朱长安 刘嘉勇 刘 军 (成都四川大学信息安全所 610064)

宽带VPN网络密钥管理的研究应用

Research and Application of Key_management Based on the Broadband VPN Network

摘要：本文主要基于中低速VPN网络环境的几种密钥管理协议出发，引出适合在高速VPN网络环境下的SKIP密钥管理协议，然后对该协议及其特点进行分析，并结合IPSEC和VPN，从密钥的产生，证书的颁发和网络框架等三个方面出发，提出基于SKIP协议的密钥管理模型,最后结合宽带VPN网络的IPSEC隧道和传输两种模式在LINUX操作系统中实现。

关键词：密钥管理 宽带VPN SKIP协议

1 引言

目前,国内外密钥管理主要应用于中低速的VPN产品中,基本上都采用基于对称密码体制的密钥管理方式，随着网络速度不断提高，现有的密钥管理已日渐不适应宽带VPN环境，一般来讲，宽带VPN的网络环境是指网络传输速度每秒达到1000M字节的虚拟专用网络。

对于网络安全技术的核心部分——密钥管理技术的研究已经有了很长的历史，在此过程中，IETF制定了几个主要的密钥管理协议，Internet安全关联和密钥管理协议（Internet Security Association and Key Management Protocol，ISAKMP)，Internet密钥交换协议（Internet Key Exchange,IKE),Oakley密钥交换协议，Photuris密钥管理协议，Internet简单密钥管理协议(Simple Key-Management for Internet Protocols，SKIP协议),这五种协议都用ESP（Encapsulated Secruty Payload）和AH（Authentication Header）对IP数据包提供安全保护，其中ISAKMP, Oakley, IKE还需要建立起双方之间的安全关联，安全关联(Security Association,SA）是两个或多个实体间的关系,描述实体间如何利用安全服务进行安全通信。它们通过专门的密钥管理信息包建立双方需要的密钥，然后才能进行安全通信，因为需要专门的管理信息包，在突发事件中应变能力较差,特别是在密钥更新的过程中常常会带来通信的延迟，在高速网络环境下，需要频繁的发布密钥管理包，不仅加重了网络负担，而且在更新过程中出现丢包，需要重传，加大了网络的延迟，因此,它们都不适合在高速网络环境下进行密钥管理。

2 SKIP协议及特点

2.1 SKIP协议概述

SKIP协议是服务于面向无会话的数据包协议如IPv4和IPv6的密钥管理机制,基于内嵌密钥的密钥管理协议。每个数据包都被一个密钥加密,这个密钥包含在数据包中同时又被另一个事先已被通信双方共享的密钥加密。SKIP协议使用经过鉴别对方的公钥值和自己的私钥来生成双方所共享的密钥，在每个IPsec通信包中都含有密钥信息，这样可以实现一包一密钥，满足随时实现密钥的更新,而不需要专门的密钥管理信息包，不会给通信带来延迟，这对于密钥更新频繁的环境特别有用。例如在一个配置策略为100M字节就要更新密钥的千兆环境中,每秒就要更新密钥,如果采用有连接状态的密钥管理，就要频繁的发布密钥管理包，不仅加重了网络负担，而且在更新过程中如果出现丢包，需要重传，加大了网络的延迟。

2.2 SKIP协议特点

SKIP协议采用无连接状态的密钥更新，可以不经过先协商而随时更新密钥。若两个节点都已经有对方节点的公钥证书，则不需要额外的密钥交换包，因为到来的数据包中已经包含供接收节点计算共享密钥，并且正确响应的足够信息。正是由于这个轻量级特点，当主机正与许多对等主机通信时，SKIP协议对错误的恢复（如系统重启动）将会非常快。SKIP协议能防御常见的攻击：对抗中间人攻击。SKIP协议使用鉴别过的Diffie-Hellman公钥值，因为这个鉴别值在获取公钥证书时，要对发布证书的实体的数字签名进行验证，通过使用会话密钥

