第 34 卷 第 5 期 计 算 机 工 程 2008 年 3 月
Vol.34 No.5 Computer Engineering March 2008
·安全技术· 文章编号：1000—3428(2008)05—0161—02 文献标识码：A 中图分类号：TP309.2

IPv6 数据包生成器 IPSender6 的设计与实现

周江涛，翟健宏，张宏莉，宋晓慧
(哈尔滨工业大学计算机网络与信息安全技术研究中心，哈尔滨 150001)

摘 要：传统的基于 IPv4 的入侵检测系统(IDS)和网管系统(NMS)必须升级以支持 IPv6。在 IDS 和 NMS 的升级过程中，需要获得各种不同特征的 IPv6 数据包，尤其是在 IP 层互异的数据包来测试和验证其功能性。该文在实验的基础上，设计并实现了 IPv6 数据包生成器 IPSender6 作为提供 IPv6 测试数据的工具，用于网管系统和 IDS 系统的研究测试。实测证明了 IPSender6 在提供测试数据方面的灵活性和有效性。

关键词：IPv6 协议；扩展首部；入侵检测

Design and Implementation of IPv6 Packet Constructor IPSender6

ZHOU Jiang-tao, ZHAI Jian-hong, ZHANG Hong-li, SONG Xiao-hui
(National Key Lab of Computer Context Information Security, Harbin Institute of Technology, Harbin 150001)

【Abstract】Traditional IPv4-based Intrusion Detection System(IDS) and Network Management System(NMS) need to be upgraded to support IPv6, which needs various IPv6 data, especially the packets with distinct extension headers on IP layer to certify their functionalities. This paper designs and implements an IPv6 packet constructor——IPSender6 based on experiments. Experiments prove that IPSender6 provides test data for IDS and NMS flexibly and effectively.

【Key words】IPv6; extension header; intrusion detection

为了适应即将来临的 IPv6 网络，各种网管系统以及入侵检测系统面临的最紧迫的任务是升级调整。在系统升级调试过程中，进行全面细致的测试是确保其正确性和全面性的前提，因此，提供各种 IPv6 测试数据变得非常必要。得到测试数据的一种方法是从现有的网络中捕获流量进行测试，但是这种方法提供的数据具有很大的随机性，同时 IPv6 的应用目前还很不充分，难以提供好的数据来源。另一种方法是在模拟目标网络流量的背景下，加入目标测试需要的数据包。该方法目的性更强，可随时根据测试需要变换数据包类型。

1 IPSender6 的设计

1.1 测试数据的需求与分析

网管系统(NMS)和入侵检测系统(IDS)的测试一般需要 2 类测试数据：(1)针对各种应用层协议的测试数据；(2)针对网络层特征的测试。对于应用层协议的测试数据比较容易获得，因为在现有的 IPv6 网络中已有各种应用，用户可以从网络流量中捕获各种应用数据进行测试，也可以自己搭建服务器来提供测试数据。目前各种常见的网络服务器和客户端的软件多半提供支持 IPv6 的补丁。而用于测试网管系统和入侵检测系统对于数据包网络层特征的反应和处理的数据较难获得，因为网络流量中的数据包一般不具备测试所需特征，这使利用捕获网络流量的方法受到较多限制，效率也比较低下。因此，IPSender6 的设计目标是提供各种用于网管系统和入侵检测系统的测试数据，并且针对测试系统对各种网络层特征数据的反应和处理提供全面的测试数据来源。

1.2 MTM 模型设计及实现机理

由于 NMS 和 IDS 需要检测流经或捕获的 IPv6 数据包的首部，并且针对不同的首部结构进行不同的处理，因此必须能够构造出具有各种扩展首部的 IPv6 数据包，用于观察系统对于这些数据包处理流程的工作情况及正确性。IPv6 的首部结构如图 1 所示[1]。

