基于Socks5代理的移动SSL VPN系统研究与实现

俞定国 舒明磊 谭成翔
(同济大学计算机科学与技术系 上海 201804)

摘 要 针对传统基于IPSec和SSL技术的移动VPN的不足,提出一种基于Socks5代理的移动SSL VPN解决方案。分析了系统的实现原理和过程,并介绍了系统的总体框架和工作流程。最后对系统进行了实现和测试,并对系统安全性能和接入、传输效率进行了分析。

关键词 SSL,Socks,移动VPN,信息安全
中图法分类号 TP393.08 **文献标识码** A

Research and Implementation of Mobile SSL VPN System Based on Socks5 Proxy

YU Ding-guo SHU Ming-lei TAN Cheng-xiang
(Department of Computer, Tongji University, Shanghai 201804, China)

Abstract We studied the current weaknesses of the mobile VPN based on traditional IPSec and SSL technology to present a solution of mobile SSL VPN based on socks5 proxy. This paper analysed the principle and the implementation process of the mobile SSL VPN, and introduced the framework and workflow of this system. Finally, we implemented and tested this system, and analyzed its security performance, access and data transmission efficiency.

Keywords SSL, Socks, Mobile VPN, Information security

随着移动通讯技术的发展和智能终端的普及,人们可以将移动终端设备通过移动网络随时随地接入因特网。但在目前,关键性、机密性要求高的业务在移动终端设备中的应用却很少,其原因主要是安全问题。

移动VPN的出现基本满足了这种需求,但当前的移动VPN技术基本是借用IPSec VPN或者SSL VPN技术,而IPSec和SSL技术最早都是针对固网的安全问题提出的。与传统的固网VPN不同,移动VPN还需要解决移动性所带来的问题,如要适应不同无线网络之间的切换和IP地址的变动;带宽低、延迟大、出错率高和传输不稳定等移动网络特性;通常的移动终端计算能力低,存储容量小。另外,移动终端设备的操作系也统差别较大,有些移动操作系统如Symbian甚至没有开放网络底层接口。这些因素都对移动VPN在性能和安全性上的设计提出了新的要求。

针对现有的移动VPN系统的不足,尤其是无法容易实现移动网络中不间断的安全传输问题,本文利用SSL和Socks代理技术相结合的方法,提出了一种新的移动VPN解决方案,即使用高效简便的方法保证应用程序与应用服务器之间的不间断安全传输,而且能够使其方便地实现在不同的移动终端平台上。

1 相关工作和技术

移动VPN的实现目前主要是借鉴传统固网VPN的思想和其中的关键技术,并针对无线环境的特点进行移植和改进。在移动环境中,IPSec和SSL仍然是实现VPN的两种主流技术,同时,由于IPSec和SSL所处的网络层次不同,在处理无线环境带来的问题时,一般会采取不同的策略和方式。

IPSec是为IP层提供数据通信安全保护而制定的一套协议族[1],但它无法支持变动的IP地址。当移动终端IP地址变动时,IPSec必须重新进行IKE协商,IKE协商需要进行大量的计算,这将给移动终端造成较大负担。移动IP是IETF移动IP工作组提出的一套新的IP路由机制和协议,是为解决Internet中节点的移动性而引入的网络层协议,它在网络节点位置移动时,保持通信过程而不需要重新配置IP参数。所以一般使用移动IP作为IPSec的承载协议,为IPSec提供移动性,屏蔽了移动节点网络切换对IPSec隧道的影响。S. Vaaralah和E. Klovning针对IPSec和移动IPv4之间存在的兼容性问题提出相应的解决方案[2]。V. Devarapalli和P. Eronen提出了一种结合移动IPv4和MOBIKE(mobility extensions to IKEv2)实现移动IPSec VPN的方案[3]。文献[4]给出了一套完整的运营商如何部署移动IPSec VPN的方案。文献[5]提出了一种基于移动IPv6的移动IPSec VPN解决方案。另外常见的移动IPSec VPN系统还有Nokia IPSec VPN[6],Bird Step公司的移动VPN[7]和Cisco VPN[8]等。IPSec与移动IP技术相结合的方法,虽隐藏了IP地址变化对IPSec的影响,然而这种方法需要传输层来实现数据流控制和会话恢复功能,增加了系统的复杂性,而且无法在不开放网络底层接口的移动终端系统上实现。

