,blowfish,CAST 等;非对称密码算法如 RSA,DSA;信息摘要算法如 MD5,SHA-1,RIPEMD,MDC2 等。

OpenSSL 软件包主要是用标准 C 编写的(底层的一些加密算法有可选的汇编语言,上层的实现工具使用了 Perl 语言和 Shell 脚本语言),可在各种 Unix 系统(包括 Linux 系统)和各种 WIN32 系统上安装使用。

从结构上看,OpenSSL 分为三层,如图 3 所示。底层为各种密码算法的实现,中间层是密码算法的抽象接口,上层是围绕加密算法的 PKCS 的实现,以及 ASN.1 的 DER、BER 编码接口,让这些抽象数据结构最终成为能够在网上传输、在硬盘上存储的数据。

	PKCS 实现	编/解码实现	X.509 实现
密码抽象算法			
流密码	分组密码算法	公钥密码算法	信息摘要算法

图 3　OpenSSL 软件包体系结构

从内容上看,OpenSSL 主要包括四部分:

①crypto 库。OpenSSL 的 crypto 库是通用的加密函数库和 X.509 证书函数库。

②它包括密码算法(Cipher)、消息摘要算法(Digest)、I/O 系统以及数据库。

③SSL 库,主要是 SSL 协议的实施,以及在服务器和客户断同时支持 SSL、TLS 的源码和命令行工具程序 openssl。

④一些实用工具程序,如 CA.pl。

3　使用 OpenSSL 签发和管理证书

通过 OpenSSL 提供的 PKCS 的实现,能方便地在有关 PKI(Public Key Infrastructure)的应用里做到标准数字证书的申请、签发和管理。下面将介绍如何使用 OpenSSL 签发和管理证书。

3.1　数字证书

数字证书包括证书申请者的信息和 CA 的信息,由

OpenSSL所颁发的数字证书均遵循X.509 V3标准。X.509数字证书内容如表1所示[5]。

表1 X.509证书内容

域	含义
Version	证书版本号,不同版本的证书格式不同
Serial Number	序列号,同一身份验证机构签发的证书序列号惟一
Algorithm Identifier	签名算法,包括必要的参数
Issuer	身份验证机构的标识信息
Period of Validity	有效期
Subject	证书持有人的标识信息
Subject's Public Key	证书持有人的公钥
Signature	身份验证机构对证书的签名

3.2 创建自签名的CA证书

建立认证机构CA的第一步是为该CA创建自签名证书。在OpenSSL中运行req命令,该命令生产一证书文件CAcert.pem和一密钥文件Cakey.pem。同时,在OpenSSL配置文件中必须指定CA证书和密钥文件的位置。然后,在浏览器中安装自签名证书,以便浏览器能够识别由该CA签发的服务器证书。一旦在浏览器中安装了CA自签名证书,浏览器将承认由该认证机构签发的任何证书。浏览器使用HTTP目录类型application/x-x509-ca-cert来装载证书。以Apache服务器为例,在其配置文件httpd.conf中增加一行"AddType application/x-x509-ca-cert"来实现证书的装载。

3.3 创建服务器证书

服务器证书用来向客户端验证服务器的身份。为了创建服务器证书,先创建证书请求,用自签名CA证书签发该请求,然后装载证书。

具体步骤如下:

①用req命令创建一个符合PKCS#10标准的证书请求,同时产生一组密钥对。

②用ca命令签发该请求,产生证书文件。

③拷贝证书和密钥文件到服务器证书目录下。

④在服务器目录下计算证书的hash值。

⑤创建DER格式的服务器证书文件。

⑥更新服务器配置文件。

3.4 创建客户端证书

客户端证书用来向服务器证实该客户的身份。不同的客户端浏览器创建客户证书的机制不同,但创建用户证书的一般步骤如下:客户端下载CA证书,用户填写个人信息,浏览器生成一组公、私密钥对,将私钥保存在客户端,并把公钥和证书请求一起提交给CA。CA签发证书后,客户端安装好证书,使得需要时随时提交。

3.5 配置服务器、建立SSL连接

如果服务器端已经安装了服务器证书,同时客户端的浏览器中已经安装签发该服务器证书的根证书,则服务器和客户端之间就可以建立SSL连接。以Apache为例,服务器端的配置如下(httpd.conf)。

```
# Set SSLVerifyClient to:
# 0 if no certificate is required
# 1 if the client may present a valid certificate
# 2 if the client must present a valid certificate
# 3 if the client may present a valid certificate but it is not required to
# have a valid CA
SSLVerifyClient 0
```

4 结束语

SSL协议以多种密码技术为基础,实现了身份认证、数据加密传输、数字签名等安全功能,保证了网络通信的机密性和完整性。OpenSSL软件包实现了SSL和TLS协议,利用OpenSSL提供的库文件能很方便地对证书进行签发和管理,构建安全WEB服务器。

参考文献:

[1] 宋志敏,王卫京,南相浩. SSL V3.0及其安全性分析[J]. 计算机工程与应用,2000(10):145-148.

[2] Kocher P C. SSL2.0.[EB/OL]. http://www.netscape.com/newsref/std/SSL-old.html. 1997-08.

[3] Freier A, Karlton P. The SSL Protocol Version 3.0[EB/OL]. http://wp.netscape.com/eng/ssl3/draft302.txt. 2000.

[4] Young E A, Hudson T J. OpenSSL[EB/OL]. http://www.OpenSSL.org/docs. 2003-10.

[5] GOC PKI X.509 Certificate and CRL Field and Extensions Profile[Z]. Draft version 2.0. 1999,10:45-50.

(上接第75页)

在J2EE平台上推荐的一种设计模型。文中采用MVC设计模式开发了远程考试系统,使系统具有良好的可扩展性和灵活性,并且易于维护。

参考文献:

[1] 文东戈. B/S结构网上考试系统的设计与实现[J]. 黑龙江科技学院学报,2002,12(4):34-37.

[2] 何建辉,许俊娟. JSP设计[M]. 北京:中国电力出版社,2002.

[3] 戚 欣,熊前兴. 基于MVC设计模式的电子商务Web应用框架[J]. 武汉理工大学学报(信息与管理工程版),2003,25(2):40-43.

[4] 何成方,余秋惠. MVC模型2及软件框架Struts的研究[J]. 计算机工程,2002,28(6):274-276.