Journal of Computer Applications
计算机应用,2013,33(10):2835-2837,2864
ISSN 1001-9081
CODEN JYIIDU
2013-10-01
http://www.joca.cn

文章编号:1001-9081(2013)10-2835-03
doi:10.11772/j.issn.1001-9081.2013.10.2835

云计算环境下密钥协商协议的应用与改进

任 敏*
(无锡工艺职业技术学院 电子信息系,江苏 宜兴 214206)
(*通信作者电子邮箱 zmrwork@qq.com)

摘 要:为解决现有密钥协商协议在云计算环境下的适应性问题,深入分析云计算场景对密钥协商协议的安全需求,结合现有IKEv2协议的安全性能缺陷,采用puzzle机制、密钥材料及身份信息推迟传递等手段对IKEv2进行改进,提出了一种适应云计算网络环境的密钥协商协议IKE-C,有效提升了协议中响应者的抗拒绝服务(DoS)攻击能力,同时解决了中间人攻击导致发起者身份泄露的问题。还对两种协议的收敛时间进行了比较,仿真结果表明,在相同的网络规模下,IKE-C协议的收敛时间低于IKEv2,并且随着客户端数量的增加,其优势逐渐明显。

关键词:云计算;密钥交换;IKEv2;拒绝服务;发起者身份隐藏
中图分类号:TP393.08 **文献标志码**:A

Application and improvement of key agreement protocol in could computation environment

REN Min*
(*Department of Electronic Information, Wuxi Institute of Arts and Technology, Yixing Jiangsu 214206, China*)

Abstract: By analyzing security requirement of key agreement in cloud computation environment and the defect of security performance for IKEv2, an improved key agreement protocol IKE-C was proposed in order to solve the problem of adaptability of the existing key agreement protocols in cloud computation environment. Puzzle, key material and delaying the transmission of ID were adopted in order to promote the ability of anti-DoS (Denial of Service) attack and overcome the problem that sender identity would be leaked because of man-in-the-middle attack. Performance comparison was conducted in the paper. The simulation result indicates that IKE-C gets shorter convergence time than IKEv2 with the same network scale, and performance superiority is more obvious as clients are increasing.

Key words: cloud computing; key exchange; Internet Key Exchange version 2 (IKEv2); Denial of Service (DoS); initiator ID privacy

0 引言

当前阻碍云计算大规模部署应用的主要问题是其安全性[1-2]。云计算使得数据与计算资源高度集中,原有的固定安全边界变得模糊,面临一系列安全问题,包括终端的合法可信与自身安全、终端与云之间的数据传输安全、用户与用户间/用户与运维者间的数据隔离与隐私保护、海量数据的存储安全等[3]。针对云计算的一系列安全问题,当前尚无得到广泛认可的安全体系,缺乏实用化的技术手段和解决方案。

无论未来的云计算安全体系如何构建,网络传输加密将是其中必不可少的一环。云计算将原来在本地计算机(PC)中完成的计算、存储等工作远程化、集中化、虚拟化。因此,原本在PC内运行的操作控制指令、用户业务数据等信息必须在本地终端和远端的云之间通过不可信、不可控的Internet进行远程传输。为了使云计算达到至少与PC同等的安全性,防止数据在传输过程中发生泄露,网络传输加密将是必不可少的安全手段。

IPSec[4]是当前主流的网络传输加密体制,也将是云计算安全体系中首选的传输加密体制。然而其原有的互联网密钥协商协议[5](Internet Key Exchange,IKE)以及互联网密钥协商协议第二版[6](Internet Key Exchange version 2,IKEv2)存在着一定的不足,国内外学者提出了大量的优化改进方案。文献[7]在简要介绍IKEv2密钥交换协议的基础上,对IKEv2密钥协商机制的安全性进行了分析,针对其扩展认证协议(Extended Authentication Protocol,EAP)交换繁琐且身份信息易暴露、假冒证书攻击和安全隧道非授权访问等安全问题,分别提出了相应的优化建议;文献[8]针对IKEv2协议的EAP认证方式问题,引入了混合认证的方案,来克服数字证书或预共享密钥单独使用时所存在的不足,增强了协议的灵活性和可扩展性;文献[9]对协议抵御中间人攻击、拒绝服务(Denial of Service, DoS)攻击和完美前向保密三方面进行了分析,并提出了相应的改进方法。尽管国内外学者提出了大量的优化改进方案,但在密钥协商协议与云计算技术体制结合方面的研究几乎没有。

