基于CBR和描述逻辑的网络安全应急响应

蒋 菲 古天龙 徐周波 常 亮
(桂林电子科技大学 广西可信软件重点实验室 桂林 541004)

摘 要 网络安全应急响应是未来信息安全策略的重心。目前应急响应主要依靠应急响应团队和安全管理者,他们虽能够有效处理部分安全事件,但不能给出在具体环境下合理、快速、有效地处理安全事件的方法。针对该问题,提出了智能化的基于案例推理和描述逻辑的网络安全应急响应方法,用以实现对具体安全事件的自动处理。首先用描述逻辑刻画网络安全应急响应领域知识,然后设计了基于细化算子和细化图的相似度匹配算法,给出了基于案例的推理(Case based reasoning,CBR)在应急响应中的具体实现过程,最后用具体实例检验了提出的方法。结果表明该方法具有清晰语义、自动分类概念和良好推理能力等特性,能够从过去的安全事件中获得目前所遇到的安全事件的解决方案,并能够给出具体环境下安全事件的处理方法。

关键词 网络安全事件,基于案例的推理,描述逻辑,应急响应
中图法分类号 TP301,TP39 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.1.031

Network Security Emergency Response Based on CBR and Description Logic

JIANG Fei GU Tian-long XU Zhou-bo CHANG Liang
(Guangxi Key Laboratory of Trusted Software,Guilin University of Electronic Technology,Guilin 541004,China)

Abstract Network security emergency response is the focus of information security policy for future. The current emergency response mainly depends on the incident response team and safety manager,which can effectively deal with part of security incidents,but not give the reasonable,fast,effective processing method for security incidents under specific environment. To solve this problem,the paper proposed an intelligent method based on case based reasoning and description logic for network security emergency response,to handle specific security incidents automatically. First,we used description logic to describe domain knowledge of network security emergency response,and then designed a good matching algorithm of similarity based on refinement operator and refinement graph,gave the realization process of the CBR in emergency response,and finally used the specific examples to validate the proposed method in this paper. The results show that the method has the characteristics of clear semantics,automatic classification of concept and good reasoning ability,and can get the current problem solution from past security incidents,and is capable of giving the handling method of security incidents under specific environment.

Keywords Network security incident,Case based reasoning,Description logic,Emergency response

1 引言

随着虚拟化、云计算、大数据、BYOD、社交化等技术的发展,安全问题更加凸显,网络攻击方法越来越复杂,越来越有针对性,单纯的防御技术已经不能满足如今的需求,应与其他的安全服务结合,共同保障网络空间安全。网络安全应急响应是一种能够在网络安全事件发生的时候进行紧急援助、避免造成更大损失的服务,在保护企业、终端安全等方面有着积极的作用,也是未来信息安全策略的重心。近年来,CERT在反击大规模网络安全事件方面起了很大作用,许多学者和机构对应急响应方面也做了大量的研究,应急响应得到了很大的发展。如Mitropoulos[1]等人就已有的研究和应用给出了详细合理的安全事件处理系统框架和企业环境下的一类安全事件的应急响应处理方法。为了提供数据模型给应急响应组织进行事件、漏洞数据和信息交换,定义安全事件的特征,文献[2]提出用于信息共享的IODEF(事件对象描述和交换格式)标准。文献[3,4]给出了处理各种类型安全事件需考虑的因素,及其详细的步骤,并为部分安全事件提供检测和分析方法,为高效处理安全事件提供建议和指导。尽管如此,相关的大量文献都集中在安全事件的防御上,且对应急响应的研究也没落实到具体环境下安全事件的解决,只是给出一些大框架式的应对可能情况的措施,对于解决具体安全事件的作用

到稿日期:2014-01-23 返修日期:2014-04-21 本文受国家自然科学基金(60963010,60903079,61262030,61363030,61100025),广西自然科学基金(2012GXNSFBA053169)资助。

蒋 菲(1988-),女,硕士生,主要研究方向为知识表示与推理、形式化方法、CBR推理、网络安全,E-mail:jiangfei0128@sina.com;古天龙(1964-),男,博士,教授,博士生导师,CCF高级会员,主要研究方向为符号计算、形式化方法等;徐周波(1976-),女,博士,副教授,主要研究方向为符号计算、智能规划、约束满足问题求解等;常 亮(1980-),男,博士,教授,CCF高级会员,主要研究方向为知识表示与推理、智能规划、形式化方法等。

微小。目前网络安全事件的处理还是高度依靠应急响应专家团队和组织，但他们也存在很多的缺陷和限制：首先，面对层出不穷的安全事件，没有良好的训练和有能力的团队，事件的检测和分析的执行将是没有效率的，还会产生代价高昂的错误；其次，受具体事件背景和人力的资源的限制，很多团队不能够全盘认识具体的安全事件，也不可能对每一个安全事件都进行应急响应，往往只是就最新的漏洞、威胁或攻击提供最新的信息；最后，应急响应团队对大多数网络安全事件的事后剖析都集中在“高影响”事件（对社会或网络安全技术等有重大影响的技术）而不是“高学习”事件（即从学习的视角看潜在有用的能提高网络安全性的事件），而这些恰恰能够提高应急响应的整体水平[5-7]。

