面向协同模型的安全追踪研究

张静 丁伟

（东南大学 计算机系，210096 南京）

【摘要】本文结合当前国内外相关领域的研究成果，讨论了面向协同模型的安全追踪问题。在此基础上给出了一个分布式的安全追踪系统的设计和实现过程，其中包括对错误的处理方法等细节问题的讨论。该系统的实现有助于提高网络管理者对攻击者的反向追踪能力，并为以后的决策提供线索和信息。

【关键词】计算机网络；网络入侵检测；安全追踪；协同；

中图分类号：TP393

Research Of Cooperation-Oriented Incident Tracking

ZhangJing， DingWei

(Southeast University, Computer Science Dept., 210096 NanJing, P.R.China)

【Abstract】The paper mainly focus on the research of distributed cooperation-oriented incident tracking. It provides the design and implementation method of a tracking system, and also talks about some detailed issues such as the way for fixing errors in the system. This system can improve the ability of network administrator to track hackers and provide information and clues to later decision.

【Key words】Computer Network；Intrusion Detection System(IDS)；Incident Tracking；cooperation。

1. 引言

安全追踪是保障系统安全的重要手段之一，它通过入侵者进行非法活动时在入侵检测系统中留下的记录和入侵检测系统（IDS）进行综合分析和决策后形成的事件报告中的有用信息，如入侵者的 IP 地址等，为起点来对入侵者进行反向的追踪，获得与攻击源相关的信息，如攻击者所在的具体网络、所使用的主机，以及在攻击的过程中成为攻击者“跳板”的网络路由等。这样使网络的管理者能够掌握攻击者的来源和信息，清楚自己的网络正在被哪里攻击，从而采取相应的措施，如加强对成为攻击源网络所发报文的信息过滤，关闭相应的路由，或者在网络遭受损失后，以此为证据向攻击源索赔，提出警告等。

在互联网环境中，子网间相互渗透和交叉，当其中的一个被攻破时，与之相连的邻居网络也面临被攻破的危险，此时只依靠单一的入侵检测系统已经不能满足保护网络安全的需要，各个网络入侵检测系统之间的协同作战才能应对这样的局面。

在网络入侵检测系统中引入分布协同机制后，安全追踪也有了更多的发挥余地，形成了分布式的系统。首先由协同决策系统根据安全事件的紧急程度和重要程度，决定一个安全事件是否要进行追踪。如果需要追踪，通过各个协同站点的合作，可以更加精确地追溯到事件的源头，避免攻击者在报文中加入的假源地址产生的错误信息对网络管理者的决策造成影响。同时在协同的过程中，通过追踪功能也可以掌握协同站点的工作情况，一旦协同站点工作效率低下或出现错误，可以远程的及时发现，减小由此带来的损失。为了表述方便，本文将进行协同决策和发起安全追踪的结点称为“监测点”，将参与协同的结点称为“协同点”。

2. 安全追踪系统的设计

本文中所讨论的安全追踪系统由四个部分组成：源点网络定位、源点主机名称查询、源点路径定位、安全追踪协同。它们之间的关系如图 1 所示。其中在系统最顶层的是协同决策系统，它负责决定对一个安全事件是否进行追踪。事实上，协同决策系统处于安全追踪系统之外，因此不在本文的讨论范围之内。此外：

- 源点网络定位的功能是确定攻击源 IP 地址所在的网络，得到其大致属于互联网的哪个区域，属于哪个公司、

[1]作者简介： 张静，硕士研究生，主要研究方向为网络安全。丁伟，工学博士，东南大学计算机系教授。

组织，或是学校和服务商所有。对攻击源进行初步的定位。

- 源点主机名称查询的功能是查询攻击源 IP 地址从属的主机。从而得到进一步关于该地址的信息。
- 源点路径定位的功能是反向追溯从攻击源到攻击目标所经过的路由，它使管理者能够掌握攻击报文到达本网络所经过的具体路径，从而对网络安全性作出评估。该功能的反向追溯范围受到网络中防火墙政策的限制。
- 安全追踪协同：监测点向各个协同点发出协同请求，以证实某个协同点是否检测到某个安全事件，直至追踪到最后一个“看到”该安全事件的协同点，通过判断这个协同点所连接的网络区域来证实攻击源确切来自某个监测区域，并可以在整个协同点的分布拓扑图上绘制出详细的攻击经过的路径。该功能需要有协同点的支持，设计的目标是实现完全分布式的思想，由单点追踪提升为多点、协同的追踪。

