基于应用运行时自保护的网络攻击溯源方法

Cyber Attack Attribution Method Based on RASP

蓝鑫冲[1,2]，郭新海[1,2]，刘　安[1,2]，丁　攀[1,2]，王　戈[1,2]（1. 中国联通研究院，北京 100048；2. 下一代互联网宽带业务应用国家工程研究中心，北京 100048）

Lan Xinchong[1,2], Guo Xinhai[1,2], Liu An[1,2], Ding Pan[1,2], Wang Ge[1,2]（1. China Unicom Research Institute, Beijing 100048, China; 2. Next Generation Internet Broadband Service Application National Engineering Research Center, Beijing 100048, China）

摘　要：

近年来，以高级持续性威胁（APT）为代表的高级网络攻击已经对政府、能源、金融、通信等诸多领域造成了巨大的影响。因此，开展网络攻击溯源技术的研究实现对高级网络攻击溯源成为网络安全领域的重要研究方向。介绍了基于应用运行时自保护技术（Runtime application self-protection，RASP）的网络攻击溯源方法，通过生成综合指纹标识网络攻击者，提高网络攻击溯源的准确性。

关键词：

应用运行时自保护；网络攻击；溯源；综合指纹

doi：10.12045/j.issn.1007-3043.2023.08.005

文章编号：1007-3043（2023）08-0019-05

中图分类号：TN915.08

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

In recent years, cyber attacks represented by APT (Advanced Persistent Threat) have had a huge impact on many fields such as government, industrial systems, finance, telecommunications, and so on. Therefore, the attribution technology of cyber attacks has become an important research direction in the field of network security. It introduces a cyber attack attribution method based on Runtime application self-protection (RASP) technology, which improves the accuracy of cyber attack attribution by generating comprehensive fingerprint identification of cyber attackers.

Keywords：

RASP; Cyber attack; Attribution; Comprehensive fingerprint

引用格式：蓝鑫冲，郭新海，刘安，等. 基于应用运行时自保护的网络攻击溯源方法[J]. 邮电设计技术，2023（8）：19-23.

1　概述

随着信息技术的飞速发展，人们的科技和生活水平达到了新的高度，网络安全的整体形势却越发严峻。人工智能的发展让攻击手段更智能，云主机让网络攻击更隐蔽，网络攻击的难度和成本越来越低，网络攻击的破坏性和复杂性却越来越高。近年来，以高级持续威胁（APT）为代表的网络攻击事件层出不穷，如2019年伊朗针对美国基础设施的Parisite攻击，2022年西北工业大学遭受的APT攻击，都造成了巨大的破坏和经济损失。网络攻击溯源技术旨在网络遭受攻击时，综合利用各种技术手段主动追踪网络攻击发起者、定位攻击源，有针对性地减缓或反制网络攻击。然而，传统网络安全防护手段，如防病毒、防火墙等溯源能力严重不足，亟需新的技术手段提高溯源能力，从而对网络攻击者进行针对性的反制或取证。本文对网络攻击溯源技术进行了分析，提出了基于RASP的网络攻击溯源方法，该方法综合采用Web追踪和威胁情报分析技术，收集较为完备的网络攻击者信息并生成综合指纹标识网络攻击者，提高溯源的准

收稿日期：2023-06-28

确性，为下一步取证和反制提供依据和支撑。

2 网络攻击溯源技术简介

网络攻击溯源在安全领域被广泛的关注和研究，刘潮歌[1]等对网络攻击溯源技术进行了总结，并将网络攻击溯源技术分为传统网络攻击溯源技术和目前主流的网络攻击溯源技术。

2.1 传统网络攻击溯源技术

在传统的网络攻击溯源技术的研究中，陈周国等[2]的工作比较具有代表性，其从攻击溯源的深度和精准度上将攻击溯源细分为4个层次，分别为追踪溯源攻击主机、追踪溯源攻击控制主机、追踪溯源攻击者、追踪溯源攻击组织机构，并介绍了每个层次的相关溯源技术。

第1层追踪溯源的目标是定位攻击主机。第1层追踪溯源技术从攻击溯源的原理上可以划分为Input Debugging[3]、Itrace[4]、PPM[5]等方法，是网络数据包层面的技术方法，主要针对非定向网络攻击（如DDoS）。

