

文章编号:1001-9081(2005)12-2772-02

利用安全协处理器加速实现 IKEv2 协议

张玲玲,潘雪增,崔玉增

(浙江大学 计算机科学与技术学院,浙江 杭州 310027)

(bearlinglg@yahoo.com.cn)

摘 要:通过对比因特网密钥交换协议 IKEv2 与 IKE 的不同之处,分析研究了 IKEv2 在实现复杂度,降低延迟方面的优越性。简要介绍了 IKEv2 的消息交换,各种密钥的生成过程,并提出了一种基于安全协处理器硬件加速功能的 IKEv2 的设计和实施方案,它在计算各类密钥,会话消息的加解密,完整性校验等方面具有较快的处理速度。

关键词:IKE;IKEv2;安全协处理器

中图分类号:TP393.08 **文献标识码:**A

Accelerating implementation of IKEv2 by using security coprocessor

ZHANG Ling-ling, PAN Xue-zeng, CUI Yu-zeng

(College of Computer Science and Technology, Zhejiang University, Hangzhou Zhejiang 310027, China)

Abstract: Comparing the difference between IKEv2 and IKE, the advantages of IKEv2 on the complex of the implementation and the low delay were analyzed. The message exchange and the generation of various keys of IKEv2 was introduced, an implementation approach of IKEv2 using the security coprocessor were proposed. This implementation can accelerate the process of key generation, message encryption and integrity verify check.

Key words: IKE; IKEv2; security coprocessor

0 引言

因特网密钥交换协议 IKE (Internet Key Exchange) 是由 IETF 制定的密钥交换协议,在通信双方进行 IPsec 的处理过程中,对双方身份进行鉴别,同时进行安全策略的协商,以及处理会话密钥的交换。由于 IKE 是由另外三种协议 (ISAKMP、Oakley 和 SKEME) 混合而成的一种协议,其实现相当复杂。IKE 第一版设计的复杂性导致其成为了整个 IPsec 系统速度的瓶颈。为此,IETF 提出了 IKEv2 第 17 号草案,其正式的 rfc 文档也将在不久后推出。

本文通过对两个版本 IKE 实现方法的比较,分析了 IKEv2 比版本一在实现的简洁性,低延迟性上的优势,同时提出了一种在安全协处理器中来实现 IKEv2 硬件加速的方法,从而进一步提高 IKE 实现的速度。

1 IKEv2 的特点

为了使 IKE 的实现效率得到提高,简化实现的复杂度,IKEv2 对原有版本进行了以下几个方面的改进。

1.1 单一文档的定义

IKEv2 将整个 IKE 协议的定义放在一个单一的文档中,这个文档代替了原有的 RFC 2407,2408 以及 2409,并且还包含了后来对 IKEv1 的各种修改,比如对 NAT 穿越,可扩展的认证,以及远程地址获取等的支持。

1.2 简化 IKE 的会话消息交换

在 IKE 第一版本中,对消息交换的定义非常复杂。为了使得 IKE 的定义更加简洁,实现的速度更快,第二版本将原来 IKE 第一阶段的 8 种不同的初始化交换简化为一种交换方

式。并且将原先在主模式 (Main Mode) 下需要的 6 条消息简化为 4 条消息。不仅如此,它还将原版本中第二阶段快速交换模式的 3 条消息简化为 2 条。

1.3 降低 IKE 的延时

在 IKEv2 的初始化交换中,由于通信双方只需要两轮交换 (即 4 条消息),降低了实施 IKE 的时间。同时,由于 IKEv2 在初始化交换完成后就能建立起第一个 Child SA (如 IPsec SA),如果用户程序只需要新建一个 IPsec SA 的话,那么就根本不需要再进行第二阶段的为创建 Child SA 而发起的交换,这样就减少了消息交换的次数,从而进一步降低了延迟。

当然,IKEv2 还在提高安全性等方面也作了一些改进工作,但由于本文主要是对如何提高 IKE 实现效率的探讨,所以在此没有单独提出来分析。

2 IKEv2 的消息交换过程

2.1 初始化消息交换

表 1 初始化交换

Initiator		Responder
1	HDR, SAi1, KEi, Ni	=>
2		HDR, SAR1, KEr, Nr, [CERTREQ]
3	HDR, SK {IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, SAi2, TSi, TSr}	=>
4		HDR, SK {IDr, [CERT,] AUTH, SAR2, TSi, TSr}