以上的四个子系统功能各有侧重，可以满足管理者对攻击源进行追踪的不同需要，进行不同粒度范围的追踪。

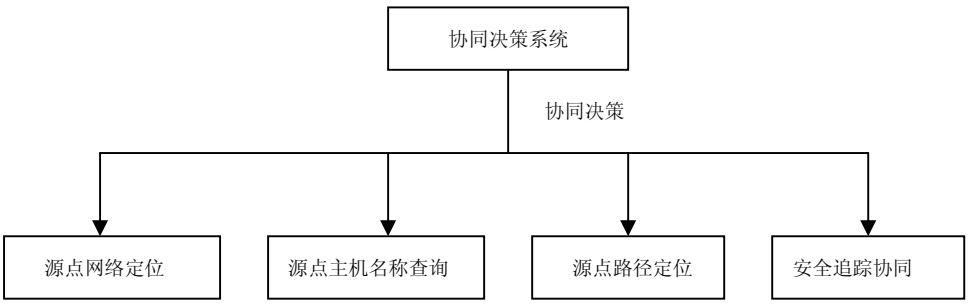

图 1 安全协同系统结构

3. 安全追踪系统的实现

3.1 源点网络定位

该功能的实现是通过检索 whois 数据库来得到某个 IP 地址所对应的网络范围。在 whois 数据库中存储有大量 IP 地址及其对应的网络信息，该数据库可以自己配置，也可借助在世界范围内的三个著名的 whois 数据库：whois.apnic.net(负责亚太地区)、whois.arin.net(负责美洲地区)、www.ripe.net（负责欧洲地区）。

本系统采用的实现方式是首先配置一个“管区数据库”，库中预先存储所有管区的网络地址以及一些著名网络、公司、教育机构、政府机构等的地址。在进行检索时首先在管区数据库中查找，如果数据库中没有相应的信息，则按照上述顺序分别和三个著名的 whois 数据库建立网络连接，通过它们的数据库进行检索。这样做的目的是为了加快查找速度，因为从建立网络连接到收到应答的过程是比较慢的，而查找本地的数据库的速度要快很多，从而可以缩短平均查找时间。

3.2 源点主机名称查询

Unix 系统中的 nslookup 命令提供了查询 IP 地址所对应主机名称的功能，源点主机名称查询就建立在这个系统功能之上，相当于是起到一个域名反向解析的作用。启动该功能后，程序首先询问最近一级的 DNS 服务器，如果在服务器中没有相应的信息，则继续向上一级的 DNS 询问，如此反复，直至获得查询成功或失败的信息。

3.3 源点路径定位

该功能实现的核心是 Unix 系统中的 traceroute 功能，它提供了对一个报文的源网络地址进行反向追踪的功能，并详细地记录每一跳所经过地路由器的 IP 地址，直至到达报文的源。源点路径定位的实现与本网络防火墙的安全政策以及路由器的配置有很大关系，如果对该功能是禁止的，或者在边界路由器上出了问题，都有可能导致不能完整追溯到地址的源头。

3.4 安全追踪协同

这是整个安全追踪系统中最重要的部分，它负责的区域与前三个功能不同，是分布式 IDS 所监控的网络范围，而在此范围之外，则不能提供详细的追踪信息。

支持这个系统的基础是分布式的入侵检测系统（IDS）。因此安全追踪协同也是一个分布式的概念。在每个监测网络之间均设置有 IDS 的监测器，它们之间可以进行信息交互以完成协同功能，安全追踪的协同就建立在 IDS 协同的基础之上，分布在一个监测点之上的安全追踪协同程序通过与其它监测点的交互来进行逐级的追踪，最终在所

