基于本体的网络攻击案例库模型研究

李文雄 武东英 刘胜利 肖 达
(数学工程与先进计算国家重点实验室 郑州 450001)

摘 要 在网络安全研究中,网络攻击案例对有效分析和防御网络非法入侵起着重要作用。然而,如何有效地构建网络攻击案例库是研究的难点之一。鉴于目前还没有一个完善的网络攻击案例库,基于本体研究了网络攻击案例库模型。首先定义了网络攻击行为的案例形式化表示,对网络攻击案例领域知识进行了分类,在此基础上,应用知识共享工具本体,构建了一个共享、重用、可扩展的网络攻击案例本体模型。最后,应用构建的基于本体的网络攻击案例库模型,对一次网络攻击事件进行知识获取,以验证模型的有效性。

关键词 网络攻击,案例表示,本体,案例库模型
中图法分类号 TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.10.039

Research on Cyber Attack Case Base Model Based on Ontology

LI Wen-xiong WU Dong-ying LIU Sheng-li XIAO Da
(State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China)

Abstract In the study of network security, cyber-attack case plays an important role for effectively analyzing and defensing network illegal intrusion. However, how to effectively build cyber-attack case base is one of the difficulties. For there is no perfect cyber-attack case base, this paper studied the cyber-attack case model based on ontology. This paper first defined formalized representation of cyber-attack case, classified cyber-attack case domain knowledge, and on this basis, applying ontology, the knowledge sharing tools, built a sharing, reusable, scalable cyber-attack case model, finally, using the model of cyber-attack case put forward based on ontology, realized knowledge acquisition of a network attack events, to verify the validity of the model.

Keywords Cyber attack, Case presentation, Ontology, Case base model

1 引言

知识库是知识工程中,针对某领域问题求解的需求,采用相应的知识表示方法,进行组织、存储、管理和共享的知识集合。知识表示是知识工程的核心问题,知识库模型的科学建立是构建过程的关键所在。基于案例推理(case-based reasoning, CBR[1])是人工智能领域的重要分支,以其知识获取相对容易、适用范围广、增量学习等特点而被广泛应用。在CBR理论中,知识以案例的形式表示和存储,而不是以抽象的规则或模型的形式表示。基于案例的知识表示不仅能表示显性知识,更能较好地解决专家系统等以规则形式无法表示的专家求解问题的隐性知识和经验。知识案例表示方法在知识工程中正得到越来越广泛的应用[2,3]。

近年来,各种网络非法攻击事件频发,给网络信息安全带来了巨大的威胁。对过去网络非法攻击事件行为的分析和研究,是感知和防御未来网络非法攻击行为的重要手段。网络攻击案例库的构建,实现了对网络非法攻击事件行为的信息化管理,有助于网络安全研究人员深入了解当前网络攻击的攻击手段和基本流程,使其更有针对性地进行网络安全防护,也能够提高网络攻防知识的交流和共享。因此,本文旨在研究如何以案例的知识表示形式,有效表示网络攻击事件行为涵盖的网络攻防知识集合,进而构建网络攻击案例库模型,为网络攻击案例库的构建提供指导和方法。

本体[4]是实现知识共享的有效工具之一,是对领域内共享概念模型的形式化规范说明。在案例知识表示中引入本体理论,统一领域内知识概念和概念关系层次结构,增强案例知识表示的规范性、一致性和可扩展性,进而实现案例库的共享、重用和互操作。

目前,还没有一个完善的网络攻击案例库。文献[5,6]以攻击者的角度研究网络攻击行为,在对网络攻击知识进行分类的基础上,利用本体理论构造了网络攻击本体,建立了基于本体的网络攻击知识库模型。但在一次网络攻击事件或攻击行为过程中,网络攻击只是整个案例知识的一部分,知识表示相对离散,缺乏关联性和整体性。此外,仅从攻击者的角度去获取知识,不能充分描述网络攻防过程中的复杂的博弈过程。文献[7]针对网络舆论监控,以半自动的方法构建了网络事件案例库,但网络攻击事件或行为相较于网络舆论的传播,有着较大的差异,该构建方法不适用于网络攻击案例库的构建。因此,需要构建一个网络攻击案例库模型。本文在深入研究网络攻击理论和技术的基础上,实现对网络攻击行为的案例

