安全本体研究进展

高建波[1] 张保稳[1] 陈晓桦[2]
(上海交通大学信息安全学院 上海 200240)[1] (中国信息安全认证中心 北京 100020)[2]

摘 要 本体概念已经被广泛地应用到人工智能系统、计算机科学、信息技术、生物医学等众多学科领域。对不同领域的本体分析构成了该领域知识表示体系的核心,同时本体研究促进了知识的共享和重用。将本体的概念应用在信息安全领域就形成了安全本体。主要从以下几个方面描述了安全本体:安全本体研究的现状及发展过程,构建安全本体的原则、方法和意义,现有的安全本体及分类,安全本体的描述语言,安全本体的应用。接着依据对现有的安全本体及其应用的分析,总结了安全本体的结构体系,描述了安全本体的知识表示及推理能力,并指出在构建安全本体、本体评估、本体学习和安全本体的应用等方面依然有待完善。

关键词 安全本体,本体,形式化,网络本体语言,信息安全
中图法分类号 TP309.09 **文献标识码** A

Research Progress in Security Ontology

GAO Jian-bo[1] ZHANG Bao-wen[1] CHEN Xiao-hua[2]
(Department of Information Security, Shanghai Jiaotong University, Shanghai 200240, China)[1]
(China Information Security Certification Center, Beijing 100020, China)[2]

Abstract Ontology is applied in various domains, including intelligence system, computer sciences, information technology, and biomedical sciences et al. The analysis of ontology becomes the core of knowledge representation system in different domains. At the same time the study of ontology facilitates knowledge sharing and reuse. Applying ontology in information security makes security ontology(SO). This paper mainly described the following aspects of SO: present and history of SO, principle, method, and meanings of building SO, existing SO and its categories, dedcription language and application of SO. Then according to above analysis, this article concluded its structural system, depicted knowledge representation and reasoning ability of SO, and pointed out there is a long way to go in building of SO, ontology evaluation, ontology learning, and application of SO.

Keywords Security ontology, Ontology, Formal, OWL, Information security

安全本体是本体概念在信息安全领域的应用。其主要用于提供安全领域内形式化的统一的术语及术语间的关系,同时具备推理和查询的功能。形式化指所有术语及术语间的关系被形式化的语言(比如命题逻辑、一阶谓词逻辑、描述逻辑等)所描述。而作为安全本体的主体——本体(ontology),起初是属于哲学的范畴,研究有关"是"以及"存在"的学问。Neches 等[1]于 1991 年定义本体为:本体给出构成相关领域词汇的基本术语和关系,以及利用这些术语和关系构成的规定这些词汇外延的规则的定义。该定义不但给出了 ontology 的定义,而且指出了构建 ontology 的方法:定义明确了 ontology包含基本的术语和术语间的关系,明确了组合术语的规则并提供了这些术语和关系的定义。从中可以看出,ontology 不仅包含准确定义的术语,还包含由这些术语可以推理出来的知识。

在信息安全领域对本体的需求是由 Donner[2]于 2003 年明确提出来的。

信息安全领域需要本体———系列对最重要概念及其之间的关系的描述。如医学院的学生,为避免失误及提高护理的质量,必须学习医学本体,将其作为他们大学教育的一部分,所有信息安全技术者应当学习安全领域相关术语并熟悉它们之间的关系。

随后出现了大量与安全本体相关的研究工作。具有代表性的有 Schumacher[3]2003 年提出的用于维护安全模式知识库的安全本体。该本体的核心概念主要有:资产、威胁、攻击、脆弱性、攻击者、风险、对策,资产所有者和安全目标(机密性、完整性、可用性等)以及它们之间的关系。Denker 等[4]创建了若干个在 Web 服务中描述与信息安全相关的本体,他们起初使用 Daml+OIL 语言,后来使用 OWL 语言。Kim 等[5]在 Denker 的研究基础上进行了改进,提出了自己的本体,并给出了其面向服务架构的一个应用。2005 年,Bill. Tsoumas

到稿日期:2011-10-10 返修日期:2012-01-20 本文受国家重大基础研究 973 计划项目(2010CB731403),公安部信息网络安全重点实验室开放课题(C09603),上海市重点科技攻关课题(11511504302)资助。
高建波(1978—),男,博士生,讲师,主要研究方向为信息安全测评;张保稳 男,副研究员,主要研究方向为信息安全测评,E-mail:Zhangbw@sjtu.edu.cn(通信作者);陈晓桦 男,教授,主要研究方向为信息安全认证。