本文研究的目的是针对云计算应用环境对密钥协商协议安全和性能的要求,以及现有IKEv2协议的安全缺陷,在现有协议基础上进行分析与改进,提出一种能够同时兼顾效率和安全的云计算专用密钥协商协议(Internet Key Exchange-Cloud computing,IKE-C)。

1 IKEv2协议缺陷分析

1.1 IKEv2协议

IKE是互联网工程任务组(Internet Engineering Task Force,IETF)专门为IPSec制定的密钥协商协议,用于完成IPSec双方的身份认证和密钥协商。但IKE存在一些明显的缺陷,包括报文来回次数多,易受DoS攻击;包含多种认证方

收稿日期:2013-04-12;**修回日期**:2013-06-06。
作者简介:任敏(1977-),女,江苏宜兴人,副教授,硕士,主要研究方向:网络安全、嵌入式系统控制。

式和交换方法,协议过于复杂,不易理解;可选项冗余等。针对IKE存在的上述问题,出现了IKEv2和快速密钥协商协议[10](Just Fast Keying,JFK)等新型的密钥协商协议,其中IKEv2取代IKE成为了IPSec的密钥协商标准。

IKEv2在保留IKE两个阶段基本思想的基础上进行了若干改进,包括减少来回报文数,第一阶段由6条变为4条,第二阶段由3条变为2条;减少认证方式,仅保留预共享密钥和数字签名两种身份认证方式,取消了公钥加密、改进的公钥加密两种方式;取消了部分冗余项;针对DoS攻击、中间人攻击、身份信息泄露等问题进行了安全性增强;交互的请求/响应报文一一绑定,并引入超时重传机制,提高协议可靠性;增加了对EAP、网络地址转换(Network Address Translation,NAT)、远程地址获取等新功能。

1.2 IKEv2协议缺陷分析

1)易受抗DoS攻击。

IKEv2通过无状态cookie机制具有一定程度的抗DoS攻击能力。其基本思想是将cookie值与发起者IP地址绑定,并通过第一轮报文交互验证cookie中显示的IP地址与发起者IP的一致性,排除伪造大量报文发起的DoS攻击。但对于分布式DoS攻击,由于攻击者控制的大量僵尸主机拥有真实IP地址,能够通过一致性验证,使得cookie抗攻击机制失效。

2)报文来回数量较多,计算量较大,整体效率较低。

3)受中间人攻击导致双方身份信息泄露。

保证参与协商双方身份私密性的最直接办法就是为报文中的身份信息提供加密保护。IKEv2协议中,发起者和响应者的身份信息分别在报文3和报文4中以密文形式交换。但由于报文2没有经过加密或认证,可能受到中间人攻击,攻击者伪装成响应者与其交换密钥参数,形成共同临时密钥。尽管在收到报文4后发起者通过身份验证能够发现攻击者的存在,但其身份信息已经泄露。

2 IKE-C协议设计

2.1 云计算环境特点

IKE-C协议的总体设计目标是在主流的IKE协议基础上进行改进,使其适应云计算环境,并克服原有的主要缺陷。

本文通过分析云安全联盟(Cloud Security Alliance,CSA)的"Security Guidance for Critical Areas of Focus in Cloud Computing"[11]、欧洲网络与信息保障局的"Cloud Computing Information Assurance Framework"[12]等相关文献资料,总结了云计算环境的特点并提取了对密钥协商的影响,具体包括:

1)C/S架构。

云计算环境下终端与"云"形成客户端服务器架构,相应地终端侧IPSec设备与"云"侧IPSec设备也将形成客户端服务器架构,进行一对多通信。一台"云"侧IPSec设备需要与多台,甚至是海量的终端侧IPSec设备进行协商,对其性能提出了较高的要求,面对DoS攻击的威胁较大。一旦"云"侧IPSec设备被攻击崩溃,则整个云计算体系无法正常运行。

同时,在C/S架构下,服务器的身份信息是公开的,这是客户端与服务器通信的前提。因此在该架构下的密钥协商机制中,没有必要为服务器端IPSec设备提供身份隐藏保护。

2)瘦客户端。

瘦客户端是随云计算出现的终端发展趋势。云计算场景下,终端本地的计算、存储等任务大量转移到云端,客户端上无需强大的处理能力,只要能支撑基本的运行环境即可。瘦客户端能够很好地适应小型化、移动化等终端使用场景,相应的IPSec设备也将变瘦,处理能力有限。