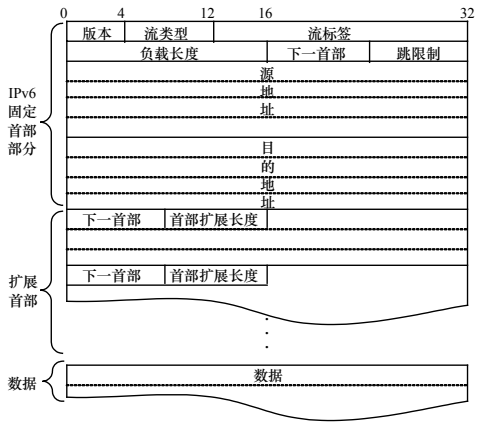

图 1 IPv6 首部结构

按照 IPv6 协议规范[2]，IPv6 扩展首部在 IP 包中出现的次序必须遵循以下顺序：IPv6 首部→逐跳选项首部→目的地址选项首部→路由扩展首部→分片扩展首部→验证扩展首部→封装有效载荷扩展首部→目的地址选项首部→上层协议首部。IPv6 数据包各扩展首部是否存在完全取决于用户的需求，用户可以通过输入特定参数来指定使用哪些扩展首部选项(或都不使用)，并且参数的指定具有一定的随机性和灵活性。为了能够满足灵活性和合法性的要求，本文提出了改进后的图灵机模型(Modified Turing Model, MTM)。MTM 具有的双

作者简介：周江涛(1981－)，男，硕士，主研方向：网络信息安全；翟健宏，副教授；张宏莉，教授、博士生导师；宋晓慧，硕士
收稿日期：2007-08-20 **E-mail：**zhoujiangtao@pact518.hit.edu.cn

缓冲带滑动读写结构是依据图灵机原理并模拟机械传送带模型而设计的，输入带上的读头用来读取输入带上的符号，并且只向右移动，而输出缓冲带中的写头可以向输出缓冲带中写入信息，并且可左右移动。MTM 模型的结构如图 2 所示。

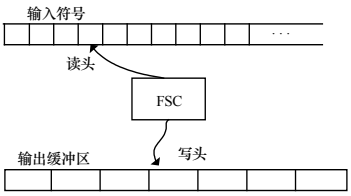

图 2　用于构造扩展首部的 MTM

图灵机 M=(Q, Σ, Γ, δ, q_0, B, F)[3]，其中，输入符号集合 Σ={HP, FDH, RH, FH, AH, ESP, BDH}，HP 为逐跳扩展首部，FDH 为由第 1 个目的节点处理的目的地址扩展首部，RH 为路由扩展首部，FH 为分片扩展首部，AH 为验证扩展首部，ESP 为封装有效载荷扩展首部，BDH 为由最终目的节点处理的目的地址扩展首部，这些输入符号由用户指定的参数得到；带符号集合 Γ=Σ U{B}；B 为空白字符。图 3 列出了状态转移函数 δ 的部分转移过程。

FDH	RH	FH	AH	ESP	BDH	B
(q_{02},C(FDH),R)	(q_{03},C(RH),R)	(q_{04},C(FH),R)	(q_{05},C(AH),R)	(q_{06},C(ESP),R)	(q_{07},C(BDH),R)	q_f
(q_{12},C(FDH),R)	(q_{13},C(RH),R)	(q_{14},C(FH),R)	(q_{15},C(AH),R)	(q_{16},C(ESP),R)	(q_{17},C(BDH),R)	q_f
	(q_{23},C(RH),R)	(q_{24},C(FH),R)	(q_{25},C(AH),R)	(q_{26},C(ESP),R)	(q_{27},C(BDH),R)	q_f
(q_{32},C(FDH),R)		(q_{34},C(FH),R)	(q_{35},C(AH),R)	(q_{36},C(ESP),R)	(q_{37},C(BDH),R)	q_f

图 3　MTM 部分状态转移函数

当读头从输入带上读到一个符号后，根据状态转移函数转移到下一个状态，并在输出缓冲区中插入相应的扩展首部，当处理完所有的输入符号，输出缓冲区中就得到了对应输入的所有扩展首部，其顺序满足 IPv6 协议规范的要求的。状态转移函数中的 C(HP)表示在输出缓冲区中查找到逐跳扩展首部应处的位置并插入逐跳扩展首部的动作，其他依此类推。