和主密钥，SKIP协议能对抗已知/选择密钥攻击，正是基于它所选用的加密算法能够对抗已知/选择明文攻击；对抗拒绝服务攻击，SKIP协议预先计算并缓存主密钥。

SKIP协议的不足是由于每个包都包含密钥信息，减少了每包的数据的传输量，相对而言每包的传输效率变低，但对于高速环境而言，这种开销相对发送密钥交换包和丢包等造成的通信延迟而言，影响很小。在宽带VPN网络环境中，若采用ISAKMP、Oakley、IKE、Photuris或SKEME等密钥管理协议，必然会频繁发送密钥更新包，如果密钥更新包丢失，则需重传，这将大大影响通信效率；而采用SKIP协议，则可以随时对密钥进行更新，而无需发送专们的密钥管理信息包。因此在宽带VPN环境中，国内外的发展趋势是尽量不采用象ISAKMP、Oakley、IKE、Photuris或SKEME等有连接状态的密钥管理协议，主要采用无连接状态的SKIP密钥管理协议。

正是由于SKIP协议不需要在建立连接之前进行连接会话和实时传输时对数据包连接状态要求，及对网络攻击的其本身具有的预防等特点，提出一种宽带网络VPN环境下的密钥管理和密钥交换解决实施方案，通过宽带VPN网络环境中实现与IPsec的结合的方案。通过与PKI（Public Key Infrastructure）相结合，颁发和识别x.509数字证书，支持证书撤消列表（CRL），支持目录服务（LDAP V3），提供支持第三方CA的接口，在LINUX操作系统中实现SKIP协议的密钥管理。

3 实现原理

3.1 VPN设备数字证书的产生、分发、撤消及设备并为第三方CA提供接口

如图1所示，设备数字证书在CA上产生，采用在线方式来分发和撤消设备的数字证书，设备的私钥及CA的公钥采用离线方式（比如：通过智能卡）分发，同时为了适应宽带VPN网络环境，这里采取“缓存证书信息”的措施，即将常用的其他设备的数字证书存放在本地的缓存中，当需要其他设备的数字证书时，首先在“证书信息缓存库”中查找有无对方的数字证书，如果没有才到公共的“证书信息库”中去取，当在CA上撤消某个设备的数字证书时，需要通知相应设备以刷新“证书信息缓存库”中的信息。同时为了提供对第三方CA的支持，系统颁发的数字证书将严格遵从X.509 V3标准，提供不同类型和不同系统之间的证书的互通性和互操作性。

3.2 基于LINUX操作系统的SKIP密钥管理协议与IPsec相结合在宽带VPN网络中的实现

在LINUX操作系统下实现SKIP协议与IPsec相结合的体系结构如图2所示。在图2中，SKIP密钥管理器负责从证书信息库中提取其他安全网关的公钥，验证该公钥的真实性，并按照图1所示的密钥产生流程最终将瞬时密钥Kp存入“核心密钥cache”中。“SKIP协议流模块”与“IPsec核心模块”位于网络接口层与IP层之间。当一个IP数据包要输出时，IPsec核心模块查找“系统策略库”以决定是否对该IP数据包实施IPsec处理，如果需要对该IP数据包实施IPsec处理，则填充IPsec头，IPsec头的位置依AH或ESP的工作模式而定，如果是工作在传输模式，则IPsec头位于原始IP头之后，位于上层协议数据之前；如果是工作在隧道模式，则IPsec头位于

