文章编号:1008-0570(2006)08-3-0055-03

IPSec 下 IKEv2 协议的实现

The Implementation of IKEV2 For IPSec

(桂林航天工业高等专科学校)杨小劲 刘建华
Yang,Xiaojin Liu,Jianhua

摘要:本文根据 IKEv2 密钥交换机制的特点,设计了实现 IKEv2 的框架结构和模块构成;通过建立交换状态与消息操作之间的转换关系,确定了消息处理的步骤和密钥交换的流程;并对各个功能模块的具体实现给出了详细的阐述。

关键词: IPSec;IKEv2;载荷;消息处理
中图分类号: TP393 文献标识码: B

Abstract:According to the characteristic of IKEv2 key exchange mechanism, we design and implement the framework and the module composition of IKEv2. Through establishing the transition relations between the exchange states and the message operation, we determine the message handling step and the key exchange flow, and elaborate the implementation of each function module in detail.

Keyword: IPSec,IKEv2,Payload, Message Handling

技术创新

1 前言

针对网上数据传输的安全问题,IETF(因特网工程任务组)于 1998 年 11 月公布了 Internet 安全协议标准:IPSec,它可以'无缝'地为 IP(IPv4 和 IPv6)引入安全特性。IPSec 采取的具体保护形式包括:数据起源地验证,无连接数据的完整性验证,数据内容的机密性(是否被别人看过),抗重播保护,以及有限数据流机密性保证。将 IPSec 协议用于主机,可实现端到端的通信安全;将 IPSec 组件配置于路由器和防火墙设备,可以很方便地构建起安全的、易于扩充的 VPN。

IPSec 的基础是安全关联(Security Association, SA)。它是两个通信实体经协商建立起来的一种协定。SA 可以通过用户手工配置的方式建立,也可以采用密钥交换的方式动态产生。前者较简易,但由于配置方法的静态特点使其缺乏安全性。而后者可以在两个通信实体之间,通过网络协商构建经过验证的安全通道,并在安全通道的保护下协商一致的 IPSec SA Proposal,令 SA 的配置生成更加灵活和安全。正是由于具有这种优势,密钥交换在通信安全领域变得越来越重要。IPSec 默认的密钥交换协议是 IKE(Internet Key Exchange)。

IKE 是一个混合型的协议,其自身的复杂性不可避免地带来一些安全及性能上的缺陷。IETF 一直在对现有版本 IKE 的不合理部分积极地征集修改意见。IPSec 工作组于 2004 年 9 月推出了最新一版的 IKE 协议草案——IKEv2,版本号是 2-17。IKEv2 在沿用原有协议的共享策略协商方法的基础上,对第一版协议进行了全面的优化和改进,从而使之具有更高的性能、更好的安全性以及更低的系统耗费。以 IKEv2 取代 IKE 作为新一代的密钥交换协议标准已逐渐成为业内人士的共识。IKEv2 的基本思想是首先验证通信双方的身份,然后协商用于保护通信的 SA。为了加快保护数据通信的 SA 的更新过程,IKEv2 将密钥协商的过程分成两个阶段:① 阶段 1 完成通信实体间身份的认证,并建立用于保护阶段 2 协商的 IKE_SA;② 阶段 2 在阶段 1 建立的 IKE_SA 的保护下,协商用于保护通信实体间数据通信的 CHILD_SA。一个在阶段 1 建立的 IKE_SA 可用于保护多个阶段 2 的 CHILD_SA 的协商,从而加快 CHILD_SA 的更新过程。

2 IKEv2 协议实现思想

对协议的实现时,力求充分考虑并支持 IKEv2 周期性密钥更新和身份重新认证,实现安全有效的密钥生成与交换机制。所需完成的功能目标为:通过消息的交换——IKE_SA_INIT 交换和 IKE_AUTH 交换实现原有 IKE 协议中阶段 1 和阶段 2 所实现的功能,即建立 IKE SA 和 IPSec SA;完整地定义协议中的各种载荷;对 SA 生命期和其他属性进行必要的控制,为确保安全性,必须能够及时删除到期的 SA,协商新的 SA;对一定的异常情况能够及时处理(如消息的超时重发)。

