网络攻击追踪溯源层次分析①

陈周国, 蒲 石, 郝 尧, 黄 宸

(电子科技集团公司 第三十研究所, 成都 610041)

摘 要: 近年来, 为了有效防御网络攻击, 人们提出了网络攻击追踪溯源技术, 用于追踪定位攻击源头. 网络安全系统能在确定攻击源的基础上采取隔离或者其他手段限制网络攻击, 将网络攻击的危害降到最低. 由于攻击追踪溯源技术能够为网络防御提供更加准确攻击源、路径等信息, 使得防御方能够实施针对性的防护策略, 其相关技术及研究得到了越来越多的关注与发展. 介绍了追踪溯源四层次划分, 重点分析追踪溯源各层次问题, 并就相应技术及追踪过程进行了深入讨论, 以期对追踪溯源有一个全面的描述, 提高对网络攻击追踪溯源的认识.

关键词: 网络攻击追踪; 追踪溯源层次; 层次分析

Levels Analysis of Network Attack Traceback

CHEN Zhou-Guo, PU Shi, HAO Yao, HUANG Chen

(Institute of Electronic Science and Technology Group Co., Ltd. 30, Chengdu 610041, China)

Abstract: In recent years, to efficiently defend network attack, traceback has been proposed to track dwon the source of attack. With the identifiability of traceback, security measure, such as isolation or others, can be carried out to do less harm in network. Because traceback mechanism is a critical part of the defense against network attack, its related technology and research has achieved more and more attention and development. This article describes the levels of traceback, focusing on analysis of issues of each traceback level and the corresponding technical, and tracking process conducted in-depth discussions on the track in order to give a comprehensive description of traceback and to improve the understanding of cyber attacks attribution.

Key words: network attack traceback; levels of traceback; levels Analysis

随着网络安全的深入发展, 传统被动防御技术已经显得“力不从心”, 无法应对新兴的、复杂的网络威胁. 人们需要更有针对性的主动防御, 确定攻击源头, 有目的地对攻击进行防御抑制, 将危害降到最低. 确定网络攻击源头的技术叫追踪溯源, 它是指确定网络攻击者身份或位置, 以及攻击的中间介质. 身份指攻击者名字、帐号或与之有关的类似信息; 位置包括地理位置或虚拟地址, 如 IP 地址、MAC 地址等. 网络追踪溯源在学术界得到了广泛关注和研究, 但大多数研究都集中在具体算法和应用研究上, 对网络追踪溯源所面临的系统性问题鲜有完整且深入的分析与研究.

网络攻击追踪溯源按照技术功能可分为被动和主动两类[1]; 按照追踪过程网络协作与否, 可分为协作与非协作两类追踪溯源技术[2]; 而从攻击追踪的深度和精准度上又可将其细分为以下四个层次的追踪[3]:

第一层: 追踪溯源攻击主机;

第二层: 追踪溯源攻击控制主机;

第三层: 追踪溯源攻击者;

第四层: 追踪溯源攻击组织机构.

追踪溯源四层次划分准确地描述了攻击追踪溯源所面临的问题与目标. 本文从追踪溯源深度和精度的角度, 描述追踪溯源四层次概念, 抽象其问题并分析

① 收稿时间:2013-06-06;收到修改稿时间:2013-07-15

相应技术解决方法，最后给出了网络追踪溯源整体过程，以系统顶层的视角对网络攻击追踪溯源进行系统全面的剖析.

1 第一层追踪溯源攻击主机分析

1.1 问题描述

第一层追踪溯源攻击主机的目的是定位攻击主机，即直接实施网络攻击的主机[3]. 其追踪溯源问题可描述如下:

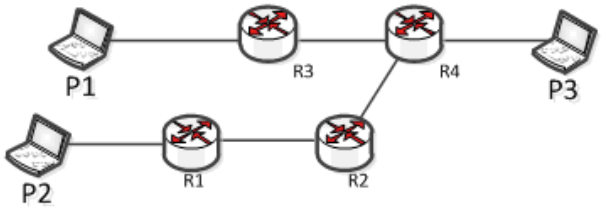

图 1 第一层追踪溯源问题描述

网络数据 S 由 P1 产生，通过 R3→R4 传输到接收端 P3，第一层追踪溯源问题可描述为，给定数据 S，如何确定 P1 的问题. 第一层追踪溯源问题又常常称为 IP 追踪(IP-Traceback).