3)网络质量良好。

云计算安全联盟和欧洲网络与信息保障局的相关文献[11-12]显示,云计算对网络质量提出了较高的要求,包括高带宽、低时延、低误码率等,若不能及时有效地在终端和云之间完成操作控制指令及用户业务数据的传输,云计算高效、低成本的优势就无法体现,将失去存在的基础。因此,在构建云计算安全体系,考虑IPSec的密钥协商机制时,可以将"网络质量良好"作为一个前提条件。在这样的条件下,IKE协议报文交互来回过多不再成为无法接受的缺陷。

2.2 IKE-C协议设计目标

根据前文中分析的现有协议缺陷及云计算环境对密钥协商机制的影响,提出如下设计目标:

1)降低服务器端(响应者)在第一轮报文交互中的资源消耗,提高响应者抗DoS攻击能力;

2)完美前向安全,防止服务器端一点被攻破造成大范围安全影响;

3)减小对客户端(发起者)计算资源及存储资源的开销,降低协议处理导致的性能负担;

4)减少协议全过程的公钥算法使用,降低计算资源消耗;

5)认证双方身份;

6)隐藏客户端身份。

2.3 IKE-C协议详细设计

本文使用的符号如表1所示。

表1 符号说明

符号	含义说明
SA_i'	发起者支持的一组用于密钥协商阶段的算法,供响应者选择
SA_r'	响应者从SA_i'中选出的一组算法
$g^{x\prime}$	x的DH指数,x为发起者i或响应者r,用于生成临时密钥K_ir
N_x'	x的nonce值,x为发起者i或响应者r,用于生成临时密钥K_ir及参与puzzle运算
k	puzzle的难度值,表示puzzle运算的哈希值前k位为0
Y	puzzle运算哈希值后128减k位的值
X	puzzle的解答,puzzle公式为$H\{N_i', N_r', X\} = 000\cdots000Y$
ID_x	x的身份信息,x为发起者i或响应者r
$CERT_x$	x的公钥证书,x为发起者i或响应者r
SA_i	发起者支持的一组IPSec参数,供响应者选择
SA_r	响应者从SA_i中选出的一组参数
g^x	x的DH指数,x为发起者i或响应者r,用于生成工作密钥WK_ir
N_x	x的用于生成工作密钥WK_ir的nonce值,x为发起者i或响应者r
K_ir	用于保护报文3、4的临时密钥,由g^i、g^r、N_i'、N_r'生成
WK_ir	用于保护后续业务流的工作密钥,由g^i、g^r、N_i、N_r生成
$E_{K\_ir}\{M\}$	以K_ir为密钥对消息M进行对称加密
$SIG_x\{M\}$	以x的私钥对消息M进行签名,x为发起者i或响应者r
$H\{M\}$	对消息M进行哈希运算
HMAC$\{M\}$	对消息M进行哈希运算,用于完整性保护

报文1 用于发起协商,发起者通过SA_i'提供一组自己支持的算法供响应者选择。这组算法主要用于第一阶段。

报文2 响应者通过SA_r'声明自己选定的一组算法;通过N_r'、k和Y向发起者提供puzzle函数的参数,要求发起者进

行 puzzle 计算;生成 DH 指数 g_r' 和 nonce 值 N_r' 作为临时密钥的密钥材料。

报文 3　发起者生成临时密钥的密钥材料 g_i' 和 N_i',通过穷举计算得出 puzzle 解答 X 的值;根据临时密钥的生成函数 $K\_ir = H\{g_i'r' \mid N_i' \mid N_r' \mid 0\}$ 计算出用于第一阶段加密的临时密钥 K_ir。在报文 3 中,以明文形式传递 g_i'、N_i' 和 X,以密文形式(以临时密钥 K_ir 加密)传递发起者支持的第二阶段协商全部套件 SA_i 以及用于防止消息重放攻击的密钥相关的哈希运算消息认证码(Hash-based Message Authentication Code,HMAC)值。

报文 4　响应者首先验证报文 3 中的 puzzle 解答 X 是否正确。若验证 X 正确,则通过报文 3 中的 g_i'、N_i' 以及本地存储的 g_r' 和 N_r' 计算临时密钥 K_ir,并解密报文 3 的密文,完成相应处理并构造报文 4。报文 4 中将包含响应者从 SA_i 中选出的一组套件 SA_r、响应者的身份信息 ID_r 和证书 $CERT_r$ 以及用于防止消息重放攻击的 HMAC 值,以上信息将由临时密钥加密,对密文做哈希运算后用响应者的私钥进行数字签名,用于身份认证和完整性保护。

