基于本体的网络入侵知识库模型研究

吴林锦 武东英 刘胜利 刘 龙
(解放军信息工程大学数学工程与先进计算国家重点实验室 郑州 450002)

摘 要 在信息安全领域,网络入侵知识库对有效分析和防御网络非法入侵起着重要作用,然而网络入侵知识库的构建是研究的难点之一。本体作为一种能为特定领域提供知识共享的概念模型建模工具,已经在各领域得到广泛应用。针对当前还没有一个完善的网络入侵知识本体,研究基于本体的网络入侵知识库模型,构建了网络入侵知识本体。首先,在深入分析网络入侵技术的基础上,形式化定义了各类网络入侵行为,给出了多层次、多维度的网络入侵知识库分类体系。接着,结合本体建模原则,构建了由网络入侵知识领域本体、任务本体、应用本体和原子本体组成的网络入侵知识本体,并给出它们之间的逻辑关系和组织结构。最后,通过两个网络场景,验证了模型用于获取网络入侵知识的有效性。

关键词 本体,知识库,网络入侵,网络场景,形式化
中图法分类号 TP393.08 **文献标识码** A

Research on Network Intrusion Knowledge Base Model Based on Ontology

WU Lin-jin WU Dong-ying LIU Sheng-li LIU Long
(State Key Laboratory of Mathematical Engineering and Advanced Computing, PLA Information Engineering University, Zhengzhou 450002, China)

Abstract In the field of information security, network intrusion knowledge base plays an important role in effective analysis and defense of the illegal invasion, but network intrusion knowledge base construction is one of the difficulties of research. As a conceptual modeling tool to provide knowledge sharing for a specific area, ontology has been widely used in various fields. Because there is no complete network intrusion ontology, the paper aimed to study the ontology-based network intrusion knowledge base model and build network intrusion knowledge ontology. Firstly, on the basis of in-depth analysis of network intrusion technology, the paper gave formalized definition of various types of network actions and the multi-level and multi-dimensional network intrusion knowledge base classification system. Then combining with the principles of ontology modeling, the paper built the network intrusion knowledge ontology composed of the network intrusion knowledge domain ontology, task ontology, application ontology and atomic ontology, giving the logical relationship and organizational structure between them. Finally, through two network scenarios the paper verified the validity of the model in the application of network intrusion knowledge acquisition.

Keywords Ontology, Knowledge base, Network intrusion, Network scenario, Formalization

1 引言

随着计算机技术的发展,网络非法入侵已经对信息安全构成巨大的威胁,有效地感知和防御网络入侵已迫在眉睫。知识库是知识工程中结构化、易利用、好操作和全面有组织的知识集,是针对某领域问题求解的需求,采用相应的知识表示方法,能进行组织、存储、管理、使用和共享的知识集合。构建完善的网络入侵知识库,有助于知识的交流和共享,有利于安全人员更好地分析网络入侵行为,将对网络防护发挥重要的作用。然而,知识获取本身就是知识工程中最重要和最艰巨的任务,知识库模型的科学建立是构建过程的关键所在。因此,本文旨在研究如何有效构建网络入侵知识库模型,为网络入侵知识库构建提供指导和方法。

本体论(Ontology)是一门新兴学科,当前已经成为知识工程、自然语言处理、信息协同系统、智能信息集成和知识管理等领域的研究热点[1]。本体提供一套对特定领域知识共享的共同认识,在特定领域内,本体对概念进行了严格的定义,消除了二义性,确保了唯一性,很好地实现了知识的共同认识和相互共享,并实现了不同主体的相互交流。当前,国内外在许多领域都出现了本体,国外研究的本体有:为机器翻译提供概念结构的 SENSUS[2],一体化医学语言系统的 UMLS[3],致力于表示人类常识的 CYC[4],解决电子资源标准问题的 Dulbin Core 本体[5],以及基于认知语言学的英语词典 Wordnet 本体[6]等;国内研究的本体有:陆汝钤院士等研制的常识知识系统[7],由中科院曹存根带领的对各学科知识进行深层次概念和知识分析的 NKI[8],北京大学金芝教授研究的基于

到稿日期:2012-11-10 返修日期:2013-03-11 本文受郑州市科技创新团队项目(10CXTD150)资助。
吴林锦(1989—),男,硕士生,主要研究方向为信息安全,E-mail:wulinjin01@163.com;武东英(1965—),女,副教授,主要研究方向为信息安全;刘胜利(1973—),男,副教授,主要研究方向为信息安全;刘 龙(1983—),男,讲师,主要研究方向为信息安全。