第2层追踪溯源的目标是确定攻击控制主机。网络攻击者为掩盖身份信息往往利用僵尸网络、匿名通信系统或跳板机进行隐蔽攻击活动，使得攻击源追溯变得异常困难。第2层追踪溯源采用的技术主要有内部监测[6]、日志分析[7]、网络流分析[8]等。

第3层追踪溯源的目标是追踪定位网络攻击者。第3层追踪溯源是将网络空间中的事件与物理世界中的事件相关联，并以此确定物理世界中对事件负责的自然人过程。完成第3层追踪目标的核心是对信息数据的收集与分析，需要收集的信息包括但不限于邮件、攻击代码[9]等。

第4层追踪溯源的目标是确定攻击的组织机构，即实施网络攻击的幕后组织或机构。第4层溯源技术需要在前3个层次的追踪基础上，结合谍报、外交、第三方情报等所有信息，综合分析评估确定幕后组织机构。

2.2 目前主流的网络攻击溯源技术

目前，在网络攻击追踪溯源理论和技术方面都进行了相应的创新，比较具有代表性的有Web追踪技术、威胁情报技术和网络欺骗技术。

a）Web追踪技术。Web在网络攻击中扮演着重要角色，不仅是攻击者探测社工信息的重要平台，还是投递攻击载荷的重要通道。2010年，Eckersley等[10]最早提出在浏览器端采集一系列属性作为区分浏览器个体的指纹，可以用来跨网站追踪用户。近年来，还有研究提出使用Canvas指纹[11]、CSS指纹[12]跨网站追踪浏览器用户。除追踪外，还有学者研究了利用浏览器特性获取用户隐私信息，如2015年，研究人员difafygi[13]就在github上公开了基于WebRTC特性得到用户内外网IP地址的方法。

b）威胁情报技术。威胁情报在追踪溯源方面的优势在于其海量多来源知识库以及情报的共享机制。防御者将已掌握的溯源线索作为输入传递给威胁情报系统，通过关联和挖掘，输出大量与已知线索存在关联的新线索。2015年杨泽明等[14]明确指出“威胁情报的共享利用将是实现攻击溯源的重要技术手段”。

c）网络欺骗技术。网络欺骗技术由蜜罐技术演化而来。刘宝旭等[15]是国内研究网络欺骗的先驱，他们最早于2002年就基于蜜罐技术提出了“陷阱防御”思路，用于发现网络攻击和溯源取证；2017年，国内的贾召鹏等[16]则系统地综述了网络欺骗技术。

3 基于RASP的网络攻击溯源方法

网络攻击溯源技术的研究积累虽然丰富，但现有网络攻击更加隐蔽，攻击溯源的难度越来越大，攻击溯源的成本越来越高，需要不断探索新的攻击溯源方法，提高攻击溯源的准确性。为此，本文提出了基于RASP的网络攻击溯源方法，通过收集完备的网络攻击者信息，并生成综合指纹唯一标识网络攻击者，提高网络攻击溯源的准确性。

基于RASP的网络攻击溯源方法的技术架构如图1所示，基于RASP类字节码修改技术的Web追踪，将溯源代码注入攻击者浏览器中，获取网络攻击者的浏览器指纹信息、攻击者内外网IP信息、攻击者虚拟身份信息等Web信息；基于RASP的Hook技术和数据流跟踪技术，能有效记录网络攻击的请求URL地址、请求头信息、网络攻击类型、网络攻击载荷、攻击调用链等网络攻击信息。同时，将收集的Web信息和网络攻击信息与威胁情报进行对比分析和挖掘，获取额外的拓展信息。最后，将收集的所有信息生成综合指纹信息唯一标识网络攻击者。

3.1 核心技术能力

本文所述网络攻击溯源方法的核心技术主要包括基于RASP技术的Web信息和网络攻击信息收集、基于威胁情报的拓展信息收集和综合指纹生成，并以综合指纹唯一标识网络攻击者，提高网络攻击者溯源

