计算机网络安全与防护技术研究

闻德军[1,2],张代远[1,2,3]
(1.南京邮电大学 计算机学院,江苏 南京 210003;
2.江苏省无线传感网高技术研究重点实验室,江苏 南京 210003;
3.南京邮电大学 计算机技术研究所,江苏 南京 210003)

摘 要:计算机和网络安全是个至关重要的话题,但是仅仅靠防护系统来保存网民、企业和政府机构的数据是远远不够的。如路由器、DNS服务器和交换机等基础设施能够很好地将网络连接在一起,否则计算机不可能进行可靠的通信。鉴于网络安全的重要性,引出了几个问题:要用怎样的基础设施来应对怎样的网络安全威胁,当然首先要考虑的是成本。但是在所有这些问题之前要知道如何去定义一个安全的系统。什么是安全?每个人都能说出点什么,但很少有人能够对安全做出精确的定义。文中将以独特的视角来定义网络安全,因为这关系到一个国家、一个组织甚至是个人用户的现在和将来。

关键词:网络安全;防范技术;SYN洪范攻击
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2012)12-0171-04

Research of Computer Network Security and Defence Technology

WEN De-jun[1,2], ZHANG Dai-yuan[1,2,3]
(1. College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;
2. Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China;
3. Institute of Computer Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: Computer and network security are critical issues. But merely protecting the systems that hold data about citizens, corporations, and government agencies is not enough. The infrastructure of networks, routers, domain name servers and switches that glue these systems together must not fail, or computers will no longer be able to communicate accurately or reliably. Given the magnitude of secure cyberspace, a reflection on what are trying to do seems in order. Several questions arise, such as what exactly the infrastructure is, what threats it must be secured against, and how protection can be provided on a cost-effective basis. But underlying all these questions is how to define a secure system. What is security? Having it is obviously good; everyone says so. But few people defines it exactly, or even nebulously. This column tries to place cybersecurity in perspective, because it is, of course, central to countries, organizations, and even home users now and in the future.

Key words: network security; defence technology; SYN Flood

1 概 述

各个国家的财报显示计算机和网络安全问题迫在眉睫,如果你对此持怀疑态度,请阅读当地的报纸,每天都有一些新的网络安全事件被曝光,最近一份报告显示,黑客攻击和病毒的传播每年在全球范围内至少造成1600亿美元的损失,这只是对公司和团体造成的直接经济损失,其间接经济损失是无可估量的。网络安全意识淡薄,网络安全防范能力薄弱,给了别有用心之人以可乘之机。我国的网络安全形势尤其严峻,信息技术起步较晚,决定当前必须学习借鉴国外先进的技术,打好理论基础,逐步发展和强化自主研发能力[1]。

1.1 计算机网络安全及防护技术概述

网络安全从其本质上讲就是网络上的信息安全。防止和检测对为授权资源的访问。网络安全的服务和

收稿日期:2012-03-19;**修回日期**:2012-06-23
基金项目:江苏高校优势学科建设工程资助项目(yx002001)
作者简介:闻德军(1989-),男,硕士研究生,研究方向为智能计算技术与应用;张代远,教授,硕士生导师,研究方向为智能计算理论、方法与应用,计算机体系结构,计算机在通信中的应用。

目标主要包括以下几点:信息传输安全隐密,对信息发送方的身份认证,接收方对信息完整性的检测,仅能访问授权资源和不可否认性[2]。

1.2 计算机网络安全的基本特征

一个较好的计算机网络系统应该具备以下特征:安全隐密性:信息不泄露给非授权的用户、实体或过程,或供其利用的特性;完整性:信息在传输过程中保持不被篡改、不被破坏的特性;可控性:对信息的传播及内容具有控制能力;授权性:可被授权实体访问,即当需要时应能存取所需的信息而拒绝未授权实体的访问、对授权实体也只能访问被授权的部分。网络环境下拒绝服务、散布电脑病毒和危害有关系统的正常运行等都属于对可用性的攻击[3]。