1.2 相应追踪技术及评估

第一层追踪溯源技术在学术界得到了广泛研究，形成了多种技术路线. 较早的技术有利用路由器调试接口的输入调试 Input Debugging 追踪技术[4]，该技术沿攻击数据流路径反向调试查询其来源，人工操作，效率较低. Bellovin 等人[5]提出了基于 ICMP 追踪技术，即 Itrace 技术，路由器节点单独发送包含网络流路径信息的 ICMP 数据包. 追踪者收集 ICMP 包含路径信息的数据，重构攻击流路径实现追踪. Savage 等人[6]提出了一种概率包标记的方法，追踪者收集带标记的数据包，算法重构攻击路径. BELENKY 等人[7]提出了确定包标记技术 DPM，标识进入网络的每一个数据包. Snoeren 等人[8]提出了基于日志的源路径隔离引擎(SPIE)，可以对单个数据包进行追踪. 通常，分析评估第一层追踪溯源技术时，我们主要需要考虑以下几个方面的问题.

(1) 能否追踪溯源单包数据?

(2) 当前路由器等网络设备是否能直接支持，不需要改造?

(3) 是否要求预先获取数据包的特征信息?

(4) 追踪溯源过程，是否需要额外的通信机制保障?

根据上述四个方面的评价标准，对已有的追踪溯源简单分析如下:

表 1 第一层次的追踪溯源技术比较

追踪方法	单包追踪	与现有网络兼容性	需预先获取追踪数据包	需额外的通信机制保障
Input Debugging	不能	兼容	需要	有时需要
Itrace	不能	不兼容	不需要	不需要
PPM	不能	不兼容	不需要	不需要
DPM	能	不兼容	不需要	不需要
SPIE	能	不兼容	不需要	需要

目前，第一层追踪溯源技术取得了丰硕的研究成果，都由包标记、日志类等基本技术方法演变而来，在追踪效率上得到了极大的提升，并向实际应用系统发展. 但是，需要指出的是，每一种追踪溯源技术都有其自身的弱点和适用性，需要根据追踪的具体需求以及应用环境选择相适宜的追踪溯源技术.

2 第二层追踪溯源攻击控制主机分析

2.1 问题描述

第二层追踪溯源的目标是确定攻击控制主机[3]. 在网络中的计算机上的事件发生总是因为某种原因或事件导致，所以我们将该层次追踪溯源模型用一种因果关系进行抽象，如图 2 所示. 比如说，一个计算机上的事件(请求服务)可能导致另一个计算机上的事件(提供服务)发生. 给定某一计算机上的事件 1，第二层追踪溯源的目标就是寻找某个“因果关系”的事件，其导致了该计算机上事件 1 的发生. 一般来说，这种“因果关系”是由按某种顺序组合的一系列计算机链路. 实际上，这种因果关系就是一种控制关系，这种控制关系可以是多对多，也可能是一对多，甚至是多对一的控制关系.