到稿日期:2013-11-05 返修日期:2014-02-16 本文受郑州市科技创新团队项目(10CXTD150),国家自然科学基金项目(61309007)资助。
李文雄(1988—),男,硕士生,主要研究方向为信息安全,E-mail:wenxionglee@foxmail.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;肖 达(1981—),男,讲师,主要研究方向为信息安全。

化知识表示。结合本体在知识共享方面的应用特点，构建基于本体的网络攻击案例库模型。最终根据相应的网络攻击事件，实例分析如何应用基于本体的网络攻击案例库模型进行知识的获取和网络攻击行为案例表示。

2 网络攻击案例表示

案例表示就是把以前发生过的事件或处理过的问题，以一定的逻辑结构表示成案例的形式，并存储在案例库中。多个案例以一定的索引方式存储，构成一个案例库。因此，本文将网络攻击案例库形式化定义为：

定义 1 $AttCBASE::=\{\{C_1,C_2,C_3,\cdots\},IndexR\}$

其中，C_1，C_2 表示网络攻击案例，$IndexR$ 表示网络攻击案例库的案例索引规则。

一个网络攻击案例是对一次网络攻击事件或行为的完整表述，是对网络攻击行为的环境、状态、资源等背景信息，以及事件过程和结果的描述。因此，本文将网络攻击案例形式化定义为：

定义 2 $AttCASE::=\{CInfo,CA,CD,CApro,CDpro,CResult\}$

其中，$CInfo$ 为网络攻击案例的基本信息，包括案例存储编号、案例名称、案例时间等背景信息；CA 为网络攻击案例的发起者；CD 为网络攻击案例的防御方；$CApro$ 为网络攻击案例的攻击过程；$CDpro$ 为网络攻击案例的防御过程；$CResult$ 为网络攻击案例的案例结果。

上述定义的网络攻击案例结构中，攻击过程和防御过程分别描述了在整个网络攻击案例过程中，攻击者采用的攻击策略和相关技术，以及遭受网络攻击的防御者采用的防御策略和相关技术。案例结果则描述了该网络攻击过程中，主体和客体攻防博弈的结果。网络攻击案例组成结构关系如图 1 所示。

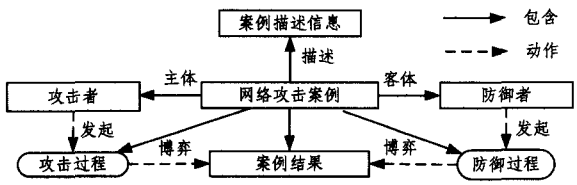

图 1 网络攻击案例描述结构

以上网络攻击案例的描述，指出了网络攻击案例的多个要素，我们可以从这些要素出发，对网络攻击案例知识进行分类，以案例主体（攻击者、防御者）、攻击过程、防御过程、案例结果 4 个要素作为案例知识分类的依据，构造网络攻击案例知识的分类体系。

2.1 案例主体

案例主体是指网络攻击案例的参与主体，包括发起该网络攻击行为或攻击事件的攻击者和遭受此次网络攻击的防御者。案例主体在网络攻击案例中，主要用于描述攻击者和防御者的属性。本文将主体属性分为社会属性和资源属性，其中资源属性分别描述了攻击者和防御者参与网络攻击案例所使用的案例资源，包括硬件属性、软件属性以及网络属性。

2.2 攻击过程

攻击过程用于描述网络攻击案例中，攻击者所采用的攻击战术或策略。通过对典型网络攻击案例[10]的分析，网络攻击的一般攻击过程可以分解为目标节点探测、网络渗透、权限提升、拒绝服务、痕迹清除 5 个可能的攻击步骤。节点探测是网络攻击的前提和基础，攻击者根据探测得到的目标信息，分析研究目标系统可能存在的渗透漏洞，进入目标主机获取更高权限，或是对目标主机实施拒绝服务攻击。在网络攻击的最后阶段，完成必要的攻击痕迹清除动作。

