Linux VPN 网关密钥交换机制的设计*)

朱艳琴　钱培德
(苏州大学计算机科学与技术学院　苏州 215006)

摘　要　介绍了在 Linux 平台上实现 VPN 安全网关的总体设计思想以及通过 IKE 动态协商安全关联 SA 的主要过程，重点讨论了所采用的椭圆曲线密钥交换方案，并给出了有效的点乘运算快速实现算法。由于椭圆曲线密码体制具有每比特最高安全强度，因此大大提高了密钥分配的效率。

关键词　VPN 安全网关，IKE，椭圆曲线密码体制，点乘运算

The Design of Key Exchange Mechanism of Linux VPN Gateway

ZHU Yan-Qin　QIAN Pei-De
(School of Computer Science and Technology , Suzhou University, Suzhou 215006)

Abstract　General design of a VPN security gateway on Linux is discussed, in which Security Association(SA) is negotiated dynamically based on IKE, focusing on the scheme of elliptic curve key exchange. And fast algorithms of point multiplication are given. As the elliptic curve cryptography has the highest security strength, the efficiency of key allocation is greatly enhanced.

Keywords　VPN security gateway, IKE, Elliptic curve cryptography, Point multiplication

随着网络应用的不断普及，信息的安全保密问题日益突出，由此产生了 VPN[1](Virtual Private Network，虚拟专用网)这种利用公共通信网络实现网络互连和信息交换的组网方式。VPN 基于某种安全协议(如 IPSec 协议)，通过隧道和加密技术，采用策略管理组建虚拟专用网，在逻辑上具有“私有性”和“专有性”的特点，可实现数据传输的完整性、机密性，为利用公共通信网络进行的连接和访问提供了安全保障。

本文所述的 VPN 安全网关基于 IPSec 协议实现[2]，通过在 IP 层上对数据进行安全处理，利用认证、加密等安全措施为上层协议提供安全保障。通信双方协商用于实现安全通信的各项安全参数，包括双方的认证机制、使用的加密解密算法、密钥等，这些安全参数共同构成安全关联(Security Association，SA)。各种应用程序可以获取 IP 层提供的安全服务，而不必设计和实现自己的安全机制，因此减小了密钥协商的开销，也降低了产生安全漏洞的可能性。

本文将首先给出 VPN 安全网关的总体设计结构，然后进一步讨论所采用的密钥交换机制。

1　VPN 安全网关的总体结构

图 1 是整个 VPN 安全网关的总体结构图。SADB(Security Association DataBase)由一系列 SA 组成。算法库存放了多种可选的验证和加密算法，在处理时将通过 SA 中的算法项来指明所需要的算法。PF_KEY[3]实现内核 SADB 和 IKE 守护进程的通信。另外，用户可手工配置 SA 或启动 IKE(Internet Key Exchange)[4]动态协商 SA。安全策略库存放了由用户或系统管理员所制定的策略，策略将决定通信的双方是否采用 IPSec 处理，以及决定采用何种协议、算法、模式等。

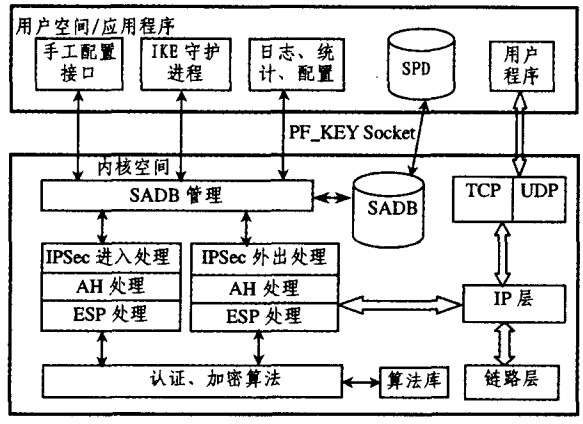

图 1　VPN 安全网关的总体结构

IKE 是一个混合协议，使用三个不同协议的相关部分，它们分别是：Internet 安全关联和密钥管理协议(ISAKMP)、Oakley 密钥确定协议和安全密钥交换机制(SKEME)，并在由 ISAKMP 规定的基本框架内运作。Oakley 和 SKEME 规定在通信双方间建立一个共享的验证密钥时必须采取的一系列步骤，IKE 利用 ISAKMP 提供的框架执行这些步骤，同时交换其它附加信息，为 IPSec 双方提供用于生成加密密钥和认证密钥的密钥信息。