由于部分扩展首部需要用户来构造 IP 层首部数据，因此实现时有 2 种选择，用户既可以使用 RAW SOCKET 来构造，也可以使用 SOCK_STREAM/SOCK_DGRAM，通过设置 SOCKET 选项来构造。RAW SOCKET 的实现相对麻烦，但给用户更多的选择和自由，而且发送 ICMPv6 的数据包只能使用 RAW SOCKET，因此，本文基于上述 MTM 模型，选用了 RAW SOCKET 编程实现 IPSender6。实践证明本文的 MTM 是实用可靠的，并且很好地满足了灵活性和合法性的要求。

由于在 IP 包构造时使用了 RAW SOCKET，并且自己填充了 IP 层数据，因此在数据包发送前，需要进行计算校验和，值得注意的是，在计算校验和的时候应使用 TCP/UDP 伪首部来计算，关于伪首部的定义和格式见 IPv6 协议规范[1]。为了便于 IPv6 分片数据的发送，IPSender6 允许用户自行定义用于发送数据的命令行参数，以发送分片偏移重叠或分片偏移量有空洞的数据片[4]。

2　IPSender6 性能测试

本文在实验室环境下对 IPSender6 各项指标进行了全面的测试，着重测试了 IPv6 数据包的发送能力。在测试中，IPSender6 提供了各种类型的数据包，并由 Smartbit6000 流量发生器每秒生成 5 000 个的 IPv4_UDP 数据包作为背景流量，将此网络数据流提供给正在调试的一个支持 IPv6 的入侵检测系统。

测试机器的配置为：P4 2.0 GHz CPU，512 MB 内存，80 GB 硬盘，Realtek RTL8139 100MTX NIC，Linux RadHat9.0 操作系统，内核版本为 2.4.20，加载 IPv6 模块。测试环境网络拓扑结构如图 4 所示。IPv6 数据包在主机 A 产生，经过交换机的连接发送到主机 B 端，主机 B 为入侵检测系统宿主机。节点之间的连接为 100 Mb/s 全双工链路。

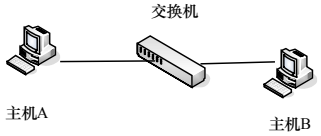

图 4　测试环境网络拓扑结构

在实验中分别构造了载荷长度为 64 B, 128 B, 512 B 和 1 KB 的 IPv6_TCP 和 IPv6_UDP 数据包进行测量，并测试了长度分别为 64 B, 128 B 和 512 B 的 ICMPv6 数据包的发送情况，在接收端对收到的数据包计数。实际测得 IPSender6 发送速度和发送长度间的关系如图 5 所示。

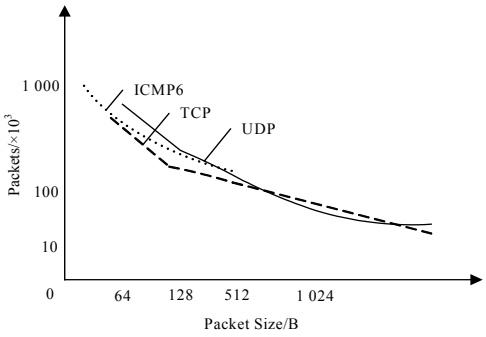

图 5　IPSender6 的发送速度

从图 5 可以看出，IPSender6 在上述网络状况下的发送能力可以满足校园网内部入侵检测系统的测试要求。

3　结束语

IPSender6 的开发为项目组进行基于 IPv6 的入侵检测系统和网管系统的研发提供了可靠稳定的测试数据，很好地配合了项目的进展。实验表明，本工具提供的测试数据是有效的，并且可以灵活构造各类测试用数据，发送速度可以满足入侵检测系统和网管系统的测试需求。

参考文献

[1] Pezaros D P, Hutchison D, Gardner R D, et al. Inline Measurements: A Native Measurement Technique for IPv6 Networks[C]//Proc. of International Conference on Networking and Communication. [S. l.]: IEEE Press, 2004.

[2] Deering S, Hinden R. Internet Protocol, Version 6 Specification[S]. RFC 2046, 1998.

[3] Hopcroft J E, Motwani R, Ullman J D. Introduction to Automata Theory, Languages, and Computation[M]. [S. l.]: Addison Wesley, 2000.

[4] 扈兆明, 苏志胜, 赵晓宇, 等. IPv6 分片重组在入侵检测系统中的实现[J]. 现代电信科技, 2005, 4(1): 45-49.