信息安全研究 第8卷 第3期 2022年3月
Journal of Information Security Research Vol.8 No.3 Mar. 2022
DOI:10.12379/j.issn.2096-1057.2022.03.09

基于异构属性图的自动化攻击行为语义识别方法

薛见新[1] 王星凯[1,2] 张润滋[1] 顾杜娟[1] 刘文懋[1]
[1](绿盟科技集团股份有限公司 北京 100089)
[2](清华大学自动化系 北京 100084)
(xuejianxin@nsfocus.com)

Semantic Recognition for Attack Behavior Based on Heterogeneous Attributed Graph

Xue Jianxin[1], Wang Xingkai[1,2], Zhang Runzi[1], Gu Dujuan[1], and Liu Wenmao[1]
[1](*NSFOCUS Technologies Group Co., Ltd., Beijing* 100089)
[2](*Department of Automation, Tsinghua University, Beijing* 100084)

Abstract At present, security operators are faced with messive device logs and need to trace the attackers according to their expert knowledge or experience, which greatly reduces the efficiency of security operation and sets a high knowledge threshold for security operation. In order to solve this problem, we propose an automatic attack behavior semantic recognition method based on heterogeneous graph, which can realize the mapping between low-level security logs and upper-level attack behaviors. Firstly, heterogeneous graph is used to model the threat of system logs. Then, taking the attack context as the semantics and combined with the knowledge map representation, the vector representation of nodes and edges in the graph is obtained. Meanwhile, hierarchical clustering is used to aggregate similar logs, and the most representative logs are found as the behavior representation of the whole class. Finally, the experimental verification of this method shows that this method has high accuracy in the abstraction of system normal behavior and malicious behavior. More importantly, in the stage of attack investigation and evidence collection, it can greatly reduce the workload of security operation.

Key words attack provenance; security operations; heterogeneous attributed graph; attack behavior; semantic recognition

摘 要 当前安全运营人员面对的是海量的设备日志,需要根据其专家知识或经验来进行调查溯源,大大降低了安全运营的效率,同时也为安全运营设置了较高的知识门槛.为了解决这一问题,提出了一种基于异构属性图的自动化攻击行为语义识别方法,能够实现底层安全日志到上层攻击行为之间的映射.首先,利用异构图对系统日志进行威胁建模;然后,以攻击行为上下文为语义并结合知识图谱表示学习得到图中节点与边的向量表示;接着,利用层次聚类把相似的日志聚合到一起,从中找出最具代表性日志作为整个类的行为表示.最后,对该方法进行了实验验证,可以看出该方法在系统正常行为与恶意行为的识别上都具有较高的精度,可以大大提高安全运营的效率.

收稿日期:2022-01-24
基金项目:科技部重点研发计划专项(2016QY071405)
引用格式:薛见新, 王星凯, 张润滋, 等. 基于异构属性图的自动化攻击行为语义识别方法[J]. 信息安全研究, 2022, 8(3): 292-300

关键词　攻击溯源；安全运营；异构属性图；攻击行为；语义识别

中图法分类号　TP309.1

企业为了更好地满足信息交流与资源共享，提高工作效率，都会建立自己的内部信息网络.然而企业内部网络信息包含很多内部机密和重要文件资料，其安全性对企业来说意义重大.企业信息网络虽然有效地提高了日常工作效率，但也带来了许多安全隐患.由于计算机网络拥有互联性、开放性的特点，从而使计算机网络的漏洞和缺陷更加突出.企业利用计算机网络进行企业信息管理，将面临系统内部和外部的双重威胁，给企业信息安全带来危害.

为了应对企业的内部和外部攻击，大多数据企业通常会部署一些检测设备，如网络侧的全流量分析平台、IPS/IDS、WAF、EDR 和蜜罐等.这些检测设备每天会产生海量日志.给企业日常安全运营带来巨大挑战，完全依靠人力进行安全运营显然是不现实的.另外，检测设备产生的日志通常是低级的、孤立的，尤其是针对 APT 攻击[1]，安全运营人员需要丰富的安全知识和经验才能针对日志进行研判，进一步增加了企业的安全运营挑战.

在安全运营的整个过程中，网络分析人员需要根据日志之间因果关系对攻击者以及其破坏范围进行溯源分析.当前已有的技术通常是事先构建溯源图[2-3]并利用之前提到的异常检测方法对溯源图进行分析，最终找到的仅仅是异常用户或是异常行为路径，这种方法的误报率通常会很高.

当前的方法本质上缺少一种系统日志到用户行为之间的语义映射，针对该挑战，已有工作[4]通过安全专家构建的威胁子图作为知识图，利用图匹配算法从系统溯源图中找到相匹配的攻击.这些方法主要是事先设计一些规则库，基于这些规则检测审计日志中的相关行为.然而，这些规则的设计严重依赖于安全专家的经验.知识图谱本身就是致力于解决这种语义鸿沟的问题，但是在安全领域知识图谱相关应用进展比较缓慢.本文借鉴了知识图谱在推荐系统上的应用方式，首先基于终端日志设计了有效的知识图谱表示形式；然后，以上下文为语义基于图表示学习方法自动提取行为信息.