本体的软件需求获取方法[9]，以及电子科大钟秀琴构建的几何学本体等[10]。总之，本体逐渐在各领域内得到了广泛的发展和应用，已经成为一种常用的知识表示工具。

目前还没有一个完善的网络入侵知识本体，因此，建立一个良好的网络入侵知识本体具有重要的意义。文献[11]利用本体构造了网络攻击本体，定义了概念之间的逻辑关系和层次结构，建立了网络攻击本体模型，其提供了一种很好的思路，但是网络攻击只是网络入侵知识中的一部分，其不可能考虑与其他网络入侵知识的关系，需要更宏观、更全面地构建网络入侵知识库模型。因此，本文在分析本体建模一般方法的基础上，结合本体在其他领域的应用，对网络入侵知识本体进行研究，构建了基于本体的网络入侵知识库模型。为了系统化构建网络入侵知识库，本文首先对网络入侵知识库进行梳理和分类，接着结合本体建模原则和方法，建立了基于本体的知识库模型，最后结合两个网络场景，实例分析了应用本体模型进行知识获取的过程。

2 网络入侵知识库的分类

本文研究的网络入侵知识库主要是指，从攻击者的角度进行一次网络入侵行动所包含的知识集合。根据网络入侵任务的不同，网络入侵知识库总体上可分为：网络侦察知识库、网络攻击知识库和网络隐蔽知识库，它们的关系如图 1 所示。

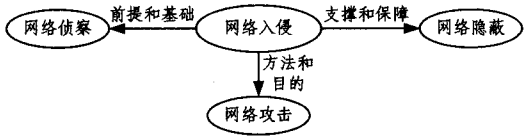

图 1 网络侦察、网络攻击和网络隐蔽的关系

其中网络侦察是网络入侵的前提和基础，网络攻击是网络入侵的方法和目的，网络隐蔽是网络入侵的支撑和保障。网络侦察、网络攻击和网络隐蔽不断地贯穿于网络入侵之中，相互作用，相互影响，相互配合。网络入侵知识库的构建有助于深入分析一次网络入侵行动，为网络安全防护提供指导和依据。

2.1 网络侦察

网络侦察的目的是收集和判断目标网络系统的结构、软硬件配置、网络服务及应用的状况，发现目标网络系统的薄弱节点，掌握目标系统类型、服务种类、系统漏洞、安全隐患、用户口令及其它特征参数。常见的侦察方法有主动探测，如端口扫描、服务扫描和漏洞扫描等以及被动窃听如网络嗅探等。为了准确描述一次网络侦察行动，本文采用了“前提-结果”的描述方式，其最早由 Peng Ning 在关于入侵检测的文章中提出[12]，前提集合表示行动进行所应具备的条件，结果集合表示行动进行后产生的结果。这种描述方式应用于网络行动的描述的优势在于：它能够动态地、具有层次性地刻画网络入侵；结果集合会落在前提集合里面，有助于循环描述网络入侵。网络侦察可以形式化定义为：

定义 1 $REC::=\{P_{rec},S_{rec},T_{rec},R_{rec}\}$

其中，P_{rec} 表示侦察前提集合，S_{rec} 表示侦察过程集合，T_{rec} 表示侦察后果集合，R_{rec} 表示行动的顺序，一般地，$R_{rec}:P_{rec}\rightarrow S_{rec}\rightarrow T_{rec}$。

通过分析常见的网络侦察，结合其形式化表示，对网络侦察进行细化，如图 2 所示。

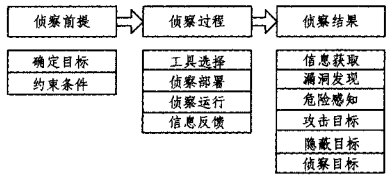

图 2 网络侦察分类

如图 2 所示，一次网络侦察行为主要包括侦察前提、侦察过程和侦察结果。其中侦察前提要选择合适目标，确定侦察的范围，并且要符合进行侦察时的约束条件；侦察过程中先要根据目标选择相应工具，然后考虑部署策略，接着侦察运行，并反馈收集到的信息反馈；侦察结果包括信息获取、漏洞发现、危险感知以及确定下一步的行动，即是进一步侦察，还是攻击或隐蔽。

2.2 网络攻击

网络攻击是在网络侦察的基础上，综合使用各种攻击武器，欺骗、干扰、破坏、摧毁攻击目标。常见的攻击方法有口令攻击、恶意代码注入攻击、拒绝服务攻击和欺骗攻击等。类似地，网络攻击可以形式化定义为：

