第29卷第3期 华中科技大学学报 Vol.29 No.3
2001年 3月 J.Huazhong Univ. of Sci & Tech. Mar. 2001

TCP/IP协议族的安全架构

陈晓苏 朱国胜 肖道举

(华中科技大学计算机科学与技术学院)

摘要: 给出了TCP/IP协议族的整体安全架构,讨论了网络层安全协议IPSec和传输层安全协议TLS,以实现在网络层和传输层提供加密和认证等安全服务.阐述了IPSec提供安全服务之前如何通过ISAKMP协议进行SA的协商以及TLS如何通过握手协议进行安全协商的问题.

关 键 词: TCP/IP协议族的安全架构;网络层安全协议;传输层安全协议;安全关联

中图分类号: TP393 **文献标识码**: A **文章编号**: 1000-8616(2001)03-0015-03

1 安全协议架构

TCP/IP协议是Internet运行的基础,其安全性问题很早就受到人们的关注.文献[1]中对TCP/IP协议族的安全问题进行了全面的分析,指出安全问题的关键在于TCP/IP的明文传输和缺乏强认证(基于IP地址及校验和的认证太弱).因此,加密(Encryption)和认证(Authentication)是防范攻击的必要手段.近年来,Internet工程任务组IETF在Internet安全性研究方面取得了重大进展,把加密和认证引入了TCP/IP协议族,形成了一系列安全协议.图1为TCP/IP协议族的安全架构(虚线框为安全协议).

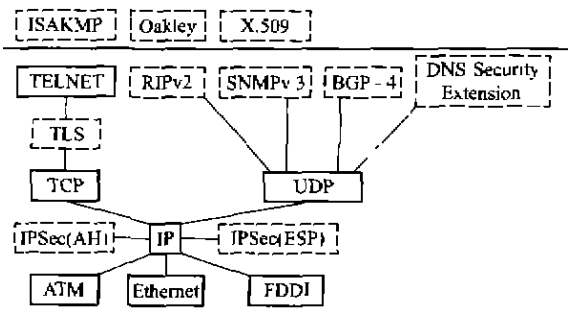

图1 TCP/IP协议族的安全架构

图1中IP层的安全协议IPSec由认证头AH(Authentication Header)和封装有效载荷ESP(Encapsulating Security Payload)两个协议组成,这两个协议在通信双方的IP层进行加密和认证,保证数据的完整性(Data Integrity)、数据源认证(Data Originality Authentication)和数据机密性(Data Confidentiality),关于IPSec的RFC是RFC2406.通常,IPSec协议的实现需要安全关联SA(Security Association)的支持,SA是通信双方协商的安全参数,如加密算法及密钥、认证算法及密钥、源地址及目的地址等.SA由ISAKMP/Oakley协议管理和维护.

传输层安全协议TLS(Transport Layer Security)是建立在安全套接字协议SSLP(Security Socket Layer Protocol)基础之上的一个协议,由TLS握手协议和TLS记录协议组成.TLS握手协议在客户和服务器双方进行保密通信前确定密钥、加密认证算法等安全参数;TLS记录协议在可靠的传输层(如TCP)之上提供加密认证等安全服务.

此外,网络的管理和控制对网络的安全运行也至关重要,DNS安全扩展、SNMPv3、RIPv2、BGP-4等是相应协议的安全扩展.

2 IPSec

基于加密技术,IPSec为IPv4和IPv6提供高效的安全服务,包括:存取控制、无连接完整性、数据源认证、数据机密性、抗重传和有限抗流量分析等.IPSec由AH和ESP两个协议组成,AH协议提供无连接完整性、数据源认证和可选的抗重传服务(在AH头中实现);ESP提供数据机密性和有限抗流量分析服务(在ESP头中实现),同时可选地提供无连接完整性、数据源认证和抗重传服

收稿日期: 2000-09-11.

作者简介: 陈晓苏(1953-),男,教授;武汉,华中科技大学计算机科学与技术学院(430074).

务(在ESP尾中实现).SA可在通信双方进行手工维护,当然更安全可靠的是由ISAKMP协议来自动维护.AH和ESP可单独使用,也可结合使用.这两个协议都具有两种工作模式:传输模式和隧道模式,其中传输模式保护IP上层包(如TCP报文);隧道模式保护整个IP包.

2.1 ISAKMP和SA的建立

ISAKMP把密钥管理、SA协商和协商双方的认证结合起来,为Internet上的通信提供所需的安全保障[2].必须指出,ISAKMP可以为各安全协议层(如TLS,RIPv2等)提供SA协商而不仅仅为IPSec服务,ISAKMP定义了建立、修改和删除SA的过程和包格式,ISAKMP属应用层协议,固定在UDP的500端口.ISAKMP消息包由固定的头和一个以上的载荷组成,载荷类型有:安全关联、标识、密钥、证书、签名和随机数等.SA的协商、证书的交换、协商双方的认证和密钥交换是通过包含各种载荷的ISAKMP消息的交换实现的.ISAKMP的协商过程分成两个阶段:第一阶段进行ISAKMP SA的协商,ISAKMP SA用于保护后续的ISAKMP会话的安全,在此阶段将得到一个共享会话密钥;第二阶段进行支持其他安全协议(如IPSec)的SA协商,这一阶段的消息交换将受到ISAKMP SA的保护.基本的ISAKMP消息的交换如图2所示.

