软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2021,32(1):194–217 [doi: 10.13328/j.cnki.jos.006105]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

面向网络取证的网络攻击追踪溯源技术分析*

刘雪花[1,2], 丁丽萍[1,3,4], 郑 涛[5], 吴敬征[6], 李彦峰[1,2]

[1](中国科学院 软件研究所 并行软件与计算科学实验室,北京 100190)

[2](中国科学院大学 计算机科学与技术学院,北京 100049)

[3](广州中国科学院软件应用技术研究所 电子数据取证实验室,广东 广州 511458)

[4](广东中科实数科技有限公司,广东 广州 511458)

[5](联通华盛通信有限公司,北京 100005)

[6](中国科学院 软件研究所 智能软件研究中心,北京 100190)

通讯作者: 丁丽萍, E-mail: dingliping@gz.iscas.ac.cn

摘 要: 首先定位网络攻击事件的源头,然后进行有效的电子数据证据的收集,是网络取证的任务之一.定位网络攻击事件源头需要使用网络攻击追踪溯源技术.然而,现有的网络攻击追踪溯源技术研究工作主要从防御的角度来展开,以通过定位攻击源及时阻断攻击为主要目标,较少会考虑到网络取证的要求,从而导致会在网络攻击追踪溯源过程中产生的大量有价值的数据无法成为有效电子数据证据在诉讼中被采用,因而无法充分发挥其在网络取证方面的作用.为此,提出了一套取证能力评估指标,用于评估网络攻击追踪溯源技术的取证能力.总结分析了最新的网络攻击追踪溯源技术,包括基于软件定义网络的追踪溯源技术,基于取证能力评估指标分析了其取证能力,并针对不足之处提出了改进建议.最后,提出了针对网络攻击追踪溯源场景的网络取证过程模型.该工作为面向网络取证的网络攻击追踪溯源技术的研究提供了参考.

关键词: 网络攻击追踪溯源;网络取证;电子数据证据可采性;电子数据证据证明力;取证过程模型;IP 追踪

中图法分类号: TP393

中文引用格式: 刘雪花,丁丽萍,郑涛,吴敬征,李彦峰.面向网络取证的网络攻击追踪溯源技术分析.软件学报,2021,32(1):194–217. http://www.jos.org.cn/1000-9825/6105.htm

英文引用格式: Liu XH, Ding LP, Zheng T, Wu JZ, Li YF. Analysis of cyber attack traceback techniques from the perspective of network forensics. Ruan Jian Xue Bao/Journal of Software, 2021,32(1):194–217 (in Chinese). http://www.jos.org.cn/1000-9825/6105.htm

Analysis of Cyber Attack Traceback Techniques from the Perspective of Network Forensics

LIU Xue-Hua[1,2], DING Li-Ping[1,3,4], ZHENG Tao[5], WU Jing-Zheng[6], LI Yan-Feng[1,2]

[1](Laboratory of Parallel Software and Computational Science, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)

[2](School of Computer Science and Technology, University of Chinese Academy of Sciences, Beijing 100049, China)

[3](Digital Forensics Laboratory, Institute of Software Application Technology, Guangzhou & Chinese Academy of Sciences (GZIS), Guangzhou 511458, China)

* 基金项目: 2019 年度南沙区人工智能应用示范项目(2019SF01); 广州市科技计划(201802020015); 国家自然科学基金(61772507); 羊城创新创业领军人才支持计划(领军人才 2016008)

Foundation item: 2019 Artificial Intelligence Application Demonstration Project of Nansha District, Guangzhou Municipality, China (2019SF01); Science and Technology Planning Project of Guangzhou Municipality, China (201802020015); National Natural Science Foundation of China (61772507); Support Scheme of Guangzhou for Leading Talents in Innovation and Entrepreneurship (领军人才 2016008)

收稿时间: 2020-01-14; 修改时间: 2020-06-04; 采用时间: 2020-06-16; jos 在线出版时间: 2020-07-27

© 中国科学院软件研究所 http://www.jos.org.cn

[4](Guangdong Chinese Academy of Sciences & Realdata Science and Technology Co. Ltd., Guangzhou 511458, China)
[5](China Unicom VSENS Communications Co. Ltd., Beijing 100005, China)
[6](Intelligent Software Research Center, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)

Abstract: Locating the source of cyber attack and then collecting digital evidence is one of the tasks of network forensics. Cyber attack traceback techniques are used to locate the source of cyber attack. However, current research on cyber attack traceback is mainly conducted from a defensive perspective, targeting at blocking cyber attack as soon as possible via locating the cyber attack source, and rarely considers digital evidence acquirement. As a result, the large amount of valuable digital evidence generated during the process of cyber attack traceback cannot be used in prosecutions, and their value in network forensics cannot be fully exploited. Therefore, a set of forensics capability metrics is proposed to assess the forensics capability of cyber attack traceback techniques. The latest cyber attack traceback techniques, including cyber attack traceback based on software defined network, are summarized and analyzed. Their forensics capability is analyzed and some suggestions are provided for improvement. At last, a specific forensics process model for cyber attack traceback is proposed. The work of this paper provides reference for research on cyber attack traceback technology targeting at network forensics.

Key words: cyber attack traceback; network forensics; the admissibility of digital evidence; the probative force of digital evidence; forensics process model; IP traceback

攻击者在实施网络攻击时,常采用各种技术手段隐藏自己以对抗追踪,如采用虚假 IP 地址、网络跳板、僵尸网络、匿名网络等技术.网络攻击追踪溯源技术[1]能够有效应对攻击者的隐藏手段,定位真实的攻击源头,以便及时阻断网络攻击.网络取证是一种对网络攻击的事后追责手段,通过对网络流量等进行取证分析,将生成的电子数据证据用于诉讼活动,从而实现对各类网络违法犯罪活动的事后追责[2,3].网络攻击追踪溯源技术与网络取证技术沿着不同路线独立发展.定位网络攻击事件源头并进行有效电子数据证据的收集,是网络取证的任务之一[2],定位网络攻击事件源头需要使用网络攻击追踪溯源技术,因此,网络攻击追踪溯源技术与网络取证技术有着密切的关联性.然而,现有的网络攻击追踪溯源技术研究工作主要从防御的角度开展,较少考虑网络取证的要求,导致其产生的大量有价值的数据无法成为有效电子数据证据在诉讼中被采用,无法充分发挥其在网络取证方面的作用.

已有文献[1,4−6]分别从不同的角度对网络攻击追踪溯源技术进行总结归纳:文献[1,4]从 4 个层面对网络攻击追踪溯源技术进行分析,分别是攻击主机的追踪溯源、攻击控制主机的追踪溯源、攻击者的追踪溯源、攻击组织机构的追踪溯源;文献[5]则根据攻击者采取的不同隐藏技术对网络攻击追踪溯源技术进行分析,分别是虚假 IP 的追踪溯源、僵尸网络的追踪溯源、匿名网络的追踪溯源、跳板的追踪溯源和局域网的追踪溯源;文献[6]则基于分布式拒绝服务攻击(distributed denial of service,简称 DDoS)场景对网络攻击追踪溯源技术进行分析.然而,这些文献较缺乏从网络取证的角度对现有的网络追踪溯源技术进行深入的思考与分析,且这些文献没有覆盖较新的基于软件定义网络(software defined network,简称 SDN)的网络攻击追踪溯源技术.

为此,本文将总结分析现有的网络攻击追踪溯源技术,并从网络取证的角度对现有的网络攻击追踪溯源技术重新加以思考.本文的主要贡献如下:

(1) 提出了一套取证能力评估指标,用于评估网络攻击追踪溯源技术的取证能力;
(2) 总结分析了现有的网络攻击追踪溯源技术,包括较新的基于 SDN 的网络攻击日志追踪溯源技术;
(3) 基于取证能力评估指标分析了现有网络攻击追踪溯源技术的取证能力,并针对不足之处给出了改进建议;
(4) 提出了针对网络攻击追踪溯源场景的网络取证过程模型,通过结合网络取证过程与网络攻击追踪溯源技术,进一步提高整体取证能力.

本文第 1 节给出网络攻击追踪溯源和网络取证相关的定义.第 2 节提出一套取证能力评估指标,用于后文分析网络攻击追踪溯源技术的取证能力.第 3 节从网络取证角度对网络攻击追踪溯源技术进行分析,首先给出技术分类并划定本文的分析范围,然后依次对基于日志存储查询的追踪溯源技术、基于数据包标记的追踪溯源技术、基于 SDN 的日志追踪溯源技术和混合追踪溯源技术进行分析,分析其发展现状、优缺点和取证能力,并

© 中国科学院软件研究所 http://www.jos.org.cn

给出取证能力的改进建议.第 4 节分析现有网络取证过程模型在网络攻击追踪溯源场景下的不足,并提出针对网络攻击追踪溯源场景的网络取证过程模型.第 5 节对本文的研究工作进行总结,并对未来值得关注的研究方向进行初步探讨.

1 网络攻击追踪溯源与网络取证相关定义

1.1 网络攻击追踪溯源相关定义

定义 1(网络攻击追踪溯源)[1]. 通过网络攻击的中间介质还原攻击路径,以确定网络攻击者的身份或位置,即网络攻击源头.确定了网络攻击源头,使得防御方能及时地制定和实施有针对性的防御措施,提高网络防御的主动性和有效性.

定义 2(网络攻击追踪溯源问题模型)[7]. 让 $R_{i1},R_{i2},\ldots,R_{in}$ 代表攻击者 A_i 和受害者 V 之间的有序路由器列表,这个有序路由器列表就是 A_i 的攻击路径.将参与攻击数据包转发并最终传递给受害者的路由器定义为攻击路由器,对于攻击路径上的任何路由器 R_{ij},将所有在路由器 R_{ij} 和受害者之间的路由器称为 R_{ij} 的前置列表,而将在路由器 R_{ij} 和攻击者之间的路由器称为 R_{ij} 的后继列表.攻击追踪溯源问题的目的是,确定直接连接到 A_i 的攻击路由器(即图 1 所示的路由器 R_{i1},其后继列表为空).

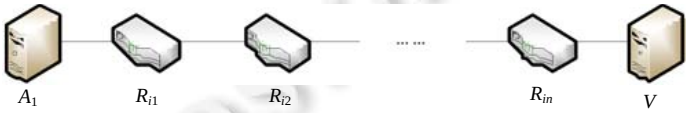

Fig.1 Sequence of routers between the attacker and the victim[7]

图 1 攻击者到受害者之间的路由器序列[7]

1.2 网络取证相关定义

定义 3(电子数据取证)[8]. 电子数据取证是指科学地运用提取和证明方法,对于从电子数据源提取的电子数据证据进行保护、收集、验证、鉴定、分析、解释、存档和出示,以有助于进一步的犯罪事件重构或者帮助识别某些与计划操作无关的非授权性活动.

定义 4(网络取证)[8]. 网络取证是电子数据取证的一个分支学科,特指通过检测、收集和分析计算机网络流量等电子数据来实现合法证据的收集和入侵检测.

2 取证能力评估指标

要发挥网络攻击追踪溯源技术在网络取证方面的价值,需重点考虑其产生的电子数据证据能否被用于网络取证,以便对攻击源头进行事后追责.为此,本文从电子数据证据的角度提出一套取证能力评估指标,用于评估网络攻击追踪溯源技术的网络取证能力.

一方面,在衡量电子数据证据能否在诉讼程序或其他证明活动中被使用时,常使用电子数据证据可采性标准和证明力标准.电子数据证据具备了可采性,且有较强的证明力,法官才会在审判中予以采用[9].电子数据证据可采性标准和证明力标准是两个定性标准,其基本概念如下[9].

1) 电子数据证据的可采性标准包括关联性、合法性与真实性.
   (1) 关联性是指证据与要证明的案件事实或其他争议事实具有直接联系;
   (2) 合法性是指证据的主体、形式及收集程序或提取方法必须符合法律的有关规定;
   (3) 真实性是指证据必须至少在形式或表面上是真实的;
2) 电子数据证据的证明力标准包括可靠性和完整性.
   (1) 可靠性是衡量电子数据证据真实程度的指标,一般可以通过细化审查的各个环节予以评估,如收集环节的可靠性、传输环节的可靠性、存储环节的可靠性等等;

© 中国科学院软件研究所 http://www.jos.org.cn

(2) 完整性一般是指在电子数据从提取到最终出示的过程中,其内容始终保持完整和未予改动.

另一方面,基于传统的证据理论,往往通过事后的调查取证来还原案件真相.因而,事后取证能力是一项衡量取证技术的基本标准.

