对 SSL 协议及其安全性分析

任 江* 袁宏春
(电子科技大学微机所 成都 610054)

【摘要】 叙述了 SSL 协议在 Internet Client/Server 通信安全方面所起的作用;给出了 SSL 协议与网络层的关系图;对 SSL 协议中的记录层和握手层协议进行了描述,并对有关 SSL 协议安全性问题进行了较详细地分析;指出了 SSL 协议的实际应用价值和对设计开发新一代防火墙的借鉴作用。

关 键 词 安全套接字; 网络安全; 国际互联网; 加密; 解密
中图分类号 TP315

随着近年来 Internet 的爆炸性增长,其安全性问题日益突出。如何维护信息的私有性,阻止"非授权"访问,阻止网络"黑客"入侵破坏等等,已成为 Internet(或者说 Internet 技术)走向商业、政府机构、军事、企业等应用的主要问题之一。为提高现有网络的安全性,当前主要解决办法有:对需公共存取的资源建立隔离区隔离敏感的私有网络,在现有的网络上加载防火墙,重新构筑采用新一代安全协议的网络等等。与此同时,也出现了一些在现有网络之上,力求为 C/S 通信双方提供认证和加密私有通道的协议,SSL 即是其一。

SSLP(Secure Sockets Layer Protocol)是由 Netscape 公司最早提出,旨在为 Internet Client/Server 通信安全提供一个实际的、应用层的、面向连接的机制,并已形成了协议规范。该公司的 Netscape Browser,微软的 IE 等流行的 WEB 浏览器均支持该协议。

1 安全套接字(SSL)协议[1]

1.1 概述

SSL 协议的设计初衷是为两个通信应用(一个客户,一个服务器)之间提供加密的私有通信,提供 Server 的认证,选项提供 Client 认证。SSL 可运行在任何一种可靠的传输协议之上(如 TCP,但并不依赖于 TCP),并能够运行在如 HTTP、FTP 和 TELNET 等应用层协议之下,为其提供安全的通信,其关系如图 1 所示。SSL 协议使用 X.509 来认证,RSA 作为其公钥算法,可选用 RC4-128、RC-128、DES、三层 DES 或 IDES 作为其数据加密算法。SSL 协议分为两层:记录层与握手层。每一层使用下一层提供的服务,并为其上层提供服务。这两层在 ISO 的七层参考模型中介于应用层与传送层之间,即:应用层→握手层→记录层→传送层→…

1.2 SSL 记录层协议

SSL 记录层提供通信、认证,并且在一个面向连接的可靠的传输协议(如 TCP)之上提供保护。在 SSL 中所有数据都被封装在记录中。一个 SSL 记录由两部分构成:记录头和非零长度的数据。记录头可以是 2 字节或是 3 字节(当有填充数据时用),该头主要用于指示记录长度。两字节头的最大记录长度是 32 767 字节,3 字节头的最大记录长度为 16 383 字节。SSL 握手层协议的报文要

