IPv6之后的网络安全问题分析

刘淑芝,吴海涛
(上海师范大学,数理信息学院 上海 200234)

摘 要:Internet网络安全问题随着Internet的日益发展而越来越被受到重视。由于许多组成Internet基础部分的早期网络协议没有充分考虑安全问题,导致其现在处于易受攻击的状态。黑客们不断地展开越来越狡猾、越来越复杂的攻击,使维护网络安全成为一种旷日持久的战斗。IPv6的出现虽然主要是为了解决IPv4地址空间有限的问题,但同时也为提高网络安全性能从协议基础上提供了支持。

关键词:网络安全;IPv6;Internet
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2006)08-0243-03

Security of Internet in the Wake of IPv6

LIU Shu-zhi, WU Hai-tao
(Mathematics, Science and Information College, Shanghai Normal University, Shanghai 200234, China)

Abstract: Internet security has been a major concern with the development of Internet. Many early network protocols that now form part of the Internet infrastructure was designed without security in mind, and hackers are continuously deploying more and more sophisticated and complex methods of attack. While the main reason for developing the new IPv6 protocol is the limited addressing available in IPv4, along with it comes an opportunity to make the TCP/IP stack more secure against the present vulnerabilities of IPv4.

Key words: network security; IPv6; Internet

0 引 言

Internet如今处于易受攻击的状况下,是由以下几点原因造成的:

* 早期的网络协议缺乏安全意识,这样就为在它们的基础上建立起来的Internet埋下了安全隐患。

* 网络发展迅猛,其结果之一,是复杂应用的快速发展导致了以牺牲安全性能来换取功能性的不良趋势。

* 缺乏训练有素而又有经验的网络管理人员来以安全的方式管理运营网络。

越来越多的主机连入Internet,这对可分配的IP地址空间提出了更大的要求。促使Internet工程任务委员会(IETF)开发出新的IP协议——IPv6。IPv6的安全性能体现在IPSec部分上,虽然IPv4也可以另外加入IPSec部分,但对IPv6来说,IPSec是其必要的组成部分。

导致技术上的易受攻击性的原因可分为3类:

1)软件或协议设计中的缺陷:一些没考虑任何安全因素的协议被投入使用。例如:用于服务器端管理文件的网络文件系统(NFS)被称为安全灾难。因其不支持认证机制,且在客户端和NFS服务器间依赖默认的信任关系。

2)软件或协议实现中的弱点:实现这些协议的应用也许会是有缺陷的。而这些缺陷是可以通过更好的程序设计和应用加以避免的。现在应用层出现的最常见的安全问题有:

* 文件存取中的竞争状况
* 不对数据内容及规模进行检测
* 不对成功或失败的状况进行检测
* 不能适应或调节资源紧张和接近枯竭的状况
* 对操作环境检测不安全
* 对系统调用的不合理运用
* 对软件模块的复用并非初衷

3)系统及网络配置中的弱点:安全问题也许会是由主机或网络的不适当的配置而引起的。例如,有的主机没有开启某一项服务,可是用于这种服务的端口却被开放了。在网络层,防火墙往往被错误地配置,结果导致那些来自非信任关系主机的连接也可以被建立[1]。

IPv6的出现并没有给网络安全提供一副万能药,网络安全问题的解决还需要与防火墙、入侵检测系统等其他防御系统配合。

1 入侵方法的演进

不管是为了寻找乐趣还是为了寻求利益,那些在一直努力发现系统薄弱环节的入侵者,已经取得了长足的进步,现今已经显示出对网络安全构成威胁的趋势。入侵者已经在以下方面取得很大进展:

收稿日期:2005-11-28
作者简介:刘淑芝(1978-),女,河南商丘人,硕士研究生,研究方向软件工程;吴海涛,副教授,研究方向为软件工程、数据挖掘。

(1)入侵者的技术知识:他们对于网络拓扑结构、操作及协议的理解更深入了。他们不辞辛苦地检验源代码以期发现程序中的弱点所在。更要命的是现在大多数系统是开放资源的,所以很容易得到更多的源代码。

(2)发现薄弱点的技术:入侵者变得越来越老练了,他们不断发明出新的复杂的攻击方法。一般来说刚接入网络的系统,从安全角度看,由于还没有完全配置好,所以很容易受到攻击。入侵者可以首先发现那些刚接入因特网的节点,从而使其成为潜在的受攻击对象。假如某个系统是安全的,他们还可以利用越岛作战的策略来建立计算机之间的信任关系。运用越岛作战策略,利用已经取得目标主机信任的主机,来建立与目标主机之间的信任关系。因为所利用的主机安全性能较弱,所以可以被轻易地利用;而又因为所攻击的目标主机的安全性能强,却对被利用的主机已经产生了信任,所以能给攻击者可乘之机而又不会轻易跟踪到攻击者。