事后取证是指在系统被攻击或者犯罪行为发生后,取证调查人员对可疑计算机开展诸如恢复数据、获取数据、分析鉴定等调查工作,收集所有可能获取的数据来进行事件重构,以确认犯罪行为实施的时间、地点和方式[10].由事后取证的定义可知:只有电子数据证据存储在非易失性存储器上,并在安全事件发生后依然存在,才能支持事后取证,而有些电子数据证据,如网络数据报文,随着安全事件的结束就会灭失,无法支持事后取证.因此,电子数据证据的非易失性对事后取证至关重要.

为此,本文基于以上两项标准的 5 个方面和非易失性能力,提出一套六维的取证能力评估指标,其取值范围和衡量标准见表 1.

Table 1 Forensic capacity metrics

表 1 取证能力评估指标

取证能力指标	取值范围	衡量标准
关联性	不支持	电子数据证据与要证明的案件事实或其他争议事实无直接联系
	支持较弱	电子数据证据与要证明的案件事实或其他争议事实有部分联系
	支持	电子数据证据与要证明的案件事实或其他争议事实具有直接联系
合法性	不支持	电子数据证据的主体、形式及收集程序或提取方法不符合法律的有关规定
	支持较弱	电子数据证据的主体、形式及收集程序或提取方法仅有部分符合法律的有关规定
	支持	电子数据证据的主体、形式及收集程序或提取方法符合法律的有关规定
真实性	不支持	电子数据证据在形式或表面上无法保证真实
	支持较弱	电子数据证据在形式或表面上部分保证真实
	支持	电子数据证据在形式或表面上是真实的
可靠性	不支持	电子数据证据收集环节、传输环节、存储环节都不可靠
	支持较弱	电子数据证据收集环节、传输环节、存储环节部分可靠
	支持	电子数据证据收集环节、传输环节、存储环节全部可靠
完整性	不支持	电子数据证据的内容可能发生缺失和改变
	支持较弱	部分电子数据证据的内容可能发生缺失和改变
	支持	电子数据证据的内容保持完整和未予改动
非易失性	不支持	电子数据证据随着安全事件的结束而灭失
	支持较弱	仅有部分电子数据证据存储在非易失性存储器上,并在安全事件发生后依然存在
	支持	电子数据证据存储在非易失性存储器上,并在安全事件发生后依然存在

3 基于网络取证角度分析网络攻击追踪溯源技术

3.1 网络攻击追踪溯源技术分类

本文在文献[1]的基础上,将网络攻击追踪溯源技术分为 8 类.

(1) 基于日志存储查询的追踪溯源技术:通过使用路由器、主机等设备,对网络中传播的数据流进行存储记录,存储记录不必记录完整的数据包信息,可以只记录一些关键信息,并通过事后对这些日志信息进行查询与分析,恢复出攻击路径;

(2) 基于路由器输入调试的追踪溯源技术:利用路由器的调试功能进行特征匹配,如果匹配成功,则该路由器在攻击路径上.一般通过从被攻击端开始回溯攻击路径;

(3) 基于数据包标记的追踪溯源技术:将路径信息进行编码后填充在网络数据包的特定字段,跟随网络数据包在网络中传播,最后在被攻击端收集这些信息,通过特定的算法恢复出攻击路径;

(4) 基于单独发送溯源信息的追踪溯源技术:路由器主动向转发的数据包目的地址发送 ICMP(Internet control message protocol)报文,用于告知该路由器在该数据包的传播路径之上;

(5) 基于 SDN 的日志追踪溯源技术:将 SDN 网络中的流相关信息以日志或者中间文件的形式记录在控制层或者单独的溯源取证服务器,并根据日志或者中间文件重构攻击路径;

(6) 基于 SDN 的路由器输入调试追踪溯源技术:通过灵活控制 SDN 路由器调试功能进行特征匹配,恢复

© 中国科学院软件研究所 http://www.jos.org.cn

攻击路径;

(7) 基于威胁情报的追踪溯源技术:通过威胁情报信息中的僵尸网络、网络跳板、匿名网络和隐蔽信道等信息进行关联,实现控制主机追踪溯源,并可通过威胁情报中黑客及其组织的特征信息进行关联,实现攻击者识别;

(8) 混合追踪溯源技术:多种技术结合的追踪溯源技术,常与采用存储查询的追踪溯源技术和基于数据包标记的追踪溯源技术这两种技术相结合,达到取长补短的目的.

获取有效的电子数据证据是网络取证的主要目标之一,而日志类型的电子数据是在取证实务中最常使用的一类电子数据证据,具有较好的可解释性和实用性.本文分析涉及日志记录的追踪溯源技术,包括基于日志存储查询的追踪溯源技术、基于数据包标记的追踪溯源技术、基于 SDN 的日志追踪溯源技术以及混合追踪溯源技术这 4 类.

3.2 基于日志存储查询的追踪溯源技术分析

3.2.1 发展现状

基于日志存储查询的追踪溯源技术可分为日志记录和攻击路径重构两个过程,日志记录在网络中的路由器上进行,通过路由器存储网络日志信息,如流经该路由器的数据包摘要、签名甚至是整个完整的数据包.攻击路径重构从被攻击端开始回溯上游转发设备,从其日志中查找是否有特定的攻击数据包的日志记录,如果有,则认为该转发设备在攻击路径之上.如此,直至攻击端,从而得到攻击路径.

基于日志存储查询的追踪溯源技术经历了一段较长时间的发展.最早由 Matsuda 等人[11]提出基于日志的 IP 追踪方法,他们在转发设备中记录每个数据包的部分信息,并使用 data-link 识别机制来进行数据包查询,以回溯攻击路径,每个数据包大约需要使用 60bytes 的存储空间,导致转发设备的存储开销过大.一直到基于数据包 hash 值日志记录方法的提出,才为基于日志的追踪溯源方法带来了应用的可能.首先,hash 值远小于原始数据大小,可极大地减少存储开销;其次,由于 hash 计算是不可逆的,不会泄露数据本身;再次,hash 值可用于确定数据的唯一性,本身更容易得到法律的认可,其在取证领域有着相当广泛的应用.

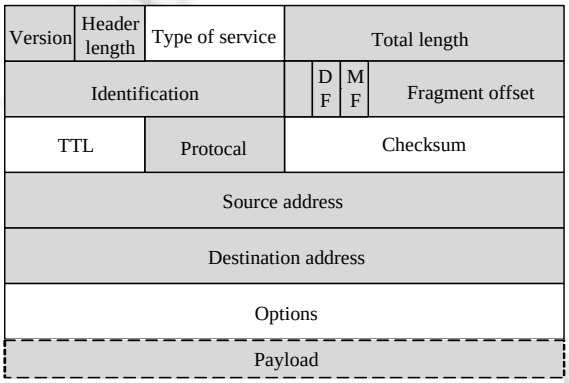

Fig.2 IP packet header field used to compute the IP packet digest
图 2 用于计算 IP 数据包摘要的 IP 包头字段

基于数据包 hash 值日志记录方法最经典的方法是由文献[12,13]首次提出的源路径隔离引擎(source path isolation engine,简称 SPIE),该方法将数据包信息用 IP 报文的摘要,也就是 hash 值来表示,并采用一种高效的数据存储结构布鲁姆过滤器(Bloom filter,简称 BF)[14]来存储数据包摘要,极大地降低了路由器的存储开销.BF 可将数据包摘要映射到位图上,并以 hash 值为索引快速查找位图上对应的元素,如果为 1,则表示该数据包经过该路由器.在重构攻击路径阶段,通过逐跳查询路由器的 BF,能够快速定位攻击路径.其中,IP 数据包的 hash 值计算仅取数据包的前 28 个字节,如图 2 中灰色部分所示,其覆盖了 IP 数据包包头有效字段和载荷前 8 个字节.文献[12,13]的作者们认为,该 28 个字节足以区分不同的数据包.该方法降低了路由器的存储开销,提高了可记录的数据量,存储开销占用每单位时间约 0.5%的链路容量,且支持基于单数据包的追踪溯源.

但是,SPIE 方法依然存在如下诸多不足[12,13]:(1) 因为 BF 中不可避免的 hash 冲突,导致 SPIE 存在一定的错误率;(2) SPIE 方法的存储开销依然过大,无法适用于大规模、高速网络环境;(3) SPIE 方法不支持 IPv6 协议;(4) SPIE 方法不适用于跨自治域的网络环境,且对跳板机、僵尸网络等攻击无法追踪到攻击源头.学者们针对这

© 中国科学院软件研究所 http://www.jos.org.cn

些不足提出多种改进方法.

(1) 针对 SPIE 错误率较高的问题,文献[15]在 SPIE 的基础上提出一种网络拓扑感知的单包 IP 溯源系统,通过利用路由器的本地拓扑信息,可以减少不必要的查询,从而极大地降低了错误率.并且,为了克服使用 BF 很难事先确定最优控制参数的难题,设计了一个 *k*-adaptive 机制,可以自动地调整最优控制参数,从而进一步降低错误率.文献[16,17]在 SPIE 提出的基于数据包 28 个字节的数据包信息的基础上增加了 TTL(time to live)字段.根据 TTL 信息,可以有效地减少查询需求,从而提高攻击路径图的构建效率,降低错误率.而文献[18]则提出了基于 IP 数据包包头的细粒度 hash 值和基于网络数据流的粗粒度 hash 值这两种数据包摘要计算方法,在查询时,通过双重验证来降低错误率.文献[19]则采用双 hash 技术,使用两种不同的 hash 函数来计算 IP 数据包摘要,在查询时,通过双重验证来降低错误率.文献[20,21]则提出通过路由器记录路径信息而非数据包信息来降低日志存储开销,并采用两级 hash 值,将路由器的存储开销变成固定不变的,从而消除了错误率;

(2) 针对 SPIE 存储开销过高的问题,文献[18]提出了基于网络流的追踪溯源系统,一条网络流一般通过源地址、目的地址、协议、源端口和目的端口来表示.与 SPIE 不同,该方法计算流的 hash 值作为摘要,同一个网络流中的数据包对应同一个 hash 值,从而减少了需要记录的信息,存储开销相比 SPIE 方法降低了 1~2 个数量级.但却只能进行网络流级别的溯源,牺牲了依据单个攻击包的溯源能力.文献[16,17]为了有效利用存储空间,提出一种动态分页方法将 BF 分页存储到辅助内存.该方法将接收允许的最大容量因子作为参数,只有当达到这个限制时才会发生分页.因此,BF 在主存中的停留时间是可变的,在网络流量较低时可能较长,在处理更多流量时可能较短,这种动态分页方法有效降低了 BF 的存储开销.文献[6,20–23]则通过记录数据包的路径信息来降低存储开销,同时也降低了计算开销,提高了正确率.文献[24]提出了 IP 追踪协议,通过定制一个 Sinkhole 路由器,在该路由器上将流经的数据包通过 hash 算法进行压缩并存入 hash 表中用于溯源分析,并进一步对 hash 表进行定期压缩,将压缩的 hash 表转存至专门的数据服务器中,从而解决路由器存储能力有限的问题;

(3) 针对 SPIE 不支持 IPv6 协议的问题,文献[19,25]通过对比 IPv6 和 IPv4 的报文结构,针对 IPv6 协议提出改进的 SPIE-IPv6 追踪溯源方法,在计算 IPv6 数据包摘要时,包含数据包头、所有的扩展字段以及载荷的前 20 个字节,以此来区分各个数据包;

(4) 针对 SPIE 适用性较差的问题,学者们根据不同的场景提出了改进方法.在跨自治域追踪溯源场景下,需要上级互联网服务提供商(Internet service provider,简称 ISP)的配合.文献[26]针对自治域的 IP 追踪溯源问题,提出了改进的 SPIE 方法,除了记录数据包信息以外,还需要记录数据包来自的自治域信息,以利于后续的跨域追踪溯源.但是 ISP 出于网络数据隐私和网络拓扑结构等机密信息等因素的考量,往往并不愿意予以配合,于是,文献[27]提出一种跨自治域的追踪溯源方法——LDPM(logging and deterministic packet marking).该方法结合使用确定包标记与包记录方法,使用转发设备编号和自治域编号来表示路径信息,不会泄露转发设备的 IP 地址,从而有效地保护了网络拓扑结构等敏感信息不外泄.实际网络攻击中,攻击者常常使用跳板来隐藏自己的行踪,因而需要跨过跳板机进行追踪溯源.在此场景下,前述追踪溯源技术只能追踪到末端跳板机,无法揭露真正的攻击者.文献[28]针对这一情况,提出一种基于 SPIE 的扩展架构,通过在 SPIE 的基础上融合跳板机检测技术,跳板机检测通过关联分析找到经过跳板机的成对的网络流,从而将追踪溯源以跳板机为线分段溯源并连接起来,最终实现多跳板机的网络攻击追踪溯源.针对僵尸网络追踪溯源的情况,文献[29]提出一种基于 DNS(domain name system)日志的僵尸网络追踪溯源方法,因为很多利用僵尸网络的攻击在攻击开始时会通过全称域名服务器查询受害主机的 IP 地址,会在域名服务器上留下相应的查询日志,通过分析 DNS 日志,从目标到源进行检查,便能追踪到被感染的僵尸机 IP 地址.

