一种基于改进IKE的移动VPN密钥协商方案

陈 楠[1] 俞定国[2] 谭成翔[2]
(杭州师范大学钱江学院 杭州 310012)[1] (同济大学计算机科学与技术系 上海 201804)[2]

摘 要 对传统IKE协议进行了改进,改进后的协议在不降低安全性的前提下实现了移动用户远程安全接入,以便其获得内网信息;扩展了IKE的认证方式,使其具有更高的协商效率和更强的可控性;实现了相应的移动VPN接入系统,该系统既支持动态内网IP分配,又支持扩展用户身份认证,从而在接入服务器端可以方便地进行基于内网IP的访问控制管理。

关键词 移动VPN,IPSec,IKE,身份认证
中图法分类号 TP393.08 **文献标识码** A

Key Exchange Solution of Mobile VPN Based on Improved IKE

CHEN Nan[1] YU Ding-guo[2] TAN Cheng-xiang[2]
(School of Qianjiang, Hangzhou Normal University, Hangzhou 310012, China)[1]
(Department of Computer, Tongji University, Shanghai 201804, China)[2]

Abstract One new solution of the key exchange introduced in this paper does improve the IKE protocol. This solution not only allows the remote mobile users security access to the intranet and get the intranet information on the premise of no reduction in security, but also extent the ways of IKE authentication, making it more efficient in negotiation and more controllable. Besides, the solution develops a corresponding mobile VPN access system which supports both dynamic distribution of intranet IP address and the extension of user identity authentication. Thus the access server can easily control and manage the intranet IP-based access.

Keywords Mobile VPN, IPSec, IKE, Identity authentication

智能终端和无线网络通讯的迅速发展使得人们可以很方便地利用移动智能终端随时随地接入因特网。但是目前机密性要求较高的业务在移动终端上的应用却很少,这是由于移动网络是开放的网络,它除了需要面对固定网络所具有的安全威胁之外,还面临着带宽低、干扰大、稳定性差、容易丢包、更容易受到窃听等问题。同时,智能终端还具有计算能力低、存储容量小、IP地址不固定的特点。移动VPN[1]技术基本满足了这种需求,采用基于IPSec[2]的VPN技术来保障移动终端的安全接入,是目前的研究热点。

IKE(Internet Key Exchange)[3]为IPSec提供自动密钥协商和交换,建立安全联盟(Security Association,SA)等服务,它具有一套自我保护机制,可以在不安全的网络上安全地分发密钥、验证身份、建立IPSec安全联盟。然而,对于远程接入用户,除了需要建立安全联盟,还需要获得安全接入服务器的内部网络信息,而这些在标准IKE中均未定义。针对此问题,现在广泛应用的解决方案有IETF提出的基于IKE的IPSec隧道模式下的DHCP配置方法[5],以及微软提出的基于L2TP/IPSec的解决方案[4]。DHCP/IPSec方案由IPSec远程接入客户端首先生成临时DHCP SA,然后在此SA保护下产生DHCP请求消息。IPSec远程接入服务器作为DHCP中继代理,将消息传送到内网的DHCP服务器,为远程接入客户端分配内网IP。此方案的不足之处是需要临时建立一个DHCP SA,不仅延长了IKE交互时间,同时给远程接入服务器带来了较大负担。而且由于接入服务器难以控制DHCP服务器,使得不同身份的用户能够选择不同的地址池分配内部地址,引发访问控制困难。而将L2TP(Layer Two Tunneling Protocol)与IPSec结合的方案虽然可以实现内网地址动态分配以及用户名、密码扩展认证,但需要额外进行L2TP协商,并且在IPSec数据传输过程中需要多次封装,导致效率低下。如何设计合理的IKE协商过程,并且不影响系统的安全性以及效率性就显得非常重要。

为了克服目前基于标准IKE的远程接入方案在系统效率和用户访问控制方面的缺陷,本文在对标准IKE改进的基础上,提出了一种移动设备与安全接入网关间密钥交换协商方案,并实现了相应的移动VPN系统。系统既支持动态内网IP分配,又支持扩展用户身份认证,从而在接入服务器端可以方便地进行基于内网IP的访问控制管理。

1 IKE协议介绍

IKE协议为IPSec隧道的两端提供用于生成加密密钥和认证密钥的密钥信息服务,以完成SA。IKE协议是IETF定义的一种混合型协议,由ISAKMP[6],OAKLEY[7]和

到稿日期:2010-08-24 返修日期:2010-11-11 本文受国家"863"计划基金项目(2006AA01Z438)资助。
陈 楠(1976—),女,讲师,主要研究方向为移动计算、信息安全,E-mail:ermunan@126.com;俞定国(1976—),男,博士生,讲师,主要研究方向为移动计算、信息安全;谭成翔(1965—),男,研究员,博士生导师,主要研究方向为信息安全。

SKEM[8]组成。ISAKMP协议是一种密钥交换框架，独立于具体的密钥交换协议。它定义了消息交换的体系结构，包括两个IPSec对等体间的分组结构和状态转换；OAKLEY协议提出了基于模式的机制在两个IPSec对等体之间达成相同加密密钥；SKEME协议描述了一种通用的密钥交换技术，提供了基于公钥的身份认证和快速密钥刷新服务。

IKE目前有两个版本：IKEv1[3]和IKEv2[9]。IKE协商的安全参数包括加密机制、散列机制、认证机制、D-H组、密钥资源以及IKE SA(ISAKMP SA)协商的时间限制等。其交换的最终结果是一个通过验证的密钥以及建立在双方同意基础上的安全联盟SA。IKEv1为每一阶段定义了不同的交换模式。对于IKEv1第1阶段，可以由主模式或野蛮模式实现。主模式能够确保密钥交换过程中IKE双方身份的隐蔽性，但它需要更多的消息交换；野蛮模式可以较少的消息交换实现IKE SA的协商，但它暴露了IKE双方的身份。对于IKEv1第2阶段，可以由快速模式实现，它处于IKE SA的保护之下，能够实现IPSec SA的快速协商，完成对传输的IP数据报的加密和完整性保护。IKEv2保留了IKEv1的基本功能，同时整合了NAT穿越、遗传认证、远程地址采集等内容，形成了一个完整的IKE协议。IKEv2在具体消息载荷上做了改进，并减少了协商轮数。在保证安全性的前提下，将第1阶段中主模式交换的消息条数由6条减少到4条，第2阶段的消息由3条变为两条，提高了协商效率。若无特别说明，下述IKE均指IKEv1。

2 IKE的改进及工作流程分析

标准的IKE阶段1的主模式交互分为3个步骤：消息1，2就加密算法、hash算法、认证方法、D-H组的选择等参数进行协商；消息3，4进行D-H交互，通信双方交换一些D-H算法，生成共享密钥所需要的基本材料信息，继而各自生成完全一样的“主密钥”，保护紧接其后的认证过程；消息5，6进行D-H认证，D-H交换需要得到进一步认证，如果认证不成功，通信将无法继续。本文对IKE的改进主要针对IKE第1阶段协商主模式的第3次交互。其它交互内容及方式同标准IKE协议。下面分析修改的内容及交互过程。

2.1 改进内容

为适应移动环境下IPSec VPN的实时性需求，简化后续业务内网IP的分配设计，我们在第5条消息中自定义一个IP-Req载荷，将用户的验证信息作为向服务器申请虚拟IP地址的请求；在第6条消息中增加一个自定义的IP地址响应载荷(IP-Reply)，将分配的内网IP地址返回给移动终端。消息5和消息6的数据包格式如图1和图2所示，重新设计后的IKE阶段1主模式信息交互流程如图3所示。

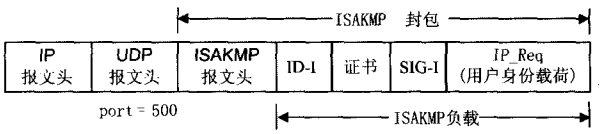

图1 消息5数据包格式

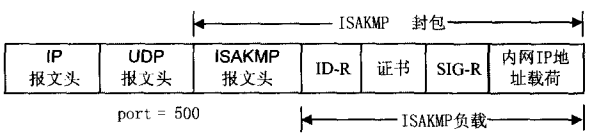

图2 消息6数据包格式

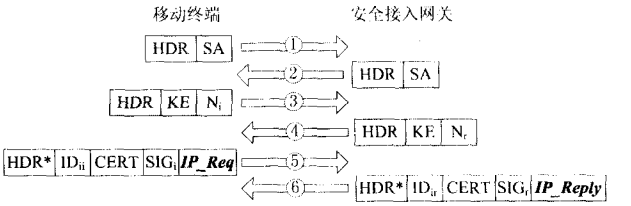

图3 修改后的IKE第1阶段主模式信息交互流程

2.2 协商工作流程

第3次消息交互是进行用户身份的认证，并建立IKE SA。其中还要完成内网IP地址的分配工作，其具体步骤是：1) 移动终端向安全接入网关发送IKE协商第1阶段主模式的第5条消息，包括标识数据ID-I、证书载荷以及自定义的用户身份载荷(用户名和密码组合)；2) 安全接入网关从移动终端接收第5条消息，从消息的用户身份载荷中提取用户身份信息，并将此信息传递给用户管理服务器。用户管理服务器首先验证用户身份合法性，若身份验证失败，则终止后续IKE协商；若是合法用户，则根据用户身份分配合适的内网IP地址，并将此内网IP地址返回给安全接入网关，由安全接入网关将此IP地址信息以内网地址载荷加入到第6条消息中发送给移动设备。因为第5，6条消息在传输过程中是经过加密的，所以可以保证用户的身份信息和分配的IP在传输过程中不被泄露。移动终端与安全接入网关间密钥交换协商的工作流程如图4所示。

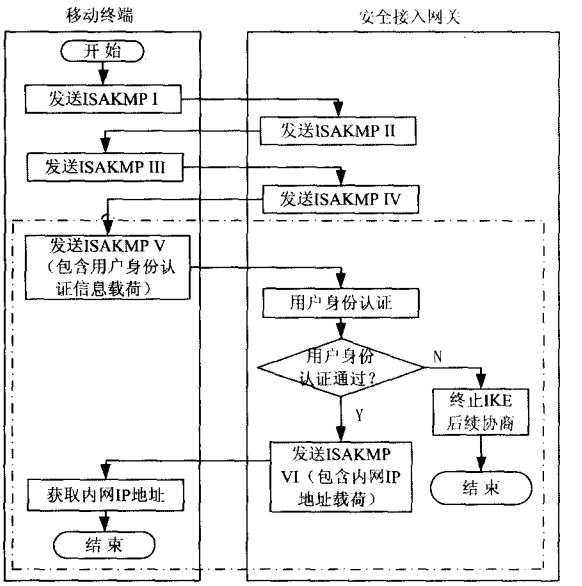

图4 移动终端与安全接入网关间密钥交换协商的工作流程

从消息5开始，ISAKMP载荷将采用由消息1和消息2协商得到的加密算法以及由消息3和消息4协商得到的加密密钥进行加密，但ISAKMP报文头本身仍然采用明文进行传输。在消息5中，双方将交换身份信息，以进行彼此的认证，ISAKMP消息中将包括终/局端身份载荷ID、证书载荷CERT以及用户身份/内网IP申请载荷(用户名+密码)。在消息6中，安全接入网关将通过验证散列来证实移动终端的身份。如果验证成功，则可以将安全接入网关的身份载荷CERT和内网IP地址载荷封装在ISAKMP消息中发送给移动终端，以使其可以进一步证实安全接入网关的身份。

安全接入网关响应移动终端第5条消息，发送第6条消

息的具体过程为：

(1) 解密消息 5；

(2) 对消息 5 进行身份验证，包括移动终端身份合法性、证书合法性以及终端用户身份合法性；

(3) 建立 ID 载荷、证书载荷(CERT-I)、内网 IP 地址载荷(IP_Reply)；

(4) 加密载荷，包括 ID 载荷、证书载荷(CERT-R)、内网 IP 地址载荷；

(5) 在状态表中将原先对应的状态删去，设置一个新的状态对象，将当前的状态改变为 STATE_MAIN_R3；

(6) 以 ISAKMP 为密钥加密整个报文并发送；

(7) 登记消息重发机制中的状态库，状态迁移；

(8) 成功，返回。

当移动终端收到消息 6 并且证实了安全接入网关的身份后，第 1 阶段的交换就完成了，准备进行第 2 阶段快速模式的协商。

3 移动 VPN 接入系统设计与实现

针对改进的 IKE 协商方法，我们设计并实现了基于 IPSec 的移动 VPN 安全接入系统原型。系统功能结构如图 5 所示。

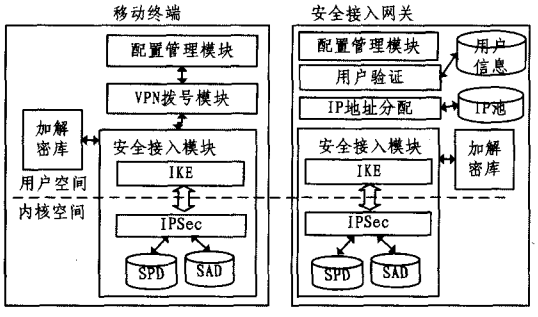

图 5 基于 IPSec 的移动 VPN 接入系统功能结构图

移动终端接入程序是基于 Visual Studio 2005 开发的，终端设备操作系统为 Windows Mobile 5.0。安全接入网关是在开源的基于 Linux 平台的 IPSec VPN 系统 Openswan 2.4.7[10,11] 基础上开发实现的，网关服务器操作系统为 Red Hat Enterprise Linux 5.0。

安全接入网关的安全接入模块主要实现基本的 IPSec 功能和内网 IP 分配功能，其主要子模块细化为 IKE 密钥协商模块、内核 IPSec 模块、内网 IP 地址分配模块和用户验证模块。

参照 Openswan 的设计，安全接入网关的安全接入模块主要分为应用层部分和内核层部分。应用层部分主要是 IKE 密钥协商模块，其主要功能是密钥协商管理，通过 SADB 和 SPDB 对密钥进行管理，为 IPSec 模块处理数据包提供策略依据；内核层部分由 IPSec 模块实现，它负责接入服务的内核层部分的实现，它的功能包括建立/维护 SA、管理 SAD/SPD、对 IPSec 进出数据包进行解析/组包处理、对数据进行加解密等。IPSec 模块和 IKE 模块之间通过 SADB，SPDB 联系。另外，在应用层上设计了内网 IP 地址分配模块和用户验证模块。用户验证模块实现对用户身份合法性的判断，为内网 IP 地址分配模块服务；内网 IP 地址分配模块也为 IKE 模块服务，对移动终端分配或释放内网 IP 地址，通过与 IKE 模块的交互，在 IKE 协商阶段即完成向移动用户分配内网 IP 地址的任务，简化整个 IPSec VPN 的流程和实现。

IKE 模块运行于应用层，是 IKE 协议的具体实现，可以自动完成 VPN 网关与移动终端间的安全联盟的协商工作。协商成功获得的 IPSec SA 能够被内核模块用来完成对输入、输出数据包的加密、认证工作。如果 IKE 协商失败，同返回错误类型信息；否则，返回 SA、密钥以及 SPI，递交给内核处理。

IKE 模块是在当前开源的 Openswan 中 IKE 实现模块 Pluto 的基础上进一步开发的，更符合移动环境下 IKE 协商的需求。针对移动网络不稳定、速度慢的弊病，改进原有密钥协商机制设计，使得移动终端和虚拟专用网网关两个应用层进程实体间可以通过 ISAKMP/UDP 进行密钥交换，并在 PF_KEY 协议和系统内核的 IP 协议栈间进行密钥存取与修改消息的交互。IKE 模块在系统中作为一个守护进程在后台运行，负责同协商实体的交互、对 IKE 载荷的加密验证处理以及同内核的交互。IKE 守护进程可通过共享内存或 Socket 消息通信的方法完成与应用层管理进程之间的通信；通过 PF_KEY 套接口完成与 IPSec 安全内核之间的消息通信，完成对 SA 队列的修改、增加、删除的操作；通过 AF_INET 套接口在 socket 通信机制下对采用 UDP 传输协议方式的 500 号端口进行监听及收发，完成 ISAKMP 数据包的发送与接收，进行动态密钥交换机制中的两个阶段关于 SA 的协商过程，最终在两个安全网关之间协商出 IPSec 保护数据包所需的安全关联。

4 系统测试

系统测试环境如图 6 所示。移动终端设备为多普达 D600 智能手机，操作系统为 Windows Mobile 5.0；VPN 安全接入网关服务器操作系统为 Red Hat Enterprise Linux 5.0，内核为 Linux 2.6.18；移动应用服务器操作系统为 Windows 2003，提供 FTP 和 Web 服务。

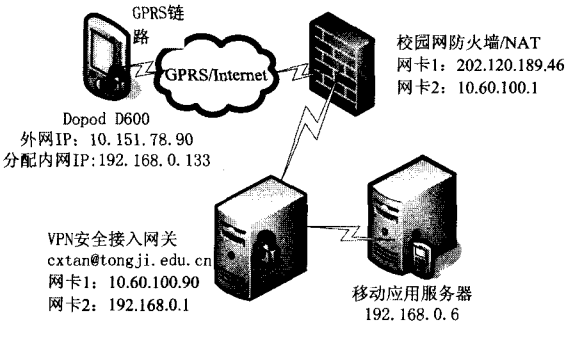

图 6 系统测试环境

在以上环境中，我们对用户身份认证、防火墙及 NAT 穿越、虚拟内网 IP 的分配与回收、访问控制和抗中间人攻击等内容进行了测试。实验结果表明，本方案可以很好地得到实现，并且可以有效地抵抗对终端的非法操作攻击、身份伪装的攻击、对链路的监听、篡改和重放的攻击以及对服务器端的否认服务、非法访问的攻击等。内网 IP 地址分配过程的部分程序执行如图 7 所示。

(下转第 99 页)

上，新算法还实现了在 SPT 中增加和删除节点。需要表明的是，删除节点的操作只是修改图中与此节点连接的边的权值为无穷大，而增加节点则需要在图中生成新边，所以增加节点较删除节点消耗更多的时间。

实验 3 在 SPT 节点规模为 1 万～10 万之间进行。实验分两部分，第一部分在 SPT 上连续删除 1000 个节点；第二部分在 SPT 上增加 100 个节点。第一部分实验数据见图 7，时间单位为 μs。第二部分实验数据见图 8，时间单位为 ms。

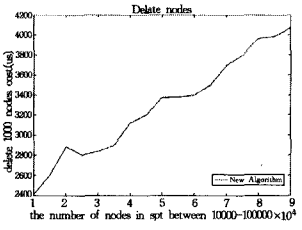

图 7 新算法在 SPT 上删除节点

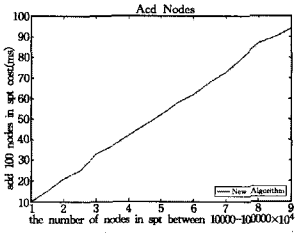

图 8 新算法在 SPT 上增加节点

结束语 新算法在 Ball-and-String 的基础上做了进一步优化。由实验数据可以看出，新算法在边的权值发生变化时更新 SPT 的效率更高。在功能上，新算法还实现了对节点的增加和删除，适合处理 SPT 的任何变化。

参 考 文 献

[1] Dijkstra E. A note two problems in connection with graphs[J]. Numerical Mathemat.,1959,1:269-271

[2] ElBlman R. On a routing problem [J]. Quarterly Appl. Mathemat.,1958,16:87-90

[3] Spira P, Pan A. On finding and updating spanning trees and shortest paths[J]. SIAM J. Computing,1975,4(3):375-380

[4] McQuillan J, Richer I, Rosen E. The new routing algorithm for the ARPANET[J]. IEEE Trans. Commun,1980,COM-28:711-719

[5] Franciosa P, Frigioni D, Giaccio R. Semi-dynamic shortest paths and breadth-first search in digraph [C] // Proc. 14th Annu. Symp. Theoretical Aspects of Computer Science. Mar. 1997:33-46

[6] Barbenn M, Hutchinson S. Increment algorithms for single-source shortest path trees[C] // Process Foundations of Software Technology and Theoretical Computer Science. 1994:113-124

[7] Xiao B, Cao Jiang-nong, Shao Z, et al. An Efficient Algorithm for Dynamic Shortest PathTree Updatein Network Routing[J]. Journal of Communications and Networks,2007,9(4)

[8] Narvaez P, Siu K-Y, Tzeng H-Y. New dynamic algorithms for shortest path tree computation[J]. IEEE Trans. Networking, 2000,8

[9] Xiao B, Zhuge Q, Sha E H-M. Minimum dynamic update for shortest path tree construction[C] // Proceedings of the GLOBECOM'01. Nov. 2001:126-130

[10] Narvaez P, Siu K-Y, Tzeng H-Y. New dynamic SPT algorithm based on a ball-and-string model[J]. IEEE/ACM Trans. Networking,2001,9:706-718

[11] Xiao B, Cao Jian-nong. Dynamic shortest path tree update for multiple link state decrements[C] // 2004 Global Telecommunications Conference. 2004

[12] Xiao B, Cao J, Zhuge Q, et al. Dynamic update of shortest path tree in OSPF[C] // Parallel Architectures, Algorithms and Networks. May 2004:18-23

[13] Chan E P F, Yang Ya-Ya. Shortest Path Tree Computation in Dynamic Graphs[J]. IEEE Transactions on Computers,2009,58(4):541-557

(上接第 95 页)

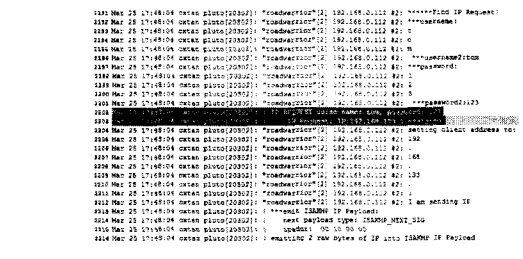

图 7 IP 地址分配程序执行过程截图

结束语 本文针对目前基于标准 IKE 的移动终端远程安全接入方案的缺陷，通过在 IKE 第 1 阶段主模式的第 5 条消息中增加用户身份载荷，接入网关根据用户身份分配合适的内网 IP 添加在第 6 条消息中，实现了对用户远程安全接入获得内网信息的支持，而且扩展了 IKE 的认证方式。根据身份分配内网 IP 的方式更有利于访问控制管理。而且，由于扩展载荷增加在第 5，6 条消息中，属于加密传输，不会降低 IKE 协商的安全性。因此，本方案不仅满足远程客户的安全接入需求，而且具有更高的协商效率、更强的可控性及灵活性，可以有效地满足用户对移动办公的安全需求。

参 考 文 献

[1] Davis C R. IPSec VPN 的安全实施[M]. 周永彬，冯登国，徐震，等译. 北京：清华大学出版社，2002

[2] Kent S, Seo K. Security Architecture for the Internet Protocol [S]. RFC 4301, Dec. 2005

[3] Harkins D, Carrel D. The Internet Key Exchange (IKE) [S]. RFC 2409, Nov. 1998

[4] Zhao A-qun, Yuan Yuan, Ji Yi, et al. Research on tunneling techniques in virtual private networks[C] // Proceedings of Communication Technology(WCC-ICCT 2000). 2000:691-697

[5] Hue C A, Kalafut A J, Gupta M. A Unified Approach to Intra-domain Security[C] // Computational Science and Engineering (CSE '09). 2009:219-224

[6] Maughhan D, Sehertler M, Sclmeider M, et al. Internet Security Association and Key Management Protocol (ISAKMP) [S]. RFC2408, Nov. 1998

[7] Orman H. The OAKLEY Key Determination Protocol [S]. RFC2412, Nov. 1998

[8] Krawczyk H. SKEME: A Versatile Secure Key Exchange Mechanism for Internet[C] // IEEE Proceedings of the 1996 Symposium on Network and Distributed Systems Security. 1996

[9] Kaufman C. Internet Key Exchange(IKEv2) Protocol[S]. IETF RFC4306, Sep. 2004

[10] Wouters P, Bantoft K. Building and Integrating Virtual Private Networks with Openswan[EB/OL]. http://www.openswan.org/,2009

[11] Ren Qing-liang, Zhou Jian. Implementation of Dynamic VPN Based on Openswan[J]. JHUT,2006

[12] 董晓虎，徐明伟，徐恪. 密钥交换协议 IKE 实现的可扩展设计[J]. 小型微型计算机系统，2004,25(6):1000-1004