报文 5　发起者解密报文 4,获取响应者证书,验证签名确认其身份,获取 SA_r,此时第一阶段协商完成。发起者通过构造发送报文 5 开始第二阶段协商,报文 5 中将包含发起者身份及证书 ID_i 和 $CERT_i$、用于生成工作密钥的 g_i 和 N_i、用于防止消息重放攻击的 HMAC 值、以及用于身份认证和完整性保护的数字签名 $SIG_i\{H\{\text{All}\}\}$,所有信息除签名外均由 K_ir 加密。

报文 6　响应者解密获取报文 5 内容,首先对发起者进行身份认证,若认证通过即开始构造并发送报文 6。报文 6 中将包含用于生成工作密钥的 g_r 和 N_r、用于防止消息重放攻击的 HMAC 值、以及用于身份认证和完整性保护的数字签名 $SIG_i\{H\{\text{All}\}\}$,所有信息除签名外均由 K_ir 加密。此时,发起者和响应者均获得了计算工作密钥 $WK\_ir = H\{g_ir \mid N_i \mid N_r \mid 0\}$ 所需的 g_i、N_i、g_r 和 N_r。

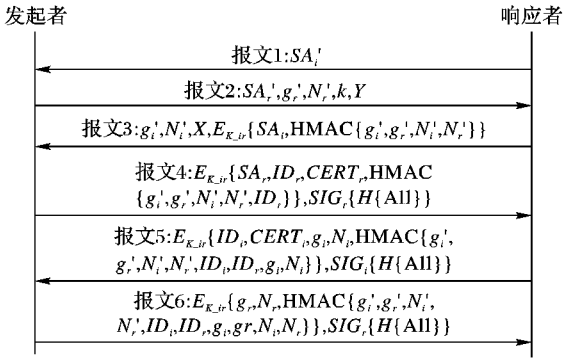

图 1　IKE-C 协议密钥交换示意图

3　IKE-C 协议分析与仿真

3.1　主要改进内容分析

IKE-C 采用了 IKEv2 两个阶段的思想,在其基础上进行了一系列改进,主要包括以下几点:

1)通过 puzzle 机制,应对计算资源耗尽的 DoS 攻击。

在云计算环境中,云侧 IPSec 设备受 DoS 攻击威胁较大,提高响应者抗 DoS 攻击能力是 IKE-C 的主要目标之一。为此,IKE-C 采用了 puzzle 计算和部分参数重用等多种手段。

puzzle 机制的核心思路是构建一个特殊的函数,要求发起者消耗较多计算资源才能得到答案,响应者通过简单的计算即可验证答案的正确性,从而增加发起者计算量,增强响应者抗 DoS 攻击能力。IKE-C 中采用的 puzzle 函数是 $H\{N_i', N_r', X\} = 000\cdots000Y$,其中 $000\cdots000Y$ 中 0 的位数(k 值)及 Y 的值由响应者指定,N_i' 可保证解答的新鲜性,防止重放过去的或其他发起者的 puzzle 解答。发起者计算 puzzle 的解答时,由于哈希函数的不可逆性,只能通过 X 的穷举来寻找 puzzle 的解答,将消耗较多资源,找到正确的 X 值作为 puzzle 的解答返回给响应者。puzzle 对发起者的计算资源消耗量可通过 k 值来调整,k 值越大,消耗量越大。响应者验证 puzzle 的解答时,只需进行一次哈希计算即可。

2)通过参数重用和密钥材料推迟传递,应对内存耗尽的 DoS 攻击。

IKE-C 提高响应者抗 DoS 攻击能力的另一种手段是重用参数 N_r'、k、Y。重用的好处是无需为每个发起者生成并存储以上参数,防止内存耗尽的 DoS 攻击。以上参数将用于两个功能,一是计算临时密钥 $K\_ir = H\{g_i', g_r' \mid N_i' \mid N_r' \mid 0\}$,其中 g_r'、g_i'、N_i' 并不重用,可保证临时密钥的新鲜性;二是 puzzle 函数 $H\{N_i', N_r', X\} = 000\cdots000Y$,其中 N_i' 并不重用,可保证答案 X 的新鲜性。

