基于国密算法的 IPSec VPN 设计与实现

张 尧,刘笑凯
(华北计算机系统工程研究所,北京 100083)

摘 要:基于国家安全和经济发展的客观需求,在安全产品中采用国密算法,确保网络通信自主安全十分必要。通过将 IPSec 协议中的默认非对称协商算法、哈希算法和对称加密算法分别采用国密 SM2、SM3、SM4 算法替代,设计并实现基于 Linux 系统内核协议栈的 IPSec VPN 系统。实践表明,采用国密算法能够有效满足 IPSec VPN 的需求。

关键词:IPSec;虚拟专用网;网络安全
中图分类号:TP393.08 **文献标识码**:A DOI:10.19358/j.issn.2096-5133.2020.06.009
引用格式:张尧,刘笑凯. 基于国密算法的 IPSec VPN 设计与实现[J].信息技术与网络安全,2020,39(6):49-52.

Design and implementation of IPSec VPN based on national secret algorithm

Zhang Yao, Liu Xiaokai
(National Computer System Engineering Research Institute of China, Beijing 100083, China)

Abstract: Based on the objective needs of national security and economic development, it is necessary to use national secret algorithms in security products to ensure autonomous and controllable network communications. By replacing the default asymmetric negotiation algorithm, hash algorithm, and symmetric encryption algorithm in the IPSec protocol with the national secret SM2, SM3, and SM4 algorithms, the IPSec VPN system based on the Linux system kernel protocol stack is designed and implemented. Practice has shown that the use of national secret algorithms can effectively meet the needs of IPSec VPN.

Key words: IPSec; VPN; cyber security

0 引言

IPSec VPN 是一种常见的 VPN 技术,具有速度快、安全可信等特点。由于 IPSec 国际协议中的标准算法可能存在算法安全性和协议安全性等问题,因此国家密码管理局制定了国家密码算法标准以及 VPN 技术规范。基于国家技术标准的指导,采用国密算法实现改进的 IPSec 协议,能够提高 IPSec VPN 的安全性,满足安全产品自主安全的需要。

1 IPSec 技术介绍

IPSec 是一种用于保护网络通信过程 IP 数据包安全的安全协议技术,可在由主机、网关作为端点构成的点到点的网络层链路上构建安全隧道,提供基于网络层的通信安全保护功能。在采用 IPSec 技术实现 VPN 时,通过在双方网关之间建立 IPSec 加密隧道,来实现由双方物理子网构建的虚拟局域网。

IPSec 主要由四部分组成:因特网密钥交换(Internet Key Exchange, IKE)协议、认证头(Authentication Header, AH)协议、安全载荷(Encapsulating Security Payload, ESP)协议以及上述模块中所需的加密算法和认证算法。其安全体系结构如图 1 所示[1-2]。

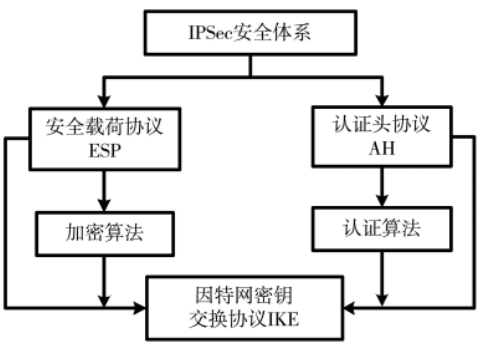

图 1 IPSec 安全体系

1.1 AH 协议与 ESP 协议

AH 协议能够为数据包提供完整性保护、数据

源认证和防重放等安全功能，一般用于只需确保数据完整性、检验发送方身份，无需数据保密的场景下。其通过在原始数据包头部之后增加 AH 头部段的方式实现。

ESP 协议除了可实现 AH 协议所提供的各项安全功能外，还对数据包整体进行加密，实现数据的保密性。根据 ESP 协议对数据的封装模式不同，分为隧道模式和传输模式，前者仅对 IP 负载进行保护，后者则将原始 IP 层头部连同负载一起进行加密保护[3]。

