一种基于知识图谱的扩展攻击图生成方法

叶子维 郭渊博 李 涛 琚安康
(信息工程大学三院 郑州 450001)

摘 要 现有攻击图生成和分析方法主要依赖漏洞评分信息,无法判断软硬件环境等外部因素对漏洞评分的影响并进行修正,导致生成的攻击图难以精确反映节点和路径的真实风险程度。知识图谱中信息抽取和知识推理等工具是对多源途径获取的漏洞相关信息进行融合的有效手段,可以更准确地反映网络中节点和路径的风险程度。首先,设计了基于原子攻击本体的知识图谱,以对攻击图的输入和显示信息进行扩展;然后,提出了基于知识图谱的扩展攻击图生成框架,并在此基础上给出了攻击图生成算法以及攻击成功率、攻击收益的计算方法,从而实现了对漏洞更全面和精确的评分;最后,通过实验验证了所提方法的有效性。

关键词 攻击图,知识图谱,攻击成功率,攻击收益,风险评估

中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/jsjkx.190400092

Extended Attack Graph Generation Method Based on Knowledge Graph

YE Zi-wei GUO Yuan-bo LI Tao JU An-kang
(The Third Institute, Information Engineering University, Zhengzhou 450001, China)

Abstract Existing attack graph generation and analysis techniques mainly depend on vulnerability scores. External factors such as hardware and software cann't be considered to judge their impact and correct vulnerability scores. As a result, generated attack graph is difficult to accurately reflect the real risk of nodes and attack paths. Information extraction and knowledge reasoning in knowledge graph technique are effective means to integrate vulnerability information acquired by multiple sources, and can be used to calculate the risk of nodes and attack paths more accurately in the network. Firstly, knowledge graph based on atomic attack ontology is designed to extend the input and display information of attack graph. Then, an extended attack graph generation framework based on knowledge graph is proposed. On this basis, the attack graph generation algorithm and calculation of attack success rate and attack profit are given, so as to achieve a more comprehensive and accurate evaluation of vulnerabilities. Finally, experimental results verify the effectiveness of proposed method.

Keywords Attack graph, Knowledge graph, Attack success rate, Attack profit, Risk assessment

1 引言

攻击图技术是一种图形化的网络脆弱性分析技术。通过对目标网络和可能遭受的攻击行为进行建模,展示攻击者发动攻击时可能选择的攻击路径,既可指导防御方采取针对性修复和防御措施,也可为攻击者制定攻击计划提供依据。目前,攻击图主要分为状态攻击图和属性攻击图两类。状态攻击图[1-2]以网络安全状态为顶点,边表示网络安全状态的转换。由于同一状态可能对应图中的多个顶点,使用状态攻击图对大规模网络进行脆弱性分析时会产生状态爆炸问题,因此近年来针对状态攻击图的研究甚少。属性攻击图[3]通常以漏洞和节点权限为顶点,边表示漏洞和权限间的依赖关系。属性攻击图由于缓解了状态攻击图的状态爆炸问题,且视觉效果上更为直观,因此得到了广泛的应用,并衍生出了渗透依赖攻击图和属性依赖攻击图[4]等。

通常用于构建属性攻击图的输入信息主要包括网络拓扑、漏洞、网络配置、节点权限等[5-8],其中漏洞是所有信息中的核心,其利用难度和利用后果将直接影响用户的决策。然而,现有攻击图技术存在以下两方面问题。

1)对漏洞的评分不够精确,导致对网络节点和路径的风险分析结果不够精确。随着攻击技术的不断发展以及漏洞数量的日渐增多,传统的基于通用漏洞评分系统(Common Vulnerability Scoring System,CVSS)的漏洞评估方式越来越难以精确地反映漏洞的影响程度,主要表现为部分高危漏洞综合评分较低,同时也存在部分低危漏洞综合评分较高的现象。文献[9]采用定量分析与定性分析相结合的方法优化 CVSS

到稿日期:2019-04-17 返修日期:2019-07-30

叶子维(1990-),男,博士生,主要研究方向为网络脆弱性分析,E-mail:yezw2014@163.com;郭渊博(1975-),男,博士后,教授,博士生导师,主要研究方向为大数据安全、态势感知,E-mail:yuanbo_g@hotmail.com(通信作者);李 涛(1992-),男,博士生,主要研究方向为知识图谱;琚安康(1995-),男,博士生,主要研究方向为多步网络攻击检测、威胁情报。

的评估结果,但缺乏对漏洞可利用性的详细分析。文献[10]研究了漏洞类型对漏洞可利用性的影响,将漏洞类型作为评分要素之一对 CVSS 评分进行了改进,提高了分值多样性和准确度。文献[11]使用 BP 神经网络对 CVSS 指标体系进行优化,强化了其评估结果的客观性。上述方法共同的问题在于不能对某个特定的漏洞根据其所处的软硬件环境进行具体分析和评估,这使得基于漏洞扫描的攻击图生成和分析技术难以精确地反映节点和路径的风险程度,导致防御方采取的防御措施难以有效阻止攻击。

2)难以适应网络攻防态势的快速变化。随着大数据分析、威胁情报等技术的发展,大量新漏洞和新攻击方式在互联网上被快速公开。同时,新的防御手段也在对已知漏洞的利用难度和利用方式产生影响。这些信息既为安全研究人员及相关厂商提供了帮助,也为攻击者提供了新思路、新手段。在这种现状下,攻防双方对攻击图的自动构建、精确评估等能力提出了更高的要求。传统的攻击图构建方法由于输入信息种类少、信息源单一等原因,已难以满足需求。为了适应网络攻防态势的变化,研究人员尝试将攻击预算[12]、攻击意图[13]、0day 漏洞存在概率[14-17]等要素作为输入来对攻击图进行扩展。文献[18-20]证明了攻击图可以在发现攻击时动态地对后续攻击目标进行预警,但当发现新漏洞和基于未知漏洞发起的攻击时,目前的普遍做法仍是重新生成完整的攻击图,而鲜有对攻击图进行局部更新的研究。因此,现有技术依然难以满足攻防双方对攻击成功率、攻击收益进行快速、精确评估的需求。

知识图谱[21]是一种在语义网络基础之上实现智能化语义检索和关联分析的技术。通过从互联网页面中抽取实体和属性信息,并对实体间可能具有的关系进行抽取或推理,来实现一种新的信息检索模式,使用户可以很容易地获取与所检索内容相关联的各类信息。针对上述两种攻击图技术存在的问题,可利用知识图谱技术的多源信息融合特性将来自多个独立信息源的同一漏洞的相关信息进行互相印证或驳斥,避免错误评估漏洞的影响程度;而其信息抽取和推理技术可用于及时发现互联网上公开的新漏洞和新攻击方法,并指导攻击图的更新,提高攻击图的时效性。知识图谱技术的引入,可以使攻击图更加精确、及时地反映当前网络的安全状态,为防御方采取更合理的防御策略或为攻击方制定更好的攻击策略提供依据。