2 计算机网络安全与防范技术概述

现阶段网络安全的几种关键技术主要通过一定的防护技术和措施来维护和保障信息安全,当前网络安全的关键技术主要包括以下几种。

2.1 访问控制技术

访问控制技术:访问控制是信息安全防范和保护的主要核心策略,它的主要任务是对限定的资源进行授权访问,有效地保证了网络安全。访问控制策略主要包括服务器安全控制、目录级控制、网络权限控制、入网访问控制、以及属性安全控制等多种手段[4]。

2.2 数据加密技术

数据加密技术:是利用加密密钥或加密函数转换为没有意义的密文,信息的接收方再通过解密密钥或解密函数还原成明文。数据加密技术通常分为“非对称式”和“对称式”。非对称式加密:加密密钥和解密密钥不同,分别被称为“公钥”和“私钥”,加密用“公钥”,解密必须用与之配对的“私钥”,否则无法打开被加密的文件(如 RSA 算法)。非对称加密算法的优越性在于,只有持有“密钥”的接收方才能解密信息,而“密钥”不需要在网络中传输,这很好地避免了密钥的传输安全性问题。但由于“公钥”是众所周知的。任何人都可以发送加密报文,这就无法鉴别数据的发送方。对称式加密:加密和解密使用同一个密钥,通信双方必须交换彼此的密钥,当需要交换信息时,发送方用自己的密钥对信息进行加密,接收方用对方给的密钥进行解密。这种加密技术目前被广泛采用,如美国政府所采用的 DES 和 MIT 的 Kerberos 就是典型的“对称式”加密法。

3 SYN Flood 攻击原理与防范

3.1 SYN Flood 的基本原理

SYN Flood 是一种利用 TCP 协议设计缺陷,向服务器发送大量伪造的 TCP 连接请求,由于 IP 地址是伪造的,服务器永远也等不到客户端返回,但服务器在等待客户端返回时,需要消耗一些资源,如果这种伪造的请求数量足够大,被攻击方的就会因为内存不足或 CPU 满负荷而无法响应正常用户的请求,SYN Flood 攻击是当前最流行的 DoS(拒绝服务攻击)与 DDoS(分布式拒绝服务攻击)的方式之一。

在分析 SYN Flood 的攻击原理前,必须要清楚 TCP 连接的建立过程:

与 UDP 不同的是 TCP 是一种可靠的、复杂的、面向连接的协议。TCP 协议保证数据报文最终一定能到达目的地,为了保证这种可靠性,通信双方必须在交换数据前建立一条端到端的连接即 TCP 连接。要建立一个服务器和客户机的一个 TCP 连接要进行三次握手(Three-way Handshaking),建立 TCP 连接的三次握手详细过程如下:

首先,连接请求的发起方(即通常所说的客户端)发送一个设置了 SYN 标志的 TCP 报文,这个报文对此条连接的一些参数进行协商(如连接双方的窗口大小、交换的最大报文大小、客户端使用的端口、打算连接服务器的端口号以及 TCP 连接的 SEQ 等),该报文发出后客户端进入 SYN_SEND 状态[5]。

其次,服务器在收到客户端的 SYN 报文后,将返回一个包含服务器初始序列号的 SYN+ACK(即确认 Acknowledgement)报文作为应答,表示接受客户端的请求,同时对确认序列号加一表示对客户端的 SYN 报文的确认,此时服务器进入 SYN_RECV 状态[6]。

最后,客户端再返回一个确认报文 ACK 给服务器端,同样对 TCP 序列号加一表示对服务端的 SYN+ACK 的确认,到此一个 TCP 连接完成,服务端和客户端可以进行 TCP 数据的传输,此包发送完毕,客户端和服务器进入 ESTABLISHED 状态,至此建立 TCP 连接的三次握手完成,双方可以进行数据传输。

