可避免数据包重复标记的可变概率分片标记算法*

段海霞
(聊城大学 计算机学院,山东 聊城 252059)

摘 要:提出了可避免数据包重复标记的可变概率分片标记算法。通过模拟试验对比该提出的算法和基本包标记算法,结果表明该方法能够消除对数据包的重复标记问题,并显著地减少反向追踪攻击源所需数据包的数目,提高了对攻击源定位的追踪的准确性和实时性。

关键词:重复标记;可变概率;传输距离
中图分类号:TP393 **文献标识码**:A

Non-repeated varying probability packet marking algorithm

DUAN Hai-Xia
(College of Computer Science, Liaocheng University, Liaocheng 252059,China)

Abstract: Non-repeated varying probability packet marking scheme is proposed.The effectiveness of the proposed schemes was calculated through simulation studies. Our studies show that the proposed schemes offer high precision and efficiency , and can dramatically reduce the number of packets that is required for the traceback process.

Key words: repeated marking ; adjusted probability;transmission distance

DoS 是 Denial of Service 的简称,即拒绝服务。造成 DoS 的攻击行为被称为 DoS 攻击,其目的是通过消耗远程计算机网络资源来使 Internet 站点拒绝提供给合法用户的服务。这种类型的攻击实施简单、防御困难、危害极大,攻击者的 IP 地址常常是经过伪装的。针对此类攻击的特点,研究者提出了很多解决方法,例如包标记、日志记录、连接测试、ICMP 追踪、覆盖网络等。本文提出了可避免数据包重复标记的可变概率分片标记算法,减少路径重构时所需的数据包数目以及运算时间,提高了对攻击源定位的追踪的准确性和实时性。

1 相关研究工作

由 Savage 等人提出的概率包标记算法 BPPM,具有许多其他方法所不具有的优点:(1)无需与 ISP 相互合作,避免了调试中高额的管理费用;(2)无需增加巨大的网络流量,可以跟踪多种攻击形式;(3)在攻击停止后很久,仍然可以被用来分析登录过程并制作用于跟踪的数据包。(4)网络路由器负载小。之后在 BPPM 的基础上不断产生出新的改进算法,例如自适应概率包标记、高级包标记和带认证的包标记,以期减少路径重构时所需的数据包,重构攻击路径时的误报率,计算复杂度(时间复杂度)。

概率包标记的思想[1]是路由器以固定的概率 p 标记数据包,将路径信息加入到 IP 头中的 16 bit 识别域(ID)中,表示为(start,end,distance)。在路由器处产生一个[0,1]之间的随机数,如果这个随机数小于 p,路由器将自己的 IP 填入到 start,同时将 distance 赋值为 0;否则将自己的 IP 地址填入到 end 中;如果路由器以概率 $1-p$ 不对包标记,则将 distance 值加 1。受害者从这些数据包中提出路径信息,重构出攻击路径。

假设每个路由器标记数据包的概率为 p,受害者从距离 d(节点与受害者间路由器的个数)的路由器收集到被标记的数据包的概率为 $p(1-p)^{1-d}$。该函数是距离 d 的严格单调递减函数,距离攻击者越远的路由器的样本越难被采集到,因此算法的时间主要集中在接收最远路由器提供样本的时间上。例如,当 d=20、P=1/2 时,受害者要收集到此路由器上的样本必须要收到平均 1 048 576 个数据包。

它最主要的缺点是随着路径的增长,所需要数据包的数量成指数增长,并且存在数据包的重复标记问题,距离攻击者近的被标记的数据包可能被下边的路由器标记,从而

* 山东省教育万科研发展计划(J08LJ20)

掩盖曾经被标记过的信息，这就不可能很快地重构路径防御攻击。

2 改进的包标记算法 NRVPPM

本论文提出一种改进的包标记算法，在包头中增加标记位 flags 来避免数据包的重复标记问题，并且使用等概率 $p=1/d_i$，使受害者主机可等概率地收集到攻击路径中路由器标记的数据包。

2.1 标记概率

设攻击者与受害主机间的距离为 d，即数据包需经过 d 个路由器（依次为 R_1，R_2，…，R_d）从能从攻击者传到受害者主机[2]，路由器 $R_i(i=1,2,\cdots,d)$ 对数据包标记的概率为 p_i^R，受害主机接收到被路由器 R_i 标记过的数据包的概率为 p_i^v，

