传输层安全协议的安全性分析及改进*

孙林红[1+], 叶顶锋[1], 吕述望[1], 冯登国[1,2]

[1](中国科学院 研究生院 信息安全国家重点实验室,北京 100039)

[2](中国科学院 软件研究所 信息安全国家重点实验室,北京 100080)

Security Analysis and Improvement of TLS

SUN Lin-Hong[1+], YE Ding-Feng[1], LÜ Shu-Wang[1], FENG Deng-Guo[1,2]

[1](State Key Laboratory of Information Security, Graduate School, The Chinese Academy of Sciences, Beijing 100039, China)

[2](State Key Laboratory of Information Security, Institute of Software, The Chinese Academy of Sciences, Beijing 100080, China)

+ Corresponding author: Phn: 86-10-88258713, E-mail: sun_lin_hong@sohu.com

http://home.is.ac.cn

Received 2001-11-12; Accepted 2002-05-13

Sun LH, Ye DF, Lü SW, Feng DG. Security analysis and improvement of TLS. *Journal of Software*, 2003,14(3):518~523.

Abstract: The analysis of security about TLS (transport layer security) protocol is proposed in this paper, based on once encipherment, access control and dual certificate. Upon the analysis, extensions are given for message process and content of TLS, the improved protocol is more secure and practical.

Key words: once encipherment; access control; dual certificate; transport layer security protocol

摘 要: 基于一次一密、访问控制和双证书机制对 TLS(transport layer security)协议进行了安全性分析,并针对分析结果,对 TLS 协议的消息流程以及消息的内容进行了扩展,改进后的协议更具有安全性和实用性.

关键词: 一次一密;访问控制;双证书;TLS 协议

中图法分类号: TP393 **文献标识码**: A

1994 年,Netscape 公司为了保护 Web 通信协议 HTTP,开发了 SSL(secure socket layer)协议.该协议第 1 个成熟的版本是 SSL2.0 版,被集成到 Netscape 公司的 Internet 产品中,包括 Navigator 浏览器和 Web 服务器产品等.SSL2.0 协议的出现,基本上解决了 Web 通信协议的安全问题,很快引起了大家的关注.1996 年,Netscape 公司发布了 SSL3.0,该版本增加了对除 RSA 算法以外的其他算法的支持和一些新的安全特性,并且修改了前一个版本中存在的安全缺陷,与 SSL2.0 相比,更加成熟和稳定,因此很快成为事实上的工业标准.1997 年,IETF 基于 SSL3.0 协议发布了 TLS(transport layer security)1.0 传输层安全协议的草案.1999 年,正式发布了 RFC2246[1].

自从 TLS1.0 成为工业标准以后,TLS1.0 在 Internet 上已得到长足的应用,除了如 S/HTTP,S/MIME, SSL-Telnet,SSL-SMTP,SSL-POP3 等常用的协议以外,人们在开发各种电子商务和电子政务系统时也是基于

* Supported by the National High-Tech Research and Development Plan of China under Grant No.2001AA140101 (国家高技术研究发展计划)

第一作者简介: 孙林红(1969－),男,江苏泰州人,博士生,主要研究领域为信息安全,密码理论.

TLS,正是由于 TLS 的重要性,所以有必要对其进行分析.目前已有不少这方面的文章[2],如形式化分析,包括 BAN 逻辑、Kailar 逻辑.本文主要从一次一密、访问控制和双证书等方面对 TLS 进行安全性分析,并根据分析,对 TLS 进行适当的改进,使其更加安全、实用.本文第 1 节从整体角度介绍 TLS 协议.第 2 节基于一次一密分析和改进 TLS.第 3 节基于访问控制分析和改进 TLS.第 4 节基于双证书机制分析和改进 TLS.

1 TLS 简介

TLS 协议的基本设计目标是为两个通信实体之间提供数据的保密性和完整性.该协议分为两层:TLS 记录协议和 TLS 握手协议,下面将简要介绍 TLS 记录协议和 TLS 握手协议.