定义 2 $ATT::=\{P_{att},S_{att},T_{att},R_{att}\}$

其中，P_{att} 代表攻击前提集合，S_{att} 代表攻击过程集合，T_{att} 代表攻击结果集合，$R_{att}:P_{att}\rightarrow S_{att}\rightarrow T_{att}$。

通过分析典型的网络攻击，结合其形式化表示，对网络攻击进行细化，如图 3 所示。

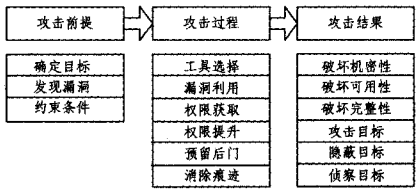

图 3 网络攻击分类

如图 3 所示，一次网络攻击行为主要包括攻击前提、攻击过程和攻击结果 3 个部分。其中攻击前提是发现漏洞，并确定攻击目标，而且要符合进行攻击时的约束条件；攻击过程包括工具选择，进行漏洞利用，不断提升权限，获取控制权，然后就是善后工作，即预留后门和消除痕迹等；攻击结果必然会破坏目标的机密性、可用性和完整性，并选择下一步的网络行动。

2.3 网络隐蔽

网络隐蔽是指在一次网络行动过程中为加强自身的安全性、隐蔽性和生存性而采取的隐蔽措施。主要的网络隐蔽可分为主体隐蔽和通信隐蔽，如：杀毒软件突破、安全机制突破和可信认证突破等属于主体隐蔽；突破流量检测和模拟正常通信等属于通信隐蔽。类似地，网络隐蔽可以形式化定义为：

定义 3 $PRO::=\{P_{pro},S_{pro},T_{pro},R_{pro}\}$

其中，P_{pro} 代表隐蔽前提集合，S_{pro} 代表隐蔽过程集合，T_{pro} 代表隐蔽结果集合，$R_{pro}:P_{pro}\rightarrow S_{pro}\rightarrow T_{pro}$。

通过分析典型的网络隐蔽，结合其形式化表示，对网络隐蔽进行细化，如图 4 所示。

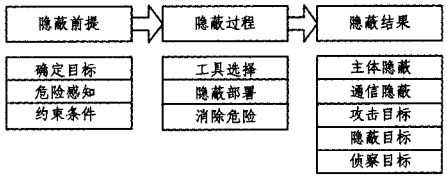

图 4 网络隐蔽分类

如图 4 所示，一次网络隐蔽行为包括隐蔽前提、隐蔽过程和隐蔽结果 3 个部分。其中隐蔽前提是根据危险感知确定隐蔽的目标，并且要符合进行隐蔽的约束条件；隐蔽过程包括隐蔽工具选择，隐蔽策略部署，进而进行隐蔽，达到消除危险的目的；隐蔽结果包括主体隐蔽、通信隐蔽，以及下一步网络行动。

综上所述，网络侦察、网络攻击和网络隐蔽分类构成了整个网络入侵知识库的分类体系。该分类体系具有以下特点：

(1)从多概念、多层次和多维度对网络入侵知识进行分类，通过该分类中各子项的有机组合，可以描述各种网络入侵行为，该分类具有较好的完备性。

(2)从攻击者的角度分析常见网络行为、层层细化的分类体系，使该分类具有现实可用性。

(3)当出现新的网络行动时，对分类标准进行升级，只需增加新的节点，而不影响整个网络入侵知识库分类体系，具有良好的可扩展性。

(4)在网络入侵行动中，侦察、攻击和隐蔽会相互影响、相互配合，采用“前提-结果”的描述方式有助于动态地刻画复杂的网络入侵行为。因此，该分类能过程性表达侦察、攻击和隐蔽三者间的相互配合，具有良好的可操作性。

3 基于本体的网络入侵知识库模型

3.1 本体

3.1.1 本体的定义

本体原本是一个哲学的概念，在哲学范畴上，本体是客观存在的一个系统解释或说明，关心的是客观现实的抽象本质[13]。随着人工智能的不断发展，本体逐渐被应用于知识工程中，成为一种知识表示常用的方法。大家对本体的理解也不断地深入，目前被多数人认同的定义是 Studer 等人提出的“本体是指对共享概念模型的明确的形式化规范说明”，它包含 4 层含义[14]，如表 1 所列。

表 1 本体的 4 层含义

含义	描述
概念模型	从现实世界进行抽象从而得到由概念建立的模型
明确	概念和概念的范畴都有明确的定义，消除二义性
形式化	能被计算机处理，具有发展的生命力
共享	概念集是公认的、能被共同认识的，从而达到共享