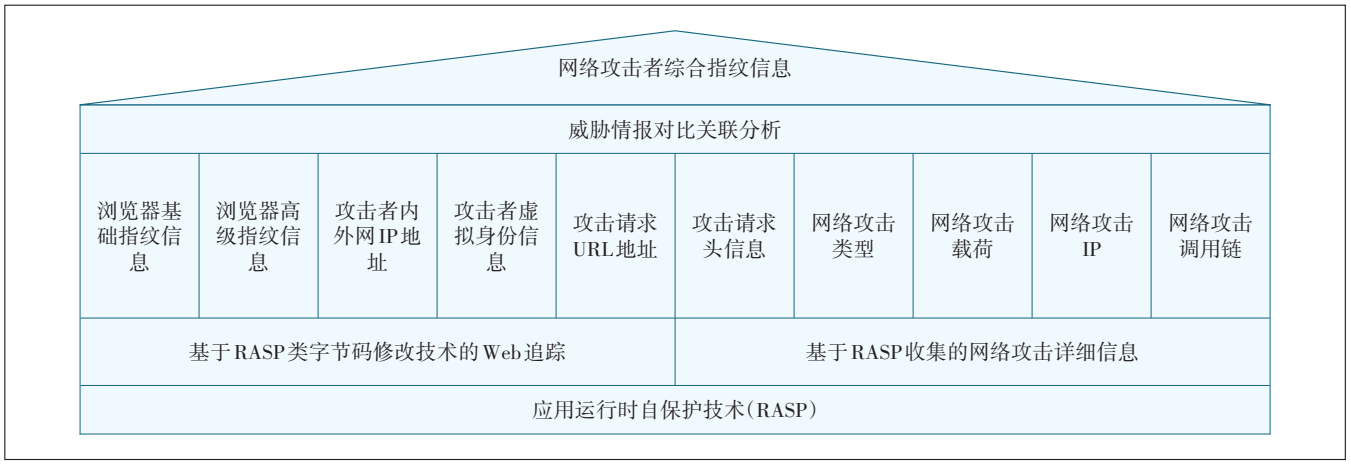

图1　基于RASP的网络攻击溯源的技术架构

的准确性。

3.1.1　基于RASP的Web信息收集

借助RASP的插桩和类字节码修改技术实现的Web追踪，能够有效获取浏览器基本指纹、浏览器高级指纹、攻击者内外网IP地址和网络虚拟身份等Web信息，详细流程如图2所示。

