一种基于IKE协议的移动VPN安全通信方案

舒明磊 谭成翔 谭 博
(同济大学电信学院计算机系 上海 201804)

摘 要 实现移动终端的安全接入、移动通信的安全传输是智能移动终端普及和移动业务扩展的重要环节。以保证移动数据安全交换为目的,针对移动终端接入企业内网所面临的安全问题,提出了一种移动VPN(Virtual Private Network)通信方案。方案对IPSec VPN的IKE(Internet Key Exchange)协商流程进行了改进,能支持多因子认证和基于角色的访问控制。分析和实验测试证明了方案的安全性和可行性。

关键词 IPSec VPN,移动安全接入,IKE,多因子验证
中图法分类号 TP393.08 **文献标识码** A

Secure Communication Scheme of Mobile VPN Based on IKE Protocol

SHU Ming-lei TAN Cheng-xiang TAN Bo
(Department of Computer, College of Electronics and Information, Tongji University, Shanghai 201804, China)

Abstract The security access control of mobile terminals and secure transmission of mobile data play an important role for the widespread usage of mobile intelligent terminals and the extension of mobile service. According to the security problem when mobile terminals access intranet, this paper put forward a secure communication scheme of mobile VPN with the aim of security exchange for mobile data. The scheme improved the negotiation process IKE protocol which is one of the important protocols in IPsec protocol suite, and the scheme can support multifactor authentication and role-based access control. The results of theoretical analysis and experiments demonstrate the practicability and the security of our scheme.

Keywords IPSec virtual private network, Mobile secure access, Internet key exchange protocol, Multifactor authentication

1 引言

移动终端设备的日益普及和相关业务的全面开展,使得终端用户的工作变得非常快捷和便利。然而由于移动网络自身传输介质和通信信道等因素的特性,与固网业务相比,移动业务更易于受到窃听、篡改和终端假冒等网络攻击。如果移动业务的安全性能不能得到保障,必然会诱发诸如移动电子政务、移动电子商务等具有大量敏感信息的相关业务的巨大安全隐患。因此,研究建立可靠的移动网络安全信息服务系统,一直是移动通讯安全领域的重要课题。采用无线专用网络是保证无线数据高效无误地进行通信的一种有效途径,但其使用成本高昂,覆盖范围受限,推广应用的可行性很低。移动VPN(Virtual Private Network)[1]技术则没有上述局限,它允许客户在各种公共移动通信网络上通过终端设备,与政府或企业的内部可信服务之间建立起安全、透明的连接。本文根据移动网络、终端设备的特性和安全需求,提出了一种基于IKE(Internet Key Exchange)协议的移动VPN接入解决方案,使得移动节点可跨异构网络漫游。分析和实验均表明了该安全方案的数据安全性及操作可行性。

2 移动VPN技术

移动VPN技术由传统的固网VPN技术发展而来,它为终端用户提供远程安全接入服务,使其可以通过公共无线网络接入到专用的内部网络中。现有的移动VPN技术大多是在应用层或网络层上实现的。在应用层上实现的移动VPN方案有Columbitech公司的无线VPN方案[2]和英国British Telecom提出的WAP远程访问解决方案[3]等。应用层移动VPN方案遵循的协议有SSL(Security Socket Layer)协议,TLS(Transport Layer Security)协议和WTLS(Wireless Transport Layer Security)协议。由这些协议构建的安全隧道具有会话恢复机制,可在安全隧道中断后快速透明地对上层应用实现重建,而且由于实施在会话层以上的层面,因此不会涉及到防火墙、NAT(Network Address Translation)网关屏蔽的问题。但是它对于保障移动终端的可信使用和安全管控等方面存在缺陷,能够挂接捆绑的应用服务也较为单一。网络层的主要实现方案有Cisco的企业级无线数据交换解决方案[4]、Bird Step公司的移动VPN方案[5]和Nokia公司的基于Symbian OS的移动用户安全管理VPN[6]等。这些方案的

到稿日期:2009-11-26 返修日期:2010-01-11 本文受国家"863"计划基金项目(2006AA01Z438)资助。
舒明磊(1979-),男,博士生,主要研究方向为身份认证、移动VPN等,E-mail:shuminglei@yahoo.com.cn;谭成翔(1965-),男,博士生导师,主要研究方向为信息安全、移动计算等;谭 博(1979-),男,博士生,主要研究方向为电子商务安全等。

特点是采用 IPSec(Internet Protocol Security)协议构建从移动节点到企业 VPN 网关的安全隧道,利用移动 IP 技术保证节点在网络切换时对上层应用的透明性,但它们采用的是专用终端的方式,无法灵活地支持应用接入,而且需要终端用户均采用对应指定的产品设备,实现成本较高。

SSL VPN 适用于建立端到端的以浏览器形式进行数据访问的安全无缝接入方案[7],IPSec VPN 适用于构建支持多种应用的端到端的虚拟逻辑子网链路。对于应用种类、应用安全的覆盖宽度要求较高的领域,IPSec VPN 更易于提供全面的解决方案[8]。在移动 IPSec VPN 系统中,终端向 IPSec VPN 网关发起接入请求,与之协商和建立安全通信隧道及隧道所需要的虚拟内网 IP,在 GSM/GPRS/CDMA 信道中成功建立 VPN 隧道之后,通过该隧道与 VPN 网关传输交换加密的数据。对于一个完善的移动 VPN 方案,它的安全性要素不仅包括系统中数据信息在终端、移动网络和固定网络之间传递的安全可靠性,还必须包括终端设备计算能力较弱、存储容量较小以及手机终端易于遗失等因素,而且在网络中存在防火墙、NAT 时,需要具备 NAT 穿越功能。

3 IKE 协议

IKE 协议[9]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以完成 SA(Security Association)并对 SA 数据库进行填充,同时它也为 IPSec 的其它协议生成 SA。IKE 属于混合型协议[10],主要有 3 个组成部分,它在 ISAKMP(Internet Security Association and Key Management Protocol)协议的框架基础上,综合了负责密钥交换的 Oakley 协议和负责共享及更新密钥的 SKEME(Secure Key Exchange Mechanism)协议。IKE 定义的可能的交换模式有 4 种,分别是主模式(Main Mode)、野蛮模式(Aggressive Mode)、快速模式(Quick Mode)和新群(New Group Mode)模式,前 3 个用于 SA 协商,最后一个用于为 D-H(Diffie-Hellman)密钥交换协商一个新的群。它的安全密钥交换过程分为两个阶段[11],第一阶段为通信双方协商一个 SA 隧道并用它保障 IPSec 的其它协议建立 SA 的协商过程的安全保密性,第二阶段使用已建立的 SA 协商建立 IPSec 其它安全服务的 SA。IKE 目前有 IKEv1 和 IKEv2 两个版本。IKEv2[12]保留了 IKEv1 的基本功能,并在确保安全性的前提下,对具体消息载荷和消息交换作了改进,同时也减少了协商轮数,提高了协商效率。

本文对 IKE SA 协商阶段的会话消息进行了修改,在不增加协商消息条数的情况下,在载荷中加入内网 IP 分配请求和移动终端的多因子验证参数等数据,以确保移动通信系统中数据信息的机密、完整和可信传输。

4 接入解决方案

4.1 网络拓扑架构

移动终端客户通过公共移动网络接入单位内部信息系统的典型网络拓扑如图 1 所示,它的应用环境包括终端、移动网络、因特网、VPN 网关以及企业内网。在整个应用环境中,负责客户接入安全和数据交换安全的 VPN 网关服务器处于移动安全通信平台的核心地位。

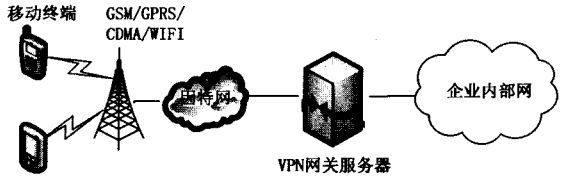

图 1 典型网络拓扑

4.2 符号说明

T:终端客户;

M:移动网络;

G:VPN 网关;

X →Y:Z 表示 X 发送消息 Z 到 Y;

P ※Q:K 表示 P 和 Q 之间互相传送消息 K;

HDR:表示 ISAKMP 头,它的交换类型就是采用的交换模式,HDR * 表明 ISAKMP 头后面的是加密载荷;

SA:带有一个或多个建议载荷的安全关联联盟;

KE:密钥交换载荷;

IDx:标识载荷,其中 x 是 ii 或者 ir,ii 代表 ISAKMP 发起者,ir 代表 ISAKMP 响应者;

HASH:杂凑载荷;

Cert-R:证书请求载荷;

CERT:证书;

AUTH:用户名、密码;

IP-Req:IP 地址请求载荷;

IP-Reply:IP 地址载荷;

NAT-T:NAT 穿越;

NAT-D:本地 IP 地址及端口的 HASH 值。

4.3 建立 VPN 连接

①T →M:用户名、密码,VPN 连接请求;

②T ※G:IKE 第一阶段协商参数;

③G:根据用户组信息,认证包含 IMEI & IMSI 信息在内的身份证书以及用户口令;

④G:分配虚拟内网 IP;

⑤G →T:虚拟内网 IP,IKE SA;

⑥T ※G:IPSec SA 协商参数;

⑦G →T:IPSec SA。

IPSec VPN 连接成功后,移动终端获得一个 IPSec SA 以及一个虚拟内网 IP 地址,此时终端就可以通过 IPSec 隧道像企业内网用户一样依据自身的权限访问企业内网的各种服务和资源。

4.4 IKE 第一阶段协商

本文设计方案的 IKE 阶段 1 主模式交互流程如图 2 所示。

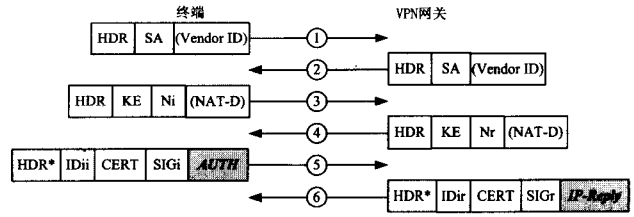

图 2 IKE 阶段 1 主模式信息交互流程

其中第 5 条消息和第 6 消息完成 D-H 认证,第 5 条消息中 AUTH 的作用是进行地址请求和加载包括 IMEI(Interna-

tional Mobile Equipment Identity)和 IMSI(International Mobile Subscriber Identity)在内的用户认证信息,第 6 条消息中 IP-Reply 为接入网关根据身份验证的结果生成的 IP 地址响应载荷并分配对应群组权限。为实现 NAT-T,在 IKE 包头中加入了整合地址和端口号的散列值,接收方使用 NAT-D 检查是否存在一个经 NAT 转换过的地址或端口号,并根据被改变的地址和端口号来确定对话方位置,当防火墙阻止在 UDP 500,UDP4500 端口进行通信时,数据包转发到端口 UDP 53 或 UDP 80。

4.5 业务请求与响应

① T→G:业务请求;

② G:访问控制权限验证;

③ G:转发业务请求;

④ G→T:业务数据。

4.6 断开 VPN 连接

① T→G:断开 VPN 连接请求;

② G:删除 IKE SA,IPSec SA,回收 IP 地址;

③ G→T:响应断开请求。

5 性能分析

本文提出的接入方案有良好的安全性和可行性。

1) 数据安全。移动终端与 VPN 接入服务器之间所传输的数据流经过基于 IPSec 的 VPN 隧道加以保护,在建立 VPN 连接的过程中,终端与服务器端首先进行证书互认证和 IKE 动态协商,攻击者即使在中途窃听、截获无线链路中的密文包,也无法正确分析出数据包中的有效信息,难以假冒局端诱骗移动终端,从而提供接入传输过程中的数据完整新鲜性、数据源认证、拒绝包重放等安全服务。

2)设备安全。采用了多因子认证的形式,即结合了 IMEI & IMSI 的基于证书和用户口令的扩展认证方式,可抵抗手机遗失带来的安全威胁。

3)基于角色的访问控制。VPN 网关采用基于用户身份的地址池分配策略,由内部地址池管理模块根据用户所属组信息分配一个唯一标识的虚拟 IP 地址,允许用户使用此 IP 地址来通过隧道方式访问网关后面的子网资源。

4)实现成本。鉴于移动终端的计算和存储性能都无法比拟台式设备的特性,方案对智能终端的计算能力没有过高的要求,也没有特定机型的限制,因此可以部署在通用的智能终端上。而且,在第 5 条交互的消息中加入了用户登录信息,此时一旦发现用户是非法身份,就可以立即中止 IKE 协商,如果是合法身份,则可以减少加解密消息次数,节省 VPN 建立过程中的系统开销。

6 系统实验与测试

本文对设计的方案进行了实现,其中 VPN 安全接入网关部署在防火墙和移动应用服务器之间,用于对内网与外部 Internet 进行分隔。终端操作系统为 Windows Mobile 5.0,网关操作系统使用 RedHat Linux,Linux Kernel 版号为 2.6.23,VPN 服务器使用 Openswan 2.4.7,开发环境为 Visual Studio 2005。

采用黑盒测试方法,对多因子认证过程、防火墙及 NAT 穿越、基于角色的虚拟内网 IP 的分配与回收、抗中间人攻击等内容进行了测试。实验结果表明,该方案可以完好地得到实现,并且可以有效地抵抗对于终端的非法操作攻击,身份伪装的攻击,对于链路的监听、篡改和重放的攻击,以及对于服务器端的否认服务、非法访问的攻击等等。

结束语 建立一个安全可信的移动信息传输环境,可以有效地满足客户对于移动办公的安全需求,因而具有重要的研究价值和应用前景。本文设计了一种新的 IKE 机制,在它的基础之上提出了一个 IPSec VPN 移动信息安全接入解决方案,该方案采用多种因子认证方式,支持根据客户角色级别提供对应服务,为数据信息的安全传输提供了保障。由于本文在实现 IKE 协商时,采用的版本是 IKEv1,下一步的工作是使用 IKEv2 标准改进交互流程,以进一步优化消息交互的过程,提高系统的整体效率。

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] Columbitech A B. Columbitech Wireless VPN technical Description [EB/OL]. http://www.columbitech.com/Products/WVPN.asp,2004

[3] Rao G. NET6 Hybrid-VPN Gateway [EB/OL]. http://www.citrix.it/REPOSITORY/docRepository/id_900_1112979921897309.pdf,2004

[4] Cisco Systems. Enterprise Mobile Wireless Data Solutions 1.0, White paper [EB/OL]. http://www.cisco.com/en/US/netsol/ns341/ns396/ns177/networking_solutions_white_paper09186a00802252b2.shtml,Aug. 2003

[5] BirdStep Corp. Introducing Birdstep Intelligent Mobile IP,v2.0 Universal Edition [EB/OL]. http://www.birdstep.com/Products/Birdstep/Birdstep-Intelligent-Mobile-IP,2004

[6] Nokia Inc. White Paper: The Evolution of Mobile VPN and its Implications for Security [EB/OL]. http://www.nokia.com/NOKIA_COM_1/About_Nokia/Press/White_Papers/pdf_files/whitepaper_evolutionofmobilevpn.pdf,2005

[7] 欧阳凯,周敬利,夏涛,等. 基于 SSL VPN 接入机制的研究[J]. 计算机科学,2005,32(5):59-63

[8] Rosenbaun G,Lau W,J ha S. An analysis of virtual private network solutions [J]. Local Computer Networks,2003,10:395-404

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

[10] Borella M S. Methods and protocols for Secure Key Negotiation Using IKE [J]. IEEE Network,2000,14(4):18-29

[11] 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

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