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之后,将数据分成易于处理的数据分组,进行数据压缩处理(可选),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 4 种类型的客户:握手(handshake)协议、警告(alert)协议、改变密码规格(change cipher spec)协议和应用数据(application data)协议.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.

TLS 握手协议建立连接会话状态的密码学参数,该过程在 TLS 记录协议之上进行.当 TLS 协议的客户和服务器开始第 1 次通信时,首先需要协商协议版本,选择密码算法,相互进行认证(可选功能),并使用公钥密码技术生成共享秘密.

TLS 握手协议包括以下步骤:

- 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,使客户和服务器能够协商 premaster secret.
- 交换证书和密码学信息,使客户和服务器能够进行相互认证.
- 使用交换的随机值和 premaster secret 生成主秘密 master secret.
- 为记录协议提供安全参数.

TLS 握手流程如图 1 所示.

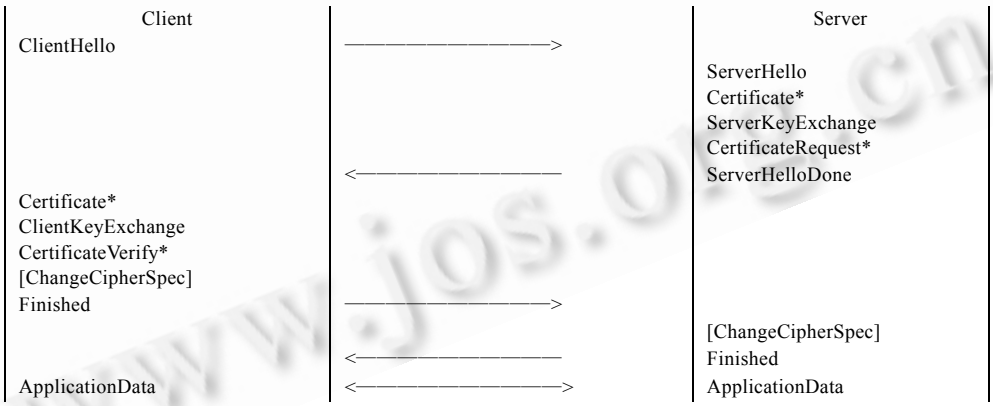

Fig.1 Message procedure of handshake

图 1 握手过程消息流程图

2 基于一次一密分析和改进 TLS

2.1 分 析

在 TLS 的加密过程中,先以 KeyExchange 产生原始密钥 pre_master_secret,然后利用随机数函数产生 master_secret=PRF(pre_master_secret,“master_secret”,ClientHello.random+ServerHello.random)[0..47],最后看当时所选用的算法及相关参数,使用 PRF 计算出长度足够的 Key_block=PRF(master_secret,“key_extensions”,ClientHello.random+ServerHelllo.random),从 Key_block 中依次取出所需的各种密钥:client_write_MAC_key,

server_write_MAC_key,client_write_key,server_write_key,再利用这些密钥对应用层数据进行加密和密码校验.

记录层协议不加解释地从高层接收非空的任意长度的数据块,并按照协议的规定对数据进行处理.记录层将高层协议数据分成小于 2^{14} 字节的 TLSPlaintext 记录.

```
struct {
    ContentType type;
    ProtocolVersion version;
    uint16 length;
    opaque fragment[TLSPlaintext.length];
} TLSPlaintext;
```

由上可以看出,在加密应用层的数据时,数据长度可以很大,而且这种情况在 Internet 上会经常发生,如在传输多媒体信息时,数据长度可以达到几百兆,这种加密方式在密码学中是不安全的,因为它可以为密码攻击者提供大量的密文信息(针对某一固定的密钥),利用这些密文信息和其他附加信息,密码攻击者可以破解密码,获得密钥.如在利用差分分析方法[3]攻击 DES 时,8 轮需要 2^{14} 个选择明文,10 轮、12 轮、14 轮和 16 轮 DES 分别需要 2^{24},2^{31},2^{39} 和 2^{47} 个选择明文.在利用线性分析方法[4]攻击 DES 时,攻击 8 轮、12 轮和 16 轮 DES 所需的已知明文数分别为 2^{21},2^{33} 和 2^{47} 个已知明文.同样,在攻击序列密码时,利用各种相关攻击[5]的方法,完全可以根据密文信息和其他附加信息,获得密钥.所以必须根据密码学一次一密的基本思想,对 TLS 的加密方式进行改进.

