文章编号:1001 - 9081(2008)07 - 1807 - 03

基于数字签名认证的 IKE 协议安全性分析及改进

何韦伟,季新生,刘彩霞
(信息工程大学 国家数字交换系统工程技术研究中心,郑州 450002)
(bnooby@ hotmail. com)

摘 要:IKE 协议的复杂性使得其存在一些安全漏洞。简要介绍基于数字签名认证方式的 IKE 协议工作机制之后,分析了 IKE 协议容易遭受的两种中间人攻击,针对中间人攻击导致用户身份泄漏的安全缺陷,提出两种改进方案并给出改进前后定量的性能分析。

关键词:IKE;数字签名;中间人攻击;公钥
中图分类号: TP393 **文献标志码**:A

Security analysis and improvement of IKE protocol with signature authentication

HE Wei-wei, JI Xin-sheng, LIU Cai-xia
(*National Digital Switching System Engineering and Technological R&D Center, Information Engineering University, Zhengzhou Henan* 450002, *China*)

Abstract: The complexity of Internet Key Exchange (IKE) protocol causes some potential security flaws. After the mechanism of IKE with signature was introduced, the two kinds of man-in-middle attack were analyzed. In order to protect the users' identities from being exposed to the outside, two solutions with some improvements were proposed. Finally the paper made a quantitative capability analysis on the whole.

Key words: Internet Key Exchange (IKE); digital signature; man-in-middle attack; public key

0 引言

IKE 是 IETF 制定的密钥交换协议标准,它是 IPSec 正式确定的密钥管理协议,为通信双方安全动态协商 IPsec 加密保护所使用的算法和密钥素材。IKE 分为两个阶段来实现:第 1 阶段用来协商保护 IKE 本身通信所使用的算法和密钥;第 2 阶段利用第 1 阶段建立的安全信道来协商 IPsec 通信中使用的算法和密钥。

近十几年来,世界各国学者对 IKE 进行了较为广泛和深入的研究,尤其是美国和欧洲的一些国家在这一关键领域投入了大量的研究经费和力量,一些研究机构和公司已对其进行了试验性的实现,而国内对它们的研究仍处于初期阶段。

1 IKE 协议概述

IKE 协议阶段 1 有主模式和积极模式两种工作模式[1],其中主模式通过 6 次消息交换来协商 ISAMKP 安全关联(SA)。主模式下基于数字签名的认证方式工作原理如图 1 所示。

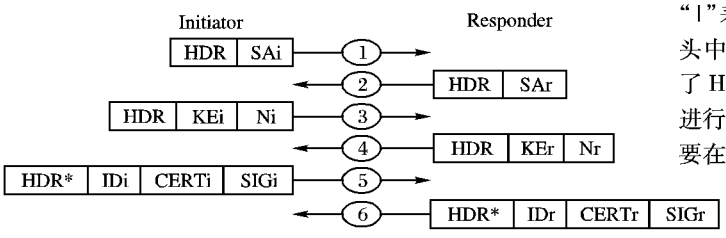

图 1 IKE 协议主模式下数字签名认证方式

HDR 是消息头载荷,SAi 是 SA 协商载荷,其中包含着发起方支持的各种算法组合的建议。在消息 2 的 SAr 中响应方表明了接受何种 SAi 中建议的算法组合。通过消息 1、2,通信双方协商出第 1 阶段所使用的对称算法、认证算法等信息。消息 3、4 中的 KEi/KEr 载荷是双方交换的 D-H 共享密钥,Ni/Nr 是当前时间载荷。通信双方通过消息 5、6 用数字签名的方式进行双向认证,其中 HDR * 表示对消息加密,IDi/IDr 是用户 ID 载荷,CERTi/CERTr 是证书载荷,SIGi/SIGr 是签名载荷。数字签名可以采用 DSS 算法或 RSA 算法,公共密钥通常从证书 CERT 中获取,IKE 允许证书的交换,也允许从一个远方通信那里索取证书。为了验证交换中的双方,协议的发起者和响应者要分别产生 HASH_I 和 HASH_R,然后发起者和响应者分别用自己的私钥 PRVKEY 对 HASH 签名,对方利用相应的公钥验证签名。