2.3 防御过程

防御过程主要用于描述网络攻击案例中，遭受网络攻击的防御者可能采取的防御策略或战术。本文根据防御者防护的不同目标对象类型，将防御过程大体分为网络防护、本地防护、数据保护 3 大类，是一个由点到面的防护过程。

2.4 案例结果

案例结果用于描述网络攻击案例攻击过程和防御过程之间的对抗博弈结果，从某种意义上说，部分描述了攻击者发起此次网络攻击的攻击效果。目标主机在遭受网络攻击后，可能存在不同程度的损坏。案例结果的描述，本文从攻击者对目标主机发起攻击的主要目的出发，对目标主机上的敏感信息的获取、目标重要组件甚至系统的破坏以及控守目标主机所产生的影响进行描述。由此，攻击案例的结果可从信息泄露、数据破坏、入侵控制和拒绝服务 4 个方面体现。

综合以上分析，本文给出一个较为全面的网络攻击案例知识的分类体系，如图 2 所示。

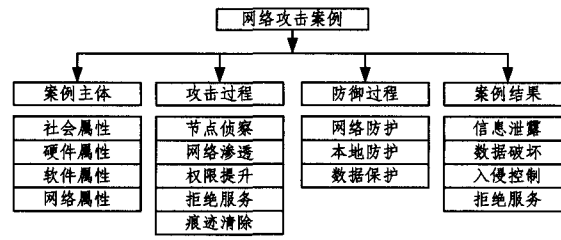

图 2 网络攻击案例知识分类体系

3 网络攻击案例本体模型

在上述定义的网络攻击案例形式化表示，以及网络攻击案例知识分类体系的基础上，通过应用共享知识工具本体，构建网络攻击案例本体模型，实现网络攻击案例知识共享。

3.1 本体

本体论（ontology）起源于哲学，主要研究物质世界的存在问题。在计算机及相关领域，本体指应用本体论的基本方法，通过概念分析、建模，把现实世界中的实体抽象为一组概念以及概念间的关系的理论和方法。从本质上说，本体是共享概念模型的明确的规范说明，是实现异构知识建模的有效工具。通过研究确立领域概念、概念之间的本质联系和隶属关系，构建领域概念的完整体系，澄清领域知识的层次结构，实现不同组织、不同系统之间的知识共享、互操作和重用等提供方法。本体由概念、关系、公理和实例等基本元素构成，从语义上讲，概念表示的是对象的集合；实例则是组成概念的成员；本体中的关系是指概念之间、实例之间以及概念与实例之间的关系，如包含关系（part-of）、实例关系（instance-of）、子类关系（subclass-of）等。

3.2 本体的构建

本体的构建[8,9]是指对某个特定领域的概念和关系按某种层次结构进行分层刻画的过程，通过基于本体的知识表示方法来组织和表达不同类型的知识，利用形式化的知识表示方法获取知识语义信息的过程。本体建模首先要确定本体应

用的领域，然后针对该领域抽象出领域概念，确立概念间层次关系，进而构建领域知识本体模型。本文采用本体技术构建网络攻击案例概念模型，描述网络攻击案例知识概念结构，从而实现网络攻击案例知识的共享。网络攻击案例本体的构建流程如图 3 所示。

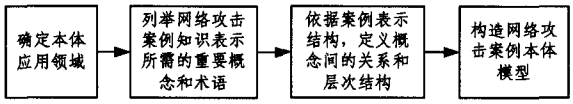

图 3　攻击案例本体构建流程

3.3　网络攻击案例本体模型

网络攻击案例是指，将一次网络攻击事件所涵盖的网络攻击知识，以案例的知识表示形式进行关联和存储。网络攻击案例本体是在把握网络攻击本质的基础上，通过抽象网络攻击案例知识及其关系约束的明确定义，实现复杂网络攻击案例知识概念的规范化描述。结合本体模型构建的基本要素，本文将网络攻击案例本体(network attack case ontology，NACO)形式化定义为：