本文的思路是利用知识图谱技术对互联网上的软硬件、漏洞、攻击条件、攻击方式等安全相关信息进行关键属性抽取和关联分析,并将结果用于攻击条件的推理、攻击成功率和攻击收益的计算等。通过对来自多源途径(特别是安全论坛等非结构化信息源)的信息进行关联分析,可以判断软硬件的重要程度和历史安全性等,以获取安全研究人员对漏洞的分析结果,并推理出对同一漏洞的不同利用方式可能导致的不同利用结果,据此对漏洞的利用难度和影响程度进行修正。当发现有新的漏洞或攻击方式时,可用更新后的知识图谱来快速检索目标网络中是否存在可能受到新漏洞或新攻击方式影响的软硬件,并进一步指导漏洞的自动化扫描和攻击图的局部更新。

相对于现有攻击图的相关技术,本文方法有以下几方面优势。

1)更高的攻击成功率和攻击收益评估,使攻击图具有更强的实用性。现有技术主要依据来自单一信息源的信息评估攻击成功率和攻击收益,忽略了其他信息源。一旦信息源给出的信息出现偏差,现有技术就无法借助其他途径获取的信息对其进行修正。本文方法通过关联多源信息对攻击成功率和攻击收益进行综合评估,提高了评估结果的精确度。

2)智能化的非结构化信息抽取和应用,降低了人工处理的时间成本,提高了信息的利用率。现有技术主要从漏洞库等结构化信息源中获取信息,对于非结构化信息则需要手工编写应用规则。本文方法借助知识图谱中的实体抽取和知识推理技术,提高了发现非结构化信息及其相互间关联关系的效率,避免了手工方式的低效和容易丢失信息的问题。

3)更高的攻击图更新效率,可适应网络攻防态势的快速变化。当用于构建攻击图的信息发生变化时,现有技术需要重新生成和分析完整的攻击图。本文方法通过将新信息与图谱中已有信息进行关联,可以发现原攻击图中与新信息相关的节点,且只对相关节点进行修改,提高了攻击图的更新效率。

本文第 2 节介绍攻击图和知识图谱领域的研究现状,及本文用到的网络安全知识库;第 3 节给出原子攻击本体设计方案和知识图谱的构建过程;第 4 节给出攻击图生成框架,及攻击成功率和攻击收益的计算方法,并通过实验验证方法的有效性;最后总结全文,并阐述未来工作的研究方向。

2 相关工作

互联网上的安全相关信息数量众多、种类繁杂,全面掌握各类已公开的安全信息,有助于防御方提高对网络脆弱性分析的精确度,以及网络防护措施的有效性。知识图谱在人工智能的认知智能阶段被广泛采用,多源数据融合的特点使其有能力整合各类网络安全知识库中的信息,以便决策者尽可能全面且结构化地掌握安全信息,目前已有研究人员对知识图谱在网络安全中的应用进行了研究。为设计适用于攻击图生成和分析的本体及知识图谱,需对攻击图和知识图谱领域的现有成果进行总结分析,以确定所需的实体及关联关系。下面介绍现有研究成果和本文方法中用到的网络安全知识库。

2.1 攻击图生成与分析

如引言部分所述,目前攻击图相关研究主要针对的是属性攻击图。在攻击图生成方面,文献[12-13]研究了将攻击者的攻击预算和攻击意图作为输入的可行性。Kotenko 等[7]提出了手工构建安全规则和攻击模式知识库来指导攻击图生成的方法。Rick 等[13]在构建攻击图时考虑了攻击所需的时间窗口。但上述成果均需人工收集和分析相关信息,效率较低,且可能存在信息收集不够全面、未发现信息间的关联关系等问题。在海量信息中自动抽取输入信息和进行关联分析,可有效提高信息处理效率和信息利用率。

攻击图生成需要耗费大量的时间。陈锋等[4]对复杂网络进行子网划分，将各子网的攻击图合并成完整的攻击图。Li 等[22]提出了一种基于超图划分的前向搜索攻击图生成算法，从目标节点向攻击者初始节点进行反向路径搜索，避免了发现无用攻击路径带来的开销。Rick[13]和 Pieters[23]等提出了各自的攻击图分析框架，在攻击发生时根据已发现的攻击行为实时生成攻击图，用于预判攻击者可能的后续攻击行为。但在实践中，当信息源更新时（例如漏洞库收录了新的漏洞），现有成果都需要重新生成完整的攻击图。而理论上，只根据与当前网络环境相关的新信息对攻击图进行局部更新，即可有效提高新攻击图的生成效率，但目前尚未有相关研究。

在攻击图分析方面，现有方法主要依据 CVSS 评分来分析单个节点的攻击成功率和攻击收益。攻击路径的攻击成功率和攻击收益主要采用贝叶斯网络[24-27]和马尔可夫模型[28-30]进行计算。一旦 CVSS 对某个漏洞给出了不符合实际情况的评分，现有方法就难以对该评分进行修正，进而导致不精确的分析结果。因此，需要通过融合多源数据来发现并修正该类漏洞的评分，以提高攻击图的实用性。

2.2　面向网络安全领域的知识图谱

目前，知识图谱在网络安全领域的主要研究方向是设计网络安全本体和实现信息抽取。Jia 等[31]提出了一种构建网络安全知识库的方法，主要用于入侵检测和态势感知，并设计了网络安全本体和网络安全知识库架构，实现了网络安全相关实体的抽取和属性及关系的推断。梁中等[32]研究了如何设计安全本体和主题爬虫，以从互联网获取的信息中抽取安全相关内容用于信息安全主题教育。Iannacone[33]和 Asamoah[34]等设计了各自的网络安全本体，用于创建针对不同目的的网络安全知识图谱。

本文的主要思路是将知识图谱应用于属性攻击图的生成和分析。属性攻击图通常以漏洞为顶点，其他信息用于发现攻击路径和计算攻击成功率及攻击收益。因此，构建可辅助攻击图生成的知识图谱，应当以漏洞为核心实体，根据需求设置其他相关实体并与漏洞实体进行关联。上述成果由于所面向的应用领域无须对攻击成功率和攻击收益进行详细计算，其设计的网络安全本体中未包含相关信息，因此无法直接用于指导攻击图的生成和分析，须针对属性攻击图重新设计本体并构建知识图谱。本文在参考上述成果中的漏洞与其他实体间的关联关系的基础上，提出了包含软件、硬件、漏洞、攻击 4 类实体的原子攻击本体，详细设计将在 3.1 节给出。