1　相关工作

本节主要从 2 个方面介绍相关的研究工作：溯源图的构建方法与基于溯源图的威胁检测.

1.1　溯源图构建

BackTracker[5]是一种经典的溯源图构建方法，它是主机侧攻击溯源工作的奠基工作，后续的相关工作均是参考 BackTracker.BackTracker 构建的溯源图主要是挖掘进程、文件与文件名之间的因果依赖关系.BackTracker 分别对主机进程之间的依赖关系、进程与文件之间的依赖以及进程与文件名之间的依赖关系进行定义.

攻击溯源图的构建是挖掘不同实体之间的因果依赖关系，但是当前关于溯源图的构建大多是基于 BackTracker，挖掘的关系本质上是实体之间的依赖关联关系，缺少因果语义.MCI[6]提出一种有效的因果推理算法挖掘系统日志之间的因果关系，不需要开发额外的应用程序或修改系统内核.MCI 利用 LDX[7]因果推理模型挖掘系统调用之间精确的因果关系.

BackTracker 的工作是后续关联攻击溯源工作的基础，后续的相关工作重点在于研究系统日志来解决依赖爆炸问题，没有考虑应用层语义，没有为跨层攻击调查提供一种通用的、可靠的解决方法.文献[8]认为将系统上所有与取证相关的事件统一到一个整体日志中可以显著提高攻击调查能力，提出了一种端到端的溯源追踪框架 OmegaLog，该框架集成了应用程序事件日志与系统日志，生成一个全局溯源图(UPG).全局溯源图集成了系统层的因果分析能力和应用事件日志的语义上下文.OmegaLog 实时解析分散的异构应用程序日志并与系统日志关联起来生成全局溯源图.OmegaLog 通过应用程序事件序列识别事件处理的环路解决依赖关系爆炸问题，同时由于集成了应用程序的日志解决了语义鸿沟问题.

上述攻击溯源的方法均是在单一主机上进行，一个完整的攻击过程不仅仅是针对单一主机，

通常是跨多个主机进行关联溯源.只有关联网络侧数据与终端侧数据才有可能溯源整个攻击过程.网络侧与终端侧关联溯源是攻击溯源的难点,相关的研究工作也比较少.文献[9]是BackTracker工作的扩展,通过相关日志记录来追踪网络数据包的发送与接收.比如主机A的进程1向主机B的进程2发送一个数据包,那么进程1与进程2就具有了因果依赖关系.当前已有很多关联数据包标记的工作,为了减少工作量,采用的是通过源地址、目标地址和序列号来标记数据,相对来说实现简单,但是这种粗粒度的关联方法会生成大量的错误关联,无法进行有效的攻击溯源,反而会有大量的计算开销.因此,该方法在工程实践中没有被广泛使用.

文献[10]提出了一个新的开源平台Zeek-Osquery,该平台主要是针对网络侧与终端侧数据细粒度的因果挖掘来实现实时的入侵检测.用网络侧数据与终端侧数据进行联合监控,构建跨主机攻击溯源图.工作核心是将操作系统级的数据与网络信息实时关联,同时还可以动态选择用于关联的操作系统相关数据.Zeek-Osquery可以灵活地适应不同的检测场景,因为Osquery主机是从Zeek脚本直接管理的,所有的数据处理都可以在Zeek中实现.例如,检测从互联网下载的已执行文件,通过SSH跳转检测攻击者的横向移动,或向Zeek提供从主机获得的内核TLS密钥,用于解密和检查网络流量.

文献[11]综合了多种技术提出了一种有效的跨主机追踪溯源方法RTAG.RTAG可以在一定程度上解决当前网络侧与终端侧数据无法关联溯源的问题.RTAG是一种可以实现跨主机攻击调查的有效数据流标记与追踪机制.

1.2 基于溯源图的威胁评估

当前溯源图构建通常包含大量的正常用户行为.如何从复杂的溯源图中找到攻击相关的上下文信息来实现复杂攻击识别与评估是当前研究工作的难点.从技术手法上主要分为2类:一类是基于异常检测思路的攻击识别,另一类是基于外部知识的攻击识别.

文献[12-13]主要是利用异常检测思路来解决复杂攻击行为识别问题.基于异常检测思路的复杂攻击识别技术主要是构建参考模型.也就是在进行攻击识别之前需要对系统的正常行为进行建模,这个思路有些类似于UEBA(user and entity behavior analytics).建立的参考模型作为系统正常运行的参照物,按正态分布来标记异常值.