HASH 的计算方法如下:

$$HASH\_I = prf(SKEYID, g^{x_i} | g^{x_r} | Ci | Cr | SAi | IDi) \quad (1)$$

$$HASH\_R = prf(SKEYID, g^{xr} | g^{xi} | Cr | Ci | SAi | IDr) \quad (2)$$

签名的计算方法如下:

$$SIGi = PRVKEY\_I(HASH\_I) \quad (3)$$

$$SIGr = PRVKEY\_R(HASH\_R) \quad (4)$$

其中:prf 是伪随机函数,通常是一个带密钥的 HASH 函数;"|"表示信息的串连;"x^y"表示 x 的 y 次幂;Ci/Cr 表示消息头中 Cookie 域的内容。为了保护用户 ID 信息,消息 5、6 中除了 HDR 载荷外,其余载荷都使用在消息 1、2 中协商出的算法进行加密保护。为了验证和保护 IKE 消息,参与通信的双方都要在生成 SKEYID 的基础之上生成另外 3 种密钥SKEYID_d、SKEYID_a 和 SKEYID_e。SKEYID 的计算方法如下:

$$SKEYID = prf(Ni\_b | Nr\_b, g^{xy}) \quad (5)$$

2 IKE 协议安全性分析及 IKE 协议的改进

作为密钥交换协议的一个重要安全特性,身份保护是指在密钥交换过程中,保护通信双方的身份不被泄漏。而 IKE

收稿日期:2008 - 01 - 14;**修回日期**:2008 - 03 - 24。 **基金项目**:国家 863 计划项目(2007AA01Z434)。

作者简介:何韦伟(1982 -),女,湖北阳新人,硕士研究生,主要研究方向:移动通信、网络安全; 季新生(1968 -),男,河南新乡人,教授,主要研究方向:电信网络安全; 刘彩霞(1974 -),女,山东烟台人,讲师,主要研究方向:电信网络安全防护。

主模式下数字签名认证容易遭受中间人攻击,因而面临用户身份泄露的安全隐患。下面详细描述两种中间人攻击的原理及改进方案。

2.1 第一种中间人攻击

攻击者可以通过篡改双方的安全关联信息,冒充双方进行通信。图2说明了这种中间人攻击的过程。

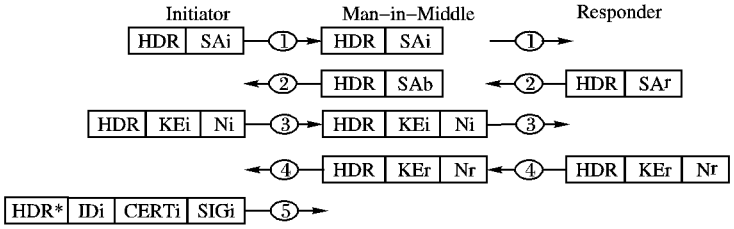

图2 第一种中间人攻击过程

在第一次交换过程中,攻击者可以截取消息2,把SAr提供的保护套件改为SAb,之后伪装成第二条消息发送给发起者,由于在最后一次交换进行验证计算散列摘要时,只用到了SAi进行验证,所以通信双方对于攻击者所做的修改可能完全不知情,并可顺利通过认证。当攻击者所提供的保护套件中的加密算法和散列算法与响应者的加密算法和散列算法不同时,攻击可能不会成功,因为在计算HASH_I和HASH_R的时候会用到这些算法,但是如果攻击者只改变了SA的生存时间等在计算HASH_I和HASH_R时不会用到的安全属性时,那么上述的攻击可能会成功并且带来安全隐患。

产生这种中间人攻击的关键所在就是没有对SAr进行验证。为了抵御这种中间人攻击,文献[2]对HASH_I和HASH_R分别作了如下修改:

$$HASH\_I' = prf(SKEYID, g^xi | g^xr | Ci | Cr | SAi | SAr | IDi) \quad (6)$$

$$HASH\_R' = prf(SKEYID, g^xr | g^xi | Cr | Ci | SAr | IDr) \quad (7)$$

式(6)中之所以要对SAi和SAr同时进行验证,是因为攻击者还可能修改发起者发送的第一条消息中的SAi载荷,如果只对SAr进行验证,可能遭受中间人冒充发起者的攻击。而如果式(6)中只对SAi进行验证,那么如果攻击者修改响应者发送的第二条消息中的SAr载荷的话,只能在发起者接收到最后一条消息之后,进行验证时才能发现,此时它必须再额外的发一条消息通知响应者删除它所建立的SA。在式(6)中同时对SAi和SAr进行验证,不管攻击者冒充发起者修改了SAi还是冒充响应者修改了SAr,最终都不能通过验证。虽然这样稍微增加了计算的工作量,但却提高了安全性。

2.2 第二种中间人攻击

攻击者可以通过监听双方协商的SA,更改D-H密钥的方式,窃取通信发起方的用户身份信息。图3说明了中间人攻击的过程。攻击者截获消息4,篡改原D-H密钥交换信息,将其中的KEr换成自己计算出的KEm,这样攻击者与发起方建立了D-H密钥对。由于消息传送前未作任何的认证工作,因此双方觉察不到消息的篡改过程。发起方所计算出的SKEYID,以及由它衍生出的其他密钥材料,攻击者也同样可以计算得到。当攻击者接收到消息5时,利用与发起方建立的密钥SKEYID_e,可以解密获得IDi。可见遭受这样的中间人攻击会导致发起方的用户ID泄漏。

针对这种中间人攻击,目前有三种解决方案:

1)文献[3]提出将IKE第1阶段的响应方最后两条消息合并发送(也即先发送响应方的身份),这种修改假设认为响应方为固定的服务器,其身份信息可以通过其他途径获得,相比而言,保护发起方的身份显得更为重要。这种假设在客户端——网关服务器模式下是适用的,但在其他类型的网络应用中,很难预言哪一方身份更值得保护。另一方面,这种将消息4、6合并的解决方法也破坏了安全关联与密钥管理协议(ISAKMP)定义的身份保护交换框架,失去了原有的3次交换结构,使消息传递失去对称性。

2)文献[4]提出将IKE第1阶段的最后两条消息中的ID载荷更改为HASH(ID),此方法又容易受到采用暴力猜测方式的"字典"攻击。一个富有侵略性的攻击者,可以先进行中间人攻击获得D-H密钥,然后解密消息5并通过字典攻击猜测ID,通过对ID的散列计算来验证。对于这种情况,由于该模式下双方没有任何预先知道的关于对方的秘密信息,中间人攻击不可避免,所以用户的ID必须保持一定的长度,以增大攻击者暴力破解的难度。

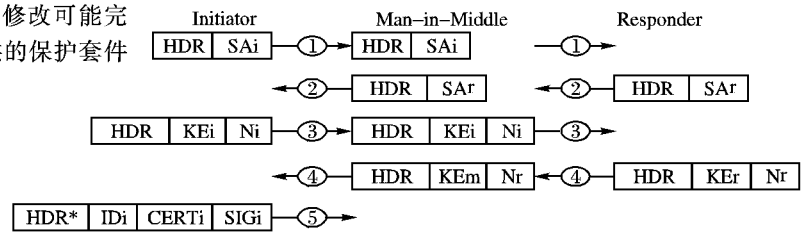

图3 第二种中间人攻击过程

3)文献[5]改进了文献[4]的方法,在HASH(ID)中引入时间变量,这样攻击者即使解密了消息5也不会得到发起方的身份信息,而且由于时间参数的引入,其企图发动的字典攻击也不会得逞。但由于引入的额外散列值的运算及定期更新的需要,在大型服务器的场合会造成服务器过度的计算负担。

基于上述分析,本文给出两个新的改进方案,改进遵循下面的原则:

原则1 改动不破坏IKE所遵循的ISAKMP框架与IKE交互的对称结构。

原则2 改动后引起的实现代价和运行时代价(包括资源消耗和时间消耗)要尽量小。

原则3 同等对待发起方和响应方的身份保护。

改进方案一如图4所示,消息有如下变化:

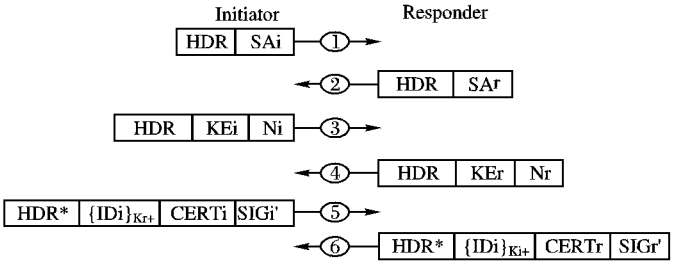

图4 改进方案一

1)在消息5、6中将双方的身份载荷IDi和IDr分别用对方的公钥Kr+和Ki+进行加密,得到{IDi}Kr+和{IDi}Ki+,将加密后的身份载荷代替原来的身份载荷。这样,对方收到消息后,可以用自己的私钥对加密身份载荷进行解密,而且这个私钥只有自己知道。攻击者即使解密了最后两条消息得到{IDi}Kr+和{IDi}Ki+,但由于没有双方的私钥,因此还是无法得到双方的ID。这样就防止了双方身份泄漏。

2)借鉴上文中对抵抗第一种中间人攻击的改进方法,在消息5、6中分别用HASH_I'和HASH_R'两种散列载荷代替

原来的 HASH_I 和 HASH_R 来计算 SIGi 和 SIGr,得到 SIGi′和 SIGr′。

改进方案二如图 5 所示,消息有如下变化:

1)在消息 3、4 中的 KE 载荷之后分别增加两个对 KE 载荷内容的签名载荷——SIG_KEi 和 SIG_KEr。其中,SIG_KEi 是发起者先对 KEi 用消息 1、2 协商好的验证算法进行 hash 计算,然后再用自己的私钥对该 hash 结果进行签名得到的;同理可以得到 SIG_KEr。这样双方就通过了对 KE 的认证,防止了攻击者对 KE 的篡改。由于数字签名要使用证书,因此 KE 和 SIG_KE 之间还应有双方各自的证书载荷 CERT。

2)借鉴上文中对抵抗第一种中间人攻击的改进方法,在消息 5、6 中分别用 HASH_I′和 HASH_R′两种散列载荷代替原来的 SIGi 和 SIGr 两种签名载荷。如果发起者或者响应者拥有多个证书,那么他们可以使用消息 3、4 提供的可选的证书载荷来向对方表明自己到底选用哪个证书。证书里面包含了个体的身份和公开密钥等信息,并且二者是绑定的,任何一个攻击者由于没有 CA 认证机构的私钥,因此无法伪造证书信息。

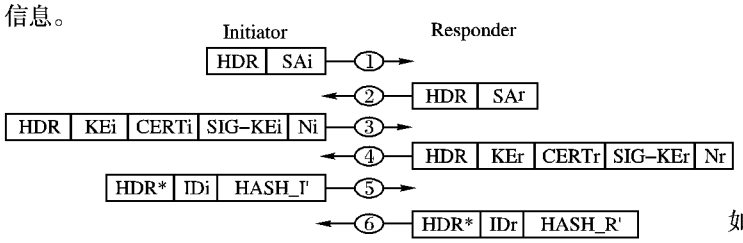

图 5　改进方案二

3　改进方案的安全性及性能分析

3.1　安全性分析

在改进方案一中,将最后两条消息中双方的身份载荷用对方的公钥加密,攻击者即使可以篡改 KE 载荷内容,解密了消息 5,但由于不知道双方的私有密钥而无法得到身份载荷。这样就保护了用户身份不被泄漏。但是攻击者仍有可能与发起者建立共享密钥,使发起者计算出的加密密钥与响应者计算出的加密密钥不一致,响应者在接收到消息 5 后无法解密整条消息,导致双方认证失败。

而在改进方案二中,在消息 3、4 中增加密钥签名载荷后,攻击者即使可以篡改 KE 载荷内容,但由于不可能知道双方的私有密钥而无法伪造 SIG_KE 载荷,因而无法通过消息接收方的认证。攻击者再也无法冒充双方生成伪造的 DH 共享值以及 4 个密钥,不管是截获消息 5 或者消息 6,都绝对不可能解密消息内容,当然也就无法获得通信双方的身份信息。这样就可以彻底地抵御本文所说的第二种中间人攻击。另外,用 HASH 散列载荷 HASH_I′和 HASH_R′来取代原来消息中的 SIGi 和 SIGr 载荷,不仅减少了签名操作中的加解密的计算量,还有效地阻止了第一种中间人攻击的发生。总的来说,对于主模式下数字签名方式的这种改进没有增加额外的 PKI 负担,在消息 3、4 中提供了对 DH 共享值的有效保护,在消息 5、6 中提供了验证功能和对双方身份的保护。

可以看出,虽然两种改进方案都防止了第一种中间人攻击,且防止了用户身份泄漏,但方案二在抵御第二种中间人攻击方面比方案一更彻底。下面对两种方案改进前后的性能做进一步分析。

3.2　性能分析

安全协议中的密码算法通常包括耗费系统计算资源的大规模的乘幂运算和公钥体制下的加解密操作,因此可以用“计算代价”来评估改进方案的性能[6]。下面给出两种方案改进前后的定量的性能分析。

如果存在第一种中间人攻击,那么修改前后都是在响应者收到消息 5 后经过重新计算 HASH_I′而检测出来。截止到发现攻击时,双方已付出的计算代价如表 1 所示。针对这一种攻击,双方在发现攻击时改进后的计算代价要比改进前的多一次公钥加(解)密操作。

如果存在第二种中间人攻击,那么在协议改进前以及改进方案一中,响应者也是在收到消息 5 后才能检测到攻击。双方及攻击者所付出的计算代价如表 2 所示。而对于改进方案二,由于在消息 3、4 中增加了身份签名载荷 SIG_KEi 和 SIG_KEr 的保护,所以根本不存在第二种中间人攻击,因此为抵御这种攻击双方需要付出的计算代价等于 0。这也是改进方案二的优势所在。

表 1　改进前后双方付出的计算代价

计算代价	改进前	改进方案一	改进方案二
发起者计算代价	一次 KE 交换 计算 4 个秘密密钥 一次 SIG_I 加密 一次对消息 5 的对称加密	一次 KE 交换 计算 4 个秘密密钥 一次公钥加密 一次 SIG_I 加密 一次对消息 5 的对称加密	一次 KE 交换 一次 SIG_KE_I 加密 一次 SIG_KE_R 解密 计算 4 个秘密密钥 一次对消息 5 的对称加密
响应者计算代价	一次 KE 交换 计算 4 个秘密密钥 一次对消息 5 的对称解密 一次 SIG_I 解密	一次 KE 交换 计算 4 个秘密密钥 一次对消息 5 的对称解密 一次私钥解密 一次 SIG_I 解密	一次 SIG_KE_I 解密 一次 KE 交换 一次 SIG_KE_R 加密 计算 4 个秘密密钥 一次对消息 5 的对称解密

表 2　改进前及方案一双方及攻击者付出的计算代价

方案	发起者计算代价	攻击者计算代价	响应者计算代价
改进前	一次 KE 交换 计算 4 个秘密密钥 SIG_I 加密 对消息 5 的对称加密	一次 KE 交换 计算 8 个秘密密钥 对消息 5 的对称解密	一次 KE 交换 计算 4 个秘密密钥 对消息 5 的对称解密 SIG_I 解密
改进方案一	一次 KE 交换 计算 4 个秘密密钥 一次公钥加密 SIG_I 加密 对消息 5 的对称加密	一次 KE 交换 计算 8 个秘密密钥 对消息 5 的对称解密	一次 KE 交换 计算 4 个秘密密钥 对消息 5 的对称解密 一次私钥解密 一次 SIG_I 解密

(下转第 1815 页)

这表明 c 的值达到一定值后,对病毒传播的影响趋于平稳。

图 7 考查了暴露主机成功执行感染文件的概率对病毒传播的影响。图中传播曲线表明,执行的成功率越高,感染高峰值越大,但感染高峰到来的时间和消除网络中所有的病毒所需时间都基本相同。

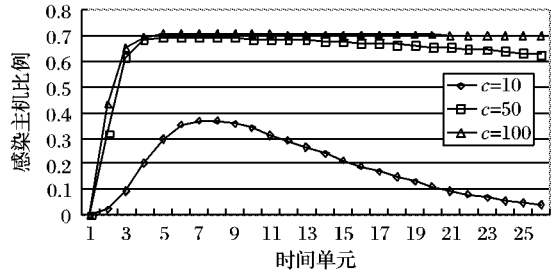

图 6　不同的 c 值对病毒传播的影响

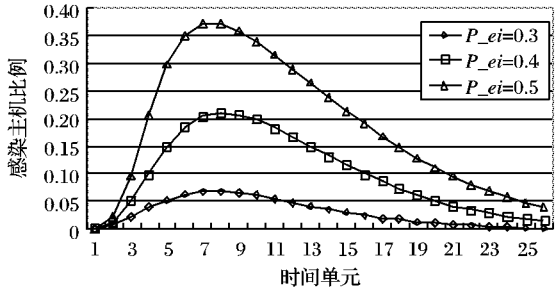

图 7　病毒文件成功执行概率对病毒传播的影响

4　结语

过去,由于 P2P 网络的规模不是很大加之病毒在 P2P 网络上传播速度较慢,因此,P2P 网络上的病毒并未怎么引起研究人员的关注。然而,在今天,随着 P2P 网络的发展,特别是 P2P 文件共享网规模和受欢迎程度的巨大提高,P2P 病毒已成为 P2P 网络的重大安全隐患。本文主要对 P2P 病毒及其传播进行了深入研究。首先,对 P2P 文件共享网络的特点和病毒传播的研究情况进行了介绍;接着在对病毒进行深入分析的基础上,提出了病毒在 P2P 网上传播的模型;最后,为了考查哪些参数对病毒传播有着重大影响,进行了大规模仿真实验。实验结果表明,不同参数对病毒传播的影响有很大不同。今后,在制定抑制病毒传播的策略时,可以考虑通过控制模型中的关键参数(如 c 和 p_{ei})来制定抑制策略。

参考文献:

[1] eDonkey2000 server list[DB/OL]. [2007 - 12 - 11]. http://ocbmaurice. no-ip. org/slist/serverlist. html.

[2] Bittorrent Protocol Specification v1.0 [DB/OL]. [2007 - 12 - 11]. http://www. bitconjurer. org/BitTorrent/protocol. html.

[3] CHEN G L, GRAY R S. Simulating non-scanning worms on peer-to-peer networks[C]// Proceedings of the 1st international conference on Scalable information systems. Hong Kong: ACM Press, 2006.

[4] MCKENDRICK A G. Applications of mathematics to medical problems[C]// Proceedings of the Edinburgh Mathematical Society. [S. l.]: Cambridge University, 1926, 44: 98 - 130.

[5] KEPHART J O, WHITE S R. Directed-graph epidemiological models of computer viruses[C]// Proceeding of the IEEE Symposium on Security and Privacy. Oakland, California: IEEE Press, 1991: 343 - 359.