2.2 改 进

改进的出发点是定义加密的颗粒度,也即一次密钥只能加密多大长度的明文数据,当长度超过颗粒度时,密钥必须更新.而颗粒度只能在握手协议中协商,所以需要对 Hello 消息进行扩展.

Hello 消息描述如下:

```
Struct {
    Random          random;
    SessionID       session_id;
    CipherSuite     ciphersuites;
    Uint8           keyrefresh;
}   ClientHello
```

说明:keyrefresh 表示加密的颗粒度为 $2^{keyrefresh}$ 个字节.

协商了加密的颗粒度之后,必须计算出加密和鉴别所需的密钥.只需对 TLS 原有的计算方法作适当的修改就可以满足要求.

修改后的密钥计算过程如下:

```
master_secret=PRF(pre_master_secret,
                  “master_secret”,
                   ClientHello.random+ServerHello.random)
Key_block=PRF(master_secret,
                “key_extensions”,
                Seq_Num+ClientHello.random+ServerHelllo.random),
```

其中 Seq_Num 的取值依次为 $0,2^{keyrefresh},2\times2^{keyrefresh},3\times2^{keyrefresh},\ldots$

3 基于访问控制分析和改进 TLS

3.1 分 析

TLS 的一些缺陷并不是自身固有的,而是由于其所依赖的 PKI 造成的,应用 PKI 的目的是管理密钥,并通过

公钥算法实现用户身份验证.但在实际应用中,存在一个问题:如果用户数目很大,通过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哪一种类型人被允许做什么.

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,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.

3.2 改 进

传统的权限解决方法是利用访问控制列表,这种方法只能解决用户量小的系统,而且管理复杂,目前正探讨利用属性证书(attribute certificate)来解决权限管理,作为 PKI 技术的新扩展,属性证书[6]提供了全新的方法以解决细粒化的访问控制问题.在许多场合下采用基于角色属性的访问控制是真正可行的实现方案.属性证书可以应用在很多方面,如 VPN 的访问控制、WEB 页面的访问控制以及在线订阅服务的访问控制等领域.

改进后的 TLS 消息流程如图 2 所示.

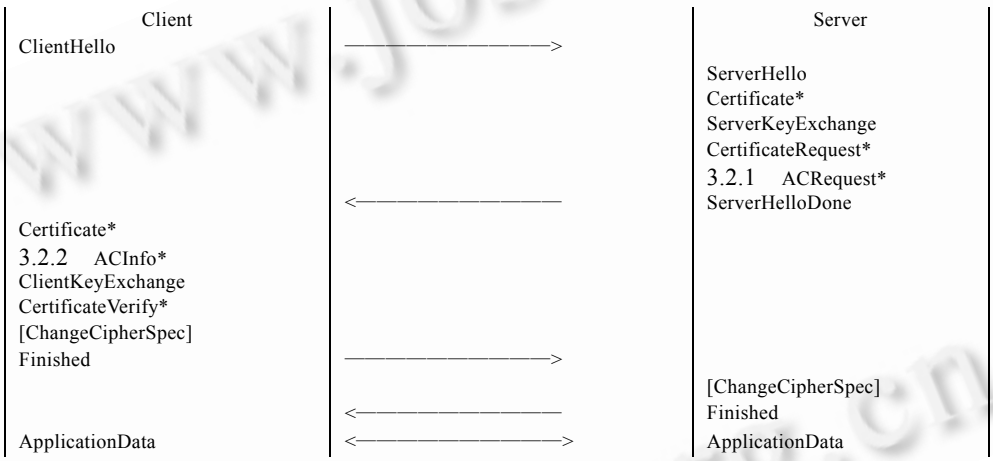

Fig.2 Message procedure of handshake

图 2 握手过程消息流程图

相关消息的描述如下:

acinfo::=[attributecert] [pkcerts]