1998 年 3 月 3 日收稿
* 男 24 岁 硕士生

求必须放在一个 SSL 记录层的记录里，但应用层协议的报文允许占用多个 SSL 记录层记录来传送。

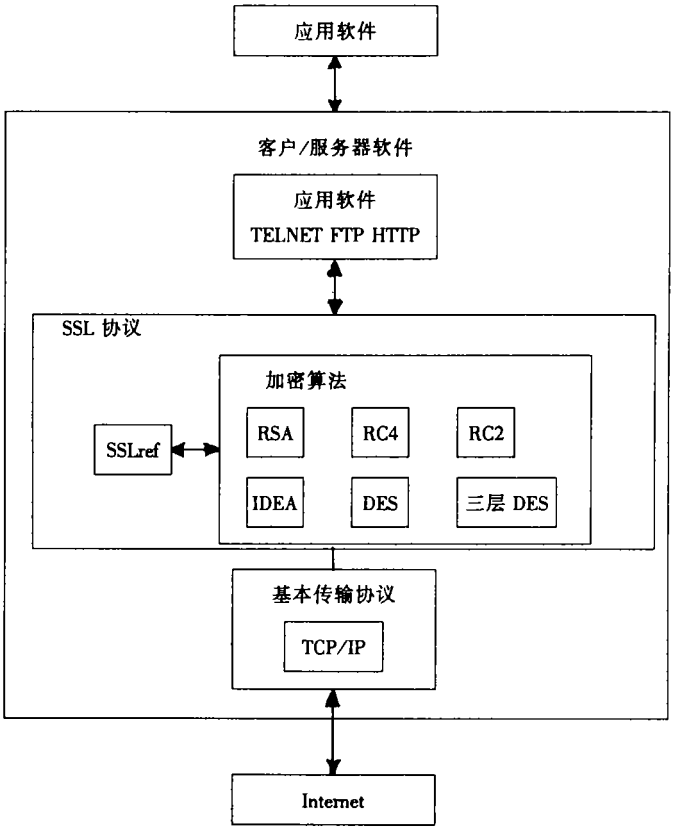

图 1　SSL 协议与相关网络层的关系图

记录的数据部分由三个部分组成：一个 MAC(Message Authentication Code)，实际的数据和填充数据，若使用“块加密”方式，加密数长度不是块长度的整数倍，就需要填充数据。记录的数据部分是完全加密的。记录层结构如图 2 所示。

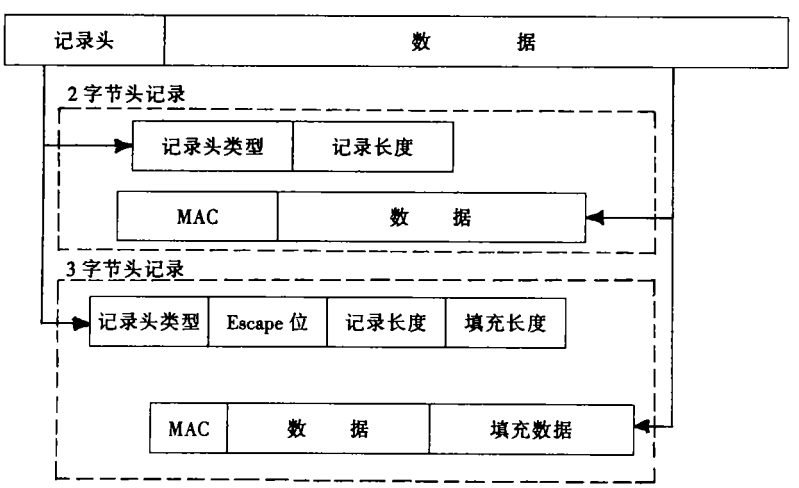

图 2　SSL 记录层结构

1.3 SSL 握手层协议

握手过程包括两个阶段:1) 选择一个主密钥、加密算法、认证服务器;2) 如果需要的话,进行客户认证,完成握手协议。握手层的报文由两部分组成:1) 一个字节的报文类型代码;2) 数据(随报文类型不同,结构不同)。所有握手层的报文以及之后的数据报文,均是通过记录层传送的。

本文通过一典型的握手过程来简介该层协议的报文流,如表 1 所示。

表 1 无会话标识、无客户认证的握手过程

报文类型	方向	传输的数据
client-hello	C > S	challenge-data, cipher-specs
server-hello	C < S	connection-id, server-certificate, cipher-specs
client-master-key	C > S	cipher-kind, clear-master-key, [secret-master-key] server-public-key
client-finish	C > S	[connection-id] client-write-key
server-verify	C < S	[challenge-data] server-write-key
server-finish	C < S	[session-id] server-write-key

注:"[data] key"表示数据 data 用钥匙 key 加密。

· Client-hello 报文为发送测试数据和客户所能支持的数个加密算法列表给服务器;

· server-hello 报文为返回一个连接标识、一个服务器证明和一个修改了的客户和服务器都能支持的加密算法列表;