本体的目标是获取某领域的知识，确定该领域内共同认识的概念，并给出概念以及概念之间关系的明确定义，最终使领域内的知识得到共享。

3.1.2 本体的建模元语

根据研究[15]，Perez 等人认为本体可以按分类法来组织，归纳出了 5 个基本的建模元语：概念、关系、函数、公理和实例。概念也称类，它是主体和事件的模型知识，能够反映事物的一般本质特征；关系代表概念之间的相互作用；函数是一种特殊的关系，它将某些概念集合映射到某一概念；公理是公认的事实或永真断言，用于知识推理；实例代表概念类中的元素。其中概念之间有 4 种最基本的关系：整体与局部关系(part-of)、继承关系(kind-of)、属性关系(attribute-of)和实例关系(instance-of)。在概念和实例的基础上，通过关系、函数和公理的演绎和作用，就能够较好地对特定领域进行本体建模，进而产生结构清晰、定义明确和具有可扩展性的知识本体。

3.2 网络入侵知识本体的构建

本体的构建是对特定领域概念按照本体建模原则进行分层刻画的过程。本体的构建首先要确定本体覆盖的范围，明确建立本体的用途，接着抽象出所关注领域的关键概念，并明确定义概念以及概念之间的关系和层次结构。前面已对网络入侵知识库进行了分类别、多层次和多维度的刻画，给出了分类体系，这为本体的构建奠定了基础。网络入侵知识本体的构建流程如图 5 所示。

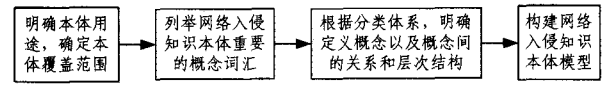

图 5 网络入侵知识本体构建流程图

在构建网络入侵知识本体的过程中，要明确定义的关系包括概念之间的关系、实例之间的关系、概念与实例之间的关系以及不同层次之间的结构关系。在网络入侵知识本体构建过程中，按照前面给出的网络入侵知识库分类体系，逐级进行分层次抽象，可以将其分为网络入侵知识领域本体、任务本体、应用本体和原子本体。其中网络入侵知识领域本体按照网络行动的不同进行高层次划分；网络入侵知识任务本体在“前提-结果”的描述方式上，根据不同网络任务的不同阶段进行分类；网络入侵知识应用本体根据不同阶段中所要采取的不同应用对任务本体进行进一步细化；网络入侵知识原子本体结合不同应用，声明可以直接应用的实体元素，是本体的最下层。

3.3 网络入侵知识本体模型

3.3.1 网络入侵知识领域本体

网络入侵知识领域本体是领域最上层本体，其包含网络入侵知识领域的概念类以及概念类与领域之间的关系。网络入侵知识的领域本体如图 6 所示，其中矩形框代表概念类，箭头代表整体与部分的关系。

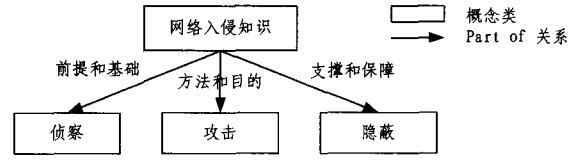

图 6 网络入侵知识的领域本体

网络入侵领域本体描述了不同网络入侵行动的概念和关系集，包括网络侦察、网络攻击和网络隐蔽。类概念之间包括 3 种关系：侦察是网络入侵的前提和基础，攻击是网络入侵的方法和目的，隐蔽是网络入侵的支撑和保障。

3.3.2 网络入侵知识任务本体

网络入侵知识任务本体是对领域本体的进一步描述，在“前提-结果”的描述方式下，以不同任务为划分，给出不同任务各阶段子领域概念以及概念之间关系的本体。按照不同任务阶段，侦察子领域可以分为：侦察前提、侦察过程和侦察结果，其中侦察子领域与它们是继承关系(kind-of)，前提、过程和结果是网络行动的不同阶段，它们之间是时间上的先后关系；攻击和隐蔽子领域也类似。