3.2.2 优点分析

(1) 与传统的网络协议和架构兼容,能够广泛应用于多种网络环境中;并且,现有的网络安全系统很容易

© 中国科学院软件研究所 http://www.jos.org.cn

支持日志查询,从而实现网络攻击的追踪溯源;

(2) 支持事后追踪溯源,因为日志信息被储存下来,即使攻击在实施追踪溯源之前已经结束,也可以通过日志信息开展追踪溯源;

(3) 支持基于单个数据包的追踪溯源,只要捕获到一个攻击数据包就能实现追踪溯源,极大地降低了追踪溯源的难度,因只需对单个数据包进行查询操作,带来的网络通信开销很小.

3.2.3 缺点分析

(1) 大部分方法的存储开销和计算开销依然较大,尤其是在高速网络环境中部署该应用,会造成成本的急剧增加;

(2) 网络攻击很多都是跨自治域的,需要ISP协助溯源取证.但是,由于大部分方法并未考虑信息保护问题,导致ISP会因隐私泄露、网络拓扑泄露等风险担忧而不愿意配合;

(3) 由于路由器存储能力有限,不能无限地存储流经的数据包信息,当达到存储上限时会刷新日志记录,冲掉之前的日志记录,因此,追踪溯源具有时限性;

(4) 日志记录存在安全隐患,如果系统或者设备被攻击者控制,攻击者可以任意删除或者篡改日志而导致这些电子数据失去真实性,而这是攻击者隐藏自己入侵踪迹时使用的常规手段.

3.2.4 取证能力分析

基于日志存储查询的追踪溯源技术产生的特有电子数据证据是其记录在路由器上的攻击路径相关的日志信息,这类方法的取证能力见表2.

(1) 支持关联性.日志信息记录了攻击包的路径相关信息,与要证明的网络攻击源有直接联系;

(2) 无需考虑合法性.网络攻击追踪溯源技术是网络取证过程中取证分析活动中用到的具体技术,单独依靠某项具体的技术是无法达到合法性要求的,过程的合法性才是证据的可采性审查的关键,这就要求结合网络取证过程的设计来弥补具体技术在合法性上的缺失.合法性问题将在第4节进一步分析;

(3) 可靠性支持较弱.可靠性是指取证各个环节的可靠性,此类追踪溯源技术只生产数据,仅需考虑数据本身的可靠性,而电子数据证据收集、传输和存储环节的可靠性一般由取证人员负责.数据本身的可靠性与真实性、完整性相关,因真实性、完整性较弱,故而其可靠性也较弱;

(4) 真实性支持较弱.因hash值和Bloom filter技术的使用,会因hash冲突为日志信息带来一定的错误率;

(5) 完整性支持较弱.因为路由器存储能力有限且日志没有安全机制加以保障,导致日志信息可能被覆盖而遗失,还可能遭受攻击被删除或者篡改;

(6) 支持非易失性.因日志信息存储在路由器端,可在事后提取分析.

Table 2 Forensics capabilities and improvements of cyber attack traceback techniques based on log storage and query

表2 基于日志存储查询的追踪溯源技术取证能力和改进

取证能力	支持情况	改进
关联性	支持	–
合法性	–	–
真实性	支持较弱	消除hash冲突提高准确率
可靠性	支持较弱	同真实性、完整性
完整性	支持较弱	增加安全日志转储机制
非易失性	支持	–

3.2.5 取证能力改进建议

常见的基于日志存储查询的追踪溯源技术的取证能力在真实性、完整性和可靠性这3方面的改进建议见表2.

(1) 改进真实性,需要降低甚至消除该类方法中的日志记录的错误率.在第3.2.1节中有较为详细的描述,其中,文献[20,21]通过采用两级hash表消除了日志记录的错误,值得借鉴;

© 中国科学院软件研究所 http://www.jos.org.cn

(2) 改进完整性,可以从架构优化的角度增加安全日志转储机制.如文献[30]提出了一个安全存储模型,该安全模型在独立于取证对象的网络中,包括一个 hash 加密引擎、日志报告模块和证据数据库,从证据被收集的那一刻起直至证据分析和展示,该模型可一直保护证据的完整性.文献[31,32]提出了一个分布式网络取证架构,该架构能够进行分布式的网络流量提取和存储、数据压缩,能够监控大规模网络.另外,随着区块链技术的发展,为保障电子数据证据的完整性产生了新的解决方案,区块链技术所具有的去中心化、防篡改、可追溯的特性,能够有效保证电子数据证据的完整性[33−35];

(3) 一旦真实性和完整性得到保证,可认为该类技术取证能力的可靠性也得到了保证.

3.3 基于数据包标记的追踪溯源技术分析

3.3.1 发展现状

基于数据包标记的追踪溯源技术包括包标记与传输和攻击路径重构两个过程:包标记与传输是指通过目标网络上的路由器对每个或者部分流经该路由器的数据包进行一定的变换,将能够反映数据包路径的信息以一种特殊的形式附加在数据包中,因为数据包头可用空间有限,常常需要将路径信息分片经多个数据包传输;攻击路径重构是指从被攻击端收集足够多的捎带有路径信息的数据包,并通过算法计算攻击路径.此类技术从某种程度上来说也是一种日志标记的方法,只是将日志信息标记在传输的网络数据包包头中.

基于包标记的追踪溯源技术相关研究成果较多,本文根据标记的内容和标记方法的不同将基于包标记的追踪溯源技术归纳为 3 类,即概率包标记方法、确定包标记方法和代数编码包标记方法.

1) 概率包标记(probabilistic packet marking,简称 PPM)方法

文献[36]提出了 3 种包标记方法,其中,

- 节点追加直接将数据包流经的每个路由器的 IP 地址追加到数据包尾部,理论上,一个数据包中包含了完整的路径信息,但其缺陷是数据包的大小随路径长度的增加而增加,会占用较多的网络带宽,影响正常的网络通信;
- 节点采样则是以一定的概率将路由器 IP 地址标记到数据包头中,而不是对每个数据包都标记.由于数据包头空间有限,只能标记一个 IP 地址,所以存在标记信息覆盖问题,离受害主机越远,收到该路由器标记过的数据包就越少.为了维持较高的准确率,随着攻击路径长度的增加,所需数据包的数量呈指数级增长;
- 边采样算法为了减少存储开销,不再直接标记路由器 IP 地址,而是用三元组(start,end,distance)来表示路径上的边信息,其中,start 和 end 表示相邻两个路由器构成的边信息;distance 则是指这条边与攻击者之间的距离,或者说路由器跳数.每个路由器以固定概率选择是否标记当前边信息,以此进一步减少总的存储开销.该三元组共需 72 个字节来存储,通过对两个路由器 IP 地址进行异或运算并分段,存入 8 个数据包头的保留字段 identification field 中,如图 3 所示.而在路径重构时,为了还原三元组信息,需要根据 distance 和 offset 进行宽度优先搜索,以对所有的分段按序重组;然后以受害者为根节点构建树,删除未标记的边来构建攻击路径,由根节点开始到叶子节点的单个子数为攻击路径.通过边信息重构攻击路径比节点采样效率更高.

PPM 方法具有实施较为简单、没有额外的网络带宽消耗和路由器存储消耗、跨自治域的追踪溯源不需要 ISP 的配合等优点.但是文献[37–41]分析了 PPM 依然存在诸多缺陷:(1) PPM 方法路径重建过程需要较高的计算量,且数据包头容量有限极大地限制了可携带的标记信息数量;(2) PPM 方法适用于 1 个攻击源的场景,在多个攻击源的场景下计算量将变得非常之大,且误报和漏报率激增;(3) PPM 方法的包标记概率是不变的,这导致距离被攻击端越远的节点,路径信息被后续节点路径信息覆盖的概率就越高;(4) PPM 方法的安全性难以保障,攻击者可以主动构造虚假的包标记信息,误导 PPM 得到错误的攻击路径;(5) PPM 方法的标记信息传输鲁棒性较弱,当被跟踪的流量传输率较低时,可能要很长时间才能完成,甚至因为缺少标记数据包而失败,在追踪软件利用攻击[42],如获取系统权限攻击和网络嗅探等攻击时尤为明显;(6) PPM 方法仅支持 IPv4 协议,无法支持 IPv6 协议.

© 中国科学院软件研究所 http://www.jos.org.cn

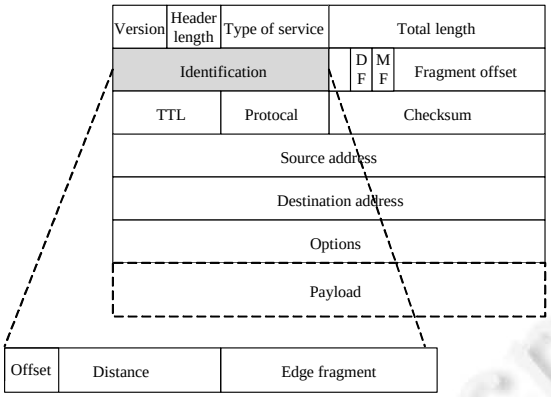

Fig.3 Edge information fragment stored in IP packet header[36]

图 3 存储在 IP 包头中的边信息分片[36]

学者们针对 PPM 方法的不足提出多种改进方法.

(1) 针对 PPM 方法存储空间有限和计算开销大的问题,很多学者为了有效利用数据包包头有限的空间,提出采用 hash 函数等作进一步压缩.如文献[39]提出的 AMS(advanced marking scheme)方法,将 IP 地址的 hash 值而不是 IP 地址本身标记到数据包中,可以缩短数据的长度,还可以扩展到 DDoS 的溯源.但是因为 hash 函数具有单向性,在分析时需要了解整个网络拓扑,亦即要知道 hash 值对应的 IP 地址,且路径重构也因为 hash 运算产生较大的运算量,很难避免 hash 冲突的产生.文献[43,44]提出了一种基于中国余数定理(Chinese remainder theorem,简称 CRT)的数据包标记方案 CRT-PPM(probabilistic packet marking based on Chinese remainder theorem).CRT 指出一个正整数可由几个互质正整数的余数来唯一确定.该方案直接使用 CRT 的模余运算取得 IP 分片的特征值,可有效避免 hash 碰撞的发生,且只需 5 个有效的数据包就能承载一个节点信息,有效地降低了重构路径的计算开销;

(2) 针对 PPM 方法不适用于多攻击源,尤其是 DDoS 攻击的追踪溯源的问题,文献[45]提出根据受害端收到的标记数据包,以受害端为根构造一棵攻击树,在每个节点上标记本地通信率,并基于流量强度来推测所有可能的 DDoS 攻击源和路径.为了使构造的攻击树趋于稳定,同时提高计算效率,使用数学方法来计算收集数据包的最小稳定时间.而由文献[46]提出的确定包标记算法,专门针对 DDoS 攻击源进行追踪溯源,具有效率高、消耗小的特点,后文对此将给出进一步阐述;

(3) 针对 PPM 方法概率固定导致的问题,文献[47]提出使用动态概率,距离被攻击端越远的节点,标记概率越大.为了预估当前节点在攻击路径中的位置,文献[47]提出 3 种距离计算方法:第 1 种是从攻击源到当前节点的距离,第 2 种是从最后一个标记包的节点到当前节点的距离,第 3 种是从当前节点到目的地的距离.并且,基于这 3 种距离分别提出标记概率计算方法,以此实现动态调整每个节点的包标记概率,从而降低概率不公平性,大大减少了重构攻击路径所需的数据包.文献[48–50]也提出了类似的动态概率调整方法;

(4) 针对 PPM 方法的安全性问题,可以通过认证和隐私保护的标记方法以预防恶意路由器伪造包标记信息来干扰追踪,同时也能减轻 ISP 关于网络拓扑泄露的担忧.文献[39]提出了验证包标记算法,这是一种 time-release keys 认证机制,这种认证机制可有效识别攻击者伪造包标记的行为.文献[51]提出时间戳密钥分发方案 TSKDS(time stamp secret key distribution scheme),并采用 HMAC-SHA1[52]加密算法对标记信息进行加密;

(5) 针对 PPM 方法的标记信息传输鲁棒性较弱的问题,文献[40]提出了一种新的概率包标记方法 OPM (opportunistic piggyback marking).OPM 将 PPM 中的标记信息内容编码和传递功能进行解耦,并将网络流量分为内部流量(需要追踪的网络流)和外部流量.在传递包标记信息时,通过充分利用外部流量

© 中国科学院软件研究所 http://www.jos.org.cn

来携带内部流量的包标记信息以降低延迟,提高成功率.并且,使用 $M^X/M/1/C$ finite queue[53]处理批量到达,可有效追踪多个攻击源.该方法能够有效地实现快速、健壮的标记消息传递;

(6) 针对 PPM 方法不支持 IPv6 协议的问题,文献[41]将边采样的三元组(start,end,distance)转换成 IPv6 版本,并将标记内容存储在 IPv6 数据包包头的 Hop-by-Hop Header 字段中进行传递.因该字段足够大,无需对标记内容进一步分片,从而能够避免基于 IPv4 协议的版本带来的状态爆炸问题.文献[54]基于 IPv6 协议及 IPv6 包结构特征[55],对 ASM 方法中的标记机制加以改进,因为 AMS 将 IP 地址的 hash 值而不是 IP 地址本身标记到数据包中,hash 值不会随着 IPv6 数据包的增大而增大.同时,使用 IPv6 数据包包头中的流标签字段(flow label field,简称 FLF)的 20 bit 来标记信息,可以安全、有效地重载 ASM 方案.文献[56]对 CRT-PPM 方法中的标记机制加以改进,通过 CRT 算法对 IPv6 地址编码后,分片存储在多个 IPv6 包头的 FLF 中.相比 IPv4 版本 CRT-PPM 算法需要 5 个片段来存储标记,IPv6 版本需要 16 个片段来存储标记,计算量相应增加.

