利用双标记的 IP 包定位方法

Double – Marks Scheme for IP Packet Locating

李宇波　范冰冰　(华南师范大学 计算机学院 广东 广州 510631)

摘　要：当前 IP 跟踪技术尚处于比较落后的阶段,对一些复杂的攻击无法实现有效定位。文章提出一种新的利用双标记的 IP 包定位方法,该方法有效地回避了现有 TCP/IP 协议存在的缺陷,允许 IP 包的获得者直接查看包中的信息定位其起始地址,而无论其源地址字段是否被伪造。而且由于该方法原理简单,不修改现有网络协议、无需大型硬件设备的投入,因此适用性广、可行性大。

关键词：IP 跟踪 双标记 IP 定位 计算机网络攻击

1　问题的引入

由于历史的原因 IP 协议本身并不能够保证 IP 数据包源地址的可靠性,攻击中经过精心伪造的 IP 包其源地址可以是任意的;而相应的 IP 跟踪技术尚处于比较落后的阶段,对一些复杂的攻击根本无法实现有效定位。

在当前这种现实情况下,社会服务转向网络却成为一种全球趋势。因此研究 IP 跟踪、定位网络攻击的必须性也与日俱增。有效地定位攻击才能更好地阻止攻击,从长远看甚至关系到一个国家的生存和繁荣。定位攻击,从而取证,实施法律诉讼、经济制裁、军事行动等,是对攻击的有效威慑,可以防止攻击的发生。定位也有助于了解攻击技术的细节,有助于防御技术的提升,从而有效阻止未来的类似攻击。有效地定位可以在攻击发生的过程中终止攻击。在攻击进行的过程中发现、定位、阻止甚至终止攻击与在攻击发生后追究责任、统计损失相比更有积极意义。

文章第 2 部分介绍现有主要 IP 跟踪方法的适用范围及其存在的问题;第 3 部分介绍文章提出的新的利用双标记的 IP 定位方法;最后的第 4 部分对文章提出的新方法进行总体评价。

2　现有的方法及存在的问题

众所周知,IP 协议本身对匿名性的相关限制太少。1985 年,Morris 曾在[1]中指出:

"IP 协议存在缺陷:数据包的产生主机自己填充包头源地址字段,并且 TCP/IP 协议并没有提供找到数据包真实源头的机制。"

尽管在由 IP 欺诈相应产生的追踪 IP 包真实发出地址的技术方面,已经有很多相关的理论提了出来,然而在实现方面始终存在一些问题。下面简要地介绍几种目前普遍认为可行性较大的理论的适用范围及其不足:

2.1　逐跳逆向追踪

逐跳逆向追踪是目前最基本最常用的 IP 追踪方法,对正在进行中的 DoS 攻击的追踪效果较好。但是该方法只适用于对大流量、持续数据包流的追踪,且要求是实时的,不能够在事后进行追踪;还需要攻击流所经过的各 ISP 提供合作,假如其中有一个不提供合作则追踪失败;如果攻击在追踪完成之前已结束,追踪同样无法圆满完成。逐跳逆向追踪工作量大,所需的跨 ISP 辖区、司法辖区、国界的合作也往往由于种种原因无法实现;对于 DDoS 这种攻击包由大量的攻击点发出,各攻击点所发出的攻击包相应较少的攻击同样没有实际意义。

2.2　入口过滤器

在 ISP 辖区内的每个边界路由器上安装入口过滤器[2]可以大大减少源地址欺诈 IP 包出现的可能。这种方法似乎很理想,然而会加大 ISP 的投入,而且由攻击者发出的攻击是否应该让 ISP 去检测和避免值得商榷。此外入口过滤器也会使一些网络服务无法实现,如 IP Tunnel,VPN 等。

