网络安全作业

张皓

201622220211

# i．DDoS防御

分布式拒绝服务(DDoS:Distributed Denial of Service)攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击，从而成倍地提高拒绝服务攻击的威力。通常，攻击者使用一个偷窃帐号将DDoS主控程序安装在一个计算机上，在一个设定的时间主控程序将与大量代理程序[通讯](http://baike.baidu.com/item/%E9%80%9A%E8%AE%AF" \t "_blank)，代理程序已经被安装在网络上的许多计算机上。代理程序收到指令时就发动攻击。利用客户/[服务](http://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1)器技术，主控程序能在几秒钟内激活成百上千次代理程序的运行。

DDoS攻击通过大量合法的请求占用大量网络资源，以达到瘫痪网络的目的。这种攻击方式可分为以下几种：

1.通过使网络过载来干扰甚至阻断正常的网络通讯；

2.通过服务器提向交大量请求，使服务器超负荷；

3.阻断某一用户访问服务器；

4.阻断某服务与特定系统或个人的通讯。

而攻击后会造成：

1.被攻击主机上有大量等待的TCP连接；

2.网络中充斥着大量的无用的数据包；

3.源地址为假 制造高流量无用数据，造成网络拥塞，使受害主机无法正常和外界通讯；

4.利用受害主机提供的传输协议上的缺陷反复高速的发出特定的服务请求，使主机无法处理所有正常请求；

5.严重时会造成系统死机。

DDoS攻击时利用一批受控制的机器向其它机器发起流量攻击，所以对此并没有太完美的办法能够解决这个问题。但是对于DDoS现在仍有一些办法能够缓解攻击影响。

1. 高性能网络设备的防御技术 首先要保证网络设备不能出现服务瓶颈，因此选择路由器、交换机、硬件防火墙等设备的时候要尽量选用知名度高、口碑好的产品。建议与网络提供商就安全服务达成协议，当大量攻击发生的时候请他们在网络节点处进行流量限制来对抗DDoS攻击是非常有效的方法。对于提供服务的服务器，可以采用分布式集群方式部署，这样能缓解小量的DDoS攻击。比如说，硬件防火墙的并发连接数，吞吐量、安全过滤带宽等。这些参数会影响抗 DDoS攻击的能力。以每个用户需要10.5个并发连接来计算，一个中小型企业网络(1000个信息点以下，容纳4个C类地址空间)大概需要10.5×1000=10500个并发连接，因此支持10500 个最大并发连接的防火墙设备便可以满足需求;大型的企事业单位网络(比如信息点数在 1000-10000 之间)大概会需要105000个并发连接，所以支持100000-120000最大并发连接的防火墙就可以满足企业的实际需要;而对于大型电信运营商和ISP来说，电信级的千兆防火墙(支持120000-200000个并发连接)则是恰当的选择。
2. 优化系统来缓解DDoS攻击

对于NT系统来说，可以加固TCP/IP堆栈来抵御拒绝服务攻击。

以下列表说明了与TCP/IP相关的注册表值，您可以在直接连接到Internet的计算机上配置这些值，以加固TCP/IP堆栈。除非特别指出，否则所有这些值均应在以下注册表项下创建: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services

注意 :除非特别指出，否则所有值均为十六进制。

数值名称 :SynAttackProtect

项 :Tcpip\Parameters

数值类型 :REG\_DWORD

有效范围 :0，1

默 认 值 :0

该注册表值可使传输控制协议(TCP)调整SYN-ACKS的重新传输值。配置该值后，如果出现SYN攻击(拒绝服务攻击的一种)，连接响应超时时间将更短。

下列参数可与该注册表值一起使用 :

0(默认值):无 SYN 攻击防护

1 :将 SynAttackProtect 设置为 1 可更有效地抵御 SYN 攻击。该参数可使 TCP 调整 SYN-ACKS 的重新传输值。将 SynAttackProtect 设置为 1 时，如果系统检测到存在 SYN 攻击， 连接响应的超时时间将更短。Windows 使用以下值确定是否存在攻击 : TcpMaxPortsExhausted

TCPMaxHalfOpen

TCPMaxHalfOpenRetried

注意 :在 Windows Server 2003 Service Pack 1 中， SynAttack Protect注册表项的默认值为 1。

数值名称 :EnableDeadGWDetect

项 :Tcpip\Parameters

数值类型 :REG\_DWORD

有效范围 :0，1(False，True)

默认值 :1(True)

下表说明了可以在该注册表值中使用的参数 :

1:将 EnableDeadGWDetect 设置为1时，将允许TCP执行失效网关检测。启用失效网关检测时，如果多个连接出现困难，TCP可能会要求Internet协议(IP)切换到备份网关。可以在“TCP/IP配置”对话框(“控制面板”中的“网络”工具中)的“高级”部分中定义备份网关。

0 :Microsoft建议您将EnableDeadGWDetect值设置为0。如果不将该值设置为0，攻击可能会强制服务器切换网关，而切换到的新网关可能并不是您打算使用的网关。

数值名称 :EnablePMTUDiscovery

项:Tcpip\Parameters

数值类型:REG\_DWORD

有效范围:0，1(False，True)

默认值 :1(True)

下表说明了可以在该注册表值中使用的参数:

1:将 EnablePMTUDiscovery设置为1时，TCP将尝试发现经由远程主机的路径传输的最大传输单位(MTU)或最大数据包大小。通过发现路径的MTU并将TCP段限制到相关值， TCP可以沿着连接具有不同 MTU 的网络的路径删除路由器上的碎片。碎片会对TCP的吞吐量产生不利影响。

0 :Microsoft建议将EnablePMTUDiscovery设置为0。如果这样做，576字节的MTU将应用于本地子网中所有非主机的连接。如果不将该值设置为0，攻击者可能会强制MTU值变得非常小，从而导致堆栈的负荷过大。

值得一提的是，将EnablePMTUDiscovery设置为0将对TCP/IP性能和吞吐量产生负面影响。尽管Microsoft建议使用该设置，也不应使用它，除非用户完全清楚这种性能损失。

数值名称 :KeepAliveTime

项:Tcpip\Parameters

数值类型:REG\_DWORD-时间(以毫秒为单位)

有效范围:1-0xFFFFFFFF

默认值 :7,200,000(两个小时)

该值控制TCP通过发送“保持活动”的数据包来验证空闲连接仍然完好无损的频率。如果仍能连接到远程计算机，该计算机就会对“保持活动”的数据包作出应答。默认情况下， 不发送“保持活动”的数据包。可以使用程序在连接上配置该值。建议将该值设置为 300,000(5 分钟)。

数值名称:NoNameReleaseOnDemand

项 :Netbt\Parameters

数值类型 :REG\_DWORD

有效范围 :0，1(False，True)

默认值 :0(False)

该值确定计算机在收到名称释放请求时是否释放其NetBIOS名称。添加该值的目的是让管理员能够保护计算机免受恶意的名称释放攻击，建议将NoNameReleaseOnDemand值设置为1。

# ii．ABE (attribute-Based Encryption)

基于属性加密（ABE），又称模糊的基于身份的加密（Fuzzy Identity-Based Encryption）。它把身份标识被看做是一系列的属性。IBE中解密者，只有当自己的身份信息和信息加密者描述的信息是一致的时候，才可以解密加密者加密的信息。和IBE不同的是，采用基于属性加密后，当用户拥有的属性超过加密者所描述的预设门槛时，用户是可以解密的。在许多情况下，当用户对敏感数据进行加密时，必须建立一个特定的访问控制策略，以便谁能够解密这些数据。例如，电子科技大学的信息与软件工程学院和计算机科学学院共同撰写了一些技术文档，两个学院想对其进行加密并且能允许自己学院的学生访问，于是可以指定以下访问结构可以访问该信息：（“信息与软件工程学院”AND“在校学生”OR“计算机科学学院”AND“在校学生”OR“电子科技大学计算机教师”）。这样只有这两个学院的学生和学校的计算机教师可以访问该加密文档，其余人则无法访问。

对此可以设计以下方案满足上述需求。

在方案构造中，如果在加密一条明文时使用了属性i，那么如果用户ID拥有属性i所对应的私钥且当ID不在属性i的用户撤销列表中，则可以计算出属性i相关且与该ID的私钥绑定的一个解密信息片段。当且仅当用户所拥有的未被撤销的属性满足密文的访问结构时，用户才能使用这些与其私钥绑定的解密信息片段恢复出明文。ABE方案一般分为四个步骤：setup，KeyGen，Encrypt，Decrypt。

令N=（），G，是阶为N的群，e是G的一个双线性映射。令为G中阶为的子群，g为的生成元；令为G中阶为的子群，Y为的生成元。

**Setup(m,n)**:令属性集合I={1,2,3,…,m}，用户集合U={1,2,3,…,n}。首先，对于任何属性iI，从中随机选取两个元素，计算,;其次，从中随机选取一个元素，对于任意i{1,2,…,n,n+2,…,2n}，计算=；最后，从中随机选取一个元素，并最终发布公钥参数PK为

PK=（N,g,,,,）

系统主私钥MSK为

MSK=（）

其中，用于与属性本身相关的计算，,用于与用户属性撤销相关的计算，，用于与用户身份信息相关的计算，Y用于对用户的私钥进行随机化。

**KeyGen(ID,**):用户IDU,I。首先从中随机选取一个元素t，从中随机选取一个元素，计算=；然后，对于任意i，从中随机选取一个元素，从中随机选取两个元素,，计算:

=

易见，用户私钥中所有与属性相关的部分（即每一个属性所对应的部分）都嵌入了身份信息，将属性i与用户ID相绑定。

令,则最终生成的用户私钥=()

**Encrypt(M,(),)**:首先从中随机选取一个向量=(s,),并计算：

对于A中的每一行,令为A的第行所代表的向量，，=U-，计算：

=

若，即：从中随机选取两个元素,计算：

=

=

=

其中，,,用于对属性撤销信息的随机化，防止潜在的由于敌手直接计算出身份信息无关的的值而导致的合谋攻击；

若，即：直接计算

=

为表述统一起见，此时令==1，即

最终的密文C为

C=（）

**Decrypt()**:首先令L=,则=,假设满足访问结构（）则对于任意,计算

=

令为A中第行所对应的恢复系数，最终恢复明文M

M=

正确性：