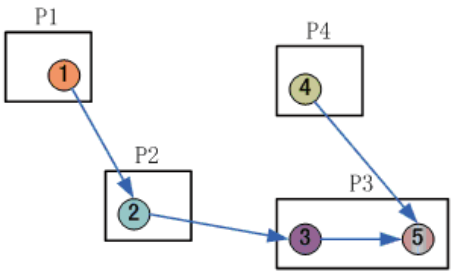

图 2 第二层追踪溯源问题抽象示意

上图中, 我们将计算机抽象成矩形方框, 事件用圆圈表示, 事件的因果关系使用带箭头的连线表示. 图中, 攻击者在计算机 P1 处触发事件 1 入侵计算机 P2, 并利用 P2 的事件 2 入侵 P3, 在 P3 中触发事件 3(比如 DDoS 代理[9]). 而攻击者可以通过计算机 P4 的事件 4 向 P3 发起一个激励或命令, 联合或直接启动事件 3 导致事件 5 的发生. 需要说明的是, 这些事件不需要同时发生. 在事件 5 发生时, 或许事件 1、2、3、4 已经完成并停止活动. 追踪者最初只看到事件 5 的发生和其导致的结果. 第二层追踪溯源的目标正是如何通过事件 5 的发生找到其最初的诱因, 即事件 1.

2.2 主机受控程度划分

通常, 攻击者有多种方式控制网络中的某台主机, 不同的控制方式及模式需要不同的入侵控制方式. 攻击者对主机的控制方式根据其对该主机的控制程度来定[9-11]. 控制程度划分如图 3 所示. 一般来说攻击者控制程度越深, 反向追踪攻击者越困难.

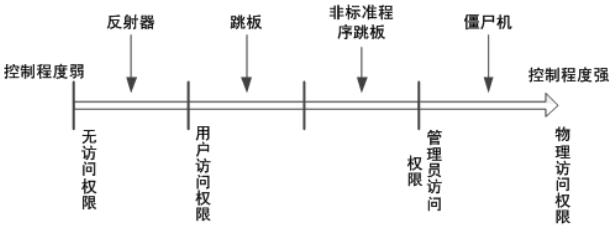

图 3 计算机控制追踪溯源情况划分

如图 3 所示, 我们将攻击者控制主机的模式划分如下:

(1) 反射控制: 此种控制模式, 攻击者无访问权限, 没有入侵主机, 也不需登录系统. 在实施反射时需要通过网络能够与该主机进行通信(发送数据). 具体来说, 攻击者能够也需要获知该主机运行有哪些程序或服务.

(2) 跳板控制: 攻击者利用已有标准的程序(如 telnet, rlogin 和 ssh 等)控制主机. 此种控制模式下, 攻击者可登录(已入侵)所控主机(即跳板). 攻击者是利用现有标准的并运行良好的程序实时地与受控主机通信, 完成控制命令等信息的收发.

(3) 非标准跳板控制: 攻击者入侵受控主机, 常常都会安装非标准的(自制的)控制程序, 以非常用的通信方式或协议控制受控主机. 这种控制模式, 我们称为非标准跳板控制. 攻击者在入侵的主机系统上安装程序并运行, 至少需要获得该主机的用户级访问权限.

(4) 僵尸控制: 在绝大多数计算机中, 普通用户权限和管理员权限安装程序的能力是有区别的, 管理员权限拥有更大的权限和自由. 攻击者入侵控制某一主机, 总是想获得其管理员权限以便于安装任意的程序或服务. 我们将这样的受控主机称为僵尸机, 犹如其精神被人控制, 丧失自我的僵尸.

(5) 物理控制: 指主机的物理实体完全在其控制之下, 控制者能根据情况删减或增加主机的硬件或软件系统等.

网络追踪者的挑战就是在未知控制模式的条件下, 确定网络中某一事件如何因另一事件控制而发生. 同时, 攻击者总是提高其攻击能力, 提升控制程度, 使用难于被追踪者发现的控制方式. 攻击者所选取的控制方式受限其能控制的程度.