2) 确定包标记(deterministic packet marking,简称 DPM)方法

文献[57]认为,PPM 方法适用于解决有大规模流量的攻击场景,如 flooding 攻击的追踪溯源,不适用于只包含少量数据包的攻击的追踪溯源.针对这一问题,文献[57]提出了确定包标记方法,仅标记该源节点 IP 地址以降低存储开销.为此,将 IP 地址分成 2 个片段,通过 2 个数据包进行传输即可.受害端接收到包标记,可还原数据包来源 IP 地址.相比 PPM 方法,DPM 方法效率高、消耗小,但却无法还原完整的攻击路径.文献[46]认为,DPM 方法缺乏扩展性,因而又提出了 FDPM(flexible deterministic packet marking)方法.该方法使用变长的包标记格式来适应不同的网络环境,单个分片的长度有 16、19 或者 24bits 这 3 种选择.并且,考虑到 DPM 可能带来的工作负载,提出参考 PPM 的思想,根据路由器能够承受的工作负载,以一定的概率来标记数据包.而文献[58]针对 DPM 全标记导致的效率较低的缺点,提出一种新的按需标记(marking on demand,简称 MOD)追踪溯源方案.为了区分哪些节点参与攻击会话,需要参与路由器安装流量监控器,当监视到网络流激增等可疑行为时,从全局共享的 MOD 服务器请求一个唯一的标记来标识可疑流,并对可疑流进行确定包标记以用于后续的追踪溯源.

3) 代数编码包标记方法

文献[59]认为,PPM 方法在基于边信息重构攻击路径时存在组合爆炸问题,于是提出将攻击路径的构造作为一个多项式重构问题加以求解,并使用代数编码理论[60]来提高标记信息传输和路径重构的鲁棒性.假设 A_1, A_2,…,A_n 为路径 P 上的路由器 IP 地址,数据包 x 的路径信息可以表示为

$$f_p(x)=A_1x^{n-1}+A_2x^{n-2}+\ldots+A_{n-1}x+A_n \tag{1}$$

不同的数据包用 x_j 表示,其路径信息用 $f_p(x_j)$表示,攻击路径可以通过求解如下 Vandermode 行列式取得:

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix} \begin{pmatrix} A_n \\ A_{n-1} \\ \vdots \\ A_1 \end{pmatrix} = \begin{pmatrix} f_p(x_1) \\ f_p(x_2) \\ \vdots \\ f_p(x_n) \end{pmatrix} \tag{2}$$

标识多个 IP 地址求解问题、数据包的路径重构问题可以通过求解该矩阵来完成.文献[61,62]认为,该方法所需的数据包较多,于是基于该方法进行了优化,进一步减少了重构攻击路径所需的数据包,并支持多攻击路径追踪溯源.

此外,文献[63]认为,基于路由器 IP 地址的追踪溯源方法只能追踪到距离攻击者最近的路由器地址,当该路由器连接多个网络或者主机时,无法进一步确定攻击者主机.于是提出基于路由器接口编号信息进行编码以间接标记一个数据包的路径信息,而不是基于路由器 IP 地址的节点采样或者边采样的方法,可以进一步追踪到攻击者主机或者上一级网络.文献[63]提出的 Huffman 编码包标记方法、文献[64]提出的 MRT(modulo and reverse modulo technique)方法、文献[20]提出的 RIHT(traceback scheme with router interface coding)方法和文献[21]提出的 HAHIT(a 16-bit hybrid single packet traceback scheme)方法都是通过数学方法对路由器接口编号信息进行编码的追踪溯源,因而能够有效地应对 DDoS 等攻击追踪溯源问题,存储消耗也得到进一步降低.

© 中国科学院软件研究所 http://www.jos.org.cn

3.3.2 优点分析

(1) 与传统的网络协议和架构兼容,能够广泛应用于多种网络环境中;

(2) 没有额外的网络带宽消耗和路由器存储消耗;

(3) 跨自治域的追踪溯源不需要 ISP 的配合,实施较为简单.

3.3.3 缺点分析

(1) 无法支持单包追踪溯源,需要较多的标记数据包才能恢复出攻击路径,所需数量取决于标记概率参数;且标记数据包是易失性数据,其重构攻击路径的成功率受攻击方式和攻击时长的影响较大;

(2) 因为需要较多的标记数据包才能恢复出攻击路径,因此计算开销大;

(3) 大部分算法对 DDoS 攻击追踪溯源支持不佳,计算量大且错误率较高;

(4) 包标记信息存在安全隐患,如果系统或者转发设备被攻击者控制,攻击者可以删除或者篡改包标记信息以误导攻击路径重构.

3.3.4 取证能力分析

基于数据包标记的追踪溯源技术产生的特有电子数据证据是其记录在数据包中的攻击路径相关的标记信息,这类方法的取证能力见表 3.

(1) 支持关联性.包标记信息记录了攻击包的路径相关信息,与要证明的网络攻击源有直接联系;

(2) 无需考虑合法性.网络攻击追踪溯源技术是网络取证过程中取证分析这一项活动中用到的具体技术,单独依靠某项具体的技术是无法达到合法性要求的,过程的合法性才是证据可采性审查的关键,这就要求结合网络取证过程设计来弥补具体技术在合法性上的缺失.合法性问题将在第 4 节进一步分析;

(3) 不支持可靠性.可靠性是指取证各个环节的可靠性,此类追踪溯源技术产生的是实时网络流量数据,除了考虑数据本身的可靠性,还需考虑传输过程的可靠性,而电子数据证据的收集和存储环节的可靠性一般由取证人员负责.数据本身的可靠性和真实性、完整性相关,因其不支持完整性,故而也不支持可靠性.而标记数据包在传输过程中因无加密机制,可被攻击者截获并篡改,因而无法支持可靠性;

(4) 支持真实性.包标记信息记录了客观真实的路径信息;

(5) 不支持完整性.因网络数据包是易失性数据,且此类追踪溯源技术不存在实时存储机制,其有效的标记数据包随攻击的结束而消失,且标记数据包在传输过程中因无加密机制,可被攻击者截获并篡改;

(6) 不支持非易失性.因为数据包是易失性数据,且没有长期存储机制.

Table 3 Forensics capabilities and improvements of cyber attack traceback techniques based on packet marking

表 3 基于数据包标记的追踪溯源技术取证能力和改进

取证能力	支持情况	改进
关联性	支持	–
合法性	–	–
真实性	支持	–
可靠性	不支持	传输过程加密认证
完整性	不支持	增加实时安全存储机制
非易失性	不支持	增加实时安全存储机制

3.3.5 取证能力改进建议

常见的基于数据包标记的追踪溯源技术取证能力在完整性、可靠性和非易失性这 3 方面的改进建议见上述表 3.

(1) 改进可靠性,可以增加加密认证机制以有效防止恶意篡改标记信息.如文献[65]提出,通过 AES-256 ECB 加密算法进行加密.文献[51]提出了时间戳密钥分发方案,采用 HMAC-SHA1[52]加密算法对标记信息进行加密,从数据传输的角度保证电子数据证据的可靠性;

(2) 改进完整性,可从架构优化的角度增加安全日志转储机制.如文献[30]提出了一个安全存储模型,该安

© 中国科学院软件研究所 http://www.jos.org.cn

全模型在独立于取证对象的网络中,包括一个 hash 加密引擎、日志报告模块和证据数据库,从证据被收集的那一刻起至证据分析和展示,该模型可一直保护证据的完整性.文献[31,32]提出一个分布式网络取证架构,该架构能够进行分布式的网络流量提取和存储、数据压缩,能够监控大规模网络.另外,随着区块链技术的发展,为保障电子数据证据的完整性产生了新的解决方案,区块链技术所具有的去中心化、防篡改、可追溯的特性,能够有效保证电子数据证据的完整性[33−35];

(3) 改进非易失性,与改进完整性相同,可从架构的角度增加标记信息安全存储机制.

3.4 基于SDN的日志追踪溯源技术分析

3.4.1 发展现状

前述网络攻击追踪溯源技术都是基于传统网络架构设计的,其操作性普遍受到网络基础设备的限制,如要求转发设备具备较高的存储空间、计算能力和进行数据包标记的能力等,这些能力并不是目前转发设备的标配,在不支持的设备上无法开展追踪溯源,而更换硬件转发设备成本太高很难执行,因而限制了大部分追踪溯源技术的使用.另外,在实际取证调查过程中,基于日志的追踪溯源方法要求取证人员对整个网络环境中的网络设备具有访问权限、能提取包记录信息等,这对传统网络架构的安全性也是一个挑战.而 SDN 作为一种新型的网络架构,提出将控制平面和数据平面分离的理念[66,67],控制平面将网络设备控制能力集中并提供统一的接口,通过灵活的编程,能够适应复杂的业务层需求,为网络攻击追踪溯源的发展带来了新的机遇.学者们基于 SDN 网络提出了多种网络攻击追踪溯源技术.

文献[68]提出了一种路由跟踪工具 SDN traceroute,该工具利用 SDN 的转发机制来追踪数据包在网络中的转发路径,通过发送带有特定 tag 的探针报文,并逐跳路由比较探针报文,达到追踪溯源的目的.该工具利用 SDN 的多流表机制,在 SDN 交换机上多配置一个流表,用于单独处理探针包,不用改变原来的网络行为.文献[69]提出了 netshark 工具,这是一个类似于 wireshark 的工具,它允许用户在整个数据包的历史记录上设置过滤器,记录它们的路径和每一跳的数据包头信息.用户可以在某一跳查看数据包属性,如包头信息、交换机 ID、输入端口、输出端口和匹配的流表版本等,以及数据包历史记录属性,如路径、路径长度等,从而实现攻击数据包的追踪溯源.文献[70]利用 SDN 控制器语言完成数据包的回溯,依据当前的包处理策略预测数据包动作表达式,进一步计算出任意数据包的所有前置转发策略,从而实现数据包的回溯.文献[71]提出一种基于 SDN 的匿名 IP 溯源方法,该方法用有向图对 SDN 网络拓扑进行建模,并在该图中保存流表信息,通过深度优先搜索算法搜索该图,可定位异常流在该 SDN 网络中的入口点,也就是第 1 步路由,且不用监控 IP 地址就能找到与攻击相关的所有的流.文献[72]提出了基于 SDN 的全局流表算法,通过控制器接口定期遍历所有交换机获取流表,将 SDN 中的每一条流维护起来,通过分析全局流表实现异常流量的追踪溯源.文献[73]在 SDN 架构中实现了优化的 PPM 方法,通过及时地将标记信息转存到特定的机器上,可以有效地缓解 PPM 算法因数据包空间有限带来的限制,并借助 SDN 架构的优势构建全局网络拓扑,简化 PPM 方法的路径重构过程,降低计算开销.文献[74]提出一种基于 SDN 和多协议标签交换(multi-protocol label switching,简称 MPLS)的追踪溯源方法,该方法利用 MPLS 技术设计一种短路径标志,用于表示攻击路径信息,只需要数十个比特,并维护一个 MAC 表和 ARP 表来记录攻击路径信息.该方法支持单包溯源,存储开销较小,错误率较低.文献[75]则提出了基于 SDN 的、适用于 IPv6 协议的追踪溯源方法,该方法通过交换机,在接入网的第 1 个跳窥探数据包中的地址信息,并将这些包转发给控制器;接着,由控制器为每个经过身份验证的终端设备生成一个可信的 IPv6 地址;然后在通信过程中,交换机隐式地在设备的原始源地址和所有传输数据包的可信地址之间进行 IP 地址转换.网络管理员可以通过解析恶意数据包获得可信地址,以有效地识别攻击者.

