doi :10.3969/j.issn.1671-1122.2012.11.022

IPv6 环境下网络取证研究

梅锋，孙东滨

（国家计算机网络应急技术处理协调中心黑龙江分中心，黑龙江哈尔滨 150001）

摘 要：随着 IPv4 地址即将耗尽，IPv4 向 IPv6 过渡已成为必经之路。IPv6 的应用将对网络取证技术产生重大影响，文章以分析 IPv6 协议的基本报文格式、IPSec 协议为基础，对 IPv6 和 IPv4 进行了对比，提出了 IPv6 环境下以及在 IPv4 向 IPv6 过渡期的网络取证的特点和存在的难点。

关键词：IPv6；IPSec；网络取证；下一代互联网

中图分类号：TP393.08 文献标识码：A 文章编号：1671-1122（2012）11-0082-04

A Research on Network Forensics in IPv6 Environment

MEI Feng, SUN Dong-bin

(*Heilongjiang Branch of China Computer Network Emergency Response Technical Team/ Coordination Center, Harbin Heilongjiang* 150001, *China*)

Abstract: As IPv4 addresses are going to exhausted, IPv4 replaced by IPv6 is the only way. The application of IPv6 will impact network forensics significantly. IPv6 addressing, packet structure, and IPSec protocols are explained in this paper. According to the contrast of IPv6 and IPv4, the main and difficult points of network forensics in IPv6 environment and during the IPv4 to IPv6 transition period are proposed in this paper.

Key words: IPv6; IPSec; network forensics; next generation internet

“网络取证”这一概念最早由美国的计算机安全专家 Marcus Ranum 在 20 世纪 90 年代提出[1]，主要指通过对网络事件的捕获、记录和分析来发现攻击事件。2001 年，在数字取证研究工作组（Digital Forensic Research Workshop，DFRWS）的会议上，经过讨论给出了网络取证的定义：利用科学的技术方法，对来自各种活动事件及传输实体的多层次主动处理过程以及数据源传递过程中的数字证据进行收集、融合、发现、检查、关联、分析和存档，以此来发现和揭示有预谋的破坏行为或已经成功的非授权的渗透攻击行为，并为应急事件的响应和系统恢复提供有用的信息[2]。网络取证主要通过对网络数据流、审计迹、主机系统日志等的实时监控和分析，发现对网络系统的入侵行为，自动记录犯罪证据，并阻止对网络系统的进一步入侵[3]。2012 年初，国家发改委、工信部等七部门联合下发了《关于印发下一代互联网“十二五”发展建设的意见的通知》，要在“十二五”期间实现互联网普及率达到 45% 以上，推动实现三网融合，IPv6 宽带接入用户数超过 2500 万，实现 IPv4 和 IPv6 主流业务互通，IPv6 地址获取量充分满足用户需求的目标，并确立了 2013 年底前开展 IPv6 网络小规模商用试点，2014-2015 年开展 IPv6 网络大规模部署和商用，逐步停止向新用户和应用分配 IPv4 地址的路线图。随着下一代互联网应用的增加，网络速度的加快和网络规模的急剧扩大，相对于 IPv4，IPv6 在网络保密性、完整性方面有了更好的改进，在可控性、抗否认性方面也有了新的保证[4]，但由此对网络取证也带来了新的挑战。本文将在分析 IPv6 的报文格式，协议特点的基础上，对 IPv6 和 IPv4 进行比较，并阐述 IPv6 环境下的网络取证特点。

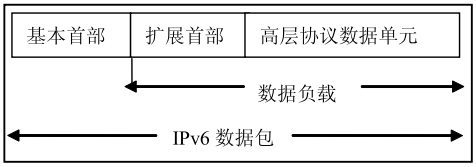

图1 IPv6数据包结构

1 IPv6 协议

1.1 IPv6协议报文格式

对于 IPv6 包结构、连接流程的理解对于网络安全事件重构、网络取证有着重要意义。IPv6 数据包结构由三部分组成：IPv6 基本首部、扩展首部和高层协议数据单元如图 1 所示。