2.3 相应追踪技术及评估

实现第二层追踪溯源目标, 最显然的思路就是沿着事件因果链一级一级的逆向追踪, 最终找到真正的(最初的)攻击源主机. 攻击源主机指能够发送网络数据的任意设备, 不限制于计算机. 从追踪者的角度看, 第二层追踪溯源是依据数据进行推理的过程. 数据的有效性非常重要, 什么数据是有效的, 依赖于追踪者所能控制的网络设备, 或者说网络设备(网络)的配合程度. 网络中的设备可以为追踪者提供帮助, 也存在被攻击者所控制利用的风险. 比如, 追踪者在某一网络主机中读取的信息正是攻击者所伪造的. 因此, 追踪溯源过程也是攻防双方博弈的过程. 一些技术方法一次能够完成追踪多级, 但是目前还没有直接追踪溯源到真正的(最初的)攻击源主机技术. 我们这里重点描述如何反向追踪到上一级主机, 主要有:

(1) 内部监测[12]: 实时监测主机行为;

(2) 日志分析[13]: 分析主机内有效的系统日志信息;

(3) 快照技术: 实时捕获主机当前系统的所有状态信息;

(4) 网络流分析[14]: 对进出主机的数据流进行相关分析, 实现攻击数据流及其上一级节点的识别;

(5) 事件响应分析: 追踪者对网络事件施加特有的干预, 以观测分析该事件在网络中的行为变化, 对网络行为变化信息分析可确认事件的因果关系, 实现追踪.

表 2　第二层次的追踪溯源技术分析比较

追踪技术	跳板控制	非标准跳板控制	僵尸控制	物理控制
内部监测	有效	无效	无效	无效
日志分析	有效	有效	有效	有效
快照技术	有效	无效	无效	无效
网络流分析	有效	无效	无效	无效
事件响应分析	有效	无效	无效	无效

反射控制的追踪可使用第一层次的追踪溯源技术较方便的实现[11,12,15]，在此不做进一步分析比较. 内部监测能够分析主机行为如何产生, 受什么控制, 进而实现其控制源的追踪; 但是对延迟攻击(攻击发生时无控制链路)的情况就束手无策了. 日志分析技术是应对第二层追踪最为有效的一种方式, 但需要确保日志数据的正确性和权威性. 快照技术与内部监测技术原理相同, 实时性、准确性更高, 但其成本更高. 网络数据分析能够基于时间、内容的相关性对数据流进行分析, 确定进出主机的数据流关系, 追踪其上一级主机; 但对采取高匿名技术(加密)攻击流的相关分析极其困难. 关于事件响应分析技术, 由于网络行为响应结果存在延后性和二义性, 该技术实时性及正确性较低, 分析过程复杂.

3　第三层追踪溯源攻击者分析

3.1　问题描述

第三层追踪溯源的目标是追踪定位网络攻击者[3], 这就要求追踪者必须找到网络主机行为与攻击者(人)之间的因果关系. 第三层追踪溯源就是通过对网络空间和物理世界的信息数据分析, 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. 如图 4 所示.

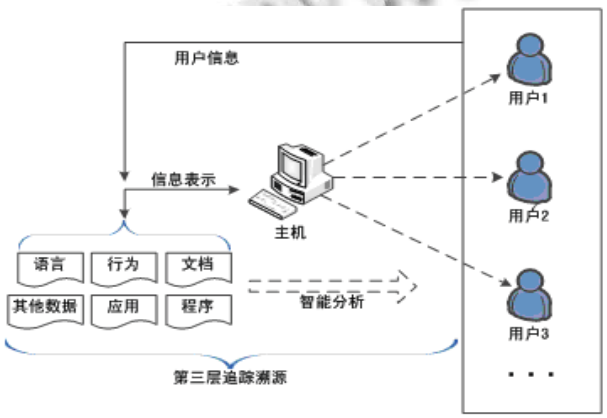

图 4　第三层追踪溯源问题描述示意

第三层追踪溯源包含四个环节: ①网络空间的事件信息确认; ②物理世界的事件信息确认; ③网络事件与物理事件间的关联分析; ④物理事件与自然人间的因果确认. 第一个环节, 前两个层次的追踪溯源技术科较好解决. 第二个环节需要物理世界中的情报、侦察取证等手段确定. 第三个环节是通过网络世界中的信息(主机位置、攻击模式、攻击行为、时间、习惯、文件语言、键盘使用方式等)与物理世界中取证的各种信息情报进行综合分析, 确认网络事件与物理事件的因果关联. 在第二层追踪定位攻击源主机基础上, 通过获取该主机攻击行为, 攻击模式、语言、文件等信息, 支持物理世界中的事件确认. 第四个环节是采取司法取证等手段, 对物理事件中的可疑人员进行调查分析, 最终确定事件责任人, 即真正的攻击者.