3.4.2 优点分析

(1) 控制器作为 SDN 的核心,能够从抽象的软件层面对网络行为和状态进行监控和管理,可对转发设备进行统一控制,且具有全局网络视图,有助于简化追踪溯源方法的设计.基于 SDN 的追踪溯源可将计算与存储开销从转发设备上解耦出来,使得追踪溯源方法对转发设备的要求大为降低,增强了网络攻击追踪溯源的效率和可操作性;

© 中国科学院软件研究所 http://www.jos.org.cn

(2) SDN 基于 OVERLAY 覆盖网的网络接入业务方式,可实现分布式网络的大二层互联互通,拓宽了网络攻击追踪溯源的范围.

3.4.3 缺点分析

(1) 此类方法仅适用于 SDN 网络环境和 SDN 交换设备,与传统的网络架构兼容性较差;

(2) SDN 因控制能力较为集中,更容易成为网络攻击的目标.而一旦控制层被攻击破坏掉,对整个网络的稳定性影响很大,因而对安全性要求更高.

3.4.4 取证能力分析

这类追踪溯源技术产生的特有电子数据证据是记录在控制层的各种攻击路径相关的日志信息,其取证能力见表 4.

(1) 支持关联性.日志信息记录了攻击包的路径相关信息,与要证明的网络攻击源有直接联系;

(2) 无需考虑合法性.网络攻击追踪溯源技术是网络取证过程中取证分析这项活动中用到的具体技术,单靠某项具体的技术是无法达到合法性要求的,过程的合法性才是证据的可采性审查的关键,这就要求结合网络取证过程设计来弥补具体技术在合法性上的缺失.合法性问题将在第 4 节进一步分析;

(3) 可靠性支持较弱.此类追踪溯源技术只生产数据,仅需考虑数据本身的可靠性,而电子数据证据收集、传输和存储环节的可靠性一般由取证人员负责.数据本身的可靠性和真实性、完整性相关,因完整性较弱,故其可靠性也较弱;

(4) 支持真实性.日志信息记录了客观、真实的路径相关信息;

(5) 完整性支持较弱.因为缺乏安全机制加以保障,导致日志信息可能遭受攻击而被删除或者篡改;

(6) 支持非易失性.因日志等信息存储在 SDN 控制层,故可在事后进行取证分析.

Table 4 Forensics capabilities and improvements of cyber attack logging traceback techniques based on SDN

表 4 基于 SDN 的日志追踪溯源技术取证能力和改进

取证能力	支持情况	改进
关联性	支持	–
合法性	–	–
真实性	支持	–
可靠性	支持较弱	增加安全日志存储机制
完整性	支持较弱	增加安全日志存储机制
非易失性	支持	–

3.4.5 取证能力改进建议

常见的基于 SDN 的日志追踪溯源技术的取证能力在完整性、可靠性这两方面的改进建议见上面的表 4.

(1) 改进完整性,可从架构优化的角度增加安全日志储存机制.如文献[76]提出,在 SDN 网络增加一个取证管理层,具有较强的存储能力、计算能力和较高的安全性,能够对 SDN 网络中的各种攻击进行实时分析和取证,从而降低 SDN 控制器的分析负载,为网络攻击追踪溯源提供了一种可借鉴的架构;

(2) 一旦当完整性得到保证,则可认为该类技术取证能力的可靠性也得到了保证.

3.5 混合追踪溯源技术分析

3.5.1 发展现状

通过第 3.2 节和第 3.3 节的分析可以发现:基于数据包标记的追踪溯源技术不会给路由器带来存储开销,但却需要较多的数据包才能实现追踪溯源,且错误率较高.而基于日志记录与查询的追踪溯源算法虽然能够实现单包溯源,但是会对路由器带来较重的存储负担.因而,学者们提出了两种算法相混合的方法,优势互补,在减少追踪溯源所需标记包数量的同时,降低路由器的存储开销.

文献[23,77]提出了一种基于日志记录和数据包标记的混合 IP 追溯方法,将路径信息部分记录在转发设备上,部分记录在数据包中,并通过数据包标记字段中可用空间是否充足来决定攻击路径信息记录的方式.如果标

© 中国科学院软件研究所 http://www.jos.org.cn

记字段中有可用空间,则路由器将其设备标识信息写入数据包;否则,路由器计算并记录数据包摘要,然后清除标记字段.文献[7]提出了两种结合包标记和包记录的混合追踪溯源机制,分别是 DLLT(distributed link-list traceback)和 PPPM(probabilistic pipelined packet marking).DLLT 方法在进行包标记之前都会把数据包中已有的标记信息存储到路由器中,然后再用新的标记信息覆盖旧的标记信息,并在受害端通过 Linklist 结构来收集存储在路由器上的标记信息,用于重构攻击路径.由于 DLLT 方法需要在路由器上长期存储标记信息,在 DLLT 的基础上提出了改进的 PPPM 方法.PPPM 方法借鉴了流水线机制,将标记信息从一个标记路由器向另一个标记路由器传播,使得标记信息能够传播到同一个目的地.

文献[63]提出的 Huffman 编码包标记方法、文献[64]提出的 MRT(modulo and reverse modulo technique)方法也是结合了包标记和日志查询技术,但是这两种方法都是通过使用路由器接口编号来标记一个数据包的路径信息,而不是采用节点采样或者边采样的方法,可实现基于单包的 IP 追踪溯源.同时,为了解决包标记类方法普遍面临的 IP 包头存储空间有限的问题,它们采用包标记与包记录相结合的方法,当 IP 包头没有多余空间记录路径信息时,则将标记信息以日志的形式临时存储在路由器上,以避免数据被覆盖.因路由器存储开销随着数据包的增加而增加,而路由器存储能力有限,当达到存储极限时需要清空 hash 表,这会导致一定程度的错误率.文献[20]提出的 RIHT(traceback scheme with router interface coding)方法、文献[21]提出的 HAHIT(a 16-bit hybrid single packet traceback scheme)方法在这类方法的基础上,为了彻底解决路由器存储开销问题,提出了一种双重 hash 表记录方法.该方法的存储开销只与网络流量路径数量有关,而与数据包的数量无关,因而给路由器带来的存储开销是固定的.基于 CAIDA(center for applied Internet data analysis)网络拓扑数据集验证,存储开销为 320KB,且不会随着数据包的增加而增加,因而不存在刷新覆盖路由器上的日志记录的情况,从而消除了错误率.然而,该方法假定网络拓扑是固定不变的,一旦网络拓扑发生变化,日志记录中的路径信息就不再有效,无法重构出正确的攻击路径.针对这一问题,文献[78]在此基础上提出了改进方法,路径的标记编码不再依赖于路由器的接口数,当网络拓扑发生改变,也就是路由器新增接口时,并不会影响溯源的正确性,可在一定程度上适应网络拓扑的变化.

3.5.2 优点分析

(1) 与传统的网络协议和架构兼容,能够广泛应用于多种网络环境中;

(2) 结合了基于日志和基于包标记这两类追踪溯源方法的优点,能够以较低的网络带宽消耗、较低的路由器存储消耗和较少的标记数据包实现追踪溯源;

(3) 相比 PPM 方法,当 IP 数据包包头没有多余空间记录路径信息时,则将标记信息以日志的形式临时存储在路由器上,以避免标记信息被覆盖,所需标记数据包减少,从而计算量也相应减少,且追踪溯源的正确率相应提高.

3.5.3 缺点分析

混合追踪溯源技术只是对基于日志记录和基于包标记追踪溯源技术面临的问题的一个缓解,无法完全避免这些问题,如存储开销和计算开销问题、日志时效性等问题;并且,跨自治域追踪溯源的隐私泄露、网络拓扑泄露等风险,以及日志记录面临的安全隐患依然存在.

3.5.4 取证能力分析

基于混合追踪溯源技术产生的特有电子数据证据是其记录在路由器上的攻击路径相关的日志信息和数据包标记信息,这类方法的取证能力见表 5.

(1) 支持关联性.日志信息和数据包标记信息中记录了攻击包的路径相关信息,与要证明的网络攻击源有直接联系;

(2) 无需考虑合法性.网络攻击追踪溯源技术是网络取证过程中取证分析这一项活动中用到的具体技术,单靠某项具体的技术是无法达到合法性要求的,过程的合法性才是证据的可采性审查的关键,这就要求结合网络取证过程设计来弥补具体技术在合法性上的缺失.合法性问题将在第 4 节进一步分析;

(3) 可靠性支持较弱.可靠性是指取证各个环节的可靠性,此类追踪溯源技术产生的电子数据证据除了日

© 中国科学院软件研究所 http://www.jos.org.cn

志信息还有部分实时网络流量数据,除了考虑数据本身的可靠性,还需要考虑传输过程的可靠性,而电子数据证据的收集和存储环节的可靠性一般由取证人员负责.数据本身的可靠性和真实性、完整性相关,因其真实性和完整性支持较弱,故而可靠性较弱.而标记数据包在传输过程中因无任何安全机制,可被攻击者截获并篡改,也导致可靠性较弱;

(4) 真实性支持较弱.因为 hash 值和 BF 技术的使用,会因 hash 冲突为日志信息带来一定的错误率;

(5) 完整性支持较弱.因为路由器存储能力有限且日志没有安全机制加以保障,导致日志信息因被覆盖而遗失,还可能遭受攻击篡改;

(6) 非易失性支持较弱.因为仅有部分路径信息被以日志信息的形式储存在路由器端.

Table 5 Forensics capabilities and improvements of hybrid cyber attack traceback techniques

表 5 混合追踪溯源技术取证能力和改进

取证能力	支持情况	改进
关联性	支持	–
合法性	–	–
真实性	支持较弱	消除 hash 冲突,提高准确率
可靠性	支持较弱	传输过程加密认证
完整性	支持较弱	增加安全日志转储机制
非易失性	支持较弱	增加实时安全存储机制

3.5.5 取证能力改进建议

混合追踪溯源技术取证能力在真实性、完整性、可靠性和非易失性这 4 方面的改进建议与第 3.2.5 节和第 3.3.5 节所述相同,这里不再赘述.

3.6 网络攻击追踪溯源技术综合对比分析

网络攻击追踪溯源技术综合对比分析见表 6

Table 6 Comprehensive comparative analysis of cyber attack traceback techniques

表 6 网络攻击追踪溯源技术综合对比分析

类别	典型技术	传统网络	存储开销	计算开销	ISP 配合	取证能力					
						关联性	合法性	真实性	可靠性	完整性	非易失性
日志存储查询追踪溯源	SPIE	支持	大	小	需要	支持	–	支持较弱	支持较弱	支持较弱	支持
数据包标记追踪溯源	PPM	支持	小	大	不需要	支持	–	支持	不支持	不支持	不支持
SDN 追踪溯源	SDN traceroute	不支持	大	小	需要	支持	–	支持	支持较弱	支持较弱	支持
混合追踪溯源	SPIE+PPM	支持	较小	较小	需要	支持	–	支持较弱	支持较弱	支持较弱	支持较弱

基于日志存储查询的追踪溯源技术和基于 SDN 的日志追踪溯源技术是存储开销型技术,基于数据包标记的追踪溯源技术是计算开销型技术,混合追踪溯源技术则在存储开销和计算开销中取得折中.基于 SDN 的日志追踪溯源技术与传统网络兼容性较差,其他 3 种追踪溯源技术则都是基于传统网络架构进行设计的.当追踪溯源跨越自治域时,只有基于数据包标记的追踪溯源技术不需要获得 ISP 的支持,这使得在有些严苛的网络环境下取证仅有这类技术可行.可见,每一种网络攻击追踪溯源技术都有其自身的弱点和适用性,这为网络取证架构选取何种网络攻击追踪溯源技术提供了参考.

而这 4 类网络攻击追踪溯源技术均无法完全满足取证能力要求,普遍在可靠性、完整性方面有所欠缺,且基于数据包标记的追踪溯源技术和混合追踪溯源技术对非易失性支持欠佳.这为网络取证架构从何种角度进行优化提供了思路.

© 中国科学院软件研究所 http://www.jos.org.cn

4 针对网络攻击追踪溯源场景的网络取证过程模型

网络取证过程是为了完成网络取证任务,将相互联系的各个活动进行排列组合所组成的体系.前文提到的网络攻击追踪溯源技术是网络取证过程中取证分析这一项活动中用到的具体技术,单靠具体技术是无法达到合法性要求的,过程的合法性才是证据的可采性审查的关键,因而需要结合网络取证过程设计来弥补具体技术在合法性上的不足.

取证过程可能因取证条件、取证对象来源、取证措施适用等要求的不同而有所不同,目前还没有一个针对网络攻击追踪溯源场景的网络取证过程.为此,本节将通过分析现有的网络取证过程模型的发展,指出其在网络攻击追踪溯源场景下的不足之处,并初步提出针对网络攻击追踪溯源场景的网络取证过程模型,为弥补网络攻击追踪溯源技术在合法性上的不足提供参考.

