文章编号:1001 - 9081(2006)04 - 0824 - 03

密钥交换协议性能测试研究

孙卫平,尹 霞, 施新刚
(清华大学 计算机科学与技术系,北京 100084)
(swp03@csnet1.cs.tsinghua.edu.cn)

摘 要:提出了一种针对密钥交换(IKE)协议性能的黑盒测试方法,该方法基于自主开发的协议集成测试系统平台。针对 IKE 协议的特点设计了灵活的测试集,并对主机上的 IKE 实现进行了测试,分析了各种参数对 IKE 性能的影响。该方法可用于测试多种不同设备上的 IKE 实现。

关键词:密钥交换协议;性能测试;协议集成测试系统
中图分类号: TP393.08 **文献标识码**:A

Research on performance testing of IKE protocol

SUN Wei-ping, YIN Xia, SHI Xin-gang
(*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084, *China*)

Abstract: A black box testing method aiming at IKE(Internet Key Exchange) protocol performance was proposed, which was based on the self-developed platform of protocol integrated test system. Flexible test suite was designed according to characteristics of IKE, and the IKE performance testing was done on one actual host, all kinds of parameters' impact on IKE performance was analyzed. This test method is applicable to IKE tests in different devices.

Key words: Internet Key Exchange(IKE) protocol; performance test; Protocol Integrated Test System(PITS)

0 引言

互联网安全协议(Internet Protocol Security, IPSec)[1]作为 IP 层安全协议,能够提供机密性、完整性、访问控制和 IP 包的数据源认证功能,IPSec 在下一代互联网中是强制实现的。互联网密钥交换(Internet Key Exchange,IKE)协议[2]实现自动的密钥协商和管理功能,是 IPSec 协议广泛部署和应用的基础,其性能优劣会对 IPSec 产生重要影响。同时网络产品的性能已经变得与功能同等重要,人们在采用各种方法提高网络产品性能的同时,也对性能测试给予了高度重视。

安全性的增强往往以牺牲性能为代价,但无论是用户还是厂商,在要求安全产品的安全性同时,对性能要求也越来越高,性能将作为产品选型的重要衡量标准,因为它们直接影响服务的质量。目前国外对 IKE 协议测试仅限于一致性测试,国内也还未发现对 IKE 协议测试的进行研究的文献,因此对于密钥交换协议进行性能测试研究具有一定的现实意义。

本文是在研究了网络设备性能测试规范[3,4]后,针对 IKE 协议进行的性能测试。简要介绍了 IKE 协议并分析了测试需求,提出了在自主开发的协议集成测试系统(Protocol Integrated Test System, PITS)平台上进行 IKE 协议性能的测试方法,对 IKE 协议进行了性能测试,分析了密码算法、Diffie-Hellman[5](简称 DH)组等参数对 IKE 性能的影响。

1 IKE 简介与测试需求分析

1.1 IKE 协议简介

IKE 协议作为互联网密钥交换协议,解决了在不安全的网络环境中安全地建立和更新共享密钥的问题。该协议能够自动协商各种安全参数,包括加密算法、认证算法、DH 组、安全协议(如 IPSec)、安全协议的工作模式(如隧道)和生存时间等(一套这些参数称为一个提议),并生成安全关联(Security Association,SA)。

IKE 使用了 ISAKMP(Internet Security Association and Key Management Protocol)[6]协议的阶段概念,包括两个阶段:第一阶段为 IKE 本身协商建立一个安全通道(即协商建立 IKE_SA),并对该通道进行认证,为双方后续的 IKE 通信提供机密性、完整性以及消息源验证服务;第二阶段使用已经建立的 IKE_SA 为 IPSec 协商 SA。在两个阶段中可以使用多种不同的模式实现安全关联协商、密钥材料交换、身份认证、会话密钥生成以及控制信息传输等功能。下面以预共享密钥认证的主模式交换和快速模式交换为例,简单介绍 IKE 协议的信息交换过程:

主模式:

1)I→R:报头,SA_i

2)R→I:报头,SA_r

3)I→R:报头,KE_i 载荷,Nonce_i 载荷

4)R→I:报头,KE_r 载荷,Nonce_r 载荷

5)I→R:报头 *,ID_i 载荷,HASH_i 载荷

6)R→I:报头 *,ID_r 载荷,HASH_r 载荷

快速模式:

7)I→R:报头 *,HASH(1),SA,Nonce_i 载荷[,KE 载荷][,IDci,IDcr]

8)R→I:报头 *,HASH(2),SA,Nonce_r 载荷[,KE 载荷][,IDci,IDcr]

9)I→R:报头 *,HASH(3)

收稿日期:2005 - 10 - 27;**修订日期**:2005 - 12 - 20
基金项目:国家自然科学基金资助项目(90104002);国家 973 规划资助项目(2003CB314801)
作者简介:孙卫平(1971 -),男,辽宁锦州人,硕士研究生,主要研究方向:密钥交换协议测试; 尹霞(1972 -),女,天津人,副教授,博士,主要研究方向:高速网络体系结构、网络协议测试; 施新刚(1981 -),男,江苏常州人,硕士,主要研究方向:网络协议测试.

其中 i 表示发起方,r 表示响应方,[ ]中为可选载荷项,*表示其后的载荷被加密。

从上面的交换过程可以看出,第一阶段的主模式总是用六条消息、三个交换来完成密钥交换。第一个交换使用第 1、2 条消息完成策略协商,并完成一次 cookie 交换;第二个交换使用第 3、4 条消息完成一次 DH 交换和 nonce 交换,主要使用 DH 算法和哈希算法来生密钥生成密钥;第三个交换双方使用第 5、6 条消息完成身份验证和数据源验证。第二阶段的快速模式交换必须在第一阶段完成后才能进行,其目的是为其他协议协商安全关联。

1.2　测试需求分析

IKE 系统性能测试中最重要的两个指标(参数)是通道容量和协商效率(时间性能)。通道容量是 IKE 设备可以同时维护 SA 的最大数量,常被厂商用以区别自己产品与其他同类竞争产品,该参数的研究备受关注。所谓协商效率,也就是 IKE 完成第一阶段和第二阶段协商建立相关 SA 的延迟时间,这对于拥有众多用户的大型 VPN 网关来说,协商效率与通道容量同等重要,但是该参数却常常被忽视。本文主要实现 IKE 协商效率的测试,不但需要研究测试方法,还需要研究加密算法、DH 组等参数对协商效率的影响。

从预共享密钥的主模式交换过程来看,该交换使用了 DH 公钥算法和对称密钥算法 DES 或 3DES[8],以及哈希验证算法 MD5[9] 或 SHA-1[10],这些加解密算法和哈希运算需要大量的计算,而该交换中的三次模幂运算的计算量更大。使用快速模式的第二阶段交换,也可能含有一个模幂运算(当使用完美前向保密时)。由于模幂运算涉及大数算法,这些计算带来的开销将对 IKE 的协商效率产生重要影响,尤其是当 IKE 同时协商多个 SA 时将会明显地增加设备的处理负担,因此研究 IKE 的协商效率具有一定的实用价值。

2　测试方案设计

2.1　测试平台

IKE 性能测试平台采用自主开发的协议测试集成系统 PITS,它是一个分布式的测试系统,可以进行测试集编辑及转换、测试选择及参数设定、测试管理及测试序列提取、测试执行以及基本互连测试、能力测试、动态特性测试、测试结果记录和分析等。PITS 是一个通用型的测试系统,它不但可以进行协议的一致性测试,还可以进行协议的互操作性测试和性能测试。在协议测试过程中,测试执行模块 (Test Execution, TE)统一控制与被测设备进行交互,读取并解释执行测试例,根据测试事件向特定的参考实现(Reference Implementation, RI)发送命令,指令 RI 与被测设备进行交互数据的发送与接收,并记录数据发送与接收的时间参数,同时通过消息队列机制将收到的数据提交给 TE。在 PITS 中,与被测协议相关的测试动作由 RI 来完成,使得 TE 对测试例的解释执行与具体协议无关,这种结构化设计使得协议测试只需要将精力放在测试集的设计、组织和参考实现的编写。