等[6]分析了构建安全本体的方法并将其应用于信息安全管理架构。他们的主要贡献在于将安全需求和技术实施分离，依据 CIM(Common Information Model)[7]标准建立基本的本体模型并利用信息安全领域相关的通用标准来充实本体，使之更加详细、规范。同时他们还制定了一个可行的信息安全管理架构。Stefan Fenz 等[8-10]依据 Landwehr[11]对信息安全领域内概念及其分类的总结设计了自己的安全本体，并将其与 ISO/IEC 27001 标准本体相结合用于风险定量分析和安全标准认证。同时引入了 OntoWorks 平台，使用户可以访问、推理以及看到可视化的本体数据。2007 年，Almut. Herzog，Nahid. Shahmehri，Claudiu. Duma[12]依据 Whitman and Mattord[13]的专注《信息安全原理(第二版)》构建了一个实实在在的安全本体，该本体的核心概念为：威胁、资产、对策、脆弱性。该本体包含 88 个威胁类、79 个资产类、133 个对策、34 个类之间的关系。同时作者分析了如何扩展安全本体的类，描述了本体的推理及查询功能。Shao-Shin Hung 等构建了基于本体的入侵检测架构[14]。2008 年，Blanco 等[15]分析比较了各个安全本体并总结出：现阶段大部分安全本体的研究都集中于特定领域或语义网中，一个完整的安全本体还没有实现。同时他们指出必须通过各个领域的信息安全专家的合作才能完成全安全领域内安全本体的构建。Teresa. Pereira 和 Henrique. Santos[16]于 2009 年提出信息安全本体概念模型并设计了构建安全本体的核心概念，同时认为这种基于本体的信息安全解决方案仍然需要进行深入的研究和探讨。Artem. Vorobiev[17]于 2010 年提出了一个基于本体驱动的信息安全解决方案，用于检测与抵抗对分布式复杂软件系统的攻击。2011 年，Carlos. Blanco 等人[18]在总结和系统比较以往安全本体的基础上，在以下 3 个方面进行了深入的研究：首先提出了整合安全本体的关键要求，其分别是整合的本体必须至少识别所研究领域中必要的、更新的概念(静态知识)；应该允许知识推理(动态的知识)；应该可重用、可分享(可重用性)。其次，他们确认了获取整合本体的最好方法是通过形式化的比较(从内容、分类、关系、公理等因素)研究最前沿的本体。同时他们确认了使用 W3C 推荐的 Protégé 软件和 OWL 语言来完成整合本体的工作是最合适的。

本文在引言中概述了本体、安全本体的概念，以及安全本体的研究历史和现状；第 1 节介绍构建安全本体的原则、方法和意义；第 2 节详细分析现有的安全本体及分类；第 3 节介绍安全本体的描述语言，主要讲述 OWL-DL 语言的相关属性；第 4 节叙述安全本体在信息安全领域的应用；第 5 节描述安全本体的知识表示能力，总结安全本体的结构体系；最后总结全文并提出若干安全本体的发展方向。

1 构建安全本体的原则方法和意义

1.1 原则

如构建本体的原则一样，安全本体的设计也遵循 Tom Gruber 提出的 5 条设计本体的基本准则[19]：1) 明确性(Clarity)；2) 一致性(Coherence)；3)可扩展性(Extendibility)；4)最小编码偏差(Minimalencoding bias)；5) 最小本体承诺(Minimal ontological commitment)。

1.2 方法

构建本体的方法首先分为两类情况进行分析：一类为针对一个领域重新开始构建新的本体，另一类为依据已有的本体构建该领域的本体。之所以要讨论后者，是因为对相同的领域，不同的专家可能构建不同的本体来完成各自的应用或任务。比如在信息安全领域，专家可以构建自己需要的本体来完成既定的目标：风险分析、标准的认证、网络脆弱性分析、入侵检测等。第二类情况又细分为两小类[20]：一类为本体结盟方法(Ontology alignment methods)，该方法为已有的本体间建立各种不同的映射，因此这种方法可以保留原有的本体。这类方法包括 ONION 方法[21]、FAC-Merge 方法[22]、Chimaera[23]和 PROMPT[24]方法。另一类为本体合并方法(Ontology merging methods)，该方法使用已有的本体生成一个唯一的本体，该方法常常要求在用于合并的已有本体之间建立映射。这类方法有 Anchor-PROMPT 方法[25]。第二类情况是以第一类为基础的，下面重点介绍对一个领域重新构建新的本体的方法。

虽然有不同的方法，但重新构建本体的方法主要分为以下几步：

首先是信息的收集，包括：安全标准(例如 ISO/IEC 17799[26]、British Standard 7799 Part2[27]、Common Criteria framework[28])、信息安全基础设施的信息、与人员相关的信息、对信息安全应达到的要求和采取的主要应对对策信息、可能受到的威胁(人力的、非人力的)等。

其次，在第一步的基础上构建本体的核心概念。这些概念有：威胁、脆弱性、风险、控制、资产、影响等。由于这一步工作量很大，因此出现了自动(半自动)信息获取的方法——本体学习[29]。

接着将获取的核心概念构成以概念为中心的部分本体，分别描述该领域的不同问题，具体实现方法见 Natalya F. Noy[30]的文章。然后将这些部分本体合并为一个完整的本体，并对概念进行完善，修改概念的属性和关系，以避免冗余。

最后是对本体进行评估。如果评估的结果不满意，则可以重新从第一步开始再做一遍，直到满意为止。

1.3 意义

正如 Teresa Pereira[16]所述，在安全领域内建立本体的原因在于：

本体可以描述不同概念间的语义关系；

本体可以在不同的成员间，比如人类和软件代理之间，共享通用的结构化的信息，而这种结构化的信息是可以自动推理分析的；

本体可以重用并随时间的推移而不断演化发展；

本体可以在不同机构之间共享以解决协同工作的问题。

2 现有的安全本体及分类

2.1 安全本体的分类

依据安全本体内部结构粒度将其区分为：轻量级本体(lightweight ontology)和重量级本体(heavyweight ontology)。轻量级本体包含概念、概念分类、概念间的关系以及描述概念的属性。重量级本体在轻量级本体上附加了公理和约束。公理和约束明确了本体中术语的意义。