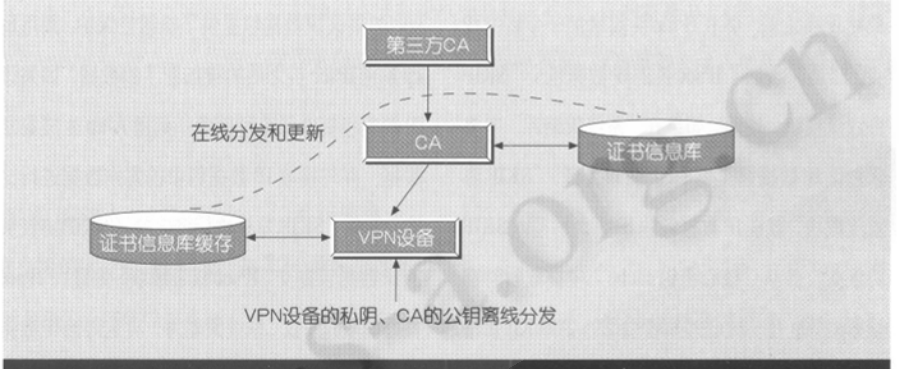

图1 证书分发、更新及支持第三方CA示意图

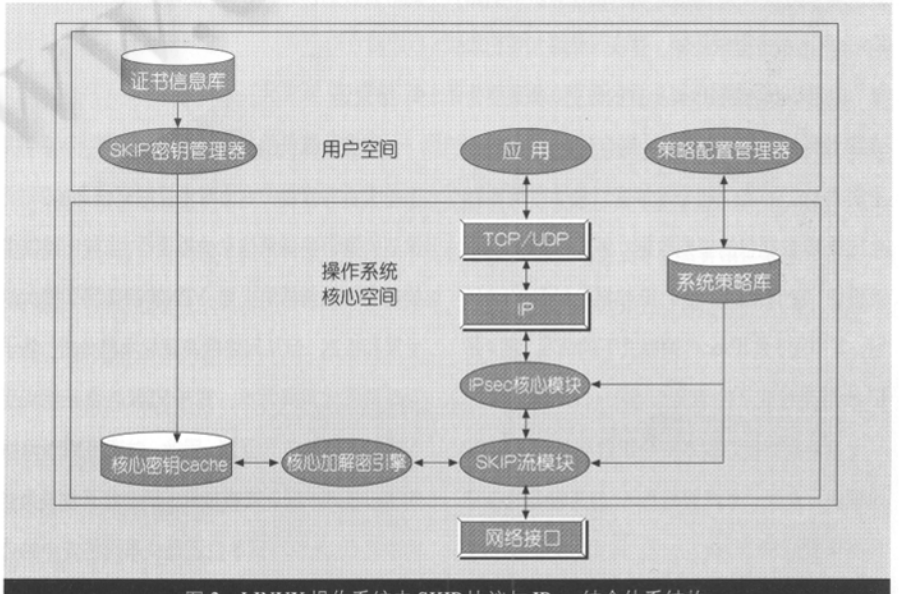

图2 LINUX操作系统中SKIP协议与IPsec结合体系结构

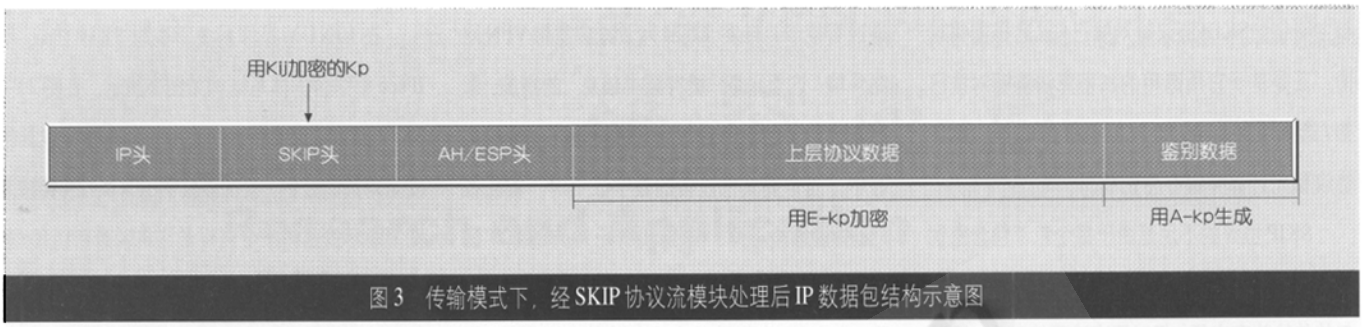

图3 传输模式下，经SKIP协议流模块处理后IP数据包结构示意图

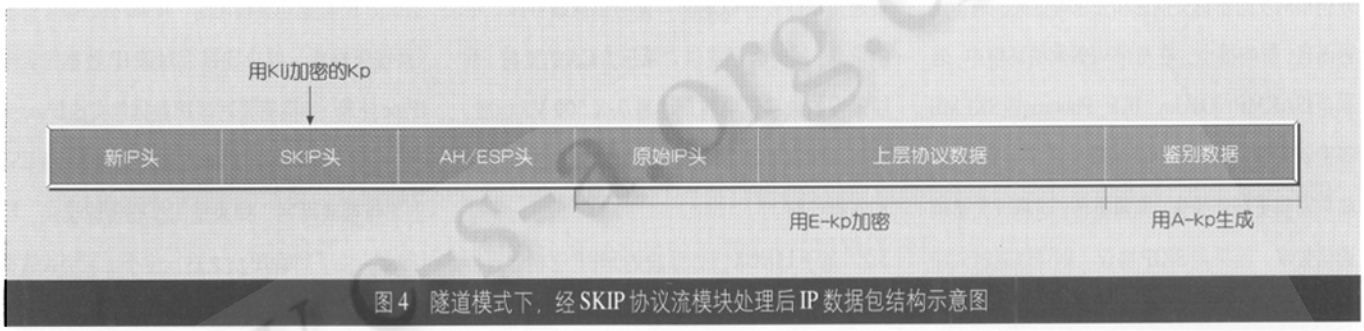

图4 隧道模式下，经SKIP协议流模块处理后IP数据包结构示意图

原始IP头之前，并在IPsec头前增加一个新的IP头。然后将增加了IPsec头的IP数据包交“SKIP协议流模块”处理，如果在“系统策略库”中要求对该IP数据包实施SKIP协议处理，“SKIP协议流模块”就在IP数据包的IP头之后插入SKIP协议头，并从“核心密钥cache”中提取瞬时密钥Kp，Kp在“核心加解密引擎”中用Kij加密之后填入SKIP协议头中。

如果为该IP数据包实施机密性保护，则由Kp分离出加密密钥E-kp，并在“核心加解密引擎”中用E-kp加密IPsec头后的数据；如果要为该IP数据包提供鉴别服务，则有Kp分离出鉴别密钥A-kp，并在“核心加解密引擎”中用E-kp生成原IP数据包的鉴别数据，经过“SKIP协议流模块”处理之后，整个IP数据包如图3、4所示，其中图3是IPsec传输模式下的情况，图4是IPsec隧道模式下的情况。

当从网络接口输入一个IP数据包时，“SKIP流模块”查找“系统策略库”，如果需要对该IP数据包实施SKIP协议处理，则用Kij解密SKIP协议头中的Kp，并由Kp分离E-kp和（或）A-kp，如果该IP数据包提供了机密性保护，则用E-kp解密IPsec头之后的被加密了的数据，如果该IP数据包提供了鉴别服务，则用A-kp生成鉴别数据，并与接收IP数据包中的鉴别数据进行比较，最后“SKIP流模块”将去掉了SKIP协议头的IP数据包提交“IPsec核心模块”处理，“IPsec核心模块”查找“系统策略库”决定对该IP数据包是否事实IPsec处理，如果需要进行IPsec处理，则对该数据包进行IPsec处理。

4 结束语

随着计算机的普及和互联网发展，无论个人还是企业等，在一方面享受互联网信息的同时，深刻的意识到保密信息的重要性。当前出现很多的安全产品包括防火墙，VPN等都得到了很大的发展和提高，但从网络的高速化角度分析，基于互联网和专用网考虑，宽带VPN才真正能实现了远程网络的安全互联，因此，对宽带VPN网络的核心技术－密钥交换技术的研究和开发成为当前的热点，无论科研单位还是从事网络安全的公司，企业都投入了很大的财力，物力。本文即从该角度出发，提出适于宽带VPN网络的密钥管理技术。

参考文献

1 Germano Caronni, Hannes Lubich etc, "SKIP - Securing the Internet", IEEE Computer Society Press, 1996.

2 B. Gleeson, A. Lin etc, "A framework for IP Based Virtual Private Networks ",RFC2764 February 2000.

3 H. K. Orman, "The OAKLEY Key Determination Protocol", Internet draft, work in progress, May 1996.

4 Ashar Aziz Tom Markson Hemma Prafullchandra," Simple Key-Management for Internet Protocols (SKIP)", April 1997.

5 D.Maughan,"Internet Security Association and Key Management Protocol",RFC2408 November 1998.