3.2　第三层追踪溯源所需信息

从上述第三层追踪溯源的问题描述中我们可以看到, 完成第三层追踪目标其核心仍然是信息数据收集与分析, 但不是所有的网络信息都可用于第三层追踪溯源中, 需要在网络空间有针对性地收集信息. 这些信息主要包括:

(1) 自然语言文档[16]: 通过对攻击源主机中的文件收集(需确认能否通过网络进入攻击源主机或司法手段), 通过文档语言的分析, 确认攻击者的身份等;

(2) Email 和聊天记录[17,18]: 收集其 Email 和聊天记录等, 分析其爱好、朋友圈、习惯甚至信仰等信息;

(3) 攻击代码[19-21]: 捕获网络攻击代码, 逆向分析确认编程习惯、语言、工具等信息;

(4) 键盘信息[22,23]: 记录攻击源主机的键盘使用信息, 确认攻击者进行网络攻击时的控制方式, 习惯右手还是左手, 键盘操作模式等信息;

(5) 攻击模型[9]: 比较流行的攻击模型是树型结构, 攻击者通过这样的树型结构控制大量主机(树的枝干)攻击受害者(树的根部节点). 通过对网络攻击模型的重构和分析, 可以分析攻击者如何调动各种资源实施攻击, 以及攻击路径、过程控制等信息.

以上这些信息数据的收集有点需要在网络空间完成, 有的需要采取司法行政手段等, 信息数据收集受到各种各样的限制, 比如网络的联通性和可访问性等. 因此完成这些信息数据收集本身就已是一项非常艰巨的任务.

3.3 相应技术的分析比较

这里所讨论的技术是从网络空间来讲的，现实世界中的司法调查取证等技术超出本文范围，不作讨论. 而事实上，现实世界中的调查取证，对第三层追踪溯源具有非常重要的作用，是最终确认攻击者的有效手段.

表 3 第三层次的追踪溯源技术分析比较

信息分析技术	获取信息	备注说明
文档分析-自然语言分析	攻击目的，字体，受教育程度，母语等	计算复杂，但准确可靠
文档分析-统计分析[16]	攻击目的，字体，受教育程度，母语等	计算较容易，但结果存在概率性
敲键频率分析	模式分析确定是习惯使用左手还是右手以及操作习惯	计算较容易，但结果存在概率性，攻击者可伪装
Email 及聊天记录分析	与文档分析类似	有时有用，确定攻击目的等信息
攻击代码分析	确定攻击者使用的工具、编程语言、知识能力等	与其他方面的信息进行综合分析. 有时通过代码分析可确定具体攻击者.
攻击模型分析	通过模型分析，可确定潜在的攻击路径等信息	

当前，第三层攻击追踪溯源不是没有对应的工具或方法，而是这些工具和方法都只能表征攻击者在某个时间片、某一方面的具体表示. 关键的问题是如何将这些零星的信息表示进行汇聚，综合多方面的数据信息，构建攻击者及其行为的完整而准确的描述，以侦辨确定可疑攻击者. 这样的综合汇聚处理需要极大的认知能力，目前还没有完全具备这样能力的系统工具或技术手段. 另一方面，在第三层追踪溯源过程中还需要确保情报信息数据的准确性和可靠性，没有数据的准确可靠，任何分析技术都将是徒劳.

4 第四层追踪溯源攻击组织机构

4.1 问题描述

第四层追踪溯源的目的是确定攻击的组织机构[3]，即实施网络攻击的幕后组织或机构. 该层次的追踪溯源问题就是在确定攻击者的基础上，依据潜在机构信息、外交形势、政策战略以及攻击者身份信息、工作单位、社会地位等多种情报信息分析评估确认人与特定组织机构的关系，如图 5 所示.