2　IKE 交互过程的实现

IKE 交互过程分为两个阶段实现。在阶段 1，通信双方建立安全、认证的通道，即建立一个 ISAKMP SA，其中包含保护通信双方协商过程的一系列安全参数，使用这个 SA 可以保护其他协议协商 SA；在阶段 2，建立其他安全服务(如

*)基金项目：江苏省自然科学基金项目(编号 BK2004039)资助。朱艳琴　副教授，主要研究方向为计算机网络安全和应用密码学；钱培德　教授，博士生导师，主要研究方向为计算机信息处理技术。

AH 和 ESP)的 SA,这一阶段的消息交换受第一阶段协商中建立的 ISAKMP SA 的保护。

2.1 阶段 1 交换

在阶段 1 交换中,主模式提供了身份保护机制,共交换了 6 条消息:

(1)发起者 → 响应者:HDR,SA

在消息 1 中,HDR 为 ISAKMP 头,SA 是带有一个或多个建议载荷的安全关联载荷,里面含有发起者支持的多种建议提案,供响应者选择。每种提案又有多个保护套件,即加密算法、签名算法、散列算法等组合。

(2)响应者→发起者:HDR,SA

在消息 2 中,响应者发送一个 SA 载荷,内含响应方所接受的提案。

(3)发起者 → 响应者:HDR,KE,Ni

在消息 3 中,KE 为密钥载荷,含有发起者的 Diffie-Hellman 公开密钥,Ni 为 nonce 载荷,含有发起者的随机数。

(4)响应者→发起者:HDR,KE,Nr

在消息 4 中,KE 含有响应者的 Diffie-Hellman 公开密钥,Ni 含有响应者的随机数。

此时,双方通过计算可以生成一致的验证密钥和加密密钥,也得到了用于第二阶段协商的密钥材料。该密钥材料将被用来产生保护用户数据的密钥。

(5)发起者 → 响应者:HDR*,IDii,AUTH

在消息 5 中,HDR* 表示后面的载荷是加密的,IDii 为发起者标识,AUTH 表示发起者用协商的签名算法对计算而得(如使用 HMAC)的哈希值进行签名。

(6)响应者→发起者:HDR*,IDir,AUTH

消息 6 与消息 5 的作用类似。在这里,IDir 表示响应者标识。

2.2 阶段 2 交换

阶段 2 交换采用快速模式。在快速模式下交换的载荷都是加密的。消息描述如下:

(1)发起者 → 响应者:HDR*,HASH(1),SA,Ni[,KE][,IDi,IDr]

在消息 1 中,发起者向接收者发送一个 HASH 载荷(内含通过计算而得的消息摘要)、一个 SA 载荷、一个 nonce 载荷 Ni(内含发起者的随机数)、可选的密钥载荷 KE、发起者的身份载荷 IDi 和接收者的身份载荷 IDr。

HASH (1)= prf (SKEYSTR_a,MsgID |SA|Ni[| KE][|IDi |IDr])

符号说明如下:

Prf:协商好的伪随机函数

SKEYSTR_a:阶段 1 中生成的密钥信息

MsgID :ISAKMP 头中的消息 ID。

(2)响应者→发起者:HDR*,HASH(2),SA,Nr[,KE][,IDi,IDr]

此消息中的载荷与消息 1 中的载荷类似。

HASH (2)= prf(SKEYSTR_a,MsgID |Ni_b |SA |Nr[| KE][|IDi|IDr])

(3)发起者 → 响应者:HDR*,HASH(3)