收稿日期:2005-06-15;修订日期:2005-09-08

作者简介:张玲玲(1981-),女,四川德阳人,硕士研究生,主要研究方向:网络安全;潘雪增(1942-),男,浙江台州人,教授,博士生导师,主要研究方向:网络信息安全、SOC;崔玉增(1969-),男,浙江杭州人,讲师,硕士,主要研究方向:网络信息安全。

初始化交换阶段有两组请求—响应对,共 4 条消息,见表 1。

2.1.1 IKE_SA_INIT

第一组请求—响应对叫做 IKE_SA_INIT,作用是双方协商 IKE_SA 的加密算法(SA payload),交换 nonce 值(N payload),以及交换一次 Diffie-Hellman 值(KE payload)。前两条消息结束后,就建立起了 IKE_SA,它用来对随后的消息交换,IPSec SA 的建立进行保护。

前一对消息结束后,通信双方就可以根据交换的信息,各自独立地计算出所建立的 IKE SA 的种子密钥(SKSEED),并由其衍生出用于各种用途的密钥,计算方法如下所示:

$$\begin{aligned} \text{SKSEED} &= \text{prf}(\text{Ni} \parallel \text{Nr}, g^i r) \\ \{\text{SK}_d \parallel \text{SK}_a \parallel \text{SK}_r \parallel \text{SK}_e \parallel \text{SK}_i \parallel \text{SK}_p \parallel \text{SK}_pr\} &= \text{prf} + \\ &(\text{SKSEED}, \text{Ni} \parallel \text{Nr} \parallel \text{SPi} \parallel \text{SPNr}) \end{aligned}$$

其中,SK_e用于对随后的 IKE 消息进行加密,SK_a用于为随后的 IKE 消息保障数据的完整性以及对数据源的身份进行验证。SK_p在建立 AUTH 载荷的时候会用到。SK_d用于为 IPSec 衍生出加密的材料。而后缀 i,r 分别表示对初始化方和响应方发出的消息使用各自相对应的密钥。prf 是一个伪随机函数,通常是协商好的散列函数的一个 HMAC 版本。

2.1.2 IKE_AUTH

第二组请求—响应对叫做 IKE_AUTH,作用是通过传送 AUTH 载荷对双方身份进行验证,并建立起第一个 Child_SA,也就是真正的 IPSec SA。从这两条消息开始,随后的消息都要通过上一组交换产生的 SK_e,SK_a进行加密和完整性校验。其中 AUTH 载荷的内容是对 IKE_SA_INIT 中的两条消息进行签名后的结果。

2.2 创建 Child_SA 交换

表 2 创建 Child_SA 交换

	Initiator		Responder
1	HDR, SK {[N], SA, Ni, [KEi], [TSi, TSr]}	=>	
2		<=	HDR, SK{SA, Nr, [KEr], [TSi, TSr]}

我们可以利用初始化交换阶段生成的一个 IKE_SA 来生成多个 Child_SA。当通信双方需要创建多个 IPSec SA 时,就可以通过这两条消息交换来实现,如表 2 所示。任何一方都可以首先发起请求。在这个过程中,双方也会各自独立计算出 Child_SA 的密钥材料,方法如下所示:

$$\text{KEYMAT} = \text{prf} + (\text{SK}_d, g^i r(\text{new}) \parallel \text{Ni} \parallel \text{Nr})$$

IPSec SA 中需要用到的加密密钥,MAC 计算密钥都可以根据密钥大小按顺序由 KEYMAT 中取得。

2.3 信息交换

通信双方在密钥协商期间,需要传送控制消息,告知对方发生的错误或通知某些事件。为了完成这些操作,IKEv2 定义了信息交换。信息交换中的消息包含了一个或多个通知载荷、删除载荷或配置载荷。

3 利用安全协处理器实现 IKEv2

3.1 系统设计目标

- (1)基本上实现 IKEv2 协议;
- (2)系统使用方便、界面友好、配置和管理简单灵活;

(3)利用安全协处理器来加速密钥的生成,消息的处理,降低延迟。

3.2 安全协处理器

从 IKEv2 的消息交换流程可以看到,在整个消息交换,包括 IKE_SA 以及 Child_SA 建立的过程中,通信双方都需要根据自身生成的一些参数,以及对方传递过来的一些参数来进行很多复杂的计算,例如各种密钥的衍生,对消息的加解密和完整性校验,以及用于对双方身份进行验证的 AUTH 载荷的计算等。这些计算如果完全依靠软件来完成将是一件非常耗时的工作,它将大大地增加 IKE 的延时。而解决的办法就是用硬件来代替软件进行这些操作,实现硬件加速的功能,从而降低延时。这里所用到的硬件就是安全协处理器。