第四层的追踪溯源更多的是国家与国家，机构与机构之间的对抗，是网络攻防的一种高级形式. 第四层追踪溯源是一个更加复杂的系统工程，但仍以第一层、第二层和第三层追踪溯源为基础. 在前三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，综合分析评估是能够确定网络攻击事件的幕后组织机构.

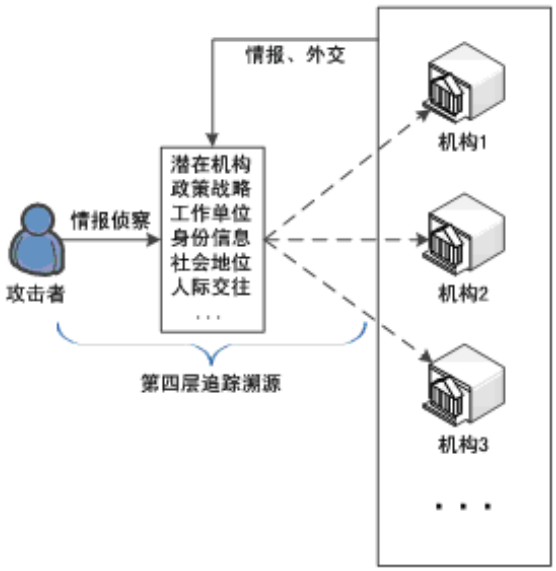

图 5 第四层追踪溯源问题描述示意

5 网络追踪溯源一般过程描述

网络追踪溯源的过程描述如图 6 所示. 网络预警系统发现攻击行为请求追踪，对攻击数据流进行追踪定位，分析确定发送攻击数据的网络设备或主机. 确定攻击主机后，通过分析该主机输入输出信息，或其系统日志等信息，判定该设备是否被第三方控制，从而导致攻击数据的产生，据此确定攻击控制链路中的上一级控制节点，如此循环逐级追踪，完成第二层追踪溯源. 在第二层追踪溯源的基础上，结合语言、文字、行为等识别分析，可以对追踪者进行分析确定，完成第三层次的追踪溯源. 在第三层追踪溯源基础上，结合网络空间之外的侦查及情报等信息，判定攻击者的目的、某后组织机构等信息，实现第四层追踪溯源.

目前，网络追踪溯源第一、二、三层追踪溯源是可以使用相关技术进行信息数据分析，辅助追踪者实现追踪定位. 在这三个层次中存在大量亟待需要突破的技术点和难点，而第四层追踪溯源更多依赖于物理自然世界的综合情报进行推理验证，比如组织机构间的体制、政策、外交、历史等综合信息. 特别强调的

是，第三层追踪是从网络设备到人的跨越，将设备的控制行为与具体的自然人相关联在技术上具有极大的挑战.