消息 3 用于对前面的交换进行认证,仅由 ISAKMP 头和 HASH 载荷组成。

HASH (3)=prf(SKEYSTR_a,0| MsgID |Ni_b|Nr_b)

其中 Ni_b 和 Nr_b 分别表示发起者和响应者的随机数。

3 椭圆曲线密钥交换方案

鉴于在目前所知的公钥密码体制中,椭圆曲线密码体制具有每比特最高安全强度[5],即在同等安全的程度下具有更快的速度、更短的密钥长度、更少的存储量及带宽优势,因此我们在 VPN 安全网关的设计中采用了基于有限域 F_{2^m} 上的椭圆曲线 Diffie-Hellman 密钥交换方案,将之应用于上述 IKE 实现的阶段 1 中。

域 F_{2^m} 上的非超奇异椭圆曲线(超奇异椭圆曲线容易受到某些攻击)$E(F_{2^m})$ 是由满足下面方程的点 $p=(x,y)(x,y\in F_{2^m})$ 连同另外一个点 O(称为无穷远点)一起所构成的集合[5]:$y^2+xy=x^3+ax^2+b$。其中 $a,b\in F_{2^m}$,$b\neq 0$。

域 F_{2^m} 上的椭圆曲线域参数具体说明了椭圆曲线 E 以及 E 上的基点 $P(x_p,y_p)$。域 F_{2^m} 上的椭圆曲线域参数是一个七元数组:

$T=(m,f(x),a,b,P,n,h)$

其中 m 是定义域 F_{2^m} 的整数,$f(x)\in F_{2^m}$ 是一个 m 次的不可约多项式,它决定了 F_{2^m} 的表示;元素 $a,b\in F_{2^m}$ 决定了由上述方程定义的椭圆曲线,p 是 $E(F_{2^m})$ 上的基点 $P=(x_P,y_P)$,素数 n 是点 P 的阶,整数 h 是余因子 $h=\#E(F_{2^m})/n$,$\#E(F_{2^m})$ 为椭圆曲线 $E(F_{2^m})$ 上所有点的个数。

假设已选取了一个椭圆曲线,其域参数为 $T=(m,f(x),a,b,P,n,h)$。则基于椭圆曲线 Diffie-Hellman 密钥交换协议,通信双方 A 和 B 之间的密钥交换过程可以概述如下[6,7]:

(1)用户 A 选取一个满足条件 $1\leqslant k_A\leqslant n-1$ 的整数 k_A,作为 A 的私钥,然后产生公钥 $Q_A=k_Ap$,这是椭圆曲线上的点(x_{Q_A},y_{Q_A})并把 Q_A 传送给用户 B。

(2)用户 B 也选取一个满足条件 $1\leqslant k_B\leqslant n-1$ 的整数 k_B,作为 B 的私钥,然后产生公钥 $Q_B=k_BP$,这是椭圆曲线上的另一点(x_{Q_B},y_{Q_B}),并把 Q_B 传送给用户 A。

(3)用户 A 生成密钥 $K=k_AQ_B$,这是椭圆曲线上的点(x_K,y_K)。

(4)用户 B 也生成密钥 $K=k_BQ_A$,即椭圆曲线上的点(x_K,y_K)。

因为 $k_AQ_B=k_A(k_BP)=k_B(k_AP)=k_BQ_A$,所以用户 A 和用户 B 生成的密钥 K 是相同的。

在上述 VPN 安全网关的设计中,可协商的椭圆曲线群为第三、第四 Oakley 群。这是两个分别在有限域 $F_{2^{155}}$ 和 $F_{2^{185}}$ 上定义的椭圆曲线群,群 ID 分别为 3 和 4,不可约多项式分别为 $x^{155}+x^{69}+1$ 和 $x^{185}+x^{69}+1$。