到稿日期:2010-03-09 返修日期:2010-05-14 本文受国家"863"高技术研究发展计划项目(2006AA01Z438)资助。
俞定国(1976-),男,博士生,主要研究方向为移动计算、信息安全,E-mail:zjydg@163.com;舒明磊(1979-),男,博士生,主要研究方向为身份认证、安全短信;谭成翔(1965年-),男,研究员,博士生导师,主要研究方向为移动计算、信息安全。

SSL 是 1994 年 Netscape 公司为了保护 Web 通信安全而开发的，1997 年 IETF 将其进行了标准化，并称为 TLS (Transport Layer Security)[9]。通过在应用层和网络层之间插入 SSL 处理逻辑，为应用层数据提供一个安全的透明传输通道。SSL 协议的优点在于对应用层透明，而且不受现有 IPv4 网络中 NAT 穿透问题的影响。另外关于数据报传输过程中的超时和丢报重传一类的问题，都可以由 TCP 来完成。针对移动终端设备的处理和存储能力较弱的现象，在 TLS 基础上做了简化，提出了 WTLS 协议[10]，以适应无线的特殊环境。WTLS 协议增加了对数据报协议的支持，对传输分组大小进行了优化，以及允许动态密钥更新等。文献[11]对 WTLS 的握手协议进行改进，提出了一种快速恢复 WTLS 会话的新方法，支持了移动 SSL VPN 能够快速恢复 SSL 会话。目前常见的移动 SSL VPN 方案主要有 WAP 远程访问 技术[11]、Columbitech Wireless VPN[12] 和 NET6 的 Hybrid VPN[13]等。

Socks 代理的初衷是为了支持应用穿越防火墙访问外部网络的一个协议。Socks[14]在协议栈的 TCP 层上运行，是介于传输层和应用层之间的中介层协议，是为了让使用 TCP 和 UDP 的客户/服务器应用程序更方便安全地使用网络防火墙所提供的服务而设计的。对于上层应用层协议来说，Socks 代理只是简单地传递数据包，而不必关心是何种应用协议(比如 FTP，HTTP 请求)。Socks 协议的工作原理与应用代理相似，作为网络边界上的 Socks 服务器接收客户的请求，并代理外部的应用服务器，使得客户与外部的联系实质上是 Socks 客户与 Socks 服务器之间的联系；而外部的应用服务器所接受的请求是来自 Socks 服务器的外部接口，也就是说 Socks 服务器对内部网络的客户来说是服务器，对外部网络的应用服务器来说是客户。

2 系统设计与实现

2.1 总体框架

本文提出的移动 VPN 系统是一种基于异地 Socks5 代理的移动 SSL VPN 系统，该系统总体由服务器端和客户终端转发平台组成，系统总体框架如图 1 所示。

图 1 系统总体框架示意图

服务器端，包含 Socks5 代理与应用挂接单元、服务器端应用服务(后台应用服务)与 VPN 局端平台。其中，作为数据传输平台的 VPN 局端包含局端 VPN 单元和 Socks5 代理转发单元。

客户端终端，包含移动 SSL VPN 终端设备、客户端应用、Socks5 数据转发单元。其中，移动 SSL VPN 终端设备包含终端 VPN 单元和 Socks5 代理单元。它是移动终端在应用层级别上利用 Socks5 协议进行数据转发搭建安全接入 VPN 的方式。

2.2 实现原理与过程

本文提出的移动 SSL VPN 系统是通过将 SSL 技术与 socks 代理技术相结合，将应用程序的数据流转发给布置在同一移动终端的移动 VPN 终端，然后通过移动 VPN 终端与局端之间的安全隧道安全地传输数据给内网的应用服务器。代理中继的使用将网络连接分成 3 部分：应用程序到移动 VPN 终端，移动 VPN 终端到移动 VPN 局端，移动 VPN 局端到内网应用服务器。3 个部分的连接相互独立，同时只有移动 VPN 终端到移动 VPN 局端之间的连接涉及无线环境，所以只要在移动 VPN 终端与局端之间实现会话快速恢复和数据流控制功能，就可以实现应用程序与内网服务器之间的不间断传输。本方案所涉及的技术都工作在应用层，不需要操作系统提供底层的网络接口，所以可以方便地实现在不同的移动操作系统上。具体实现过程如图 2 所示。

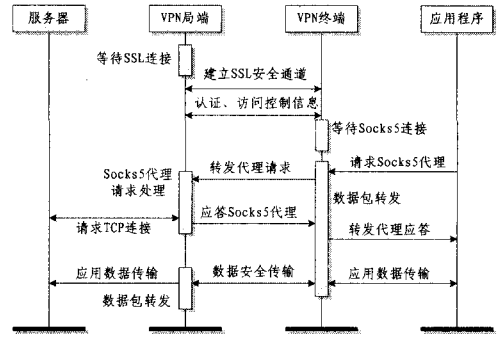

图 2 系统实现过程示意图

1)安全传输：VPN 终端与 VPN 局端之间使用 SSL 协议进行安全传输，给代理请求数据和应用数据提供一个安全的传输通道。VPN 局端在特定端口上监听 SSL 连接请求。VPN 终端首先与局端进行 SSL 握手，使用 X509 证书实现终端与局端的相互认证。建立好 SSL 通道后，终端与局端进行用户名/密码认证，从而实现多因子认证，提高安全性。然后终端与局端进行进一步协商，VPN 终端提供本身相关信息如设备标识、操作系统、安全状态等给 VPN 局端，VPN 局端根据这些信息实现访问控制，提供可访问的资源列表给终端。安全通道建立完之后，VPN 终端与 VPN 局端就可以为移动应用程序提供安全传输功能。

2)后台挂接：VPN 终端与局端共同实现 Socks5 代理服务器的功能：VPN 终端实现代理请求转发和传输数据的转发，VPN 局端实现 Socks5 代理逻辑。VPN 终端程序在移动设备上开启 Socks5 监听端口，处于同一设备上的应用程序向该端口发起代理请求，VPN 终端程序转发代理请求给 VPN 局端，VPN 局端程序处理代理请求，与服务器建立连接。代理连接建立好之后，应用程序与服务器之间通过由 VPN 终端和 VPN 局端组成的代理服务器转发数据，实现数据的交互。Socks5 代理支持 TCP 协议和 UDP 协议。

2.3 工作流程

1) 终端工作流程

终端具体工作流程如图 3 所示。首先终端从用户界面读取的参数与 VPN 服务器协商建立 SSL 通道，此步骤完成后，用户将自身用户名和密码经过自定义的数据结构封装成数据包通过 SSL 通道传输给 VPN 服务器。自定义的数据结构除了用于在转发中指明数据包的性质(TCP、UDP 还是控制信息)，还以端口号来保持连接来回的一致性。这样传输的数据

包除了本身需要传输的数据(该数据可以是 Socks 代理请求及相关消息,也可以是用户应用数据),还主要包括了连接的端口号、IP 地址以及数据包类型。通过认证之后,VPN 服务器返回给客户端一个可访问的资源列表。此时的数据均是经过加密通过 SSL Tunnel 传输的。

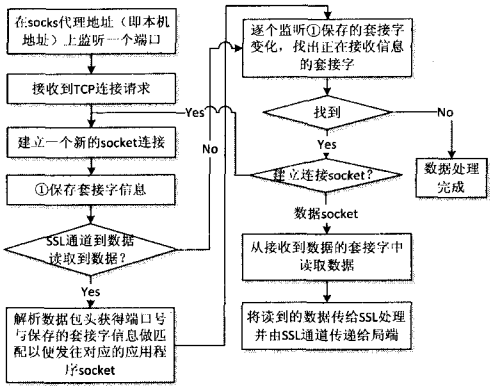

图 3　终端工作流程图

客户端拿到资源列表之后,就在本机地址上监听 Socks 代理端口,每当有应用发起 Socks 连接请求,这个 socket 将被记录下来,以便接收将来从 VPN 服务器传送过来的发给该应用程序的数据包。此时,被监听的端口包括 Socks 代理 bind 端口、SSL 连接端口、数个 Socks socket 连接端口。SSL 连接端口如果收到数据,则将数据解密后,读取数据包头中端口号,从而传给相应的应用;如果 Socks 连接收到数据,则将数据做好新的自定义封装,然后转交给 SSL 通道加密后传输;如果是 Socks 代理 bind 监听端口收到连接请求,则建立新的 socket 连接并保存这个连接。

2)局端工作流程

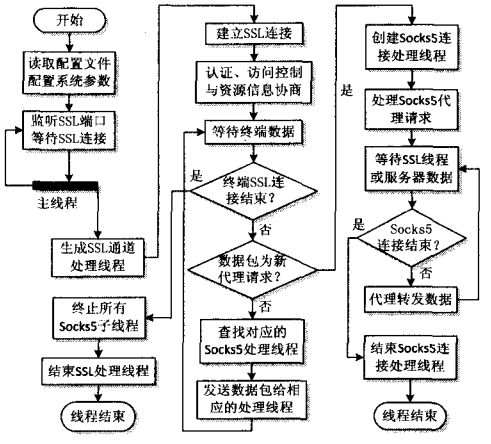

图 4　局端工作流程图

局端具体工作流如图 4 所示,局端首先启动程序读取配置参数然后监听 SSL 端口,从客户端发来 SSL 请求后与之建立连接并进行用户名身份鉴权以发给相信的可访问后台资源列表。SSL VPN 通道建立好之后,数据传输通信均使用该通道进行安全传输。局端等待终端数据包。如果该数据包所使用的端口号并未被记录,则判定为新包,局端为此次客户端请求建立新的 Socks5 连接处理线程,此时的数据也可以为后台应用服务传送的数据包,连接处理线程解析数据格式进行对应代理转发。如果数据包头所含端口号已有记录,则查找之前与之对应的 Socks5 处理线程,并将数据转发给该线程,该线程进行相应的代理转发处理,然后再次等待终端数据。

3　系统测试与分析

为了测试系统的正确性和可行性,本文搭建了真实的应用环境。移动终端通过 GPRS 连接 Internet,然后与内网的 VPN 局端系统建立 SSL 连接,最后接入内网并根据用户权限进行受限的访问控制。系统的测试环境如图 5 所示。