2.2　测试方案

本文借助集成测试系统 PITS,采用黑盒测试方法对已经成为标准的 IKE 协议进行测试,从被测设备外部观察其表现,从而评估性能,主要侧重于对同一协议不同实现的性能比较。整个测试系统组成如图 1 所示。被测协议实现(Implementation Under Test,IUT)通过交换机与现有的集成测试系统 PITS 连接,测试程序的发送方和接收方都运行在 PITS 上,这样使发送方和接收方容易实现同步,便于时间测量。

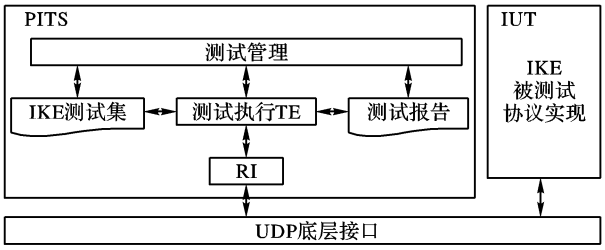

图 1　IKE 测试系统组成

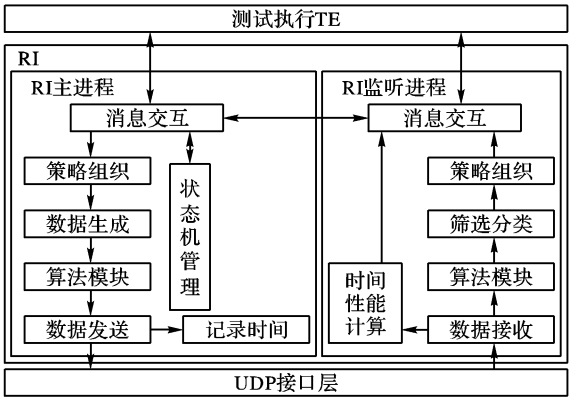

图 2　IKE 参考实现结构

从图 1 中可以看出 RI 是和 TE 紧密相关的模块,它在测试过程中将协助测试部件完成与具体协议相关的测试动作,主要是测试数据的收发,因此需要为不同的被测协议编写不同的参考实现。IKE 的参考实现 RI 逻辑结构如图 2 所示,它与 IKE 被测协议实现通过 UDP 协议进行通信,所需要完成的功能描述如下:

数据接收模块:侦听 UDP 端口,准备接收来自另外一个 IKE 协议实现的协商数据;

报文筛选模块:从数据接收模块接收数据,进行报文分类,即根据报文找到相应的 SA,然后转到策略组织模块中进行处理;

状态机管理模块:为每个 SA 维护一个测试过程中的状态机,存贮测试过程中的状态数据,同时对收到的数据根据状态机进行相应的处理;

策略组织模块:接收并反馈 TE 的要求和请求,对数据进行合法性分析,同时为 IKE、IPsec AH(Authentication Header)和 IPsec ESP(Encapsulating Security Payload)生成 SA;

数据生成模块:通过策略组织模块得到数据组织方式,将待发送的数据按照相应的要求进行格式化,组成相应的数据包;

数据发送模块:接收来自数据生成模块组织好的数据,同时调用算法模块,对数据进行加密、哈希等操作;

算法模块:提供各种密钥生成函数、生成和管理伪随机数(用于生成 nonce 和 cookie)以及管理 DH 公钥算法,完成数据的加密解密功能,实现认证和完整性保护功能;

时间性能计算模块:记录发送与接收数据包的时间,再配合网络平均延迟时间,计算协商延迟。

以测试系统作为发起方为例,描述测试过程如下:测试开始,RI 组织 IKE 协商数据包,其中可能涉及 cookie 生成、nonce 生成以及加密等操作,然后使用 UDP 将数据包发送给对等协商方,并开始计时(计为 Ts);等待被测试协议实现 IUT 发来的应答数据包,收到 IUT 应答数据包并计时(计为 Tr),经一