4 点乘运算的快速实现算法

上述椭圆曲线 Diffie-Hellman 密钥交换方案中的主要操作是点乘,即椭圆曲线上一个点 P 被一个整数 K 相乘的运算。为了给出有效的实现算法,首先定义 NAF[8]。正如每个正整数具有唯一的二进制代码一样,每个正整数都有唯一的 NAF 扩展,它是 n 的一种有符号二进制扩展,并且任意两个相邻的系数不会同时为非 0。这种扩展被称为"非毗邻形式"(nonadjacent form,NAF)。而一个正整数的 NAF 扩展具有比二进制扩展少得多的非 0 系数。为求一正整数的 NAF 形式,允许剩余是 0 或±1。例如,因为 $29=2^5-2^2+2^0$,则

(下转第 71 页)

般都是一个很小的数。所以，虽然操作集计算也会带来一些时空上负荷，但都是线性复杂度，且很小。

通过操作集计算获得的好处是保证每次操作都是有效的，致使文档结构总是有效性的，从而提高编辑生成质量。同时，有缺省操作有效性保证，可以使得工作效率提高，也使用户集中关注数据项有效性。

以操作有效性来保证文档结构有效性，是一种前效策略，可以消除盲目性，提高了效率。而一致性验证发现错误是后效手段，不能避免重复工作。而且，如果对结构认识不清楚，这种后效手段还是无法从根本上解决问题。对于数据内容编辑，除了 ECA 机制进行及时验证外，还可以通过采用相应数据类型编辑控件来保证数据有效性。从某种意义上可以认为编辑控件的功能也是一种有效操作。

结束语 基于上述三个基本操作上的操作集合定义已经满足了 XML 文档的编辑需要。而作为编辑理念中的复制、剪切和粘贴这 3 个操作也容易在基本操作集的基础上扩充实现。复制的目的是为了粘贴。所以，对复制操作可以不做约束，完全由粘贴操作有效性计算来控制。复制的对象应该是以当前节点为根的子树。粘贴的结果是在当前节点前后或者子节点中插入一颗子树。在操作对象类型一致的前提下，粘贴操作的有效性等同于插入操作有效性。剪切操作是删除和复制的操作组合。所以，剪切操作的有效性可以等同于删除操作的有效性。对于鼠标的拖放操作，也可以采用同样的方式计算其有效性。

综上所述，本文提出了一种基于操作集计算方法来保证 XML 数据文档的结构有效。如果结合 ECA 机制或者借助编辑控件对简单类型数据进行验证，就可以完全保证编辑生成的 XML 文档的有效性。

参 考 文 献

1 Radiya A, Dixit V. The basics of using XML Schema to define elements. http://www.ibm.com
2 van der Vlist E. Using W3C XML Schema. http://www.xml.com/pub/a/2000/11/29/schemas/part1.html
3 XML Schema: Part 0: Primer. http://www.w3.org/TR/xmlschema-0
4 董亚绢，卑小贤，等. 一种 XML 文档模式有效性验证算法. 计算机工程与应用(已录用)
5 Bailey J, Poulovassilis A, Wood P T. An Event-Condition-Action Language for XML. WWW2002, 2002

(上接第 64 页)

NAF(29)=(1,0,0,−1,0,1)

计算 NAF 和通过 NAF 求解点乘的运算分别由算法 1 和算法 2 给出。

算法 1 求 NAF 值

输入：正整数 k
输出：NAF(k)
(1)$i\leftarrow 0$
(2)While $k\geq 1$do
If k is odd then:
$k_i\leftarrow 2-(k \bmod 4)$, $k\leftarrow k-k_i$
Else: $k_i\leftarrow 0$
$k_i\leftarrow k/2$, $i\leftarrow i+1$
(3)Return $(k_{i-1}k_{i-2},\cdots,k_1,k_0)$.

算法 2 NAF 方法求点乘

输入：NAF(k)$=\sum_{i=0}^{l-1}k_i2^i$
输出：kP
(1)$Q\leftarrow 0$.
(2)For i from l-1 downto 0 do
$Q\leftarrow 2Q$
If $k_i=1$ then $Q\leftarrow Q+P$.
If $k_i=-1$ then $Q\leftarrow Q-P$.
(3) return(Q).