2.3　网络安全知识库

构建攻击图所需的网络安全知识可分为两类：漏洞信息和攻击信息。漏洞信息主要来自各国政府或安全企业建立的漏洞信息库，前者包括公共漏洞和暴露 CVE[1)]、美国国家漏洞数据库 NVD[2)]、中国国家信息安全漏洞共享平台 CNVD[3)]等；后者包括知道创宇 Seebug 漏洞平台[4)]、360 补天漏洞响应平台[5)]等。通常，漏洞库中收录的漏洞包含了漏洞编号、影响范围、威胁等级、利用方式、利用收益等信息，使安全相关企业和从业人员可以对漏洞进行原理分析、防御和修复。由于收录途径和评分机制存在差异，漏洞库之间通常存在某些漏洞只被部分漏洞库收录、同一漏洞的风险程度评分不同等现象，为全面掌握已公开漏洞带来了困难。

攻击信息是指具体的漏洞利用方式及攻击难度、攻击收益等信息。随着攻击技术的发展，能否全面收录已被公开的攻击信息决定了能否在已发现全部安全漏洞的基础上对网络安全状态进行精确评估。攻击信息主要从安全论坛中获取，如 i 春秋论坛[6)]等；或从各安全相关企业构建的应急响应中心获取，如腾讯安全应急响应中心 TSRC[7)]、阿里安全响应中心 ASRC[8)]等。

3　基于原子攻击本体的知识图谱构建

知识图谱的基本组成要素是实体、实体间的关系和实体具有的属性。本文旨在借助知识图谱来提高对攻击图中节点和攻击路径的攻击成功率、攻击收益等信息的评估准确度，因此在研究了影响攻击成功率和攻击收益因素的基础上进行了本体、实体和知识图谱的设计。

3.1　本体设计

知识图谱反映的是具体信息和信息间的关联关系，而本体是概念和概念间关系的一种抽象表达，因此良好的本体设计有助于明确知识图谱中应包含的信息和关系种类。在攻击图相关技术中，最小攻击单位称为原子攻击，针对原子攻击设计本体并构建攻击图，可以实现对单次攻击行为的细粒度分析。如第 1 节所述，属性攻击图缓解了状态攻击图的状态爆炸问题，在对大规模网络进行脆弱性分析时具有更高的效率和更好的可视化效果，因此本文采用属性攻击图，并根据属性攻击图的基本构建思想提出了原子攻击本体，如图 1 所示。

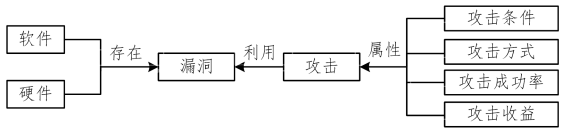

图 1　原子攻击本体

Fig. 1　Atomic attack ontology

在属性攻击图中，原子攻击通常由顶点表示，其实际意义是一次漏洞利用行为，因此漏洞是属性攻击图的核心。一方面，漏洞依附于软硬件实体而存在；另一方面，漏洞的存在又是攻击发生的必要前提。而攻击的实施条件、攻击成功的收益等属性决定了攻击图中节点之间的连接关系和节点及路径的风险程度，这是使用攻击图技术对网络进行脆弱性分析的主要依据。本文为原子攻击本体共设计软件、硬件、漏洞、攻击 4 种实体。

1) http://cve.mitre.org

2) https://nvd.nist.gov

3) http://www.cnvd.org.cn

4) https://www.seebug.org

5) https://butian.360.cn

6) https://www.ichunqiu.com

7) https://security.tencent.com

8) https://security.Alibaba.com

1)软件。目标网络中使用的各类存在的已知漏洞的软件,以软件的名称和版本号进行标识。软件与漏洞之间为多对多映射关系,即特定版本的软件可能存在多个漏洞,而同一漏洞可能存在于同一软件的多个版本中。

2)硬件。目标网络中使用的各类存在的已知漏洞的硬件,以硬件的品牌和型号进行标识。硬件与漏洞之间同样为多对多映射关系。

3)漏洞。目标网络中存在的已知软硬件漏洞,以漏洞 ID 进行标识。如 2.2 节所述,由于各漏洞库收录的漏洞不完全相同,且每个漏洞库都有独立的漏洞 ID 编码方式,因此应尽可能采用某个漏洞收录全面、应用范围广泛、评分方式公认合理的数据库的漏洞 ID。

4)攻击。攻击者可能采取的具体的漏洞利用行为,以通用攻击模式列举和分类(Common Attack Pattern Enumeration and Classification,CAPEC)中收录的攻击方式的对应 ID 和利用的漏洞 ID 进行标识。每个攻击实例包含 4 种属性,分别为攻击条件、攻击方式、攻击成功率和攻击收益。攻击条件指发动攻击需具备的基本条件,如远程访问、本地访问、本地管理权限等;攻击方式指具体的漏洞利用过程,如缓冲区溢出、格式化字符串、SQL 注入等;攻击成功率指单次攻击的成功概率,受所需知识、时间窗口、经济成本等因素的影响;攻击收益指攻击成功实施后攻击者的收益或网络可能遭受到的损失,如信息泄露、拒绝服务或权限提升等。

基于上述原子攻击本体构建的知识图谱,可以实现对同一漏洞的多种攻击条件、攻击方式、攻击收益的标记,避免了传统脆弱性分析技术中只能对同一属性进行单一值标记而导致的分析结果不够精确的问题。

3.2 知识图谱的构建

知识图谱的构建过程包含信息获取和图谱构建两部分。信息抽取是知识图谱构建过程中须解决的关键问题,其含义是从多种异构数据源中抽取指定的实体、关系和属性信息。通常采用爬虫技术,从漏洞信息库、安全论坛和各企业应急响应中心等多种信息源获取所需信息,这方面已有很多成熟的方法和工具,其内容不是本文研究的重点。在信息抽取阶段,可根据目标网络的特征筛选信息源,使生成的知识图谱对一般网络或工业控制网络、移动互联网等特种网络均可起到辅助安全分析的作用。图谱构建通过对获取到的海量信息进行信息抽取和推理,来实现信息的关联分析,并以图形化结构存储信息处理结果。完成图谱构建后,即可在知识图谱的指导下针对具体的网络环境生成攻击图。在攻击图生成过程中,攻击实例的攻击方式和攻击条件可用于指导前后置条件的匹配,从而发现攻击路径;攻击成功率和攻击收益属性可用于辅助后续的风险程度分析。