1.3 后散逆向追踪

后散逆向追踪[3]是当前应用中一种很好的追踪实现方案,主要应用于 DDoS 攻击中。该方法只需对路由器做一些配置,不修改任何路由协议也无任何其它设备要求。利用的是目前多数 DDoS 工具对攻击包源地址字段填充的随机地址中所含的非法地址。很明显这种方法并不能够完全阻止 DDoS 攻击,因为非法 IP 地址只是随机 IP 地址的一部分;同时即使找到了这种包的发出主机也并不表示就找到了攻击的源头,因为 DDoS 攻击包大都由傀儡机发出,即使在后续的过程中递归地利用该方法也并不能够进一步从傀儡机追踪到攻击的幕后控制主机;此外这种追踪方法依赖大流量的攻击包;且只要攻击者对攻击工具的随机 IP 生存算法稍做改进只生成合法 IP 或是不对攻击包的源地址进行伪造,就能够轻易使这种追踪方法失效。

1.4 利用叠层网络

本质上是利用叠层网络[4]优化逐跳逆向追踪,从而简化追踪的过程,节约时间提高成功率。这种方法具有逐跳逆向追踪的不足;另外增加了 ISP 路由器网络的复杂性,路由表更新容易出现错误;而且 IP 管道存在流量瓶颈,在 DoS 发生时叠层网络本身会强化攻击效果。

1.5 利用抽样包

利用抽样包的 IP 追踪方法目前主要应用于以下两种情况。

(1) 生成跟踪包

iTrace[5]要求修改路由器和现有协议,使接受者具备对 iTrace 包的响应能力。只适用利用大流量数据包的攻击;而且攻击者可以通过发送伪造的 iTrace 包影响路径的重构。

(2) 包标记

包标记方案[6,7]类似于 iTrace,与 iTrace 有相似的不足。

另外需要特别指出的是利用抽样包拼接路径的计算量非常大。

1.6 单包 IP 逆向跟踪

单包 IP 逆向跟踪一直是业界的梦想。但存储容量始终是现有单包 IP 逆向跟踪方法无法回避的问题,短暂的存储时间片要求对攻击的发现、响应必须快速和自动化,这就对设备的配备有较高要求,需要较大的资金投入。而且,当对路由器纪录的查询是跨区域甚至是跨国界的时候,相关工作的完成往往需要政治等诸多方面的协调,这是超出技术范畴的,而且当前相关的交涉协议并不完善。

3 利用双标记的 IP 定位

这部分将介绍一种新的利用双标记的 IP 定位方法,这种方法由于原理简单、部署方便,可以有效地运用在当前实际的网络环境中。正如上述:IP 协议存在缺陷,数据包的产生主机自己填充包头源地址字段,并且 TCP/IP 协议并没有提供找到数据包真实源头的机制。这种方法所考虑的正是在利用 IP 包信息定位的同时忽略包源地址字段的真伪。

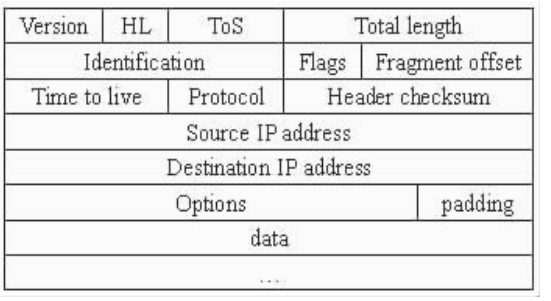


图 1 IP 包的结构

IP 包的结构如上图 1 所示。包头长度字段是 4 个位,可以表示 15 个字段 60 个字节(每个字段四个字节)。所以,根据下面的图 2 所示,可选部分最多可以容纳 10 个字段。本方法考虑利用其中的两个字段分别容纳两个标记,然后利用这两个标记实现 IP 定位。第一个字段的内容为一个 IP 包进入网络时所经过的第一个路由器的入口 IP 地址;第二个字段将陆续被后续所经过的路由器的入口 IP 地址覆盖。