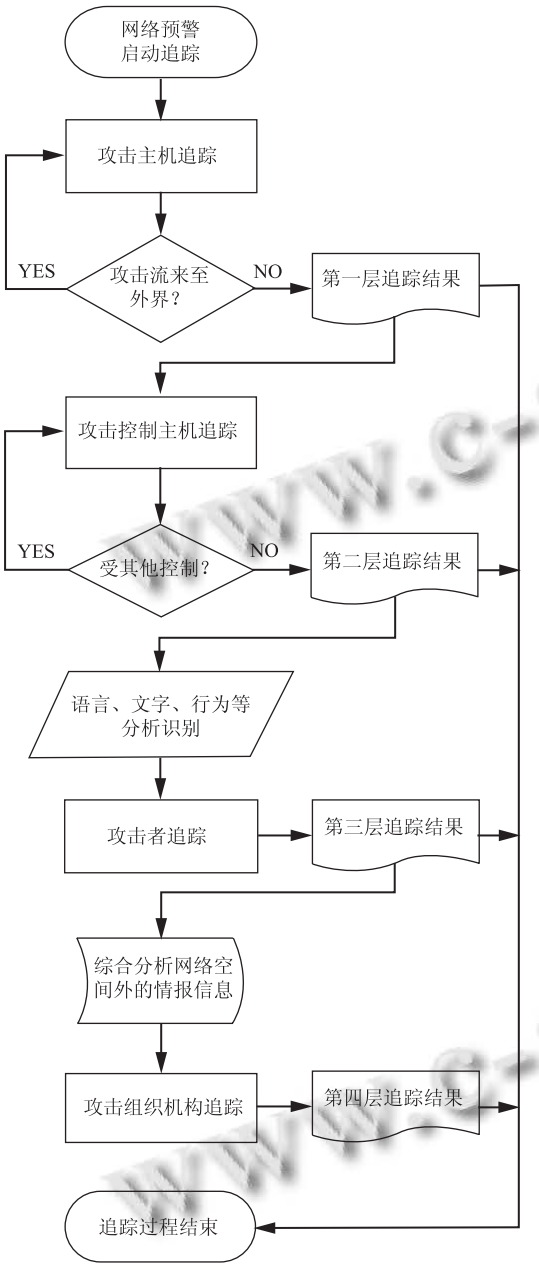

图 6 追踪溯源四层次流程示意

6 总结

网络追踪溯源四层次划分是从追踪深度和精准度上对追踪溯源提出的目标. 追踪难度从第一层到第四层，由浅入深，逐步增大. 每个追踪溯源层次所面对的问题和环境完全不同，所能使用的技术或信息亦有区别，产生了多种技术体制应对相应问题. 目前第一、第二层次追踪溯源技术研究较多，成果丰富，正朝着实际应用方向发展；而第三、第四层次由于追踪的复杂性，相应的研究还比较初级. 随着技术的发展和投入的增多，相信网络追踪溯源技术能够得到更大的发展和全面的解决. 网络追踪溯源挑战巨大，但不是不可完成的任务.

参考文献

1 Santhanam L, Kumar A, Agrawal DP. Taxonomy of IP Traceback. Journal of Information Assurance and Security, 2006,(1): 79–94.

2 陈周国,蒲石,祝世雄.一种通用的互联网追踪溯源技术框架. 计算机系统应用,2012,21(9):166–170.

3 Cohen D, Narayanaswamy K. Attack Attribution in Non-Cooperative Networks. Proc. of the 2004 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY 10-11 June, 2004.

4 Stone R. CenterTrack: an IP overlay network for tracking DoS floods. Proc. of the 2000 USENIX Security Symposium, Denver, CO. July 2000.

5 Bellovin S, et al. ICMP Traceback message. IETF Internet Draft draft-ietf-itrace-04. txt, Feb 2003.

6 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.

7 Belenky A, Ansari N. IP traceback with deterministic packet marking. IEEE Commun. Lett., 2003,7(4): 162–164.

8 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.

9 诸葛建伟,韩心慧,周勇林,等.僵尸网络研究.软件学报,2008, 19(3):702–715.

10 Cooke E, Jahanian F, McPherson D. The zombie roundup: Understanding, detecting and disrupting botnets. Proceedings of Usenix Workshop on Stepts to Reducing Unwanted Traffic on the Internet (SRUTI'05), Cambridge, MA, July2005.

11 李少鹏.基于跳板攻击的军用网络入侵追踪的实现技术. 四川大学学报(自然科学版),2007,44(6).