3.3.3 网络入侵知识应用本体

网络入侵知识应用本体是在任务本体上的进一步描述，根据网络入侵知识分类体系，以侦察为例，各侦察的应用本体描述如下：

侦察前提应用本体包括确定目标和约束条件；侦察过程

应用本体包括工具选择、侦察部署、侦察运行和信息反馈；侦察结果应用本体包括信息获取、漏洞发现、危险感知、攻击目标、隐蔽目标和侦察目标。

侦察子领域应用本体如图 7 所示，其中任务本体和应用本体是整体与部分的关系。

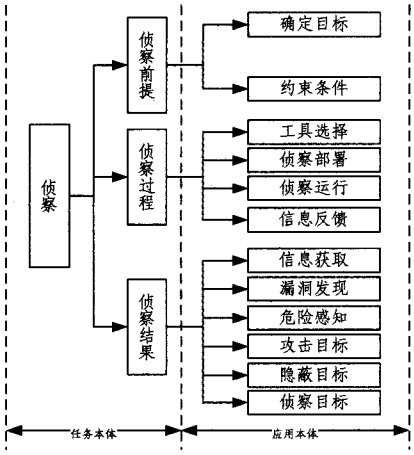

图 7　侦察子领域应用本体

类似地，结合网络入侵知识分类体系，可以构造出攻击和隐蔽子领域的应用本体，分别如图 8 和图 9 所示。

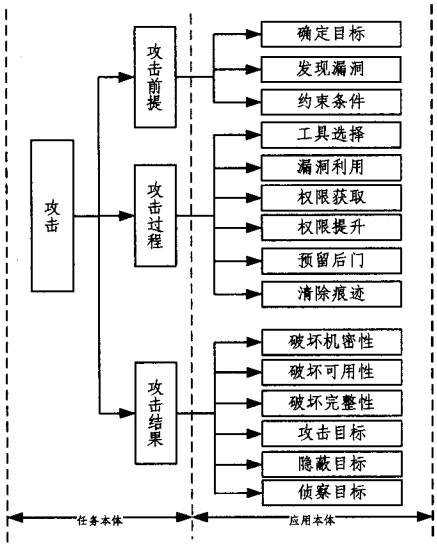

图 8　攻击子领域应用本体

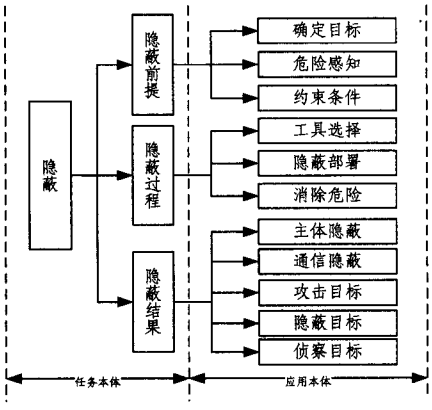

图 9　隐蔽子领域应用本体

3.3.4　网络入侵知识原子本体

网络入侵知识原子本体是可直接应用实体概念的声明，原子本体中实例与应用本体中概念的关系是实例关系(instance-of)，原子本体是最下层本体，它是网络入侵知识概念类元素，是不可再分的实例。网络入侵知识中，实例只需要根据本身的任务类型以及任务完成的不同阶段，映射到相应的网络入侵知识应用本体，就可以找到其对应的概念类。例如，侦察过程工具选择的原子本体如图 10 所示。

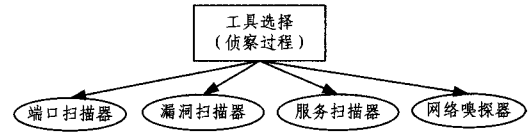

图 10　侦察工具选择原子本体

如图 10 所示，椭圆框代表实例，实例与上层应用本体是实例关系(instance-of)，工具选择的原子本体包括：端口扫描器、漏洞扫描器、服务扫描器和网络嗅探器。由于篇幅原因，就不一一列举出网络入侵知识的各原子本体。

综上所述，由网络入侵知识领域本体、任务本体、应用本体和原子本体构成的网络入侵知识本体模型，实现了网络入侵知识领域概念分层次、多维度地刻画，体现了网络入侵知识由细化到抽象的升华过程，它能够从较高层次、易于理解地实现对网络入侵知识的认识和分析，起到了较好的知识共享和互用。其中，网络入侵知识各本体之间的组织结构如图 11 所示。

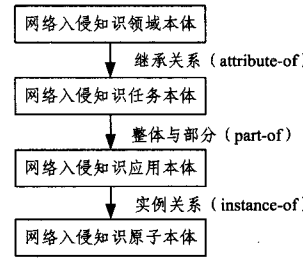

图 11　网络入侵知识本体的组织结构

通过 4 层的网络入侵知识本体结构，能够清晰地从不同的层次，不断深入、层层抽象地分析一次网络入侵行动，体现了知识获取的一般过程，能够为网络入侵知识库构建提供指导和方法。