系列处理,可能涉及解密、检验合法性与完整性等,确认正确后,本轮协商完成;IUT 对本轮消息协商的处理时间 $Tp = Tr - Ts - Td$。其中:Td 为网络延迟时间,可以通过从测试系统 ping 被测设备得到。从前面的 IKE 密钥交换过程来看,对于 IKE 协商时间性能的测试,集成测试系统 PITS 既要充当协商的发起者(测试第 2、4、6、8、10 条消息时间延时),也要充当响应者(测试第 1、3、5、7、9 条消息时间延时)。

本文主要考察 IKE 的协商效率,即同一被测试协议实现使用不同的 DH 组、加密算法、哈希算法情况下 IKE 的时间性能。

2.3 测试集设计

集成测试系统可以让用户轻松地使用多种算法和其他参数的组合,这样可以测试各种因素对协商效率的影响。我们设计的测试集可以支持以下参数的组合:加密算法包括 3DES、DES、IDEA、Blowfish 和 CAST 等;DH 组包括 1、2、5、14、15、16、17 和 18 等;哈希算法包括 MD5、SHA-1 和 Tiger 等;验证方法包括共享密钥、RSA 签名和 DSS 签名等;提议的个数为 1、2、3、4 等。用户可以任意地使用上述参数的组合来生成测试例。

在集成测试系统 PITS 中,测试集的编写采用了树表结合的 TTCN[11] 表示法。目前在我们的测试系统 PITS 中已经实现对验证方法为共享密钥、提议个数为 1、两种加密算法(DES 和 3DES)、两种哈希算法(MD5 和 SHA1)以及三个 DH 组(1、2 和 5)的组合测试支持。表 1 只列出了哈希算法为 MD5 的 6 个测试例。

表 1 部分测试例

编号	测试目的
TC1	加密算法 DES,哈希算法 MD5,DH 组为 1 的时间性能测试
TC2	加密算法 DES,哈希算法 MD5,DH 组为 2 的时间性能测试
TC3	加密算法 DES,哈希算法 MD5,DH 组为 5 的时间性能测试
TC4	加密算法 3DES,哈希算法 MD5,DH 组为 1 的时间性能测试
TC5	加密算法 3DES,哈希算法 MD5,DH 组为 2 的时间性能测试
TC6	加密算法 3DES,哈希算法 MD5,DH 组为 5 的时间性能测试

3 测试结果分析

表 2 测试结果(时间单位:ms)

消息	测试例					
	TC1	TC2	TC3	TC4	TC5	TC6
1	2.085	2.232	2.454	2.668	2.341	2.572
2	2.065	2.752	2.134	2.018	2.051	2.022
3	39.07	85.447	470.105	40.288	85.04	468.897
4	49.161	102.244	611.118	50.89	102.782	611.651
5	13.785	26.896	156.554	13.911	26.768	153.422
6	1.153	1.265	1.821	1.179	1.361	1.731
7	3.385	3.516	3.504	3.571	3.612	3.606
8	3.052	3.222	3.211	3.275	3.304	3.307
9	1.107	1.337	1.284	1.431	1.356	1.361
10	1.155	1.151	1.138	1.164	1.156	1.151
总耗时	116.017	230.062	1253.323	120.395	229.771	1249.72

按照前面所讲的测试方法,对目前支持 IKE 协议实现的一款主机进行了两个阶段协商的协商效率测试。按照测试例将测试分为两组:测试系统作为发起者和响应者各一组,每组由 6 个测试例组成,其中测试例 TC1 ~ TC3 是加密算法固定为 DES、哈希算法固定为 MD5 的条件下,DH 组分别为 DH1、DH2 和 DH5;而 TC4 ~ TC6 是加密算法固定为 3DES、哈希算法固定为 MD5 的条件下,DH 组分别为 DH1、DH2 和 DH5。每个测试例执行 10 次,对测试结果取平均值,其测试结果数据如表 2 所示(表中的行是测试例 TC1 ~ TC6,列是 IKE 密钥协商过程中的 1 ~ 10 条消息)。