从 TCP 连接的建立过程来看,在服务器发出 SYN+ACK 确认报文后要等待收到客户机对服务器的 SYN 的确认报文后才完成一个 TCP 连接的建立。服务器在发出 SYN+ACK 确认应答报文后,服务器会为此连接维持一个定时器,在定时器超时之前收到客户端的 ACK 报文则 TCP 连接建立成功,如果在定时器超时之前没有收到客户端的 ACK 报文,服务器就会丢弃这个未完成的连接。这个定时器的时间长度称之为 SYN Timeout(这个时间一般为 30 秒 ~ 2 分钟)。SYN Flood 正是利用了服务器必须为客户端进程维持一个 SYN Timeout 时长来进行攻击,如果是攻击者伪造了大量的 TCP 请求导致服务器有大量处于 SYN_RECV 状态的连接,服务器端将为了维护这些半连接请求而消耗大

量的 CPU 时间和内存。SYN flood 就是伪造大量的 TCP 连接请求来对服务器进行攻击,可以想象大量的保存、遍历并且对列表中的 IP 进行 SYN+ACK 重试也会消耗非常多的 CPU 时间和内存,服务器的负载将会变得非常巨大。随着半连接数的持续增加最终会导致 TCP/IP 堆栈溢出而导致服务器宕机[7]。由于攻击者可以利用多台机器以很高的频率发送攻击报文,所以正常用户的请求相对于攻击报文来说是极少的,服务器大部分时间都被用来处理攻击者伪造的 TCP 连接请求导致正常用户的请求得不到响应(表现为打开页面缓慢或服务器无响应)。

从防御角度来讲,存在几种的解决方法:

第一种缩短服务器维持每个半连接的定时器的时间长度(即缩短 SYN Timeout)。服务器保持的 TCP 半连接数显示了 SYN Flood 攻击的效果,TCP 半连接数 = SYN Timeout * 发送 SYN 请求包的频度,虽然无法左右请求包的发送频度,但是可以通过缩短定时器的时长来降低服务器端的 TCP 半连接数。在受到 SYN Flood 攻击时,定时器为 30 秒的服务器的负载要比定时器为 2 分钟的服务器负载小 4 倍。如果定时器被设置为 30 秒以下就有可能影响到对正常用户的服务。

第二种方法是对每一个 SYN 请求设置一个本地 Cookie,就是服务器在收到 SYN 包并返回 SYN+ACK 后,根据 SYN 包计算出一个 Cookie,根据 Cookie 值来判断某一个 IP 的发送 SYN 请求包的频率,若同一个 IP 发送请求报文的频率过大,则认为此报文是来自这个 IP 的攻击报文,服务器会保存该 IP,并丢弃所有从该 IP 发出的请求报文。

以上的两种方法只是对比较原始的 SYN Flood 攻击的防御,在攻击源少和攻击频度不高的情况下,缩短 SYN Timeout 时间才会有明显的效果,如果攻击者增加攻击源或者加大攻击频度,服务器对此也无计可施。SYN Cookie 更依赖于攻击方使用真实的 IP 地址,如果攻击方利用 SOCK_RAW 可以自己随机定义 IP 报文中的源地址,SYN Cookie 方法将毫无用武之地,同时为每个请求的 IP 地址保存 Cookie 也将增加服务器的负担。

3.2 SYN Flood 攻击的监测与防御初探

目前尚没有针对 DOS 攻击,特别是 DDOS 攻击的很好的监测和防御方法,需要系统管理员深刻理解 SYN Flood 攻击的原理,利用攻击程序的实现缺陷,再结合系统架构制定一些防御措施。判断是否受到 SYN Flood 攻击的方法也很简单:由于大多数的攻击者都会使用原始套接字伪造 IP 地址,所以只要服务器上有大量状态是 SYN_RECV 的半连接,且是 IP 地址是随机的,这是就基本可以认为受到了 SYN Flood 攻击[7,8]。

