IPSec网络安全构架

同济大学计算机科学与工程系　徐竹冰

摘要：IPSec是网络层的安全协议标准，它提供了IP层上的多种安全服务。本文对IPSec的工作原理、工作模式，及其主要的两个安全协议进行了分析。

关键词：IPSec　安全连接　加密　认证

引言

IPSec(IP Security)是IETF委员会制定的网络层安全协议标准，它提供了一个开放系统的安全框架，向IPv4|Ipv6提供互操作的、高质量的、基于密码的安全性，其服务包括保密、认证、完整性控制和反重发保护，它们主要由下面两个协议来实现：AH(Authentication Header，认证头)协议、ESP(Encapsulating Security Payload，封装安全负载)协议。IPSec根据系统所选择的安全协议提供IP层上的安全服务，决定服务所需的算法和密钥，并在主机之间、安全网关之间或主机与安全网关之间建立起一条或多条安全连接。

工作原理

IPSec的工作原理如图1所示，当IP模块收到一个IP分组时，通过查询安全策略数据库SPD(Security Policy Database)，以决定对收到的这个IP数据分组的处理：丢弃、IPSec转发或IPSec处理，通过查询安全连接数据库SAD(Security Association Database)，以获取安全连接所需的参数。

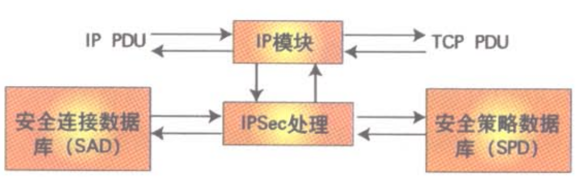

图 1　IPSec工作原理图

安全连接

安全连接(SA)是与一个或一组网络通信相关的安全信息，是一种提供安全服务的简单“连接”，通过AH或ESP协议来实现，但不是同时使用AH和ESP协议。如果对一个报文同时提供AH和ESP保护，那就需要建立起两条(或更多条)安全连接，例如，在两个主机之间或安全网关之间的双向通信中，需要两条安全连接，每个方向一条。

安全连接的参数包括：

(1)顺序号计数器：一个用来产生AH或ESP协议头中顺序号的32bit的值。

(2)顺序号计数器溢出标志：一个表示顺序号计数器溢出时是否产生一个审核事件并阻止安全连接上剩余报文继续传输的标志。

(3)反重发窗口：一个确定内部AH或ESP报文是否为重传报文的32bit计数器。

(4)AH认证算法及其使用的密钥。

(5)ESP加密算法、算法模式及其使用的密钥。

(6)ESP认证算法及其使用的密钥。

(7)安全连接的生命期。

(8)IPSec协议模式：隧道、传输。

(9)路径最大传输单元。

安全连接的类型有两种：传输模式和隧道模式。如图2所示。

(1)传输模式的安全连接要求必须建立在两台主机之间。在IPv4中，传输模式的安全协议头位于IP报头和可选部分之后，上层协议(如TCP或UDP)之前。在IPv6中，安全协议头出现在基本首部和扩展首部之后，目的端可选部分之前或之后，上层协议之前。对于ESP，传输模式的安全连接仅为上层协议提供安全服务，不为IP的基本首

部和扩展首部提供安全服务；对于AH，这种保护也提供给部分被选择的基本首部、扩展首部和可选部(包括IPv4首部，IPv6端对端扩展首部，IPv6目的端扩展首部)。

(2)隧道模式的安全连接实质上是一种应用在IP隧道上的安全连接。在隧道模式的安全连接中，有一个外层IP首部指定IPSec处理的目的端，内层IP首部指定IP包的最终目的端。安全协议头位于外层IP首部之后，内层IP首部之前。如果在隧道模式中使用AH协议，部分外层IP首部和所有的隧道IP包(包括内层IP首部和上层协议)可以受到保护；如果使用ESP协议，仅仅只有隧道IP包受到保护。

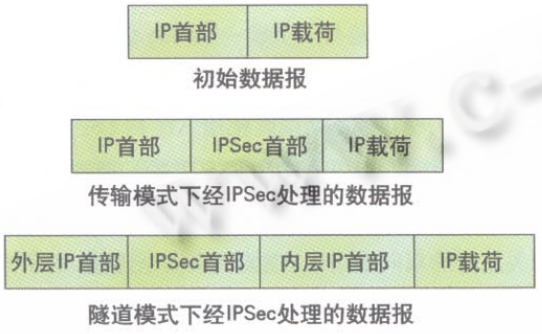

图 2 安全连接的模式

当安全连接的任意一端为安全网关时，安全连接必须是隧道模式。两台主机间也可以建立隧道模式安全连接。这种要求任意一条包括安全网关的安全连接必须采用隧道模式是为了避免一些潜在的问题，如IPSec包在分片和重组时可能遇到的问题，以及在安全网关后存在多条通往同一目的主机的路径引起的问题等。

