IPv6 下的网络攻击和入侵分析*)

张岳公　李大兴
(山东大学网络信息安全研究所　济南 250100)

摘　要　IPv6 有更好的安全特性,但 IPv6 消除不了网络攻击和入侵。本文分析了 IPv6 带来的安全增强,IPv6 网络中依然存在的安全问题,以及 IPv6 引入的新的网络攻击和入侵方式,并特别分析了 IPv4 向 IPv6 过渡阶段技术带来的网络入侵问题,最后给出了网络管理和配置的建议。

关键词　IPv6,网络攻击,入侵检测,入侵特征

Analysis of Network Attack and Intrusion under IPv6

ZHANG Yue-Gong　LI Da-Xing
(Institute of Network Information Security, Shandong University, Jinan 250100)

Abstract　IPv6 contains numerous features that make Internet more security, but it can't eliminate network attack and intrusion. In this paper, we first discuss the improvement of network security after the deployment of IPv6, then we find out the vulnerability that still remains and the new attack approaches that was brought in by the IPv6. In particular, we discuss the security of the transition mechanisms during the shifting from IPv4 to IPv6. And finally, we give some advise on the secure configuration of network.

Keywords　IPv6, Network attack, Intrusion detection, Intrusion signature

1　引言

在 Internet 上,IPv6 取代 IPv4 是历史的必然。这是由于 IPv4 协议固有的弱点决定的,IPv4 地址资源面临枯竭,并在安全上、服务质量上和面向移动的、智能网络的支持等方面上存在严重的不足。新一代互联网协议 IPv6 克服了 IPv4 的许多先天不足。首先,它拥有 128bit 地址空间,相对于 IPv4 的 32 位地址,为互联网的进一步发展提供了近乎于无限的地址空间;其次,可汇聚的、分级的地址结构大大减少了各级路由表的大小,自动配置等功能方便了人们的使用,并使得大量智能终端上网成为可能,IPv6 还支持 QoS,有更好的安全特性[1]。目前,IPv6 已开始在世界范围内的实验网络甚至商用网络中部署。我国的"中国下一代互连网示范工程"(CNGI: china next generation internet)计划投资 14 个亿在 2005 年底以前构筑连接到中国各主要城市的 IPv6 商用骨干网,2006 年正式开始 IPv6 商用服务,可以说全世界,特别是中国已经逐步进入 IPv6 时代。

无疑,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 IPv6 不是一个安全问题的万能药,网络攻击与防御永远会道高一尺、魔高一丈。IPv6 作为一个新的技术,人们对其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,来进行网路攻击和入侵。所以分析 IPv6 的安全机制,掌握 IPv6 下网络攻击与入侵的特点,已经是非常迫切的事情。

2　网络攻击和入侵技术概述

网络攻击和入侵破坏网络信息系统的机密性、完整性和可用性,从总体上来说,可以分为被动攻击和主动攻击。被动攻击是指攻击者通过窃听、监听通信流量等手段,获取网络中传输的数据流,窥探其中的信息和数据,使被攻击者信息的机密性受到破坏。主动攻击手段范围较广,大致可分为:(1)在信息传输路途中进行信息篡改和信息伪造;(2)对网络信息系统的拒绝服务攻击;(3)对计算机信息系统的入侵访问攻击;(4)利用病毒、蠕虫等对计算机系统的渗透攻击。信息篡改和信息伪造破坏了信息的完整性;拒绝服务攻击是破坏系统可用性的攻击,它是通过发起恶意的网络流量阻塞网络或造成系统资源耗尽,从而使计算机系统不能提供正常的服务;入侵访问攻击是攻击者企图获得非授权的访问权限,进而非法访问系统资源,偷窃数据,或非法利用系统资源;病毒、蠕虫则是另一类缓慢的渗透入侵技术[2]。