定义 3　$NACO::=\{KNA,RNA,ANA,INA\}$

其中，KNA 用来描述网络攻击案例知识概念集；RNA 描述案例知识概念间的关系集；ANA 描述案例知识概念的属性集；INA 描述网络攻击案例知识概念实例集。

由于网络攻击案例知识的复杂性，结合网络攻击案例表示定义 2，本文将 KNA 进一步形式化为：

定义 4　$KNA::=\{Subject,AttackProc,DefendProc,CaseResult\}$

其中，*Subject* 描述网络攻击案例主体知识，包括案例攻击者和防御者；*AttackProc* 用于描述案例攻击者的攻击过程案例知识；*DefendProc* 用于描述防御者的防御过程案例知识；*CaseResult* 用于描述网络攻击案例的案例结果知识。

本文通过分别定义领域本体、应用本体和原子本体，层次化描述网络攻击案例领域知识本体。它们之间的关系如图 4 所示。

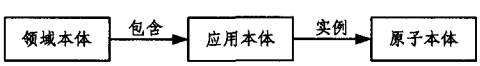

图 4　网络攻击案例本体层次关系

(1)攻击案例领域本体

领域本体是专业性的本体，提供了某个特定领域内的概念集以及概念之间的关系。

攻击案例领域本体用于描述当前攻击所需的概念和关系集：根据网络攻击案例本体定义 3，攻击案例领域本体包含 4 个子类：案例主体、攻击过程、防御过程、攻击结果。攻击类概念之间包含 4 种关系：案例主体(即案例攻击者和案例防御者)参与网络攻击，分别发起攻击过程和防御过程，经过攻防博弈之后产生案例结果，如图 5 所示。

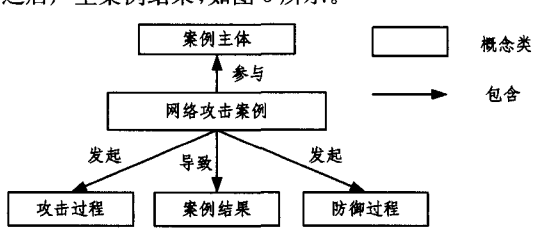

图 5　网络攻击案例领域本体

(2)攻击案例应用本体

应用本体是对领域本体的进一步描述，根据以上对网络攻击案例领域子类的划分，可对各领域子本体作进一步描述。

a)案例主体子领域应用本体包括社会属性、硬件属性、软件属性、网络属性。

b)攻击过程子领域应用本体包括节点侦察、网络渗透、权限获取、拒绝服务、痕迹清除。

c)防御过程子领域应用本体包括网络防护、本地防护和数据保护。

d)案例结果子领域应用本体包括信息泄露、数据破坏、入侵控制和拒绝服务。

图 6 示出网络攻击案例应用本体、攻击案例领域本体和应用本体之间的包含关系。

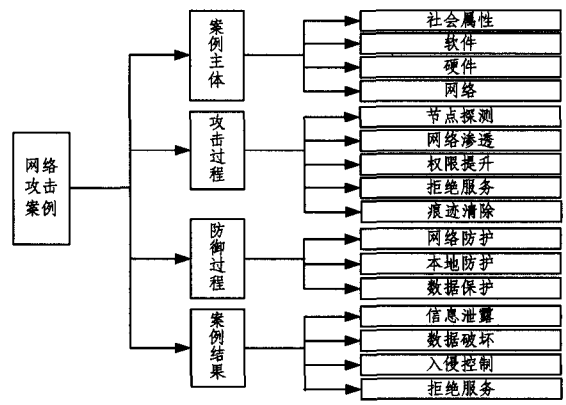

图 6　网络攻击案例应用本体

(3)攻击案例原子本体

网络攻击案例原子本体是网络攻击案例本体可直接应用的实体概念的声明，原子本体中的实例与应用本体中的概念是类与实例(instance-of)的关系。各类攻击应用本体的原子本体描述如下。

a)攻击案例主体原子本体

攻击案例主体原子本体用于详细描述案例参与者即攻击者和防御者的社会属性，以帮助网络安全人员在分析网络攻击案例过程中挖掘出更多的有效信息。案例主体资源属性描述了攻击者和防御者在进行网络攻防博弈的背景资源信息。案例主体领域原子本体如图 7 所示。