pkcerts::=OCTETS

struct {opaque acinfo⟨1…2^24−1⟩} ACRequest

struct {opaque acinfo⟨1…2^24−1⟩} ACInfo

原来的 CertificateVerify 消息的内容为对 ClientHello,ServerHello,Certificate,ServerKeyExchange,CertififateRequest,ServerHelloDone,Certificate,ClientKeyExchange 的签名,则应改为 ClientHello,ServerHello,Certificate,ServerKeyExchange,CertififateRequest,ACRequest,ServerHelloDone,Certificate,ACInfo,ClientKeyExchange 的签名.在 Server 端发 Finished 消息之前应增加对属性证书的验证,由于属性证书是和身份证书相关联的,所以属性证书验证的前提是身份证书的验证,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,并且更重要的是确定用户身份是否与证书声明的拥有者身份一致.最后,应用程序检查属性证书中的内容,以确定是否允许此用户存取其所需的资源及服务.

4 基于双证书机制分析和改进 TLS

4.1 分 析

目前,随着应用环境的变化以及安全层次的提高,PKI 已得到进一步的发展,一个重要的发展就是由原先的单证书机制演变到双证书机制,所谓的双证书就是用户可以拥有两张证书:签名证书和加密证书,这样可以解决原来由于证书更新而引起的不安全间隙期.在 X.509 中,签名证书和加密证书的区别主要体现在扩展域 Keyusage.签名证书的 KeyUsage={Digital Signature},加密证书的 KeyUsage={Key Encipherment},所以在实际应用中,用签名证书识别身份,加密证书加密数据或交换密钥.

在 TLS 中,无论是身份识别还是密钥交换都采用同一个证书,如 server certificate 消息:

该消息表示服务器发送证书,在 server hello 消息之后立即被发送.证书的类型必须与所选择的 CipherSuite 中的密钥交换算法相匹配,一般情况下是 X.509v3 格式的证书,证书中要包含与密钥交换算法相匹配的密钥.而 server key exchange 消息:仅在服务器发送的 server certificate 消息中没有包含足够的信息使客户可以交换 premaster secret 的时候发送,为客户端协商 premaster secret 传递密码信息.所以必须根据双证书机制来改进 TLS,用签名证书识别用户的身份,用加密证书进行密钥交换.

4.2 改 进

首先改进 TLS 握手协议的消息流程,如图 3 所示.

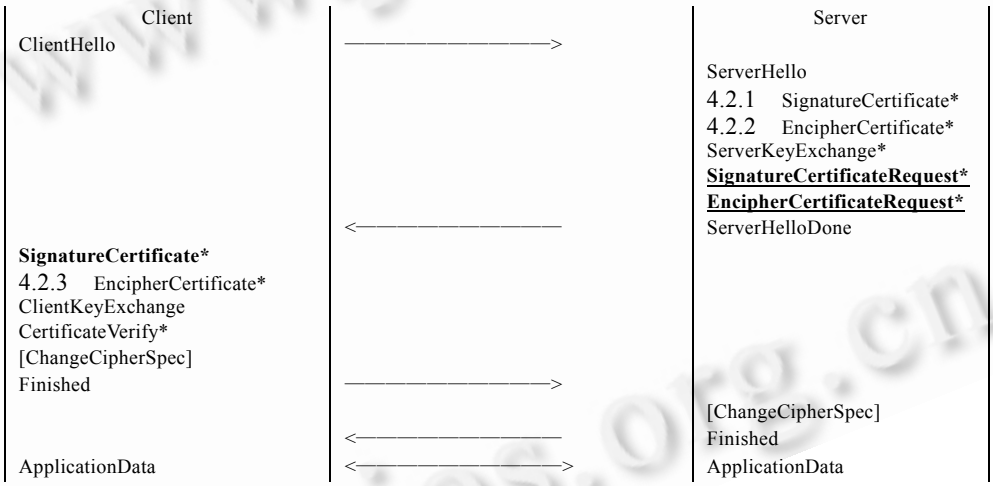

Fig.3 Message procedure of handshake

图 3 握手过程消息流程图

相关消息的描述如下:

SignatureCertificate EncipherCertificate::=sequences of certificate

SignatureCertificateRequest EncipherCertificateRequest::=sequences of trusted_authority

server key exchange:仅在服务器发送的 server Enciphercertificate 消息中没有包含足够的信息使客户可以交换 premaster secret 的时候发送,为客户端协商 premaster secret 传递密码信息.