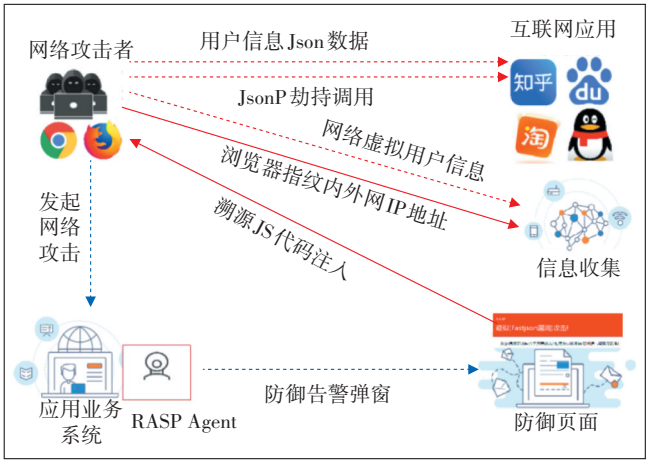

图2　基于RASP的Web信息收集

a）应用业务系统中部署了RASP探针，并且开启了防御功能。

b）攻击者对应用系统发起攻击，并被RASP Agent检测到，拦截攻击行为并弹出拦截页面。

c）拦截页面中已经嵌入了相关溯源JavaScript代码，当用户点击该拦截页面后，JavaScript代码将植入攻击者浏览器。

d）调用Navigator接口，并执行相关命令获取浏览器的基本指纹信息。

e）调用Canvas接口，生成隐藏图像，对图像进行哈希计算，得到的哈希值作为Canvas指纹。

f）调用Audio Context接口，生成音频信息流，并对音频信息流进行动态压缩处理后，计算哈希值作为Audio Context指纹。

g）调用WebGL接口，生成WebGL报告并转换成为哈希值作为WebGL指纹。

h）调用WebRTC插件，解析UDP通信包获取攻击者的内外网IP地址。

i）执行JavaScript脚本访问其他互联网应用的JsonP接口获取攻击者的网络虚拟身份信息。

j）攻击者浏览器将收集的网络攻击者信息反馈给防御页面的信息收集模块，最终完成对Web信息的收集。

3.1.2　基于RASP的网络攻击信息收集

RASP作为一种新型应用安全保护技术，它将自身防御逻辑注入到应用程序的底层代码中，与应用程序融为一体，使应用程序具备自我保护能力，目前支持Java、PHP和Python等主流编程语言，并且以Java RASP的技术最为成熟。Java RASP通过插桩技术Hook了一些敏感函数，比如数据库操作、文件操作、命令执行等，并跟踪和记录应用交互上下文，当检测到攻击行为时，通过Java Agent技术加入防御逻辑字节码，最终完成对攻击行为的拦截并记录网络攻击信息。通过RASP云端管理系统能够查看收集的网络攻击信息，主要包括请求URL地址、请求头信息、网络攻击类型、网络攻击载荷、攻击调用链等网络攻击信息。

3.1.3　基于威胁情报的拓展信息收集

为了收集更加完备的网络攻击者信息，需要借助威胁情报技术，将基于RASP收集的网络攻击信息和

Web信息与威胁情报库进行比对分析，挖掘出更多的拓展信息，最终生成完备的网络攻击者信息，原理如图3所示。为了获得准确的网络攻击者信息，需要维护准确的威胁情报，不仅需要将多方威胁情报库进行情报交换，还需要将原始信息库与生成的拓展信息库进行多轮比对，去除噪声数据，最终生成完备的网络攻击者信息库。

3.1.4 综合指纹生成

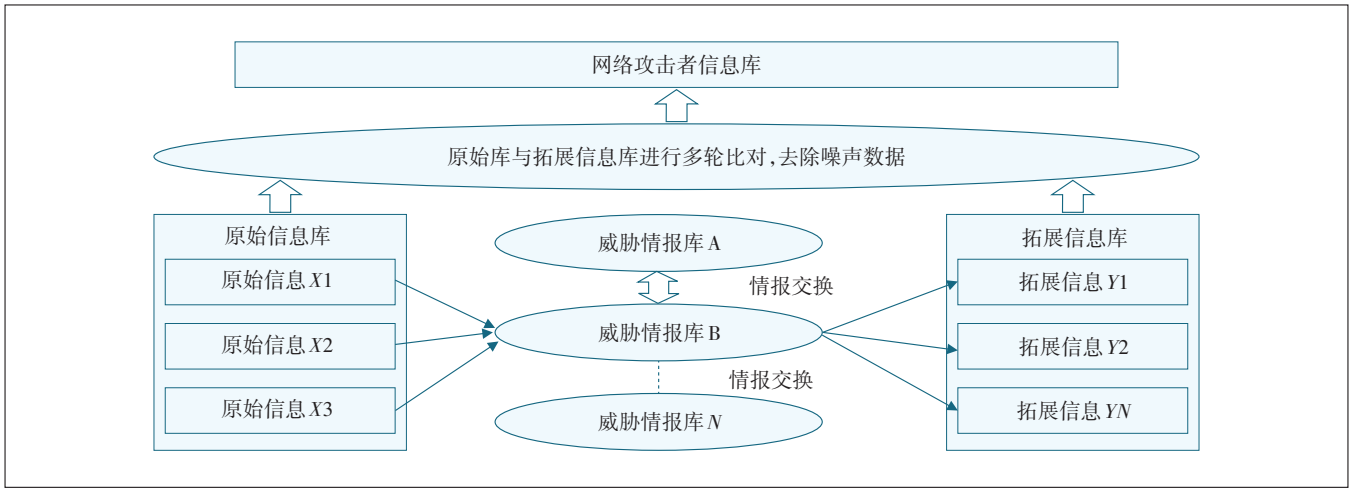

图3　基于威胁情报的拓展信息收集

在网络攻击溯源中，攻击取证是为了避免网络攻击者的抵赖。因此，为了让攻击取证的证据更有说服力，采用技术手段唯一标识网络攻击者成为亟需解决的问题。生成综合指纹的方式可以作为一种有效手段解决上述问题，如图4所示，通过将收集的Web信息、基于RASP收集的网络攻击信息、威胁情报生成的拓展信息进行去重、归并和格式化处理，保存为固定格式的文本文件，并将该文本文件进行MD5加密，以生成的MD5值作为综合指纹标记网络攻击者。综合指纹基于完备的攻击者信息生成，其MD5值碰撞概率很低，可以作为唯一标记标识网络攻击者，为溯源取证提供有力的依据，提高网络攻击者溯源的准确性。