依据领域的依赖程度将安全本体分为：领域级和应用级安全本体。领域级的安全本体描述全信息安全领域内的概念及概念之间的关系。而应用级安全本体仅描述安全领域内与

特殊应用相关的概念及概念之间的关系。

2.2 现有的安全本体

Denker 等人构建的本体是领域级的，他们创建了许多用于标识代理和 Web 服务的安全本体。本体描述语言起初使用的是 Daml+OIL 语言，后来使用 OWL 语言。这些本体描述了安全领域内众所周知的概念，使得我们可以将安全标准互联起来。该本体主要由两个部分本体构成：用于获取高级安全概念的安全机制及用于定义认证方法的证书。Kim 等人在 Denker 研究的基础上进行了改进，构建了 NRL 安全本体。该本体关注于资源的功能标识方面，可以表述一些安全事宜，例如机理、协议、算法和证书。主要由 7 个部分本体构成，其中安全服务本体、安全代理本体、信息对象本体的构建是基于已经存在的 DAML 安全本体。证书本体、安全算法本体、安全保证本体、主安全本体是新建的本体。它们之间的关系为：证书本体、安全算法本体、安全保证本体为主安全本体概念的属性提供数值；安全服务本体为在 Web 服务中使用主安全本体的安全概念提供方法；信息对象本体使用安全算法本体为 Web 服务输入输出提供标识。

Bill Tsoumas 等人分析了构建信息安全领域内本体的方法以及将本体应用于信息安全管理的架构，他们的主要思想在于将安全本体需求和技术实施方法分离，以便于安全管理。同时依据 CIM 建立了安全领域内的本体并通过使用安全标准(CC，ISO/IEC17799，BS7799)丰富、规范本体的内容。以上提到的构建新本体的方法主要是基于他们的思想。同时在信息收集环节，Tsoumas 等人亦做了深入的研究。图 1 是他们所构建的本体。图 1 中以风险分析为主线，构建了一个安全本体。以下是对其的详细分析：威胁机构发起威胁，威胁利用资产的脆弱性攻击资产，导致有害的威胁产生，而且资产的脆弱性会激活风险。威胁又会产生风险，风险生成有害的威胁，同时脆弱性本身也会发起有害的威胁，有害的威胁对资产产生影响。资产所有人拥有安全措施，安全策略包含控制方法，而控制方法包含对策，对策以威胁和资产为研究的对象，其目的为减少资产的脆弱性，降低有害威胁产生的影响。从以上分析可以看出，威胁、资产、脆弱性、对策在这个安全本体中占据着举足轻重的位置。

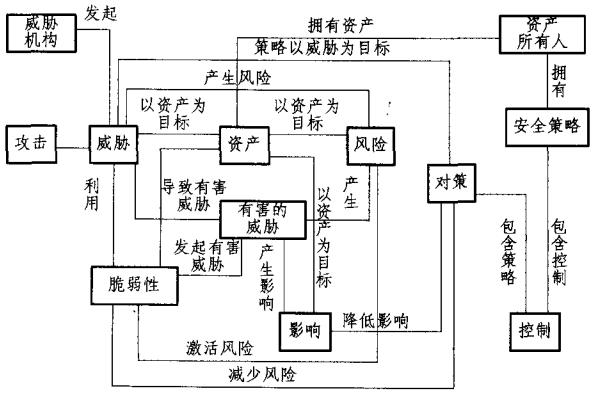

图 1 风险分析安全本体概念模型

2007 年，Almut. Herzog 等人在信息安全领域内构建的安全本体核心概念有：威胁、资产、对策、脆弱性。概念之间的关系为：威胁利用资产的脆弱性对资产构成了威胁，同时受到威胁的还有安全目标。对策可以保护资产，同时其本身也是资产。对策通过使用防御策略保护安全目标和资产。例如，对策“备份”通过恢复(一种防御策略)来保护资产的完整性和可用性(安全目标)。在 Herzog 构建的安全本体中，概念防御策略的实例包括：预防、检测、恢复、纠正、威慑、偏离。安全目标的实例有：机密性、完整性、可用性、真实性、可鉴定性、可说明性、匿名性、可信性、可授权性、可纠正性、可证明性、不可否认性、策略适应性、私密性、保密性和可信任性。安全目标之间也互相有联系，例如，与私密性相联系的有机密性、匿名性和保密性。作者使用基于描述逻辑的 OWL 语言构建了整个安全本体，详细描述了威胁、对策、资产。以下是属于安全策略的备份和属于威胁的间谍程序 spyware 的 OWL 表示方法及解释。

```
Class(Backup partial
Countermeasure
restriction(protects allValuesFrom(intersectionOf(
unionOf(_Availability _Integrity) _Data _Recovery)))
restriction(protects someValuesFrom(_Availability))
restriction(protects someValuesFrom(_Data))
restriction(protects someValuesFrom(_Recovery))
restriction(protects someValuesFrom(_Integrity)))
)
```

该段 OWL 语句描述的是：备份是一种对策。它通过属于防御策略的恢复只保护可用性、完整性和数据。

```
Class(Spyware partial
MaliciousCode
restriction(threatens someValuesFrom(
intersectionOf(_Privacy _Human)))
restriction(threatens someValuesFrom(
intersectionOf(_Availability _Host)))
restriction(threatens someValuesFrom(
intersectionOf(_Integrity _Host)))
)
```

该段 OWL 语句表示：间谍程序是隶属于恶意代码，它威胁个人的私密性和主机的可用性和完整性。作者还论述了如何扩展安全本体的类，描述了本体的推理及查询功能。

3 安全本体的描述语言

构建本体的语言分为两类，一类为基于 FLogic 和一阶谓词逻辑的经典本体语言，包括：Ontolingua、KIF、LOOM、OCML、FLOGIC。另一类为基于网络的本体语言(本体标记语言)，这类语言的语法是基于标记语言 HTML 和 XML 的，主要目的在于数据表示和数据交换，包括：SHOE、XOL、RDF(S)、OIL、DAML+OIL、OWL。其中 OWL(Web Ontology Language)的知识表示(knowledge representation)基础为描述逻辑。