令 $p_1^v=p_1^R$，$p_2^v=p_2^R(1-p_1^R)$，…，$p_d^v=p_d^R\prod_{1\leqslant i<d}(1-p_i^R)$

$$(d>1)\sum_{1\leqslant i<d}p_i^R=1$$

当 $p_1^v=p_2^v=\cdots=p_d^v$ 时，可得 $P_i^R=1/(d+1-i)$。

2.2 标记格式

为了节省标记存储空间，不给用户带来过多的影响，算法使用 IPv4 中的 16 位标识符字段（Identifer）[1]、1 位闲置的标志位（Flags）、13 位片位移字段（据统计目前少于 0.25%的数据包需要分片）[3]，以及一般很少使用的 8 位 TOS（Type-of-Sevice），总共 38 位来存储包标记信息。标记格式如表 1 所示。

表 1 标记格式

flags	start	end	offset	distanse	hash
2 位	8 位	8 位	2 位	5 位	13 位

把 32 位的 start 路由器的 IP 地址和 32 位 end 路由器地址分为 4 块。在 start 和 end 子域以等概率放置 IP 地址的 4 个 8 位的片段，并相应地设置偏移 offset 子域值。

(1)flgs：如果 flags=0，则表示数据包没有被标记过；flags=1，则 start 子域已被标记过；flags=2，则 start、end 子域均被标记过。flgs 的初始位被置为 0。

(2)start 和 end：用来存储边的信息。

(3)distance：用 5 位的 distance 来记录数据包开始发送的路由器开始经过的跳数。distance 的初始值被置为 0。

(4)offest：用 2 位来记录 start 和 end 的 4 个偏移。

(5)hash：hash(IP)取其后 13 位。

2.3 标记过程

把 32 位的 start 路由器的 IP 地址和 32 位 end 路由器地址分为 4 块，在 start 和 end 子域以等概率放置 IP 地址的 4 个 8 bit 的片段，并相应地设置偏移 offset 子域值。路由器以概率 $p=1/d$ 对数据包 w 进行标记。在路由器 R_i 处，让 x 为[0,1]之间的随机数，y 为[0,3]之间的随机数，如果 $x<p$，(a)当 flags=0 时，则把路由器 R_i 的 IP 地址的第 y 个分片放入 start 域，distance 域置为 0；(b)当 flags=1 时，则表明 start 域已经标记过，把路由器 R_i 的 IP 地址的第 w.offset 个分片放入 end 域，flags 的值加 1。如果 flags=2，则表明数据包 w 的 start、end 域均已经标记过，直接将 distance 的值加 1，转发数据包。

标记算法[4]为：

```
Algorithm1  Marking procedure at router ri
    for each packet w
    let x be a random number from [0,1]
    let y be a random number from [0,3]
    let f be a fragment of ri at offset y
    let h be a fragment of ri at offset w.offset
      if w.TTL>64
        write 64 into w.TTL;
      endif
      p=1/(65-w.TTL);
    if x<p
     if flags=0
       write f into w.start
       write y into w.offset
       write Hash(ri ) into w.hash
       write 0 into w.distance
       else
        if flags=1
          write h into w.end
          flags=2
        endif
     end if
    if flags=2
       increment w.distance
    endif
   endif
  endfor
```

2.4 重构过程

攻击路径重构的目标是建立一棵包含所有攻击路径拓扑信息的树 T，重构的第一步是建立一个只包含根节点 V 的树 T。第二步根据每个节点与受害主机 V 的距离，把采样到的边插入到树的结构之中，离各个攻击源最近的路由器就是树的各个叶子，最后检查整棵树，删去与节点的距离 d 不等于 distance 的节点。该算法参考了参考文献[4]。

重构算法为：

```
Algorithm 2. Reconstruction procedure at v
let T be a tree with root v
let an edge of T be a tuple (start,end,count)
let E be a two dimension array of the tuples
for each packet w
replace the fragment at offset w.offset of
```

E[w.distance][w.hash].start with w.start
Replace the fragment at offset w.offset of
E[W.distance][w.hash].end with w.end
increment E[w.distance][w.hash].count
end for

3 仿真试验

为了测试本文方案的性能，通过模拟实验比较了 2 种方案在路径重构时所需要的数据包的数目，实验数据利用 CAIDA[5](Cooperrative Association for Internet Data Analysis)提供的跟踪路由数据库进行仿真攻击试验，如图 1 所示，选取的攻击路径长度为 1~30，每个长度进行 1 000 次试验取平均值。

