网络安全评估工程中的知识基础设施构建研究*)

毛捍东　陈　锋　张维明　朱　承　宋峻峰
(国防科技大学信息系统与管理学院　长沙 410073)

摘　要　从建立网络安全评估工程中的知识基础设施、获取知识优势出发，以网络渗透本体作为网络安全评估工程的知识基础设施，总结了网络安全评估的通用框架，提出了一种网络渗透本体构建方法 NEOCA；应用 NEOCA 方法构建了一个想定的本体示例，说明该方法的具体工作过程。对于相关工作进行了分析比较，最后给出了结论和下一步工作。

关键词　网络安全评估，网络渗透，本体，知识基础设施

Study on Knowledge Infrastructure Construction for Network Security Assessment

MAO Han-Dong　CHENG Feng　ZHANG Wei-Ming　ZHU Cheng　SONG Jun-Feng
(School of Information System and Management, NUDT, Changsha 410073)

Abstract　For establishing the knowledge infrastructure of network security assessment and gaining the knowledge superiority, in this paper, network exploit ontology is used as the knowledge infrastructure of network security assessment and NEOCA is proposed to construct network exploit ontology; then a scenario situation ontology is constructed by using NEOCA to illustrate the procedure of this approach. Finally, the related works are introduced, and the conclusion and our future work are given.

Keywords　Network security assessment, Network exploit, Ontology, Knowledge infrastructure

1　引言

网络系统已经成为人们生活中重要组成部分，人们总是希望网络系统能够带来更多的便利。但是网络系统自身以及与网络系统相连的网络环境的特点与局限性决定了网络系统的发展和应用将遭受木马、病毒、恶意代码、物理故障、人为破坏等各方面的威胁。如何确保组织网络系统能够在长时间内处于较高的安全水平，是目前亟需解决的问题。网络安全管理是一个系统工程，不能期望通过一个安全产品就能把所有的安全问题都解决。实践表明，需要基于安全评估来建立网络安全战略，有效地进行网络安全评估工程是网络安全管理的第一步[1]。

在网络安全评估工程中，需要对大量网络信息，如网络脆弱性信息、网络渗透等信息等进行分析处理。目前获取这些信息的工具也越来越成熟，但如何有效利用这些信息，将信息优势转化为知识优势成为网络安全评估工程中的一个关键问题。为了解决这个问题，首先需要建立一个合适的知识基础设施(knowledge infrastructure)。

目前，关于网络安全评估的研究主要集中于网络安全评估基本概念[2,3]、网络安全评估方法[4~7]、安全评估模型和算法[8,9]等等。总的来讲，都是围绕如何获取网络信息以及对这些信息进行处理的方法、模型而展开的。很少有如何构建网络安全评估工程中的知识基础设施、获取知识优势的研究。

本体是对概念化的详细说明[18~28]，在语义 Web 和人工智能领域，开展了大量以本体为基础的知识表示[16~19]、自动推理[21~24]、知识共享[14,18,19,27]的研究，根据这些研究成果，我们使用本体作为知识基础设施是合适的。

从建立网络安全评估工程中的知识基础设施、获取知识优势出发，以网络渗透本体作为网络安全评估工程的知识基础设施，总结了网络安全评估的通用框架，提出了一种网络渗透本体构建方法 NEOCA；应用 NEOCA 方法构建了一个想定的示例，说明该方法的具体工作过程。对于相关工作进行了分析比较，最后给出了结论和下一步工作。

2　网络安全评估和网络渗透本体

当前的研究者提出了众多的网络安全评估框架[10~13]，从这些框架可以看出网络安全评估方法发展的趋势：(1)从手动评估向自动评估发展；(2)从自然语言描述向形式化语言描述发展；(3)从小规模网络向大规模网络评估发展。在此基础上，本文总结了一个通用的网络安全评估框架，如图 1 所示，包括网络系统参数抽象、网络安全基础知识库构造以及安全分析等几个核心功能模块。

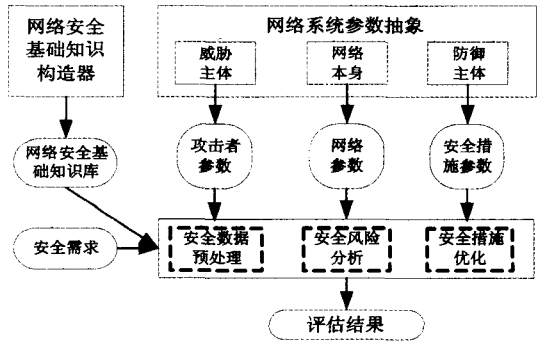

图 1　通用网络安全评估框架

*)本课题得到国家自然科学基金(项目编号 70371008)资助。毛捍东　博士研究生，主要研究方向为安全评估、内网安全；陈　锋　博士研究生，主要研究方向为安全评估、密码学；张维明　教授，博导，主要研究方向为信息安全、信息决策。

网络系统参数抽象是对当前各种信息的收集，包括威胁主体、网络本身以及防御主体三个方面。网络安全基础知识库描述了所有可能导致安全事故的途径和场景，是风险识别和风险分析的基础。安全分析是对网络系统当前信息和网络安全基础知识的综合处理，最终输出评估结果。从图1可以看出，无论是哪种安全评估方法，网络安全基础知识库都是不可或缺的。而且，在不同的评估方法中，网络安全基础知识库是可共享的。所不同的是，不同的研究者对网络安全基础知识库的称呼和描述有所差异。Swiler等[10]称之为攻击模板，攻击模板表达了已知攻击的通用步骤，包括攻击发生必须依赖的条件。为了使用模型检测技术自动创建攻击图，Jha[13]等称之为原子攻击模式库，采用四元素进行描述：入侵者前提条件(intruder preconditions)、网络的前提条件(network preconditions)、对入侵者的影响(intruder effects)、对网络的影响(network effects)。

在本文中，我们统一称为网络渗透本体(*NEO*)。*NEO*由三部分组成：脆弱性实体、前提集和结果集。前提集描述威胁主体试图利用一个脆弱性所需具备的必不可少的条件的集合，只有威胁主体满足前提集时，才可能成功利用此脆弱性。结果集描述通过成功利用此弱点而产生的结果，包括权限的提升、连通关系的增加、数据安全的破坏以及服务安全的破坏等。*NEO*采用本体形式化语言进行描述，形式化的描述可以使其更好地适应成熟的推理引擎，更加有利于后续的安全分析工作。*NEO*是网络安全评估的基础。同时，由于本体具有知识共享的特性，网络渗透本体还可以直接应用于入侵检测、渗透测试等领域。

3 构建网络安全评估工程中的知识基础设施

为了争取知识优势，需要建立网络安全评估工程中的知识基础设施——网络渗透本体*NEO*(network exploit ontology)

3.1 构建网络攻击本体所用的本体语言

目前常见的本体语言有XOL、SHOE、OML、RDF(S)、OIL、DAML+OIL和OWL，可以按照表达能力由弱到强的顺序给上述语言排序：XOL、RDF(S)、SHOE、OML、OIL、DAML+OIL和OWL[32]。

这些语言都采用XML作为语法基础。其中，XOL和SHOE的形式化基础是框架(Frames)，OML的形式化基础是概念图(Conceptual graph)，框架和概念图都缺乏精确的语义。而RDF(S)的表达能力非常有限，只能算做"原始"的本体语言。为了获得表达能力更强大、能够更精确刻画语义的本体语言，在继承RDF(S)的语法和表达能力的基础上，OIL[37]、DAML+OIL[37]和OWL[33~37]都对RDF(S)进行了扩展。OIL是欧洲的研究者开发的一种本体语言；DAML+OIL是由美国&欧盟特别主体标记语言委员会开发的，它是DAML-ONT(由美国DARPA主体标记语言项目组开发)与OIL相结合的产物；OWL是W3C制定的本体语言，它采用DAML+OIL作为起点，是对本体语言进行研究的最新成果。

OWL有三个子集：OWL Lite、OWL DL、OWL Full。OWL Lite的表达能力最有限，推理效率高；OWL DL在保证推理的完备性和可判定性的前提下，有尽可能强的表达能力；OWL Full有最强的表达能力，但不对推理做任何保证。OWL Lite的形式化基础是描述逻辑SHIF(D)[20]，OWL Lite的蕴含是EXPTIME问题，有实用的推理算法，比如FaCT[25]系统和RACER[26]系统就都为OWL Lite提供了实用的优化的推理算法；OWL DL的形式化基础是描述逻辑SHOIN(D)[20]，OWL DL的蕴含是NEXPTIME问题，尚未找到实用的推理算法。

在构建本体的过程中，实践证明，构造器O比构造器I的用处要广泛得多[23]，但具有高效推理系统的OWL Lite的形式化基础却只包含构造器I而不含构造器O。为了获得更好的知识表达能力，本文采用受限制的OWL DL作为构建网络渗透本体所用的本体语言——该限制是禁用inverseOf(对应到OWL DL的形式化基础中，就是禁用构造器I)，我们称这个受限制的OWL DL为OWL LDL(Limited DL)。OWL LDL的形式化基础为SHON(D)，文[23]给出的推理算法可以作为OWL LDL的推理算法，并且已经在FaCT系统中实现了该算法。

3.2 领域、领域概念化、领域本体、本体

我们严格区分本体和领域本体的定义。参考了文[16~19]中的相关说明，给出领域、领域概念化、领域本体、本体的定义如下：

定义1 领域是世界的一个片断，对该片断我们想要表示一些知识；领域概念化是依据所需要解决的任务和所应用本体语言的本体承诺，将领域抽象成一个术语集和一知识集；领域本体={领域术语集，领域知识集}，是对领域概念化的详细说明，一般用本体语言将这个详细说明写出来；本体是对世界概念化的详细说明，关于这个世界只有一个本体，任何应用都不可能需要用到整个本体。

在实际应用中，需要的是领域本体，或者多个领域本体的集成。

定义2 设应用需要用到的领域D可分为n个子领域，可以通过集成这n个子领域的领域本体来获得关于D的领域本体。

3.3 构建网络渗透本体的方法NEOCA

把网络渗透本体看成是关于网络安全渗透这个领域的领域本体，我们无法一次建立网络渗透本体，只能针对网络渗透的各个子领域(如通信窃听、本地缓冲溢出、远程缓冲溢出、木马控制等等)由相关安全专家逐个建立领域本体，然后将这些领域本体集成，以获得整个安全领域的网络渗透本体。

由此可知，构建网络渗透本体的方法NEOCA(network exploit ontology construction approach)包含两个基本方法：

- NEOCA_Ⅰ：构建网络渗透子领域的领域本体。
- NEOCA_Ⅱ：集成网络渗透多个子领域的领域本体。

构建网络渗透本体的方法NEOCA的具体过程是：

第一步，应用NEOCA_Ⅰ方法对网络渗透各个子领域逐个建立领域本体。

第二步，应用NEOCA_Ⅱ方法集成这些子领域的领域本体，集成所得的结果就是网络渗透本体NEO。

第三步，当网络渗透有新的子领域需要建立领域本体时，应用NEOCA_Ⅰ方法建立之。

第四步，当新的子领域的领域本体以NEOCA_Ⅰ方法创建出来后，应用NEOCA_Ⅱ方法将之与已有的网络渗透本体集成，集成所得的结果就是新的网络渗透本体NEO。

通过使用NEOCA方法，我们将逐渐获得越来越完善的网络渗透本体，该网络渗透本体就是网络安全评估工程中的知识基础设施，是争取知识优势的基础。

下面分别详细说明NEOCA_Ⅰ方法和NEOCA_Ⅱ方法

的具体过程。

3.3.1 NEOCA_Ⅰ：构建网络渗透子领域的领域本体

NEOCA_Ⅰ方法的具体过程是：

第一步，创建领域术语集——依据所需要解决的任务和所用本体语言 OWL LDL 的本体承诺，创建领域术语集。此阶段的工作主要是由本体工程师来完成的。

不同的本体语言有不同的本体承诺，例如，命题逻辑本体承诺于事实，即世界由事实构成；一阶逻辑本体承诺于对象、关系，即世界由对象和关系构成[17]。给出 OWL LDL 的本体承诺如下：

定义 3 OWL LDL 本体承诺于类、数据类型、对象属性、数据类型属性、个体和数据值（分别对应于描述逻辑中的概念、具体数据类型、抽象角色、具体角色、个体和值），即世界由类、数据类型、对象属性、数据类型属性、个体和数据值构成。

本体工程师按照以下 2 个原则创建领域术语集：

(1)依据所需要解决的任务来决定领域术语集中的术语；不是领域中所有的术语都需要表达出来，只需要表达与所需解决任务相关的术语。

(2)依据所应用本体语言的本体承诺来决定领域术语集中的术语；在此，按照 OWL LDL 的本体承诺，领域术语集中的所有术语可划分为 6 种，分别是类、数据类型、对象属性、数据类型属性、个体和数据值。

第二步，创建领域本体——依据 OWL LDL 的语法规则，使用领域术语集中的术语，创建领域知识集；领域本体＝{领域术语集，领域知识集}，所以我们在这里就得到了领域本体。此阶段的工作主要是由本体工程师来完成的。

依据 OWL LDL 和 SHON (D)的对应关系，OWL LDL 书写的类、数据类型、对象属性、数据类型属性、个体和数据值可对应到 SHON (D)所考虑的概念、具体数据类型、抽象角色、具体角色、个体和值，OWL LDL 书写的公理和事实可对应到 SHON (D)规定的 Tbox、Abox 和 role hierarchy。

第三步，调用合适的推理系统进行一致性检查——调用可以完成 OWL LDL 所书写领域本体之推理问题的推理系统（例如 FaCT 系统）进行一致性检查，以防止互相矛盾的知识出现。此阶段的工作是由机器自动完成的。

3.3.2 NEOCA_Ⅱ：集成网络渗透子领域的领域本体

定理 1 有 m 个领域，已经为这 m 个领域逐个建立了领域本体。设需要集成这 m 个已经构建好了的领域本体：do_1、do_2、…、do_m，这些领域本体由 OWL LDL 写成，分别可以用 uri_1、uri_2、…、uri_m 来定位（OWL LDL 采用 URI 命名机制，所以这里使用 URI 来定位）；$\forall i\in[1,m]$，do_i＝{v_i, k_i}，其中 v_i 是 do_i 的领域术语集，k_i 是 do_i 的领域知识集，那么

(1)m 个领域本体的集成 $\overset{m}{\underset{i=1}{Integration}}(\text{do\_}i)$ 是

$$\overset{m}{\underset{i=1}{Interation}}(\text{do\_}i)=\{\bigcup_{i=1}^{m}\text{v\_}i,(\bigcup_{i=1}^{m}\text{k\_}i)\cup(\text{IBK})\}$$

其中 IBK(integration built knowledge)是使用术语集 $\bigcup_{i=1}^{m}\text{v\_}i$ 中的术语、以 OWL LDL 写出的知识集，与 $\bigcup_{i=1}^{m}\text{k\_}i$ 不同（$\bigcup_{i=1}^{m}\text{k\_}i$ 反映的是 m 个领域的知识的并集），IBK 反映了 m 个领域集成在一起所新产生的知识，且（$\bigcup_{i=1}^{m}\text{k\_}i$）∪IBK 中的知识须保持一致性。

(2)$\#(\bigcup_{i=1}^{m}\text{v\_}i)=\sum_{i=1}^{m}\#(\text{v\_}i)$，其中“#”表示集合的基数。

证明：m 个领域本体的集成 $\overset{m}{\underset{i=1}{Integration}}(\text{do\_}i)$ 是关于这 m 个领域的领域本体，且有 $\forall i\in[1,m]$，do_i＝{v_i, k_i}，所以可直接利用已经定义好了的 m 个领域本体中的术语作为 $\overset{m}{\underset{i=1}{Integration}}(\text{do\_}i)$ 的术语，得 $\overset{m}{\underset{i=1}{Integration}}(\text{do\_}i)=\{\bigcup_{i=1}^{m}\text{v\_}i$，关于 m 个领域的领域知识集}。

关于 m 个领域的领域知识集包括两部分，一部分是 $\bigcup_{i=1}^{m}\text{k\_}i$，反映的是 m 个领域的知识的并集；另一部分是 m 个领域集成在一起所产生的知识集 IBK，IBK 中的知识无法在单个领域中实现；（$\bigcup_{i=1}^{m}\text{k\_}i$）∪IBK 中的知识须保持一致，否则表明关于 m 个领域的领域知识集是矛盾的。综上，定理的第一部分得证。

因为采用 URI 命名机制，所以每个术语都是惟一的，所以 $\#(\bigcup_{i=1}^{m}\text{v\_}i)=\sum_{i=1}^{m}\#(\text{v\_}i)$，定理的第 2 部分得证。

证毕！

根据定理 1，在多领域本体集成中，因为 $\bigcup_{i=1}^{m}\text{v\_}i$ 和（$\bigcup_{i=1}^{m}\text{k\_}i$）可以利用已有的领域本体生成，所以多领域本体集成的关键是如何创建 IBK。基于这个思想，NEOCA_Ⅱ方法的具体过程是：

第一步，创建 IBK——以 uri_IBK（uri_IBK 可以是新建的 URI，也可以使用已有的 URI）来定位 IBK，设 do_i 中定义了术语 t，若在 IBK 中需要引用、或者扩充定义之，则在 IBK 中可以利用 uri_i#t 来代表术语 t；当所有需要的引用或者扩充定义完成之后，即得到了 $\overset{m}{\underset{i=1}{Intergration}}(\text{do\_}i)$。此阶段的工作主要是由本体工程师来完成的。

第二步，检查一致性——在扩充定义后需要保持一致性，使得多个领域本体的集成是无矛盾的。调用可以完成 OWL LDL 所书写领域本体之推理问题的推理系统（例如 FaCT 系统）进行一致性检查。此阶段的工作是由机器自动完成的。

4 应用实例

为了说明 NEOCA 方法的应用，我们采用 NEOCA 方法构建一个试验环境本体示例，该实验环境下的网络渗透本体是实际环境的简化。试验网络的拓扑结构如图 2 所示，网络为交换网络，目标网络分为用户区和服务区。用户区有 8 台工作站，分别标识为 $IP_{W1}\sim IP_{W8}$，它们的操作系统全部为 windows xp，没有对外开放任何服务。服务区有三台服务器，分别标识为 $IP_{S1}\sim IP_{S3}$，它们的操作系统都是 Linux，同时上面运行若干服务程序，其中，主机 IP_{S1} 上开放 Telnet 服务和 Web 服务，主机 IP_{S2} 上开放 sshd 服务和 ftp 服务，主机 IP_{S3} 上开放 sendmail 服务和 database 服务。试验网络中，防火墙将目标网络和外部网络分开，防火墙允许外部主机 IP_{S1} 对内部主机的 Web 服务进行访问，其它访问均被阻止。主机 IP_{S3} 信任来自主机 IP_{S2} 上的所有网络连接。

通过对试验环境的分析，发现该环境中存在 $v_1\sim v_9$ 共 9 个脆弱性，通过对这些脆弱性的利用，可能存在 $e_1\sim e_{10}$ 共 10 个渗透原子。这些渗透原子总共覆盖了 5 种渗透类型，它们分别为：网络窃听渗透、远程缓冲溢出渗透、本地缓冲溢出渗透、信任渗透以及木马渗透，每种类型对于网络渗透本体而言，都是一个领域本体。每个渗透原子的详细描述如表 1。

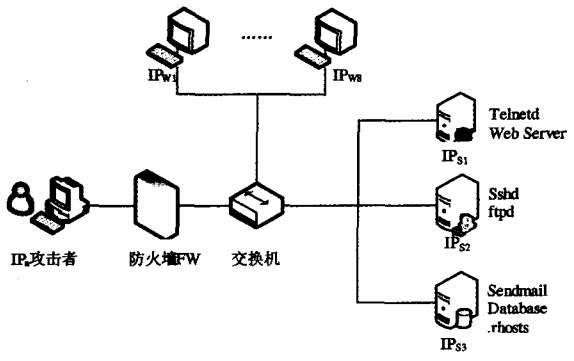

图 2　试验环境

表 1　渗透原子的详细描述

渗透原子	被利用的脆弱性	所在主机	渗透类型
e_1	v_1(CVE-2006-4832)	IP_{S1}	远程缓冲溢出渗透
e_2	v_2(——)	IP_{S1}	网络窃听渗透
e_3	v_3(CVE-2004-0646)	IP_{S1}	远程缓冲溢出渗透
e_4	v_4(CVE-2006-2421)	IP_{S2}	远程缓冲溢出渗透
e_5	v_5(CVE-2005-3524)	IP_{S2}	远程缓冲溢出渗透
e_6	v_5(CVE-2005-3524)	IP_{S2}	木马渗透
e_7	v_6(CVE-2002-1337)	IP_{S3}	远程缓冲溢出渗透
e_8	v_7(CVE-2005-2558)	IP_{S3}	本地缓冲溢出渗透
e_9	v_8(——)	IP_{S3}	信任渗透
e_{10}	v_9(——)	IP_{W1}	木马渗透