根据 IETF 的 RFC2460[5]，IPv6 报文基本首部格式如图 2 所示，其长度固定为 40 字节。

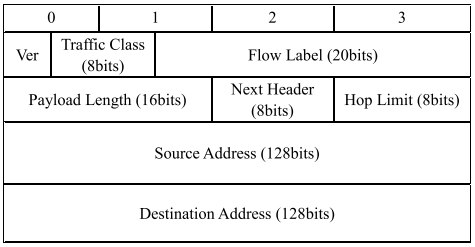

图2 IPv6基本首部格式

收稿时间：2012-09-13

作者简介：梅锋（1983-），男，黑龙江，工程师，博士，主要研究方向：网络安全；孙东滨（1977-），男，黑龙江，硕士，主要研究方向：网络安全。

首部各字段具体涵义如下：

版本（Ver）：4bits，Internet 协议版本号，IPv6 协议值为 6。

传输类别（Traffic Class）：8bits，用于指明 IPv6 数据包类别或优先级，并能够执行类似 IPv4 的 ToS 字段的功能。

流标签（Flow Label）：20bits，用于指明数据包属于源地址与目的地址之间的一个特定数据包序列，并且它需要中间 IPv6 路由器进行特殊处理。数据流标签可以用于非默认的 QoS 连接，比如实时数据（音频和视频）使用的连接。默认值为 0。

负载长度（Payload Length）：16bits，无符号整数。用于指明 IPv6 有效载荷长度（即不包含首部）。也就是以八位组为单位，在这个包中 IPv6 首部后面的其余部分的长度。如果负载长度大于 65535 字节，本字段置 0，并须设定超长负载选项（Jumbo Payload）。

下一首部（Next Header）：8bits，用于指明紧接在 IPv6 首部后面的第一个扩展首部（如果存在）的类型。使用与 IPv4 协议字段及后续协议相同的数值。

跳数限制（Hop Limit）：8bits，无符号整数，用于指明 IPv6 数据包传输时在被丢弃前经过的最大链路数量，类似 IPv4 的生存时间（TTL）字段。在每个传输此包的节点处递减 1。如果跳数限制减为零，丢弃此包，并给源地址发送一个 ICMPv6 Time Expired 消息。

源地址（Source address）：128bits，用于指明发送者的主机地址。

目的地址（Destination Address）：128bits，用于指明 IPv6 数据包的预期接收者的地址（如果存在路由首部的话，可能不是最终的接收者）。

1.2 IPv6扩展首部

在 IPv6 里，可选的网络层信息在一个独立的首部编码，位于数据包中 IPv6 首部与上层协议首部之间。扩展首部的个数不多，一个 IPv6 首部可以携带零个、一个或者多个扩展首部，每个扩展首部由前一个首部中的“ 下一个首部 ” 字段标识。

1.3 IPSec分析

1.3.1 IPSec的体系结构及工作原理

IPv6 强制引入了 IPSec 协议，IPSec 是利用密码技术的来保护现有服务和安全协议的套件，能提供的安全服务集包括访问控制、数据源认证、无连接的完整性、抗重播保护、保密性和有限传输流保密性。

IPSec 位于传输层的下面，它的安全服务程序可以被应用程序透明地继承。它提供了一种标准的、健壮的以及包容广泛的安全机制，它可为 IP 及上层协议提供安全保证。IPSec 安全功能在 IPv4 协议中可选的，在 IPv6 协议中是必须支持的 [6]。IPSec 的设计目标就是提供一个同时适用于 IPv4 和 IPv6 的、可以互操作的、高质量的和基于加密的互联网安全机制。IPSec 的体系结构如图 3 所示。