CertificateVerify 消息的内容为对 ClientHello,ServerHello,SignatureCertificate,EncipherCertificate,ServerKeyExchange,SignatureCertifiFateRequest,EncipherCertifiFateRequest,ServerHelloDone,SignatureCertificate,EncipherCertificate,ClientKeyExchange 的签名.

5 结束语

TLS 的发展不能脱离 PKI 的发展,目前,无论是在学术研究还是实际应用中,PKI 还不成熟.属性证书和双证书正是这几年 PKI 研究最新的成果,本文主要是利用 PKI 的成果和密码学的思想对 TLS 作了部分改进.由于篇

幅有限,本文此处不对完整的改进协议加以描述.

References:

[1] Freier AO, Karlton P, Kocher PC. The SSL protocol version 3.0. 1996. http://home.netscape.com/eng/ssls/ssl-toc.html.

[2] Wagner D, Schneier B. Analysis of the SSL protocol. In: Countpane Labs., ed. Proceedings of the 2nd USENIX Workshop on Electronic Commerce. USENIX Press, 1996. 29~40.

[3] Biham E, Shamir A. Differential Cryptanalysis of the DES. New York: Springer-Verlag, 1993. 211~219.

[4] Matsui M. Linear cryptanalysis of DES cipher. In: Proceedings of the Eurocrypt'94. Berlin: Springer-Verlag, 1994. 109~117.

[5] Meier W, Staffelbach O. Fast correlation attacks on stream ciphers. In: Advances in Cryptology-EUROCRYPT'88. LNCS 330, Brelin: Springer-Verlag, 1989. 301~314.

全国第 7 届计算语言学联合学术会议(JSCL 2003)

征 文 通 知

中国中文信息学会、中国计算机学会、中国人工智能学会和北京市语言学会于 2003 年 8 月 8 日~11 日在哈尔滨市与哈尔滨工业大学联合举办“全国第 7 届计算语言学联合学术会议(JSCL 2003)”。

一、征文范围

(1) 计算语言学的理论基础：知识表示、语义学、语用学、语料库语言学、记忆模型、机器学习、知识获取和推理技术；

(2) 现代汉语的句法分析和语义分析：汉语分析的策略、句法分析和语义分析中的计算问题、汉语分析的展望；

(3) 汉语语料库技术及系统；

(4) 汉语人机接口技术及系统；

(5) 机器翻译技术、系统及评测方法；

(6) 话语和篇章的分析与生成：话语的心理学和语言学模型、篇章分析、话语生成；

(7) 自然语言处理的应用系统：汉语自动分词系统、智能检索系统、自动文摘系统、自动校对系统、文本自动分类系统、信息抽取、信息过滤、智能搜索引擎、文本挖掘、智能拼音汉字转换等；

(8) 计算语言学的资源研究及建设：树库、语法词典、词汇语义分类体系和语义词典、汉语分词词表、概念词典、知识库等；

(9) 服务于计算语言学的支撑环境和软件技术。

二、来稿要求

全文不超过 8000 字，每篇论文均应有中英文两种文字标题、作者、姓名、单位和不超过 200 字的摘要。来稿全文一式 3 份,作者请自留底稿。会议概不退稿。大会录用的论文将收入有出版书号的会议论文集。

三、重要日期

(1) 截稿日期：2003 年 4 月 1 日(以邮戳为准) 注：来稿请在首页上标明“JSCL 2003”。

(2) 录用通知发出日期：2003 年 5 月 1 日

(3) 作者提交的论文激光印刷版日期：2003 年 6 月 1 日(以到达日期为准)

四、联系方式

来稿邮寄地址：100084 清华大学计算机科学与技术系 陈群秀 收

联系电话：010–62781479