从下面的例子中可以看出描述逻辑是如何形式化语句的。该语句用自然语言表达为：文件访问控制(FileAccessControl)是访问控制的子概念，它保护文件的机密性或完整性，同时它确保访问者只能按照制定好的文件访问策略访问文件。其描述逻辑语言表达式为：

AccessControl and protects some(_File and _Confidentiality or _Integrity) and protects some(_Human and _Policy-

Compliance)

以上语句的等价符号表达式为：

AccessControl∩(∃protects(_File∩(_Confidentiality∪_Integrity)))∩(∃protects(_Human∩_PolicyCompliance))

描述逻辑具有较强的表述事物的能力，可用于形式化描述的对象，同时它是一阶谓词逻辑的一个可判定子集，具有严格的语法和严谨的推理，非常适合于构建本体。而由 W3C 组织推荐的描述本体的 OWL 语言的知识表示基础为描述逻辑，同时由 Horrocks 等人的方法可以将描述逻辑表示的本体转化为 OWL 语言表示的本体[33]。所以大量的本体使用更适合于语义网的 OWL 语言。使用该语言构建本体的优点还包括可以使用 OWL 推理机(FaCT，Racer，Pellet 等)和 OWL 查询语言[34]。

4 安全本体的应用

本体在信息安全领域得以广泛应用。其已应用于信息安全的认证[8]、风险评估[10,35]、风险与资产管理[36,37]、电子政务[38]和电子商务[39]。下面具体介绍部分应用。

安全本体可以用于信息安全管理中的风险分析。首先建立一个信息安全领域的风险分析本体，该本体主要包括如下概念：访问、攻击者、资产、攻击、安全事件、事件发生的时间、事件引起的损失、处理事件的方法、脆弱性、安全对象、对策、风险等。风险分析本体还包括关系、约束、公理、规则。风险的定量分析参见 Stefan Fenz 的论文[10]。其主要思想为：首先列举出所有资产，包括它们的价值以及可能受到的威胁，其次估计威胁发生的概率和它对资产的破坏程度，最后依据以上两项计算风险的大小。

同时在信息安全风险分析中可以使用模糊逻辑。Soo Hoo[46]在他的论文中将风险造成的损失表述为以下式子：

$$ALE_k=\sum_{i=1}^{n}\{F_0(B_i)D_0(B_i)\prod_{j=1}^{m}[(1-E_f(B_i,S_j)I_k(S_j))(1-E_d(B_i,S_j)I_k(S_j))]\}$$

式中，B_i 为威胁事件，$i=\{1,2,3,\cdots,n\}$；S_j 为安全策略，$j=\{1,2,3,\cdots,m\}$；$I_k(S_j)$为二进制值，如果使用了安全策略，则其值为 1，否则为 0；$F_0(B_i)$为没有安全策略时威胁事件发生的概率；$D_0(B_i)$为没有安全策略时威胁事件产生的影响；$E_f(B_i,S_j)$为安全策略 S_j 对威胁事件发生频率的减轻度；$E_d(B_i,S_j)$为安全策略 S_j 对威胁事件产生影响的减轻度；ALE_k 为使用安全策略后每年耗费的损失。

威胁发生的概率、威胁对资产产生的影响、使用策略后对威胁发生概率的降低程度、使用策略后对资产的保护程度，所有这些概念都具有不确定性，因此需要模糊逻辑来表达，这样更能反映现实的状况。

本体也可应用于网络攻击效果评估，因为人的活动及人之间的关系(朋友关系、信任关系、依赖关系等)会影响网络攻击的效果。人的活动包括浏览网站、使用电子邮件、即时通讯软件、在线社交网站等(如 Facebook)。本体由于可以描述概念及概念之间的关系，因此可以很好地描述以上提到的人与人的关系，并且网络攻击正是沿着这种关系迅速扩张到整个互联网。对社交网络进行本体建模，研究社交网络空间内各个节点之间存在的社会组织行为关系及其特征，研究基于本体的网络空间安全防护对象的建模和安全防护策略，具体描述这种关系对网络攻击效果的影响，建立这种影响的数学模型，正是本课题组正在跟踪的研究方向之一。

5 关于安全本体的一些讨论

5.1 安全本体的结构体系

安全本体的结构体系如图 2 所示。本体主要由类、关系、个体、约束、公理构成。而要形成本体则必须利用形式化的语言(基于框架的逻辑、一阶谓词逻辑、描述逻辑等)去描述要研究的安全领域知识，并形成本领域的知识库(Knowledge Base)，如果用描述逻辑作为形式化语言，知识库主要包括 TBox 和 ABox。其中 TBox 是术语体系，即应用领域的词汇；ABox 是采用这些词汇对个体的断言。知识库用来表示本体。

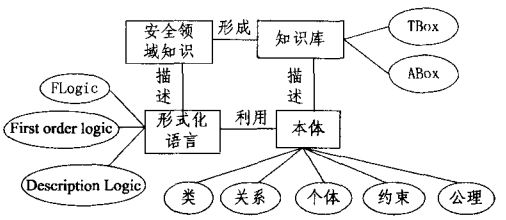

图 2 安全本体的结构体系

5.2 安全本体的知识表示及推理能力

由以上分析知，要先将待研究的安全领域的知识用形式化的语言描述好并形成知识库，再用知识库去表示本体，然后依据本体具有的推理、查询、一致性检验能力去分析所研究领域的知识。例如，Almut. Herzog 等描述的信息安全本体[12]首先用 OWL 语言(该语言的知识表示基础为描述逻辑)描述安全领域的重要概念：资产、威胁、脆弱性、对策；然后建立这些概念之间的相互约束关系，包括类与实例的关系、类之间的关系、类的属性约束，由此形成研究领域的知识库并用来表示本体；再依据推理算法和知识表示领域的公理，推出被研究领域没有被显示定义的类之间的包含被包含关系、实例的断言问题和所定义知识库内部的一致性问题。