1.2 IKE 协议

为了实现 AH 和 ESP 协议，通信双方需要首先采用密钥管理协议来建立安全联盟(Security Association，SA)，以同步密钥和身份信息。

IKE 协议包括 ISAKMP、Oakley 和 SKEME 三个协议。其中 ISAKMP 主要定义在 IKE 伙伴(IKE Peer)之间的 IKE 联盟(IKE SA)建立过程；而 Oakley 和 SKEME 协议主要通过迪菲-赫尔曼(Diffie-Hellman，DH)密钥交换算法实现双方身份验证和密钥安全分发。目前，由 RFC 文档所规定的 IKE 协议共有 IKEv1 和 IKEv2 两个版本。

IKEv1 的协商过程分为两个阶段。其中第一阶段主要用于协商建立 IKE SA，又分为主模式、野蛮模式两种交互策略。主模式是使用最频繁的协商策略，协商双方通过交换 3 对消息，确定对等体双方 IKEv1 安全策略、协商密钥信息、验证身份，最终建立 SA；野蛮模式双方仅交换 3 条消息即建立 SA，通过牺牲一定的安全性来提高协商效率。第二阶段在第一阶段的 IKE SA 保护下进行，用于协商 IPSec SA 所需的密钥和参数、封装方式、认证方式等，双方交换 1 对信息。

1.3 IPSec 中的密码算法

IPSec 通过密码算法来保证数据机密性、完整性，采用非对称密钥的特性来实现密钥安全协商。在 IPSec 中使用了对称加密算法、公钥算法、摘要算法和 DH 密钥交换算法。在国际标准中，对称算法包括 AES、3DES 等，摘要算法包括 MD5、SHA 等，非对称算法包括 RSA、ECC 等[4]。

2 国密算法介绍

国密算法是一套由我国密码安全机构自主研发的密码算法，可用于国家信息安全相关各个领域中，其中由我国《IPSec 技术规范》中所规定在 IPSec 协商过程中要使用到的算法包括 SM2 椭圆曲线算法、SM1 或 SM4 分组密码算法、SM3 密码杂凑算法[5]。

2.1 SM2 算法

SM2 椭圆曲线公钥算法是国密标准中的非对称算法，属于对椭圆曲线密码学(Elliptic Curve Cryptography，ECC)算法的一种拓展，其数学基础建立在椭圆曲线离散对数问题上。SM2 算法所规定公钥长度为 512 位，私钥长度 256 位[6]。

与 RSA 算法相比，采用基于 ECC 的 SM2 算法能够在密钥长度相当的情况下，提供更高的安全性保护。192 位 SM2 密码的强度能够超过 2 048 位的 RSA 密码。

2.2 SM3 算法

SM3 算法是国密标准中的杂凑算法，其功能包括数字签名与验证、消息认证码生成和伪随机数的生成等，可用于多种密码应用。SM3 算法的安全性及效率与 SHA-256 相当[5]。

2.3 SM4 算法

SM4 算法是国密标准中的分组对称密钥算法，明文、密钥、密文长度均为 128 位，加密和解密所用密钥相同，可用于流式数据的快速解密。SM4 算法的实现流程如图 2 所示。

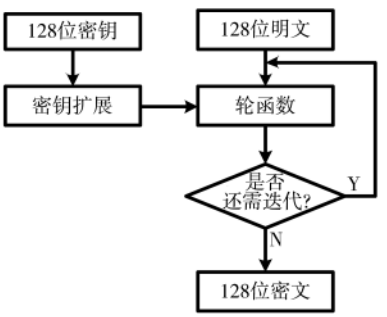

图 2 SM4 算法实现流程

SM4 算法的加密与密钥扩展算法均通过 32 轮非线性迭代过程实现。轮函数中使用轮密钥对 128 位数据进行处理，在解密所使用的轮密钥是加密轮密钥的逆序。在加密过程中，首先将 128 位密钥按照每 32 位一组分为 4 组，然后进行密钥扩展，生成 32 组 32 位轮密钥，再将输入明文按照 32 位一组分成 4 组，进行循环运算，得到 128 位密文。

3 国密算法替换

基于 Linux 2.x 操作系统内核协议栈，FreeS/WAN 提供了开源的 IPSec 协议的内核态实现。而 Openswan

项目继承该项目进行了后续开发[7-8]。通过对比国际 IPSec 标准与我国国密 IPSec 标准，找出所需更改的部分对 Openswan 的相关代码模块进行替换，能够实现基于国密算法的 IPSec VPN。