· client-master-key 报文为以明文返回选定的加密算法和主密钥,主密钥前 40 位不加密,其余位加密(这一规定是因为美国对加密软件的出口限制)。实际的密钥并非 master-key,而是由 master-key 生成的两个密钥:client-write-key(server-read-key),client-read-key(server-write-key)。从这时起,以后客户用 client-write-key 加密发送报文,服务器则用 server-read-key 解密;同样服务器用 server-write-key 加密发送报文,客户用 client-read-key 解密[2,3]。

·client-finish 报文为用 client-write-key 加密发送之前服务器送来的 connection-id。

· server-verify 报文为用 server-write-key 加密发送之前客户送来的测试数据,用于客户验证服务器。

· server-finish 报文包含了一个用 server-write-key 加密的"会话标识号"。这样,以后当同一客户和服务器对再次"握手"时,可不必再协商加密算法和主密钥。

2 对协议安全性的分析

2.1 "监听"和"中间人"攻击

SSL 协议使用一个经通信双方协商的加密算法和密钥。对安全需求级别不同的应用,都可找到不同强度的加密算法用于通信数据加密。它的钥匙管理也处理得比较好:在每次连接时通过哈希(hash)随机函数生成一个短期使用的会话密钥,除了不同次连接使用不同的密钥外,在一次连接的两个传输方向上它都使用了单独的密钥。从上面对 SSL 协议的介绍来看,尽管它给监听者提供了很多明文,但由于其较好的密钥保护(采用 RSA 交换密钥),以及频繁更换密钥,因此,对于"明文"、"监听"及"中间人"攻击而言,其安全性应是可靠的。

2.2 “流量数据分析”攻击

这种攻击,其核心是通过检查数据包的未加密字段或未加保护的包的属性来试图进行攻击。例如:通过检查 IP 包中未加密的 IP 源地址和目标地址、或检测网络流量,攻击者可知道谁正在参与交互通信,它们在使用何种服务,有时候甚至能得到或推测出一些商业或个人之间的关系。

用户在通常情况下认为这种分析是相对无害的,SSL 协议也未尝试阻止这种攻击。但也有一些特殊情况,可能会给攻击者提供较大的成功概率。例如:当一个 WEB 浏览器通过 SSL 向一个 WEB 服务器发出请求(在 HTTP 协议中,它应传送 GET 请求,并在后面跟上 URL 地址),GET 请求和 URL 地址均以密文传送,但 WEB 服务器地址和请求长度,可通过 IP 包分析被攻击者获得,此后 WEB 服务器将请求的 WEB 页面传回浏览器,同样其长度也可获得,通过对 URL 请求长度和取回的 HTML 页面长度的综合分析,结合对该 WEB 服务器使用 WEB 页面搜索技术,很容易发现是什么 WEB 页被存取了。我们曾做了一个 WEB 搜索引擎,可以很容易地对一个指定的 WEB 服务器、针对指定长度的 URL 请求,找到返回指定长度 HTML 数据的 WEB 页面。

2.3 “截取再拼接”攻击

仅对通信使用非常强的连接加密,其安全性仍值得考虑。

这种攻击方式的大致过程是:首先,从一些包含敏感数据的包中“切下”一段密文;然后,再把这段密文拼接到另外一段密文中,被拼接的这段密文是经过仔细选择的,使得接收端非常有可能泄漏出经过解密后的明文。例如:在仅有连接加密的情况下,攻击者可能把截下的一段密文拼接在由服务器传回客户的 WEB 页面中的一个 URL 主机名部分。这样,当浏览器收到这个数据包后,就会解密这个 URL 链接——即拼接上的那段特殊密文(说不定是一用户的加密口令)被解密成了主机地址,于是当用户点了这个链接以后,浏览器会把这段拼接上的特殊密文当做主机名,从而以明文形式传送一个 DNS 域名解析报文,这个报文就会被攻击者偷听截获到。

SSL3.0 基本上已经阻止了这种攻击。首先,它对不同的上下文使用了独立的“会话标识符”,这就阻止了“截取再拼接”攻击在不同次连接之间截取和拼接;其次,SSL3.0 对所有的加密包使用了较强的认证,在这种防卫之下,“截取再拼接”攻击已基本不易成功。