文献[14]从CTI报告和IOC描述中,将威胁猎杀问题形式化,开发了POIROT系统.该系统可以得到一个表示攻击成功可能性的分数.简而言之,给定一个用图表示的IOCs及其之间的关系(描述了APT),称之为查询图.然后在系统运行中产生的更大溯源图中寻找与其匹配的图.也就是根据外部情报构建攻击相关的威胁子图,然后在溯源图中匹配满足威胁子图模式的子图,通过引入外部情报把威胁评估转换成子图匹配.

HOLMES[2]从主机审计数据(例如Linux审计或Windows ETW数据)开始,并产生检测信号,该信号反映了APT活动的各个阶段.HOLMES从一定程度上解决了低级别审计数据与攻击者目标、意图和能力相关高级杀伤链视角之间的巨大语义差距,但是这完全依赖于专家知识撰写规则,可扩展性较低.

文献[15]提出一种有效的终端事件溯源方法.当前终端EDR产品的检测规则一般参考ATT&CK,在构建依赖图时就可以通过ATT&CK相关知识过滤掉与攻击不相关的数据.与已有的攻击溯源技术相比,RapSheet通过溯源图根据ATT&CK抽象出TPG战术溯源图,利用相关的知识对溯源进行裁剪.

2 安全运营中溯源调查的现状

当前企业安全面临的挑战不再是检测设备检测的准确性问题,而是涉及到更上层的攻击者的战术、技术以及攻击过程等不同层面的分析.当前安全运营面临的最大难题就是低层日志与上层行为之间的语义鸿沟问题.本文首先提出一种基于异构图的威胁建模方法,相比溯源图有更好的表达效果.然后,使用自动化的方法从系统日志中抽象出上层系统行为,并利用语义相似度聚类方法把语义上相似的行为日志聚合到一起,即使不能给出合理的解释标签,这种聚类也是有意义的.理论上来说,相关的系统行为已经根据语义进行了聚类,安全分析人员只需要从聚类中标记有代表性的系统行为,就可以分析这些代表性系统行为来

快速进行调查取证.除了能有效减少行为分析的工作量外,自动的行为抽取可以为内部或外部攻击行为模式提供前瞻性的分析.

可以看出行为语义提取是当前安全运营挑战的一个有效解决方法,但依然面临挑战:行为语义的差异性和行为识别.行为语义的差异性是指相同的日志在不同的上下文中具有不同的行为语义,这里的行为语义的差异性与自然语言中的语义差异性相似.行为识别的挑战更明显,因为系统日志的规模与高度交织性导致对其进行行为划分是异常困难的.通过行为识别得到的语义信息以及相关的安全知识如何表示是安全运营人员面临的另一个挑战.知识图谱技术通常是利用其实体或关系的上下文来表示其语义.本文也借鉴这种表示,以日志相关实体在图中的上下文表示日志的行为语义.可以通过聚合多个相关的日志来表示系统行为.基于这种表示,相似的行为可以被聚到一起.此外,通过聚类之后的安全知识图谱可以提供一个关于高水平行为的边界,这种边界可以作为一种参考,通过关联多日志生成相应的具有语义的行为信息.

下面以 DARPA TC 项目[20]中的攻击场景为例进行说明,后续方法中的相关实例也是以该专题为背景的.

图 1 中的场景描述如下:企业内部员工想利用自己的权限窃取一些敏感信息,该员工是软件测试工程师.其日常工作包括使用 git 同步代码,使用 gcc 来编译源代码,使用 apt 命令安全相关的测试依赖包.如果该员工想窃取敏感文件(secret.txt),为了躲避检测,他需要模拟他的日常工作行为模式.首先该员工把敏感文件复制到该员工常用的工作目录中并重命名为 pro2.c 文件.然后,对该文件利用 gcc 进行编译,当前这个文件本身不是一个有效的源文件,因此编译结果是不成功的,这里只是为了模拟他日常工作行为模式.最后,把该文件上传到 github 上.该企业员工试图通过这种策略来窃取敏感数据.

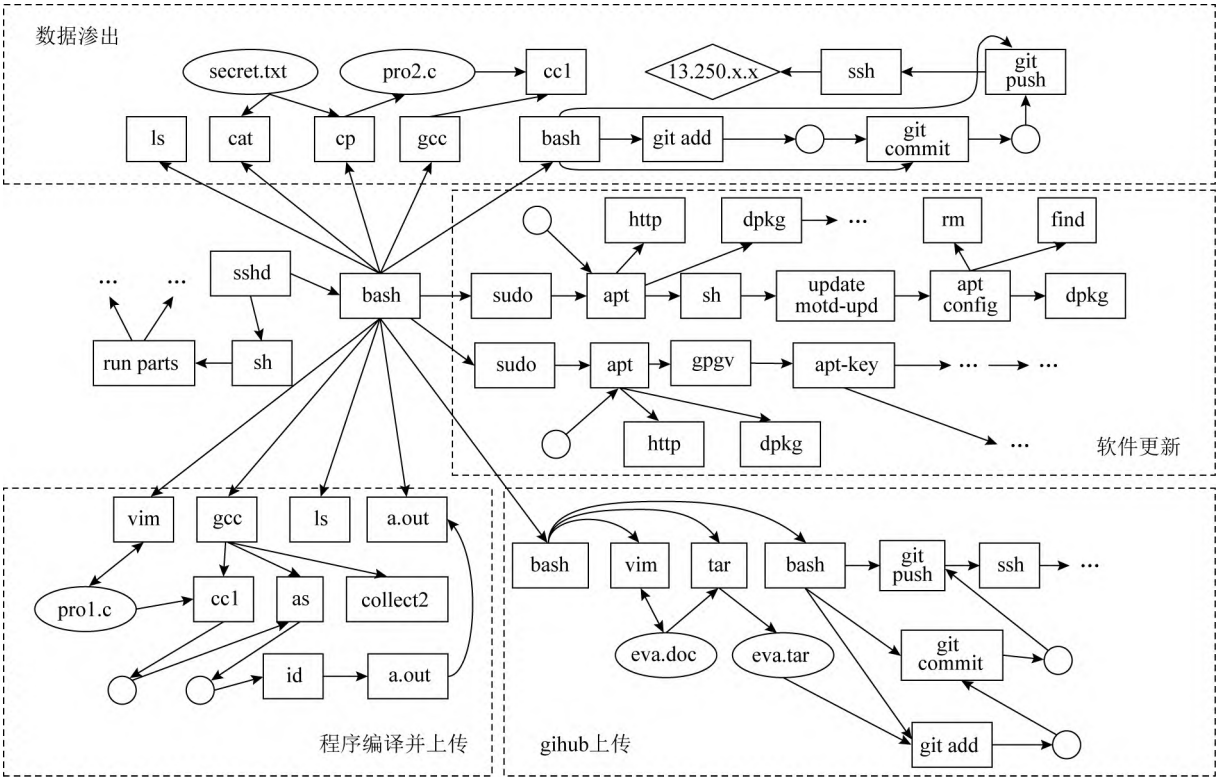

图 1　应用实例的溯源图

为了对攻击行为进行有效的因果分析,当前已有的方法主要是基于审计日志构建有效的溯源图[7]来进行分析.本质上溯源图是一个系统行为因果关系的通用表示方式.图 1 即是上面场景的溯源图.边的方向表示不同实体之间的数据流向.在攻击调查过程中,分析人员通过对溯源图进行分析来

找到与攻击相关的信息片段.在图1的实体中,分析人员首先会根据一个确定的事件进行后向溯源来找到攻击的起源.然而,分析人员可以利用前向溯源技术,从确定的攻击事件来确定其攻击后果.利用溯源技术,安全分析人员不仅能推断该攻击事件的根因与攻击结果,还能给出高层的抽象行为.

当前终端设备记录的日志信息不仅仅包含攻击行为也包含系统的正常行为.虽然溯源图提供了具有因果依赖关系的系统行为的直观表示,但对于安全分析人员调查分析来说依然是非常耗时的.从日志中提取出抽象行为对于安全分析人员来说是有效的方法.本质上行为信息是对系统日志的一种抽象,安全分析人员在系统行为层面的处理将大大减少其工作量.因此从系统日志中自动化提取高水平行为信息成为智能安全运营的核心工作.

3 基于异构属性图威胁建模

为了有效分析事件的上下文语义,需要一种能集成多种类型数据的异构数据模型.因此,本文使用异构属性图对整个系统日志进行威胁建模.相比较溯源图模型,异构属性图模型有更强的表示能力.

终端侧采集的日志主要使用以下8种构建终端溯源图:

1)网络连接日志.

终端网络连接日志记录的是终端网络连接行为.对于网络连接的日志行为,需要根据direction字段的in和out确定网络连接的方向.direction为in表示有主机通过网络连接访问本机,其在异构属性图中表示为remote_ip ⇒process,remote_ip表示主机ip地址,process表示本机相关进程.direction为out表示有本机访问其他主机,其在终端溯源图中表示为remote_ip ⇒process.由于不同主机会有相关的进程pid,为了区分,对于进程需要考虑时间与主机.

2)进程行为日志.

终端进程行为日志描述进程之间的调用关系,其在终端溯源图中表示为parent_process ⇒children_process.三元组的源节点表示父进程,目标节点表示子进程,三元组的边是进程操作.

3)注册表操作日志.

注册表操作日志表示终端对注册表的操作行为.其在终端溯源图中表示为process ⇒registry_path,三元组的源节点是用户加进程,目标节点是注册表路径,边表示注册表的相关操作.

4)终端登录日志.

终端登录日志描述终端的登录行为.其在终端溯源图中表示为proces ⇒ip,三元组的源节点表示登录IP或用户,目标节点表示终端与登录相关的进程,边表示登录操作.

5)系统服务日志.

系统服务日志描述的是操作系统服务操作.其在终端溯源图中表示为process ⇒service,三元组源节点表示与系统服务相关的进程,目标节点表示相关服务,边表示服务类型.