有监测点范围内的拓扑图上形成一个攻击报文经过的完整路径。而且每一个监测点都可以独立地发起追踪工作，并得到其它监测点的响应支持，形成一个完全分布式的追踪系统。

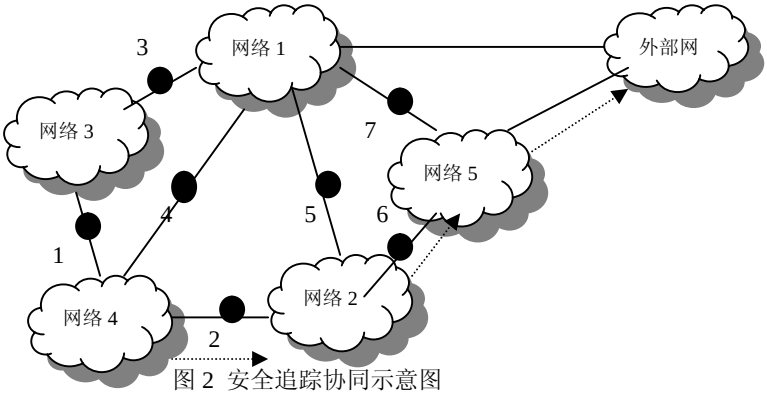

图 2 安全追踪协同示意图

图中黑点的部分表示分布式的 IDS，它们的监控范围为网络 1 至 5。为了讨论方便，将它们按顺序编号。如图所示，在所有网络的连接处都分布有 IDS。而外部网则不在监控范围之内。

在所有分布的 IDS 上都运行着协同守护进程，它负责接收其邻居监测点发出的协同请求，并将结果返回给发出协同请求的监测点。

如果一个来自外部网的攻击经过网络 5、网络 2，最终到达它的目的地：网络 4。那么 2 号，6 号监测点在正常工作的情况下都应该记录到这个攻击行为。为了避免每个记录到该攻击行为的监测点都发出协同请求，产生大量的报文使网络拥塞，因此规定由最靠近攻击目标的那个监测点来负责这个任务。这样监测点 2 将向它的邻居监测点发出协同请求，其它监测点此时都成为协同点。这时协同点 5 号和 6 号都会收到 2 号发出的协同请求，其中 6 号会返回“证实”信息，即表明它记录到了这个攻击行为，而 5 号则返回“证否”信息，表明它没有看到该攻击行为。根据拓扑图可以知道，6 号协同点的邻居是 7 号，2 号在收到 6 号的“证实”信息后，继续发送协同请求给 6 号的邻居，得到 7 号返回的“证否”信息。因此可以得出结论，攻击行为来自于外部网，而非在监测范围之内。

整个算法的基本思想是采用递归的方式，既首先由一点出发，向它的所有邻居发送协同请求，在收到某个邻居（第一层邻居）的“证实”信息后，根据预先存储的拓扑图得到与该邻居相邻的所有“第二层”邻居，再向这些点发出协同请求。以此类推，直至一个点的所有邻居都返回“证否”信息，可知该点就是第一个看到攻击行为的点，而与之相连的网络就是攻击源所在的具体位置。

为了防止在协同过程中出现报文丢失而导致错误的结论，当一个点的所有邻居都返回“证否”信息时，则再向这些邻居的邻居点发出协同请求。如仍收不到“证实”信息，则可以确定没有错误发生；如果有“证实”信息返回，则以返回“证实”信息的点为新的邻居，继续追踪过程。在这个过程中需要记录下所有已经返回“证实”信息的点，并在以后的协同中剔除它们，以防止出现一个点的第二层邻居是自己的情况，使协同过程出现死循环。

拓扑图的存储表示采用的数据结构是集合，既把一个点的所有邻居看作一个集合。当然也可以采用图论的方式，用适当的数据结构（例如邻接表，矩阵）表示。

4. 结论

安全追踪的功能为网络管理者提供了一个对攻击者进行反向追踪的工具，使他们能够掌握有关攻击源的信息以及攻击报文经过的详细路径，因而可以更好地进行安全决策，对攻击者的行为和来源作到“心中有数”。而具备这样功能的 IDS 也使攻击者害怕暴露自己的真实位置，从而收敛自己的行为。

在分布式的 IDS 之上，安全追踪功能也体现了分布式的特点，通过多个监测点的共同参与，使追踪的范围和精确度都较单一系统有明显提高。

分布式安全追踪的功能不会仅局限于这几个方面，随着网络安全研究的不断深入，它在 IDS 中的地位也会不断提高，许多方面仍有待于我们进行进一步的研究。

5. 参考文献（略）