2.4 “短包”攻击

“短包”攻击,相对而言,应用机会较少。它的基本过程是假设现在的通信是用 DES 加密数据,并用 TCP 传送,那么当传送最后一个报文时,可能明文就只有一个字节,而其后就是填充数据。这时,当攻击者截到报文以后,就可用已知“明文/密文”对的另外一个加密块去置换这个报文。然后,它可以通过 TCP 校验和是否有效,知道自己截得是否正确。即使不正确,也只不过是使接收方的 TCP 协议认为其出错而丢包,用户不会知道;但如果正确,则可通过接收方发回的 ACK 获知。

SSL 尽管在这点上看起来能被攻击的可能性很小,比如用 SSL 传送 WEB 页、URL 请求,但如果客户是经常收发一个字节长度报文的 TELNET,那么就需要对这种攻击做较强的保护了。

2.5 “报文重放”攻击

“报文重放”攻击是一种比较容易被阻止的攻击,SSL 通过在 MAC 数据中包含进“序列号”阻止了“重放”攻击。同时,这种机制也阻止了“延迟”、“重排序”、“删除数据”等攻击方式。

2.6 钥匙管理中的一些问题

设计一个安全秘密的钥匙交换协议是相当复杂的[4]。因此对于 SSL 的握手层协议,也存在一些需探讨的问题:1) 客户与服务器在互送自己能支持的加密算法时,是以明文传送的,这时是否有被攻击者修改的可能,导致它们均使用加密位数最短的算法,如 40 位。2) SSL 3.0 的实现要兼容 SSL2.0,则有可能将客户的 3.0 HELLO 报文修改成 2.0 的 HELLO 报文。3) 所有的会话密钥均由

MASTER-KEY 生成。握手协议的安全,将完全依赖于对 MASTER-KEY 的保护,因此,MASTER-KEY 应尽可能地少用在通信中。

3 结束语

综上所述,SSL3.0 采用了通信数据加密、身份验证等安全技术。它在不同层次连接、不同的传送方向上都使用了不同的密钥;客户和服务器间采用了数字签名和认证,较好地保证了数据在传送过程中的完整性,防止了欺骗、修改等多种攻击。在提供较好安全性的同时,SSL3.0 也有值得探讨和改进的地方:如钥匙管理等等。通过分析其设计思想与实现,观测其实际应用,证明 SSL 协议在为 Internet 应用提供实际的通信安全方面,走出了非常有价值的一步。

现今的网络信息系统,大都需要建立自己的防火墙系统来抵御各种攻击,保护网络信息流的安全。传统的"包过滤"和"应用代理"型防火墙在发展中除了二者相互结合以外,更增加了诸如实现虚拟私有网(VPN)、可信的身份鉴别、审计追踪等功能[5]。在密钥管理、钥匙交换、数字签名、身份验证这些方面,SSL 无疑也提供了可供分析和借鉴的作用。

参 考 文 献

1 Karlton A Freier, Kocher P. The SSL protocol. Internet Draft, 1996

2 Bellovin S. IP security protocols. Usenix Association, 1996:205 ~ 214

3 RSA Data Security Inc. Public-key cryptography standards. 1993

4 Aziz Ashar, Markson Tom. Simple key-management for internet protocols. Internet Draft, 1995

5 Greenwald Michal B, Singhal Sandeep K, Stone Jonathan R *et al*. Desiging an academic firewall. NCRL paper Univ Standford, 1996

Analysis of Security SSL

Ren Jiang Yuan Hongchun

(Inst. of Microcomputer, UEST of China Chengdu 610054)

Abstract This paper describes the function of the SSL protocal in client/server communications security and provides the relation between SSL protocal and network level. The recording level protocal and clasp hands level protocal in the SSL protocal is discussed, and the security problems of SSL protocal is analyzed. This paper also points out the value of SSL to the practical applications and its help to the design and development of the new generation firewall system.

Key words secure socket layer; network security; internet; encryption; decryption

编辑 叶 红