为了使领域本体的格式简洁，我们采用描述逻辑语法来书写，这些描述逻辑形式可以转换成相应的 OWL LDL 形式，对应关系见文[37]。

建立该网络渗透本体的过程是：

第一步，应用 NEOCA_Ⅰ方法对网络渗透基本成分领域、网络窃听渗透领域、远程缓冲溢出渗透领域、本地缓冲溢出渗透领域、信任渗透领域以及木马渗透领域逐个建立领域本体。

(1)网络渗透基本成分领域本体——URI 是 uri_NetworkExploit，该领域本体定义了脆弱性(Vulnerability)、前提集(Precondition)、后果集(Postcondition)、操作系统(OS)、应用程序(Application)、访问要求(Preaccess)、CIA 属性(CIA)、权限提升(Postaccess)、网络连通(Postconn)等类。

Vulnerability;
Precondition;
Postcondition;
OS;
Application;
Preaccess;
CIA;
Postaccess;
Postconn;

(2)网络窃听领域本体——URI 是 uri_NetworkSniffer，该领域本体定义了一种网络窃听渗透 e_2。该渗透原子的发生是因为登录"telnetd"服务时的帐号/口令为明文，当威胁主体使用网络窃听工具捕获网络数据包时，可能分析出合法用户的登录帐号/口令。e_2 的发生对目标主机的权限没有要求，渗透成功发生后，对 CIA 属性的破坏分别为 0、5 和 7。同时威胁主体在目标主机上的权限提升到 user 权限，并且增加了到目标主机 21 号端口的连接。

Vulnerability≡hasElement. Name:"No_encrypt"
Precondition≡Application⊓Preaccess;
Application≡hasElement. Name:"telnetd";
Preaccess≡hasElement. Src_access:2⊓hasElement. Des_access:0;
Postcondiction≡CIA⊓Postaccess⊓Postconn;
CIA≡hasElement. Availability:0⊓hasElement. Confidentiality:5⊓hasElement. Integrity:7;
Postaccess≡hasElement. post_access:1;
Postconn≡hasElement. post_conn:21;

(3)远程缓冲溢出渗透领域本体——URI 是 uri_RemoteBufferExploit，该领域本体定义了一种远程缓冲溢出渗透 e_7。该渗透原子的发生是因为版本为 5.79 至 8.12.7 的 sendmail 服务存在脆弱性 CVE-2002-1337，当威胁主体远程攻击者通过发送特定格式的发送人地址和收信人地址而产生缓冲溢出攻击，可以执行任意代码。e_7 的发生对目标主机的权限没有要求，渗透成功发生后，对 CIA 属性的破坏分别为 8、5 和 0。同时威胁主体在目标主机上的权限提升到 root 权限。

Vulnerability≡hasElement. Name:"CVE-2002-1337"
Precondiction≡Application? Preaccess;
Application≡hasElement. Name:"sendmail";
Preaccess≡hasElement. Src_access:1⊓hasElement. Des_access:0;
Postcondiction≡CIA⊓Postaccess⊓Postconn;
CIA≡hasElement. Availability:8⊓hasElement. Confidentiality:5⊓hasElement. Integrity:0;
Postaccess≡hasElement. post_access:2;

使用类似的方法再分别建立本地缓冲溢出渗透领域本体 uri_LocalBufferExploit、信任渗透领域本体 uri_TrustExploit 以及木马渗透领域本体 uri_HorseExploit。由于篇幅原因，不在此详细列出。

第二步，应用 NEOCA_Ⅱ方法集成这些领域本体得到网络渗透本体。

本体工程师通过对网络渗透基本成分领域本体和其他领域本体的分析可知，基本成分领域本体中定义的脆弱性(Vulnerability)、前提集(Precondition)、后果集(Postcondition)等类与其他领域本体种定义的是同一个类，除此以外，没有其他因集成而新产生的知识。那么在 IBK 中，我们需要引用基本成分领域本体中定义的脆弱性(Vulnerability)等类和其它领域本体中定义的脆弱性(Vulnerability)等类，并声明两者是等价的，这样就完成了 IBK 的构建。调用 FaCT 系统对这些领域本体的集成进行一致性检查，检查结果证明两者的集成是无矛盾的。

上面两个步骤完成了试验环境的网络渗透本体 *NEO* 的创建。在此基础上，假设威胁主体的渗透目标是获取主机 IP_{S3} 的 root 权限，初始状态下，威胁主体仅仅与主机 IP_{S3} 的 80 端口可达，使用描述逻辑可以表示如下：

$\langle IP_{S3}, root\rangle$:hasGoal;
$\langle IPa, IP_{S1}, 80\rangle$:hasReach;

将 *NEO*、渗透目标以及初始条件输入 FaCT 系统进行推理分析，发现在满足渗透目标的前提下共有 21 条渗透路径，其中成功概率最大、渗透路径最短的有三条，它们分别为：$\{e_1, e_7\}$、$\{e_2, e_7\}$和$\{e_3, e_7\}$。进一步分析可以得出，存在三个最小渗透集合，它们分别为：$\{e_1, e_2, e_3\}$、$\{e_7, e_8, e_9\}$和$\{e_7, e_9, e_{10}\}$，如果修复三个最小渗透集合中的任何一个，则所有的渗透路径不可到达，确保目标系统安全。

5　相关研究工作

国内外相关研究主要集中于网络安全评估方法以及本体的应用研究。

网络安全评估方法有典型的四种方法：基于脆弱性扫描的安全风险分析、BS7799 [5]提供的方法和 OCTAVE 方法[7]、基于模型的安全评估方法。基于脆弱性扫描的安全风险分析是最早使用的一种方法，如 ISS security scanner、Nes-

sus、Retina network security scanner 等都是属于这种方法。基于模型的安全评估方法是当前研究的热点，主要包括 UML 评估方法[43]、攻击树评估方法[11]、攻击图评估方法[9,10,13]、渗透图评估方法[8]、Petri net 评估方法[44~46]、投入/产出模型评估方法[47]以及博弈论评估方法[48]。

描述逻辑是一种知识表示语言，它是一阶谓词逻辑的可判定子集，能够精确刻画语义、同时综合权衡了知识表达能力和推理效率，是知识表示领域研究的热点。文[38]详细介绍了描述逻辑的起源、理论基础、应用情况。描述逻辑的推理算法是 Tableau 算法[21~24]，目前实现了的最好的描述逻辑推理系统是 FaCT[25]系统和 RACER[26]系统。以描述逻辑为形式化基础建立了许多本体语言，如 OIL[37]、DAML＋OIL[37]和 OWL[33~37]等等，其中 OWL 是 W3C 提出的标准。

关于本体集成的研究有 OntoMapO 框架[39]、面向本体共享的 IFF 框架[40]、面向本体融合的 FCA-Merge 方法[41]、面向本体映射的 IF-Map 方法[42]等。这些本体集成方法有三大不足：没有严格区分本体和领域本体、没有采用标准的本体语言、没有考虑推理效率，这使得它们难以在网络安全评估这样大的分布式环境中发挥实际的功效。

结论和展望 本文所做工作的主要特色之处在于应用描述逻辑、本体语言等相关方面的研究成果，从建立网络安全评估工程中的知识基础设施、争取知识优势出发，以网络渗透本体作为网络安全评估工程的知识基础设施，总结了网络安全评估的通用框架，提出了一种网络渗透本体构建方法。具体实例分析表明 NEOCA 可用性较强，方法行之有效。通过分析国内外相关研究工作，进一步说明了本课题研究的广阔前景和独特之处。

由于本体语言 OWL LDL 表达能力的限制，所构建的网络渗透本体不可能涵盖网络安全评估的全部知识。但我们应该认识到，使用 OWL LDL 构建的网络渗透本体是面向机器的，可以由机器作自动处理的，由于网络渗透本体规模巨大且分布，人难以快速有效地对之进行处理，所以机器能够作自动处理对于争取安全评估知识优势和决策优势是相当重要的。对于无法使用 OWL LDL 刻画的知识，只能采用自然语言刻画之，并且只能主要由人来处理。为了能在实践中应用表达能力更强的本体语言(如 OWL DL、OWL Full 等等)，这需要对它们的推理算法的做进一步研究和优化。同时，如何更加准确地描述网络渗透原子以及更加完善丰富网络渗透本体也是下一步研究的重点。

参 考 文 献

1 毛捍东，陈锋，张维明．信息安全风险评估方法研究．见：中国信息协会信息安中国信息协会信息安全专业委员会年会文集，2004

2 Rowe W D. An Anatomy of Risk. New York: John Wiley and Sons, 1997

3 Ansell J, Wharton F. Risk: Analysis, Assessment, and Management. Chichester: John Wiley & Sons, 1992

4 SSE-CMM Model Description Document Version 2.0. 1999, http://www.sse-cmm.org

5 International Organization for Standardization. Code of Practice for Information Security Management. ISO/IEC 17799: 2000. December 2000

6 International Organization for Standardization. ISO/IEC TR 13335. Guidelines for the Management of IT Security (GMITS). 1996-2001

7 Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE) Framework 1.0 (CMU/SEI-99-TR-017), Alberts C J; Behrens S G; Pethia R D; et al. Pittsburgh, PA: *Software Engineering Institute, Carnegie Mellon University*, 1999

8 Li W, Vaughn R. An Approach to Model Network Exploitations Using Exploitation Graphs. In: Military, Government, and Aerospace Simulation Symposium: Proceedings of the 2005 Spring Simulation Multiconference (SMC'05), San Diego, California, April 2005, The Society for Modeling and Simulation International, 2005. 237～244

9 Sheyner O, Jha S, Wing J M, et al. Automated Generation and Analysis of Attack Graphs. In: 2002 IEEE Symposium on Security and Privacy. Oakland, California, 2002

10 Swiler L P, Phillips C, Gaylor T. A Graph-based Network-Vulnerability Analysis System: [Technical Report]. SAND97-3010/1. Sandia National Laboratories, Albuquerque, New Mexico and Livermore, California, 1998

11 Schneier B. Attack Trees. Dr Dobbs Journal, December, 1999

12 Ou Xinming, Boyer W F, McQueen M A. A Scalable Approach to Attack Graph Generation. In: Proceedings of the 13th ACM conference on Computer and communications security, 2006. 336～345

13 Jha S, Sheyner O, Wing J. Two Formal Analyses of Attack Graphs. In: Proceedings: 15th IEEE Computer Security Foundations Workshop (CSFW'15), Cape Breton, Nova Scotia, Canada, *IEEE Computer Society*, 2002. 49～63

14 Davies J, Fensel D, van Harmelen F. Towards the Semantic Web: Ontology-driven Knowledge Management [M]. England: John Wiley & Sons Ltd, 2003

15 Matheus C J, Kokar M M, Baclawski K. A Core Ontology for Situation Awareness [A]. In: Proc. eedings of Sixth International Conference on Information Fusion [C]. Cairns, Australia: IEEE, 2003. 545～552

16 Nilsson N J. Artificial Intelligence: A New Synthesis [M]. Beijing: China Machine Press & Morgan Kaufmann Publishers, 1999. 215～316.

17 Russell S, Norvig P. Artificial Intelligence: A Modern Approach [M]. Beijing: Pearson Education North Asia Limited and People's Posts & Telecommunications Press, 2002. 221～226

18 Gruber T B. A translation approach to portable ontologies [J]. Knowledge Acquisition, 1993, 5(2): 199～220

19 Gruber T B. Towards principles for the design of ontologies used for knowledge sharing [J]. International Journal of Human-Computer Studies, 1995. 907～928

20 Horrocks I, Patel-Schneider P F. Reducing OWL entailment to description logic satisfiability [A]. In: Proc. eedings of the 2003 International Semantic Web Conference [C]. Florida, USA: Springer, 2003. 17～29

21 Horrocks I, Sattler U, Tobies S. Practical reasoning for very expressive description logics [J]. Logic Journal of the IGPL, 2000, 8(3): 239～263

22 Horrocks I, Sattler U, Tobies S. Practical reasoning for expressive description logics [A]. In: Proc. eedings of the 6th International Conference on Logic for Programming and Automated Reasoning [C]. Tbilisi, Georgia: Springer, 1999. 161～180

23 Horrocks I, Sattler U. Ontology reasoning in the SHOQ(D) description logic [A]. In: Proc. eedings of the 17th Int Joint Conf on Artificial Intelligence [C]. Washington, USA: Morgan Kaufmann, 2001. 199～204

24 Horrocks I, Sattler U, Tobies S. Reasoning with individuals for the description logic SHIQ [A]. In: Procceedings of the 17th Int Conf on Automated Deduction [C]. Pittsburgh, USA: Springer, 2000. 482～496

25 Horrocks I. Using an expressive description logic: FaCT or fiction? [A]. In: Proc. eedings of the 6th Int Conf on Principles of Knowledge Representation and Reasoning [C]. Trento, Italy: Morgan Kaufmann, 1998. 636～647