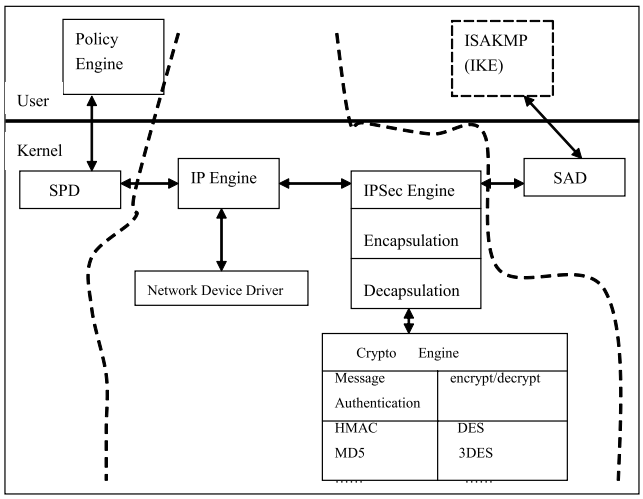

图3 IPsec的体系结构框图

IPSec 体系结构分为用户态和核心态（系统态）两部分，前者主要由用户事先定义需要使用 IPSec 进行通信时的安全策略、加密算法等相关信息；后者由系统提供整个 IPSec 通信的详细过程，也就是 IPSec 的具体实现。

整个 IPSec 的安全体系是以 IETF 定义的 RFC2401（Security Architecture for the Internet Protocol）为基础的。文档 RFC2401 定义了 IP 层上的一些最关键、最通用的安全概念，包括安全策略数据库（SPD）和安全联盟数据库（SAD），以及安全需求，还规定了 IP 安全技术的机制。它是整个 IPSec 安全体系结构的核心和关键，IPSec 的实施均遵守该文档的规范。

IPSec 通过两大传输协议、认证头（AH）、封装安全负载（ESP）以及通过密钥管理过程和协议的使用来完成其功能。使用于任何环境中的 IPsec 协议集及其使用的方式由用户、应用程序、和 / 或站点、组织对安全和系统的需求来决定。

IPSec 使用的身份验证首标（AH）和封装的安全数据负载（ESP）中，前者为数据通信提供了数据源的身份验证和数据完整性检查功能，后者提供了数据保密功能。

1.3.2 密钥管理

密钥管理分为密钥确定和密钥分发两大方面，最多需要四个密钥：AH 和 ESP 在发送和接收时各需两个密钥。密钥管理包括手工和自动两种模式。

手工管理（Manual）：在采用手工管理模式时，管理员使用自己的密钥或其它系统的密钥手工设置每个系统。这种方法比较适合在小型网络环境中使用。

自动管理（Automated）：自动管理是指通信双方通过某种密钥管理协议，在实际的数据通信之前通过协商确定相互之间所需密钥的一种密钥管理方式。采用自动密钥管理模式时，可以随时建立新的 SA 密钥，并可以对较大的分布式系统上使用的密钥进行定期更换。

自动管理模式有很大的灵活性，但设置过程需要花费使

用者较多的时间和精力，而且需要利用较多的软件，IPSec 默认采用的自动管理密钥协议是 IKE。

1.3.3 IPSec的数据处理流程

在介绍了 IPSec 基本概念及其密钥管理后，接下来描述一下 IPSec 的数据处理流程，如图 4 所示。

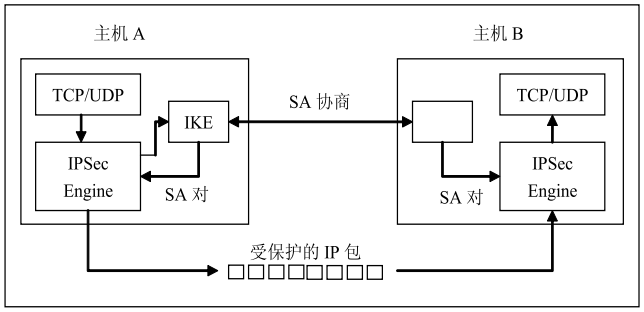

图4 IPSec的数据处理流程

为简单起见，在图 4 中我们只考虑从主机 A 向主机 B 发送消息的情况，主机 B 向主机 A 发送消息的情况与之相似。并且假定每台主机都激活了 IPSec 引擎，其具体处理流程如下：