基于案例的推理（Case based reasoning，CBR）是一种试图模仿人类专家行为、从过去的案例中学习经验、探索利用过去的经验解决目前所遇到问题的推理算法，已经在很多的领域得到了应用。网络安全应急响应中涉及的新的各种类型的安全事件虽持续发生，但是这些事件总有相似的地方，相似事件对应的解决方案也会具有共同点，因而可以将 CBR 应用到网络安全事件的应急响应中，通过查找案例库中相似的安全事件案例，生成针对当前事件的应急预案，为具体安全事件的处理提供辅助决策和帮助[8]。此外，因为 CBR 还具有良好的学习功能，许多的经验会被保存下来为我们所利用，也就弥补了目前很多应急响应组织所面临的安全事件的学习只重“高影响”不重“高学习”的缺陷。

应急响应以一种有效的方式检测、分析和响应网络安全事件，尽管目前安全事件的处理高度依靠专家安全团队，一个自动处理安全事件的系统还是高度期望的[7,9]。为了实现自动处理这一过程，所有的信息首先必须能够识别、分类而被机器所使用。为了让机器自动理解网络安全应急响应方面的信息，首先需解决将信息表示为计算机能够理解和处理的形式即知识的表示问题。描述逻辑（Description Logic，DL）在众多知识表示的形式化方法中，具有清晰的语义特征，能够基于概念描述表示领域知识，可以以结构化和形式化的方式对应用领域的知识进行描述并提供有用的推理服务，事实上已成为知识表示的标准。此外，因为描述逻辑能够自动分类概念、识别实例和描述结构案例，对于 CBR 中案例的管理、案例的表示、案例的检索和案例的修正问题也都有相当的好处。考虑到以上 CBR 和描述逻辑的优势，本文设计了 DL-CBR 系统来解决网络安全应急响应问题，试图解决网络安全事件的自动响应问题，以有效地响应网络安全事件。本文的主要贡献有：创造性地提出将 CBR 和 DL 结合用于解决网络安全应急响应问题，事实证明其具有良好的效果，能够提供有效的安全事件的应急响应方法；利用 DL 描述了网络安全应急响应领域的知识，该方法比其他表示方法如属性值对、本体、基于对象的表示法等在知识的刻画方面更细致准确，能够刻画知识之间的内在联系，知识覆盖面更广；对 CBR 案例检索采用细化算子和细化图的方法计算相似度，使之更贴近目标问题，还用具体的事例证实了本文的优势所在。

本文第 2 节介绍基于案例推理的模型和描述逻辑，给出了描述逻辑引入 CBR 中的诸多优点；第 3 节介绍网络安全应急响应方法、过程及系统的框架；第 4、5 节结合描述逻辑将网络安全应急响应的知识进行了表示，构建了 DL-CBR 系统并引例说明所给定的方法；最后总结和讨论目前存在的问题和将来的工作。

2 预备知识

2.1 基于案例的推理（CBR）

基于案例的推理从认知科学发展而来，是一种知识管理机制和问题解决型范式，其基本思想是 similarity problems have similarity solutions，即相似的问题具有相似解。CBR 在对问题进行求解时，可以探索类似的历史问题的求解经验，获取知识并推理，将问题与历史的相似问题进行匹配和差异调整得到问题的解。CBR 适用于解决领域知识不完全、需要依赖丰富经验的问题，已经在医疗、法律、信息服务、规划及故障诊断等领域有广泛应用[10]。CBR 涉及的核心问题有：案例的表示、案例的检索、案例的修正和案例的存储。在文献[11]中作者将 CBR 分解成了 4 个阶段 4R：retrieve 检索、reuse 重用、revise 修正、retain 保存或存储，如图 1 所示。CBR 的基本工作过程可以简单地描述如下。

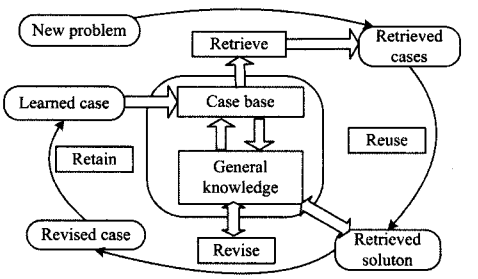

图 1 CBR 工作循环图

案例的表示：将包含在领域里的经验知识表示出来。通常可以分为问题和解决方案的描述，可能还有额外需要添加的知识要描述，这取决于知识利用的意图，例如，也有人将问题的目标、结果、教训等列入案例表示中。案例的表示与案例的检索有很大的依赖性，不同的表示法需要不同的相似性度量方法来检索。

案例的检索：检索出与目标问题相似的案例。检索的任务开始于（部分）问题的描述，最终得到与目标案例匹配的最好的先前的历史案例。在 CBR 中，检索是基于相似度的匹配，检索得到相似案例的效果完全取决于相似度计算方法，相似的案例会影响之后案例的重用和修改，相似案例效果好的可以直接减少重用和修改的工作量，因而相似度对于整个 CBR 过程而言是相当重要的。