12 张萧木.基于主机入侵检测系统的设计与实现[硕士学位论文].济南:山东大学,2007.
13 Buchholz F, Shields C. Providing Process Origin Information to Aid in Network Traceback. California USA, Proc. of the 2002 USENIX Annual Technical Conference, USENIX, 2002: 261–274.
14 Wang XY, Reeves DS. Robust Correlation of Encrypted Attack Traffic through Stepping Stones by Flow Watermarking. IEEE Trans. on Dependable and Secure Computing, May-June 2011,8(3): 434–449.
15 Wang BT, Schulzrinne H. A Denial-of-service resistant IP Traceback Approach. Proc. ISCC 2004. the 9th International Symposium on Computers and Communications, 28 June-July, 2004, Alexandria, Egypt.
16 Fung G. The Disputed Federalist Papers: Support Vector Machines Feature Selection via Concave Minimization; TAPIA 2003, Atlanta, Georgia.
17 Argamon S, Saric M, Stein S. Style Mining of Electronic Messages for Multiple Authorship Discrimination: First Results, SIGKDD 2003.
18 Stiles RA, Deppen SA, Figaro MK, Gregg WM, Jirjis JN, Rothman RL, Johnston PE, Miller RA, Dittus RS, Speroff T. Behind-the-Scenes of Patient-Centered Care: Content Analysis of Electronic Messaging among Primary Care Clinic Providers and Staff, Medical Care, Lippincott Williams & Wilkins, 2007,45(12):1205–1209.
19 Weeber S, Spafford E. Software Forensics: Can We Track Code to Its Authors? Computers & Security, 1993,12(6).
20 Bayer U, Moser A, Kruegel C, Kirda E. Dynamic analysis of malicious code, Springer, J Comput Virol, 2006,2:67–77.
21 Moser A, Kruegel C, Kirda E. Limits of static analysis for malware detection. Annual Computer Security Applications Conference (ACSAC). Miami Beach, 2007.
22 Dowland P, Furnell S, Papadaki M. Keystroke Analysis as a Method of Advanced User Authentication and Response. Proc. of of IFIP/SEC 2002 - 17th Int. Conf. on Information Security, Cairo, Egypt. Kluwer, 2002.
23 Karatzouni S, Clarke NL. Keystroke Analysis for Thumb-based Keyboards on Mobile Devices. Proc. of the 22nd IFIP International Information Security Conference (IFIP SEC 2007), Sandton, South Africa, 14-16 May 2007:253–263.

(上接第 48 页)

6 结语

本文提出了基于业务模型语义的制造企业管理信息系统重构方法, 并就构建具有清晰语义的业务模型、业务模型到信息系统的映射和业务模语义驱动的系统重构等关键技术进行了论述. 该方法无需依赖于软件开发商的参与, 通过企业用户对业务模型的配置完成信息系统功能的调整, 支持制造企业自主实施系统重构, 提高了系统重构的效率.

在基金项目支持下, 将基于业务模型语义的系统重构技术应用于某压机制造企业的工艺管理系统, 明显降低了压机改型后的工艺调整周期, 使新工艺准备周期从原来的一个月以上缩短至现在的 15 天以内, 产生了明显的经济效益. 在压机企业的应用实践表明, 该技术适应了企业业务发展和变革的需要, 对提升制造企业管理信息系统重构水平具有重要促进意义.

参考文献

1 朱传军,饶运清,张超勇,李培根.基于 CORBA 的可重构制造执行系统研究.中国机械工程,2004,15(23):2097–2101.
2 Shishkov B, Van SM, Quartel D. SOA-driven business-software alignment. Proc. of the IEEE International Conference on e-Business Engineering. Shanghai: IEEE Computer Society. 2006. 86–94.
3 郑彦树.基于构件的可重构 ERP 系统研究.计算机工程与设计,2006,27(17):3168–3171.
4 王琦峰,刘飞,黄海龙.面向服务的离散车间可重构制造执行系统研究.计算机集成制造系统,2008,14(4):737–743.
5 张金,涂俊翔,陈卓宁,严晓光.基于动态解释的管理信息系统多维重构技术.计算机应用研究,2009,26(7):2540–2542.
6 王忠杰,徐晓飞,战德臣.一种面向重构的业务过程模型.计算机集成制造系统,2004,10(11):1349–1355.
7 Seidewitz E. What models mean. IEEE Software, 2003, 20(5): 26–32.