为了进一步减少算法 1 的运行时间，我们在算法 1 基础上使用了窗口技术[9]。假设宽度为 w，则整数 k 可表示为 $k=\sum_{i=0}^{l-1}k_i2^i$，其中每个非零系数 k_i 是奇数，且$|k_i|<2^{w-1}$。此时，先计算整数 k 的窗口为 w 的 NAF 表示，记为 NAF$_w$(k)，然后再计算点乘。只需将算法 1 稍作修改，便可求得 NAF$_w$(k)。修改之处为：算法 1 步骤(2)中原来的“$k_i\leftarrow 2-(k \bmod 4)$”改为“$k_i\leftarrow k \bmod 2^w$”，其中“$k_i\leftarrow k \bmod 2^w$”表示满足下式的整数 u：$u\equiv k(\bmod 2^w)$，且$-2^{w-1}\leqslant u<2^{w-1}$。例如，给定窗口 $w=4$，$k=22310$，则有

$22310=2^{15}-5\times 2^{11}-7\times 2^5+3\times 2$

因此，在计算 $22310P$ 时，可预先计算 $3P$，$5P$，$7P$，然后计算

$22310P=10^{15}P-2^{11}(5P)-2^5(7P)+2(3P)$

算法 3 窗口 NAF 方法求点乘

输入：整数 k，w，$P(x,y)\in E(F_{2^m})$
输出：kP
//预计算，仅需一次
//计算 uP，for u 为奇数，且 $2<u<2^{w-1}$
(1)$P_0\leftarrow P$, $T\leftarrow 2P$.
(2)For i from 1 to $2^{w-2}-1$ do
$P_i\leftarrow P_{i-1}+T$
//主计算
(3)计算 NAF$_w(k)=(u_{l-1},u_{l-2},\cdots,u_1,u_0)$.
(4)$Q\leftarrow O$.
(5)For j from $l-1$ downto 0 do
$Q\leftarrow 2Q$
If $u_j\neq 0$ then:
$i\leftarrow(|u_j|-1)/2$
If $u_j>0$ then $Q\leftarrow Q+P_i$;
Else $Q\leftarrow Q-P_i$
(6)return(Q)

总结 椭圆曲线密码体制的诱人之处在于，它是建立在有限域椭圆曲线离散对数问题这个数学难题之上的，而此难题比大整数分解及素域乘法群离散对数问题更为难解。因此，与其他公钥密码体制相比，椭圆曲线密码体制在同等安全强度下可以使用长度短得多的密钥，在存储效率、通信带宽及计算效率等方面表现出明显的优势。本文在 Linux VPN 网关的设计中，将椭圆曲线 Diffie-Hellman 密钥交换应用于 IKE 实现过程，达到了动态协商和管理 IPSec SA 的基本要求，大大提高了密钥分配的效率。对于椭圆曲线密码体制而言，点乘运算是最耗时的操作，为此在实现过程中采用了点乘运算的快速实现算法。考虑到由于进行加密和隧道通信，VPN 安全网关负载增大，因此下一步的主要工作将是采取措施对整个系统进行优化，以减轻网关 CPU 的负担。

参 考 文 献

1 Stallings W. Cryptography and Network Security: Principles and a Practice(Third Edition). Prentice Hall, 2002
2 Davis C R. IPSec: VPN 的安全实施. 周永彬，等译. 北京：清华大学出版社，2002
3 RFC2367. PF_KEY Key Management API, Version 2, 1998
4 RFC2409. The Internet Key Exchange (IKE), 1998
5 IEEE P1363. Standard Specification for Public-key Cryptography, 2000
6 ANSI X9.63. Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, 1999
7 朱艳琴. 基于 ECC 的密码系统研究与设计. 微电子学与计算机，2003,20(12):51～53
8 周玉洁，冯登国. 公开密钥密码算法及其快速实现. 北京：国防工业出版社，2002
9 Hankerson D, et al. Software Implementation of Elliptic Creve Cryptography Over Binary Fields:[Technical report CORR 2000-42]. University of Wtaerloo, 2000. http://www.cacr.math.uwaterloo.ca