针对内存耗尽的 DoS 攻击,IKE-C 的另一个改进是推迟 g_i'、N_i' 的传递。IKEv2 在报文 1 中传递 g_i'、N_i',因此响应者不得不为每个发起者存储其密钥材料,容易受到内存耗尽的 DoS 攻击。IKE-C 将发起者的密钥材料放在报文 3 中传递,因此响应者可在完成 puzzle 验证,确认发起者不是攻击者之后才存储其密钥材料,可防止针对其内存资源的 DoS 攻击。

3)推迟传递发起者身份,防止中间人攻击造成身份信息泄露。

IKEv2 协议中,发起者和响应者的身份信息分别在报文 3 和报文 4 中以密文形式交换。但由于报文 2 没有经过加密或认证,可能受到中间人攻击,攻击者伪装成响应者与其交换密钥参数,形成共同的 K_ir。尽管在收到报文 4 后发起者通过身份验证能够发现攻击者的存在,但其身份信息已经泄露。

在 IKE-C 协议中,发起者身份信息不在第一阶段出现,而是在通过报文 4 确认响应者身份后才在第二轮协商中发送自己的身份信息,可有效防止中间人的欺骗,保证身份信息的私密性。这种设计会对响应者产生一定的影响,一是在第一阶段无法获知发起者身份,需以发起者的 nonce 值作为发起者的临时身份标识,但不会产生安全问题;二是每次在第二阶段中都要进行签名验证,将一定程度上增加响应者的公钥计算量。

4)降低公钥运算量,提升密钥协商效率。

在计算量上,IKE-C 只在后三个报文中进行公钥运算,用于数字签名的生成及验证,且签名运算的对象是整个报文的哈希值,通常为 128 b 或 256 b。对于采用证书认证的协议,已经达到了公钥运算量的最低值,明显低于 IKEv2。

3.2　协议性能仿真评估

鉴于"网络质量良好"是构建云计算安全体系的前提条件,本文的仿真实验将无线链路带宽固定为 100 Mb/s,客户端数量由 100、200 递增至 1 000,随着网络中客户端数量不断变化,来比较 IKEv2 和 IKE-C 两种密钥交换协议的收敛时间。

仿真结果表明,两种协议收敛时间均呈逐渐增长的趋势,这是由客户端/服务器的网络模式所决定。而 IKE-C 由于采用 puzzle、密钥材料及身份信息推迟传递等机制,在网络规模相同的情况下,其密钥交换的收敛时间明显少于 IKEv2。而且随着客户端数量的不断增加,其优势越来越大。例如在客

(下转第 2864 页)

验中利用算法生成一个加密矩阵,用这个矩阵对 QR 的数据编码区域进行异或操作得到密文,然后再对密文进行掩模操作。和前面实验中的处理方式一样,唯一不同之处在于加密图像的功能区域全部用 255 进行填充,这是为了在图像上显示的方便。从图中可以看出加密效果是比较好的。

(a) 明文图像 (b) 加密图像 (c) 密文图像

图 7 加密效果对比

4 结语

QR 码在信息技术领域中具有广泛而重要的应用。为了保证 QR 码的通信和存储安全,本文提出了一种 QR 码的加密算法。与现有的几种 QR 加密算法不同,本文从 QR 码的编码原理出发,使密文保留了版本和格式信息。在设计具体加密算法时借用了 Ising 物理模型的思想,保证了加密的高效性,同时可支持加密和解密的并行计算。实验结果表明,本文算法具有良好的随机性和敏感性,可有效保证 QR 码的安全。

参考文献:

[1] FLOTT L W. Bar codes[J]. Metal Finishing, 2002, 100(8): 42 - 47.

[2] KAO Y W, LUO G H, LIN H T, *et al*. Physical access control based on QR code[C]// Proceedings of the 2011 International Conference on Cyber - Enabled Distributed Computing and Knowledge Discovery. Washington, DC: IEEE Computer Society, 2011: 285 - 288.

[3] OH D S, KIM B H, LEE J K. A study on authentication system using QR code for mobile cloud computing environment[C]// Proceedings of the 6th International Conference on Future Technology. Berlin: Springer, 2011: 500 - 507.

[4] 刘彦伟, 王根英, 刘云. QR 码信息加密的研究与实现[J]. 铁路计算机应用, 2012, 21(11): 37 - 40.

[5] 张雅奇, 张定会, 江平. 一种提高 QR 码安全性的方法[J]. 信息技术, 2012, (11): 90 - 95.