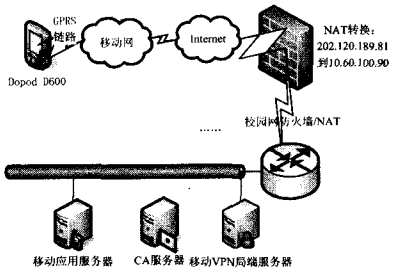

图 5　测试环境示意图

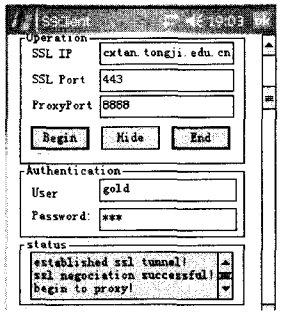

图 6　终端连接界面

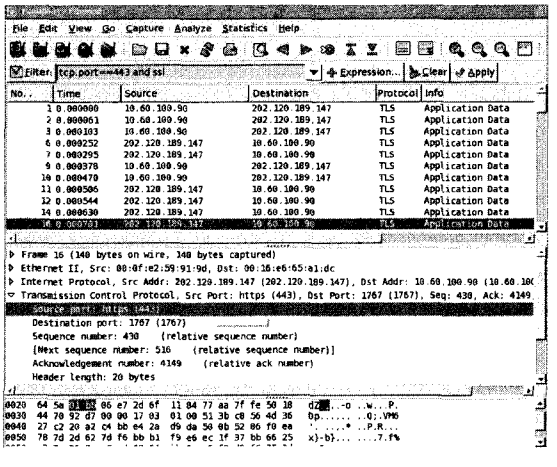

图 7　经过加密的数据抓包

实验室 GPRS 上网的最高速率大约为 115.2kbit/s,CDMA 1x 系统的峰值速率大约为 153.6kbit/s。GPRS 的平均速率达到 20kbit/s～40kbit/s,CDMA 1x 的平均速率为 80kbit/s～100kbit/s[4]。在此 GPRS 环境下,我们对移动终端的接入效率及安全性能、传输过程中数据的机密性和完整性以及传输效率等性能进行了完整的测试。终端安全接入界面如图 6 所示,经加密的数据抓包结果如图 7 所示。并通过对经 SSL 封装的 FTP 数据传输来测试系统的数据传输效率。SSL 握手阶段使用 RSA 来签名验证,SSL 传输阶段使用

(下转第 144 页)

the 14th Annual Network and Distributed System Security. Symposium(NDSS07). 2007
[4] Vulnerability Type Distributions in CEV[EB/OL]. http://cve.mitre.org/docs/vuln-trends/vuln-trends.pdf,2007
[5] Wojtczuk R. UQBTng:a tool capable of automatically finding integer overflows in Win32 binaries. November 2005
[6] Cifuentes C, et al. UQBT[EB/OL]. http://www.itee.uq.edu.au/.cristina/uqbt.html
[7] Necula G C, McPeak S, Weimer W. CCured: type safe retrofitting of legacy code[C]//Proceedings of the Symposium on Principles of Programming Languages. 2002
[8] Jim T, Morrisett G, Grossman D, et al. Cyclone: A safe dialect of c[C]//USENIX Annual Technical Conference. 2002
[9] Seward J, Nethercote N. Using valgrind to detect undefined value errors with bit-precision[C]//Proceedings of the USENIX05 Annual Technical Conference. Anaheim, California, USA, April 2005
[10] Howard M. Integer overflow and operator::new[EB/OL]. http://blogs.msdn.com/michael_howard/archive/2005/12/06/500629.aspx, Dec. 2006
[11] Evans D, Guttag J, Horning J, et al. LCLint: A tool for using specification to check code[C]//Proceedings of the ACM SIGSOFT 94 Symposium on the Foundations of Software Engineering. 1994:87-96
[12] Larus J, et al. Righting software[C]//IEEE SOFTWARE. IEEE Computer Society, 2004
[13] Sarkar D, et al. Flow-insensitive Static Analysis for Detecting Integer Anomalies in Programs[C]//Proceedings of the 25th Conference on IASTED International Multi-Conference: Software Engineering. 2007
[14] PaX Project. The PaX project[EB/OL]. http://pax.grsecurity.net/,2004
[15] Akritidis P, et al. Preventing memory error exploits with WIT [C]//IEEE Symposium on Security and Privacy. May 2008
[16] Budiu A M, Erlingsson M, Ligatti J. Control-flow integrity[C]//Proceedings of the 12th. ACM Conference on Computer and Communications Security(CCS05). 2005
[17] http://www.cve.mitre.org/cgi-bin/cvekey.cgi? keyword=integer
[18] Intel Corporation. IA-32 Intel Architecture Software Developers Manual-Volume1: Basic Architecture[S]. November 2006
[19] Drewry W, Ormandy T. Flayer: Exposing Application Internals [C]//Proceedings of the First USENIX Workshop on Offensive Technologies(WOOT '07). Boston, Massachussetts, USA, August 2007
[20] Lin Z, Zhang X, Xu D. Convicting exploitable software vulnerabilities: An efficient input provenance based approach[C]//Proceedings of the 38th Annual IEEE/IFIP International Conference on Dependable Systems and Networks(DSN'08). Anchorage, Alaska, USA, June 2008
[21] Gilmore S. Programming in Standard ML[Z]. 1997
[22] Ada95 Language Reference Manual[M]. ISO/IEC, 1995