4.1 发展现状

自 2001 年开始,就有专家学者陆续提出各种通用电子数据取证过程模型,这些通用过程模型同样也适用于网络环境.文献[8]首次提出了一个线性过程模型概念,奠定了电子数据取证过程模型的基础,文献[79]对其内涵进行了完善和补充.该电子数据取证过程模型包括如下阶段.

(1) 识别.从指示器识别事件并确定其类型;
(2) 保存.隔离、保护和保存物理证据和数字证据的状态;
(3) 收集.使用标准和认可的程序记录物理场景和复制的数字证据;
(4) 检查.对涉嫌犯罪的证据进行深入、系统的搜查,重点是识别和定位潜在的证据,并为分析构建详细的文档;
(5) 分析.确定重要性,重建数据片段,根据发现的证据得出结论;
(6) 展示.总结和解释结论;
(7) 决策.根据分析报告进行决策.

同时,文献[79]也指出了该模型的缺点:过程模型过于宽泛而不适用于实际使用;没有简单或明显的方法来测试该模型的有效性;模型中没有一个明显的监督链,而监督链对保持电子数据证据的完整性具有重要意义.改进的模型被陆续提出[80−88].

但是,直到 2005 年,文献[89]才首次提出网络取证的通用过程模型,该模型提出以下 6 个阶段.

(1) 捕获.从数据源获取数据.数据源包括中间节点和受害端节点数据.捕获数据不能破坏隐私,而且被监视的网络不应知道捕获;
(2) 复制.将原始数据逐位复制到只读媒体、传输网络或分析机器上;
(3) 传输.将复制的数据传输到取证分析机,传输安全必须得到保证;
(4) 分析.包括数据筛选、元分析和综合分析,如 IP 包统计分析、协议分析、会话分析等;
(5) 调查.利用各种追踪溯源工具和技术定位攻击源和攻击者;
(6) 陈述.陈述结论和得出结论的步骤.

美国国家技术标准局(National Institute of Standards and Technology)指出:取证的目的除了为法律程序和内部纪律行动收集证据,还包括应急响应[90].文献[91]认为,应急响应和计算机取证流程虽然不同,但其目标相似,其将应急响应和计算机取证过程相结合,提供了一个通用的模型.而文献[92]将应急响应也加入到网络取证过程模型中来,使得网络取证过程模型更加完善.该网络取证过程模型包括准备、检测、应急响应、收集、保存、检查、分析、调查和展示 9 个过程.文献[93]在此基础上作了进一步的改进,提出在第 1 步增加认证阶段,认证阶段需要获得相关部门的法律许可,以启动调查过程,以此来保证取证过程的合法性;并且,提出在收集阶段之前需要增加策略规划过程,规划人员投入、时间投入、所涉及的成本使用何种工具等.

然而,现有的网络取证模型无法很好地支持网络攻击追踪溯源的场景,其面临着以下 3 个方面的难题.

(1) 现有的网络取证过程模型设计都是基于网络流量的提取和分析,数据流体量过大导致取证效率低下.

© 中国科学院软件研究所 http://www.jos.org.cn

通过第 3 节的分析可知:在网络攻击追踪溯源过程中,数据源还可以是路由器上的日志信息或者网络数据包中的标记信息,具有不同的时效性.不同的数据源提取策略和提取的时机有所不同,不能一概而论;

(2) 攻击路径的重构属于调查阶段,而在基于概率包标记的追踪溯源算法中,攻击路径的重构与数据收集阶段相互制约,其制约关系未体现在已有的过程模型中;

(3) 追踪溯源和应急响应之间存在博弈,尤其是基于概率包标记方法的追踪溯源需要收集大量的数据包才能恢复出完整的攻击路径,导致追踪溯源时间跨度较大;而应急响应则一般在检测到攻击的第一时间就阻断攻击,导致没有足够的携带标记的数据包来进行攻击路径重构.

4.2 针对网络攻击追踪溯源场景的网络取证过程模型

为此,本文提出针对网络攻击追踪溯源场景的网络取证过程模型,该模型能够更好地适用于网络攻击追踪溯源的场景,同时满足取证能力评估指标中的合法性和可靠性.该网络取证过程模型包括如下 12 个阶段.

(1) 认证.获得相关部门的法律许可,以保证取证过程的合法性.尤其是在跨ISP的网络环境中,认证许可更加重要;

(2) 准备.在网络关键节点部署入侵检测系统、数据包分析仪、防火墙、流量监测等网络探针和摸排路由器对追踪溯源技术的支持情况;

(3) 预收集.追踪溯源电子数据证据收集.在追踪获取系统权限攻击和网络嗅探等攻击时,因攻击数据流很小,往往检测到异常时攻击可能已经结束,此时需要预先收集攻击数据包以免缺失;

(4) 检测.入侵检测系统检测到入侵或者异常并告警,同时可触发网络攻击追踪溯源过程;

(5) 决策.根据检测结果和采用的追踪溯源手段,对接下来的流程进行决策;

(6) 应急响应.根据检测结果或者调查结果进行应急响应;

(7) 容忍.在一个安全的环境下继续收集数据而不影响原网络行为[94],一般通过引流或者流量镜像的方法来实现;

(8) 收集.收集追踪溯源电子数据证据、网络拓扑等信息;

(9) 保存.将收集的电子数据证据保全后进行储存;

(10) 分析.对电子数据证据进行分析,包括对指标进行分类和关联,以使用现有的攻击模式推断重要的观察结果.相比检测阶段,能够更加准确地判断攻击类型、攻击目的等;

(11) 调查.根据收集的电子数据证据重构攻击路径,并根据结果反馈决策阶段;

(12) 展示.将以上结果以可理解的语言向法律人员展示,同时解释得出结论所使用的各种程序.

针对网络攻击追踪溯源场景的网络取证过程逻辑如图 4 所示,其中,决策过程是该过程模型的核心,其工作流程大致如下.

(1) 如果采用的是基于包标记的方法,为了保证收集足够多的数据包,需要对攻击进行容忍;

(2) 如果是基于包记录方法,则可直接进入收集阶段;

(3) 决策过程需要调查过程进行交互,以根据攻击路径重构效果来决定何时可以完成溯源进入应急响应阶段.如果追踪溯源结束,则停止数据收集进入应急响应阶段;

(4) 如果不满足继续追踪溯源的条件,则回到准备阶段.

该过程模型通过提出预收集阶段来实现主动数据收集的目的,将追踪溯源时机尽可能地提前,以解决对少量数据包攻击类型的追踪溯源,并通过容忍阶段来延长数据收集过程,收集足够重构攻击路径的数据包,从而解决上述的难题(1).该模型提出决策阶段以协调数据收集和调查,当调查阶段重构出完整的攻击路径时即可停止数据收集,以解决上述的难题(2).同时,该模型通过决策阶段来决定是否采取容忍机制或进入应急响应阶段以保障调查阶段攻击路径重构的成功,同时保证系统的安全性,以解决上述的难题(3),从而实现一个网络攻击追踪溯源支持良好的网络取证过程模型.

© 中国科学院软件研究所 http://www.jos.org.cn

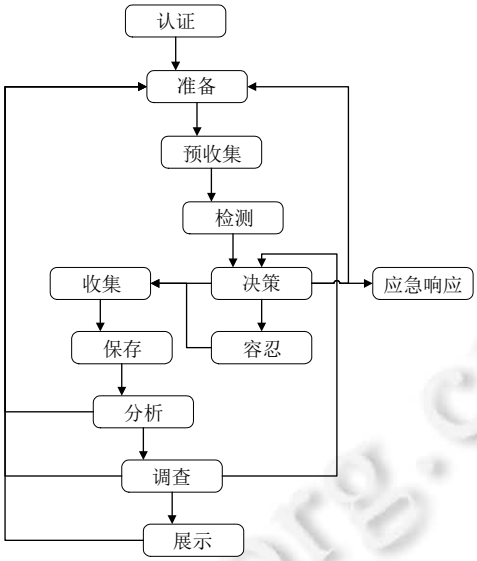

Fig.4 Schematic diagram of the network forensics process model for cyber attack traceback

图 4 针对网络攻击追踪溯源场景的网络取证过程模型示意图

4.3 模型评估

文献[95]提出,取证过程规范与否,是检验取证结果“合法性”程度的重要标准,规范的取证过程模型设计应满足适用性、科学性、合理性等要求.文献[96]基于大量现有取证过程模型总结出取证过程模型在步骤设计和过程安排上的共有特性,并在此基础上提出了取证过程规范化评估方法.即,一个满足规范化要求的取证过程模型应完全覆盖准备、收集与保存、检验与分析、报告与提交以及结束与后处理这 5 类活动指标.对这 5 类活动指标的释义见表 7,这 5 类活动的具体内容会因取证场景的不同而有所不同.

Table 7 Index definition of standardization evaluation method for forensics process model

表 7 取证过程模型规范化评估方法指标释义

指标名称	释义
准备	取证活动开展前的一系列准备活动,是取证活动顺利开展的前提
收集与保存	为了尽可能地从待取证对象中获取与事件相关的一切潜在电子数据而进行的一系列活动
检验与分析	对收集的电子数据进行检验和取证分析的一系列活动
报告与提交	取证报告的制作、提交并对取证所见进行分析说明等一系列活动
结束与后处理	取证活动结束的一系列整理活动

本文基于该评估方法对针对网络攻击追踪溯源场景的网络取证过程模型进行评估.由第 4.2 节对各阶段活动的解释可知:本模型中的认证、准备、检测、应急响应这 4 个阶段均是取证准备活动,预收集、决策、容忍、收集和保存这 5 个阶段共同完成了收集和保存活动,分析和调查阶段完成了检验与分析活动,展示阶段完成了报告提交活动,决策阶段同时负责结束与后处理活动,见表 8.该取证过程模型能够完整地覆盖规范化设计的 5 项指标,因而满足取证过程规范化要求.

Table 8 Standardization assessment of network forensics process targeting at cyber attack traceback

表 8 针对网络攻击追踪溯源场景的网络取证过程模型规范化评估

序号	阶段名称	准备	收集与保存	检验与分析	报告提交	结束与后处理
1	认证	✓				
2	准备	✓				
3	预收集		✓			
4	检测	✓				

© 中国科学院软件研究所 http://www.jos.org.cn

Table 8 Standardization assessment of network forensics process targeting at cyber attack traceback (Continued)

表 8 针对网络攻击追踪溯源场景的网络取证过程模型规范化评估(续)

序号	阶段名称	准备	收集与保存	检验与分析	报告提交	结束与后处理
5	决策		✓			✓
6	应急响应	✓				
7	容忍		✓			
8	收集		✓			
9	保存		✓			
10	分析			✓		
11	调查			✓		
12	展示				✓	

5 总结与展望

本文从网络取证的角度对网络攻击追踪溯源技术进行了研究综述,主要贡献包括:基于电子数据证据可采性标准和证明力标准的 5 个方面和非易失性能力提出了一套六维的取证能力评估指标;分析了基于日志存储查询的追踪溯源技术、基于数据包标记的追踪溯源技术、基于 SDN 的日志追踪溯源技术和混合追踪溯源技术;基于取证能力评估指标分析了网络攻击追踪溯源技术的取证能力,对其不足给出改进建议;分析了现有网络取证过程模型在追踪溯源场景下的不足,并提出了针对网络攻击追踪溯源场景的网络取证过程模型,通过结合网络取证过程与网络攻击追踪溯源技术以进一步提高整体取证能力.本文的工作为面向网络取证的网络攻击追踪溯源技术的研究提供了参考.

通过本文的分析可以发现:

- 网络攻击追踪溯源技术在实际应用中面临的挑战包括存储开销、计算开销和网络带宽开销过大等等.而为了发挥网络攻击追踪溯源技术在网络取证方面的作用,需要完善其取证能力,这势必会增加相应的开销.如文献[65]提出的数据包标记方法在 PPM 方法的基础上增加了时间戳等标记信息和加密运算可以增强其取证能力,但却导致标记信息大小从 PPM 方法的 72bits 增加到了 256bits,由此带来的网络带宽消耗增加了 3 倍多.类似的矛盾进一步影响到其实用性,因而,如何在两者之间取得平衡,使得面向网络取证的网络攻击追踪溯源技术能够具有实用性,是未来研究的重点之一;
- 因为传统网络体系结构和网络协议的设计缺乏对网络攻击追踪溯源和网络取证的支持,导致网络攻击追踪溯源技术的设计存在较多的局限,如通过数据包标记路径信息可能会对数据包分片功能造成影响[36]等;现有技术过于依赖网络基础设备的支持,导致很多网络攻击追踪溯源技术无法落地应用.即便在 SDN 这类新型的网络架构中,也只是对设备的依赖性有所缓解,因网络体系结构等设计带来的挑战依然存在.这就给下一代互联网体系结构设计带来一些启发:是否需要在下一代互联网体系结构设计中实现对追踪溯源和网络取证的支持,是一个值得慎重考虑的问题;
- 随着物联网的迅猛发展,其安全问题日益突出,针对物联网攻击的追踪溯源研究迫在眉睫.物联网特有的传感网络[97]是物联网安全的薄弱环节,传感网络中广泛存在的传感节点极易成为攻击者的攻击目标.而传感网络结构不同于传统网络结构,现有的网络攻击追踪溯源技术和取证技术不再适用于传感网络,因而,基于物联网攻击的追踪溯源和取证是一个新的课题、新的挑战,值得深入研究.

