一种通用的互联网追踪溯源技术框架①

陈周国, 蒲 石, 祝世雄

(保密通信重点实验室, 成都 610041)

摘 要: 近年来, 应对网络威胁, 学术界提出并发展了网络追踪溯源技术, 产生了多种追踪溯源技术体制; 然而, 多数追踪溯源的技术研究主要集中在具体的溯源技术及算法上, 对网络追踪溯源的技术框架研究较少. 文章从协作网域和非协作网域两个方面分析追踪溯源技术, 提出非协作网域追踪溯源体制, 设计一种通用的互联网追踪溯源技术框架, 将多种有效的追踪溯源技术或方法统一在该框架中, 发挥各种的溯源技术的优势, 实现全球互联网空间的追踪溯源能力, 提高网络安全防护的主动性和有效性.

关键词: 追踪溯源; 协作追踪溯源; 非协作追踪溯源; 追踪溯源技术框架

General Traceback Technical Framework for Internet

CHEN Zhou-Guo, PU Shi, ZHU Shi-Xiong

(Science and Technology on Communication Security Laboratory, Chengdu 610041, China)

Abstract: In recent years, to deal with cyber threats, in academic community the traceback is proposed and developed, and a variety of traceback technology is researched. However, the majority of these research focuses on the specific traceability technology and algorithms, and traceback technical framework is lessly done. This articles from two aspects of collaboration domain and non-collaboration domain analysis the traceback technology, to track traceability system proposed non-cooperative domain, design a general traceback technical framework for Internet, which involve various traceback techniques or methods and play all kinds of technology advantages, realize traceback in the global Internet space, improve network security initiative and effectiveness.

Key words: traceback; cooperative traceback; non-cooperative traceback; traceback technical framework

我国经济社会对网络基础设施的依赖性逐年增强. 在各种层出不穷的新兴技术及应用的推动下, 互联网及其应用发展迅速, 网络已成为人们日常生活中不可缺少的一部分, 其安全性受到了更为广泛的关注和重视. 互联网的发展是以容易使用和便于共享为基础的, 软件友好, 为此却增加了网络的脆弱性. 随着网络黑客技术工具化、普及化的发展趋势, 基于网络的入侵事件愈发频繁, 越来越多潜在的犯罪份子将网络入侵作为获利手段, 给网络社会带来了巨大的安全威胁. 同时, 网络泄密和利用网络恶意煽动、扭曲事实给国家和社会健康发展带来了更为严重的安全隐忧, 网络安全管理面临巨大的挑战.

一般来说, 网络攻击者在攻击过程中, 总是使用伪造 IP 地址等技术隐藏自身, 逃避追踪, 使得防御方难于确定其源头, 而不能实施有针对性的防御反制策略, 更不能将其绳之以法, 追究其责任.

1 网络追踪溯源

网络追踪溯源是指确定网络攻击者身份或位置及其中间介质的过程. 身份指攻击者名字、帐号或与之有关系的类似信息; 位置包括其地理位置或虚拟地址, 如 IP 地址、MAC 地址等. 追踪溯源过程还能够提供其他辅助信息, 比如攻击路径和攻击时序等. 网络管理者可使用追踪溯源技术定位真正的攻击源, 以采取多种安全策略和手段, 从源头抑制, 防止网络攻击带来更大破坏, 并记录攻击过程, 为司法取证提供必要的

① 收稿时间:2011-12-26;收到修改稿时间:2012-02-29

信息支撑. 在网络中应用追踪溯源我们可以[1]:

① 确定攻击源, 制定实施针对性的防御策略;

② 确定攻击源, 采取拦截、隔离等手段, 减轻损害, 保证网络平稳健康的运行;

③ 确定攻击源, 记录攻击过程, 为司法取证提供有力证据.

当前各种网络追踪溯源技术的有效性都与网络及其网络运营商的密切配合相关, 使用网络运营商提供的数据信息或者在其允许下部署相应溯源设备都能较好的完成追踪溯源. 考虑全球互联网空间, 根据网络或网络运营商的配合程度, 我们可以将网络空间分为可控网域和非可控网域. 可控网域是指用户能够通过管理技术或行政命令等手段实施控制的网域, 与之相反非可控网域就是指用户不能上述手段实施管理控制的网域. 由于可控网域与非可控网域为追踪溯源提供的信息与辅助程度截然不同, 据此, 我们将网络追踪溯源分为协作网域追踪溯源和非协作网域追踪溯源.