表 2 中的各项时间性能数据是去掉了网络延迟时间 Td 以后的绝对时间性能,而用户实际感觉到的时间是加上 Td 后的。在我们的软硬件环境下,Td 值经过测算约为0.6345ms,与 IKE 处理时间数量级相差比较大,说明网络延迟时间在 IKE 对外表现性能中的影响不是很大。

不同测试例在处理每条协商消息时所花费的时间是不同的,其变化趋势如图 3 所示。

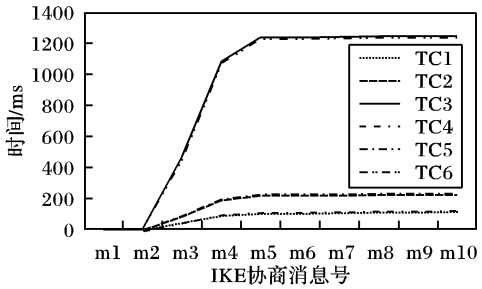

图 3 协商时间变化趋势

从表 2 和图 3 中可以看出:

1)消息 3、4、5 所花费的时间在整个协商中的比例是最大的,比例最小值为 87.9%,最大值为 98.8%,这主要是因为这三条消息的生成和处理都需要进行大数运算来生成密钥材料,因此如果能有效地减少这三条消息的生成和处理时间将显著改善 IKE 协议的时间性能;

2)使用不同 DH 组的测试例在时间性能上差异明显,如 TC2 的总协商时间大约是 TC1 的总协商时间的 2 倍,TC3 的总协商时间大约是 TC2 的总协商时间的 5.4 倍,这主要是因为使用不同的 DH 组来生成密钥材料(进行大数运算)所需的时间不同,使用大的 DH 组生成密钥材料需要更多的计算时间;

3)使用相同 DH 组的测试例在时间性能上差异不大,如 TC1 和 TC4、TC2 和 TC5、TC3 和 TC4 仅有几毫秒的差距,TC1 和 TC4 的差别是使用了不同的加密算法,由此我们可以看出加密算法对协议的时间性能影响不大;

4)使用大 DH 组的测试例在时间性能上明显劣于使用小 DH 组的测试例。使用大 DH 组的测试例会提供较高的安全性能,使用小 DH 组的测试例会提供较好的时间性能,IKE 协议实现需要在两者之间进行平衡。

4 结语

本文提出了一种基于自主研发的集成测试系统测试 IKE 协议性能的黑盒测试方法,详细描述了测试方法和步骤,研究了各种加密算法和 DH 组对 IKE 实现性能的影响,搭建了测试平台,完成了对一个 IKE 协议实现的测试实践,分析了各种参数对 IKE 性能的影响。这种方法的优点是测试环境构造快速方便,利用集成测试系统的集成测试环境编写测试例,再借助编写的底层扩展参考实现就可完成测试;不但可以测试包含 IKE 协议实现的主机系统,而且还可以测试路由器等不同IKE协议实现。进一步研究的工作包

文章编号:1001 - 9081(2006)04 - 0827 - 03

基于复合混沌系统的数字图像加密方法研究

赵雪峰[1],殷国富[2]
(1. 淮海工学院 计算机科学系,江苏 连云港 222005; 2. 四川大学 制造科学与工程学院,四川 成都 610065)
(snowpeak@hotmail.com)

摘 要:分析了现有图像加密方法的安全性,提出了一种改进的图像加密方法,将两套 Logistic 映射组合起来构成参数变化的双 Logistic 映射复合混沌系统,系统中的 Logistic 映射相互控制对方的 μ 参数,并产生两个混沌序列。然后用其中一个混沌序列对图像矩阵进行置乱,另一个混沌序列用于对图像信息进行异或加密。计算机仿真结果表明,该加密方法具有良好的加密效果,具有可行性,算法实现简洁,有较强的抗攻击和抗噪声能力。