(上接第 121 页)

AES 的 128 位密钥的 CBC 模式加密来保护传输的数据，使用 MD5 算法做 ESP 阶段的消息认证码计算，移动终端客户程序采用 handyGet。测试得到的数据如表 1 所列。从测试的数据中可以看到，加入 SSL 处理后，传输时间增加大约 20%，其并没有由于传输文件的增大而增加。

表 1 系统接入速度的传输效率

文件大小(MB)/应用协议	隧道建立时间(s)	ftp 协商时间(s)		数据传输时间(s)		传输速率(kB/s)	
		不使用 VPN	使用 SSL 隧道保护	不使用 VPN	使用 SSL 隧道保护	不使用 VPN	使用 SSL 隧道保护
1/ftp	5	12	17	192	215	5.2	4.7
2.66/ftp	5	14	15	524	731	5.0	3.6
7.5/ftp	5	15	13	1595	1916	4.7	3.9

结束语 本文提出的移动 SSL VPN 方案采用在应用层级别上利用 Socks5 协议进行数据转发搭建安全接入 VPN 的方式，将客户端应用程序到局端应用服务的 TCP 连接利用 Socks5 代理中继分为 3 段，Socks5 代理功能由异地的终端和局端共同实现。系统改善了 SSL VPN 在无线网络中的连接性能，减小了无线网络速率极不稳定、易断线的缺点带来的连接性能影响，很好地支持了移动漫游时的安全稳定接入。在跨越上海、江苏、浙江的外场移动漫游的联动实测验证了系统的安全性能和使用效率。目前该系统已初步在物流运输部门投入实际运用，并表现了较高的现实意义和应用价值。

参 考 文 献

[1] Kent S. Security Architecture for the Internet Protocol [S]. IETF RFC 2401. Nov. 1998
[2] Vaarala S, Klovning E. Mobile IPv4 Traversal across IPSec-Based VPN Gateways[S]. IETF RFC 5265. 2008
[3] Devarapalli V, Eronen P. Secure Connectivity and Mobility Using Mobile IPv4 and IKEv2 Mobility and Multihoming(MOBIKE)[S]. IETF RFC 5266. 2008
[4] Benenati D. A seamless mobile VPN data solution for CDMA 2000, UMTS and WLAN users[J]. Bell Labs Technical Journal, 2002,7(2):143-165
[5] 薛海波. 移动 VPN 的研究和实现[D]. 北京:北京交通大学, 2006
[6] Nokia Inc. White Paper: The Evolution of Mobile VPN and its Implications for Security [EB/OL]. http://www.nokia.com, 2009
[7] BirdStep Corp. Introducing Birdstep Intelligent Mobile IP, v2.0 Universal Edition [EB/OL]. http://www.birdstep.com, 2009
[8] Cisco Systems. Enterprise Mobile Wireless Data Solutions 1.0 [EB/OL]. White paper. http:/www.cisco.com/, Aug. 2003
[9] Dierks T, Allen C. The TLS Protocol Version 1.0[S]. IETF RFC 2246. January 1999
[10] Wireless Transport Layer Security Specification[EB/OL]. WAP Forum, February 2000
[11] Kim K, Hong J, Lim J. A Secure and Efficient Communication Resume Protocol for Secure Wireless Networks[Z]. International Federation for Information Processing, 2005
[12] Columbitech Wireless VPN technical Description [EB/OL]. Columbitech AB. ttp://www.columbitech.com/Products/WVPN.asp, 2004
[13] Goutham Rao. NET6 Hybrid-VPN Gateway [EB/OL]. http://www.citrix.it/REPOSITORY/docRepository/id_900_111297 9921897309.pdf, 2008
[14] Marcus L. SOCKS Protocol Version 5[S]. IETF RFC 1928. 1996