对付信息窃听、篡改、信息伪造的有力武器是加密、鉴别等密码技术,要解决数据包传输过程中的这些问题需要在 IP 层增加保证机密性、完整性的机制,IPv4 协议制定之初没有考虑这些,后来产生的 IPSec 协议在 IPv4 网络中算一个补丁措施,但其没有被广泛部署。其它的主动攻击都是利用 TCP/IP 协议中的弱点或应用程序的漏洞,弱点和漏洞是难于避免的,因此想消灭攻击和入侵是不可能的,但可以通过对 TCP/IP 协议加强、填补应用程序的漏洞来加大攻击和入侵的难度,从而使系统有更好的抗攻击能力。如,在网络攻击和入侵前,攻击者一般要对系统进行扫描,以寻找漏洞和突破口,如果采取一定的措施,使攻击者难以进行扫描,这就增大

*)基金项目:国家科技部 863 项目,《信息安全基础设施关键技术体系研究》(2001AA141070)。张岳公　博士研究生,主要研究方向:网络信息安全,入侵检测,防病毒;密码学与信息安全。李大兴　教授,博士生导师,主要研究方向:密码学与信息安全。

了攻击和入侵的难度，从而提高了系统的安全性。另外，在IPv4网络中，由于没有地址鉴别的机制，地址假冒很容易，这为网络的恶意扫描、拒绝服务攻击等攻击行为带来方便，攻击者可以肆无忌惮，如果有方法能抑制IP地址假冒行为，就能有效抑制多种攻击和入侵。IPv6的实施就能提供一些较好的安全特性，增加了网络攻击和入侵的难度，从而提高了系统的安全性。

3 IPv6对网络攻击和入侵的影响

3.1 IP层的安全机制

IPv6从设计之初，就对安全问题进行了关注，因此和IPv4相比，IPv6使IP层总体上有了更好的安全特性。通过使用ESP和AH两个扩展头，IPv6把IPSec协议作为协议完整的一部分，而不再像IPv4协议中那样扮演一个可有可无的补丁角色。通过IPSec的加密功能，数据包在网络传输中不再能被偷窥，数据的机密性得到了保证；IPSec的鉴别验证功能，保证了数据包的完整性，防止了数据被更改、数据包重放；地址鉴别功能防止了IP地址假冒，这给许多基于IP地址欺骗技术的攻击和入侵带来难度。

但是由于密码运算的代价，以及IPSec协议在设备认证、密钥协商等方面实施的复杂性(这方面IPsec还有待完善)，不是所有的应用场合下都能配置IPSec，因此偷窥、篡改、假冒在一些情况下还会存在。

3.2 IPv6带来的其他网络安全改善

(1)巨大的IP地址空间给网络恶意扫描和病毒、蠕虫的传播带来困难　通过IP地址对网络进行扫描进而了解网络结构和主机信息往往是网络攻击和入侵的第一步，IPv6地址是128位的，而且和IPv4不同，IPv6所有子网的子网掩码是64位，也就是说所有子网网段有2^{64}的地址空间，而且IPv6的地址可以是自动配置的，一个典型的地址配置是从路由器获得网络前缀，子网内地址采用RFC2373定义的EUI-64地址[3]。如果配置者能够正确配置的话，稀疏的地址空间使它对恶意的扫描具有较高的抵制力，用目前高性能的PC机，扫描整个2^{64}个IPv6地址，需要十多年的时间。同样，这也给通过自动扫描并繁殖的网络病毒和蠕虫的传播带来困难，这些病毒或者蠕虫还想通过扫描地址段的方式来找到有问题的其它主机，非常困难，基本上不可能了。

但是，因为IPv6的地址是128位，很不好记，一些网络管理员们可能会给服务器、路由器等选择一个好记的IPv6地址，这些好记的地址降低了恶意扫描的难度。应该尽量杜绝分配有特征的地址。