4　网络场景

在实际网络环境中，网络入侵是非常复杂的过程，它以网络入侵目标为牵引，通过一系列复杂的实施过程，经过网络侦察、网络攻击和网络隐蔽相互交替、相互配合，最终完成入侵任务。网络入侵是分步骤、分阶段进行的，前一阶段的结果作为下一阶段的行动依据，层层推进，不断深入，直到达到目标。按照每一阶段网络入侵的目的，可以将网络入侵过程分为若干个网络入侵序列，隶属于同一网络入侵过程的行动序列称为网络场景。根据网络侦察、攻击和隐蔽的形式化定义，网络场景定义如下：

定义 4　$NETSEC::=\{REC, ATT, PRO, SEQUENCE\}$

其中，$NETSEC$ 表示网络场景集合，REC、ATT 和 PRO 如上定义，$SEQUENCE$ 表示行动顺序的集连，$SEQUENCE$：$R_{rec} \times R_{att} \times R_{pro}$。

网络场景是由若干网络侦察、攻击和隐蔽行动，根据网络入侵目的，按照一定行动顺序结合而成的，其能有效地刻画网

络入侵，因此，网络场景是网络入侵知识库的核心和主要组成部分。网络场景对应着多个不同的网络入侵行动序列，每个网络入侵行动序列都对应着行动目的，把这个行动目的称为网络意图。网络场景可以看成一系列网络意图的组合，一次网络意图对应着多个网络原子操作，因此，网络场景和网络意图能够较好地应用网络入侵知识本体模型去获取网络入侵知识。一次具体的网络意图可以看成一系列网络入侵知识原子本体节点的有序组合，按照网络入侵知识本体的 4 层结构，网络场景和网络意图也呈观出层次性，使得我们能更为深刻地认识网络入侵行动，具体而又抽象地把握行动的本质。当然，这也是知识获取的一般过程，从具体到抽象，认识不断上升、凝聚总结的过程，网络场景和网络意图就像桥梁使得网络入侵知识本体模型能够用于获取网络入侵知识。

5 实例分析

下面通过实例，分析如何运用网络场景和网络意图，结合网络入侵知识本体模型获取网络入侵知识。从攻击者的角度，假定对目标实施两类行动：漏洞利用攻击和系统控制。漏洞利用攻击是进行网络攻击过程中最直接的突破方法，效果明显，威胁程度巨大；系统控制是指攻击者在入侵目标后，为了达到持续稳定控制而采取的措施，如：自身隐蔽、口令破解和消除痕迹等。下面构建这两类行动的网络场景，给出其网络意图，结合网络入侵知识本体模型，分析网络入侵知识的获取过程。

5.1 网络场景 1：漏洞利用攻击

局域网中攻击者首先探测网络上有哪些存活主机，然后探测存活主机的 MS08-067 漏洞，对存在这些漏洞的主机采用构造特定的 RPC（Remote Procedure Call）造成缓冲区溢出[16]，进行远程代码执行，最终达到该主机的远程控制。该网络场景可用多个网络意图来描述，如图 12 所示，每一个方框代表一种网络意图。

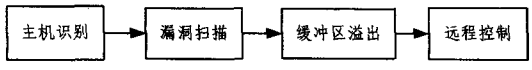

图 12 漏洞利用攻击的网络场景

结合网络入侵知识本体模型，分析该网络场景的知识获取过程。在网络入侵知识领域本体层次，该网络场景进行了侦察→侦察→攻击的过程；在任务本体层次，每个侦察和攻击的行动又经过了从前提→过程→结果的过程；在应用本体层次，根据网络意图的不同，也可以进行相应的分解；最后从原子本体层次构建网络入侵知识的实体，于是可以得出该场景的知识获取，如图 13 所示，其中，网络入侵知识原子本体的实例是可以根据需要添加的。

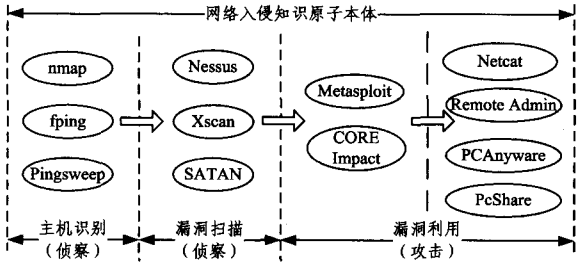

图 13 漏洞利用攻击场景的知识获取

5.2 网络场景 2：系统控制

为了达到对已经入侵目标的持续控制，需要采取一系列的网络行动：信息收集、隐蔽实现和口令破解等。假定在初始控制的远程主机上，首先进行系统信息探测，感知目标的安全状况，目标主机 UAC 机制开启后对 UAC 机制进行突破，接着进行该主机的口令破解。该网络场景的网络意图如图 14 所示。