3.2 优劣势对比

目前，业界主流的网络攻击溯源方法主要包括Web跟踪、威胁情报和网络欺骗，在溯源方面各有优劣势，如表1所示。其中，Web跟踪溯源方法的优势是资源消耗较少，不易被攻击者发现；其劣势是需要对Web应用系统进行改造，增加溯源代码，部署较为复杂，攻击者信息收集不全，溯源准确率不高。威胁情报溯源方法的优势是部署简单，不会被攻击者发现；其劣势是威胁情报的完备性和准确性直接决定了溯源的准确性。网络欺骗溯源方法的优势是能收集较完备的攻击者信息，溯源准确率较高；其劣势是需要部署蜜罐、密网等欺骗系统，消耗资源较大，部署较为复杂，而且欺骗系统非真实业务容易被攻击者发现。相较于以上几种溯源方法，本文所述溯源方法以RASP作为技术基础和纽带，综合采用了Web追踪技术和威胁情报分析技术，部署较为简单，资源消耗较少，能够收集完备的攻击者信息，生成的综合指纹能够唯一标识网络攻击者，溯源准确率较高，而且不易被攻击者发现。

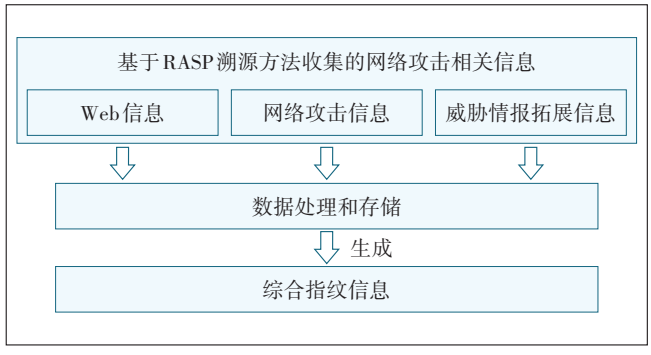

图4　综合指纹生成过程

表1　本文溯源方法与其他溯源方法的对比

溯源方法类别	攻击者信息	溯源准确率	部署复杂度	资源消耗	被攻击者发现
Web跟踪方法	一般详细	较低	较复杂	较少	不易被发现
威胁情报分析方法	较详细	较高	简单	中等	不会被发现
欺骗技术方法	较详细	较高	复杂	较多	容易被发现
基于RASP的溯源方法	详细	高	简单	中等	不易被发现

4 应用场景

本文所述溯源方法基于RASP技术实现，在满足RASP探针部署到Web应用系统的前提下，能够在以下应用场景中获得较好的溯源效果。

a）跨网站追踪的场景。攻击者同时拥有一个已公开的白身份和一个未公开的黑身份，虽然2个身份访问了不同的网站，但可以提取到相同的Web指纹信息，因此能通过Web指纹关联来溯源攻击者的真实身份。

b）漏洞不易修复的Web应用系统。针对漏洞不易修复的Web应用系统，RASP能够通过打补丁的方式Hook漏洞关联的函数，在漏洞被利用时识别网络攻击，并在拦截网络攻击的同时进行溯源。

c）网络欺骗技术不易部署的场景。由于部署蜜罐、密网等需要消耗大量资源，维护和管理困难，并且一旦逃逸，易引入新安全风险。因此，在欺骗溯源技术不易部署的场景，可以采用基于RASP的溯源方法进行网络攻击溯源。

d）重要Web应用系统需要具备取证和溯源反制的场景。作为关键基础设施的重要Web应用系统在遭受到网络攻击的时候，根据管理要求需要具备取证和溯源反制的能力，基于RASP的溯源方法能够很好地支撑相关需求。