(2)层次性的可会聚地址网络结构缓解IP地址假冒问题　IPv4网络是没有结构的，一个IPv4地址或子网可以分布在世界中的任何地方，IPv4源地址假冒是很容易的事，黑客可以使用随机产生的任意IP地址来作为他的攻击IP数据包的源地址，跟踪和回溯假冒的IPv4地址的真正来源是一个很难做到的事情。在IPv6中，由于IPv6网络采用会聚的网络地址结构，IPv6的上级互联网服务供应商(ISP)可以对自己客户的IPv6地址段进行会聚，这使得发布假冒地址报文的难度增大了，ISP可以在路由器或网关设备中使用RFC2827中推荐的过滤器来对网络流量进行过滤，只允许自己客户地址范围内的源地址通过，这样黑客就不能使用任意的源地址来假冒，同时，这使跟踪和回溯假冒的地址变得容易[4]。

尽管RFC2827有推荐，但如果ISP不对自己的客户的网络进行会聚和过滤，则达不到效果，因此要防止IP地址的假冒，需要全社会一致的行动。

(3)不同作用域范围地址对主机访问的保护　在IPv6的地址结构中，一台主机的一个网络接口上可以对应多种IPv6的地址，这些地址分为链路本地地址、站点本地地址、单播全球地址等，这些不同地址有不同的作用域，一台主机上可以只有一个链路本地地址，那么这台主机只能和同一个子网内部的其它主机通讯；一台主机上可以有一个链路本地地址和一个站点本地地址，那么这台主机不但可以和一个子网内部的其它主机通讯，也可以和单位其它的主机通讯；一台主机上可以有一个链路本地和一个站点本地地址，还有一个全局的IPv6地址，那么这台主机不但可以和一个子网内部的其它主机通讯，可以和单位其它的主机通讯，也可以和全球上任何其它有IPv6全局地址的主机建立联系。这样的地址结构为网络管理员加强网络安全管理提供了方便，管理员只分配接口访问域内的地址，外部的节点访问不到它。

(4)IPv6报头中不再有选项字段，而是采用扩展报头的方式，使得防火墙对其的处理更加规整有效　IPv6在数据包的传送路由中，不再支持数据包的分片，而只支持用分片扩展报头，支持端到端的大数据包分片，RFC2460中规定IPv6最小的MTU是1280个字节，这样不应有小于1280字节的数据包被分片，这使得防火墙可以过滤碎片攻击数据包，从而有效遏制IP碎片攻击[5]。

3.3 IPv6下仍然存在的安全问题

虽然IPv6通过对IP层安全机制的加强可以缓解TCP层和应用层的安全问题，但IPv6毕竟是IP层的协议，它对直接针对TCP层的弱点和应用层的程序漏洞的攻击和入侵技术影响不大。在IPv4网络中存在的针对TCP和应用层的攻击技术在IPv6中依然有效。

(1)IPv6对基于TCP协议的攻击或探测手段不能防止，如SYN flood攻击、利用TCP标志位的扫描探测攻击。但在IPv6网络中，追溯攻击的源头要比在IPv4中容易一些，这给针对TCP的攻击带来难度。

(2)针对应用层漏洞的入侵技术，如缓冲区溢出攻击、格式化字符串攻击、Web服务器漏洞等攻击技术在IPv6网络中依然有效，现在一些经典的攻击程序都有了IPv6下的版本。虽然受到很大的抑制，但病毒、蠕虫等的传播机制还是有效的，一些特洛伊木马、后门机制仍然有效。一些经典蠕虫、后门、僵尸代理等程序都在互连网上发布了其IPv6的补丁包。

(3)不管是IPv4还是IPv6，都需要使用DNS，一个IPv6网络中的DNS服务器是很容易发现的。对它的各种攻击技术仍然有效。通过攻击DNS，可以得到大量的在线IPv6的主机地址，进而发起对主机服务的攻击和入侵。

3.4 IPv6带来的新的攻击形式

(1)IPSec协议在IPv6中被普遍支持，任何两个通信节点可以通过IPSec协议建立保密的通信流。这个特点如果被攻击者利用，进行端到端的攻击，由于数据是加密的，防火墙和网络入侵设备都不能解析其数据流，也就不能对其实施安全策略和防护措施。