2 协作网域追踪溯源

2.1 问题描述

考虑网络通信, 终端 P1 产生网络数据 S, 通过 R1->R2 等一系列中间介质传输到接收端 P2, 如下图所示. 协作网域追踪溯源问题可描述为, 在一个可控的网域中, 给定 S, 如何确定 P1.

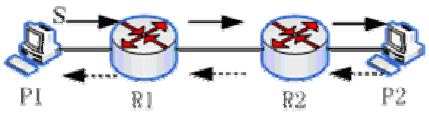

图 1 协作网域追踪溯源问题模型

由于追踪溯源在可控网域中, 因此能够通过行政或网络管理等技术手段, 从网络提供商(ISP)那里获取网络拓扑、路由、IP 地址分配等信息; 或者在其允许下部署相应设备主动采集或标记网络路径信息. 通过对这些信息数据的分析处理, 还原数据传输信息, 重构其路径, 达到追踪溯源之目的. 目前, 协作网域的追踪溯源技术研究较为成熟, 形成了不同的技术路线, 主要有输入调试、日志、包标记等技术方法.

2.2 输入调试技术(Input Debugging)

此种技术方法是通过带有 input debugging 功能的路由器进行一级一级的查询追踪. 目前该技术在可控的网络中已得到应用. ISP 通过设备升级改造或安装支持查询追踪的路由器, 提高追踪效率及能力. 但是此技术的效率比较低, 需要在攻击发生时人工操作实施, 需要大量的人力及各网络提供商之间的配合, 且无法满足事后追踪要求. 系统原理[2]如下图所示:

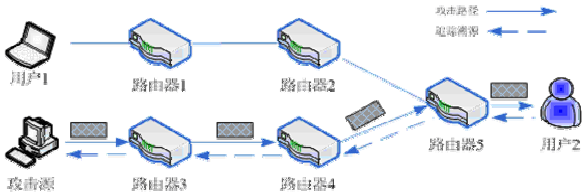

图 2 Input debugging 原理示意图

2.3 日志类(Logging)

日志类使用具有日志记录功能的路由器或在网络中部署日志记录设备, 记录网络传输的数据, 包括其源、目的地址及载荷等信息, 这些日志信息存储在路由器或特定的数据库中. 在攻击发生时或者攻击发生后, 由追踪者根据攻击数据包特性与数据库存储的某路由节点日志信息分析比较, 如果匹配, 表明攻击数据流经该节点, 如此一级一级的追踪. 此方法由于记录存储了网络数据包信息, 因此可以进行事后追踪溯源, 但却占用路由器大量的资源(处理、存储)并需要额外的数据库支持. 然而基于 HASH[3,4]算法的日志类方法极大的减少了存储空间, 是一种很有实用价值的方案. 日志类技术原理如下图所示:

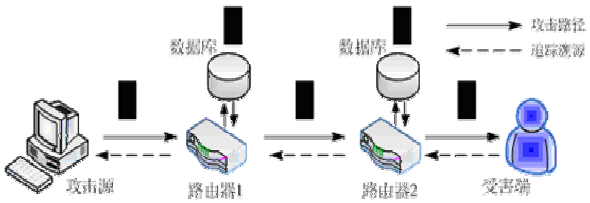

图 3 Logging 技术原理示意图

2.4 包标记技术(Packet Marking)

包标记是指网络中的路由器或部署的特定设备以一定概率(为减少网络处理量, 一般选取的概率为 1/20000)对通过的数据包标记, 将路径信息标记在 IP 数据包预留的字段. 受害者端接收到被标记处理的数据包, 通过路径重构算法, 重构其路径. 与前述的方法相比, 包标记具有一定的优势, 其不需要 ISP 配合(需改造路由器或部署特殊设备), 也不需要大量的人力资源等. 具有代表性的有概率包标记法(PPM[5])、确

定概率报标记(DPM[6])和自适应概率包标记法(APPM[7]). 其原理示意图如下图所示:

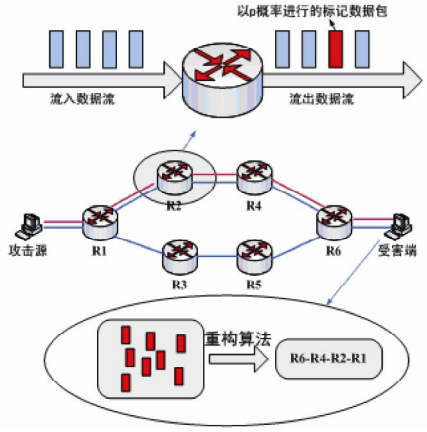

图 4　Packet Marking 技术原理示意图

综上分析, 在可控网域中, 与网络运营商协作配合, 获取信息数据, 改造网络设备, 部署相应的溯源设备. 通过分析处理能够满足网络追踪溯源要求, 重构攻击路径, 完成追踪溯源. 在实际使用中采用何种协作网域溯源技术, 则需要综合评估网络负载, ISP 配合与否等多种因素[8], 如下表所示, 择优选取.

表 1　协作网域追踪溯源技术比较表

技术类别	网络负载	路由负载	是否需要ISP配合支持	计算量	人力资源
输入调试	低	高	需要	低	高
日志类	低	高	部署设备	中	中
包标记	低	低	部署设备	高	低

3　非协作网域追踪溯源

3.1　问题描述

从协作网域追踪溯源技术可以看到, 网络追踪溯源的主旨思想是对网络数据信息进行记录分析, 通过分析实现网络路径的重构. 这些网络数据信息可从两个渠道获取: (1)与网络营运商协作, 由其直接提供(2)在网络营运商的许可下, 部署相应设备, 按需采集或记录信息. 显然, 这些手段在协作网域中都能较为容易的实现, 从而有效实施追踪溯源. 然而, 这些有用信息在非协作网域中却难以获得.

在全球互联网空间, 不可能获得每个网域营运商的协作或者被允许部署设备, 全球范围追踪溯源的实施受到极大限制. 而另一方面, 攻击者又总是能够在一个广泛的网络空间中发起大规模的网络攻击, 通过第三方或非可控的网域发起攻击, 如下图所示(以 DDOS 为例), 图中的网络区域 1、2、3 可能属于不同的国家或第三方机构, 由于各种因素(政治、安全等)限制, 这些网域不提供任何信息, 而导致追踪过程的中断, 不能溯源定位真正的攻击源. 对此, 我们需研究在非可控网域的追踪溯源技术[9], 满足全球互联网空间的追踪溯源需求.

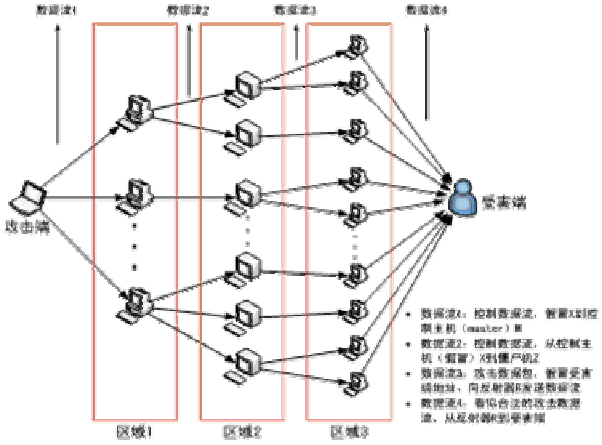

图 5　跨网域攻击模型示意

3.2　基于网络信息主动感知的非协作追踪溯源技术

为了在非可控网域中有效实施追踪溯源, 必先解决非可控网络的信息获取问题, 以支撑非协作网域的追踪溯源. 我们提出基于网络信息主动感知的非协作追踪溯源技术, 通过对非可控网域的信息主动探知获取相应信息, 其功能框图如下所示. 在非可控网域的网络感知为追踪溯源模块提供信息支撑. 比如网络拓扑主动发现能够生成非可控网络的整体拓扑, 从而可实施可控 DoS 技术追踪[10], 或者有的放矢的采集监测数据流, 分析网络链路信息等.

