

利用双证书机制改进 SSL/TLS 协议

李晓峰, 赵海, 周艳, 宁宣杰

(东北大学信息科学与工程学院, 辽宁 沈阳 110004)

【摘要】在PKI技术规范发展的过程中目前形成两种证书机制:单证书机制和双证书机制^[1]。近年来,在欧洲等国家又掀起多证书协议的研究^[2],但尚不成熟。单证书是目前广泛存在和应用的证书机制,但用证书的加密和签名在PKI中是两种应用,因为,在SSL协议的应用中都采用双证书机制。为此,论文重点讨论了双证书机制的实现与应用,以及它对SSL/TLS通信协议进行的安全性改进,如改进了TLS的访问控制、增加抵抗DoS攻击特性等相关研究。

【关键词】数字证书; SSL协议; SSL/TLS通信协议; PKI; PMI; ACL; DoS攻击

【中图分类号】TP309 **【文献标识码】**A **【文章编号】**1009-8054(2007) 11-0022-03

Improving SSL/TLS protocol using double-certificate mechanism

LI Xiao-feng, ZHAO Hai, ZHOU Yan, NING Xuan-jie

(School of Information Science and Engineering Northeastern University, Shenyang Liaoning 110004, China)

【Abstract】 At present, there are two certificate mechanisms with the development of PKI system, one is single-certificate mechanism, and the other is double-certificate mechanism. In these years, there are many researches on double-certificate mechanism in Europe, while which are not mature enough. Although single-certificate mechanism is widespread presently, yet the encryption and the signature using certificates are two different applications, and it is double-certificate mechanism that has been used in SSL protocol. Therefore, this article puts emphasis on the implementation of double-certificate mechanism and the improvement of SSL/TLS protocol using this mechanism, such as improving the access control of TLS, enhancing the counteraction ability of DOS attack.

【Keywords】 Certificates; SSL protocol; SSL/TLS communication protocol; PKI; PMI; ACL; DOS attack

0 引言

SSL协议^[3]从1994年Netscape公司提出后被广泛接受,现在所有主要的Web浏览器和服务器以及其他的软硬件产品都采用SSL。到目前为止,SSL协议主要的版本是:SSL2.0协议,它存在着一些如“中间人”(man-in-the-middle)攻击的弱点。因此,公司在1996年对该协议进行了一些修改,发布了保密通信技术(PCT, Private Communication Technology)协议,并运用于Internet Explorer等产品中。1996年Netscape公司发布了SSL3.0,增加了对除RSA算法之外的其他算法的支持,以及改进了SSL2.0中MAC算法的

构建方法,增加了HASH算法支持的消息密钥长度,并且对抵御中间人攻击方面进行了改进。另外SSL3.0在协议的功能方面也进行了改进和增强,如SSL3.0可以对证书链进行处理、可以使用Diffie-Hellman和Forteza协议进行密钥交换、可以使用非RSA密钥(如椭圆算法ECC)体系的证书,以及可以对记录压缩和解压缩等处理。目前,微软公司也已经开始在各种基于TCP/IP的软件版本中支持SSL。

1 SSL/TLS协议安全问题

SSL/TLS协议^{[3][4]}的基本设计目标是在两实体(客户和服务端)之间提供一个安全的管道。为了防止客户/服务器应用中的监听、篡改以及消息伪造,SSL/TLS提供了服务器认证和可选的客户端认证。通过在两个实体之间建立一个共享的密钥提供保密性和完整性。SSL协议分为TLS记录协议和TLS握手协议两层。TLS记录协议的一条记录包含长度域、描述域和内容域。记录协议得到要发送的消息后,将数据分

收稿日期:2007-09-07

作者简介:李晓峰,1962年生,男,辽宁沈阳人,东北大学博士研究生;赵海,1959年生,男,辽宁沈阳人,东北大学教授,博士生导师;周艳,东北大学博士在读,研究领域:嵌入式技术;宁宣杰,东北大学博士在读,研究领域:嵌入式技术。

成易于处理的数据分组,进行数据压缩处理,计算数据分组的密码校验值 MAC,加密数据,然后发送数据。接收到的消息首先被解密,然后校验 MAC,解压缩,重组,最后传递给协议的高层客户。

记录协议有四种类型的客户:握手协议、警告协议、更改密码规范协议和应用数据协议^{[4][5]}。为了便于 TLS 协议的扩展,记录协议可以支持额外的记录类型^[6]。TLS 握手协议负责建立当前会话状态的加密学参数,包括以下步骤^{[3][4][6]}:交换 hello 消息以协商密码算法,交换随机值并检查会话是否可重用;交换必要的密码学参数,使客户和服务端能够协商 pre master secret;交换证书和密码学信息,使客户和服务端能够进行相互认证;使用交换的随机值和 pre master secret 生成主密钥 master secret;为记录协议提供安全参数。