(3)入侵者对软件工具的使用:能发起网络攻击的工具已经变得越来越有效、越来越容易使用、容易被那些对计算机系统了解不深的人所获得。甚至一个对网络一无所知的人都可以使用交互界面友好的工具来发起一些攻击[3]。这些工具包括:

* 网络扫描器
* 密码破解工具及大型字典
* 嗅探器
* 各种木马程序库
* 各种选择性修改系统日志文件的工具
* 各种自动修改系统配置文件的工具
* 报告伪造检测和的工具

2 网络攻击的种类

网络攻击的大体分类如下[2]:

* IP 欺骗
- 盲目和非盲目的欺骗
- LAND 攻击
- Smurf 攻击
* 嗅探器
* 操作系统指纹
* SYN 攻击
- SYN 洪水攻击
- 猜测 ISN 序列号
* 路由攻击
- 路由器重新定位
- 虚假路由信息
- 虚假子网掩码
* DNS 攻击
- DNS 缓存中毒
- DNS 零转换
* 碎片攻击
- 死亡之 PING
- 微小碎片攻击
- 眼泪攻击

3 IPv6 的问题

除了从 IPv4 到 IPv6 转换的安全问题外,IPv6 还带来了一些其他的问题:

* 通过使用针对处理器的强有力的密码系统方法,实施 DoS(Denial of Service,拒绝服务)攻击变得更容易。

* 如果使用 ESP(Encapsulated Security Payload)头,则对于防火墙来说是有可能分析出上下文的。在使用管道模式时,由于 IP 地址对于防火墙是不可见的,那么在一个内部网中便可建立一个与非信任主机的连接。

* IPv6 需要自动配置,这就给 DoS 攻击以可乘之机,因为系统对于欺骗性的子网掩码回复的免疫力是很弱的。

* 移动通讯方面的安全专家已发现一些安全漏洞。

* DNS 更为复杂,这样将会导致安全问题。由于性能问题,DNS 的认证询问与答复都不具有太多的可行性。

IPv6 在解决某些问题上是无能为力的。如,一个被授权的用户滥用其权利;防火墙和主机的配置错误;若代码中有漏洞,IPv6 也无法挽回破坏安全的局面。用户和管理员往往会有一种安全的错觉,事实上,IPv6 虽然被设计地可以提供更高的安全性,但并不是一副万能药[1]。

4 防火墙的作用

4.1 防火墙的定义

防火墙是用于网络级访问控制机制的设备。在大多数情况下防火墙用来阻止外来人员访问内部网络。防火墙设备通常是单独的计算机、路由器或防火墙固件。防火墙固件通常是运行定制或专用操作系统的专用硬件设备。

防火墙被设计为出入网络的控制点。它们评判收到的连接请求。防火墙根据预先定义的一套规则或"政策"来查看网络通信是否被允许,只有从授权主机到授权目的的连接请求才能被处理,其他的连接请求被丢弃[3]。

4.2 IPSec 简介

IPv6 的安全性能主要体现在 IPSec 上,IPSec 的结构如下:

1)AH(An Authentication Header)。IP 的认证头部,使通讯方确认数据在传输过程中没被修改并且数据来源正确。

2)ESP(An Encapsulating Security Payload)。IP 的封装的安全有效载荷形式,可以加密数据使其在传输过程中不会泄密。

3)IKE(Internet Key Exchange)。一个用于协议交流和钥匙交换的协议,使通讯方通过 ESP 和 AH 交流安全通讯认证的方法[4]。

4.3 IPSec 与防火墙

要知道 IPSec 的存在并没有使防火墙成为冗余的,事

实上,两者是相辅相成的。防火墙关注于基于安全策略的以及特定网络间的连接种类,与此同时 IPSec 确保特定连接的认证机制和机密性。接受还是拒绝与内网间一些内部主机的连接取决于 IPSec 所提供的特性。如果和防火墙一起使用,IPSec 可用于组建 VPN(Virtual Private Networks,虚拟内网)。同样,防火墙可以在 IPSec 下发挥更好的效用。

有一些防火墙的功能 IPSec 就无法处理。防火墙可以保护所有内部主机的不恰当配置。虽然很难确保所有内网中的节点都被正确配置,但不管配置正确与否,在防火墙级很容易控制与这些节点连接的建立。这样防火墙也可以限制对有问题系统的访问,这些系统往往易受到外来的攻击。