主机 A 取 IP 包的五元组信息（源 IP 地址、目的 IP 地址、协议号、源端口号、目的端口号），IPSec 引擎检查其 IP 策略，查验数据包是否需要保护以及需要受到何种程度的保护，即丢弃、旁路或使用 IPSec。

若需要使用 IPSec，则 IPSec 引擎通知 IKE 进行安全协商。

主机 B 上的 IKE 收到安全协商请求通知。

两台主机建立第一阶段 SA，各自产生共享“主密钥”。若两台主机在之前的通信中已经建立起第一阶段 SA，则可跳过这一步直接进入第二阶段 SA 协商。

协商建立第二阶段 SA 对：入站 SA 和出站 SA。SA 包括密钥和安全参数索引（Security Parameter Index，SPI）。

主机 A 的 IPSec 引擎利用出站 SA 对数据包进行签名（完整性检查）与 / 或加密。

IPSec 引擎将数据包传递至 IP 层，由 IP 层将数据包发送至主机 B。

主机 B 的网络适配器驱动程序将接收到的数据包转交给 IPSec 引擎。

主机 B 的 IPSec 引擎利用入站 SA 查验完整性签名与 / 或对数据包进行解密。

主机 B 的 IPSec 引擎将解密之后的数据包提交给上层 TCP/IP 驱动程序，再由 TCP/IP 驱动程序将数据包提交主机 B 的接收应用程序。

以上便是 IPSec 的一个完整工作流程，所有操作对最终用户是完全透明的。

2 IPv6 地址特点及其与 IPv4 对比

作为新的协议标准，IPv6 的网络地址与 IPv4 的网络地址相比有以下几个特点。

1）大容量地址空间，IPv6 采用 128 位地址，共有 2128 个不同的 IPv6 地址，也就是全球可分配地址数为 340,282,366,920,938,463,463,374,607,431,768,211,456 个。

2）取消广播地址，IPv6 没有广播，改用多种组播，支持 AnyCast。

3）自动配置，IPv6 采用地址自动配置技术，即“即插即用”，不需要任何人工配置，就可以将一个 IP 节点接入 IPv6 网络并启用。IPv6 采用启动协议（BOOTstrap Protocol，BOOTP）和动态主机配置协议（DHCP）来支持即插即用的网络连接。这两种协议采用了“状态自动配置”（Stateful Autoconfiguration），即 BOOTP 服务器或 DHCP 服务器必须保存并管理每个节点的状态信息，IP 节点可以通过这些服务器获得配置信息。

在报文格式上，IPv4 与 IPv6 的主要区别有以下几点：

报头：前者虽然是固定格式但是含多个 Options，有报头校验和；后者固定长度，简化头部，采用扩展报头处理选项，无校验和，使用流标签，改用跳数限制等。

地址：前者采用 32 位地址，有广播地址；后者采用 128 位地址，取消广播地址，增加即插即用功能。

分片：前者是全路径中可分片，头部字段有 Flag 和 FragOffset 支持；后者只在发送端分片，引入分片扩展头。

安全性：前者本身无协议安全措施，附加 IPSec；后者通过 AH 和 ESP 两种扩展头实现内置 IPSec，增加了协议级安全。

3 IPv6 环境下网络取证的特点分析

对于网络取证而言，对 IPv6 的地址特点、包结构的掌握是十分必要的。IPv4 与 IPv6 地址之间最显著的区别在于地址长度：IPv4 地址长度为 32 位，而 IPv6 地址长度为 128 位。IPv4 地址一般以 4 部分以小数点分开的 0~255 间数字的形式来表示，例如：127.0.0.1，255.255.255.0。IPv6 地址的表达方式是 8 组以冒号分隔开的 4 位 16 进制数，每组 16 位，共计 128 位，例如：2031:0000:1F1F:0000:0000:0100:11A0:ADDF。为了简化 IPv6 地址的表述，RFC2373 提出地址中起始的 0 可以省略，连续的 0 可省略为“::”，但双冒号只能出现一次 [7]。IPv6 寻址模型与 IPv4 很相似，每个单播地址标识一个单独的网络接口。IPv6 的地址被指定给网络接口而不是节点，因此一个拥有多个网络接口的节点可以同时拥有多个 IPv6 地址，其中任何一个 IPv6 地址都可以代表该节点。

另外，利用网络抓包工具对网络流量分析也是网络取证的重要手段，因为数据包是真实客观的，可以还原攻击场景。现在，大多数协议分析工具包括 tcpdump、wireshark 等都支持解析 IPv6 数据包，因此可以利用工具在 IPv4 和 IPv6 混杂的网络流量中将 IPv6 的流量抓取出来。以 tcpdump 为例，在默认端口采集所有 IPv6 的流量命令为：

tcpdump ip6

采集使用某一物理地址(MAC)的所有进出IPv6网络流量：

tcpdump ip6 and ether host 00:24:1D:6E:D7:3C

采集使用某一本地单播IPv6地址的所有进出IPv6网络流量：

tcpdump ip6 and host fe80::a809:2dcf:e95f:ba7f

采集使用某一全球单播IPv6地址的所有进出网络流量：

tcpdump ip6 and host 2001:da8:b800:101:230:bf31:f17e:e23a

采集所有IPv6消息控制协议（ICMPv6）流量：

tcpdump icmp6

采集所有IPv6多播（ICMPv6）流量：

tcpdump ip6 multicast

在IPv4向IPv6的过渡期，会存在大量IPv6节点通过IPv4网络隧道访问IPv6网络资源。以IPv6-over-IPv4 GRE(通用路由协议封装）隧道为例，使用tcpdump采集的进入隧道的流量如下所示，可以看出IPv4 GRE头部在IPv6包之前。

```
[root@localhost admin]# tcpdump  -i eth2 host 10.0.2.3 -v
tcpdump: listening on eth2, link-type EN10MB (Ethernet), capture size 96 bytes
15:23:34.875346 IP (tos 0x0, ttl 255, id 302 offset 0, flags [none], proto: GRE(47), length: 124) 10.0.2.3 > 10.0.2.1: GREv0, Flags [none], length: 104) IP6 (hlim 64, next header: ICMPv6 (58), length: 60) 2001:da8:b800:101:230:bf31:f17e:e23a > 2001:da8:b800:101:230:bf31:f17e:e230: ICMP6, echo request, length 60, seq 0
15:23:34.875658 IP (tos 0x0, ttl 255, id 317 offset 0, flags [none], proto: GRE(47), length: 124) 10.0.2.1 > 10.0.2.3: GREv0, Flags [none], length: 104) IP6 (hlim 64, next header: ICMPv6 (58), length: 60) 2001:da8:b800:101:230:bf31:f17e:e230 > 2001:da8:b800:101:230:bf31:f17e:e23a: ICMP6, echo reply, length 60, seq 0
15:23:34.876373 IP (tos 0x0, ttl 255, id 303 offset 0, flags [none], proto: GRE(47), length: 124) 10.0.2.3 > 10.0.2.1: GREv0, Flags [none], length: 104) IP6 (hlim 64, next header: ICMPv6 (58), length: 60) 2001:da8:b800:101:230:bf31:f17e:e23a > 2001:da8:b800:101:230:bf31:f17e:e230: ICMP6, echo request, length 60, seq 1
15:23:34.876668 IP (tos 0x0, ttl 255, id 318 offset 0, flags [none], proto: GRE(47), length: 124) 10.0.2.1 > 10.0.2.3: GREv0, Flags [none], length: 104) IP6 (hlim 64, next header: ICMPv6 (58), length: 60) 2001:da8:b800:101:230:bf31:f17e:e230 > 2001:da8:b800:101:230:bf31:f17e:e23a: ICMP6, echo reply, length 60, seq 1
```

IPv4到IPv6的过渡是一个循序渐进的过程，在过渡期内，IPv4和IPv6将长期共存，通过以上对IPv6协议及IPv6流量采集实例分析，在IPv6环境下的网络取证有以下特点。