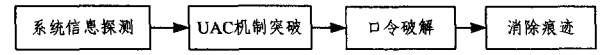

图 14 系统控制的网络场景

结合网络入侵知识本体模型，对该网络场景的知识获取过程进行分析。在网络入侵知识领域本体层次，该场景进行了侦察→隐蔽→攻击的过程；在任务本体层次，每类网络行动经过了前提→过程→结果的过程；在应用本体层次，根据网络意图的不同，进行应用细化；最后从原子本体层次构建网络入侵知识的实体，于是可以得出该场景的知识获取，如图 15 所示，同样原子本体的实例是可以添加的。

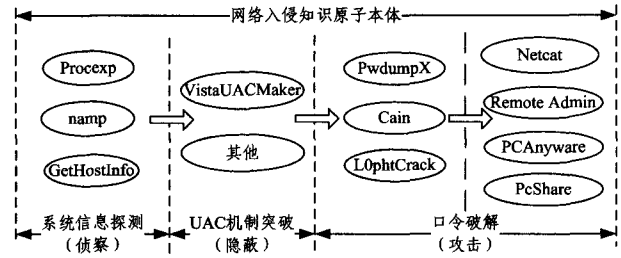

图 15 系统控制场景的知识获取

结束语 如何有效地构建网络入侵知识库是研究的难点之一。本文首先从攻击者角度，深入分析了常见的网络入侵行动，引入了“前提-结果”的描述方式，形式化定义了网络侦察、攻击和隐蔽行动，并提出了多维度多层次的网络入侵知识库分类体系。接着本文有机结合该分类体系和本体理论，依据本体建模原则，提出了由网络入侵知识领域本体、任务本体、应用本体和原子本体组成的网络入侵知识本体，构建了基于本体的网络入侵知识库模型。为了有效应用模型去获取网络入侵知识，引入网络场景和网络意图的概念，并形式化定义了网络场景。最终应用两个网络场景，给出了运用模型获取网络入侵知识的过程，验证了模型的有效性。

参 考 文 献

[1] Towards G T. Principles for the Design of Ontologies Used for Knowledge Sharing[J]. International Journal of Human-Computer Studies, 1995, 43(5/6): 907-928

[2] Knight K, et al. Filling knowledge gaps in a broad-coverage Machine Translation system[C]// Proceedings of the 14th International Joint Conference on Artificial Intelligence, IJCAI95. Montréal, Québec, Canada, Morgan Kaufmann, 1995(2): 1390-1396

[3] Bodenreider O. The unified medical language system(UMLS): integrating biomedical terminology[J]. Nucletic Acids Research, 2004, 32(Database issue D): 267-270

[4] Lenat D B, Guha R V. Building Large Knowledge-Based Systems: Representation and Inference in the Cyc Project[D]. Reading MA: Addison-Wesley Publishing Company, Inc., 1989

[5] Weibel S. The Dublin Core: A Simple Content Description Model for Electronic Resources[J]. Bulletin of the American Society for Information Science and Technology, 1997, 24(1): 9-11

（下转第 129 页）

含内核信息安全管理模块和应用层信息安全保护模块时，其对不可识别入侵处理的效果很好，最高可达 98.2%。

(3)实时性保障实验

该实验使用实验(1)中的攻击源，且各种攻击出现频率相同，主要针对两方面进行测试：可识别入侵处理和不可识别入侵处理。对于不可识别入侵来说，“Threshold”值大小对系统实时性的影响为实验目标。图 10 为系统实时性在不同信息安全处理条件下的情况。

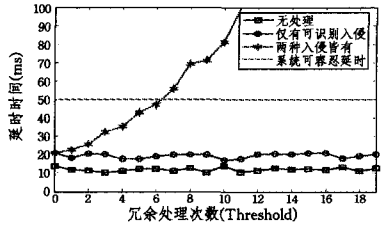

图 10 不同信息安全处理下的系统实时性

由实时性保障验证实验结果可以看出，当系统仅有可识别入侵处理时，其实时性仍可满足需求；而当有不可识别入侵处理且冗余处理次数的阈值设定超过 6 时，系统实时性已经不能满足需求了。故保障系统信息安全的前提应是准确设置软冗余处理的次数阈值。

