基于 IPSec 的虚拟专用网技术及其在 Linux 上的实现*)

IPSec based VPN Technology and its Implementation on Linux

吴亚南　何　涛　刘　颖　杨寿保

(中国科技大学计算机科学技术系　合肥230026)

Abstract　IPSec provides the functions of encryption and authentication at the layer of as low as IP, therefore, it is very nature to employ it in the field of VPN(Virtual Private Network). This is also its most valuable application. This paper introduces some of the basic terminologies of IPSec and Virtual Private Network first, and then discusses IPSec based VPN implementation under Linux.

Keywords　IPSec, Virtual private network, Secure channel

1. 前言

随着 Internet 的不断发展，其方便快捷的特点愈受重视，很多大公司和政府部门或民间组织都用它来传输数据。然而在 Internet 上，数据随时可能会被不怀好意的网络入侵者窃取或修改，因此，数据在传输过程中必须被加密，接收方和发送方通过一个虚拟的安全隧道来传输信息，这就是虚拟专用网技术。如果是在 TCP 或 UDP 层加密，那么通过截取 IP 层的数据同样可以获得机密信息，在 IP 层使用加密和认证就非常安全了，这就是 IPSec(IP 安全体系结构)技术。目前利用 IPSec 来实现 VPN(虚拟专用网)已经成为一种发展趋势[9]。

2. IP 协议的安全体系结构

IPv4的包本身没有提供任何安全保护，黑客可以通过信息包探测、IP 电子欺骗、连接截获、重播攻击(replay，是一种不断发送相同序列号的包使系统崩溃的攻击方法)等方法来进行攻击和破坏[5]。因此，我们收到的数据包存在着以下危险：并非来自合法的发送者；数据在传输过程中被人修改；数据内容已被人窃取(想想如果是军事机密等重要信息的话，这是致命的)。IPSec 的目的就是为了实现数据传输的完整性(源地址验证和保证数据没有被修改)和机密性(没有被人看过)以及提供一定程度的对 replay 攻击的保护。IPSec 可用它为 IP 及其上层协议(TCP 和 UDP 等)提供安全保护。

RFC2401规定了 IPSec 的基本结构，它利用认证头标(AH)和封装化安全净荷(ESP，Encapsulate Secure Payload)来实现数据传送的认证和加密[1]。前者用来实现数据的完整性[2]，后者用来实现数据的机密性[3]。同时对数据的传输规定了两种模式：传送模式和通道模式。在传送模式中，IP 头与上层协议头之间嵌入一个新的 IPSec 头(AH 或 ESP)；在通道模式中，要保护的整个 IP 包都封装到另一个 IP 数据包里，同时在外部与内部 IP 头之间嵌入一个新的 IPSec 头。两种 IPSec 头都可以同时以传送模式和通道模式工作，图1说明了分别在两种模式下的 IP 包。

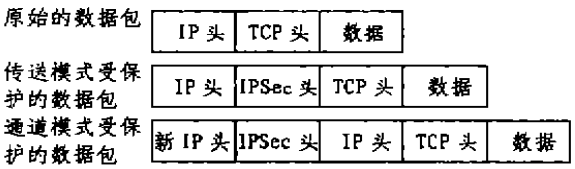

图1　处于传送和通道模式下的受 IPSec 保护的数据包

IPSec 由四大组件组成，即因特网密钥交换进程、IPSec 进程本身、安全联盟数据库和安全策略数据库[4]。

IPSec 中有两个重要的数据库，分别是安全联盟数据库 SAD(Secure Alliance Database)和安全策略数据库 SPD(Secure Policy Database)。SAD 中的每一个元组是一个安全联盟 SA，它是构成 IPSec 的基础，是两个通信实体经协商建立起来的一种协定，它决定了用来保护数据包安全的 IPSec 协议、转码方式、密钥以及密钥的有效存在时间等。SPD 中的每一个元组是一条策略，策略是指应用于数据包的安全服务以及如何对数据包进行处理，是人机之间的安全接口，包括策略定义、表示、管理以及策略与 IPSec 系统各组件间的交

*)本文受国家863项目863-317-01-08-99"IPv6示范系统"课题支持。吴亚南　硕士生，主要研究方向为下一代因特网的网络安全。何　涛　硕士生，主要研究方向为网络安全和密码学。杨寿保　教授，主要研究方向为计算机网络与信息安全。

互[5]。这两个数据库联合起来使用，对于发送方，每个SPD的元组都有指针指向相关的SAD的元组。如果一个SPD的元组没有指向适合发送包的SA，那么将会创建新的SA或SA束，并将SPD的元组和新的SA元组链接起来。对于接收方，通过包头信息包含的IP目的地址、IP安全协议类型(AH或ESP)和SPI(安全参数索引)在SAD中查找对应的SA。SA中其他字段为序列号、序列号溢出标志、Anti-replay窗口、AH认证算法和密钥、ESP加密算法和密钥及初始化矩阵、ESP认证算法及密钥等等。