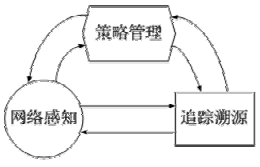

图 6　网络信息主动感知的追踪溯源原理

网络信息主动感知的非协作追踪溯源技术包含信息探知及溯源两方面的能力, 主要功能模块包括网络感知、追踪溯源和策略管理. 利用拓扑主动发

现、网络扫描、渗透等网络主动感知技术在非协作网域中实施信息获取. 追踪溯源模块对网络感知获取的信息进行分析处理, 重构数据传输路径, 并将分析结果与网络感知和策略管理模块进行交互, 以调整相应系统运作策略和感知内容. 网络感知、追踪溯源、策略管理三个功能模块是相互交织联动的统一体, 通过持续不断的分析处理, 重构非协作网域攻击数据流路径等信息, 实现非协作网域的追踪溯源能力.

3.2.1 网络感知

网络感知是一种分布式的架构, 由多个感知节点组成. 综合使用多种技术, 完成扫描、探测和信息收集, 分析汇聚成追踪溯源所需的基础信息. 网络感知与分析评估、追踪溯源交互信息, 根据分析评估和追踪溯源的实际需求, 动态调整其探知内容和目标.

3.2.2 追踪溯源

追踪溯源通过特殊的路径重构算法及链路检测等技术对网络感知汇聚的信息进行深度分析处理, 如网络数据流相关性分析处理. 在网络感知模块获取信息基础上, 可综合采用可控 DoS 和网络流分析技术, 对攻击行为进行追踪.

可控 DoS 技术, 是 Burch 等人在 2000 年提出的一种用于追踪溯源的链路检测技术[10]. 该技术的最大优势就是不需要 ISP 的任何配合, 然而其本身却是一种网络攻击. 设计思想是在攻击发生时, 通过对受害端上一级的网络链路进行 DOS 攻击测试, 如果对某一条链路进行可控 DOS 时, 受害端的网络攻击数据量明显的减少, 则判定该链路是攻击链路. 如此, 一级一级的回溯, 完成追踪. 网络感知模块可提供非可控网域较为详细的网络拓扑等信息, 因此可以利用可控 DoS 技术对特定链路进行测试.

网络流分析技术是在非协作网域中主动获取必要数据进行分析检测, 识别网络数据传输链路. 该技术在学术界获得了极大的关注. 如果网络数据传输没有加密, 可通过内容相关分析, 确定网络节点的进出端口. Staniford 等人是此类技术的最早提出者[11]. 如果网络数据传输采取加密机制保护, 仍可以通过时间信息的相关分析, 确定其链路关系. 通常, 网络攻击跳板间通信都采用加密机制保护, 然而攻击跳板链路通信数据却具有较高的时间相关性. Zhang 等人是时间相关分析技术的最早提出者[11].

3.2.3 策略管理

策略管理负责实时调整网络感知和追踪溯源策略, 根据追踪溯源的具体需求, 对网络感知的精度和内容进行调整, 使其按需提供相应信息.

3.3 一种通用网络追踪溯源技术框架

结合协作与非协作追踪溯源原理, 设计提出一种通用的网络追踪溯源技术框架, 由协作网域、非协作网域追踪溯源和溯源控制系统组成, 如图 7 所示.

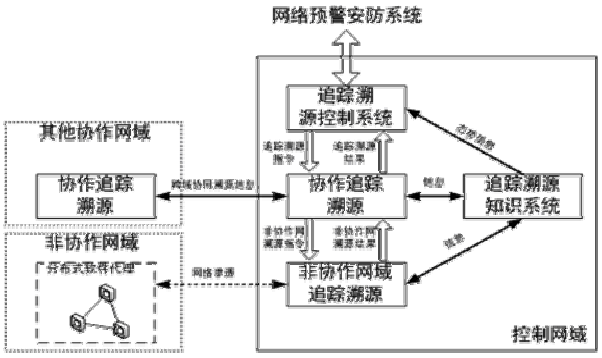

图 7 通用的网络追踪溯源技术框架

通过在可控网域部署相应的溯源设备, 完成协作网域的追踪溯源任务. 一旦追踪到可控网域边界, 则根据攻击数据入口信息确定可能的非可控网域, 进而采取网络信息主动感知的追踪溯源技术, 对非可控网域的攻击路径进行分析重构, 从而实现在全球网络空间中的追踪溯源.

协作追踪溯源分系统将包含多种网络追踪溯源技术, 互为补充. 根据具体的攻击行为, 智能选取最优溯源技术及策略完成追踪.