实体抽取是信息抽取的核心。实体抽取也称为命名实体识别(Named Entities Recognition,NER)[35],是从信息源中获取命名实体的过程。通常采用条件随机场(Conditional Random Field,CRF)、隐马尔可夫模型(hidden Markov Model,HMM)、最大熵模型等机器学习方法来实现,以识别的精确率和召回率作为指标来评估识别的质量。本文方法中需要抽取的实体即 3.1 节所述的 4 类实体。

关系抽取是从信息源中抽取实体与实体间、实体与属性间的关系,现有方法包括模式匹配、面向开放域的信息抽取框架、条件随机场等。本文方法中需要抽取的关系包括漏洞与软硬件的存在关系、攻击的 3 种属性与漏洞之间的存在关系。

属性抽取是从信息源中获取特定实体的属性信息。本文方法中的属性主要包括软件的名称和版本、硬件的厂商和型号、漏洞的 ID,以及攻击的方式、难度和收益。其中,软硬件和漏洞的属性在结构化信息源中较易获取,攻击方式等需要从非结构化的攻击信息源中获取。

知识推理是根据知识图谱中已有的实体、关系和属性,通过推理方法建立新的关系或发现新的属性,从而对知识图谱进行扩展。本文提出的方法中,知识推理主要根据攻击条件和攻击方式来对攻击成功率和攻击收益进行推理。路径排序算法[36]是目前知识推理方面利用推理规则实现关系建立的经典方法之一,其核心思想是根据两个实体间的连接路径来判断是否存在潜在的关系。例如,假设漏洞 v 可对软件 s_1 发动缓冲区溢出攻击,则同样存在漏洞 v 的软件 S_2 也可能受到由漏洞 v 引发的缓冲区溢出攻击。相较于词嵌入向量[37]和概率图模型[38]等知识推理技术,路径排序算法具有容易预测、准确性较高、无需预先了解知识图谱的拓扑等优点。以集合 $Rule=\{\langle$实例,关系,实例$\rangle|\langle$实例,关系,属性$\rangle|\langle$实体,关系,实例$\rangle\}$表示推理规则,3 个三元组分别表示对实例间关系的推理、对实例具有的属性的推理、对实体和实例间关系的推理。

图 2 为从 CVE、CNVD 漏洞信息库和腾讯、360 等应急响应中心采集真实数据生成的知识图谱。如图 2 所示,"Intel Xeon Processor E5 Family"为硬件实例,"CVE-2017-5753"为漏洞实例,两者之间为存在关系,与实体间的关系对应;同理,"Microsoft Office 2016"为软件实例,"CVE-2018-0802"为另一个漏洞实例,两者之间也为存在关系。攻击实例的 4 种属性从左至右依次为攻击条件、攻击方式、攻击成功率和攻击收益。为了便于查询,将攻击实例的 4 种属性关联到对应的漏洞实例。

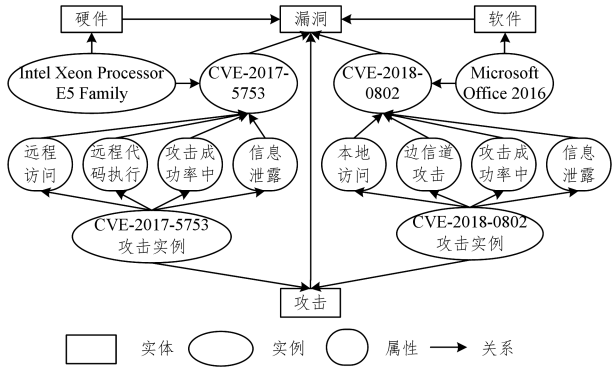

图 2 局部知识图谱

Fig. 2 Part of knowledge graph

4 攻击图的生成与分析

4.1 攻击图的生成

本文提出的扩展攻击图生成框架如图 3 所示。该框架中的信息获取和知识图谱构建部分在 3.2 节已有说明。在攻击图生成部分,拓扑扫描和漏洞扫描是属性攻击图生成的基础;属性标记是对漏洞对应的攻击实例的各项属性进行标记,以

便在后续过程中检查攻击条件是否匹配，为节点和路径的风险程度计算提供依据等；攻击条件匹配是根据节点连接关系、攻击条件、攻击收益等信息来判断节点间是否存在攻击行为的因果关系，即发现攻击路径；可视化展示是将生成的攻击图以易于理解和观察的方式进行展示。构建的知识图谱主要在属性标记和攻击条件匹配两个步骤中，通过查询漏洞的编号、对应的攻击实例的攻击条件、方式、成功率和收益，来指导从目标节点出发的反向路径搜索。每个漏洞对应的攻击条件和攻击收益中与权限相关的部分表明攻击者利用该漏洞所需要的权限和成功利用漏洞后可获取的权限，即攻击的前置条件和后置条件。

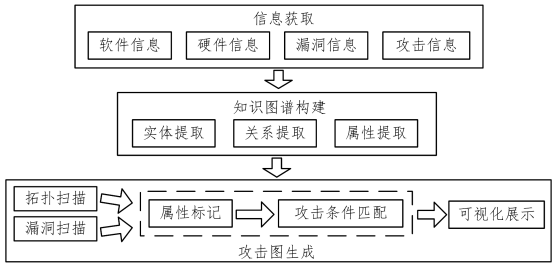

图 3　基于知识图谱的攻击图生成框架

Fig. 3　Framework of attack graph generation based on knowledge graph

属性标记和攻击条件匹配两个步骤对应的攻击图生成算法如算法 1 所示。

算法 1　基于知识图谱的扩展攻击图生成算法

输入：节点集合 $N=\{n_1,n_2,\cdots,n_p\}$，漏洞集合 $V=\{v_1,v_2,\cdots,v_q\}$，网络节点邻接矩阵 AM，原子攻击知识图谱 AKG

输出：攻击图 AG

```
1. for v_a∈V,1≤a≤q
2.     MarkAtt(v_a,AKG);
3. for n_i∈N,1≤i≤p
4.     v_i=GetVul(n_i);
5. if v_i=NULL
6.     continue;
7.     else
8.     while n_j=FindAdjacent(n_i,AM) do
9.         MarkRead(n_j);
10.    while GetVul(v_j)=true&& Pro(n_j)≥Con(n_i) do
11.        CreactLink(v_i,v_j);
12.     end while
13.     end while
14. end if
15. ClearRead(N);
16. end for
17. return AG
```