(2)自动配置是IPv6的一个优点，它使IPv6根据需要相对容易地配置或重新配置地址。但如果一个入侵者已经入侵了一个子网，这为他进一步的入侵带来方便，入侵者可以发布假的路由和地址信息，引起网络配置的错误，从而进一步实施入侵。入侵者还可以通过自动配置实施拒绝服务攻击。

4 IPv6迁移机制带来的网络入侵

由于IPv4在互联网领域广泛而成功的应用，IPv4到IPv6的迁移会经历相当长的一个历史时期，在这个时期内，

IPv4 网络将和 IPv6 网络共存，并逐步迁移。迁移的过程应该是：开始时是 IPv4 网络的海洋中出现 IPv6 的孤岛；IPv6 的岛逐渐增多增大，连接起来，IPv4 网络区域逐渐减少；最后整个网络迁移到 IPv6。一套 SIT(Simple Internet Transition，Internet 简单过渡)的机制已经开始实施，它包括一些协议和管理规则来简化迁移。这些过渡和迁移技术大致分为三类：(1)双协议栈技术；(2)隧道技术；(3)协议转换技术。双协议栈技术是指通信节点同时支持 IPv4/IPv6 两种协议，可以同时与两种协议节点通信，在 IPv4 向 IPv6 迁移的初期，这是必需的，同时双协议栈机制也是后面两种迁移技术的基础。隧道技术是迁移过程中广泛应用的技术，它使 IPv6 的小岛在 IPv4 海洋中通过隧道进行通信，具体又分为许多种隧道，如手动配置的隧道，自动配置的隧道，6to4 机制的隧道和 6over4 的隧道以及 Teredo 隧道协议等。协议转换技术是为了 IPv6 网络和 IPv4 网络主机之间进行通信，并进行上层协议互相访问。

这些迁移协议和机制给网络的迁移带来方便，但同时也给网络安全带来威胁，因为对不熟悉 IPv6 的网络管理员来说，这些机制繁多而复杂，难免出现疏忽或网络配置错误，而别有用心的黑客早已熟悉这些机制并知道怎样利用它。下面以应用较多的 6to4 隧道技术为例说明隧道技术带来的可能网络入侵。