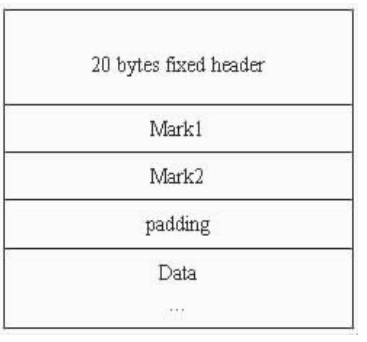
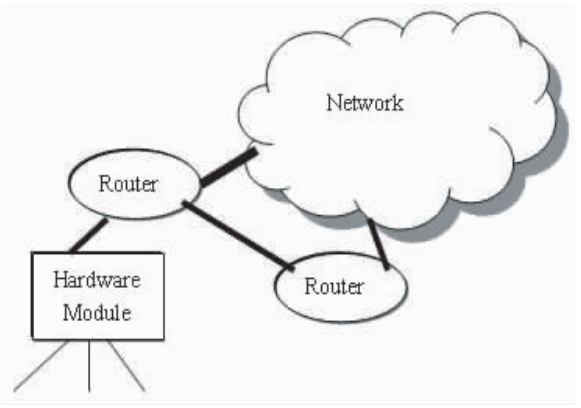


图 2 标记后的 IP 包结构

这种方法考虑利用硬件模块完成相关的所有功能,让每个入口地址拥有全局 IP 的路由器都绑定一个模块,这样既可以不修改现有协议,在设备的投入方面也不需要太大的成本。配备硬件模块后的网络结构模型如下图 3 所示:



注意:只有入口地址具有全局 IP 的路由器才配备该硬件模块

图 3　配备硬件模块后的网络结构模型图

3.1 标记算法

硬件模块对所经过的每个 IP 包的标记过程如下:

```
switch( ){
    case 1: (mark1 || mark2 == NULL)
        mark1 = IP of the entry port of current router;
    case 2: (mark1 != NULL && mark2 == NULL)
        if(mark1 == IP code of the previous router's out – port that connects to this router's this port)
            mark2 = IP of the entry port of current router;
        discard the packet;
    case 3: (mark1 != NULL && mark2 != NULL)
        if(mark2 == IP code of the previous router's out – port that connects to this router's this port)
            mark2 = IP of the entry port of current router;
        discard the packet;
    default: discard the packet;
    break;
}
```

算法要求硬件模块检查每个到达 IP 包的两个标记字段,从实现上来说,这一功能可以通过一个比较电路来完成。比较后会出现以下三种情况之一:

第一种情况:IP 包的两个标记字段都为空。这意味着:

(1)该包是由与模块相连的主机生成(或是中途分包后的子包,后面会做介绍),刚进入网络,此硬件模块是其所经过的第一个模块。此时,模块只需要把自身所捆绑的路由器的相应入口 IP 地址写入第一个标记字段即可。

(2)两个标记字段被蓄意清空。这种情况下模块对第一个标记字段进行标记后,IP 定位只能定位到该路由器端口,完整的定位到发包主机需要后续工作。

第二种清况:IP 包的第一个标记字段非空,第二个字段为空。模块判断包的第一个标记字段是否为上游路由器的相应出口 IP,如果是则把第二个标记字段标记为包当前所经过的路由器的入口 IP 地址;否则弃包。判断过程分两步:

(1)判断上游设备的种类,是路由器还是对包有修改能力的终端主机。

硬件模块并不能够有效完成此判断,技术本身也不能够有效解决这个问题。需要相关政策的辅助,需要相关职能部门政策性地强制对所有具有全局 IP 地址且捆绑有硬件模块的路由器信息进行注册备案,纪录每个此类路由器各端口的 IP 和与其所连接的设备类型;把备案的相关信息配置给硬件模块,让硬件模块具有一个注册表(register),这样硬件模块就能够查询自身的注册表获知当前端口所连接的上游设备是具有全局 IP 的主机还是具有全局 IP 的路由器。

(2)判断标记中的 IP 数据是否与上游端口的 IP 相符。

这就需要模块具有本路由器各端口地址和其所连接的其它路由器相应端口地址的映射表(mapping table),可以通过设计硬件模块查询路由器的路由表实现;由于这些各端口都具有全局 IP 地址的路由器其端口的 IP 地址相对稳定,所以给硬件模块配置映射表这一工作同样可以考虑人工实现,以减少硬件模块的