该算法中各行对应操作的说明如下：

步骤 1 和步骤 2 中，对于全部 $v\in V$，在知识图谱 *AKG* 中检索对应的原子攻击本体，读取和记录该漏洞对应的攻击实体的攻击条件、攻击方式、攻击成功率和攻击收益属性，攻击条件 *Con* 作为漏洞的前置条件，攻击收益 *Pro* 作为后置条件。

步骤 3－步骤 16 中，依次将 N 中的节点作为攻击目标节点，执行步骤 4－步骤 15，查找其前置节点并建立连接关系，直到遍历 N 中的全部节点。

步骤 4 获取攻击目标节点 n_i 存在的漏洞 v_i。步骤 5－步骤 6 中，若 n_i 不存在漏洞，则选择 N 中的下一个节点作为攻击目标节点。

步骤 7－步骤 14 中，若 n_i 存在漏洞 v_i，则在邻接矩阵 ***AM*** 中查找与 n_i 相邻的未读取节点，将其设为 n_j，并将 n_j 标记为已读取；若 n_j 存在漏洞 v_j，且 v_j 的攻击收益能满足 v_i 的攻击条件，则为 v_i 和 v_j 建立连接关系，v_j 为 v_i 的前置漏洞；若 n_j 不存在符合条件的 v_j，则重复步骤 8－步骤 13，直至 n_i 的全部邻接节点都被标记为已读取。

步骤 15 清除全部节点的已读取状态，以便为下一个节点建立连接关系。

步骤 17 完成攻击图的生成。

在攻击图构建完成后，攻击方式用于指导防御方采取针对性防御措施，攻击成功率用于判断全部网络节点的防御优先级。攻击条件和攻击收益中与权限无关的部分分别用于对这两项属性的量化计算，以便对攻击路径的风险程度进行比较。

相对于现有攻击图生成方法，本文方法需要对每个漏洞顶点都进行大量的额外信息标记，会产生更大的空间开销。由于对每个漏洞顶点标记了相同类型的额外信息，因此额外的空间开销主要与漏洞数目有关。设漏洞顶点数目为 m，边数目为 l，则额外的空间开销的复杂度为 $O(m)$。根据文献[39]，现有开源或商用的攻击图生成和分析工具的复杂度均为 $O(m^2)$或 $O(m\log m)$，高于 $O(m)$，因此本文方法产生的额外空间开销是可以接受的。

算法 1 的设计借鉴了广度优先搜索的思想，其时间复杂度与广度搜索算法相同。根据文献[40]，该算法的时间复杂度为 $O(m+l)$。如果从安全知识库中获取新的漏洞信息，则只需在知识图谱中添加相应的实例、关系和属性，并对攻击图进行局部改动。这种局部改动的时间复杂度为 $O(\Delta m+\Delta l)$，即网络中存在的新漏洞数及与之关联的边数规模之和。由于新漏洞的集合 ΔV 和边的集合 ΔE 为全局漏洞集合 V 和边集合 E 的真子集，因此 $O(\Delta m+\Delta l)<O(m+l)$。这表明本文方法相对于重新生成完整的攻击图，减小了时间开销，提高了攻击图的时效性。

4.2　攻击成功率与攻击收益的计算

攻击成功率和攻击收益的计算是从攻击图中判断攻击者可能选择的攻击路径的重要前提。攻击成功率反映了攻击者在某条攻击路径上成功完成全部攻击行为的概率，攻击收益反映了每条攻击路径的投入与产出比。传统攻击图分析技术中，对攻击成功率和攻击收益的计算主要依据来自单一信息源的漏洞评分信息，一旦信息源的评分方式不合理，就会严重影响计算结果的精确性；此外，传统技术较少考虑攻击者目的、能力等缺乏可靠依据、实践中难以获取的参数，从而导致实用性不足。

基于知识图谱生成的攻击图可以实现攻击成功率和攻击收益的智能化分析。通过对来自多源的攻击信息的实体、关系和属性的抽取，可以从非结构化信息中发现不会在漏洞库中体现的漏洞相关信息（如存在漏洞的软硬件的重要程度、攻击对时间窗口的要求、对设备的物理损伤等），从而实现较传

统方法更高的攻击成功率和更精确的攻击收益分析。

对于单个原子攻击，其攻击成功率应当是综合评估所有可能影响成功率的因素而得到的唯一值。设共有 a 个影响攻击成功率的因素，每个要素各自的权重为 1，则该原子攻击的攻击成功率 $Suc_{\text{node}}=\sum_{i=0}^{a} l_i Suc_i$，$node\in N$。

单个原子攻击的攻击收益，可能会由于攻击者的攻击目的、攻击手段不同而产生多种结果，因此同一攻击实体可以具有多个攻击收益属性。设共有 b 个攻击收益属性，则该原子攻击的综合攻击收益为 $Ben_{\text{node}}=\sum_{i=0}^{b} Ben_i$，$node\in N$。

对于任意包含 x 个节点的攻击路径，设其从初始节点到目标节点的节点序号依次为 1 至 x，则该路径的综合攻击成功率 $Suc_{\text{path}}=\prod_{i=1}^{x} Suc_i=\prod_{i=1}^{x}\sum_{j=0}^{a} l_{ij}Suc_{ij}$，路径的综合攻击收益 $Ben_{\text{path}}=\sum_{i=1}^{x} Ben_i=\sum_{i=1}^{x}\sum_{j=0}^{b} Ben_{ij}$。

4.3 实验分析

以文献[15-16，19-20]中的实验场景为例，设计如下实验来验证本文方法的主要优势。

图 4 所示的网络拓扑为一个简易的典型内部网络模型。防火墙将互联网与内网路由器隔离，主机 1、主机 2 和 FTP 服务器直接连接到路由器上，主机 1 和主机 2 可访问 FTP 服务器，数据库服务器连接到 FTP 服务器上，接收和响应来自 FTP 服务器的请求。网络中存在的漏洞列表如表 1 所列，各项属性从 CVE 获取。假设攻击者在穿透防火墙后对内部网络发起攻击，则使用传统方法生成的攻击图如图 5 所示。

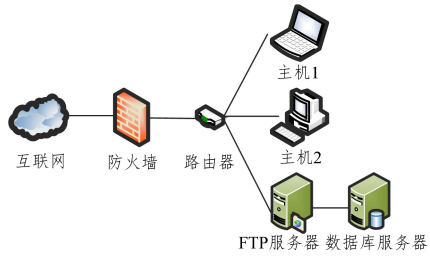

图 4 网络拓扑结构

Fig. 4 Network topology

表 1 漏洞信息

Table 1 Information of vulnerabilities

所在位置	漏洞 ID	CVSS 评分	攻击条件	攻击复杂度	攻击后果
路由器	CVE-2016-6415	5.0	network	low	信息泄露
主机 1	CVE-2017-0290	9.3	network	medium	信息泄露和系统破坏
主机 2	CVE-2017-8464	9.3	network	medium	信息泄露和系统破坏
主机 2	CVE-2016-5195	7.2	local	low	权限提升
FTP 服务器	CVE-2014-0160	5.0	network	low	信息泄露
数据库服务器	CVE-2014-3566	4.3	network	medium	信息泄露

