第 34 卷 第 14 期 计 算 机 工 程 2008 年 7 月
Vol.34 No.14 Computer Engineering July 2008
·安全技术· 文章编号：1000—3428(2008)14—0143—03 文献标识码：A 中图分类号：TP309

TIPSec 安全传输协议的设计和实现

杨卫兵[1,2]，孙凝晖[2]
(1. 中国科学院研究生院信息科学与工程学院，北京 100049；2. 中国科学院计算技术研究所国家智能计算机研究开发中心，北京 100080)

摘 要：介绍 TIPSec 安全传输协议的设计和实现，它能同时满足 3 个目标：应用无关性，良好的 NAT 网络穿越能力，较高的数据流处理效率。TIPSec 工作在操作系统内核中以保证应用无关性和处理效率，采用应用层封装，保持加密数据流的原始传输层特征以便于 NAT 设备处理。实际测试结果表明，在采用相同加密算法的前提下，TIPSec 的带宽性能比 IPSec NAT-T 高出 15%左右。
关键词：TIPSec 协议；通信安全；传输协议

Design and Implementation of TIPSec Secure Transport Protocol

YANG Wei-bing[1,2], SUN Ning-hui[2]
(1. School of Information Science and Engineering, Graduate University of Chinese Academy of Sciences, Beijing 100049;
2. National Research Center for Intelligent Computing Systems, Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080)

【Abstract】This paper discusses a secure transport protocol called TIPSec, which is specially designed to be: application transparent, well adapted to NAT networks, highly efficient. TIPSec works in the OS kernel to guarantee the transparency and efficiency, and performs application-payload-only encapsulation, so as to keep the original transport layer information exposed in the encrypted datastream to ease NAT processing. Performance test shows that, equipped with the same ciphers, TIPSec provides about 15% higher bandwidth than IPSec NAT-T.
【Key words】TIPSec protocol; communication security; transport protocol

1 概述

网络通信安全是计算机安全领域中的一个基本问题，目前主要存在 2 种解决方案：应用层安全和IP层安全。对于前者，应用程序通常需要与一个安全库链接在一起，该安全库提供信道保护参数的协商及数据的安全收发等功能，可取代操作系统提供的标准套接字(socket)函数，目前应用较多的安全库包括OpenSSL[1], Kerberos API[2]等。IP层安全通常实现在操作系统内核中，对应用程序透明，依据系统管理员指定的安全策略对进出本节点的数据流进行保护，IPSec[3]就是典型的实例。

以上 2 种技术各有优缺点。安全库的优点是加密后的数据流仍然表现为普通的TCP/UDP流，能够方便地被通信路径上的NAT设备处理，但缺点是原有的应用必须经过改写；IP层安全的优点是能够对多种应用程序进行透明保护，但缺点是加密数据流不再表现为TCP/UDP流，难以被NAT设备处理。为了使IPSec数据流正确穿过NAT设备，研究者们做了很多工作[4]，基本上都是通过嵌套封装的手段使加密数据流重新成为一条UDP流，但这无疑也增加了数据的传输开销和处理开销。

有时需要对某些应用进行透明保护，又要避免采用存在NAT穿越问题的IPSec，因此，人们开发了隧道技术，典型代表是SSH[5]，其工作原理如图 1 所示。隧道技术事实上是一种应用层转发技术，它既能够对多种应用通信进行透明保护，又能够避免IPSec存在的问题，但缺点是效率较低，因为受保护应用所传输的数据在客户机和隧道服务器上需要多次进出操作系统内核。

本文介绍了 TIPSec 的安全传输协议，它保持了隧道技术的应用透明性和 NAT 穿越能力，而且具有更高的效率。

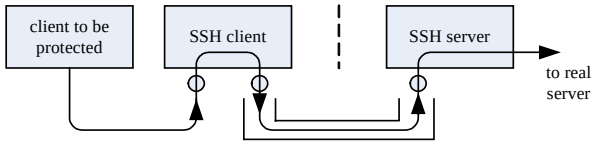

图 1 SSH 隧道工作原理

2 能力服务器

能力服务器[6]是一种基于分布式虚拟机技术的虚拟计算环境，通过大规模资源共享提高资源的利用率和效率密度，达到低成本高效能的目的。能力服务器由一组高性能服务器互联而成，在每台服务器上运行着虚拟机监控系统(Virtual Machine Monitor, VMM)，它能够利用本机物理资源构造出多个相互隔离的虚拟硬件平台(即虚拟机)，每台虚拟机都可以运行各种传统操作系统(Guest OS)，对于Guest OS而言，一台虚拟机和一台真实的计算机并无差别。各个VMM能够通过协作将一台虚拟机的虚拟CPU、虚拟内存和虚拟硬盘等虚拟部件分别映射到不同物理服务器的相应部件上并保持对Guest OS透明。通过动态调整虚实部件间的映射关系，能够有效提高全系统各物理资源的利用率。能力服务器体系结构如图 2 所示。