在本例中，先用描述逻辑定义好各个概念：Asset、Countermeasure、Vulnerability、Threat；然后新建立一个类 CountermeasureViews，用来测试本体的推理功能，并在该类下建立一个子类 ConfidentialityOfData，其意义为保护数据机密性的所有对策，描述逻辑表达式如下：

Countermeasure and protects some(_Confidentiality and _Data)

建立这个测试类之后，没有必要再在这个类下以定义的方式声明所有可以保护数据机密性的子类，而只需要利用本体附带的推理机就可以推理出符合条件的子类。推理前、后的有关 ConfidentialityOfData 类的层次关系图如图 3、图 4 所示。由于图片过大，图 4 中只列出了 ConfidentialityOfData 类的下属第一层子类。

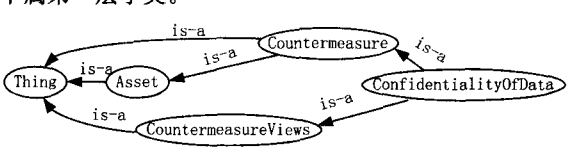

图 3 推理前 ConfidentialityOfData 类的层次结构

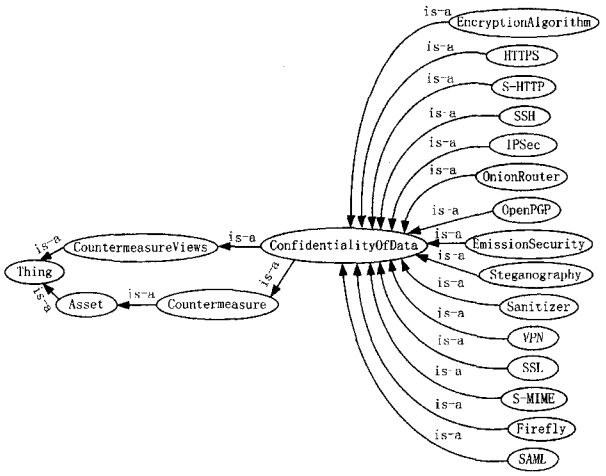

图 4　推理后 ConfidentialityOfData 类的层次结构

使用本体可以表示信息安全领域的知识，其优势在于可以创建类(概念)之间的关系、实例(个体)之间的关系、类和实例(个体)之间的关系，以及可以附加属性到这些关系上，同时可以自动推理、查询和一致性检验[47]。基于本体的这些特性，本课题组[48]使用安全本体对等级保护标准体系进行了建模和分析的尝试。主要过程如下：首先利用本体构建等级保护模型；其次利用模型中的概念、关系描述各级等级保护的条款；然后利用本体的推理能力校验条款之间的包含和一致性关系；最后利用逻辑和算法进行数学推理，从理论上验证本体推理的结果。问题的关键在于两点：首先要建立标准的本体模型，其次要使用描述逻辑算法证明如果一个系统满足高等级保护的某项条款，那么它必须要满足低等级保护的对应条款。例如第 1 级基本要求中网络安全的结构安全要求中有一项条款为："应保证关键网络设备的业务处理能力，满足基本业务需要"；该条款在第 3 级中变为："应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要"；以上两句话在本体中对应的描述逻辑表达式如下：

$$\forall \text{hasAsset}((\text{Netequipment} \cap (\exists \text{hasValuePartion. pivotal})) \cap (\exists \text{hasSatisfy}(\text{businessRequirement} \cap (\exists \text{hasValuePartion. basic}))) \text{ or}(\text{Netequipment} \cap (\exists \text{hasValuePartion. } (\text{all} \cap \neg \text{pivotal})))) \quad (1)$$

$$\forall \text{hasAsset} (((\text{Netequipment} \cap (\exists \text{hasValuePartion. main})) \cap (\exists \text{hasTechnologyRequirement. Redundancy})) \cap (\exists \text{hasSatisfy} (\text{businessRequirement} \cap (\exists \text{hasValuePartion. peak})))) \quad (2)$$

依据结构化包含算法(Structural subsumption algorithms)及概念包含和可满足性的关系(C 被 D 包含$\Leftrightarrow C \cap \neg D$ 是不可满足的)，可以证明(2)$\subseteq$(1)[48]，也即如果满足第 3 级中的要求则必定满足第 1 级中的相应要求。

结束语　由以上讨论可知，可将安全本体相关领域的研究分为两大类：一类为本体本身的研究，包括构建本体的方法及方法论[40]、本体的合并方法[41]、本体描述语言及相关推理逻辑、本体学习的方法[29]；另一类为本体在安全领域的应用，包括本体在标准的逻辑验证方面、风险定性、定量分析[9,10]、安全访问控制[42]、入侵检测系统[14,31]、信息智能检索[43]以及信息系统中基于本体的信任模型[44,45]等方面的应用。