[6] CHUNAG J C, HU Y C, KO H J. A novel secret sharing technique using QR code[J]. International Journal of Image Processing, 2010, 4(5): 468 - 475.

[7] BARRERA J F, MIRA A, TORROBA R. Optical encryption and QR codes: Secure and noise-free information retrieval [J]. Optics Express, 2013, 21(5): 5373 - 5287.

[8] 周庆, 胡月, 廖晓峰. 一种自适应的图像加密算法的分析及改进[J]. 电子学报, 2009, 37(12): 2730 - 2734.

[9] 周庆, 陈刚, 胡月. 一个用简单物理模型构建的加密系统[J]. 物理学报, 2011, 60(4): 339 - 344.

[10] 中国物品编码中心. QR Code 二维码技术与应用[M]. 北京: 中国标准出版社, 2001.

[11] 张志东. 伊辛模型的研究进展简介[J]. Chinese Journal of Nature, 2007, 30(2): 1 - 6.

[12] HOU A L, YUAN F, YING G. QR code image detection using run-length coding[C]// International Computer Science and Network Technology, Washington, DC: IEEE Computer Society, 2011: 2130 - 2134.

(上接第 2837 页)

户端数量为 300 时,IKE-C 的收敛时间比 IKEv2 减少了17 s;当客户端数量增至 1 000 时,IKE-C 的收敛时间比 IKEv2 减少了 186 s。

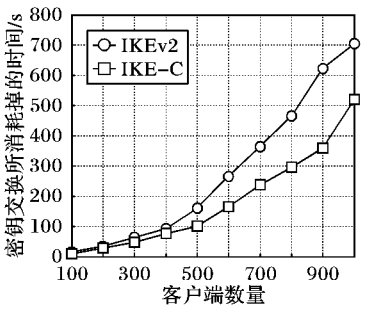

图 2 不同网络规模条件下的协议收敛时间对比

4 结语

为满足云计算应用场景对密钥协商协议安全性和高效性的要求,本文针对云计算环境下 C/S 架构、瘦客户端、网络质量良好等特点,结合现有主流密钥协商协议 IKEv2 易受 DoS 攻击、易受中间人攻击导致双方身份泄露、计算量较大效率不高等缺陷,在现有 IKEv2 协议基础上进行针对性的改进,提出 IKE-C 协议。该协议能够抵抗针对响应者计算资源和内存资源的 DoS 攻击,同时解决了发起者身份泄露的问题。通过仿真实验表明,在网络规模相同的情况下,IKE-C 密钥交换的收敛时间明显少于 IKEv2。

参考文献:

[1] 王伟, 高能, 江丽娜. 云计算安全需求分析研究[J]. 信息网络安全, 2012(8): 75 - 78.

[2] 荆继武. 看待“云雾”中的密码挑战[J]. 信息安全与保密通信, 2012(11): 15 - 16.

[3] 张云勇, 陈清金, 潘松柏, 等. 云计算安全关键技术分析[J]. 电信科学, 2010(9): 64 - 69.

[4] IPSec architecture[S/OL]. [2013-03-01]. http://www.ietf.org/rfc/rfc2401.txt.

[5] HADDAD H, BERENJKOUB M, GAZOR S. A proposed protocol for Internet Key Exchange (IKE) [C]// Proceedings of the 2004 Canadian Conference on Electrical and Computer Engineering. Piscataway: IEEE, 2004: 2017 - 2020.

[6] IKEv2[S/OL]. [2013-01-20]. http://www.ietf.org/rfc/rfc4306.txt.

[7] 高翔, 李亚敏, 郭玉东, 等. IKEv2 协议安全性分析与改进[J]. 计算机应用, 2005, 25(3): 563 - 572.

[8] 唐佳佳, 李学哲, 陈国新. IKEv2 中混合认证的研究与扩展设计[J]. 南通职业大学学报, 2009, 23(2): 82 - 85.

[9] 王琳琳, 何国良. IKEv2 协议分析与安全性研究[J]. 技术前沿, 2008, 10(8): 65 - 69.

[10] AIELLO W, BELLOVIN S, EFICIENT B M. Secure key exchange for Internet protocols[C]// Proceedings of the 9th ACM Conference on Computer and Communication Security. New York: ACM, 2002: 48 - 58.

[11] Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing v2.1[S/OL]. [2013-01-20]. http://www.cloudsecurityalliance.org.

[12] European Network and Information Security Agency. Cloud computing information assurance framework[R/OL]. [2013-01-20]. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework.