IPv6 下 TCP 分片攻击的研究和检测实现

廖光忠　胡　静

(武汉科技大学计算机科学与技术学院　武汉 430081)

摘　要　IPv6 相对于 IPv4 来说,有更好的安全特性,但不能完全消除网络攻击和入侵。通过分析 IPv6 下的分片重组机制以及 IPv6 分片重组在 Snort 入侵检测系统中的实现,设计了在 Snort 下进行 TCP 分片攻击的试验,实验表明只要入侵检测系统与服务器本身的 TCP/IP 堆栈对数据包的处理方式上存在着不同,TCP 分片攻击是非常有效的从底层绕过入侵检测系统检测的攻击方式,最后给出了网络管理和配置的建议。

关键词　IPv6,Snort,网络攻击,入侵检测,分片重组

随着 Internet 的迅速增长,IPv4 定义的有限地址空间将被耗尽,地址空间的不足必将影响互联网的进一步发展。为了扩大地址空间,拟通过 IPv6 重新定义地址空间。在 IPv6 的设计过程中除了一劳永逸地解决地址短缺问题以外,还考虑了在 IPv4 中解决不好的其它问题。

显然,IPv6 会进一步推动互联网络的发展,网络越发展,网络安全越重要,因为网络越有价值,网络上的攻击和入侵行为就会越多。IPv6 的一些特性带来网络安全的加强,但并非十全十美,不可能解决所有问题,它作为一个新的技术,人们对它的认识和掌握需要一个过程,在这个过程中,黑客们往往走在网络管理员的前面,利用技术掌握的时间差来进行网络攻击,所以分析 IPv6 的安全机制,掌握 IPv6 下网络攻击与入侵检测的特点,已经是非常迫切的事情。

1　IPv6 及网络入侵技术概述

1.1　IPv6 简介

IPv6 是"Internet Protocol Version 6"的缩写,也被称作下一代互联网协议,它是由国际互联网工程任务组(IETF)设计的用来替代现行的 IPv4 协议的一种新的 IP 协议。IPv4 采用 32 位地址长度,只有大约 43 亿个地址,估计在 2005～2010 年间将被分配完毕,而 IPv6 采用 128 位地址长度,几乎可以不受限制地提供地址。按保守方法估算 IPv6 实际可分配的地址,整个地球每平方米面积上可分配 1000 多个地址[1]。

IPv6 有如下的特点,这些特点也可以称作是 IPv6 的优点:

(1)更大的地址空间。IPv4 中规定 IP 地址长度为 32,即有 2^32－1 个地址;而 IPv6 中 IP 地址的长度为 128,即有 2^128－1 个地址。

(2)增强的组播支持以及对流的支持。这使得网络上的多媒体应用有了长足发展的机会,为服务质量控制提供了良好的网络平台。

(3)加入了对自动配置的支持。这是对 DHCP 协议的改进和扩展,使得网络(尤其是局域网)的管理更加方便和快捷。

(4)更高的安全性。在使用 IPv6 网络中用户可以对网络层的数据进行加密并对 IP 报文进行校验,这极大地增强了网络安全。

1.2　网络入侵技术概述

网络安全从其本质上来讲就是网络上的信息安全。从广义来说,凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域[2]。常用入侵方法主要有:

(1)口令入侵:是指用一些软件解开已经得到但被人加密的口令文档,不过许多黑客已大量采用一种可以绕开或屏蔽口令保护的程序来完成这项工作。

(2)特洛伊木马术:它最典型的做法可能就是把一个能帮助黑客完成某一特定动作的程序依附在某一合法用户的正常程序中,这时合法用户的程序代码已被改变。一旦用户触发该程序,那么依附在内的黑客指令代码同时被激活,这些代码往往能完成黑客指定的任务。

(3)监听法:网络节点或工作站之间的交流是通过信息流的转送得以实现,而当在一个没有集线器的网络中,数据的传输并没有指明特定的方向,这时每一个网络节点或工作站都是一个接口[3]。

廖光忠　硕士,讲师,主要研究方向:计算机网络及信息安全、多媒体、系统软件开发;胡　静　硕士研究生,主要研究方向:计算机网络及信息安全。

2 IPv6 下的网络攻击和入侵

2.1 IPv6 带来的网络安全的改善

(1)IP 安全协议 IPSec 是 IPv4 的一个可选扩展协议,而在 IPv6 则是一个必备组成部分。IPSec 协议可以无缝地为提供安全特性,如提供访问控制、数据源的身份验证、数据完整性检查、机密性保证,以及抗重播(Replay)攻击等[4]。

(2)防止网络放大攻击 IPv6 在设计上不会响应组播地址和广播地址的消息,不存在广播,所以,只需要在网络边缘过滤组播数据包,即可阻止由攻击者向广播网段发送数据包而引起的网络放大攻击。

(3)防止碎片攻击 IPv6 认为最大传输单元(MTU)小于 1280 字节的数据包是非法的,处理时会丢弃 MTU 小于 1280 字节的数据包(除非它是最后一个包),这有助于防止碎片攻击。

2.2 引入 IPv6 带来新的安全问题

IPv6 是新的协议,在其发展过程中必定会产生一些新的安全问题,主要包括应对拒绝服务攻击乏力、包过滤式防火墙无法根据访问控制列表正常工作、入侵检测系统遭遇拒绝服务攻击后失去作用、被黑客篡改报头等问题[5]。

此外,在 IPv6 中还有一些问题有待解决,主要包括:

(1)IP 网中许多不安全问题主要是管理造成的。IPv6 的管理与 IPv4 在思路上有可借鉴之处,但对于一些网管技术,如简单网络管理协议(SNMP)等,不管是移植还是重新策划,其安全性都必须从本质上有所提高。由于目前针对 IPv6 的网管设备和网管软件几乎没有成熟产品出现,因此缺乏对 IPv6 网络进行监测和管理的手段,缺乏对大范围的网络故障定位和性能分析的手段。

(2)IPv6 协议仍需在实践中完善,例如 IPv6 组播功能仅仅规定了简单的认证功能,所以还难以实现严格的用户限制功能,而移动 IPv6(Mobiel IPv6)也存在很多新的安全挑战。

3 IPv6 分片重组在 Snort 入侵检测系统中的实现

有了新的入侵方式就会产生新的入侵检测技术,下面着重分析一下 IPv6 分片重组在 Snort 入侵检测系统中的实现。

总的来说,在 IPv4 下的所有分片攻击都能在 IPv6 中重现,只是在实现的具体机制上有所不同。当需要传输的 IP 数据包超过链路所能支持 MTU 时,一个原始 IP 数据包将被拆分成多个分片包;当属于同一个原始 IP 数据包的分片包到达目的节点之后,由目的节点完成分片包的重组。

3.1 IPv6 分片及其重组机制

与 IPv4 不同,IPv6 的包分片操作只能在源节点进行,这简化了中间节点对包的处理,有利于提高中间节点的包转发速率;IPv6 的分片重组操作则与 IPv4 一样,也是在目的节点进行。通过使用路径 MTU 发现机制,源节点可以确定其到目的节点之间的整个路径中能够传送的最大包长度,从而可以避免在中间节点进行分片处理。IPv6 规范中要求最大传输单元的值至少为 1280 byte,并建议将链路配置为至少可以传送包长为 1500 byte 的包。IPv6 规范建议在发送任意长度的包之前,必须检查由源节点到目的节点的路径,计算出可以无需中间节点分片而发送的最大包长度,也就是获得路径最大传输单元。当需要传输的数据包长度超过路径最大传输单元时,源节点就实施分片操作,而目的节点将两个或者多个分片包重组成分片包前的数据包。

从数据包分片的角度看,一个完整的 IPv6 数据包可以分成不可分片部分和可分片部分。不可分片部分包括原始数据包的 IPv6 基本头和每个分片包中必须携带的三种可能出现的 IPv6 扩展头。这三种可能出现的 IPv6 扩展头分别是:逐跳扩展头、目的地选项扩展头和路由扩展头。这三种扩展头如果在原始数据包中出现,每个分片头中都必须携带该扩展头。可分片部分包括可能出现的其他 IPv6 扩展头和数据载荷部分。不可分片部分必须出现在每个分片包中,而可分片部分则被切成两个或者两个以上的部分出现在不同的分片包中,这些分片包拥有相同的分片标志,但是分片偏移量各不相同。因此对于每一个分片包,必须包含三个部分,依次是原始数据包的不可分片部分、分片扩展头、原始数据包的可分片部分的某一个分片[6]。

3.2 IPv6 分片重组在 Snort 中的实现

Snort 是一个轻量级但功能强大的网络入侵检测系统,其软件组织采用插件形式,具有良好的扩展性和可移植性,非常适合通过在标准版本基础上加载新的插件来检测新的攻击。因此通常选用 Snort 软件来实现 IPv6 入侵检测[7]。

对于每一个新接收的 IPv6 分片包,首先从该包中解析出如下数据:分片偏移量,是否还有后续分片的标志量,分片净载荷的起始指针,分片净载荷的长度。Snort 根据源地址、目的地址、分片标志和下一个头的类型这四个元素来惟一地标志属于同一个原始 IP 数据包的所有 IP 分片包,通过在二叉树中以这四个元素为依据来搜索和存储每一个分片包。在将新收到的分片包插入到二叉树之前,系统会实施一系列的检查,主要是检查是否发生分片重复和存在分片空洞。无论是收到第一个包还是收到最后一个包,相应的分片标志记录位都会被置位。比较新

收到的分片包与二叉树中已经存储的分片包的分片偏移量，如果两者相等说明发生了分片重复，我们保留早到的分片包，将后到的包丢弃。分片到齐的首要条件是第一个分片包和最后一个分片包已经到达，接着就要检查该二叉树上属于同一个原始 IP 数据包的所有 IP 分片包了，实际上是检查每一个分片包的分片偏移量是否正好等于上一个分片包的分片偏移量加上一个分片包的分片大小。如果检查完所有分片包后发现没有空洞存在，那就表示所有的分片包都已经到齐，可以进行重组操作了。