6)操作系统计划任务日志.

操作系统计划任务表示用户执行的操作系统计划任务.其在终端溯源图中表示为user ⇒service,三元组源节点表示用户,目标节点表示相关任务,边表示任务行为.

7)终端应用程序日志.

终端应用程序日志表示终端应用程序的相关日志记录.其在终端溯源图中表示为user ⇒app,三元组源节点表示终端用户,目标节点表示应用程序,边表示用户对应用程序的相关操作.

8)文件操作日志.

文件操作日志描述终端的文件操作.其在终端溯源图中表示为process ⇒file,三元组源节点表示进程,目标节点表示文件,三元组边表示进程对文件的相关操作.

4 系统行为语义识别

行为语义识别过程主要包括以下3部分:行为语义表示、行为语义抽取和代表行为识别.

4.1 行为语义表示

从系统日志中提取有效的行为语义信息需要理解系统日志的行为语义.异构属性图模型中的实体与关系的语义更加复杂,如何从异常图中获取有效的行为语义是关键.知识图谱的语义表示给出了语义的有效表示方法——上下文信息.本文也通过系统日志在上下文信息来表示其行为语义.

利用知识图谱图嵌入表示学习方法可以从系统日志的上下文信息中学习其语义表示.其中的关键是需要把图中三元组映射到同一个向量空间.当前已有的知识图谱表示学习方法 Trans 系列方法均可实现图中三元组到同一向量空间的映射.下面通过图 2 的实例说明上下文语义的表示.假设现有 2 条系统日志:(cc1,read,a.c)和(cc1,read,b.c),第 1 条日志表示 cc1 进程读 a.c 文件,第 2 条日志表示 cc1 进程读 b.c 文件.显然这 2 条日志具有相同的上下文(cc1,read),这暗示它们具有相似的行为语义.显然向量化是一种有效的语义表示方法,在对每个元素进行向量化时尽可能让 a.c 和 b.c 的向量距离近一些.因此可以使用 TransE[16] 模型来学习每个元素的向量表示.

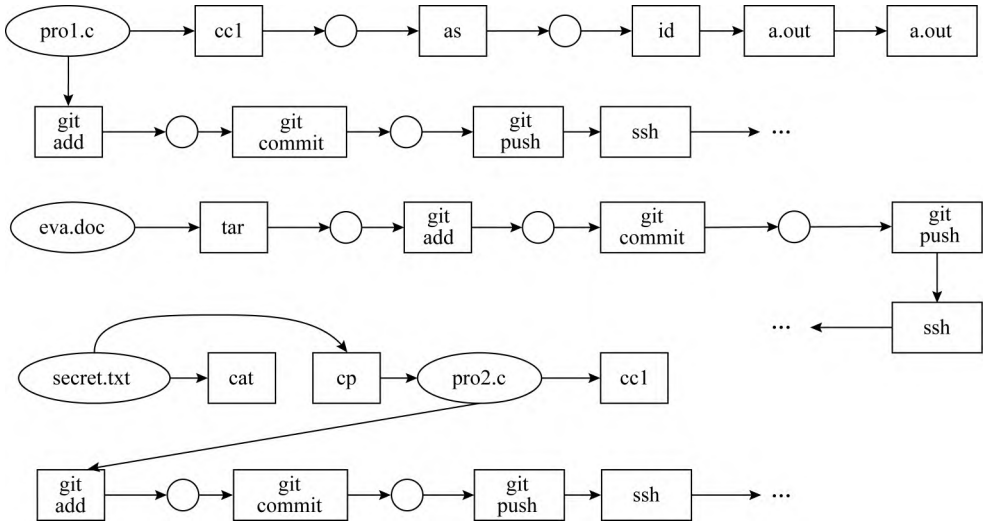

图 2　攻击场景溯源图

嵌入模型中的嵌入空间描述的是图三元组中 Head,Tail 和 Relation 之间的关系.TransE 模型的嵌入空间是基于以下这种理论假设:Head+Relation≈Tail,其表示在 TransE 模型的嵌入空间中 Head 实体的向量加上 Relation 的向量表示等于 Tail 的向量表示.以(cc1,read,a.c)和(cc1,read,b.c)为例,a.c 与 b.c 的向量表示是通过(cc1,read)表示,因此 a.c 与 b.c 向量表示是相近的.

在嵌入表示学习过程中,图中的每个元素都需要进行初始化.可以利用独热编码对每个元素进行编码,然后以该向量作为训练过程的输入.训练阶段采用 TransE 模型本身的目标函数.

TransR[17] 与 TransH[18] 是 transE 模型的改进算法,针对 1 对多和多对多关系的处理进行改进.尤其是 TransR 模型在实体空间与多个关系空间中建模实体与关系,因此在处理多关系方面较 TransE 有更好的性能.