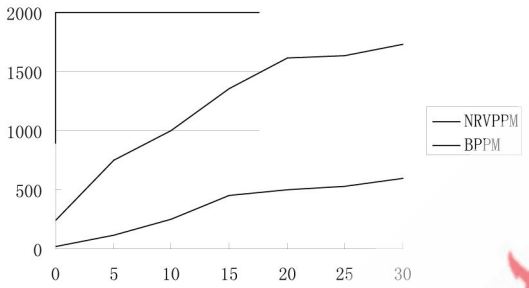

图 1 两种方案重建攻击路径需要的数据包数量

图 1 横坐标为路径长度，纵坐标为重构路径时所需的数据包数目。从图 1 可以看出，在重构路径时，本方案重组攻击路径所需的攻击数据包的数量随着攻击路径长度的增加而增加，但增加的速度却随着路径长度的增加逐渐减小，与传统的标记方法相比，传输路径越长，本方案所需的数据包的个数就越具有优势。因为需要的数据包数量比基本包标记少得多，计算量也会大大减少。所以本方案只需要少量数据包就可以在短时间内重构出攻击路径。

追踪攻击源是打击网络犯罪的必经阶段，它不仅是查找攻击者的重要手段，而且对提供网络犯罪的证据也具有非常重要的作用，所以攻击源追踪技术引起了越来越多的重视。本文提出的算法能够消除对数据包的重复标记问题，并显著地减少反向追踪攻击源所需数据包的数目，提高了对攻击源定位的追踪准确性和实时性。但是要追踪到真正的攻击者，还有许多亟待解决的问题。例如攻击源追踪只能得到可疑攻击路径的集合、只能是近似的回溯、以及如何减少错误路径还需要进一步的研究。

参考文献

[1] SAVAGE S, WETHERALL D,KARLIN A, et al. Network support for IPtraceback[J]. ACM/IEEE Transactions on Networking, 2001,9(3):226-237.

[2] 胡汗平，王凌斐，郭文轩，等.一次性可变概率分片标记及其压缩标记[J].华中科技大学学报:(自然科学版)，2007，35(3):15-18.

[3] RICHARD S W，著.TCP/IP 详解—卷 1：协议[M].范建华，胥光辉，张清，等译.北京：机械工业出版社.2000.

[4] 梁丰，赵建新，DAVID Y.通过自适应随机数据包标记实现实时 IP 回溯[J].软件学报，2003，14(05)：1000-9825.

[5] DAVID M. CAIDA cooperrative association for internet data analysis[EB/OL].http://www.caida.org.2004.

(收稿日期:2009-07-18)

艾默生 Fisher® Control-Disk™ 旋转阀荣获产品创新奖

新型 Fisher®Control-Disk™ 阀门于 2009 年度在美国流体控制(Flow Control)杂志流体控制产品创新评选活动中荣获了产品创新奖，这标志着 Fisher 阀门技术在该行业的客户认可度中又实现了新的突破。

流体控制杂志社每年举办一次流体控制创新产品评选活动，获奖厂家由流体控制杂志的读者投票决定。创新奖授予该年度在流体控制技术方面具有卓越成效和创新技术的产品。2009 年该奖项的投票达 1300 张，是流体控制杂志社 12 年来投票的新高。

艾默生 Fisher®Control-Disk™ 阀门凭借优良的性能在 40 多个参选产品中脱颖而出，以选票数第二获得产品创新奖。新型 Control-Disk 阀门具有良好的调节性能，是快速响应和压降多变工况的理想之选，例如：碳氢、冶金、化工、纸浆和造纸及金属和采矿工业。Control-Disk 阀门的调节范围是传统蝶阀的两倍，而且其控制更加接近设定点。这一改良性能使其在不受过程干扰影响的情况下使控制参数更加接近目标设定点，从而减少过程变量。Control-Disk 阀门性能可靠且维修成本低，适用范围广，特别是当它配备了 Fisher 弹簧和膜片式执行机构及 FIELDVUE® 数字式阀门定位器时，性能更佳。该组件可以获取并发送诊断数据到 AMS®ValveLink® 软件，提供精确的阀门、执行机构及数字式阀门控制器性能参数。这使它成为 PlantWeb® 数字化工厂架构的核心组成部分。

投票人评论说："Control-Disk 阀门可以在保持现有管道的情况下，为传统蝶阀的多种控制问题提供成本合理的解决方案。"

(艾默生过程控制供稿)