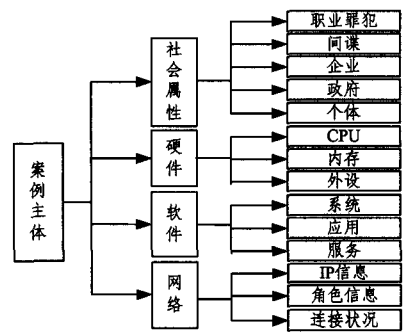

图 7　案例主体领域原子本体

b)攻击案例攻击过程原子本体

攻击过程原子本体用于进一步描述网络攻击案例中攻击者为达到攻击目的具体所采用的攻击策略和技术手段，如图 8 所示。

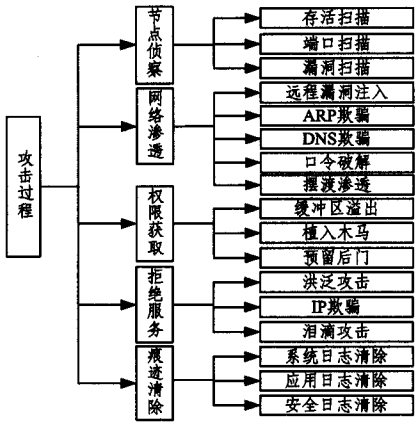

图 8　网络攻击案例攻击过程原子本体

c)攻击案例防御过程原子本体

同攻击过程原子本体类似，攻击案例防御过程原子本体是防御者在遭受网络攻击时所采用的防御策略和技术手段，如图 9 所示。

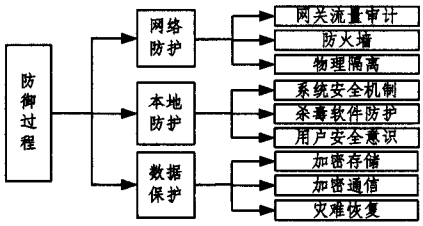

图 9　网络攻击案例防御过程领域本体

d)攻击案例结果原子本体

案例结果原子本体进一步描述了网络攻击案例攻防博弈的结果，如图 10 所示。

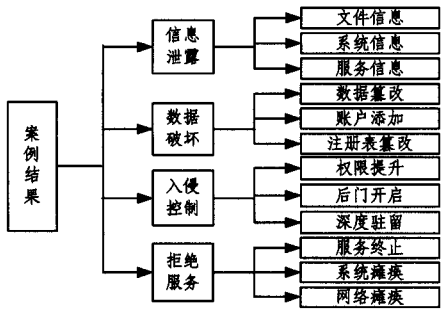

图 10　攻击案例结果原子本体

通过定义网络攻击案例的领域本体、应用本体和原子本体，层次化描述了网络攻击案例领域知识，为网络攻击案例的共享和复用提供语义基础，也可根据实际应用模型构建案例库过程的需要，对其进行扩展。

4　实例分析

假定以某黑客组织针对某互联网企业用户进行渗透攻击为例，根据上述定义的基于本体的网络攻击案例模型，对该实例实现案例化表示，以验证该模型的有效性。

网络渗透[10]是指攻击者出于某种经济或政治目的针对某个远程目标主机采取的入侵行为，从而使得该目标主机完全受控于攻击者。目前比较流行的网络渗透技术有远程漏洞注入、中间人渗透、XSS 跨站脚本注入、SQL 注入、口令破解等技术。