TLS 握手流程如图 1 所示^{[3][7]}。TLS 应用 PKI 管理密钥并通过公钥算法实现用户身份验证,它存在以下问题:

问题一:如果用户数目很大,通过基于证书的身份验证仅可以确定用户身份,但却不能区分出每个人的用户权限,即不能决定谁被允许做什么和被允许的人对所要操作事务的实际权限。解

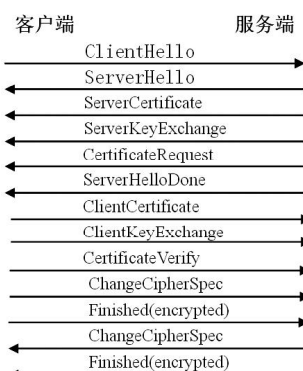


图 1 TLS 握手协议的消息流程

决这个访问控制问题的传统做法是使用访问控制表 ACL^{[8][9]},每增加一个新用户,都要求在每个应用程序的 ACL 中添加该用户项,其结果是,要么 ACL 长度在各地迅速增长,要么产生一个集中式的大型 ACL,所有应用程序必须联机访问。从管理角度来说两者都是噩梦。

问题二:在 TLS 中,无论是身份鉴别还是密钥交换都采用同一个证书(包含与密钥交换算法相匹配的密钥,如 Server Certificate 消息)完成加密操作和签名操作。用于密钥交换操作的这个密钥应该经常更新,从而保证其可靠性;而对代表 TLS 通信方身份的身份鉴别密钥,不应经常更换。因此,身份鉴别和密钥交换使用同一对密钥(即应用同一张证书)给证书和密钥管理带来了许多不可解决的问题,同时也影响到 TLS 协议的安全性。

2 改进 TLS 安全性

针对上述 TLS 安全性的第二个问题,可以使用双证书机制解决。在 TLS 协议中使用双证书的过程如下:在 TLS 中,用签名证书识别用户的身份,用加密证书进行密钥交换。在

TLS 协议中应用双证书机制进行加密和签名操作的分开管理,改进后的 TLS 握手协议的消息流程如图 2 所示。

相关消息的描述如下:

Signature Certificate Encipher Certificate ::= sequences of certificate

Signature Certificate Request Encipher Certificate Request ::= sequences of trusted authority

Server Key Exchange: 仅在服务器发送的 server Encipher certificate 消息中没有包含足够的信息使客户可以交换 pre master secret 的时候发送,为客户端协商 pre master secret 传递密码信息。Certificate Verify 消息的内容为对 (Client Hello, Server Hello, Signature Certificate, Encipher Certificate, Server Key Exchange, Signature Certificate Request, Encipher Certificate Request, Server Hello Done, Signature Certificate, Encipher Certificate, Client Key Exchange, Certificate Verify, ChangeCipherSpec, Finished(encrypted), ChangeCipherSpec, Finished(encrypted)) 的签名。

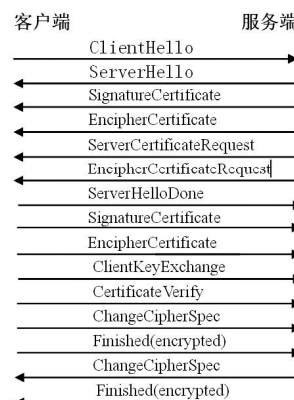


图 2 采用证书机制改进 TLS 握手协议的消息流程

3 其他改进的讨论

3.1 改进 TLS 访问控制特性

在 TLS 中涉及到身份验证的消息主要有 certificate request、client certificate、certificate verify,在这些消息中所用到的证书为身份证书,所以在 TLS 握手中仅能识别双方的身份,但不能确定双方对应用层数据的访问权限。如在操作系统中,用户分为系统管理员、超级用户、一般用户和自定义用户等,在这些权限设置中是无法用身份证书来解决的。在电子商务中,应用服务器的资源一般分为不同的安全级别,不同的用户只能访问其所对应的资源,而在利用 TLS 解决用户访问服务器时,是无法解决用户的访问权限。在大多数应用中,权限的应用范围远远大于身份的应用,所以必须对 TLS 进行改进,使其应用范围更广。因此,我们可以通过应用特权管理体系 (PMI) 中的属性证书的手段改进 TLS 协议,增强它的访问控制特性。