成本。

第三种情况：IP 包的两个标记字段皆为非空。于是模块需要判断包的第二个标记的内容是否为与本路由器的该端口所连接的上游路由器的相应端口 IP。如果是，则用本端口 IP 覆盖第二个标记字段；不是，则弃包。

如果出现其它情况，模块认为 IP 包为非法包，可能是传输的过程中由于线路的原因出错，或是被恶意修改，模块弃包。

此外，硬件模块应该有修改包头长度和计算包头检验和的电路，在标记完成后重新修改包头的长度值和包头的检验和，使得 IP 包在后续的路径中能够顺利地被转发。

硬件模块的工作原理如下图 4 所示。

由图可以看出，在路由器捆绑有硬件模块的网络环境下，收到数据包的主机可以相信包中的两个标记字段，并利用第一个标记字段的信息得到数据包的发出地址。方法有效地回避了现有 TCP/IP 协议的不足，实现了定位 IP 包发出地址的同时忽略包源地址字段的真伪。

由图可以看出，在路由器捆绑有硬件模块的网络环境下，收到数据包的主机可以相信包中的两个标记字段，并利用第一个标记字段的信息得到数据包的发出地址。方法有效地回避了现有 TCP/IP 协议的不足，实现了定位 IP 包发出地址的同时忽略包源地址字段的真伪。

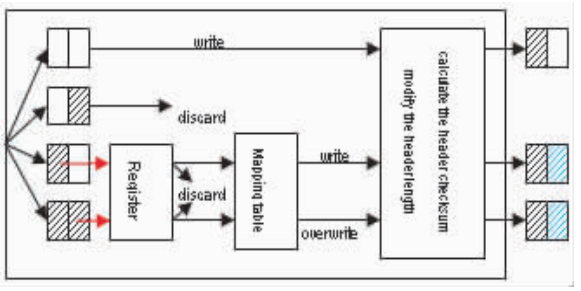


图 4　硬件模块的工作原理图

3.2 分析

算法原理简单易于实现，但在实际的应用中依然存在一些问题待解决以使算法更加完善。

(1) 标记会导致分包

近期的相关统计[9]表明网络流量的分包率小于 0.25%，而且按照本方法的实现原理即使出现分包，分裂出的各子包在中途依然会分别标记，达到目标主机会再次重组，重组后的 IP 包并不影响定位工作。

(2) 标记会增加网络流量

从上面所介绍的现有方法可以明显看出没有任何一种方案不是以增加投入为代价来实现 IP 追踪的，只是投入的形式有所差异，或是增加硬件设施，或是修改软件功能，或是硬、软件两方面同时投入。而且目前网络的发展趋势显示，无论是 IPsec、Mobile IP 还是 IPv6 都无一不增大了 IP 包头的数据量。本方法是以广泛配置功能硬件模块和增加网络流量为代价来实现 IP 定位的，但很明显相对而言投入并不大。此外，如何去评估一个方案的投入应该参考其所实现的功能。

(3) 适用范围

该方法可以定位包的生成点（有些情况下可能只能定位到一个大致网络管理辖区）。算法表明对于大流量直指受攻击者的 DoS、多起点汇聚到受攻击者的 DDoS 都是适用的，而且可以实现单包定位。

(4) 抗攻击性

在 IP 包的始发处：

第一种情况：第一个标记字段被伪造而且第二个标记字段为空。硬件模块会利用其端口映射表判断出异常并弃包。

第二种情况：第一个标记字段被伪造；第二个标记字段被非法填充真实的当前 IP。根据硬件模块工作原理图可知，模块利用数据包的第二个标记检索自身的注册表能够识别出上游设备是主机，因为只有主机才具备修改包的能力，而从主机发过来的数据包的两个标记应该为空，这样模块就可以判断出异常并弃包。