每个用户使用一台或多台虚拟机，并能够在其中执行任何在真实 PC 上能够执行的操作，包括访问物理服务器所在的物理网络。由于能力服务器旨在研究能够惠及大众的低成本信息化技术，因此它的用户不必来自同一机构，相互之间可以毫无信任关系，甚至可以是黑客。

作者简介：杨卫兵(1977－)，男，博士研究生，主研方向：高性能计算，嵌入式系统，网络安全；孙凝晖，研究员、博士生导师
收稿日期：2007-08-17 **E-mail：**ywb@ncic.ac.cn

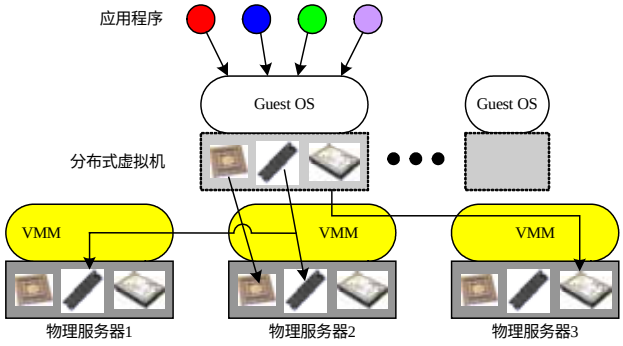

图 2　能力服务器体系结构

这种应用场景下，恶意用户能够通过自身虚拟机对各 VMM 间的协作通信以及其他用户与自身虚拟机间的远程桌面通信进行监听和攻击，因此，系统必须对这些通信进行加密和认证保护。这种保护必须实现以下目标：

(1)能力服务器中的各种系统服务在开发时均未加入安全考虑，如果利用安全库对它们进行改写将带来巨大的工作量，因此，能力服务器的安全架构必须能够对已有应用进行透明保护。

(2)由于活动虚拟机的数量通常很大，系统难以提供足够的外部 IP，因此在能力服务器中，每台虚拟机都通过 DHCP 动态获取一个私有 IP，并通过能力服务器的 NAT 网关与外界通信。在这种情况下，NAT 网关需要转发大量经过加密的远程桌面通信，因此，加密数据流必须便于 NAT 处理。

(3)远程桌面通信对延迟比较敏感，延迟的大小直接影响到用户的人机交互体验，因此，通信保护还必须非常高效。

现有的通信保护技术均不能同时满足这 3 个要求，因此，出现了一种新的安全传输协议——TIPSec。

3　TIPSec 总体设计

3.1　体系结构

TIPSec 的基本功能是对 2 个节点间的 TCP/UDP 通信提供加密、认证和完整性保护。为了实现上述 3 个目标，本文提出了以下设计思想：

(1)采用应用层数据封装形式，即仅对一个 TCP/UDP 包的应用层负载进行加密，保持其原始的传输层协议头不变。这样，经过 TIPSec 处理后的数据流仍表现为普通的 TCP/UDP 流，非常便于 NAT 设备进行端口转发。

(2)工作在操作系统内核中，以数据包为粒度进行处理，以提供应用无关性和高效性。

(3)采用三方信道协商机制进行信道保护参数的生成和发布，解决通信双方分别位于 NAT 网络而无法直接进行信道协商的问题。

3.2　数据包封装格式

TIPSec 在数据包的应用负载和传输层协议头之间插入一个 TIPSec 协议头，如图 3 所示。其中，version 表示 8 位的协议版本号；hdrlen 表示 8 位的协议头长度(字节数)；padlen 表示应用数据尾部可能存在的填充数据的字节数(有些加密算法要求作用于定长的数据块)；SN 表示 40 位的序列号，用于防止重放攻击(同一连接在同一方向上的所有数据包均具有不同的序列号，对于重传包也是如此)；CID 指出了对该数据包进行封装处理的上下文对偶的标识；AD 表示所有传输层负载(含 TIPSec 协议头)的加密摘要，提供该数据包的源认证和完整性保护。