4.2　行为语义抽取

在表示系统日志语义之后需要根据这些语义表示通过聚合提取有效的行为信息.因此行为提取可以归约为从构建的威胁图谱中提取语义相关的子图.与传统基于路径[3] 的方法相比,可以在威胁图谱中划分子图来表示行为实例.利用子图划分而不选择基于路径划分的原因是单一路径不能保留多分支数据传输行为的完整上下文.例如,基于路径划分的方法在数据泄露行为中并不能有效地把相关行为实例关联到一起,比如程序编译与 github 上传可能在不同的路径中.

为了从威胁图谱中抽取出描述行为实例的子图,可以采用一种自适用的前向深度优先遍历方法.图 2 给出了行为概要子图的示例.在图遍历过程中考虑了行为的时序关系,也就是后一个行为要发生在前一个行为之后.这种时间约束会过滤掉一大部分依赖关系.此外,可以看出一个系统实体的祖先通常包含关键行为上下文,然而这种祖先节点在前向深度优先遍历中是捕获不到的,因为其属性后向依赖节点.因此,在图遍历过程中需要包含其 1 跳入边.

由于系统日志记录的是粗粒度的依赖关系，因此不可避免地要面临依赖爆炸的问题.然而解决依赖爆炸问题并不是这里讨论的内容.

4.3 代表行为识别

基于以上处理之后，可以基于行为语义把整个图划分为一些语义相似的类别.但是这些语义是一些向量化的表示，如何表示这类行为是一个难点.一种比较简单的方法是把该类中所有元素的向量相加.然而，这种方法的有效性是建立在如下假设基础上的：划分后的威胁子图所包含的所有元素对行为语义的贡献都是相同的.显然这种假设实际上是很难满足的.对于一个上层针对攻击行为的分析任务来说，它可能包含了底层一系列相关操作，但是每个底层操作的重要性与必要性对于该任务是不同的.例如图2中的程序编译过程，用户通常不会直接编译源代码，而是先利用ls或是dir命令定位源代码.像ls和dir这种命令能表示用户的行为，但是对高层任务的语义贡献较小.关键的问题是如何自动化地给出每一个操作的相对重要度(重要性权重).通过观察可以看到与行为不相关的日志在会话中会更普遍，因此它们在不同的行为中不断地重复，而实际与行为相关的日志发生的频率反而较低.基于该观察，可以使用日志的频率作为事件重要度的一种度量.这里可以使用IDF(inverse document frequency)来定义日志对于所有行为的重要度.为了与IDF的使用相对应，日志记录可以看成文档中的词，整个日志可以看成文档.单个系统的IDF计算公式表示如下：

$$w_{\mathrm{IDF}}(e)=\log\left(\frac{s}{s_e}\right). \tag{1}$$

针对每个行为划分中的日志都有使用IDF计算的权重，用以表示其对于该行为语义的重要度或贡献度.

在当前场景中一个行为可以认为是一些语义相似的行为实例的集合.因此，聚类中的标签性的行为实例是具有代表性的实例(如聚类中性).如果能够确定有效的行为标签，安全运营人员就不需要对聚类空间中所有的行为实例进行调查，而仅仅调查具有代表性的行为实例即可，这将大大提高攻击调查的自动化水平.在已知不同行为实例的向量表示后，可以使用cosine相似度计算它们之间的语义关系：

$$s(\boldsymbol{F}_m,\boldsymbol{F}_n)=\frac{\boldsymbol{F}_m\cdot\boldsymbol{F}_n}{\|\boldsymbol{F}_m\|\times\|\boldsymbol{F}_n\|}=\frac{\sum\limits_{e_i\in\boldsymbol{F}_m}\sum\limits_{e_j\in\boldsymbol{F}_n}e_i\cdot e_j}{\sqrt{\sum\limits_{e_i\in\boldsymbol{F}_m}e_i}\times\sqrt{\sum\limits_{e_j\in\boldsymbol{F}_n}e_j}}. \tag{2}$$

为了把具有相似语义的行为实例聚合到一起，可以采用凝聚层次聚类分析算法(HCA)[19].在对威胁图谱进行聚类后，以距离聚类中心最近的行为为代表，使用该日志表示聚类中所有日志.

5 实验分析

本节通过DARPA TC数据集[20]对本文方法进行实验验证.DARPA TC数据集通过真实的APT攻击模拟采集了大量的相关数据，针对DARPA TC TA5.1的数据按第3节采用的8种日志构图方式构建溯源图.例如，NetFlowObject中的数据可以根据网络连接日志方式构建成remote_ip⇒process形式.这样针对DARPA TC数据可以构建一个完整的溯源图.

首先对于行为语义提取的精度进行实验分析.为了验证本文方法的有效性，选择了17种正常系统行为和8种攻击行为进行对比分析.针对这25种行为的语义识别分别从准确率、召回率、F1score这3种评估维度进行了评估，其中图表示学习方法选择的是经典的TransR模型.其实验结果如图3所示.