实施非协作追踪溯源时, 需要考虑网络感知(主动拓扑发现、渗透等)带来的不利影响. 网络感知说到底, 也是某种程度上的网络攻击行为. 因此使用网络主动感知的非协作追踪溯源, 一方面可能被攻击者察觉而采取更为谨慎的措施反制追踪定位, 另一方面还可能因为非可控网域的抵制抗议而牵涉到经济、法律, 甚至国家政治、外交等方面的问题.

4 总结

网络追踪溯源技术是网络对抗中的关键技术之一, 是网络管理、防范网络犯罪的有效方法. 使用追踪溯源可以及时确定网络攻击源, 制定有针对性的防御策

略, 提高网络主动防御的能力, 威慑潜在的网络攻击行为. 设计通用化的网络追踪溯源技术框架可以在更加广泛的网络空间中应用追踪溯源技术, 更好地维护互联网健康发展.

后续还需深入研究非协作网域追踪溯源技术, 提高其精准性和实用性, 降低其实现复杂度; 同时, 考虑其隐蔽性; 进一步验证并完善非协作追踪溯源整体框架.

参考文献

1 彭丹,史志才,陶龙明,马武.IP 追踪技术研究.大连大学学报, 2008,29(3):61−66.

2 Savage S, Wetherall D, Karlin A, Anderson T. Practical Network Support for IP Traceback. Department of Computer Science and Engineering University of Washington Seattle, WA, USA,2000.

3 Snoeren AC, Partridge C, Sanchez LA, Jones CE, Tchakountio F, Kent ST, Strayer WT. Hash-Based IP Traceback:BBN Technologies10 Moulton Street, Cambridge, MA 02138,2001.

4 Strayer TW, Jones CE, Tchakountio F, Snoeren AC, Schwartz B, Clements RC, Condell M, Partridge C. Traceback of Single IP Packets Using SPIE, BBN Technologies10 Moulton Street, Cambridge, MA 02138. Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'03), 2003.

5 Goodrich MT. Efficient Packet Marking for Large-Scale IP Traceback, Department of Info. & Computer Science, University of California, 2002.

6 Belenky A, Ansari N. IP Traceback With Deterministic Packet Marking. IEEE Commun. Lett.,2003,7(4):162−164.

7 Rizvi B, Fermandez-Gaucherand E. Analysis of Adjusted Probabilistic Packet Marking, IEEE, IPOM2003, 2003,9−13.

8 Kuznetsov V, Simkin A, Sandstrom H. An evaluation of different IP traceback approaches. Department of Computer Science and Electrical Engineering Lulea University of Technology, SE-971 87 Lulea, Sweden, 2003.

9 Cohen D, Narayanaswamy K. Attack Attribution in N-on-Cooperative Networks, 2004.

10 Burch H, Cheswick B. Tracing Anonymous Packets to Their Approximate Source. Proc. of the 14th Conf. Systems Administration, Usenix Assoc.,2000,313-322.

11 Staniford-Chen S, Heberlein LT. Holding Intruders Accountable on the Internet. http://seclab.cs.ucdavis.edu/papers/thumb.ieee95.pdf. from proceedings of the 1995 IEEE Symposium on Security and Privacy ,1995.

12 Zhang Y, Paxson V. Detecting Stepping Stones. http://www.usenix.org/publications/library/proceedings/sec2000/full_papers/zhangstepping/zhangstepping.pdf. 9th USENIX Security Symposium, Denver, Colorado. August 14−17, 2000.

(上接第 201 页)

式与系统设计.吉林工业大学自然科学学报,1999,29(95):67−72.

3 Gastaldo P, Zunino R. Hausdorff distance for target detection. Proc. of the 2002 IEEE International Symposium on Circuits and Systems, 2002,5:661−664.

4 雷松泽,姚红革,郝重阳,齐敏.利用 Hausdorff 距离的快速人耳检测.西安工业大学学报,2008,28(3):249−253.

5 陶杰,毕笃彦,吉彦军.一种基于 Hausdorff 距离的目标跟踪算法.微计算机信息,2009,25(2):233−235.

6 Jialing C, James CHC, et al. CT and PET lung image registration and fusion inradiotherapy treatment planning using the chamfer-matching method. Int'l J.Radiation Oncology Biol. Phys, March 1999,43(4):883−891.