因特网密钥交换(IKE，Internet Key Exchange)是IPSec最为重要的部分，在用IPSec保护一个IP包之前，必须先建立一个SA，IKE用于动态建立SA[7]。IKE代表IPSec对SA进行协商，并对SAD数据库进行填充。RFC2409所描述的IKE是一个混合型的协议，它建立在由Internet安全联盟和密钥管理协议(ISAKMP)定义的一个框架上，见RFC2408[4]。IKE使用了两个阶段的ISAKMP。第一阶段建立IKE安全联盟，第二阶段利用这个既定的安全联盟，为IPSec协商具体的安全联盟。

IPSec进程本身就是用来实现整个IPSec的守护进程，用户可以通过和这个进程打交道来管理自己的安全策略，实现适合自己需要的网络安全。当然，每个开发组织的源代码不一样，用户管理的界面和方式就不一样，但是它们都必须遵守RFC的规范，最终的目的都应该是差不多的。通常IPSec的源代码是嵌入到内核IP层源代码中的，也有人提出其层次在IP之上或TCP之下，两种方式都可以[8]。

3. 虚拟专用网VPN

虚拟专用网(VPN)是专用网的扩展，通信两端之间通过的是公用传输介质如Internet。VPN允许我们在两台计算机之间通过公共传输介质通信，就好像是自己的端到端的专用网一样。为了模拟端到端的专用网，数据必须被加上一个路由信息头，以便能够在Internet上找到正确的路径；同时为了数据的安全，数据包在传输过程中必须被加密[3]。图2说明了VPN的逻辑概念，VPN连接使用户可以在家工作或者在出差的旅途中利用公用介质如Internet来和公司总部的机器连接。从用户的角度来看，VPN是一个VPN的客户端与服务器端的端到端的连接，Internet等公共介质的网络结构是无关紧要的，因为从逻辑上看，数据是在专用网上传输。VPN也可以使公司在地域上分割的各个分部之间通过Internet传输信息，信息必须在一个安全的通道中传播，从逻辑上看就像是一个WAN上的专用网。

VPN的一个重要的特征就是安全性，通过VPN通信的两台主机必须通过一个安全的通道(tunnel)。这个tunnel是逻辑上的，并不真正存在，因此通过数据的加密和认证使得数据包即使被截获也不容易破译。在如何实现的问题上，以前的VPN很多采用SSL等方法对数据进行加密，但其缺点是配置安全策略不够灵活，另外，需要在高层协议上开发大量的代码，唯一的优点就是能够对DOS(服务拒绝)攻击提供较好的防御[9]。

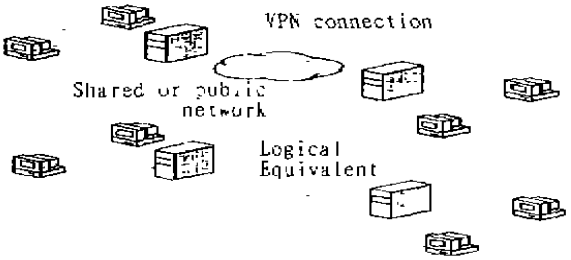

图2 VPN的逻辑概念图

4. 基于IPSec的虚拟专用网

当IPSec用于路由器时，就可以建立虚拟专用网[6]，在路由器连接内部网络的一端，如图2所示，是一个受保护的网络，另一端则是不安全的公共网络。两个这样的路由器建立起一个安全通道，通信就可以通过这个通道从一个本地的保护子网发送到一个远程的保护子网，这样就形成了一个虚拟专用网VPN。

在这个VPN中，每一个具有IPSec的路由器都是一个网络聚合点，试图对VPN进行通信分析将会失败。目的是VPN的所有通信都经过路由器上的SA来定义加密或认证的算法和密钥等参数，即从VPN的一个路由器出来的数据包只要符合安全策略，就会用相应的SA来加密或认证(加上AH或ESP报头)。整个安全传输过程由IKE控制、密钥自动生成、保护子网内的用户根本不需要考虑安全，所有的加密和解密由两端的路由器全权代理。

我们来看看数据包的处理过程，先看看数据包的外出处理：

(1)源主机TCP层通过调用ip_output()函数，调用IP层，令其发送一个数据包给路由器；

(2)路由器针对目的主机的数据包，查询策略引擎，根据安全策略强制加上AH或ESP头；

(3)IKE处理，对没有SA的安全策略建立新的SA；

(4)SA处理，增加序列号字段；

(5)通道模式处理，通常VPN用的是通道模式，因此加上一个额外的IP头；

(6)路由器发送这个安全的数据包。

接收方的处理过程：

(1)另一端的路由器收到这个包,剥去额外的IP头,并利用数据包的AH或ESP头调用IPSec层;

(2)IPSec层从AH或ESP头摘录出SPI,从IP头中选出源和目的地址及协议;

(3)IPSec层用以上的参数从SAD中取出所需的SA,如果没找到,就丢弃这个包;

(4)SAD返回SA,IPSec将会根据AH和ESP定义的规则对这个包进行处理;