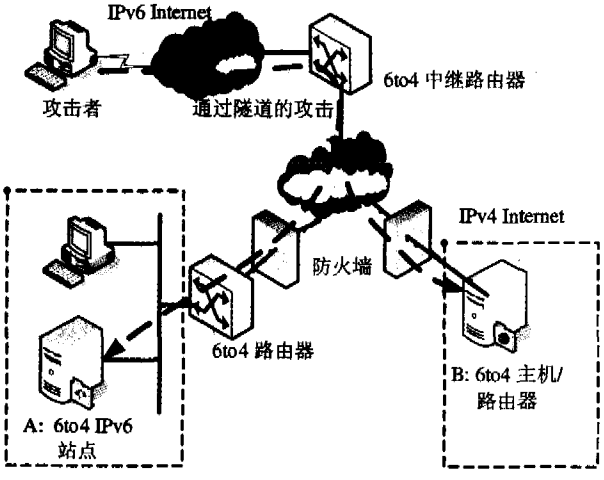

图 1　6to4 隧道协议网络连接示意图

6to4 隧道技术可以实现 IPv6 节点之间使用不经过事先声明的 IPv4 隧道通过 IPv4 网络进行通信，它使用 2002：4VADDR::/48 的地址前缀，其中 4VADDR 是隧道端点的 IPv4 地址。地址的其它部分享有普通 IPv6 地址享有的特性，如地址自动配置，邻居发现和 IPv6 内部路由等。如图 1 所示，6to4 隧道应用在 IPv6 孤岛和 IPv6 网络之间、IPv6 孤岛之间，其中的 IPv6 孤岛可以是 IPv6 的站点(如图 1 中的站点 A)，也可以是一台 IPv4 网络中配置了 6to4 地址和路由支持的双协议站主机(如图 1 中的 B)，后者相当于一个浓缩到一台机器的站点。6to4 路由器是 IPv6 和 IPv4 网络的结合点，在这里 IPv6 的数据包被封装在 IPv4 的数据包中送到其它的 6to4 网路，或通过默认路由将数据包送到位于纯 IPv6 网络边缘的 6to4 中继路由器。中继路由器也完成 IPv6 网络中数据到 6to4 网络数据包的封装。目前支持 6to4 协议机制的操作系统，都可以充当 6to4 主机/路由器，如图 1 中网络 B，可以是任何一台具有合法 IPv4 地址的 Windows XP 或 Linux 主机，由于 Windows XP 和 Linux 已经可以很好地支持 IPv6 和一些隧道协议，这些机器不需要依赖其它支持 IPv6 的路由设备，就可以连接到纯 IPv6 的网络，如 Internet6 或 6Bone。目前许多机构为了推动 IPv6 的发展，在 IPv6 试验网上设置了许多免费的 6to4 中继路由器方便人们的连接[6]。

6to4 隧道机制提供了一个非常方便的自动隧道协议，但同时也给网络攻击带来了方便，正如前面所述，6to4 机制使得 IPv6 孤岛可以方便地通过隧道连接到 IPv6 网络，如果不采取其它网路安全措施的话，这也同时打开了一个从 IPv6 网络或其它 6to4 网络对其攻击的通道。由于目前许多的防火墙和入侵检测设备还不支持对 IPv6 隧道的支持，或虽支持还未引起管理员重视而正确配置，因为许多管理员还未意识到其网络中的一些主机已经通过 6to4 机制连接到了外面的 IPv6 网络上。黑客利用这些 IPv6 隧道，躲过了防火墙、入侵检测系统进入了用户的网络。6to4 机制还可以使黑客通过 6to4 路由器或中继服务器向任何 IPv4 地址主机发送恶意的数据包，发起拒绝服务攻击，因为黑客只要构造一个 6to4 的地址，里面包含要攻击的 IPv4 的地址，6to4 路由器或中继路由器就会以为这是一个隧道数据包，从而用相应地进行 IPv4 封装并发送过去。

其它的隧道协议针对的通信需求不同，但由于都采用了类似的隧道方式，如果没有采取相应的保护措施，都有被攻击者利用的可能。有些机制如 Teredo 类型的 UDP 隧道技术，甚至让一个私网空间地址的设备变得全局可见，且可访问，而且可以越过 NAT 设备和防火墙，这更为黑客攻击带来方便。入侵者可以攻克简单的工作站并将它们设置为隧道路由器，从而躲过路由器或防火墙，直接访问用户的网络。

结束语　IPv6 作为新一代互联网协议，比 IPv4 在性能和安全机制方面有显著的提高，但 IPv6 并不能解决所有安全问题，而且在 IPv4 到 IPv6 的过渡时期，一些过渡和迁移机制甚至带来更大的安全风险，我们应该认识和规避这些风险。如果你已经使用 IPv6 网络，你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，你应该在你的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，这可能需要你将防火墙和入侵检测等设备进行升级。总之，IPv6 已经来到我们面前，我们必须熟悉它，使用好它。

参 考 文 献

1　[美]Davies J 著，张晓彤，等译. 理解 IPv6. 北京：清华大学出版社，2004

2　胡道元，闵京华. 网络安全. 北京：清华大学出版社，2004

3　Hinden R, Deering S. IP Version 6 Addressing Architecture. RFC2373, 1998

4　Ferguson P, Senie D. Network Ingress Filtering: Defeating Denial of Service Attacks Which employ IP Source Address. RFC 2827, 2000

5　Deering S, Hinden R. Internet Protocol, Version6 Specification. RFC 2460, 1998

6　Carpenter B, Moore K. Connection of IPv6 Domains via IPv4 Clouds. RFC 3056, 2001