References:

[1] Zhu SX, Chen ZG, Zhang XS, Chen RD. Traceback Cyber Attacks. Beijing: National Defence Industry Press, 2015. 102−131 (in Chinese).

[2] Khan S, Gani A, Wahab AWA, Shiraz M, Ahmad I. Network forensics: Review, taxonomy, and open challenges. Journal of Network and Computer Applications, 2016,66:214−235.

[3] Ding LP. Network forensics and theory research of computer forensics. Netinfo Security, 2010,10(12):38−41 (in Chinese with English abstract).

© 中国科学院软件研究所 http://www.jos.org.cn

[4] Chen ZG, Pu S, Hao Y, Huang C. Levels analysis of network attack traceback. Computer Systems Applications, 2014,23(1):1−7 (in Chinese with English abstract).

[5] Jiang JG, Wang JZ, Kong B, Hu B, Liu JQ. On the survey of network attack source traceback. Journal of Cyber Security, 2018,3(1): 111−131 (in Chinese with English abstract).

[6] Singh K, Singh P, Kumar K. A systematic review of IP traceback schemes for denial of service attacks. Computers & Security, 2016,56:111−139.

[7] Al-Duwairi B, Govindarasu M. Novel hybrid schemes employing packet marking and logging for IP traceback. IEEE Trans. on Parallel and Distributed Systems, 2006,17(5):403−418.

[8] DFRW. A road map for digital forensics research. 2001. http://www.dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf

[9] Mai YH. Digital Forensic Judicial Practice. Beijing: Law Press, 2012. 26−45 (in Chinese).

[10] Ding LP. Research on the models, policies and implement of real-time forensics operating system [Ph.D. Thesis]. Beijing: Graduate University of Chinese Academy of Sciences, 2006 (in Chinese with English abstract).

[11] Matsuda S, Baba T, Hayakawa A, Nakamura T. Design and implementation of unauthorized access tracing system. In: Werner B, ed. Proc. of the 2002 Symp. on Applications and the Internet (SAINT 2002). Los Alamitos: IEEE Computer Society, 2002. 74−81.

[12] Snoeren AC, Partridge C, Sanchez LA, Jones CE, Tchakountio F, Schwartz B, Kent ST, Strayer WT. Single-packet IP traceback. IEEE/ACM Trans. on Networking, 2002,10(6):721−734.

[13] Snoeren AC, Partridge C, Sanchez LA, Jones CE, Tchakountio F, Kent ST, Strayer WT. Hash-based IP traceback. In: Proc. of the 2001 Conf. on Applications, Technologies, Architectures, and Protocols for Computer Communications. New York: ACM, 2001. 3−14.

[14] Bloom BH. Space/Time trade-offs in hash coding with allowable errors. Communications of the ACM, 1970,13(7):422−426.

[15] Zhang LF, Guan Y. TOPO: A topology-aware single packet attack traceback scheme. In: Singhal M, Baras J, eds. Proc. of the 2006 Securecomm and Workshops. Piscataway: IEEE, 2006. 1−10.

[16] Hilgenstieler E, Duarte EP, Mansfield-Keeni G, Shiratori N. Improving the precision and efficiency of log-based IP packet traceback. In: Proc. of the 2017 IEEE Global Telecommunications Conf. Piscataway: IEEE, 2007. 1823−1827.

[17] Hilgenstieler E, Duarte EP, Mansfield-Keeni G, Shiratori N. Extensions to the source path isolation engine for precise and efficient log-based IP traceback. Computers & Security, 2010,29(4):383−392.

[18] Kai T, Hashiguchi A, Nakatani H. Proposal for and evaluation of improved method of hash-based IP traceback system. In: Proc. of the 2nd Int'l Conf. on Computer Science and Its Applications. Piscataway: IEEE, 2009. 1−7.

[19] Katyal K, Malik M, Dutta M. Implementation of single-packet hybrid IP traceback for IPv4 and IPv6 networks. IET Information Security, 2018,12(1):1−6.

[20] Yang MH, Yang MC. RIHT: A novel hybrid IP traceback scheme. IEEE Trans. on Information Forensics and Security, 2012,7(2): 789−797.

[21] Yang MH. Hybrid single-packet IP traceback with low storage and high accuracy. The Scientific World Journal, 2014,2014:1−12.

[22] Lu N, Wang YL, Su S, Yang FC. A novel path-based approach for single-packet IP traceback. Security and Communication Networks, 2014,7(2):309−321.

[23] Gong C, Sarac K. A more practical approach for single-packet IP traceback using packet logging and marking. IEEE Trans. on Parallel and Distributed Systems, 2008,19(10):1310−1324.

[24] Jeong E, Lee B. An IP traceback protocol using a compressed hash table, a sinkhole router and data mining based on network forensics against network attacks. Future Generation Computer Systems, 2014,33(4):42−52.

[25] Strayer WT, Jones CE, Tchakountio F, Hain RR. SPIE-IPv6: Single IPv6 packet traceback. In: Jha S, Hassanein H, Bulusu N, Frank M, Boukerche A, Hood C, eds. Proc. of the 29th Annual IEEE Int'l Conf. on Local Computer Networks. Los Alamitos: IEEE Computer Society, 2004. 118−125.

[26] Boudaoud K, LeBorgne F. Towards an efficient implementation of traceback mechanisms in autonomous systems. In: Brunner M, Westphall CB, Granville LZ, eds. Proc. of the 2008 IEEE Network Operations and Management Symp. Piscataway: IEEE, 2008. 1015−1018.

[27] Wang XJ, Xiao YL. IP traceback based on deterministic packet marking and logging. In: Li K, Min G, Zhu Y, Qiu M, Qu W, eds. Proc. of the Int'l Conf. on Scalable Computing and Communications; the 8th Int'l Conf. on Embedded Computing. Los Alamitos: IEEE Computer Society, 2009. 178−182.

© 中国科学院软件研究所 http://www.jos.org.cn

[28] Strayer WT, Jones CE, Schwartz BI, Mikkelson J, Livadas C. Architecture for multi-stage network attack traceback. In: Hassanein H, Waldvogel M, eds. Proc. of the IEEE Conf. on Local Computer Networks. Los Alamitos: IEEE Computer Society, 2005. 778−785.

[29] Takemori K, Fujinaga M, Sayama T, Nishigaki M. IP traceback using DNS logs against bots. In: Proc. of the Int'l Symp. on Computer Science and its Applications. Los Alamitos: IEEE Computer Society, 2008. 84−89.

[30] Ibrahim MI, Jantan A. A secure storage model to preserve evidence in network forensics. In: Zain JM, Wan MW, El-Qawasmeh E, eds. Proc. of the Software Engineering and Computer Systems. Berlin: Springer-Verlag, 2011. 391−402.

[31] Chhabra G. Distributed network forensics framework: A systematic review. Int'l Journal of Computer Applications, 2015,119(19): 31−35.

[32] Tafazzoli T, Salahi E, Gharaee H. A proposed architecture for network forensic system in large-scale networks. Int'l Journal of Computer Networks & Communications, 2015,7(4):43−56.

[33] Liang XP, Shetty S, Tosh D, Kamhoua C, Kwiat K, Njilla L. Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In: Proc. of the 17th IEEE/ACM Int'l Symp. on Cluster, Cloud and Grid Computing (CCGRID). Los Alamitos: IEEE Computer Society, 2017. 468−477.

[34] Qian WN, Shao QF, Zhu YC, Jin CQ, Zhou AY. Research problems and methods in blockchain and trusted data management. Ruan Jian Xue Bao/Journal of Software, 2018,29(1):150−159 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5434.htm [doi: 10.13328/j.cnki.jos.005434]

[35] Li CX, Chen S, Zheng LS, Zuo C, Jiang BY, Liang G. RepChain—A permissioned blockchain toolkit implemented by reactive programming. Ruan Jian Xue Bao/Journal of Software, 2019,30(6):1670−1680 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5743.htm [doi: 10.13328/j.cnki.jos.005743]

[36] Savage S, Wetherall D, Karlin A, Anderson T. Network support for IP traceback. IEEE/ACM Trans. on Networking, 2001,9(3): 226−237.

[37] Li DQ, Su PR, Feng DG. Notes on packet marking for IP traceback. Ruan Jian Xue Bao/Journal of Software, 2004,15(2):250−258 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/15/250.htm

[38] Park K, Lee H. On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack. In: Proc. of the IEEE INFOCOM 2001 Conf. on Computer Communications. Piscataway: IEEE, 2001. 338−347.

[39] Song DXD, Perrig A. Advanced and authenticated marking schemes for IP traceback. In: Proc. of the IEEE INFOCOM 2001 Conf. on Computer Communications. Piscataway: IEEE, 2001. 878−886.

[40] Cheng L, Divakaran DM, Lim WY, Thing VLL. Opportunistic piggyback marking for IP traceback. IEEE Trans. on Information Forensics and Security, 2016,11(2):273−288.

[41] Amin SO, Kang MS, Hong CS. A lightweight IP traceback mechanism on IPv6. In: Zhou X, Sokolsky O, Yan L, Jung E-S, Shao Z, Mu Y, Lee DC, Kim DY, Jeong Y-S, Xu C-Z, eds. Proc. of the Emerging Directions in Embedded and Ubiquitous Computing. Berlin: Springer-Verlag, 2006. 671−680.

[42] Hussain A, Heidemann J, Heidemann J, Papadopoulos C. A framework for classifying denial of service attacks. In: Proc. of the 2003 Conf. on Applications, Technologies, Architectures, and Protocols for Computer Communications. New York: ACM, 2003. 99−110.

[43] Wuu LC, Liu TJ, Yang JY. IP traceback based on Chinese remainder theorem. In: Alhajj RS, ed. Proc. of the 6th IASTED Int'l Conf. on Communications, Internet, and Information Technology. Calgary: ACTA Press, 2007. 214−219.

[44] Bhavani Y, Janaki V, Sridevi R. IP traceback through modified probabilistic packet marking algorithm using Chinese remainder theorem. Ain Shams Engineering Journal, 2015,6(2):715−722.

[45] Law KT, Lui JCS, Yau DKY. You can run, but you can't hide: An effective methodology to traceback DDoS attackers. In: Boukerche A, Das SK, Majumdar S, eds. Proc. of the 10th IEEE Int'l Symp. on Modeling, Analysis and Simulation of Computer and Telecommunications Systems. Los Alamitos: IEEE Computer Society, 2002. 433−440.

[46] Xiang Y, Zhou WL, Guo MY. Flexible deterministic packet marking: An IP traceback system to find the real source of attacks. IEEE Trans. on Parallel and Distributed Systems, 2009,20(4):567−580.

[47] Peng T, Leckie C, Ramamohanarao K. Adjusted probabilistic packet marking for IP traceback. In: Gregori E, Conti M, Campbell AT, Omidyar CG, Zukerman M, eds. Proc. of the 2nd Int'l IFIP-TC6 Networking Conf. on Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications. Berlin: Springer-Verlag, 2002. 697−708.

© 中国科学院软件研究所 http://www.jos.org.cn

[48] Kim B. Efficient technique for fast IP traceback. In: Luo Y, ed. Proc. of the Int'l Conf. on Cooperative Design, Visualization and Engineering. Berlin: Springer-Verlag, 2006. 211−218.

[49] Liu J, Lee ZJ, Chung YC. Dynamic probabilistic packet marking for efficient IP traceback. Computer Networks, 2007,51(3): 866−882.

[50] Tian HC, Bi J, Jiang XK, Zhang W. A probabilistic marking scheme for fast traceback. In: Mauri JL, Sendra S, Tomás J, Wu WW, eds. Proc. of the 2nd Int'l Conf. on Evolving Internet. Los Alamitos: IEEE Computer Society, 2010. 137−141.

[51] Kim H, Kim E, Kang S, Kim HK. Network forensic evidence generation and verification scheme (NFEGVS). Telecommunication Systems, 2015,60(2):261−273.

[52] Group NW. HMAC: Keyed-hashing for message authentication. RFC 2104, 1997.