如果将属性证书应用在访问控制方面,就不必使用 ACL,也不再基于用户身份,取而代之的是基于具有的属性来决定其对某一资源或服务是否拥有访问权。这样,应用程序中的访问控制规则可以简单地被定义成属性的有效期(在属性证书中规定)来决定访问权,非常简单、容易理解,并且

更易维护。应用属性证书进行访问控制还意味着这是一个可伸缩的方案,既可以支持无穷尽的用户,又不用对应用程序作任何改变(假定所有用户都可以被定义成同一套属性集合)。在TLS协议中应用属性证书进行细粒度权限控制,即先通过PKI身份证书进行身份确认,而后服务器端通过获得客户端属性证书,进而获得客户端在该服务器上面的操作属性,从而为客户端分配相应的权限。改进后的TLS消息流程如图3所示。

应用属性证书改进后的TLS协议在安全性方面没有减弱(应用PKI身份证书进行认证和使用相关的加密算法形成加密管道),只是通过属性证书的使用增强了TLS协议的访问控制特性,增强了

TLS协议的实用性。相关消息的描述如下:

```
ac info ::= [attribute cert][pkcerts]
pkcerts ::= OCTETS
struct { opaque ac info <1...2^24-1> } AC Request
struct { opaque ac info <1...2^24-1> } AC Info
```

原来的Certificate Verify消息的内容为对(Client Hello、Server Hello、Server Certificate、Server Key Exchange、Certificate Request、Server Hello Done、Certificate、Client Key Exchange)的签名,现在应改为对(Client Hello、Server Hello、Certificate、Server Key Exchange、Certificate Request、Attribute Certificate Request、Server Hello Done、Client Certificate、Attribute Certificate Info、Client Key Exchange)的签名。在Server端发Finished消息之前应增加对属性证书的验证,由于属性证书和身份证书相关联,所以属性证书验证的前提是身份证书的验证通过,然后确定发放属性证书机构的可信度、证书签名是否有效、证书是否过期,等等。最后,应用程序检查属性证书中的内容,来确定是否允许此用户存取其所需的资源及服务。

3.2 增加抵抗DoS攻击的特性

在TLS协议中使用双证书和属性证书可以增强TLS协议在认证和权限控制方面的安全性,但并没有改变TLS协议不能抵抗拒绝服务攻击(DoS)的弱点。一个应用TLS协议的服务器经常为大量的客户端应用提供安全服务,这些客户端应用可以非常容易地强制服务器执行过载的计算任务(如进行

大量的指数级运算),耗尽服务器的资源和CPU的时间。下面我们将通过改进后的TLS协议对这方面的问题进行解决。

解决一个协议是否可以抵抗拒绝服务攻击的方法多数采用在通信的过程中使用Cookie(一个由服务器产生的随机数)进行控制。通过Cookie可以避免非法的客户端无限次地提交与服务器端的握手请求。

3.3 ETLS—改进的TLS协议

下面是改造后的协议的消息流程,如图4所示。从图中可以看出,在进行TLS通信的早期阶段,改进后的协议使用了两个消息进行服务器与客户端之间的Cookie传递。通过Cookie可以使服务器与客户端进行同步,使服务器获得有关消息发出点(消息源)的信息,从而可以抵制通过伪装信息发出点(伪装信息源)对服务器发送大量信息的攻击,即可以抵抗拒绝服务攻击。

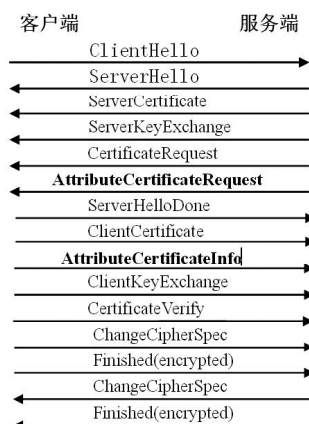


图4 可抵抗DoS攻击的TLS握手协议的消息流程

4 结语

本文在对SSL/TLS

协议进行安全性分析的基础上,利用前面关于双证书机制的讨论结果以及使用属性证书对SSL/TLS进行改进。这种改进不是针对TLS协议运行需要的支撑环境,即算法集合,而是针对TLS运行所需要的PKI环境,重点放在TLS应用时不容忽视的访问控制和证书管理问题上。本文最后提出了一个改进的TLS协议,改进后的TLS协议具有抵抗拒绝服务攻击(DoS)的特性,更加安全和实用。