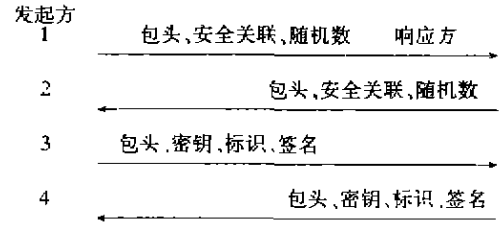

图2 基本的ISAKMP交换(发起方和响应方是ISAKMP Server进程)

第1个消息包中,发起方构造一个安全关联载荷,这是一个发往对方的SA建议,同时还发送随机数载荷,响应方将在第4个包中对之签名以认证响应者;第2个消息包中,响应方从SA建议中选择可接受的SA参数,同时也构造一个完成同样功能的随机数载荷;第3和第4个消息包中,双方相互交换密钥载荷、标识载荷和签名载荷,标识和签名将验证双方的身份,密钥交换建议使用Oakley密钥决定协议,该协议使用Diffie-Hellman(DH)密钥产生技术.双方通过传递DH公共部分而各自得到一个并没有在网络上传输的公共的会话密钥.

2.2 认证头AH(Authentication Header)

AH协议为IP数据报提供数据源认证以及数据完整性服务,重传保护是可选的,取决于相应的SA参数.其头格式如图3所示.

下一协议头类型	载荷长度	保留
安全参数索引(SPI 32 bit)		
序列号(SN 32 bit)		
认证数据(可变长度)		

图3 IP认证头(AH)格式

下一协议头类型表示AH头之后是什么,在传输模式下将是处于保护中的上层协议的值,比如TCP或UDP协议的值,在隧道模式下,将是值4或41,表示IPV4或IPV6.

载荷长度表示AH头本身的长度,其值为32 bit的字数减2.

安全参数索引SPI是一个32 bit的整数,它和目的地址唯一地确定了一个SA;序列号SN是用于检测重传的计数值;认证数据是对IP数据报进行安全哈希运算而得到的消息认证码MAC,用于完整性检查和数据源认证,其计算表达式为:$HMAC(K, M) = H(K \oplus P1, H(K \oplus P2, M))$,其中,K为双方共同拥有的私钥;M为消息报文(如IP数据报);P1和P2为选定的字符串常量;H为哈希函数(如MD5或SHA).在传输模式和隧道模式下,M有不同的作用范围,如图4(以IPv4为例)所示.

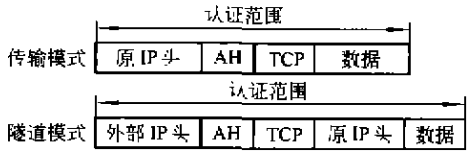

图4 AH协议传输模式和隧道模式的认证计算范围

应注意,可变域(如IP头中的存活时间和AH头中的认证数据本身)在计算时作0处理.

2.3 封装有效载荷ESP

ESP(Encapsulating Security Payload)通过加密来保证数据机密性、数据源认证、数据完整性,重传保护是可选的,取决于相应的SA参数.其头格式如图5所示.

安全参数索引(SPI 32 bit)	
序列号(SN 32 bit)	
载荷(可变长度)	
	填充数据
	填充长度 | 下一协议类型
认证数据(可变长度)	

图5 封装有效载荷(ESP)头尾格式

安全参数索引SPI、序列号SN和认证数据所起的作用和AH头格式中的各相关部分相同;载

荷是被加密后的数据报；由于某些加密算法要求固定长度的块，因此需要填充数据，填充长度用于指示所填充的数据字节数；下一协议头类型则指出加密前的载荷是什么类型的包．传输模式和隧道模式下的加密及认证范围如图 6（以 IPv4 为例）所示．

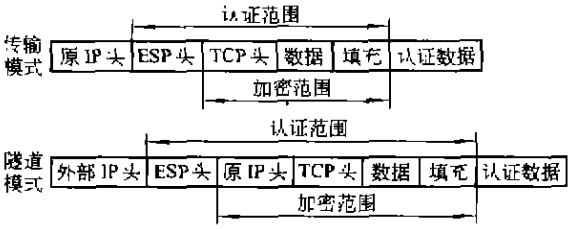

图 6　ESP 协议转输模式和隧道模式的加密和认证范围

应该注意的是，认证数据的计算和 AH 的认证数据计算不同之处是 ESP 对外部的 IP 头不进行认证．

3　传输层安全协议 TLS

3.1　TLS 记录协议

TLS 记录协议位于可靠的传输层如 TCP 之上，它根据握手协议协商的参数，对上层交付的数据进行分段、压缩、计算 MAC、加密，然后发送出去，接受方则按相反的次序进行解密、验证 MAC、解压缩和重组．TLS 记录协议把数据封装在各种记录里，记录类型有：分段记录、压缩记录、加密记录等．以加密记录为例，用类 C 语言表示的 TLS 加密记录定义如下：

```
struct {
  ContentType type;
  ProtocolVersion version;
  uint16 length;
  select (CipherSpec.cipher_type) {
    case stream: GenericStreamCipher;
    case block: GenericBlockCipher;
  } fragment;
} TLSCiphertext;
```