在系统检测到 SYN Flood 攻击时,管理员可使用 Netstat - P - N TCP > TCPStatus. txt 命令将记录系统当前所有 TCP 连接的状态保存到文件以供分析所用,如果使用网络嗅探器(如影音神探、酷抓、影音嗅探专家等)或 TcpDump 之类的工具,详细记录 TCP SYN 报文(如源地址、TTL 值(Time to Live)、生存时间、IP 首部中的标识、TCP 首部中的序列号等),虽然攻击者可以使用原始套接字伪造这些信息,但是对分析也还是能起到一定的作用。特别是 TTL 值,TTL 是定义了数据包可以被中转的次数,数据包每经过一次转发,TTL 值就会被减一,故可以根据数据包的 TTL 值攻击源与我们之间的路由器距离(甚至可以根据 TTL 值推断出对方的操作系统类型),通过过滤特定 TTL 值的请求报文将大多数攻击报文,减轻被攻击系统的压力,从而使正常的请求报文有机会可以得到响应,这种方法也可能影响到正常用户的访问。

对于 Win2003 系统,注册表项 HKEY_LOCAL_MACHINE \ Sytem \ CurrentControlSet \ Services \ Tcpip \ Parameters 被默认设置为 1(默认开启 SYN 攻击防护)[9]。

增加一个类型为 REG_DWORD 的键值 TcpMaxHalfOpen,这个键值定义了系统与同时打开的半连接数,取值范围是 0x100 ~ 0xFFFF, windows server 2003 Stardard Edition 的默认值是 100, Datacenter Edition 和 Enterprise Edition 版本的 windows server 2003 是 500,这个值取决于服务器维持的 SYN-RECV 状态的 TCP 连接的数量。具体的值需要管理员根据经验和系统历史负载峰值来决定,为了最大限度地发挥出系统自身对攻击的防御能力,将 TcpMaxHalfOpen 值设为 TcpMaxHalfOpenRetried 值的 1.25 倍。

增加一个类型为 REG_DWORD 的键值 TcpMaxHalfOpenRetried,取值范围是 80 ~ 0xFFFF, windows2003 的默认值是 80, Stardard Edition 是 100, Datacenter Edition 和 Enterprise Edition 版本的 windows server 2003 是 400,这个参数决定在服务器所维持的处于 SYN-RECV 状态的连接数达到多少系统会打开 SYN 攻击保护。

来简单分析一下 windows 2003 对 SYN Flood 攻击防护机制:windows 2003 对建立 TCP 连接三次握手的 SYN-ACK 的重试次数、SYN Timeout 时间等参数做一个常规设置。一旦服务器检测到 SYN 半连接的数量超过 TcpMaxHalfOpenRetried 的设置,就认为自己受到了攻击,此时 SynAttackProtect 键值中的选项开始生效,发送 SYN-ACK 确认包的重试次数减少, SYN Timeout 时间缩短,为了避免对 TCP/IP 堆栈溢出,将攻击的危害降到最低,已在缓冲区中的 SYN_ACK 报文会被延时发送,如果攻击者还在不断地向服务器发送

伪造的 SYN 报文,半连接数量超过了 TcpMaxHalfOpen 键值的设置,此时系统为了保证 TCP/IP 堆栈不会溢出,将会丢弃接下来所有的 SYN 报文,包括正常用户的请求。

这种通过设置注册表防御 SYN Flood 攻击,是一种被动的防御策略。下面来看看另外一种比较有效的方法[10]。

介绍这种方法前,首先来了解一下 SYN Flood 的攻击方法:SYN Flood 只在攻击开始前一次性解析出要攻击服务器的 IP 地址。这种一次解析目标 IP 地址的攻击方式暴露它最大的弱点:当攻击目标在检测到自己受到了 SYN Flood 攻击后迅速更换自己的 IP 地址,那么由于攻击者没有对被攻击系统的 IP 地址重新解析,接下来的 SYN 攻击包被发给了一个并不存在的主机,攻击的效果就无法达到了。为了不影响正常用户的访问,管理员只需将域名的 DNS 解析更改到新的 IP 地址,在本地 DNS 的刷新之前用户的正常访问会受到影响。