在对目标主机进行渗透之前，攻击者首先得明确目标局域网内的存活主机信息，包括存活主机的主机类型、操作系统版本、开放服务以及可能的漏洞等信息。在对远程目标进行详细侦察后，发现某目标机器存在 RPC 漏洞，进而发起漏洞注入攻击。突破目标机器可能存在的安全防护机制后，植入后门程序，实现驻留，然后再对目标局域网内其他主机进行渗透攻击，最终控制整个目标局域网络。

根据构建的网络攻击案例本体模型，分别从案例描述信息、案例主体、攻击过程、防御过程和案例结果 5 个方面对上述案例进行描述，如图 11 所示。

从图中可以看出，通过运用基于本体的网络攻击案例库模型，渗透攻击案例知识得到了较全面的描述，有效地表示了案例的攻击过程和防御过程，案例中攻击者和防御者之间的攻防博弈过程得到了一定程度的体现，知识间关联性较强，较丰富的案例背景知识也有利于网络安全研究人员对该渗透攻击案例进行更深入的分析研究。

从上述渗透攻击实例的知识表示过程可以分析得出，通过引入案例的知识表示方法，对网络攻击案例中的攻击过程知识和防御过程知识进行有效关联，更符合网络攻击案例攻防双方深度博弈的特点，有效地弥补了仅从攻击者这个单一角度研究网络攻击知识表示的不足。

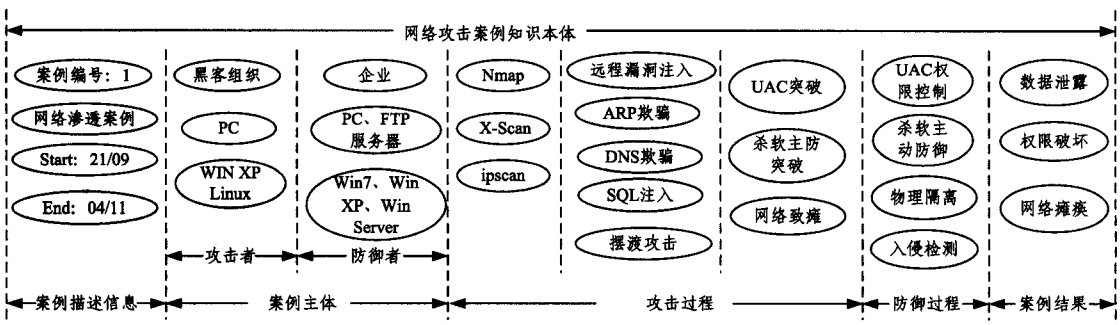

图 11　渗透攻击案例的知识获取

结束语　本文以案例的角度，研究网络攻击行为和攻击事件，以更全面地获取网络攻防知识。结合案例表示通用方法，给出了网络攻击案例的形式化定义，并提出了网络攻击案例知识分类体系，继而构建了网络攻击案例领域知识本体模型，为构建一个共享、重用、可扩展的网络攻击案例库提供语

（下转第 195 页）

了一种基于模糊身份密码学的身份认证方案，其利用用户的生物信息作为身份标识来验证中继节点的身份，使得恶意节点无法通过伪造属性来获得转发机会，从而提高了报文投递率。同时，我们以典型的基于上下文信息的转发协议 Propicman 为基础给出了具体的实施方案，并进行了仿真实验。实验表明，基于模糊身份密码学的 Propicman 在性能上与原协议基本保持一致。而当网络环境中存在大量的恶意节点时，F-ONIAS Propicman 方案具有较高的报文投递率及较低的路由开销率。

参 考 文 献

[1] 熊永平，孙利民，牛建伟，等. 机会网络[J]. 软件学报，2009，20(1)：124-137

[2] Grossglauser M，Tse D. Mobility increases the capacity of ad-hoc wireless networks[C]// Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies(INFOCOM 2001). 2001，3：1360-1369

[3] Spyropoulos T，Psounis K，Raghavendra C S，et al. Single-copy routing in intermittently connected mobile networks[C]// 2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks，2004 (IEEE SECON 2004). IEEE，2004：235-244