在单独的安全连接上传输的IP报文只能由一个安全协议提供保护：AH或ESP。有时一种安全策略需要为特定的报文提供一组服务，它不能由单个的安全连接来实现，在这种情况下，必须使用多条安全连接来实现所需的安全策略。所谓的“安全连接束”就是指一系列为实现所需安全策略的安全连接，这些安全连接的顺序由安全策略来决定。组成安全连接的安全连接束可以终止于不同的端点。例如，一条安全连接可以建立在一个可移动主机和一个安全网关之间，另一条安全连接可以连接到安全网关后的一台主机上。

安全连接可以通过两种方式来组成安全连接束：传输邻接和嵌套隧道。

(1)传输邻接指不通过隧道，在相同的IP报文上提供一个以上的安全协议。这种组合AH和ESP的方法只允许在一个层次上进行。

(2)嵌套隧道指应用IP隧道实现多层安全协议。由于每个隧道能起始或终止于路径不同的IPSec结点，这种方法允许多嵌套层次。

传输邻接和嵌套隧道这两种方式也可以组合起来使用，一个安全连接束可以包括一个隧道模式安全连接和一个或两个传输模式安全连接。传输模式安全连接的安全协议顺序只有一种，因为AH协议提供IP载荷和部分IP首部的保护，而ESP只提供对IP载荷的保护，所以AH协议头必须出现在ESP协议头之前。

AH和ESP协议

1. 协议头格式

AH提供的服务包括：完整性控制、数据源认证、数据分组的反重发保护。它的协议头格式如图3所示。

图 3 AH协议头格式

(1)下一扩展头：标识AH头后的负载类型。

(2)负载长度：以32位字长为单位，其值为AH头长度减2。当认证数据为标准的96位时，该值为4。

(3)保留：留作将来使用，必须置为0。

(4)安全参数索引(SPI)：与目的端IP地址及安全协议(AH)一起唯一表示该报文的安全连接。它通常在建立安全连接的基础上由目的端系统来选择。

(5)顺序号：用于反重发服务，但无论接收方是否选择该服务，它都照常记数。

(6)认证数据：含有该报文的完整性检查值(ICV)。长度可变，但必须是32的倍数。该域可能含有填充数据，以确保整个AH协议头长度为32的整数倍(IPv4)或64的整数倍(IPv6)。

ESP提供的服务包括：加密、完整性控制、数据源认证、数据分组的反重发保护。协议头格式如图4所示。

图 4 ESP 协议头格式

(1)安全参数索引(SPI)、顺序号的含义与AH中的相同。

(2)负载数据：包含下一扩展头中描述的数据。

(3)填充域：该域是可选的，包含0-255个字节，任何算法必须支持填充数据的产生和清除。

(4)填充长度：指示填充域中填充的字节数。

(5)下一扩展头：指示负载数据域中所含数据的类型，如IPv6中的扩展首部或对上层协议的标识。

(6)认证数据：该域是可选的，只有在建立安全连接时选择了认证服务才有，它包含对ESP报文中除去认证数据后计算的一个完整性检查值(ICV)，其长度由认证函数决定。

2. 算法

AH和ESP计算ICV的认证算法由安全连接决定。对于端到端通信，有基于对称加密算法(如DES)或单向哈希函数(如MD5，SHA-1)的消息认证代码。对于多目广播通信，可以采用与非对称签名算法相结合的单向哈希算法。所有的AH实现必须支持哈希消息认证码HMAC (Hashed Message Authentication Code)的不同算法，如HMAC-MD5、HMAC-SHA-1。

ESP中的加密算法由安全连接决定，与对称加密算法一起使用。由于IP报文可能不是按顺序到达，所以每个报文必须携带一些信息以使接收端为解密建立保密同步。这些信息可以放在负载数据域中，如初始向量(Initialization Vector)，也可以从报头中提取。由于ESP中的信息是明文的，ESP的加密算法可以采用块或流模式。所有的ESP实现必须支持DES in CBC mode、HMAC-MD5、HMAC-SHA-1、NULL认证算法、NULL加密算法。

3. 输出报文处理

AH的报文输出处理过程：

(1)查找安全连接。

(2)产生顺序号。发送方计数器在安全连接建立时初始化为0，当进行输出报文处理时自动递增，并把新值加入到顺序号域中。如果选择了反重发服务(缺省)，发送端在插入新值前需要检查并确保计数器没有循环，如果计数器已经循环，发送端将建立一个新的安全连接和密钥。如果没有选择反重发服务，发送端不需要监测并重置计数器，当计数器达到最大值时，将重新返回到0。

(3)计算完整性检查值。AH完整性检查值的计算是针对IP报头、AH头、上层协议数据进行的，计算前主要包括两方面的处理：

①处理可变域。如果某一域中的值在传输过程中被改变了，则将该域的值置0；如果域的值是可变的，但可以被接收端预测，则将该值插入到域中。在计算时，认证数据域中的值将置0。置0的方法保证了对齐，也保证了域长度在传输过程中不被改变。

②填充。包括认证数据填充和报文填充。认证数据填充是为了确保AH头长度为32的倍数(IPv4)或64的倍数(IPv6)。对于一些认证算法，进行完整性检查值计算的字节流必须为算法所定义的块长度的整数倍，如果包括AH头在内的IP报文不符合该要求，那么必须在报文的末尾加上填充数据，填充数据必须为0，且不随报文一起发送。

(4)分片。在传输模式中，分片处理在AH处理之后进行，经过AH处理的IP报文可以由路由器来分片，但在接收端必须在AH处理前进行重组。在隧道模式中，可以对已经分片的IP报文进行AH处理。

ESP的报文输出处理过程与AH大致相同，主要有以下两点区别：

①在查找安全连接之后，需要进行报文加密。发送方把上层协议信息(传输模式)或整个IP报文(隧道模式)封装到ESP负载域中，然后添加必要的填充信息，最后用安全连接中指定的密钥、加密算法、算法模式以及保密同步数据对结果数据(包括负载数据、填充、填充长度、下一扩展头)进行加密。如果选择了认证服务，那么必须在认证之前进行加密，而且加密对象不能包括认证数据域。这种顺序加快了接收端检测和拒收重发报文或伪报文的速度，从而减少了服务拒绝攻击的影响。同时它也允许接收端对报文进行并行处理，也就是说，解密和认证可以同时进行。

②完整性检查值计算的对象有所不同。在ESP中，ICV计算的对象是整个ESP报文中除了认证数据以外的

部分。

4. 输入报文处理

AH的报文输入处理过程:

(1)重组。如果需要的话,重组将在AH处理之前进行。

(2)查找安全连接。在收到包含AH协议头的报文之后,接收方根据目的端IP地址、安全协议(AH)和SPI确定相应的安全连接。如果无有效的安全连接存在,接收方丢弃该报文。

(3)顺序号检查。当安全连接建立时,接收方报文计数器必须初始化为0,在一个安全连接生命期内,对于每一个到达的报文必须确保其顺序号没有重复,重复的报文将通过使用滑动接收窗口被丢弃。如果接收端没有选择反重发服务,就不需要对输入报文进行该项检查。

(4)完整性检查值验证。接收方用指定的认证算法,对报文的相应域计算ICV,并与报文的认证数据域中的ICV进行比较,如果不一致,则丢弃该报文。

ESP的报文输入处理过程比AH多一个报文解密过程。接收方使用安全连接中指定的密钥、加密算法、算法模式以及保密同步数据对负载数据、填充、填充长度、下一扩展头进行解密,然后用加密算法中指定的方法处理填充数据,最后重建初始IP报文,对于传输模式,从ESP负载域中提取IP报头和初始上层协议信息,对于隧道模式,从ESP负载域中提取隧道IP头和整个IP报文。如果选择了认证服务,ICV验证和解密可以串行或并行地进行。如果串行执行,将先进行ICV验证;如果并行执行,那么在对解密报文进行进一步处理前必须完成ICV验证。

小结

IPSec提供了网络层IP的安全机制,大大加强了Internet上信息传输的安全性,对于构建虚拟专用网络(VNP)以及远程用户通过拨号访问专用网络具有特殊的意义。但是,在使安全性能提高的同时,它也增加了系统开销,所以在实际应用中应当考虑从硬件级实现其各种算法。

Internet上的安全是相对的,不安全是绝对的。任何安全措施都无法保证网上信息传输的绝对安全。尽管IPSec提供了多种安全服务,它还是无法防止所有的安全攻击,如传输分析等。因此,更有效、更全面的安全技术有待今后的进一步研究。■

参考文献

1 R.Atkinson,Security Architecture for the Internet Protocol,RFC 2401,1998.11

2 R.Atkinson,IP Authentication Header,RFC 2402,1998.11

3 R.Atkinson,IP Encapsulating Security Payload,RFC 2406,1998.11

4 用TCP/IP进行网际互连. 电子工业出版社. 1998.4