5 结束语

国内外网络安全形势越来越严峻，网络攻击溯源成为网络攻击反制和取证的前提。目前，业界对网络攻击溯源技术的研究不断创新，以Web追踪技术、威胁情报技术和网络欺骗技术为代表的攻击溯源技术成为攻击溯源的主流技术。因此，在分析已有攻击溯源技术的基础上，借助RASP的技术优势，提出了基于RASP的网络攻击溯源方法，收集完备的网络攻击者信息并生成综合指纹标识网络攻击者，提高网络攻击溯源的准确性。网络攻击溯源面临的困难依然很多，需要综合利用各种溯源手段，本文所述的溯源方法作为新的技术手段，希望能为业界网络攻击溯源提供参考和借鉴。

参考文献：

[1] 刘潮歌，方滨兴，刘宝旭，等. 定向网络攻击追踪溯源层次化模型研究[J]. 信息安全学报，2019，4(4)：1-18.

[2] 陈周国，蒲石，郝尧，等. 网络攻击追踪溯源层次分析[J]. 计算机系统应用，2014，23(1)：1-7.

[3] STONE R. CenterTrack：an IP overlay network for tracking DoS floods [C]//Proceedings of the 9th USENIX Security Symposium. Denver，Colorado，USA：USENIX Association，2000：1-14.

[4] BELLOVIN S M，LEECH M，TAYLOR T. ICMP traceback messages [R/OL]. [2023-05-04]. https://academiccommons. columbia. edu/doi/10.7916/D8FF406R.

[5] SAVAGE S，WETHERALL D，KARLIN A，et al. Practical network support for IP traceback[J]. ACM SIGCOMM Computer Communication Review，2000，30(4)：295-306.

[6] BUCHHOLZ F P，SHIELDS C. Providing process origin information to aid in network traceback[C]//Proceedings of the General Track of the Annual Conference on USENIX Annual Technical Conference. Berkeley，CA，United States：USENIX Association，2002：261-274.

[7] WANG X Y，REEVES D. Robust correlation of encrypted attack traffic through stepping stones by flow watermarking[J]. IEEE Transactions on Dependable and Secure Computing，2011，8(3)：434-449.

[8] WANG B T，SCHULZRINNE H. A denial-of-service-resistant IP traceback approach[C]//Proceedings. ISCC 2004. Ninth International Symposium on Computers and Communications (IEEE Cat. No.04TH8769). Alexandria，Egypt：IEEE，2004：351-356.

[9] SPAFFORD E H，WEEBER S A. Software forensics：can we track code to its authors?[J]. Computers & Security，1993，12(6)：585-595.

[10] ECKERSLEY P. How unique is your Web browser?[C]//Privacy Enhancing Technologies. Berlin，Heidelberg：Springer，2010：1-18.

[11] MOWERY K，SHACHAM H. Pixel perfect：fingerprinting canvas in HTML5 [EB/OL]. [2023-05-04]. https://hovav. net/ucsd/dist/canvas.pdf.

[12] TAKEI N，SAITO T，TAKASU K，et al. Web browser fingerprinting using only cascading style sheets[C]//2015 10th International Conference on Broadband and Wireless Computing，Communication and Applications(BWCCA). Krakow，Poland：IEEE，2015：57-63.

[13] GitHub. Webrtc-ips[EB/OL]. [2023-05-04]. https://github.com/diafygi/Webrtc-ips.

[14] 杨泽明，李强，刘俊荣，等. 面向攻击溯源的威胁情报共享利用研究[J]. 信息安全研究，2015，1(1)：31-36.

[15] 刘宝旭，曹爱娟，许榕生. 陷阱网络技术综述[J]. 网络安全技术与应用，2003(1)：65-69.

[16] JIA Z P，FANG B X，LIU C G，et al. Survey on cyber deception[J]. Journal on Communications，2017，38(12)：128-143.

作者简介：
蓝鑫冲，工程师，硕士，主要从事网络与信息安全研究工作；郭新海，工程师，硕士，主要从事网络与信息安全研究工作；刘安，工程师，硕士，主要从事网络与信息安全研究工作；丁攀，工程师，硕士，主要从事网络与信息安全研究工作；王戈，工程师，硕士，主要从事网络与信息安全研究工作。