关键词:混沌; Logistic 映射; 图像加密;信息安全
中图分类号: TP309.7 **文献标识码**:A

Research on digital image encryption method based on hybrid chaotic system

ZHAO Xue-feng[1], YIN Guo-fu[2]
(1. *Department of Computer Science, Huaihai Institute of Technology, Lianyungang Heilongjiang* 222005, *China*;
2. *College of Manufacturing Science and Engineering, Sichuan University, Chengdu Sichuan* 610065, *China*)

Abstract: The security of image encryption methods was analyzed, and improved method of image encryption named changing parameters and chaotic complex system of double Logistic-maps was presented, which consisted of two sets of Logistic-maps. In this system, the two Logistic-maps can control the parameter μof each other and thus produce two chaotic sequences. Then one of the sequences is used to disturb the image matrix, while the other sequence to encrypt the image. The computer simulation results proved that the method is easy, feasible, and effective in encryption. Besides, this method is also well against attack and noises.

Key words: chaos; logistic-map; image encryption; information security

0 引言

为了对图像信息进行保护,产生了各种图像加密技术,如图像像素置乱的图像加密、基于秘密分割和秘密共享的图像加密、基于现代密码学体制的图像加密, 以及基于混沌动力学体制的图像加密等[1]。

基于混沌力学体制的图像加密技术中,通常使用一维的 Logistic 映射,二维的 smale 映射和 Henon 映射[2],以及三维的 Lorenz 系统[3]。针对制造企业信息化系统安全建设的需要,本文提出了基于 Logistic 映射的双 Logistic 映射复合混沌系统,由两套 Logistic 映射组合起来构成。每套 Logistic 映射都能够通过自己产生的实数混沌序列,在某种有效策略的控制下来扰动另一套映射的参数。充分利用 Logistic 映射对参数敏感的特点,使得生成的实数混沌序列具有更大的随机性,以加强对图像的加密效果,保证图像信息的高安全性。

1 双 Logistic 映射复合混沌系统算法分析

1.1 混沌的定义及 Logistic 映射

混沌现象是在非线性动力系统中出现的确定性的、类似随机的过程,这种过程既非周期又不收敛,对初始值有极其敏感的依赖性,关且具有白噪声的统计特性。通过混沌系统对初始值和结构参数的敏感依赖性,可以提供数量众多、非相

收稿日期:2005 - 10 - 08;**修订日期**:2005 - 01 - 08 **基金项目**:四川省重点研究项目资助(03GG010-002)

作者简介:赵雪峰(1976 -),男,四川西充人,讲师,硕士,主要研究方向:计算机网络、信息安全、图形学及数字图像处理; 殷国富 (1956 -),男,四川成都人,教授,博士生导师,博士,主要研究方向:CAD/CAM、智能 CAD 与专家系统技术、CIMS、信息安全、网络环境下远程协同设计制造方法.

括:路由器和 VPN 网关中的通道容量测试,包括测试方法研究、以及加密算法、DH 组等参数对通道容量影响的研究。

参考文献:

[1] Security Architecture for the Internet Protocol, RFC2401[S].
[2] The Internet Key Exchange(IKE), RFC2409[S].
[3] Benchmarking Methodology for Network Interconnect Devices, RFC2544[S].
[4] Benchmarking Terminology for Network Interconnection Devices, RFC1242[S].
[5] DIFFIE W, HELLMAN ME. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, IT-22(6): 644 - 654.
[6] Internet Security Association and Key Management Protocol(ISAKMP), RFC2408[S].
[7] 吴建平, 陈修环, 郝瑞兵, 等. 基于形式化技术的协议集成测试系统——PITS[J]. 清华大学学报(自然科学版), 1998, 38(S1): 26 - 29.
[8] The ESP DES-CBC Cipher Algorithm, RFC2405[S].
[9] The MD5 Message Digest Algorithm, RFC1321[S].
[10] FIPS 180-1. Secure Hash Standard[S].
[11] ISO/IEC 9646-3. Information Processing Systems, Open System Interconnection, OSI Conformance Testing Methodology and Framework. Part 3: The tree and tabular combined notation[S].