本文通过修改 Linux 的现有 IKE 源码来实现 IKEv2,分别涉及到 Linux 系统、IKE 源码、IKEv2 协议机制三个方面,经过综合分析,实现 IKEv2 面临的问题有:Linux 现有的 IKE 实现缺乏清晰的框架结构,不同交换类型、状态以及消息处理缺乏清晰的介定;采用现有 IKE 实现,用户想发起动态协商时,配置文件书写繁琐,运行命令参数比较复杂,IKEv2 实现时需简

杨小劲:讲师
基金支持:广西区科技攻关项目(桂科攻 0428002-1)

化用户配置的过程;IKEv2 加密验证机制和密钥生成方法与 IKE 截然不同,需要重新定义;IKE 中 SA 的生命期是双方协商产生。IKEv2 协议规定不再协商 SA 生命期,各方对自己 SA 的生命期负责。对 SA 到期事件,通信双方必须作出适当处理;现有 IKE 实现中,当程序运行到阶段 2 时生成 IPSec SA Proposal, 而在 IKEv2 中,要求初始交换第三条消息就必须发送 IPSec SA 载荷,因此需提前生成 IPSec SA Proposal。

针对上面的那些问题, 为了实现 IKEv2 的功能目标,采取了以下的方法:对 IKEv2 密钥交换过程的各重要环节、用户空间与内核空间的交互需求以及为用户提供方便简洁的 IKEv2 配置接口这几方面进行综合考虑,设计了 IKEv2 协议实现的总体框架,并按照功能划分出不同的模块。不再设置多种易混淆的交换类型,采用初始交换作为实现密钥协商的程序主体。消息处理函数采用了原有 IKE 以 ident_ 为开头的命名方法;设置加密验证模块用于 IKEv2 的加解密及完整性验证、身份验证以及密钥生成,并在初始交换流程的适当位置实现这些功能;为 IKEv2 发起者定义新的 IPSec SA Proposal 生成函数; 为接收者定义新的 IPSec SA 初始化函数。按照 IKEv2 通信双方的程序流程,对 IPSec SA 进行协商。根据协议要求定义 SA 到期处理函数。设置配置管理模块用于生成 IPSec SA 和处理到期 SA 这类需与内核 SAD (Security Association Database)、SPD (Security Policy Database)交互的功能的实现。

3 实现 IKEv2 的框架结构和模块构成

IKEv2 实现按功能主要划分为五个模块: 会话监听模块、控制与转换模块、配置管理模块、消息处理模块、加密验证模块。图中虚线外的区域属内核部分。算法库采用 OpenSSL 提供的密钥算法库。管理员可以通过用户界面配置安全策略和各项安全属性,以及启动协商会话的监听。IKEv2 的用户界面采用基于 Java 语言的可扩展开发平台 Eclipse 编写。内核 SPD、SAD 与配置管理模块的接口采用 PF_KEY 密钥管理接口。其结构框图如图一所示。

其中会话监听模块负责对网络会话信息以及内核发起协商的需求信息进行监听接收。当内核有动态协商需求时,通信方以发起者的身份开始发起密钥交换;当从网络接收到对方的协商请求时,通信方则以响应者的身份对密钥交换请求进行回应。无论哪种情况引起的密钥交换,都会交付给控制与转换模块进行交换状态的确定。不同的交换状态决定着消息中不同的载荷类型和顺序。消息处理模块是 IKEv2 实现的核心部分,它负责消息的发送处理和接收处理。在初始交换的后两条消息处理中,消息处理模块还需要和加密验证模块交互, 从算法库中提取出相应的算法,对消息进行加解密和完整性验证、对通信实体的身份进行验证。当 IKEv2 协商过程完成,通过配置管理模块完成对内核 SAD 的添加以及到期 SA 的处理。当 IPSec SA 到期, 配置管理模块接收到内核发来的 PF_KEY 消息,删除到期 SA。如果是发起者接收到了 IPSec SA 到期消息,还需转入控制与转换模块,重新开始协商。