其它异常情况：数据包将被模块视为非法包，根据算法会被丢弃。

在 IP 包被传递的途中：

根据硬件模块所具备的功能，攻击者要在途中截取并修改 IP 包而且使其能够继续被传递，那么唯一的做法是让修改后的 IP 包满足在始发点不被丢弃的条件。这样该 IP 包将被定位在截取点。如何定位包的生成点需要后续递归性的工作。

(5) 改进

必须得说这种利用双标记的 IP 定位方法需要填充 64 位的数据到 IP 包头。由于第一个 32 位标记是用

于全局的 IP 定位,所以出于碰撞率的考虑,并不能够压缩该字段。而第二个 32 位标记字段只是被用于下一跳硬件模块的判断,涉及到 IP 码数量很少,碰撞几率很低,可以考虑利用 Hash 函数进行压缩以减少附加到 IP 包头的数据量,而且相关资料显示如果每个数据包的平均大小是 128 字节,那么每增加一个字节的数据量将减少带宽的 1% ,可见减少包头数据量是很必要的。但是另一个因素必须注意,IP 包头的长度是用字段表示的,要求 IP 包头的长度必须的 4 个字节的倍数,所以单纯地对第二个标记字段进行压缩是没有意义的。有一种考虑是压缩第二个标记字段然后将其填充到包头的片偏移字段中,而这又会影响分包时的定位,因而此时就需要在定位的精确率和包负载二者间进行权衡;同样出于网络负载的考虑,可以让硬件模块对 IP 流进行抽样标记,但是这种考虑是以牺牲单包 IP 定位功能和硬件成本为代价的。

4 总结

文章陈述了当前的网络环境,简要的介绍了现有的主要 IP 追踪方法及其存在的问题,然后给出了这种利用双标记的 IP 包定位方法。该方法可用于 DoS、DDoS,并且可以实现单包 IP 定位。这种方法理想地回避了其它一些依赖存贮包信息所带来的隐私问题;很大程度上减少了跨区域追踪所需要的人力合作,从而大大提高了现有社会环境下 IP 追踪的成功率;最重要的是该方法的基本理念是利用 IP 包信息定位的同时又忽略 IP 包源地址数据的真伪,因而可以应用于 NAT、分包、IP Tunnel 等情况下。然而,不可避免的是该方法仍然存在一些问题有待解决以使功能完善,比如怎样才能在保证定位效果不变的情况下有效减少包负载。

参考文献

1 Morris RT. A Weakness in the 4.2BSD Unix TCP/IP Software. Technical Report Computer Science #117, AT&T Bell Labs, Feb. 1985.

2 Ferguson P, Senie D. RFC 2827: Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing. Network Working Group, IETF.

3 Gemberling B W, Morrow C L, Greene B R. ISP Security - Real World Techniques. Presentation, NANOG, October 2001.

4 Stone R. CenterTrack: An IP Overlay Network for Tracking DoS Floods, 199 - 212. 9th USENIX Security Symposium. Denver, Colorado, August 14 - 17, 2000.

5 Bellovin S, Leech M, Taylor T. ICMP Traceback Messages. Internet Engineering Task Force (IETF) Draft—Work in Progress.

6 Savage S, Wetherall D, Karlin A R, Anderson T. Practical Network Support for IP Traceback, 295 - 306. Proceedings of ACM SIGCOMM 2000. Stockholm, Sweden, Aug. 28 - Sept. 1, 2000. New York: Association for Computing Machinery, 2000.

7 Song D, Perrig A. Advanced and Authenticated Marking Schemes for IP Traceback, IEEE Infocom 2001:878 - 886.

8 Snoeren A, Partridge C, Sanchez L, Jones C, Tchakountio F, Kent S, Strayer T. Hash - Based IP Traceback, 3 - 14. Proceedings of ACM SIGCOMM 2001. San Diego, California, Aug. 27 - 31, 2001. New York: Association for Computing Machinery, 2001.

9 Stoica I, Zhang. H Providing guaranteed services without per flow management. in SIGCOMM'99, 1999:81 - 94.