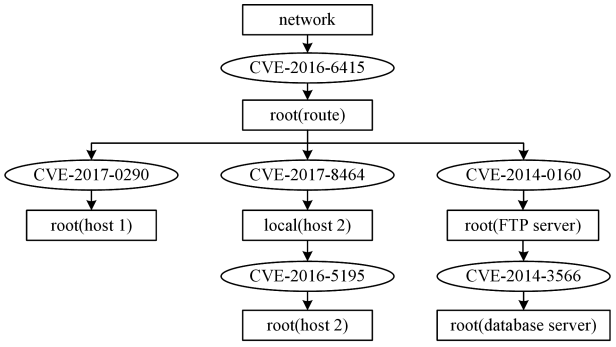

图 5 传统攻击图

Fig. 5 Traditional attack graph

通过使用传统攻击图对网络脆弱性进行分析，可知当前网络环境存在以下特点：

1）路由器是所有攻击路径的第一个节点，保证路由器的安全即可保证整个内部网络的安全；

2）攻陷路由器后，对主机 1 仅需实施一次攻击即可获取 root 权限，且主机 1 存在的漏洞评分最高，攻击后果最严重；

3）对主机 2 需实施两次攻击才能获取 root 权限，两次攻击的目的分别是获取 local 权限和将 local 权限提升为 root 权限；

4）对 FTP 服务器实施一次攻击即可获取 root 权限，但 FTP 服务器存在的漏洞评分较低，攻击后果较轻；

5）对于数据库服务器，在攻陷 FTP 服务器后须再实施一次攻击才能获取数据库服务器的 root 权限，且数据库服务器存在的漏洞评分更低，攻击后果也较轻。

根据上述分析，可得出各节点的防御优先级为路由器＞主机 1＞主机 2＞FTP 服务器＞数据库服务器。然而，实际应用中，FTP 服务器和数据库服务器上存在的漏洞都是 OpenSSL 协议的漏洞，其风险程度应当为高危。CVSS 给出中等评分的原因是这两个漏洞的利用后果中不包括破坏系统。

采用本文方法构建知识图谱和生成攻击图时，首先使用命名实体识别技术从安全论坛、安全新闻网站等信息来源中获取漏洞的相关信息。目前，命名实体识别工具主要有宾夕法尼亚大学的 NLTK[41] 和斯坦福大学的 Stanford NER[42]，两种工具的对比如表 2 所列。

表 2 NLTK 与 Stanford NER 的对比

Table 2 Comparison between NLTK and Stanford NER

工具	开发机构	开发语言	是否支持中文	语法解析效果	可扩展性
NLTK	宾夕法尼亚大学	Python	否	差	好
Stanford NER	斯坦福大学	Java	是	好	差

由于 NER 具有良好的中文支持和可扩展性，因此选择 NER 进行相关信息的抽取。根据 FreeBuf[1]、知道创宇[2] 等网站或团队发布的分析报告，CVE-2014-0160 可用于获取服务器内存中存储的用户名、密码、私钥等信息；CVE-2014-3566 可用于窃取使用 SSLv3 协议加密的通信内容。而 OpenSSL 协议被广泛应用于电子商务、VPN 隧道建立等领域，显然该

协议存在的信息泄露漏洞较一般软件的信息泄露漏洞存在更大的安全隐患，由此可知这两个漏洞的风险程度评分应当由来自漏洞库的中危评分修正为高危。此外，由多个应急响应中心的公开信息可知，CVE-2017-8464 和 CVE-2017-0290 的攻击收益都包括了一般信息泄露和系统破坏，因此这两个漏洞的综合攻击收益应为这两项独立攻击收益之和。对于本案例中的其余漏洞，从各类知识库中获取的攻击成功率和攻击收益信息与 CVE 给出的结果相同，因此直接采用 CVE 的结论。

图 6 为基于本文方法生成的攻击图。漏洞顶点左侧的攻击实例属性框中列出的依次为攻击方式、攻击条件、攻击成功率、攻击收益。

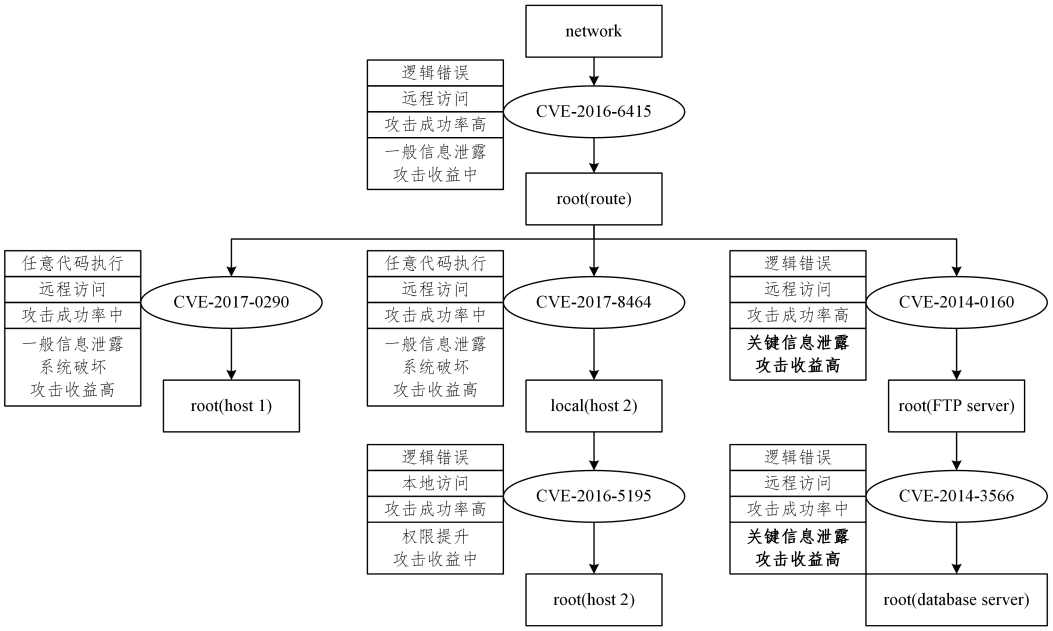

图 6　基于知识图谱的攻击图

Fig. 6　Attack graph based on knowledge graph

在基于知识图谱生成的攻击图中，对路径的攻击成功率和攻击收益的分析精确度随着对节点分析精确度的提高而提高。例如，对于路由器→FTP 服务器→数据库服务器这条攻击路径，由于扩展后的攻击图中 FTP 服务器和数据库服务器的攻击收益均修正为高，该路径的整体攻击收益计算结果也会提高。根据扩展后的攻击图，各节点的防御优先级为路由器＞主机 1≈FTP 服务器＞数据库服务器＞主机 2。参考上文对两个服务器上存在的漏洞的风险程度的分析可知，使用基于知识图谱的攻击图分析出的防御优先级序列相比使用信息源单一的传统攻击图分析出的防御优先级序列更加符合实际情况。