还有一个和使用加密相关的问题,根据安全策略应该由防火墙和 IPSec 来解决。防火墙允许使用主机对主机、防火墙对主机或防火墙对防火墙加密连接[5]。

(1)主机对主机加密:对防火墙来说,由于无法看到包中的内容所以难以运用安全策略,例如:在管道模式下 IP 地址和端口号都加了密,一个主机便可以连接到一个被禁止的外部主机上。

(2)防火墙对主机/防火墙对防火墙加密:包的信息可以被内网的主机嗅探到,大多数嗅探器是由内网的主机启动的。

5 入侵检测系统的作用

入侵检测系统用于检测可能存在的入侵行为,通过计算机网络或计算机系统中的若干关键点收集信息并进行分析,从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。更重要的是,入侵检测系统检测并发现存在的网络攻击以及网络错误。安装在网络中的入侵检测系统就如同一个房间中安装的用于防止盗贼的防盗报警器,能发现网络中的非法入侵行为,并根据相应的情况发出警告或者报警[3]。

入侵检测系统往往和防火墙同时配合使用,管理并控制进出网络的数据。这两种安全工具在网络中起到完全不同的作用,防火墙如同房前的警卫,保护房子的安全并阻止入侵者闯入屋子中。入侵检测系统则检测网络是否正在受到攻击。

入侵检测系统是防御系统的最后一道防线。它可以检测到,从而可以帮助避免一些可穿越防火墙的入侵。即使是使用 IPSec,那些被授予了权限而又滥用权限的用户仍然无法被阻止,入侵检测系统可以检测到此类入侵。

6 结 论

尽管 IPSec 试图解决 IPv4 中的主要安全问题,但其本身的引入也带来了新的问题。虽然 IPSec 解决了很多问题,但仍然有些问题留待解决。

同时可得出的结论是:IPSec 并没有使其他安全防御体系成为冗余,如防火墙、IDS(入侵检测系统)。对于整个安全体系来说,此三部分:IPSec、防火墙、IDS 应该是共同存在、互相扶持,其安全效果胜于任何一个的单独使用。

参考文献:

[1] Chauhan Y. Security in the wake of IPv6[EB/OL]. A Term Paper Report for Advanced Computer Networks (CS625). Department of Computer Science & Engineering, Indian Institute of Technology, Kanpur. http://www.cse.iitk.ac.in/, 2000.

[2] 黄 鑫,沈传宁. 网络安全技术教程[M]. 北京:中国电力出版社,2002.

[3] Anonymous. 最高安全机密[M]. 王东霞,等译. 北京:机械出版社,2004.

[4] Triulzi A. Intrusion Detection Systems and IPv6[EB/OL]. http:// www.alchemistowl.org/ arrigo/Papers/SPI2003 - IDS - and - IPv6.pdf,2003.

[5] Abie H. An Overview of Firewall Technologies[EB/OL]. http://www.nr.no/~abie,2000 - 01.

(上接第 210 页)

上教学系统的模型。该系统可采用 Java 语言编程,因其具有动态性、分布性、多线性、与平台无关性和它在分布异构环境中面向对象编程方法和对象序列化、映像 API 和远程方法调用 RMI 等优点,最适合该系统的特点[3,4]。

文中 NTS 在功能与技术上有较好的分离,适用于 Internet 网,也适用于校园网上的教学。与传统的智能化教学系统相比,在人机交互的基础上增加了系统与学生的交流,增强了系统的人性化,更能准确地、实时地按照学生的学习水平来建议学习策略与学习路径;并在学生有疑问时及时地实现个别化答疑或提供讨论式的教学环境,以实现因材施教的原则[5]。基于多 Agent 的网上教学系统,教学资源的自适应组织,有利于个性化网络教学的开展,能适合于多个学生同时共享系统中的资源,满足不同学习者的需求,从而降低教育成本,以提高系统的教学效率。

参考文献:

[1] 何炎祥,陈莘萌. Agent 和多 Agent 系统的设计与应用[M]. 武汉:武汉大学出版社,2001.

[2] 徐英卓. 基于多智能体和 CSCW 的协同远程教学系统[J]. 计算机应用,2003,23(11):112 - 114.

[3] 李拥军,王惟言. 基于多 Agent 网际实时教学系统的研究和实现[J]. 计算机工程与应用,2003,39(18):181 - 183.

[4] 申瑞民,许彦青,张同珍,等. 基于多代理的智能型远程教学环境研究[J]. 计算机工程与应用,2002,38:253 - 255.

[5] 董武绍. 关于基于多 Agent 系统的远程教学模式研究[J]. 电化教育研究,2001,9:36 - 39.