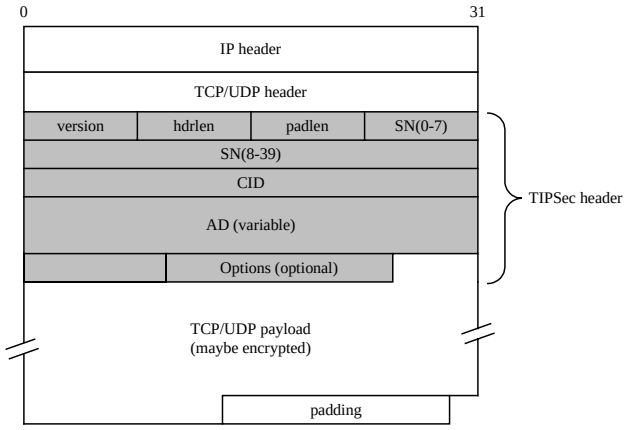

图 3　TIPSec 封装格式

3.3　核心数据结构

TIPSec 进行上述封装所基于的数据结构包括请求上下文、访问上下文和上下文映射表。

(1)请求/访问上下文

请求/访问上下文总是成对出现的，2 个配对的请求/访问上下文称为一对上下文对偶，它们对 2 个节点间某种特定类型的服务通信进行保护，其中请求上下文由这 2 个节点中的服务端持有，访问上下文由客户端持有。2 个构成对偶的上下文具有相同的 CID(Context ID)并包含相容的算法和密钥。

(2)上下文映射表

每个上下文对偶仅代表一种服务保护方案，并不特定于任何具体的服务连接。为了描述服务连接与保护方案间的对应关系，本文引入上下文映射表。表中每一项由一个连接相关的五元组标识(源 IP、源端口、目的 IP、目的端口和传输协议)，并指出了相应的保护方案(即上下文对偶)的 CID，以及其他一些连接相关的信息(例如该连接在发送和接收方向上的 TIPSec 序列号等)。

对于每个节点来说，它所持有的所有请求/访问上下文均通过三方信道协商动态获取，而上下文映射表则由该节点本地生成和维护。

3.4　出口数据流的处理

TIPSec 对出口数据流进行处理的第 1 步是截获操作系统即将发送到网络上的数据包。截获一个数据包后，需要根据其中的源 IP、源端口、目的 IP、目的端口和传输协议检索上下文映射表，并根据检索结果分别处理如下：

(1)上下文映射表检索成功

此时只需要根据检索到的上下文映射表项所指出的上下文对数据包进行如图 3 所示的封装即可。

(2)上下文映射表检索失败

这表明发送节点正在试图建立一条新的出口连接，此时需要确定对这一新建连接的保护方案，并生成相应的上下文映射表项。因此，需要根据该数据包的目的地址、目的端口和传输协议检索发送节点当前持有的访问上下文列表，并进行如下处理：

1)访问上下文检索成功。只需创建一个新的上下文映射表项，并利用检索到的上下文对当前数据包进行封装即可。

2)访问上下文检索失败。此时协议实现需要生成一个上下文匹配失败的事件通知，而该事件通知被某个特定的后台进程捕获后将触发一次新的信道协商。

生成上述事件通知后，对当前数据包进行何种处理可以

有多种选择，例如可以推迟该数据包的发送并期待上述事件通知所触发的信道协商能够成功完成，或立即将该数据包发送到网络上，还可以简单地将其丢弃。每种策略都有其优缺点，本文采用了第 1 种策略。

3.5 入口数据流的处理

TIPSec 对入口数据流进行处理的第 1 步同样是截获操作系统刚刚从网络上接收到的数据包。随后根据包头中的相关字段检索上下文映射表并根据检索结果进行如下处理：

(1)上下文映射表检索成功。此时需要根据检索到的上下文映射表项所指出的上下文对该数据包进行解密和认证。如果解密和认证失败，则必须丢弃该包并生成一项日志记录。

(2)上下文映射表检索失败。这表明该数据包是一个新的入口连接请求，此时需要根据包头中的相关字段检索请求上下文列表并根据检索结果进行如下处理：

1)存在匹配的请求上下文。此时首先需要尝试利用该请求上下文对该数据包进行解密和认证。如果解密和认证过程能够成功完成，则创建一个新的上下文映射表项，否则丢弃该数据包并生成一项日志记录。

2)不存在匹配的请求上下文。此时当前数据包必须被丢弃，但接收节点无须自动触发信道协商。换言之，如果 2 个节点间的某种服务通信需要采用 TIPSec 进行保护，则相应的信道保护参数的协商必须由客户端触发进行。