Openswan 项目的架构如图 3 所示。

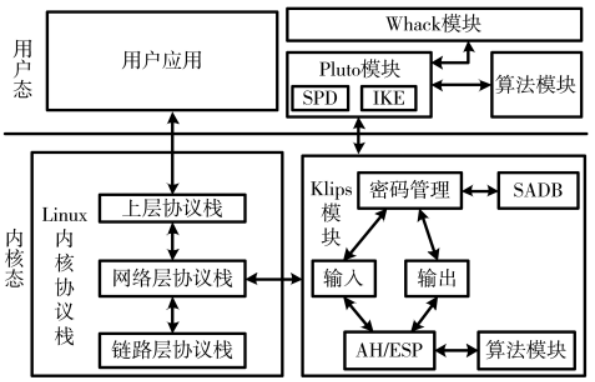

图 3 Openswan 项目架构示意图

Openswan 实现分为应用态和内核态的两部分，其中 Pluto 模块、Whack 模块位于 Linux 用户态。Whack 模块负责建立连接前的参数配置、管理 VPN 连接状态、系统日志等；Pluto 模块负责进行 IKE 协商、建立 SA；Klips 模块在 Linux 内核态下运行，接收来自 Linux 内核协议栈的网络数据包，根据已经配置的 SA，对数据包进行 AH 协议、ESP 协议的封装或解封处理。

3.1 协商流程的替换

在 Openswan 项目中，由 Pluto 模块在用户态实现 IKE 协商。IKE 的协商过程中，采用交换数字证书的形式，由通信双方各自进行身份认证，确认对方已得到授权。根据国密要求，在 IKE 协商过程中需要使用基于 X.509 格式的国密 SM2 数字证书进行身份认证，在 IKE 认证过程中，首先要采用国密 SM2 算法进行数字证书签名、验签。

根据 IKEv1 标准，认证第一阶段的主模式协商过程在 Pluto 模块中的实现如图 4 所示。

认证第二阶段的快速模式协商过程在 Pluto 模块中的实现如图 5 所示。

在国密标准中，IKE 主模式协商的流程与图中所示一致，但其中 SA 载荷部分需要替换成国密 SM3、SM4 相关参数。具体实现如表 1 所示。

根据 Pluto 模块相关函数的处理流程，证书相关数据应在主模式第二包中 CERT 相关字段中进行处理。因此，在 Openswan 源码中，向 main_inI1_outR1 相关流程里添加国密证书导出操作。向 main_inR1_outI2 相关流程里添加响应方国密证书导入操作，从而实现协商流程的国密算法替换。

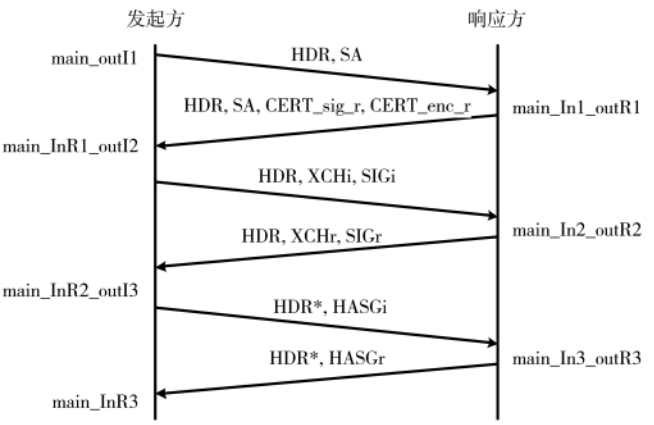

图 4 Pluto 模块中 IKE 主模式协商实现

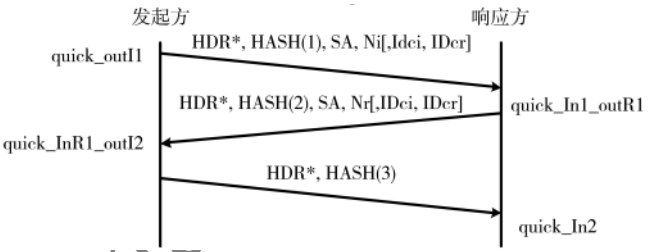

图 5 Pluto 模块中 IKE 快速模式协商实现过程

表 1 国密标准 SA 载荷参数

参数名称	标准数值
生存时间/s	3 600
加密算法	SM1 或 SM4
密码杂凑算法	SHA1 或 SM3
身份认证方式	公钥数字信封认证
密钥长度/位	128 或 256
非对称密码算法	SM2