[4] LeBrun J，Chuah C N，Ghosal D，et al. Knowledge-based opportunistic forwarding in vehicular wireless ad hoc networks[C]// Vehicular technology conference，2005. VTC 2005-Spring. 2005 IEEE 61st. IEEE，2005，4：2289-2293

[5] Jones E P C，Li L，Schmidtke J K，et al. Practical routing in delay-tolerant networks[J]. IEEE Transactions on Mobile Computing，2007，6(8)：943-959

[6] 李东生，杨志义，郭斌，等. 基于机会网络的社会性活动组织研究[J]. 计算机科学，2013，40(2)：35-39

[7] Hui P，Crowcroft J，Yoneki E. Bubble rap：Social-based forwarding in delay-tolerant networks[J]. IEEE Transactions on Mobile Computing，2011，10(11)：1576-1589

[8] Boldrini C，Conti M，Jacopini J，et al. Hibop：a history based routing protocol for opportunistic networks[C]// IEEE International Symposium on World of Wireless，Mobile and Multimedia Networks，2007(WoWMoM 2007). IEEE，2007：1-12

[9] Lindgren A，Doria A，Schelén O. Probabilistic routing in intermittently connected networks[J]. ACM SIGMOBILE Mobile Computing and Communications Review，2003，7(3)：19-20

[10] Seth A，Keshav S. Practical security for disconnected nodes [C]// 1st IEEE ICNP Workshop on Secure Network Protocols，2005 (NPSec). IEEE，2005：31-36

[11] Kate A，Zaverucha G M，Hengartner U. Anonymity and security in delay tolerant networks[C]// Third International Conference on Security and Privacy in Communications Networks and the Workshops，2007(SecureComm 2007). IEEE，2007：504-513

[12] Shikfa A，Onen M，Molva R. Privacy in context-based and epidemic forwarding[C]// IEEE International Symposium on a World of Wireless，Mobile and Multimedia Networks & Workshops，2009(WoWMoM 2009). IEEE，2009：1-7

[13] Trifunovic S，Legendre F. Trust in Opportunistic Networks[J]. 2009

[14] Keränen A，Ott J，Kärkkäinen T. The ONE simulator for DTN protocol evaluation[C]// Proceedings of the 2nd International Conference on Simulation Tools and Techniques，ICST (Institute for Computer Sciences，Social-Informatics and Telecommunications Engineering). 2009：55

(上接第 176 页)

义基础。最后，通过对网络攻击实例的有效知识获取，验证了基于本体的网络攻击案例库模型的有效性。

参 考 文 献

[1] López B. Case-Based Reasoning：A Concise Introduction[J]. Synthesis Lectures on Artificial Intelligence and Machine Learning，2013，7(1)：1-103

[2] Acorn T，Walden S. SMART：Support management automated reasoning technology for Compaq customer service[C]// Proceedings of the Tenth National Conference on Artificial Intelligence. MIT Press，1992

[3] William M. Bain Judge：a case-based reasoning system Machine learning[M]// a guide to current research. Kluwer Academic Publishers Norwell，MA，USA，1986

[4] 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

[5] 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

[6] 吴林锦，武东英，刘胜利，等. 基于本体的网络入侵知识库模型研究[J]. 计算机科学，2013，40(9)：120-124，129

[7] 谢新洲，夏晨曦. 网络事件案例库建设与案例数据分析[J]. 情报学报，2012，31(1)：72-81

[8] Amailef K，Lu J. Ontology-supported case-based reasoning approach for intelligent m-Government emergency response services[J]. Decision Support Systems，2013，55(1)：79-97

[9] Akmal S，Batres R，Shih L H. An Ontology-based Approach for Product-Service System Design[M]// The Philosopher's Stone for Sustainability. Springer Berlin Heidelberg，2013：67-72

[10] McClure S，Scambray J，Kurtz G. 黑客大曝光：网络安全机密与解决方案[M]. 2006