3.6 信道协商

所有的请求/访问上下文都是通过一种三方信道协商机制生成和发布的，而任何一次信道协商都是由服务请求者发起并由该请求者、服务节点和一个集中的授权中心参与进行的。一次信道协商中的消息传递如图 4 所示。

图 4 TIPSec 三方信道协商

在#1 消息中，请求者向授权中心提交一个信道协商请求(NegReq)，指出了目标节点和目标服务类型。授权中心对该请求进行评估，并在成功后生成一对上下文对偶分别发布给请求者和服务节点。随后请求者直接对服务节点发起连接，并利用刚刚获得的上下文对偶对这一连接进行保护。

在这一过程中须考虑几个关键问题：(1)授权中心对协商请求的评估算法；(2)请求上下文的发布问题(由于服务节点在协商过程中保持静默)；(3)上下文的安全传输问题；(4)信道协商的触发时机问题。本文对这些问题不作深入论述。TIPSec 仅是能力服务器安全架构的一个组成部分，对上述问题的回答与这一架构中的其他功能密切相关。

4 TIPSec 的性能评价

本文对 TIPSec, SSH 和 IPSec 进行性能对比分析。主要的性能指标为传输延时和传输带宽。测试平台如图 5 所示。

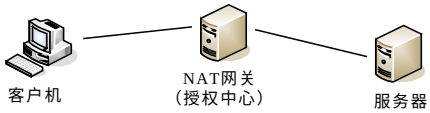

图 5 TIPSec 性能测试平台

各节点的配置如下：CPU 为 2×1.6 GHz，内存为 1 GB DDR SDRAM，OS 为 RedHat 9.0，Ethernet 为 2×100 Mb/s。

传输延时的测试方法为：在客户机上运行 telnet，访问服务器上的 echo 服务，并用 tcpdump 记录服务器的响应时间。分别采用 SSH 隧道方式(NAT 网关作为隧道服务器)、TIPSec 方式和 IPSec NAT-T 方式进行了测试，三者的响应时间如表 1 所示。

表 1 TIPSec 传输延时测试

通信保护方式	响应时间/ms
SSH 隧道	8.8
TIPSec	1.7
IPSec NAT-T	2.2

在 SSH 隧道方式中，通信数据需要在 3 个节点上多次进出操作系统内核，并且只有当 SSH 客户端和服务端进程被调度运行时才能处理隧道数据，因此，具有较大的延时；在 IPSec NAT-T 方式中，数据包需要经过多层嵌套封装，处理开销较大，因此，传输延时也大于仅采用一层封装的 TIPSec。

传输带宽的测试方法为：在客户机上运行 ftp 客户端下载服务器上的一个 200 MB 的文件，记录 ftp 客户端统计的带宽数据。同样在上述 3 种通信保护方式下进行了这一测试，测试结果如表 2 所示。

表 2 TIPSec 传输带宽测试

通信保护方式	传输带宽/(Mb·s^{-1})
SSH 隧道	5.3
TIPSec	8.7
IPSec NAT-T	7.6

在该项测试中，TIPSec 也表现出了最佳的性能。SSH 隧道的应用层转发方式显著降低了它的带宽性能，IPSec NAT-T 方式虽然工作在操作系统内核中，但它过多的封装层次降低了数据包中有效负载的比例，从而导致了有效带宽的下降。

5 结束语

本文讨论了一种新型的安全传输协议 TIPSec 的设计思想和实现方法，并对它进行了性能测试。测试结果表明，TIPSec 在传输延时和传输带宽方面均好于传统的应用层隧道技术和 IPSec 技术，能够很好地满足能力服务器中的通信保护需求。

参考文献

[1] OpenSSL. The OpenSSL Project[Z]. (2000-01-02). http://www.openssl.org.

[2] MIT Information Systems. Kerberos V5 API[Z]. (1996-09-01). http://cryptnet.net/mirrors/docs/krb5api.html.

[3] Atkinson R, Kent S. Security Architecture for the Internet Protocol[S]. RFC 2401, 1998-11.

[4] 王 力, 刘海静. 支持 NAT 穿越的 IKE 协商[J]. 微机发展, 2003, 13(12): 42-43.

[5] Ylonen T, Lonvick C. The Secure Shell (SSH) Protocol Architecture[S]. RFC 4251, 2006-01.

[6] 孙凝晖, 孙毓忠, 许 鲁. 能力服务器——低成本信息化[Z]. 北京: 中国科学院计算技术研究所, 2005-03.