3.2 业务算法替换

在 IPSec VPN 通道成功建立，SA 成功生成后，双方在业务通信阶段使用 ESP 协议的隧道模式来加密保护数据报文。根据国密要求，在 ESP 协议包的传输过程中，需要采用 SM1 或 SM4 对称加密算法进行数据机密性的保护，并且选用 SM3 或 SHA-1 算法来进行数据内容的完整性保护。

由于 Openswan 项目代码中用户态和内核态两部分各自使用独立的算法模块，因此需要在内核态中再次实现 SM1 或 SM4、SM3 或 SHA-1 算法。内核态的加密算法调用流程如图 6 所示。

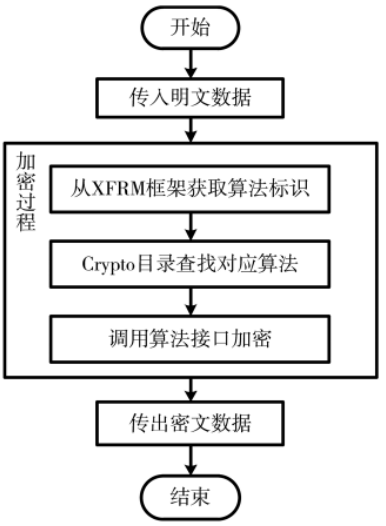

图 6 内核态的加密算法调用流程

在 Openswan 源码实现中，内核协议栈收到的网络业务数据由 Linux 在内核态直接执行加密算法，以便减少操作系统状态切换过程中产生的不必要的性能损失。这一过程中，Linux 采用 XFRM 框架进行算法查找和调用。在使用国密算法进行替换时，需要在内核进行国密算法的注册。其过程如下：

(1)根据 Linux 内核源码中的算法标识结构定义，构建国密算法的加密算法标识结构。

在 Linux 内核中，XFRM 框架对加密算法标识的定义包括位于源码目录下的 xfrm.h 头文件里，其数据结构包括 xfrm_algo_desc 和 sadb_alg_desc。在 Linux 内核源码 include/linux./pfkeyv2.h 中添加 XFRM 在 SPDB 中查找 SM1、SM3、SM4 国密算法所用到的算法标识，并在 net/xfrm/xfrm_alog.c 中加入这些国密算法所需的算法描述结构。这样就完成构建国密算法的加密算法标识结构的过程。

(2)在 Linux 内核的算法库中对国密算法进行注册。在 Linux 内核中的 NETLINK 模块里，提供算法注册的方式，其中 crypto_alg 结构用于描述对称加密算法，shash_alg 结构用于描述杂凑算法。由驱动程序调用 XFRM 框架的 crypto_register_alg 函数，完成向操作系统内核注册国密加密算法的过程。

4 结论

基于国密 SM2、SM3、SM4 等算法，在 Openswan 开源项目和在 Linux 操作系统的基础上进行代码修改和算法的替换，从而设计并实现了基于国密算法的 IPSec VPN 系统。经实验，替换后的 IPSec VPN 能够达到与预期相当的吞吐量，在保证了性能的同时，提高了 VPN 的自主可控水平。

参考文献

[1] 李辉.移动 VPN 技术综述[J].中国电子科学研究院学报，2019，14(9)：903-912.

[2] RFC 4301，Security architecture for the internet protocol[S].USA：IETF，2005.

[3] 张娜.基于 IPSec 的 VPN 网络安全的实现[J].中国新通信，2016，18(19)：83-83.

[4] 王欢.基于 IPSEC 协议的网络安全技术应用分析[J].中国新通信，2016(3)：88-88.

[5] GM/T 0022-2014.IPSec VPN 技术规范[S].国家密码管理局，2014.

[6] 孙荣燕，蔡昌曙，周洲，等.国密 SM2 数字签名算法与 ECDSA 算法对比分析研究[J].网络安全技术与应用，2013(2)：60-62.

[7] 李松涛.一种动态可配置多路串口网关设计[J].信息技术与网络安全，2019，38(11)：82-85.

[8] 张朕荣.一种将国密算法添加至 Openswan 的方法[J].现代计算机(专业版)，2015(6)：11-14.

(收稿日期：2020-03-27)

作者简介：

张尧(1995-)，男，硕士研究生，主要研究方向：计算机科学与技术。

刘笑凯(1977-)，男，硕士研究生，高级工程师，主要研究方向：保密通信。

版权声明