如今要完全杜绝 DDOS 攻击是不可能的,但可通过适当的方法增加 DDOS 攻击者的成本,那么很多攻击者不能承受这样的成本开销而放弃攻击,也算是成功抵御了 DDOS 攻击。由于 DDOS 不可能完全杜绝,只能通过采取一定的措施将攻击带来的危害降到最低。互联网的专家们一直在努力寻找更好的方法,让我们拭目以待新技术和新产品的诞生[11]。

4 结束语

当今计算机网络飞速发展同样也带来了很大的隐患,不怀好意的黑客攻击和病毒的肆虐给计算机安全带来巨大压力,计算机安全方面的专家们也在为维护网络安全作不懈的努力。但是各种攻击手段在不停地更新,一方面要加强系统自身的安全性,不给人以可乘之机,另一方面,要对现存的攻击手段做详细分析,以便更新对攻击的防范手段[11]。

文中通过叙述威胁计算机网络安全的因素有哪些,然后通过一个具体的实例(SYN Flood 攻击)分析其具体的防范技术,对其他的网络安全问题也起到一定的启发作用,让人们在生活和工作时能够放心地畅游计算机网络世界。

参考文献:

[1] 赵 敬,孙洪峰. 信息与网络安全防范技术[J]. 现代电子技术,2003(8):5-9.

[2] 宋渊明,杨 明. 信息与计算机通信网络安全技术研究[J]. 信息技术,2003(4):202-251.

[3] 戴启艳. 影响信息系统安全的主要因素及主要防范技术[J]. 中国科技信息,2010(6):34-58.

[4] 李晓明,付丹丹. 计算机网络攻击分析及防范技术[J]. 电脑学习,2010(6):24-26.

[5] 韩 卫,薛 健,白 灵. 一种基于安全隧道技术的 SSL VPN 及其性能分析[J]. 科学技术与工程,2005(12):791-796.

[6] 张大成,韩 坤. 信息加密技术分析[J]. 科技信息(学术版),2007(5):53-53.

[7] 刘 伟. 访问控制技术研究[J]. 农业网络信息,2007(7):96-97.

[8] 万 琳,张 鹰,李 理. 浅谈基于角色的访问控制技术[J]. 计算机与数字工程,2007,35(10):145-148.

[9] Microsoft Windows Server 2003 TCP/IP Implementation Details[M]. Microsoft Corporation,2010:12-24.

[10] Jurjens J. Code security analysis of a biometric authentication system using automated theorem provers[C]//21st Annual Computer Security Applications Conference (ACSAC 2005). [s.l.]:IEEE Computer Society,2005:54-58.

[11] Rubin A D,Geer D E. A Survey of Web Security[J]. Computer,1998,31(9):34-41.

(上接第 170 页)

人民大学出版社,2004.

[8] Milanovic N, Malek M. Current Solutions for Web Service Composition[J]. IEEE Internet Computing,2004,8(6):51-59.

[9] 黄建忠,谢长生,曹 强,等. 基于三方通信构架的可信任网络存储安全系统的研究[J]. 华中科技大学学报(自然科学版),2005,33(S1):158-160.

[10] 黄建忠,谢长生,罗东健,等. 一种基于权能标识的三方安全协议的设计和分析[J]. 计算机科学,2007,34(3):50-53.

[11] 欧洲银行标准委员会. 加密算法使用与密钥管理指南[S]. TR406V2-CN,2001.

[12] 王全民,周 清,刘宇明,等. 文件透明加密技术研究[J]. 计算机技术与发展,2010,20(3):147-150.