上述实验分析说明了基于知识图谱的攻击图相对于传统攻击图，对网络安全状态的评估更加精确。需要注意的是，在将本文方法应用到大规模网络时，可能存在较大的额外空间开销，具体开销量在 4.1 节已有说明，其空间复杂度为$O(m)$。

为了进一步测试本文提出方法的性能，将其与文献[18]和文献[27]中的方法进行对比。为测试本文所提方法在攻击图局部更新方面的性能，首先从输入信息中去除数据库服务器及其上存在的漏洞 CVE-2014-3566，使用 3 种方法分别生成原始攻击图，记录所需时间；然后在输入信息中加入数据库服务器及漏洞 CVE-2014-3566，使用 3 种方法更新攻击图，记录所需时间，测试结果如表 3 所列。实验环境中，操作系统为 Kali 2.0.0，内存为 2.0GB。

表 3　攻击图生成时间的对比

Table 3　Comparison of generation time of attack graph

（单位：ms）

方法	生成原始攻击图	更新攻击图
文献[18]方法	20	22
文献[27]方法	19	20
本文方法	21	3

对比表 3 中的数据可知，在生成原始攻击图时，本文方法需要从知识图谱中读取和记录更多的漏洞相关信息，因此时间消耗相对于文献[18]和文献[27]的方法有轻微的提升；但是，文献[18]和文献[27]的方法无法对攻击图进行局部更新，当有新的信息输入时只能重新生成完整的攻击图，而本文方法可以仅对与新的输入信息有关的部分进行更新，因此消耗的时间远少于文献[18]和文献[27]的方法。

文献[18]和文献[27]与本文研究内容在漏洞信息源、分析精度、攻击图局部更新能力等方面的比较如表 4 所列。

表 4　各文献研究内容的对比

Table 4　Comparison of contents of each literature

文献	漏洞信息来源	攻击成功率与收益分析精度	支持攻击图局部更新	复杂度
文献[18]	CVSS	主观，不精确	否	$O(m^2)$
文献[27]	CVSS	客观，不精确	否	$O(m\log m)$
本文	多源途径	客观，精确	是	$O(m+l)$（生成） $O(\Delta m+\Delta l)$（更新）

[1] https://www.freebuf.com/atricles/web/31553.html

[2] https://www.seebug.org/vuldb/ssvid-92692

结束语 本文设计了基于软硬件资产、漏洞和攻击的原子攻击本体及知识图谱，提出了利用知识图谱来辅助构建和分析攻击图的方法。通过对来自多种信息源的漏洞和攻击信息进行抽取和关联，可以实现对原子攻击的方式、难度和收益的智能化分析，从而实现对攻击路径的攻击成功率和收益的高效、精确判断。该方法适用于各种一般或特种网络环境，具体适用的网络类型取决于构建知识图谱时选择的知识库。例如，选择工业控制系统漏洞数据库[1)]可适用于工业控制网络，选择移动互联网漏洞数据库[2)]可适用于移动互联网。该方法解决了现有攻击图生成和分析技术中由于相关信息获取不全面导致的不能及时、准确反映当前网络安全状态的问题，为采取网络防御措施提供了更加完善的依据。

下一步将主要研究如何优化本文方法在大规模网络中应用时的性能。此外，本文设计的原子攻击本体为通用性设计，未来将通过选取特定领域的安全知识库来实现对工业控制网络、移动互联网、信息物理系统等特种网络的攻击图生成和分析，并根据具体类型的特种网络设计原子攻击本体，以提高对特种网络的针对性。

参 考 文 献

[1] JHA S, SHEYNER O, WING J. Two formal analyses of attack graphs[C]// Proceedings 15th IEEE Computer Security Foundations Workshop(CSFW-15). IEEE, 2002: 49-63.

[2] SHEYNER O, HAINES J, JHA S, et al. Automated generation and analysis of attack graphs[C]// IEEE Symposium on Security and Privacy. IEEE, 2002: 273-284.

[3] WANG L, NOEL S, JAJODIA S. Minimum-cost network hardening using attack graphs [J]. Computer Communications, 2006, 29(18): 3812-3824.

[4] CHEN F, MAO H D, ZHANG W M, et al. Survey of attack graph technique [J]. Computer Science, 2011, 38(11): 12-18. (in Chinese)
陈铎，毛捍东，张维明，等. 攻击图技术研究进展[J]. 计算机科学，2011，38(11)：12-18.

[5] WANG S, ZHANG Z, KADOBAYASHI Y. Exploring attack graph for cost-benefit security hardening: a probabilistic approach[J]. Computers & Security, 2013, 32(1): 158-169.

[6] HONG J, KIM D S. Harms: hierarchical attack representation models for network security analysis[C]// The 10th Australian Information Security Management Conference. Western Australia, 2012: 1-8.

[7] KOTENKO I, STEPASHKIN M. Attack graph based evaluation of network security [C] // IFIP International Conference on Communications and Multimedia Security. Springer Berlin Heidelberg, 2006: 216-227.

[8] WANG L, ISLAM T, LONG T, et al. An attack graph-based probabilistic security metric[C]// IFIP Annual Conference on Data and Applications Security and Privacy. Springer Berlin Heidelberg, 2008: 283-296.

[9] LIU Q, ZHANG Y. VRSS: A new system for rating and scoring vulnerabilities[J]. Computer Communications, 2011, 34(3): 264-273.

[10] LEI K, ZHANG Y, WU C. A system for scoring the exploitability of vulnerability based types [J]. Journal of Computer Research and Development, 2017, 54(10): 2296-2309.

[11] LIAO D, ZHOU M, LIU D, et al. Assessment method of automatic optimizing CVSS v2.0 vulnerability indicators [J]. Computer Engineering and Applications, 2015, 51(2): 103-107.

[12] OU X, BOYER W F, MCQUEEN M A. A scalable approach to attack graph generation[C]// The 13th ACM Conference on Computer and Communications Security. ACM, 2006: 336-345.