本体正在渐渐融入社会的各行各业并发挥着积极的作用。本文主要从以下几个方面描述了安全本体：安全本体研究的现状及发展过程，构建安全本体的原则、方法和意义，现有的安全本体及分类，安全本体的描述语言，安全本体的应用。展望未来，本体在以下几个方面仍有巨大的发展：因为利用本体可以清晰描述概念及概念间的关系，所以可以用本体来描述机器可读、可共享、可重用的重要领域知识。比如：信息安全领域对风险、资产、脆弱性、策略等关键概念分类及概念间关系的论述；社交网络中对人与人之间关系的本体建模，以及具体描述这种关系对网络攻击效果的影响。本体因为具有可推理、可查询的特征，所以可以用来对需要逻辑推理的领域进行建模。对标准进行一致性检验，对大量数据进行语义搜索，它较传统搜索具有更高查全率和查准率。

同时关于本体本身的研究也是未来的研究重点。将非结构化的知识形式化为计算机可读的本体是一个巨大的工程，所以本体学习仍将是本体研究的一个方向。构建本体虽然有着它的方法和方法论，但很多研究人员依然依据自己的经验构建本体，因此对同一领域会有多个版本的本体，如何将这些本体融合为一个公认的本体又是一个本体未来研究的方向。因为本体是用来表示知识的，但知识本身是随时间而变化的，所以可扩展性也是构建和维护本体的另一个关键问题和研究方向。由于安全本体还处于研究的初始阶段，在信息安全领域还有很多问题有待利用本体的概念去解决，因此本体的构建以及本体的应用方面依然有许多工作要去完成。

参 考 文 献

[1] Neches R, Fikes R E, Finin T, et al. Enabling technology for knowledge sharing[J]. AI Magazine, 1991, 12(3): 36-56

[2] Donner M. Toward a security ontology [J]. IEEE Security and Privacy, 2003, 1(3): 6-7

[3] Schumacher M. Security engineering with patterns: Origins, theoretical model, and new applications [C]// Lecture Notes in Computer Science 2754. Springer-Verlag, 2003

[4] Denker G, Kagal L, Finin T, et al. Security for DAML Web Services: Annotation and Matchmaking[C]// Proc. of the 2nd International Semantic Web Conference(ISWC2003). Sanibel Island, Florida, 2003

[5] Kim A, Luo J, Kang M. Security Ontology for Annotating Resources[C]// Proceedings of the On the Move to Meaningful Internet Systems: CoopIS, DOA, and ODBASE, Lecture Notes in Computer Science 3761. Springer-Verlag, 2005: 1483-1499

[6] Tsoumas B, Dritsas S, Gritzalis D. An ontology-based approach to information system security management[C]// 3rd International Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security. Russia, 2005

[7] DMTF CIM Policy Model v. 2.81 [EB/OL]. http://www.dmtf.org/standards/published_documents.php, 2005-02

[8] Fenz S, Goluch G, Weippl E. Information Security Fortification by ontological Mapping of the ISO/IEC 27001 Standard[C]// 13th IEEE International Symposium on Pacific Rim Dependable Computing. 2007: 381-388

[9] Ekelhart A, Fenz S, Klemen M, et al. Security ontology: Simulating threats to corporate assets[C]// Bagchi A, Atluri V, eds. Information Systems Security, volume 4332 of Lecture Notes in Computer Science. Springer, 2006: 249-259

[10] Ekelhart A, Fenz S, Klemen M, et al. Security ontologies: Improving quantitative risk analysis[C]// 40th Hawaii International Conference on System Sciences. HICSS2007, number 0-7695-2755-8, Waikoloa, HI, USA, IEEE Computer Society, 2007: 156-162

[11] Avizienis A, Laprie JC, Randell B, et al. Basic concepts and taxonomy of dependable and secure computing[J]. IEEE Transactions on Dependable and Secure Computing, 2004, 1(1): 11-33

[12] Herzog A, Shahmehri N, Duma C. An Ontology of Information Security[J]. International Journal of Information Security and Privacy, 2007, 1(4): 1-23

[13] Whitman M E, Mattord H J. Principles of information security (2nd ed)[M]. Thomson Course Technology, 2005

[14] Hung S, Liu D. A user-oriented ontology-based approach for network intrusion detection[J]. Computer Standards & Interfaces, 2008(30): 78-88

[15] Blanco C, Lasheras J, Valencia-Garcia R, et al. A Systematic Review and Comparison of Security Ontologies[C]// Proceedings of the 2008 Third International Conference on Availability, Reliability and Security- Volume 00: IEEE Computer Society. 2008

[16] Pereira T, Santos H. An Ontology Based Approach to Information Security[C]//CCIS 46. Berlin Heidelberg: Springer-Verlag, 2009: 183-192

[17] Vorobiev A. An Ontology-Driven Approach Applied to Information Security[J]. Journal of Research and Practice in Information Technology, 2010, 42(1): 61-76

[18] Blanco C, Lasheras J, Fernández-Medina E, et al. Basis for an integrated security ontology according to a systematic review of existing proposals[J]. Computer Standards & Interfaces, 2011, 33: 372-388

[19] Gruber T. Towards principles for the design of ontologies used for knowledge sharing[J]. International Journal of Human Computer Studies, 1995, 43(5/6): 907-928

[20] Noy NF, Musen MA. SMART: Automated Support for Ontology Merging and Alignment[C]// Gaines B R, Kremer B, Musen M A, eds. 12 th Banff. Alberta, Canada, 1999(4-7): 1-20

[21] Gangemi A, Pisanelli D M, Steve G. An Overview of the ONIONS Project: Applying Ontologies to the Integration of Medical Terminologies[J]. Data & Knowledge Engineering, 1999, 31(2): 183-220