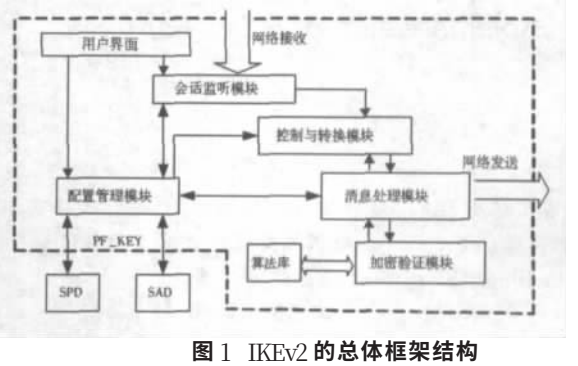

图 1 IKEv2 的总体框架结构

4 关键模块的实现方法

4.1 会话监听模块

IKEv2 主要需要监听处理两类信息: 来自于内核的配置信息和来自于协商对方的 ISAKMP(Internet Security Association and Key Management Protocol)信息。会话监听模块负责这两类信息的监听、接收、解析以及向下一功能模块的递交。首先为要监听的两类信息建立套接字:ISAKMP 套接字和 pfkey 套接字。然后进行监听,当收到消息时,判断消息的出处:如果收到的套接字信息属于 ISAKMP 协商会话信息, 则调用 ISAKMP 句柄(isakmp_handle)处理该消息,处理完交付给 IKEv2 控制与转换模块;如果是内核发来的 pfkey 配置信息,则调用 pfkey 句柄(pfkey_handle)处理该消息,处理完交付给配置管理模块。

4.2 控制与转换模块

控制与转换模块负责 IKEv2 协商前初始化、消息接收与消息发送的衔接、交换状态与消息处理函数之间的转换。协商前初始化包括创建 ph1handle 结构和设置初始状态,以及根据初始状态 SIT_START,通过数组 sitexchange 寻找并进入消息处理模块的相应函数 ident_i1send 或 ident_r1recv。消息接收与消息发送的衔接由函数 switch_main 完成, 当接收处理完毕返回,查找交换状态改变后对应的消息发送函数,转入消息发送处理流程。在这一模块设置了状态转换数组用于建立交换状态与消息处理函数之间的对应关系。

4.3 消息处理模块

消息的处理包括消息发送处理与消息接收处理。消息发送处理指的是按协议的要求组装各类载荷,并利用载荷链依次为各载荷装载通用载荷头。如需进行加密或加载验证数据时与加密验证模块交互,依照算法规范作必要的密钥运算,并装载加密载荷头。最后加载 IKEv2 消息头部, 将消息从 UDP/500 端口发送。共有四个主要的消息发送处理函数: 两个属发起者,

两个属响应者。消息接收处理是消息发送处理的逆操作。首先剥去消息头部，拆卸消息中各载荷，根据载荷类型作相应的处理。如果消息头的“下一个载荷”域表明是加密载荷，则需与加密验证模块交互，先对加密载荷进行解密和完整性验证，从解密后的数据中分离出各类型载荷，再作进一步的处理。如果消息中有AUTH载荷，由加密验证模块对其进行验证。共有四个主要的消息接收处理函数：两个属发起者，两个属响应者。消息处理流程如图二所示。