[13] RICK V H. A framework for the motivation of attackers in attack tree analysis [D]. Holland, Delft: Delft University of Technology, 2015.

[14] WANG L, JAJODIA S, SINGHAL A, et al. k-Zero day safety: measuring the security risk of networks against unknown attacks[J]. Lecture Notes in Computer Science, 2010, 11(1): 573-587.

[15] WANG L, JAJODIA S, SINGHAL A, et al. k-Zero day safety: a network security metric for measuring the risk of unknown vulnerabilities[J]. IEEE Transactions on Dependable & Secure Computing, 2014, 11(1): 30-44.

[16] WANG L, ZHANG M, JAJODIA S, et al. Modeling network diversity for evaluating the robustness of networks against zero-day attacks[C]// European Symposium on Research in Computer Security. Springer International Publishing, 2014: 494-511.

[17] ZHANG M, WANG L, JAJODIA S, et al. Network diversity: a security metric for evaluating the resilience of networks against zero-day attacks[J]. IEEE Transactions on Information Forensics & Security, 2016, 11(5): 1071-1086.

[18] FADLALLAH A, SBEITY H, MALLI M, et al. Application of attack graphs in intrusion detection systems: an implementation [J]. International Journal of Computer Networks, 2016, 8(1): 1-12.

[19] AHMADINEJAD S H, JALILI S, ABADI M. A hybrid model for correlating alerts of known and unknown attack scenarios and updating attack graphs [J]. Computer Networks, 2011, 55(9): 2221-2240.

[20] LIU W X, ZHENG K F, WU B, et al. Alert processing based on attack graph and multi-source analyzing[J]. Journal on Communications, 2015, 36(9): 135-144.

[21] WU Y B, YANG F, LAI G H, et al. Research progress of knowledge graph learning and reasoning[J]. Journal of Chinese Mini-Micro Computer Systems, 2016, 37(9): 2007-2013. (in Chinese)
吴运兵，杨帆，赖国华，等. 知识图谱学习和推理研究进展[J]. 小型微型计算机系统，2016，37(9)：2007-2013.

[22] LI H, WANG Y, CAO Y. Searching forward complete attack graph generation algorithm based on hypergraph partitioning

1) http://ics.cnvd.org.cn

2) http://mi.cnvd.org.cn

[J]. Procedia Computer Science，2017，107(5)：27-38.

[23] PIETERS W，DAVARYNEJAD M. Calculating adversarial risk from attack trees：Control strength and probabilistic attackers [M]// Data Privacy Management，Autonomous Spontaneous Security，and Security Assurance. Springer International Publishing，2015：201-215.

[24] ZHANG S J，LI J H，SONG S S，et al. Using Bayesian inference for computing attack graph node beliefs[J]. Journal of Software，2010，21(9)：2376-2386.

[25] FRIGAULT M，WANG L. Measuring network security using Bayesian network-based attack graphs[C]// The 3rd IEEE International Workshop on Security，Trust，and Privacy for Software Applications. IEEE，2008：698-703.

[26] POOLSAPPASIT N，DEWRI R，RAY I. Dynamic security risk management using bayesian attack graphs[J]. IEEE Transactions on Dependable & Secure Computing，2011，9(1)：61-74.

[27] FANG Y，YIN X C，LI J Z. Research of quantitative network security assessment based on Bayesian-attack graphs[J]. Application Research of Computers，2013，30(9)：2763-2766.

[28] MIEHLING E，RASOULI M，TENEKETZIS D. Optimal defense policies for partially observable spreading processes on Bayesian attack graphs[C]// The Second ACM Workshop on Moving Target Defense. ACM，2015：67-76.

[29] DURKOTA K，LISY V，BOSANSKY B，et al. Optimal network security hardening using attack graph games[C]// Twenty-Fourth International Joint Conference on Artificial Intelligence. 2015：7-14.

[30] ABRAHAM S，NAIR S. Predictive cyber security analytics framework：a non-homogenous markov model for security quantification[J]. Journal of Communications，2014，12(9)：899-907.

[31] JIA Y，QI Y，SHANG H，et al. A practical approach to constructing a knowledge graph for cybersecurity[J]. Engineering，2018，4(1)：53-60.

[32] LIANG Z，ZHOU J K，ZHU H，et al. Research on Aggregation Technology for Information Security Knowledge Based on Security Ontology[J]. Netinfo Security，2017，196(4)：78-85. (in Chinese)

梁中，周嘉坤，朱汉，等. 基于安全本体的信息安全知识聚合技术研究[J]. 信息网络安全，2017，196(4)：78-85.

[33] IANNACONE M，BOHN S，NAKAMURA G，et al. Developing an ontology for cyber security knowledge graphs[C]// Cyber and Information Security Research Conference. ACM，2015：12.

[34] ASAMOAH C，TAO L，GAI K，et al. Powering filtration process of cyber security ecosystem using knowledge graph[C]// IEEE International Conference on Cyber Security and Cloud Computing. IEEE，2016：240-246.

[35] NADEAU D，SEKINE S. A survey of named entity recognition and classification[J]. Lingvisticae Investigations，2007，30(1)：3-26.

[36] LAO N，MITCHELL T，COHEN W W. Random walk inference and learning in a large scale knowledge base[C]// Conference on Empirical Methods in Natural Language Processing. 2012：529-539.

[37] BENGIO Y，DUCHARME R，VINCENT P，et al. A neural probabilistic language model[J]. Journal of Machine Learning Research，2003，3(2)：1137-1155.

[38] MNIH A，HINTON G. Three new graphical models for statistical language modelling[C]// Proceedings of the24th International Conference on Machine Learning. ACM，2007：641-648.

[39] YE Z W，GUO Y B，WANG C D，et al. Survey on application of attack graph technology[J]. Journal on Communications，2017，38(11)：125-136. (in Chinese)

叶子维，郭渊博，王宸东，等. 攻击图技术应用研究综述[J]. 通信学报，2017，38(11)：125-136.

[40] CHEN X，FANG B，TAN Q. Inferring attack intent of malicious insider based on probabilistic attack graph model[J]. Chinese Journal of Computers，2014，37(1)：62-72.

[41] TANJA B，MARCOS K，HEIKO S，et al. Using natural language processing to enable in-depth analysis of clinical messages posted to an internet mailing sist：a feasibility study[J]. Journal of Medical Internet Research，2011，13(4)：e98.

[42] FINKEL J R，GRENAGER T，MANNING C. Incorporating non-local information into information extraction systems by Gibbs sampling[C]// Proceedings of the 43rd Annual Meeting of the Association for Computational Linguistics. Association for Computational Linguistics，2005：363-370.