参考文献

- [1] Carlisle Adams, Steve Lloyd. Understanding Public-Key Infrastructure: Concepts, Standards and Deployment Considerations. Macmillan Technical Publishing, 1999.
- [2] [RFC3039] S. Santesson, W. Polk, P. Barzin, et al. Internet X.509 Public Key Infrastructure Qualified Certificates Profile. 2001-1. <http://ftp.rfc-editor.org/notes/rfc3039.txt>.
- [3] IETF INTERNET-DRAFT The SSL Protocol

(下转第27页)

3.1 引导型病毒的防范

引导型计算机病毒主要感染磁盘的引导扇区,也就是常说的磁盘的BOOT区。我们在使用被感染的磁盘(无论是软盘还是硬盘)启动计算机时,它们就会首先取得系统控制权,驻留内存后再引导系统,并伺机传染其他软盘或硬盘的引导区。如果确诊计算机已被感染了引导型病毒,最好用杀毒软件加以清除,或在“干净的”系统启动引导下,用备份的引导扇区覆盖^[5]。预防引导型计算机病毒,可以采用以下一些方法:

- (1) 坚持从不带毒的硬盘引导系统。
- (2) 安装能够实时监控引导扇区的杀毒软件,或经常用能够查杀引导型病毒的杀毒软件对系统进行检查。
- (3) 经常备份系统引导扇区。
- (4) 某些底板上提供引导扇区计算机病毒保护功能(Virus Protect),启用它对系统引导扇区也有一定的保护作用。

3.2 文件型病毒的防范

文件型病毒在计算机病毒中占绝大多数,它们一般只传染磁盘上可执行文件(.COM, .EXE),在用户调用染毒的可执行文件时,计算机病毒首先被运行,然后计算机病毒驻留内存伺机传染其他文件,其特点是附着于正常的程序文件,成为程序文件的一个外壳或部件。如果确诊计算机已被感染了文件型病毒,建议最好先用查杀毒软件进行清除,或者直接删除带毒的应用程序,然后重新安装。预防文件型计算机病毒,可以采用以下一些方法:


- (1) 安装最新版本的、有实时监控文件系统功能的查杀毒软件,并经常用其对系统进行查杀工作。
- (2) 及时更新查杀毒引擎,一般要保证每月至少更新一次,并在计算机病毒突发事件时及时更新。
- (3) 对关键文件,如系统文件、保密的数据等,要在没有计算机病毒的环境下经常备份。
- (4) 在不影响用户正常工作的情况下对系统文件设置最低的访问权限,以防止文件型病毒的侵害。

4 结语

随着计算机的不断普及和网络的发展,计算机病毒造成的危害越来越大。1999年4月26日的CIH病毒大爆发给我们带来了巨大损失,而其后出现的Melissa、Explore ZIP、July-Killer等病毒也在计算机用户中造成了不小的恐慌,但这往往是因为不了解病毒而产生的。我们认为,只要真正了解计算机病毒本质,熟悉病毒传播模型、运作机制、触发机制、破坏机制等方面的规律,选用合适的反病毒产品,受到病毒危害的几率就会大大减少。此外,还应树立计算机病毒意识,积极采取预防措施,通过各种有效手段,将


计算机病毒拒之门外。

参考文献

- [1] 刘东华. 网络与通信安全[M]. 北京:人民邮电出版社, 2004: 203.
- [2] 肖军模. 网络信息对抗[M]. 北京:机械工业出版社, 2005: 138.
- [3] 刘尊全. 计算机病毒防范与信息对抗技术[M]. 北京:清华大学出版社, 2001: 122 ~ 123.
- [4] 郭祥昊, 钟义信. 计算机病毒传播的两种模型[J]. 北京邮电大学学报, 2005; (3): 92 ~ 94.
- [5] 傅建明. 计算机病毒分析与对抗[N]. 北京:清华大学出版社, 2005: 10. 

(上接第24页)

Version 3.0, November 1996.

- [4] Dierks T, Allen C. The TLS Protocol, Version 1.0. Request for Comments 2246, Jan. 1999. <http://www.ietf.org/rfc/rfc2246.txt>.
- [5] David Wagner, Bruce Schneier. Analysis of the SSL 3.0 Protocol. April 1997.
- [6] R. Oppliger. Internet and Intranet Security. Artech House, Norwood, MA, 1998.
- [7] E Biham, A Shamir. Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, New York, N.Y. 1993.
- [8] Brian Tung. Kerberos: A Network Authentication System. Addison Wesley Longman, Inc. 1999.
- [9] Rolf Oppliger. Security Technologies for the World Wide Web. Artech House Inc. 2000. 

本栏目协办单位