可以看出对于大部分系统行为，本文方法都可以进行有效的提取其攻击行为语义.

当前图表示学习方法较多，本文对比了不同的图表示学习方法，利用F1score进行评估各种方法的效果.对比方法有Node2vec[21]，Metapath2vec[22]，TransH，TransR和TransE，后面3个模型之前有过介绍.Node2vec是图表示学习的一种经典方法，主要是一种基于随机游走来刻画图中节点特征的方法.Metapath2vec是一种处理异构图的表示学习方法，在学习节点嵌入表示过程中加入了元路径的概念.

通过对比分析发现TransR方法相比其他表示学习方法的性能更好.之前的图表示学习方法通

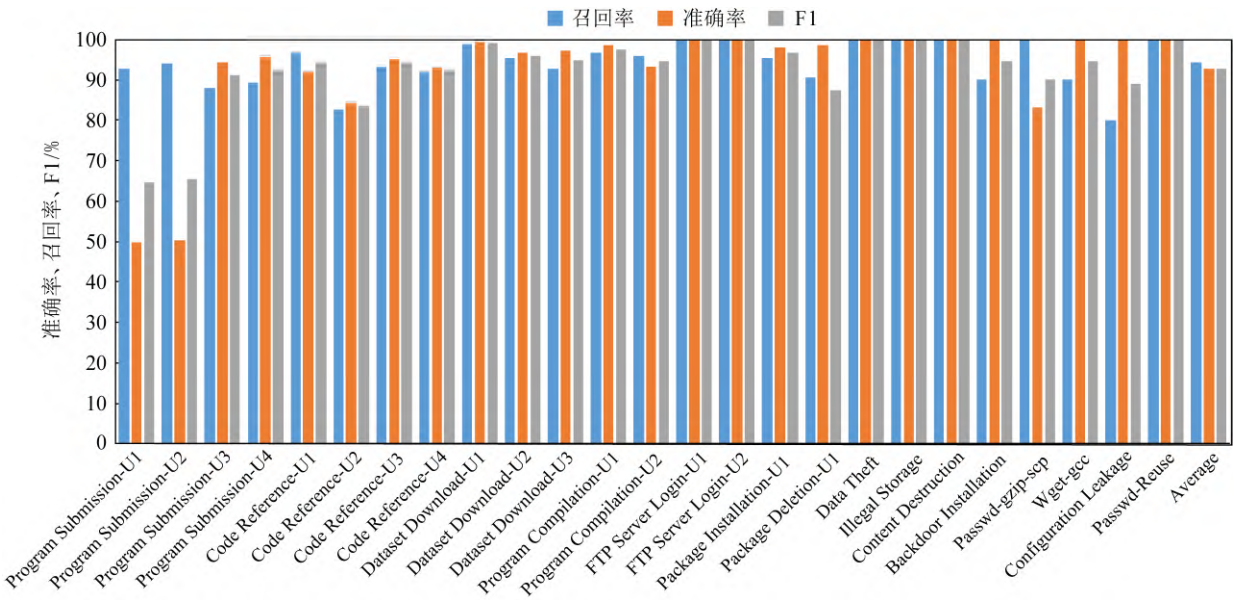

图 3　行为语义识别结果

常是将实体与关系映射到同一空间中，但是在攻击场景中存在多种类型的实体与关系，不同实体与关系具有不同属性. TransR 在处理实体空间与关系空间时会针对不同关系对应实体的不同属性，每一类关系又对应特定的关系空间. 这样可以大大提高攻击场景中的表示能力，从而得到更好的行为语义识别结果.

6　结　　语

针对当前企业安全分析过程中的日志与行为之间语义鸿沟问题，本文研究了当前的建模与方法，提出了一种自动化的系统行为语义识别方法. 这里借鉴了知识图谱在推荐系统上的应用方式，首先基于终端日志设计了有效的异构属性图表示方法，可以更好地描述整个威胁场景；然后，以上下文为语义基于知识图表示学习方法自动提取行为信息，完成了从底层日志到上层行为语义的关联，为安全分析人员提供更抽象的行为信息，从而大大降低了安全分析人员的知识门槛. 但是本文方法依然缺少可解释性，通过聚类得到的代表性行为需要安全专家人工进行解释与标注语义. 后续溯源图需要与安全知识图谱关联获取更丰富的语义，如果把动态的日志与静态的安全知识进行关联依然是一项具有挑战的工作.