[22] Stumme G, Maedche A. FCA-MERGE: Bottom-Up Merging of Ontologies[C]// Nebel B, ed. Proceedings of the Seventeenth International Joint Conference on Artificial Intelligence (IJCAI 2001). Seattle, Washington: Morgan Kaufmann Publishers, 2001: 225-234

[23] McGuinness D, Fikes R, Rice J, et al. The Chimaera Ontology, Environment[C]// Rosenbloom P, Kautz HA, Porter B, eds. 17th National Conference on Artificial Intelligence (AAAI'00). Austin, Texas, 2000: 1123-1124

[24] Noy N F, Musen M A. PROMPT: Algorithm and Tool for Automated Ontology Merging and Alignment[C]// Rosenbloom P, Kautz H A, Porter B, eds. 17th National Conference on Artificial Intelligence (AAAI'00). Austin, Texas, 2000: 450-455

[25] Noy N F, Musen M A. Anchor-PROMPT: Using Non-Local Context for Semantic Matching[C]// Gómez-Pérez A, Gruninger M, Stuckenschmidt H, eds. IJCAI'01 Workshop on Ontologies and Information Sharing. Seattle, Washington, 2001: 63-70

[26] ISO/IEC 17799. Information technology-Code of practice for information security management[S]. ISO, 2000

[27] British Standard 7799. Information Technology-Specification for Information Security Management System (Part 2)[S]. BSI, 1999

[28] ISO/IEC 15408-1, 2, 3. 1999 Information technology-Security techniques-Evaluation criteria for IT security-Part 1: Introduction and general model, Part 2: Security functional requirements, Part 3: Security assurance requirements[S]. 1999

[29] Kietz J U, Maedche A, Volz R. A Method for Semi-Automatic Ontology Acquisition from a Corporate Intranet[C]// Aussenac-Gilles N, Biébow B, Szulman S, eds. EKAW'00 Workshop on Ontologies and Texts. 2000

[30] Noy N, McGuiness D. Ontology Development 101: A Guide to Creating Your First Ontology[S]. Stanford Knowledge Systems Laboratory Technical Report KSL-01-05 and Stanford Medical Informatics Technical Report SMI-2001-0880. March 2001

[31] Undercoffer J, Joshi A, Pinkston J. Modeling Computer Attacks: An Ontology for Intrusion Detection[C]// The Sixth International Symposium on Recent Advances in Intrusion Detection. Springer, 2003

[32] ISO/IEC FDIS 27001. Information technology Security techniques Information security management systems Requirements [S]. ISO copyright office, Geneva, Switzerland, 2005

[33] Horrocks I, Patel-Schneider P F, Harmelen FV. From SHIQ and RDF to OWL: The making of a web ontology language[J]. Journal of Web Semantics, 2003, 1(1): 7-26

[34] Prud'hommeaux E, Seaborne A. SPARQL query language for RDF[EB/OL]. World Wide Web Consortium(W3C), 2006

[35] Fenz S. Ontology-based generation of IT-security metrics[C]// ACM Symposium on Applied Computing (SAC). ACM, Sierre, Switzerland, 2010: 1833-1839

[36] Liu F H, Lee W T. Constructing enterprise information network security risk management mechanism by ontology [J]. Tamkang Journal of Science and Engineering, 2010, 13(1): 79-87

[37] Li S H, Wang K C. Applications of ontology in management of information asset[C]// International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP). IEEE Computer Society, 2009: 230-233

[38] Sourouni A-M, Kourlimpinis G, Mouzakitis S, et al. Towards the government transformation: An ontology-based government knowledge repository[J]. Computer Standards & Interfaces, 2010(32): 44-53

[39] Albrecht C, Dean D L, Hansen J V. An Ontological Approach to Evaluating Standards in E-Commerce Platforms [J]. IEEE Transactions on Systems, Man and Cybernetics—Part C: Applications and Reviews, 2007, 37(5): 846-859

[40] Santoso H A, Haw S C, Abdul-Mehdi Z T. Ontology extraction from relational database: Concept hierarchy as background knowledge[J]. Knowledge-Based Systems, 2011(24): 457-464

[41] Duong T H, Jo G S, Jung J J, et al. Complexity Analysis of Ontology Integration Methodologies: a Comparative Study[J]. Journal of Universal Computer Science, 2009, 15(4): 877-897

[42] Lu J, Wang C, Zhang G Q, et al. Collaborative management of web ontology data with flexible access control[J]. Expert Systems with Applications, 2010(37): 3737-3746

(下转第 41 页)

TrustValue)远远低于恶意节点原始信任值(OriginalTrustValue);另外当 *mrate*=0.05 时,也即复杂恶意节点以很小的概率作恶时,恶意节点的信任值高于 0.8,甚至可能高于善意节点的信任值,模型也能够很快地识别出恶意节点作恶行为,对其信任值进行降低处理,从而保证善意节点在进行节点选择时,能够进行准确的选择。

3.3 成功交易率

成功交易率就是整个系统成功交易次数在所有交易次数中所占的比例,它直观地反映了信任模型的应用效果。

本组实验设置 3 种实验场景:1) 节点根据信任评价选择响应,考虑了节点的不确定因子,信任评价算法使用本文所述的信任模型,记为 Our-Model;2) 节点根据信任评价选择响应,但不考虑节点的不确定因子,记为 No-Uncertainty-Factor;3) 节点随机地选择响应节点下载,记为 No-Trust。