结束语 为改善工业自动化系统中 EPLC 出现的信息安全问题，本文提出了两级信息安全恢复控制策略，并在基于 CortexA8-Linux 的 EPLC 平台上进行了入侵检测和处理效果验证，通过两级安全防护，其在满足系统实时性要求的同时很好地保证了系统的信息安全。不可识别入侵处理依赖于软冗余处理阈值“Threshold”，构建合理的方法来优化阈值的选择将会进一步提高系统的入侵处理能力，使得系统安全性能进一步提高。

参 考 文 献

[1] 王晓光. 嵌入式 PLC 的设计与研究[D]. 成都：西华大学，2011

[2] 贺无名，余强国. 基于嵌入式软 PLC 的矿井提升机控制系统设计[J]. 煤矿机械，2011，32(6)：244-246

[3] 孟庆春，刘云卿. 应用于 PLC 控制程序的 Petri 网执行模型[J]. 计算机科学，2009，36(10)：150-159

[4] Koopman P. Embedded system security[J]. IEEE Computer，2004，37(07)

[5] 张帅. ICS 工业控制系统安全风险分析[J]. 信息安全与通信保密，2012(3)：15-19

[6] 杨智君，田地，马骏骁，等. 入侵检测技术研究综述[J]. 计算机工程与设计，2006，27(12)：2119-2123，2139

[7] 方来华. 工业控制系统的信息安全[J]. 电气时代，2008(10)：118-121

[8] Stouffer K，Falco J，Scarfone K. Guide to Industrial Control Systems Security[R]. UK：National Institute of Standards and Technology，2011

[9] 唐文. 工业自动化控制系统信息安全研究[J]. 计算机安全，2012(4)：2-7

[10] 田海，崔桂梅，王晓红，等. 西门子 PLC 控制网络的配置策略与应用[J]. 电气传动，2010(01)：76-80

[11] 陈慕宁. 工业自动化控制系统的设计[J]. 电脑编程技巧与维护，2008(16)：27，62

[12] 刘阳. 基于免疫原理的无线传感器网络入侵检测系统研究[D]. 北京：中国科学院研究生院(计算技术研究所)，2008

[13] 刘俊年. 基于 linux 系统的安全策略研究及其实现[D]. 成都：四川大学，2008

[14] 赵中敏. 冗余设计在 PLC 控制系统中的应用[J]. 机床电器，2007(3)：42-45

[15] 白琳. 基于免疫优势克隆网络聚类的入侵检测[J]. 计算机科学，2012，39(07)：82-86，118

[16] Hettich S，Bay S. The UCI KDD Archive[OL]. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. Irvine，CA：University of California，Department of Information and Computer Science，1999

[17] 翟光群，陈向东，胡贵江. 蜜罐与入侵检测技术联动系统的研究与设计[J]. 计算机工程与设计，2009，30(21)：4845-4847，4867

(上接第 124 页)

[6] Miller G A. WordNet：a lexical database for English[J]. Communications of the ACM，1995，38(11)：39-41

[7] 陆汝钤，石纯一，张松懋，等. 面向 Agent 的常识知识库[J]. 中国科学 E 辑，2000，30(5)：453-463

[8] 曹存根，丰强泽，高颖，等. Progress in the Development of National Knowledge Infrastructure[J]. 计算机科学技术学报：英文版，2002，17(5)：523-534

[9] 金芝. 基于本体的需求自动获取[J]. 计算机学报，2000，23(5)：486-492

[10] 钟秀琴，符红光，余莉，等. 基于本体的几何学知识获取及知识表示[J]. 计算机学报，2010，1(33)：167-174

[11] 王前，冯亚军，杨兆民，等. 基于本体的网络攻击模型及其应用[J]. 计算机科学，2010，37(6)：114-117

[12] Peng Ning，Yun Cui，Douglas S. Constructing Attack Scenarios through Correlation of Intrusion Alerts[C]// The 19th ACM Conference on Computer and Communications Security，ACM CCS 2002. Washington：North Carolina State University，2002：245-254

[13] 邓志鸿，唐世渭，张铭，等. Ontology 研究综述[J]. 北京大学学报：自然科学版，2002，38(5)：730-738

[14] Studer R，Benjamins V R，Fensel D. Knowledge Engineering，Principles and Methods[J]. Data and Knowledge Engineering，1998，25(1/2)：161-197

[15] Perez A G，Benjamins V R. Overview of Knowledge Sharing and Reuse Components：Ontologies and Problem-Solving Methods[C]//Proceedings of the IJCAI-99 workshop on Ontologies and Problem-Solving Methods(KRR5). 1999：1-15

[16] 诸葛建伟. 网络攻防技术与实践[M]. 北京：电子工业出版社，2011