将所有到齐之后的分片包重组操作需要重点考虑下述三个问题。首先是不可分片部分的确定与保留问题。必须且只保留第一个分片包的不可分片部分，而所有后续分片包的不可分片部分必须排除在外，这可以通过移动拷贝源地址指针来完成。在具体确定第一个分片包的不可分片部分、分片扩展头、可分片部分时，不能简单地认为 IPv6 基本头之后就是分片扩展头，因为在 IPv6 基本头之后、分片扩展头之前还有可能包含有逐跳扩展头、目的地选项扩展头和路由扩展头中的一种或者多种，因此确定不可分片部分的结尾必须依靠逐层检查下一个头是否是分片扩展头。其次是重组完成之后的 IP 数据包中不能包含有分片扩展头。所以在拷贝数据的时候必须将分片扩展头也排除在外。最后是必须将不可分片部分的最后一个头的下一个头指示域设置为可分片部分的第一个头的类型。该类型原本在分片扩展头的下一个头指示域中，所以在排除分片扩展头之前应该将该域保存下来。只有这样，重组完成后得到的 IP 数据包才和未分片的原始 IP 数据包完全一致[6]。

3.3 试验测试

出于测试的需要，开发一个工具：fragout，它可以拦截、修改、重写、重排发往特定机器的数据包，几乎可以完全控制数据包的发送方式。

3.3.1 测试环境

测试通过两台机器进行，攻击计算机与检测计算机都是安装了 RedHat AS3 的机器，攻击计算机上面的安装了 fragout 和一个简单的 CGI 扫描器。检测计算机作为受攻击的机器，上面安装了 Snort 和 apache，在 apache 的 cgi-bin 目录中故意放入了几个有漏洞的脚本。

3.3.2 测试过程

对检测计算机进行 CGI 扫描攻击，同时在攻击机器上打开 fragout 分片转发，对攻击数据包进行 TCP 分片处理。对 fragout 设定的规则是 TCP 包每片一个字节数据，打乱发送次序并夹杂着虚假重传包。查看此次攻击的 Snort 记录，可以看到全部是误报，攻击已经被有效地隐蔽过去了。查看攻击过程中交换的数据报片断，发现攻击数据包都是只含一个字节数据的报文，而且发送的次序已经乱得不可辨别，但对服务器 TCP/IP 堆栈来说，它还是能够正确重组的。服务器程序重组数据包，经过 apache 处理后返回的结果，可见扫描攻击是成功的。

3.3.3 试验结论

TCP 分片攻击是非常有效的从底层绕过入侵检测系统检测的攻击方式，最新版本的 Snort 1.8.6 不能正确处理这类攻击，其他的入侵检测系统产品都可能或多或少地存在这类问题。试验证明只要入侵检测系统与服务器本身的 TCP/IP 堆栈对数据包的处理方式上存在着不同，都存在着被利用的机会。

结束语 由于当前 IPv6 尚未普及，利用 IPv6 展开的入侵也未在因特网上传开，因此今后的工作将主要围绕提高系统稳定性和处理性能展开，并跟踪国外 IPv6 入侵检测领域的最新动态，及时更新特征规则库和各种处理插件。如果你已经使用 IPv6 网络，就应该注意正确配置网络以发挥 IPv6 的优势，如：在重要的电子商务应用中，应积极使用 Ipsec 协议；在网络的边界过滤一些私有的 IPv6 地址，拒绝这些地址进入和流出网络；对于系统上的主机，使用标准的而不是显而易见的 IPv6 地址，从而增加外部黑客猜测网络地址的难度。每一级网络管理员应该在自己的边界路由设备上配置符合 RFC2827 的网络过滤器来共同防止 IPv6 的地址假冒。如果你还没有使用 IPv6 网络，应该在网络边界严密监视有无各种封装了 IPv6 的隧道数据包进入，并在网络内部监视有无 IPv6 数据报存在，以防攻击者通过 IPv6 隧道入侵了你的网络，这可能需要将防火墙和入侵检测等设备进行升级。

参 考 文 献

1 中国协议分析网[EB/OL]. http://www.cnpaf.net

2 宋献涛，芦康俊，李祥和. 入侵检测系统的分类学研究[J]. 计算机工程与应用，2002(8)

3 Bace G R 著. 入侵检测[M]. 陈明奇等译. 北京：人民邮电出版社，2001

4 关立华，王安文. 入侵检测技术研究[J]. 电信交换，2006(1)：24～28

5 张岳公，李大兴. IPv6 下的网络攻击和入侵分析[J]. 计算机科学，2006，33(2)：100～102

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

7 陈义全. 网络入侵检测系统 Snort 的安全性分析[D]. 浙江：浙江工商大学，2005