3.3.1 存在策略型节点情形交易的成功率

为了测试网络中存在善意节点和策略型节点时的成功交易率,分别对 T=0.8 和 T=0.85 进行了测试。在本实验中,善意节点的个数为 50,策略型节点的个数为 50,仿真了 3000 个周期,结果如图 3 所示。

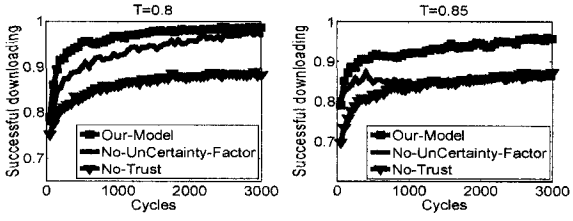

图 3 策略型节点存在时的交易成功率

由图 3 可以看出,当网络中存在大量策略型恶意节点时,Our-Model 能够很好地抵御策略型恶意节点的这种欺骗行为,整个网络的成功交易率高于 No-Uncertainty-Factor 模型和 No-Trust 模型。当 T=0.85,也即该恶意节点的信任值可能高于善意节点时可以看到,在没有考虑节点不确定因子的 No-Uncertainty-Factor 模型中虽然节点是根据信任评价进行选择的,但是其成功交易率比较低,而考虑了节点不确定因子的 Our-Model 的成功交易率还是维持在比较高的水平。

3.3.2 复杂恶意节点存在下交易成功率

为了测试网络中存在善意节点和复杂恶意节点时的成功交易率,分别对 *mrate* 取 0.1 和 0.05 进行了测试。本实验中善意节点的个数为 50,复杂恶意节点的个数为 50,仿真 3000 个周期,结果如图 4 所示。

由图 4 可以看出,当网络中存在复杂恶意节点时,Our-Model 能够很好地辨识出节点的动态行为,使得网络的整体成功交易率高于 No-Uncertainty-Factor 模型和 No-Trust 模型。当 *mrate* 取值 0.05 时,复杂恶意节点虽然以很小的概率作恶,但是也难以掩盖其作恶的本质。由于 Our-Model 引入了不确定因子,使得恶意节点一旦作恶,就能够通过不确定因子达到对恶意节点惩罚的目的,从而保证了网络的整体成功交易率。

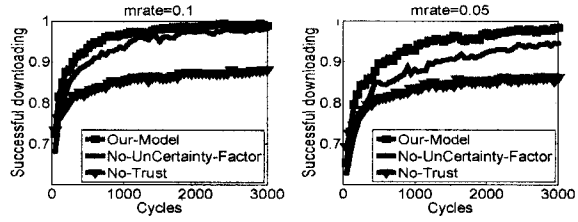

图 4 复杂恶意节点存在时的交易成功率

结束语 本文在传统的云模型的基础上提出了一种符合人类社会关系网中人类心理认知习惯的信任模型。在该模型中,人类认知习惯的引入较好地解决了信任模型中的计算复杂度问题。同时利用云模型,较好地解决了信任的不确定性问题。分析和仿真表明,该模型可以有效抵御网络中恶意节点的欺骗行为和波动行为,提高了 P2P 网络的安全性。如何引入激励机制是以后工作的重点。

参 考 文 献

[1] 李小勇,桂小林. 动态信任预测的认知模型[J]. 软件学报,2010(1):164-176

[2] Beth T,Boreherding M,Klein B. Valuation of Trust in open network[A]// Proceedings of the European Symposium on Research in Computer Security (ESORICS)[C]. New York: Springer-Verlag,1994:3-18

[3] 唐文,陈钟. 基于模糊集合理论的主观信任管理模型研究[J]. 软件学报,2003,14(8):1401-1408

[4] 张光卫,康建初,孟祥怡,等. 基于云模型的主观信任表示研究[J]. 计算机科学,2006,33(11):158-161

[5] 路峰,吴慧中. 基于云模型的信任评估研究[J]. 中国工程科学,2008,10(10):84-90

[6] 李德毅,杜鹢. 不确定性人工智能[M]. 北京:国防工业出版社,2005

[7] 刘常昱,李德毅,杜鹢,等. 正态云模型的统计分析[J]. 信息与控制,2005,34(2):236-239

[8] 孙秋景,曾凡平. 一种信誉机制与云模型相结合的 P2P 环境信任模型[J]. 小型微型计算机系统,2010(7):1328-1332

[9] QueryCycleSimulator[EB/OL]. http://p2p.stanford.edu/www/demos.htm,2004

(上接第 19 页)

[43] Castells P,Fernández M,Vallet D. An Adaptation of the Vector-Space Model for Ontology-Based Information Retrieval[J]. IEEE Transactions on Knowledge and Data Engineering,2007,19(2):261-272

[44] Bimrah K K,Mouratidis H,Preston D. Information Systems Development:A Trust Ontology[C]// Lecture Notes in Computer Science(LNCS). 2007,4805:25-26

[45] Bimrah K K,Mouratidis H,Preston D. Trust Ontology for Information Systems Development [C]// Information Systems Development:Challenges in Practice,Theory,and Education,2009(2):767-779

[46] Hoo K. How much is enough? a risk-management approach to computer security[EB/OL]. Consortium for Research on Information Security and Policy (CRISP). http://iis-db.stanford.edu/pubs/11900/soohoo.pdf. 2000

[47] Thomas C J. Just What Is an Ontology, Anyway [J]. IEEE Computer Society,2009,11(5):22-27

[48] Gao J B,Zhang B W,Chen X H. A logic analysis of ontology-based Classified Protection Standard[C]// International Conference on Computer and Network Technology (ICCNT). 2011(5):337-341