26 Haarslev V, M¨oller R. RACER system description [A]. In: Proceedings of IJCAR2001 [C]. Siena, Italy: Springer, 2001.

701～705
27 徐振宁. 基于 ontology 的 Web 数据语义信息的表示与处理方法研究[D]:[博士学位论文]. 长沙: 国防科大, 2002
28 金芝. 知识工程中的本体论研究[A]. 见:世纪之交的知识工程与知识科学[C]. 北京: 清华大学出版社, 2001. 447～465
29 Guarino N. Formal Ontology and Information Systems [A]. In: Proceedings of the 1st International Conference on Formal Ontologies in Information Systems [C]. Trento, Italy: IOS Press, 1998. 3～15
30 Berners-Lee T. Weaving the Web [M]. San Francisco, USA: Harper, 1999
31 Berners-Lee T, Hendler J, Lassila O. The Semantic Web [EB]. http://www. scientificamerican. com/article. cfm? articleID = 00048144-10D2-1C70-84A9809EC588EF21&pageNumber = 1&catID=2, 2001
32 宋峻峰,等. OWL DL 的形式化基础研究[J]. 小型微型计算机系统(录用待发表)
33 McGuinness D L, van Harmelen F. OWL Web Ontology Language Overview [EB/S]. http://www. w3. org/TR/owl-features/, 2004
34 Smith M K, Welty C, McGuinness D L. OWL Web Ontology Language Guide [EB/S]. http://www. w3. org/TR/owl-guide/, 2004
35 Dean M, Schreiber G. OWL Web Ontology Language Reference [EB/S]. http://www. w3. org/TR/owl-ref/, 2004
36 Patel-Schneider P F, Hayes P, Horrocks I. OWL Web Ontology Language Semantics and Abstract Syntax [EB/S]. http://www. w3. org/TR/owl-semantics/, 2004
37 Horrocks I, Patel-Schneider P F, van Harmelen F. From SHIQ and RDF to OWL: The making of a web ontology language [J]. Journal of Web Semantics, 2003, 1(1):7～26
38 Baader F, McGuinness D, Nardi D, et al. The Description Logic Handbook: Theory, Implementation and Applications [M]. Cambridge, UK: Cambridge Univ Press, 2003. 1～100, 436～459
39 Kiryakov A, Simov K, Dimitrov M. OntoMap: Portal for Upper-Level Ontologies [A]. In: Proceedings of the 2nd International Conference on Formal Ontology in Information Systems (FOIS'01)[C]. Ogunquit, Maine, USA: ACM Press, 2001. 47～58
40 Kent R. The information flow foundation for conceptual knowledge organization [A]. In: Proceedings of 6th International Conference of the International Society for Knowledge Organization [C]. Toronto, Canada: International Society for Knowledge Organization, 2000. 111～117
41 Stumme G, Maedche A. Ontology Merging for Federated Ontologies on the Semantic Web [A]. In: Proceedings of the International Workshop for Foundations of Models for Information Integration (FMII-2001)[C]. Viterbo, Italy: FMLDO, 2001
42 Kalfoglou Y, Schorlemmer M. Information-Flow-based Ontology Mapping [A]. In: Proceedings of the 1st International Conference on Ontologies [C], Databases and Application of Semantics (ODBASE'02)[C]. Irvine, CA, USA: Springer, 2002. 1132～1151
43 Dimitrakos T, Bicarregui J, StØlen K. CORAS-a framework for risk analysis of security critical systems. ERCIM News, 2002 (49):25～26
44 Helmer G, Wong J, Slagell M, et al. Software Fault Tree and Colored Petri Net Based Specification, Design and Implementation of Agent-Based Intrusion Detection System. Requirements Engineering, 2000,7(4):207～220
45 McDermott J. Attack Net Penetration Testing. In:Proc. eedings: 2002 New Security Paradigms Workshop (NSPW'00), Cork, Ireland, ACM/SIGSAC, 2002. 15～21
46 Steffan J, Schumacher M. Collaborative Attack Modeling. In: Proceedings:2002 ACM Symposium on Applied Computing (SAC 2002), Madrid, Spain, ACM/SIGAPP, 2002. 253～259
47 Templeton S, Levitt K. A Requires/Provides Model for Computer Attacks. In: Proceedings of the 2000 Workshop on New Security Paradigms, New York: ACM Press, 2001
48 Alpcan T, Basar T. A Game Theoretic Approach to Decision and Analysis in Network Intrusion Detection. In: Proceedings: IEEE Conference on Decision and Control, Maui, Hawaii, IEEE Computer Society, 2003. 2595～2600

(上接第 77 页)

布式系统本身所存在的安全漏洞(2.2 节所述的问题),又保证了严重报警的及时传送以及后续的风险评估的实时性,在安全性与实时性之间取得了很好的平衡。DoS 报警虽为较严重的报警,但多以耗尽系统资源(例如带宽)为目标,本自适应的聚合方法恰好可以减少报警对系统带宽资源的占用,不会"放大"DoS 的攻击效果,从而可以较好地应对 DoS 攻击。

总结 本文所提出的报警聚合方法可以有效聚合重复报警,减轻重复报警所产生的网络通讯负担和对报警处理中心的压力,解决了重复报警所可能带来的重复响应等问题,能够在报警数量和报警种类之间取得很好的平衡。此外,和传统的基于手工设置固定滞留时间阈值的报警聚合方法相比,本聚合方法可以在系统运行过程中不断学习、修正聚合报警的滞留时间阈值,从而使聚合方法具有了自适应性,实现了报警聚合与后续深入报警处理的较好结合,解决了安全性与实时性之间的矛盾。

参 考 文 献

1 穆成坡, 黄厚宽, 田盛丰, 等. 基于模糊综合评判的入侵检测报警信息处理. 计算机研究与发展, 2005,42 (10):1679～1685
2 穆成坡, 黄厚宽, 田盛丰. 入侵检测系统报警信息聚合与关联技术的研究综述. 计算机研究与发展,2006,43(1):1～8
3 穆成坡. 自动入侵响应系统的研究:[博士论文]. 北京交通大学计算机与信息技术学院, 2006.06
4 Cuppens F, Toulouse O. Managing Alerts in a Multi-Intrusion Detection Environment. In:Proc. eeding of 17th Annual Computer Security Applications Conference (ACSAC), New-Orleans, December 2001
5 Cuppens F, Miege A. Alert Correlation in a Cooperative Intrusion Detection Framework. In:Proc. eedings of the IEEE Symposium on Security and Privacy, Oakland, CA, May 2002
6 Mu C P, Huang H K, Tian S F. Intrusion Detection Alert Verification Based on Multi-level Fuzzy Comprehensive Evaluation. In: Proceeding of 2005 International Conference on Computational Intelligence and Security, LNAI 3801, Springer-Verlag, Berline Germany, 2005. 9～16
7 Schnackenberg D, Holliday H, Smith R, et al. Cooperative Intrusion Traceback and Response Architecture. In:Proceeding of DARPA Information Survivability Conference and Exposition, 2001
8 Staniford S, Hoagland J A, McAlerney J M. Practical Automated Detection of Stealthy Portscans. Journal of Computer Security, 2002, 10(1-2)