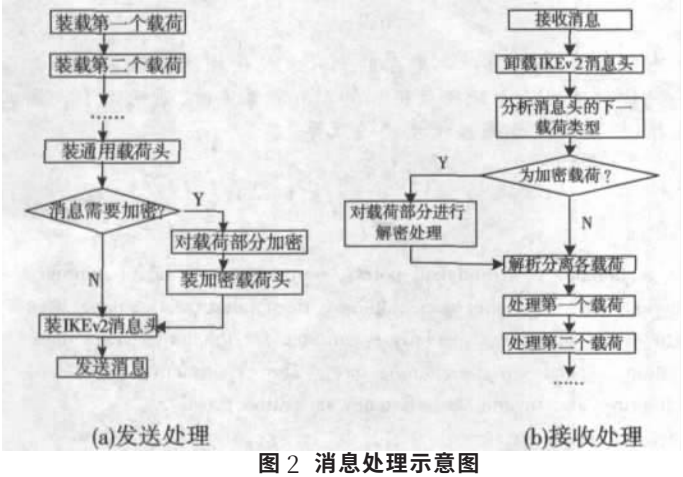

图2 消息处理示意图

4.4 加密验证模块

加密验证模块主要承载了三部分的功能：密钥素材的生成、消息的加解密和完整性验证、对通信方身份信息的验证。编写三个函数分别生成基密钥SKEYSEED、用于加解密和建立子SA交换的密钥材料、用于AUTH载荷身份验证信息的密钥材料。加解密和完整性验证应用于第三、四条消息及初始交换之后的所有消息。IKEv2协议在规定加密载荷格式时以明文方式把初始向量IV放在加密数据区之前，本文的实现中考虑到这种方式IV较易泄露，同时根据协议要求，可以伪随机地生成或是用前一条发送消息的最后一个密文分组来作为IV。因此对IKEv2的加密载荷格式进行了改进——不在加密载荷的结构中设置IV域，而采用前一条发送消息的最后一个密文分组的方式来衍生IV。

AUTH载荷的验证数据域中放置签名或当使用预共享密钥时的MAC。对于响应者，所签名的字节包括整个第二条消息（在第二条消息发送前，将其存为r_buf），还要附加Ni、prf(SK_pr,IDr')的值。prf是伪随机函数。对于发起者，所签名的字节包括整个第一条消息（在第一条消息发送前，将其存为i_buf），还要附加Nr、prf(SK_pi,IDi')的值。

5 创新点总结

本文的创新点是根据IKEv2密钥协商的原理，并根据密钥交换过程的各重要环节、用户空间与内核空间的信息传递以及为用户提供方便简洁的IKEv2配置接口这几方面的要求，设计IKEv2协议实现框架、划分各功能模块。根据发起方与响应方角色的不同确定密钥协商的程序流程，利用状态转换数组来转换交换状态与处理函数，控制消息处理等等。

参考文献：

[1]Ari Huttunen, "UDP Encapsulation of IPsec ESP Packets", http://www.faqs.org/rfcs/rfc3948.html, 2005.1

[2]Richard Petersen,Linux技术大全,机械工业出版社,2002.1

[3]Carlton R.Davis,IPsecVPN的安全实施，清华大学出版社，2002.1

[4]林永和.基于IP技术的端对端通信网络安全模型分析设计[J]微计算机信息，2005，10-3:1-2

作者简介：杨小劲：男，1969-，籍贯：江西南昌，桂林航天工业高等专科学校计算机系讲师，主要研究方向：数据库应用技术、网络信息安全；Email: yxjbuaa@sohu.com;刘建华：男，1972-，籍贯：湖南衡阳，桂林航天工业高等专科学校计算机系讲师，硕士，主要研究方向：计算机图形图像处理、网络信息安全；E-mail: ljh101574@sohu.com

(541004 桂林 桂林航天工业高等专科学校计算机系) 杨小劲 刘建华

(Guilin College of Aerospace Technology, Guilin 541004) Yang,Xiaojin Liu,Jianhua

通讯地址：(541004 桂林航天工业高等专科学校计算机系) 杨小劲

(投稿日期:2006.1.5) (修稿日期:2006.2.20)

(接111页)模式，增强了系统的可扩展性。

参考文献：

[1]巫世晶著.设备管理工程.北京:电力出版社,2005.1

[2]甄镭编著..NET与设计模式.北京:电子工业出版社,2005

[3](美)Christian Thilmany著..NET模式:架构、设计与过程.北京:中国电力出版社，2005,4,陈永强,谢维成,李茜编著.SQL Server数据库企业应用系统开发.北京：清华大学出版社，2004

[5]梅中辉，经亚枝..Net中的数据访问技术-ADO.NET[J].微计算机信息,2003,1:70

作者简介：夏晖，男，1980年生，杭州，汉，硕士研究生，研究方向：Web Services与数据仓库，E-mail:wukong1106@sohu.com;董平，女，副教授，北京科技大学，硕士生导师；苏力萍，女，高级工程师，北京科技大学，硕士生导师。

Biography:XIA Hui, male, born in 1980, Hangzhou, Han nationality, master, research interest includes Web Service and Data Warehouse

(100083 北京海淀 北京科技大学信息学院)夏晖 董平 苏力萍

(School of Information, Beijing University of Science and Technology, Beijing 100083, China)Xia,Hui Dong,Ping Su,Liping

通讯地址：(100083 北京海淀 北京科技大学信息学院102信箱)夏晖

(投稿日期:2005.12.18) (修稿日期:2006.1.20)

技术创新