其中：type 域说明加密前的数据类型，指出加密前的记录是 TLS 压缩记录还是 TLS 分段记录；version 为版本；length 为 fragment 的长度；fragment 是加密后的数据．TLS 将处理后的数据以记录的形式向下层传递．

3.2　TLS 握手协议

TLS 握手协议完成类似 ISAKMP 的功能，当客户通过 TLS 协议和服务器进行通信时，执行 TLS 握手协议协商安全参数、相互认证对方、产生主密钥 MK[3]．典型的 TLS 握手过程如图 7 所示．

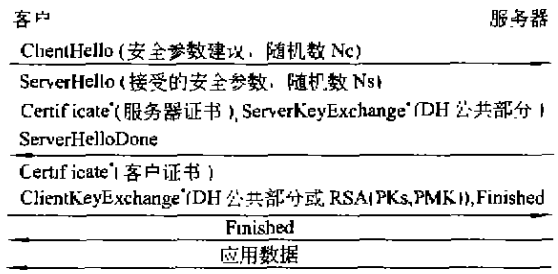

图 7　TLS 握手协议的消息交换（带 * 为可选）

第一步，客户发送包含安全参数建议和随机数 Nc 的 ClientHello 消息；第二步，服务器回应包含接受的安全参数和随机数 Ns 的 ServerHello 消息，并在要求服务器认证时，发送自己的证书．当采用 DH 技术时，服务器发送包含 DH 公共部分的 ServerKeyExchange 消息；第三步，当要求客户认证时，客户首先发送自己的证书，并发送 DH 公共部分，然后客户和服务器同时用 DH 公共部分和自己的私有部分计算出预主密钥 PMK．为增强安全性，PMK 并不用于数据传输而是由 Nc、Ns 和 PMK 导出主密钥 MK．最后，相互发送 Finished 消息后就可以开始应用数据的传输．Finished 消息包含根据 MK 和过去消息计算的安全哈希值，收到的一方对它进行验证，以保证整个过程是成功的．

在 TCP/IP 协议族的安全问题中，网络层和传输层的安全处于中心地位．本文论述了引入加密和认证机制的网络层的安全协议 IPSec 和传输层的安全协议 TLS．IPSec 的特点是它的透明性，用 IPSec 来保护通信无需修改应用程序，而用 TLS 则必须对应用程序进行修改；二者在对应用数据进行保护前都要进行安全参数的协商．

参　考　文　献

[1] Bellvoin S. Security Problems in the TCP/IP Protocol Suite. Computer Communication Reviews, 1989, 4: 32～48

[2] Refik M. Internet Security Architecture. Computer Networks, 1999, 31: 787～804

[3] 韦　卫，王德杰，张　英等．基于 SSL 的安全 WWW 系统的研究与实现．计算机研究与发展，1999，5：619～624

（下转第 21 页）

标准.京京工作室译.北京：机械工业出版社，2000.

参 考 文 献

[1] Doraswamy N, Harkins D. IPSec：新一代因特网安全

A Simplified Implementation of IP Security

Chen Xiaosu Song Xiuyao Xiao Daoju

Abstract: A simplified implementation of IP Security is proposed. The tunnel operation mode and the Encapsulating Security Payload protocol are adopted without weakening IPSec security. An implementation model is designed and the functionality of each part is explained. The pack/unpack technology is expounded.

Key words: IPSec; Mini-IPSec; pack/unpack technology; security tunnel

Chen Xiaosu Prof.; College of Computer Sci. & Tech., HUST, Wuhan 430074, China.

(上接第 17 页)

A Security Architecture of TCP/IP Protocol Suite

Chen Xiaosu Zhu Guosheng Xiao Daoju

Abstract: The Security architecture of TCP/IP protocol suite is given. The internet protocol security IPSec and the transport layer security TLS are studied. The encryption and authentication services at the network layer and transport layer respectively are provided. ISAKMP is introduced to carry through the association of SAs by IPSec and TLS handshake protocol is presented to carry through the association of security parameters by TLS.

Key words: security architecture of TCP/IP protocol suite; IPSec; TLS; security association

Chen Xiaosu Prof.; College of Computer Sci. & Tech., HUST, Wuhan 430074, China.