由于IPv6采用的是128位地址，在进行协议分析时，必须采用新的数据结构，以适应IPv6数据包格式。

IPv6环境下网络层的分片数据重组完全不同于现行的IPv4，它采用的是分片扩展头，对分片的重组必须建立在对扩展报文头的完整汇集并详细分析的基础之上。而分片数据的存储，分片数据包的正确顺序确定，都需要进行认真分析处理。

IPv6的强制标准IPSec协议对网络取证的影响重大。这使得在启用了IPSec的网络环境里直接通过网络侦听来获取犯罪证据几乎成为不可能的事情，要想提取出有用的证据数据，就必须借助相应的密码分析技术，将被通过ESP加密的数据进行解密，这样才能得到用以进一步分析的有效数据。

在IPv6环境下，一个主机可以拥有多个IPv6地址，而一个IPv6的网络节点在一个接口上也可以同时拥有多个地址。这对于安全事件的追踪来说，要在某个时间点确定到底是哪一个IP发起的攻击就变得十分困难。例如一个黑客利用某个IPv6地址成功攻入一台主机，然后再以这台主机的另外一个IPv6地址作为跳板继续深入攻击该主机所在网络，要发现这种关联性就变得十分困难。在这种情况下，整个系统要有时钟同步，这样在日志分析中才有可能将攻击场景进行还原。

在过渡期，大量系统将同时支持IPv4和IPv6，双栈和隧道机制将被广泛采用。攻击者可以利用双栈机制中两种协议间存在的安全漏洞或过渡协议的问题来逃避安全监测乃至实施攻击行为。双栈机制可能让网络服务在无意间暴露到网络上[8]，例如IPv6的有效连接可能会允许攻击者通过IPv4的防火墙或网关设备，这样网络服务或主机就直接暴露在网络上。而对于隧道机制而言，它只是对来源的数据包只进行简单的封装和解封，并不对IPv4和IPv6地址的关系做严格的检查，也存在防火墙被“穿透”的问题，在这种情况下，如果主机或安全设备缺少对某一类协议的日志记录，在确定攻击是从那个网络发起的将变得比较困难。更进一步，隧道技术还会让追踪溯源变得复杂，使得溯源只能找到隧道代理或网关，而无法追踪到真正的攻击者。

4 结束语

网络取证技术还在不断发展之中，而新的网络技术的出现和发展都将对其产生影响，本文从IPv6协议的基本报文格式、IPSec协议分析入手，对IPv6和IPv4进行了对比，并在此基础上对IPv6环境下以及IPv4向IPv6过渡期的网络取证的特点进行了分析，为打击网络犯罪，在网络取证上提供技术支持提供了一些参考。（责编 程斌）

参考文献：

[1] Marcus Ranum. Intrusion Detection: Challenges and Myths, Network flight recorder [EB/OL]. http://www.sans.org/reading_room/whitepapers/detection/intrusion-detection-systems-definition-challenges_343, 1998.

[2] 李炳龙，王鲁，陈性元. 数字取证技术及其发展趋势 [J]. 信息网络安全，2011，(01)：52-55.

[3] 张有东，王建东，叶飞跃等. 网络取证及其应用技术研究 [J]. 小型微型计算机系统，2006，27（03）：558-562.

[4] 王艳华，左明. 基于IPv6的互联网安全问题探讨 [J]. 网络安全技术与应用，2011，(02)：22-25.

[5] RFC 2460, Internet Protocol, Version 6 (IPv6) Specification[EB/OL]. http://tools.ietf.org/pdf/rfc2460.pdf, 1998.

[6] RFC 2401, Security Architecture for the Internet Protocol[EB/OL]. http://tools.ietf.org/pdf/rfc2401.pdf, 1998.

[7] RFC 2373, IP Version 6 Addressing Architecture[EB/OL]. http://www.ietf.org/rfc/rfc2373.txt, 1998.

[8] Bruce J. Nikkel. An introduction to investigating IPv6 networks[J]. The International Journal of Digital Forensics and Incident Response, 2007, 4(2).