3.2.1 安全协处理器的作用

安全协处理器实际上起到的就是硬件加速的作用。它可以代替软件来实现一些安全通信协议,如 IPSec, PPTP, SSL, IKE 等。目前,要在网络硬件设备上加入安全功能,其中最重要的方法就是用一个安全协处理器和一个网络处理器或者通用处理器一起工作。安全协处理器负责系统中与安全性相关的任务,允许非安全协处理器去完成主要的系统功能。这种功能上的分离简化了设计流程并且提高了系统性能。

3.2.2 Hifn 公司的 HIP 系列芯片

下面,以 Hifn 公司生产的 HIP 系列芯片为例,我们来看看它是如何实现 IKEv2 硬件加速的功能的。图 1 显示了它的整个结构。安全协处理器通过 PCI 总线与主机间进行通信。HIP 芯片拥有自己的 SDRAM。主机将要处理的数据以及相关的命令参数通过 PCI 总线传送到 SDRAM 中,HIP 芯片再根据命令对传入数据进行相关的操作,对于数据包的加解密,MAC 计算,以及压缩解压等操作会在包处理引擎中完成,而各种公共密钥的操作则在公钥计算处理器中完成。同时,安全芯片还可以根据用户需要通过随机数生成器产生随机值。最后,将输出再通过 PCI 送给主机。

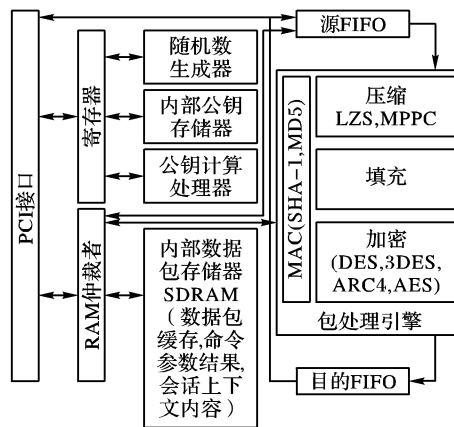


图 1 芯片功能结构

Hifn 为了使主机上的用户程序方便地使用 HIP 芯片的功能,实现它们间的通信,还提供了一套软件开发包 SDK (Software Development Kit)。SDK 用来控制和管理 HIP 芯片对数据包处理的过程,以及协调主机和 HIP 芯片间的协处理关系。SDK 运行在主机上的 CPU 上。

3.3 系统功能模块介绍

IKEv2 的实现可以分为以下几个模块,如图 2 所示。

(1)IKEv2 界面管理模块,负责与用户的交互,配置一些相关信息参数。

(下转第 2786 页)

$$1.358\cos(1.00323\sqrt{r}) + 0.742984 \quad (6)$$

表 2 列出了各项的比较结果。

(2) 根据实例 2 的实际数据,改进 GEP 演化的较好模型为:

$$T = 1.20745x_2 \sqrt{1.56821\sin(1.16616 \sqrt{\ln(x_2)})/x_5 + 1.54341\sin(1.31856x_2\sin(x_1) + x_3)/x_5 + 0.894467z + 1.40203 \times 10^{x_2/x_3\sin(x_3)}/10^{x_5} + 0.888907 \sqrt{\cos(\sin 2x_5 \times x_6(\sin(x_5) - x_5 - x_6))} \quad (7)$$

表 3 列出了各项的比较结果。

由表 2 和表 3 可以看出,改进 GEP 建模所得到的结果除了少数几个相对误差比 GP-GA 和单纯 GEP 得到的稍大一些以外,其余样本的相对误差均比单纯 GEP 所得模型计算结果的相对误差要小,稳定性高,可靠性好。

5 结语

针对传统的解决建模问题的方法中存在的困难与不足,根据 GEP 具有染色体简单、线性和紧凑、易于进行遗传操作和郭涛算法^[5]的搜索高效性、收敛的全局性等优点而采用改进的 GEP 方法进行演化建模。它不要求编程人员对具体问题作深入的了解,也不要求编程人员事先规定好所求的目标函数的结构。通过实例的计算与分析可知,采用改进的 GEP 方法进行演化建模,可以自动找出数据内部隐含的关系,获得更能反映实际数据的复杂函数,所得到的结果优于 GP 和单

纯 GEP 得到的结果。

参考文献:

- [1] 潘正君,康立山,陈毓屏. 演化计算[M]. 北京:清华大学出版社,1998.
- [2] 周明,孙树栋. 遗传算法原理及应用[M]. 北京:国防工业出版社,1999.
- [3] FERREIRA C. Gene Expression Programming: A New Adaptive Algorithm for Solving Problems[J]. Complex Systems, 2001, 13(2): 87-129.
- [4] FERREIRA C. Gene Expression Programming in Problem Solving [A]. Invited tutorial of the 6th Online World Conference on Soft Computing in Industrial Applications[C]. 2001. 10-24.
- [5] 郭涛,康立山,李艳. 一种求解不等式约束下函数优化问题的新算法[J]. 武汉大学学报(自然科学版), 1999, 45(5): 771-775.
- [6] 苏小红,杨博,王亚东. 基于进化稳定策略的遗传算法[J]. 软件学报, 2003, 14(11): 1863-1868.
- [7] 唐丽珏,李森,张建. 混合 GP-GA 用于信息系统建模预测的研究[J]. 计算机工程与应用, 2004, 40(25).
- [8] 李曲,蔡之华,朱莉,等. 基因表达式程序设计方法在采煤工作面瓦斯涌出量预测中的应用[J]. 应用基础与工程科学学报, 2004, 12(1): 49-54.
- [9] 唐常杰,张天庆,左吉力,等. 基于基因表达式编程的知识发现——沿革、成果和发展方向[J]. 计算机应用, 2004, 24(10).

(上接第 2773 页)

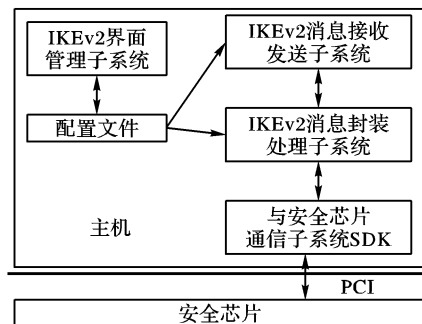


图 2 IKEv2 的功能模块和接口

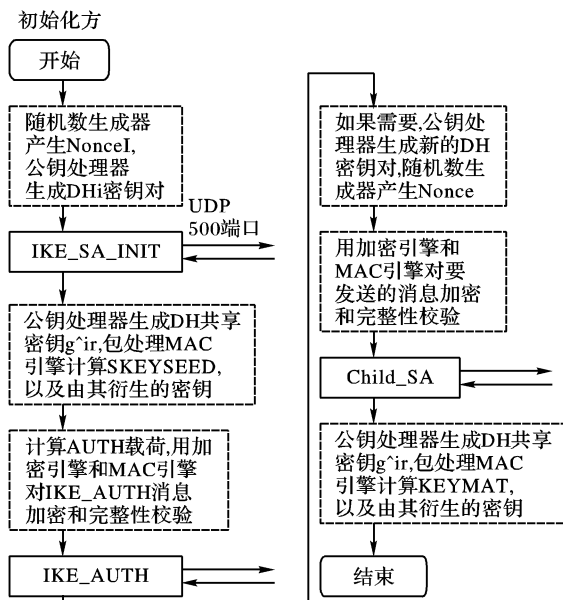


图 3 IKEv2 的实现流程

(2) IKEv2 消息发送接收模块,负责接受发送 IKE 消息。

(3) IKEv2 消息封装处理模块,根据各种载荷的格式来封装或读取相应的消息内容。

(4) IKE 主机与安全芯片通信模块 SDK,负责主机与安全芯片的协调工作。

3.4 IKEv2 的实现流程图

下面以初始化方为例,以流程图的方式介绍利用 IKEv2 建立新的 IPsec SA 的整个过程,如图 3。响应方的实现方法是类似的。图 3 中,虚线框表示 HIPP 安全芯片上实现的功能。实线框表示 Host 上实现的功能。横向的箭头表示与响应方通信。

4 结语

IKEv2 同第一版本相比,实现上更加简洁,速度更快。但是如果仅仅依靠软件来实现,在进行密钥的计算,消息数据包的处理等复杂运算的时候,仍然会耗费大量的时间。为了更有效地降低延时,提高效率,可以利用安全协处理器来实现硬件加速。

参考文献:

- [1] KAUFMAN C. Internet Key Exchange(IKEv2) Protocol[EB/OL]. <http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ikev2-17.txt>, 2004.
- [2] HARKINS D. The Internet Key Exchange(IKE)[EB/OL]. <http://www.faqs.org/rfcs/rfc2409.html>, 2005.
- [3] Hifn Inc. HIPP7815_7855_Device_Specification[Z]. <http://www.hifn.com/products>, 2004.
- [4] Hifn Inc. HIPP_SDK_API_Guide[Z]. <http://www.hifn.com/products>, 2004.