[6] ZOU C C, GONG W, TOWSLEY D. Code red worm propagation modeling and analysis[C]// Proceedings of the 9th ACM Conference on Computer and Communication Security. Washington, DC: ACM Press, 2002.

[7] ZOU C, TOWSLEY D, GONG W. Email worm modeling and defense[C]// Proceedings of the 13th International Conference on Computer Communication and Networks. [S. l.] : IEEE Press, 2004: 409 - 414.

[8] QIU D, SRIKANT R. Modeling and performance analysis of BitTorrent-like peer-to-peer networks[C]// Proceedings of ACM SIGCOMM. Portland, USA: ACM Press, 2004.

[9] DUMITRIU D, KNIGHTLY E, KUZMANOVIC A. Denial-of-service resilience in peer-to-peer file-sharing systems[C]// Proceeding ACM Sigmetrics. Banff, Canada : ACM Press, 2005.

[10] THOMMES R W, COATES M J. Modeling virus propagation in peer-to-peer networks[R]. Department of Electrical and Computer Engineering, McGill University, 2005.

[11] STUTZBACH D, REJAIE R, SEN S. Characterizing unstructured overlay topologies in modern P2P file-sharing systems[C]// Proceedings of the 15th ACM Internet Measurement Conference. Berkeley, California: ACM Press, 2005: 49 - 62.

[12] MA J, CHEN X M, XIANG G L. Modeling passive worm propagation in peer-to-peer system[C]// Proceedings of the IEEE 2006 International Conference on Computational Intelligence and Security. [S. l.] : IEEE Press, 2006: 1129 - 1132.

[13] P2p-worm. win32. achar. a[DB/OL]. [2008 - 01 - 02]. http://www. viruslist. com/en/viruses/encyclopedia?virusid = 23893.

[14] W32. hllw. gotorm[DB/OL]. [2008 - 01 - 03]. http://securityresponse. symantec. com/avcenter/venc/data/w32. hllw. gotorm. html.

[15] W32/bare. worm[DB/OL]. [2008 - 01 - 05]. http://www. virus-scan-software. com/latest-virus-software/latest-viruses/w32bare-worm. shtml.

[16] Sophos virus analysis: Troj/krepper-g[DB/OL]. [2008 - 01 - 05]. http://www. sophos. com/virusinfo/analyses/trojkrepperg. html.

(上接第 1809 页)

4　结语

本文首先对 IKE 协议第一阶段基于数字签名认证的原理进行了描述。然后分析了协议容易遭受的两种中间人攻击,针对攻击导致的身份保护缺陷提出改进方案。从安全性及性能分析的结果看出,提出的两种改进方案都能有效防止中间人攻击,尤其是方案二的综合性能更优于方案一。由于 IKE 协议的灵活性及复杂性,不仅使得对其分析的难度增大,还导致其存在种种其他已知或未知的安全缺陷,为了更好地保证数据的通信安全,IKE 协议还有待于进一步完善。

参考文献:

[1] RFC2409, The Internet Key Exchange(IKE)[S]. 1998.

[2] 宋育芳, 张宏科. Internet 密钥交换协议的安全性分析[J]. 计算机工程与应用, 2004, 40(8): 136 - 139.

[3] PERLMAN R, KAUFMAN C. Analysis of the IPSec key exchange standard[C]// Proceedings of the 10th IEEE International Workshops on WEIICE: [S. l.]: IEEE Press, 2001: 150 - 156.

[4] 卫剑钒, 唐礼勇, 陈钟. IKE 协议两种身份保护缺陷的改进[J]. 计算机工程与应用, 2004, 40(26): 33 - 35.

[5] 陈艳红, 韩秀玲, 刘文超. IKE 协议主模式认证机制的分析与改进[J]. 计算机工程与应用, 2006, 42(9): 120 - 121.

[6] 张琳, 王汝传. IKE 协议中基于数字签名验证的主模式研究[J]. 南京邮电大学学报, 2007, 27(1): 70 - 73.