(5)验证和这个包对应的策略,进而决定IPSec处理的应用是否正确,策略是通过SA中的指针获得或利用选择符查询SPD得来;

(6)如果验证正确,那么解密并把这个包转发到真正的目的主机。

5. VPN在Linux上的实现

我们实现的基于IPSec的VPN选用Linux操作系统作为两端的路由器,其结构如图2所示,这是一个典型的VPN结构。两边的路由器定义了相同的安全策略,也就是说,两端的通信都遵守相同的安全规则,例如都使用HMAC-MD5算法对WWW服务进行验证,都使用TRI-DES算法对telnet进行加密等等。IPSec的四大部分都在作为路由器的Linux机器上。

所有的源代码都编译到内核中,嵌入到IP层,与用户打交道的是可执行的程序ipsec,放在/usr/local/sbin目录下,用户通过它来使通信启动IPSec。同时通过/etc/ipsec.conf和/etc/ipsec.secrets来配置安全参数。系统在启动的时候有一个IPSecd的守护进程负责对通信进行加密和解密,并将数据传入到网络层。如果想对我们的源代码做深入的了解,请与作者联系。

两端的路由器的IP地址分别是202.38.64.185和202.38.75.75,我们的测试方案是从64.185内的主机host1和75.75内的主机host2的ftp通信,host1和host2有相应的域名解析,分别对应各自内部的IP地址。公共网络是校园上的Internet网,如图3所示。

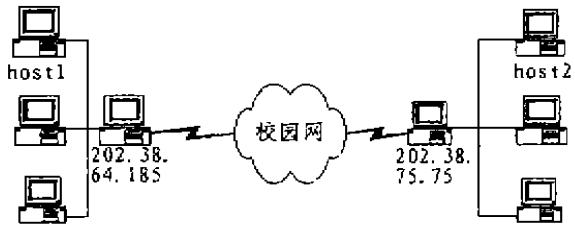

图3 基于IPSec的VPN在Linux上的实现环境

经过测试表明,从host1到host2的IP包全部被封装了一个额外的IP头,所有的上层协议都是经过加密的乱码,无法分析其内容,黑客获得的唯一信息就是这个包是64.185和75.75之间的通信(ESP应用TRI-DES算法)。为了比较应用IPSec后的系统效率下降程度,我们的测试方案是在两台机器之间用ftp传输大量的数据,应用TRI-DES的结果使得网络吞吐量下降了25%左右,这是由于在路由器上所做的加密和解密过程都需要耗费一定的时间。

我们在Linux上实现的基于IPSec的VPN有以下优点:

(1)在IP层增加AH或ESP头实现网络安全使得通信安全可靠;

(2)IKE协议可以自动产生需要的SA,并且SA的生存期非常短,使得破译更加困难;

(3)定义安全策略方便灵活,只需要在配置文件里进行编辑,就可以实现安全策略,例如如果一种算法被破解,立刻换另一种算法(目前AH支持HAMC-MD5,HAMC-SHA1;ESP支持DES-CBC,TRI-DES-CBC,BLOWFISH-CBC,CAST128-CBC)。

关于使用IPSec使得网络吞吐量明显下降的问题,如果加密解密纯粹由软件来实现的话,这是不可避免的。因此,可以用硬件来实现IPSec中的加密解密过程,即在通信两端的网卡上内置专用的加密芯片,所有的加密和解密的操作都由这块芯片来执行,这样就大大减少了对CPU的占用,从而提高网络的吞吐量。这样的网卡已经可以买到。

小结 IPSec的提出使得VPN有了更好的解决方案。在网络层就进行安全服务,使得密钥协商的开销被大大削减了,因为多种传送协议和应用程序可共享由网络层提供的密钥管理结构(IKE)。其次,假如网络安全服务在较低层实现,那么需要改动的应用程序就要少得多。IPSec是目前唯一一种能为任何形式的Internet通信提供安全保护的协议,因此,可以预见,未来的VPN实现方案将会更多地利用IPSec。如果加密解密纯粹由软件来实现的话,使用IPSec会使得网络吞吐量下降,这个问题可以通过使用加密解密硬件来实现。

参考文献

1 Kent S. RFC 2401 Security Architecture for the Internet Protocol. Nov. 1998
2 Kent S. RFC 2402 IP Authentication Header. Nov. 1998
3 Kent S. RFC 2406 IP Encapsulating Security Payload (ESP). Nov. 1998
4 Maughan D, Schertler M, Schneider M, Turner J RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP). Nov. 1998
5 Gai S. Internetworking Ipv6 with Cisco Routers. 机械工业出版社
6 Available at: http://www netbsd org/Documentation/network/ipsec/
7 Harkins D, Carrel D. RFC 2409 The Internet Key Exchange (IKE). Nov. 1998
8 Doraswamy N, Harkins D. IPSec: the new security standard for the Internet, Intranets, and virtual private networds. Prentice Hall PTR
9 Available at: http://www. firstvpn. com/papers/ms/master. zip