参　考　文　献

[1] 彭祯方，邢国强，陈兴跃. 人工智能在网络安全领域的应用及技术综述[J]. 信息安全研究，2022，8(2)：110-116

[2] Pasquier T，Han X，Moyer T，et al. Runtime analysis of whole-system provenance [C] //Proc of ACM Conf on Computer and Communications Security (CCS'18). New York：ACM，2018：1601-1616

[3] Pasquier T，Han X，Moyer T，et al. Practical whole-system provenance capturer [C] //Proc of the 2017 Symp on Cloud Computing. New York：ACM，2017：405-418

[4] Milajerdi S，Gjomemo R，Eshete B，et al. HOLMES：Real-time APT detection through correlation of suspicious information flows [C] //Proc of 2019 IEEE Symp on Security and Privacy (SP). Piscataway，NJ：IEEE，2019：1137-1152

[5] King S T，Chen P M. Backtracking intrusions [C] //Proc of the 19th ACM Symp on Operating Systems Principles 2003. New York：ACM，2003：223-236

[6] Kwon Y，Wang F，Wang W，et al. MCI：Modeling-based causality inference in audit logging for attack investigation [C] //Proc of Network and Distributed System Security Symp. Rosten，VA：ISOC，2018

[7] Kwon Y，Kim D，Sumner W N，et al. LDX：Causality inference by lightweight dual execution [C] //Proc of ACM SIGARCH Computer Architecture News 2016. New York：ACM，2016：503-515

[8] Hassan W U, Noureddine M A, Datta P, et al. OmegaLog: High-fidelity attack investigation via transparent multi-layer log analysis [C] //Proc of Network and Distributed System Security Symp. Rosten, VA: ISOC, 2020

[9] King S T, Mao Z M, Lucchetti D G, et al. Enriching intrusion alerts through multi-host causality [C] //Proc of Network & Distributed System Security Symp. Rosten, VA: ISOC, 2005

[10] Haas S, Sommer R, Fischer M. Zeek-Osquery: Host-network correlation for advanced monitoring and intrusion detection [G] //IFIP Advances in Information and Communication Technology. Berlin: Springer, 2020: 248-262

[11] Ji Y, Lee S, Fazzini, et al. Enabling refinable cross-host attack investigation with efficient data flow tagging and tracking [C] //Proc of the 27th USENIX Security Symp. Berkeley, CA: USENIX Association, 2018: 1705-1722

[12] Liu Y, Zhang M, Li D, et al. Towards a timely causality analysis for enterprise security [C] //Network and Distributed System Security Symp. Rosten, VA: ISOC, 2018

[13] Hassan W U, Guo S, Li D, et al. NoDoze: Combatting threat alert fatigue with automated provenance triage [C] //Network and Distributed System Security Symp. Rosten, VA: ISOC, 2019

[14] Milajerdi S M, Eshete B, Gjomemo R, et al. POIROT: Aligning attack behavior with kernel audit records for cyber threat hunting [C] //Proc of ACM Conf on Computer and Communications Security (CCS'19). New York: ACM, 2019: 1795-1812

[15] Hassan W U, Bates A, Marino D. Tactical provenance analysis for endpoint detection and response systems [C] //Proc of 2020 IEEE Symp on Security and Privacy (SP). Piscataway, NJ: IEEE, 2020:1172-1189

[16] Bordes A, Usunier N, Garcia-Duran A, et al. Translating embeddings for modeling multi-relational data [C] //Proc of the 26th Int Conf on Neural Information Processing Systems. New York: Curran Associates Inc, 2013: 2787-2795

[17] Yankai L, Zhiyuan L, Maosong S, et al. Learning entity and relation embeddings with entity description for knowledge graph completion [C] //Proc of the 29th AAAI Conf on Artificial Intelligence. Menlo Park: AAAI, 2015: 2181-2187

[18] Wang Z, Zhang J, Feng J, et al. Knowledge graph embedding by translating on hyperplanes [C] //Proc of the 29th AAAI Conf on Artificial Intelligence. Menlo Park: AAAI, 2014: 1112-1119

[19] Jain A K, Murty M N, Flynn P J. Data clustering: A review [J]. ACM Computing Surveys, 1999, 31(3): 264-323

[20] Eshete B, Gjomemo R, Hossain M N, et al. Attack analysis results for adversarial engagement 1 of the DARPA transparent computing program [J/OL]. [2022-01-24]. https://arxiv.org/abs/1610.06936

[21] Grover A, Leskovec J. node2vec: Scalable feature learning for networks [C] //Proc of the 22nd ACM SIGKDD Int Conf on Knowledge Discovery and Data Ming. New York: ACM, 2016: 855-864

[22] Dong Y, Chawla N V, Swami A. metapath2vec: Scalable representation learning for heterogeneous networks [C] //Proc of the 23rd ACM SIGKDD Int Conf on Knowledge Discovery and Data Ming. New York: ACM, 2017: 125-144

薛见新

博士.主要研究方向为网络安全、安全知识图谱.

xuejianxin@nsfocus.com

王星凯

博士.主要研究方向为网络安全.

wangxingkai@nsfocus.com

张润滋

博士.主要研究方向为网络安全、AISecOps.

zhangrunzi@nsfocus.com

顾杜娟

博士,主任研究员.主要研究方向为网络安全、安全知识图谱.

gudujuan@nsfocus.com

刘文懋

博士.主要研究方向为云安全、容器安全.

liuwenmao@nsfocus.com