[53] Tian NS, Zhang G. Vacation Queueing Models Theory and Applications. Boston: Springer-Verlag, 2006. 1−7.

[54] Dang XH, Albright E, Abonamah AA. Performance analysis of probabilistic packet marking in IPv6. Computer Communications, 2007,30(16):3193−3202.

[55] Group NW. Internet protocol, version 6 (IPv6) specification. RFC 2460, 1998.

[56] Bhavani Y, Janaki V, Sridevi R. Modified probabilistic packet marking algorithm for IPv6 traceback using Chinese remainder theorem. In: Saini HS, Sayal R, Rawat SS, eds. Proc. of the Innovations in Computer Science and Engineering. Berlin: Springer-Verlag, 2017. 253−263.

[57] Belenky A, Ansari N. IP traceback with deterministic packet marking. IEEE Communications Letters, 2003,7(4):162−164.

[58] Yu S, Zhou WL, Guo S, Guo MY. A feasible IP traceback framework through dynamic deterministic packet marking. IEEE Trans. on Computers, 2016,65(5):1418−1427.

[59] Dean D, Franklin M, Stubblefield A. An algebraic approach to IP traceback. ACM Trans. on Information and System Security, 2002,5(2):119−137.

[60] Guruswami V, Sudan M. Improved decoding of Reed-Solomon and algebraic-geometric codes. In: Proc. of the 39th Annual Symp. on Foundations of Computer Science. Los Alamitos: IEEE Computer Society, 1998. 28−37.

[61] Sattari P, Gjoka M, Markopoulou A. A network coding approach to IP traceback. In: Proc. of the 2010 IEEE Int'l Symp. on Network Coding (NetCod). Piscataway: IEEE, 2010. 1−6.

[62] Sattari P, Markopoulou A. Algebraic traceback meets network coding. In: Yang Y, Guo Y, Luo Q, Liu Y, Zhang X, eds. Proc. of the 2011 Int'l Symp. on Networking Coding. Piscataway: IEEE, 2011. 1−7.

[63] Choi KH, Dai HK. A marking scheme using Huffman codes for IP traceback. In: Hsu DF, Hiraki K, Shen S, Sudborough H, eds. Proc. of the 7th Int'l Symp. on Parallel Architectures, Algorithms and Networks. Los Alamitos: IEEE Computer Society, 2004. 421−428.

[64] Malliga S, Tamilarasi A. A proposal for new marking scheme with its performance evaluation for IP traceback. WSEAS Trans. on Computer Research, 2008,3(4):259−272.

[65] Kim HS, Kim HK. Network forensic evidence acquisition (NFEA) with packet marking. In: Proc. of the 9th IEEE Int'l Symp. on Parallel and Distributed Processing with Applications Workshops. Los Alamitos: IEEE Computer Society, 2011. 388−393.

[66] Monsanto C, Reich J, Foster N, Rexford J, Walker D. Composing software-defined networks. In: Feamster N, Mogul J, eds. Proc. of the 10th USENIX Conf. on Networked Systems Design and Implementation. Berkeley: USENIX Association, 2013. 1−14.

[67] Feamster N, Rexford J, Zegura E. The road to SDN: An intellectual history of programmable networks. ACM SIGCOMM Computer Communication Review, 2014,44(2):87−98.

[68] Agarwal K, Rozner E, Dixon C, Carter J. SDN traceroute: Tracing SDN forwarding without changing network behavior. In: Proc. of the 3rd Workshop on Hot Topics in Software Defined Networking. New York: ACM, 2014. 145−150.

[69] Handigol N, Heller B, Jeyakumar V, Mazi D, McKeown N. I know what your packet did last hop: Using packet histories to troubleshoot networks. In: Proc. of the 11th USENIX Conf. on Networked Systems Design and Implementation. Berkeley: USENIX Association, 2014. 71−85.

[70] Zhang H, Reich J, Rexford J. Packet traceback for software-defined networks. Princeton: Department of Computer Sciences, Princeton University, 2015. 1−7.

[71] Francois J, Festor O. Anomaly traceback using software defined networking. In: Proc. of the 2014 IEEE Int'l Workshop on Information Forensics and Security (WIFS). Piscataway: IEEE, 2014. 203−208.

[72] Ren QZ, Qiu XF, Chen PC, Liang XD. The global flow table based on the software-defined networking. In: Proc. of the 2015 IEEE Int'l Conf. on Communication Problem-solving (ICCP). Piscataway: IEEE, 2015. 264−267.

© 中国科学院软件研究所 http://www.jos.org.cn

[73] Ren D, Jiang W, Li H, Sun G. An OpenvSwitch extension for SDN traceback. In: Au MH, Yiu SM, Li J, Luo X, Wang C, Castiglione A, Kluczniak K, eds. Proc. of the Network and System Security. Berlin: Springer-Verlag, 2018. 423−435.

[74] Hadem P, Saikia DK. SMITE: An SDN and MPLS integrated traceback mechanism. In: Bohra MK, Shekhawat RS, Dhaka VS, Gaur MS, Elci A, eds. Proc. of the Security of Information and Networks. New York: ACM, 2017. 171−177.

[75] Li C, Wu Q, Li H, Zhou J. SDN-Ti: A general solution based on SDN to attacker traceback and identification in IPv6 networks. In: Proc. of the Int'l Conf. on Communications. Piscataway: IEEE, 2019. 1−7.

[76] Khan S, Gani A, Wahab AWA, Abdelaziz A, Bagiwa MA. FML: A novel forensics management layer for software defined networks. In: Bansal A, Singhal A, Nagpal R, Sehgal R, Gupta R, Agrawal AP, Choudhary A, Sehgal S, eds. Proc. of the 6th Int'l Conf. on Cloud System and Big Data Engineering (Confluence). Piscataway: IEEE, 2016. 619−623.

[77] Gong C, Sarac K. IP traceback based on packet marking and logging. In: Proc. of the 2015 IEEE Int'l Conf. on Communications. Piscataway: IEEE, 2005. 1043−1047.

[78] Murugesan V, Shalinie M, Yang M. Design and analysis of hybrid single packet IP traceback scheme. IET Networks, 2018,7(3): 141−151.

[79] Reith M, Carr C, Gunsch G. An examination of digital forensic models. Int'l Journal of Digital Evidence, 2002,1(3):1−12.

[80] Montasari R, Peltola P, Evans D. Integrated computer forensics investigation process model (ICFIPM) for computer crime investigations. In: Jahankhani H, Carlile A, Akhgar B, Taal A, Hessami AG, Hosseinian-Far A, eds. Proc. of the Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security. Berlin: Springer-Verlag, 2015. 83−95.

[81] Yusoff Y, Ismail R, Hassan Z. Common phases of computer forensics investigation models. Int'l Journal of Computer Science & Information Technology (IJCSIT), 2011,3(3):17−31.

[82] Ademu IO, Imafidon CO, Preston DS. A new approach of digital forensic model for digital forensic investigation. Int'l Journal of Advanced Computer Science and Applications, 2011,2(12):175−178.

[83] Kohn MD, Eloff MM, Eloff JHP. Integrated digital forensic process model. Computers & Security, 2013,38:103−115.

[84] Shrivastava G, Gupta BB. An encapsulated approach of forensic model for digital investigation. In: Proc. of the 2014 IEEE 3rd Global Conf. on Consumer Electronics (GCCE). Piscataway, NJ: IEEE, 2014. 280−284.

[85] Liu CW, Singhal A, Wijesekera D. A logic-based network forensic model for evidence analysis. In: Peterson G and Shenoi S, eds. Proc. of the Advances in Digital Forensics XI. Berlin: Springer, 2015. 129−145.

[86] Lutui R. A multidisciplinary digital forensic investigation process model. Business Horizons, 2016,59(6):593−604.

[87] Mutawa NA, Bryce J, Franqueira VNL, Marrington A, Read JC. Behavioural digital forensics model: Embedding behavioural evidence analysis into the investigation of digital crimes. Digital Investigation, 2019,28:70−82.

[88] Reza M. A standardised data acquisition process model for digital forensic investigations. Int'l Journal of Information Computer Security, 2017,9(3):229−249.

[89] Wei R, Hai J. Modeling the network forensics behaviors. In: Proc. of the Workshop of the 1st Int'l Conf. on Security and Privacy for Emerging Areas in Communication Networks. Piscataway: IEEE, 2005. 1−8.

[90] Kent K, Chevalier S, Grance T, Dang H. Guide to integrating forensic techniques into incident response. Gaithersburg: NIST, 2006. 26−29.

[91] Freiling F, Schwittay B. A common process model for incident response and computer forensics. In: Proc. of the SIG SIDAR Conf. on IT-incidents Management & IT-forensics 2007. 2007. 19−40.

[92] Pilli ES, Joshi RC, Niyogi R. Network forensic frameworks: Survey and research challenges. Digital Investigation, 2010,7(1): 14−27.

[93] Kaur P, Bijalwan A, Joshi RC, Awasthi A. Network forensic process model and framework: An alternative scenario. In: Singh R, Choudhury S, Gehlot A, eds. Proc. of the Intelligent Communication, Control and Devices. Berlin: Springer-Verlag, 2018. 493−502.

[94] Lin C, Li ZT, Gao CX, Liu YS. Modeling and analyzing dynamic forensics system based on intrusion tolerance. In: Shi X, Jin H, Zheng R, Zou D, eds. Proc. of the 9th IEEE Int'l Conf. on Computer & Information Technology. Los Alamitos: IEEE Computer Society, 2009. 230−235.

[95] Reza M, Richard H, Victoria C, Amin HF. The standardised digital forensic investigation process model (SDFIPM). In: Jahankhani H, Kendzierskyj S, Jamal A, Epiphaniou G, Al-Khateeb H, eds. Proc. of the Blockchain and Clinical Trial: Securing Patient Data. Berlin: Springer-Verlag, 2019. 169−209.

© 中国科学院软件研究所 http://www.jos.org.cn

[96] Ding LP, Liu WM, Qiu XF, *et al*. The study of detection, response and forensics of malicious behaviors in cloud computing. Technical Report, Beijing: Service National Science and Technology Report, 2018. 153−158 (in Chinese with English abstract).

[97] Li JR, Li XY, Gao YL, Gao YQ, Gao YQ, Fang BX. Review on data forwarding model in Internet of things. Ruan Jian Xue Bao/Journal of Software, 2018,29(1):196−224 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5373.htm [doi: 10.13328/j.cnki.jos.005373]

附中文参考文献:

[1] 祝世雄,陈周国,张小松,等.网络攻击追踪溯源.北京:国防工业出版社,2015.102−131.

[3] 丁丽萍.网络取证及计算机取证的理论研究.信息网络安全,2010,10(12):38−41.

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

[5] 姜建国,王继志,孔斌,等.网络攻击源追踪技术研究综述.信息安全学报,2018,3(1):111−131.

[9] 麦永浩.电子数据司法鉴定实务.北京:法律出版社,2012.26−45.

[10] 丁丽萍.实时可取证操作系统的模型、策略及实现研究[博士学位论文].北京:中国科学院研究生院,2006.

[34] 钱卫宁,邵奇峰,朱燕超,金澈清,周傲英.区块链与可信数据管理:问题与方法.软件学报,2018,29(1):150−159. http://www.jos.org.cn/1000-9825/5434.htm [doi: 10.13328/j.cnki.jos.005434]

[35] 李春晓,陈胜,郑龙帅,左春,蒋步云,梁赓.响应式许可链基础组件——RepChain.软件学报,2019,30(6):1670−1680. http://www.jos.org.cn/1000-9825/5743.htm [doi: 10.13328/j.cnki.jos.005743]

[37] 李德全,苏璞睿,冯登国.用于 IP 追踪的包标记的注记.软件学报,2004,15(2):250−258. http://www.jos.org.cn/1000-9825/15/250.htm

[96] 丁丽萍,刘文懋,裘晓峰,等.云计算环境下的恶意行为检测、响应与取证技术研究.北京:国家科技报告服务系统,2018.

[97] 李继蕊,李小勇,高雅丽,高云全,方滨兴.物联网环境下数据转发模型研究.软件学报,2018,29(1):196−224. http://www.jos.org.cn/1000-9825/5373.htm [doi: 10.13328/j.cnki.jos.005373]

刘雪花(1985－),女,博士,工程师,主要研究领域为信息安全,电子数据取证.

吴敬征(1982－),男,博士,副研究员,主要研究领域为系统安全,漏洞挖掘,移动安全.

丁丽萍(1965－),女,博士,研究员,博士生导师,主要研究领域为信息安全,电子数据取证.

李彦峰(1984－),男,博士,工程师,主要研究领域为隐蔽信道,信息安全.

郑涛(1986－),男,硕士,主要研究领域为5G 移动通信.

© 中国科学院软件研究所 http://www.jos.org.cn