案例的重用：直接或间接地将检索得到的源案例应用到当前问题中，得到初始解决方案。

案例的修正：修改生成的案例的解决方案，最终得到合理的问题的解决方案。评估生成的案例的解决方案被重用之后是否成功，如果成功，从案例中学习经验并选择性保存案例；否则，当源案例与目标案例出现矛盾，案例的重用不成功，需要对它们之间的差异进行调整和修正，重复重用和修正的过程，直到重用成功。如果重用多个回合还是不能满足要求，就修改问题的检索条件进行检索，再重复重用、修改的过程，最终得到问题合适的解决方案。

案例的保存：对新的有用的案例进行保存，使 CBR 系统积累更多经验和知识。

2.2 描述逻辑

描述逻辑事实上在许多应用领域已经成为了一种知识表

示的标准。20 世纪 90 年代，描述逻辑由于在知识获取、表示和 CBR 研究中具有诸多优点，因此被引入 CBR 中成为知识密集型案例推理系统的技术选择。将描述逻辑引入 CBR 的优势主要有：描述逻辑表示案例具有清晰的语义，让人容易理解；在 CBR 中，DL 使索引的过程自动进行，具体来说就是 DL 允许概念的自动分类，概念的自动分类逐渐地促进了概念分层；描述逻辑具有很强的表达能力和可判定性，并具有良好的推理能力，它能保证推理算法停止并返回正确的结果，还能够从显式表示的知识中推导出隐含的知识，而这将有利于提高案例检索的准确性和完备性[12,13]。

描述逻辑有着多种不同的形式，拥有着不同的表达能力和推理复杂度，这些很大程度上都是依赖于语言上可利用概念构造算子的构造程度。考虑到不同描述逻辑的表达能力、推理复杂度以及对网络安全应急响应领域知识的良好刻画，在本文中使用了描述逻辑 $ALCO(D)$ 来表示网络安全应急响应领域的可能知识和概念。下面简要介绍 $ALCO(D)$。

对 ALC 进行不同的扩展，加入将个体名整合成一个集合的概念的枚举算子 O 和包含如数值、字符串、时间等这类有型对象的有型域算子 D 可以得到 $ALCO(D)$。

设 A 为原子概念，N_C 为 $ALCO(D)$ 概念名集合，N_R 为角色名集合，N_f 为特征式集合，N_R 和 N_f 彼此不相交，概念名 $C_1, C_2 \in N_C$，角色名 $R \in N_R$，枚举个体为 O；$ALCO(D)$ 的角色集合是 $N_R \cup N_f$，特征式 $f_1 \cdots f_n$ 合成特征链，$u_1, u_2, \cdots, u_n$ 是特征链（n 表示整数）；有型域 D 是一个二元组 $(\Delta^D, pred(D))$，其中 Δ^D 为有型论域，$pred(D)$ 为谓词集合，任意 n 元谓词 $P \in pred(D)$ 是论域上的 n 元关系，即：$P^D \subseteq (\Delta^D)^n$，则 $ALCO(D)$ 的概念可以由如下产生式生成：

$$C_1, C_2 ::= A \mid \top \mid \bot \mid \neg C_1 \mid C_1 \sqcap C_2 \mid C_1 \sqcup C_2 \mid \exists R.C_1 \mid \forall R.C_1 \mid \{O\} \mid \exists u_1 \cdots u_n.P \mid \forall u_1 \cdots u_n.P$$

$ALCO(D)$ 的解释 $I=(\Delta^D, \Delta^D \cdot {}^I)$ 是一个向量，其中 Δ^I 是非空集合的解释域，Δ^D 是有型论域，$\cdot^I$ 是解释函数，集合 Δ^D 与 Δ^I 不相交。解释函数 $\cdot^I$ 将每个概念解释为 Δ^I 的一个子集，将每个角色映射为 $\Delta^I \times \Delta^I$ 上的一个二元关系，将每个特征式映射为 $\Delta^I \times \Delta^D$ 的一个子集。$ALCO(D)$ 的概念和公式满足的语义如下：

$A^I \in \Delta^I$

$\bot^I \in \phi$

$\neg C_1 = \Delta^I / C_1^I$

$(C_1 \sqcup C_2) = C_1^I \cup C_2^I$

$(C_1 \sqcap C_2) = C_1^I \cap C_2^I$

$(\exists R.C_1)^I = \{x \in \Delta^I \mid \exists y, (x,y) \in R^I \wedge y \in C_1^I\}$

$(\forall R.C_1)^I = \{x \in \Delta^I \mid \forall y, (x,y) \in R^I \rightarrow y \in C_1^I\}$

$\{O\}^I = \{O^I\} = \{O\}$

$(\exists u_1, \cdots, u_n.P)^I = \{x \in \Delta^I \mid \exists a_1, \cdots, a_n \in \Delta^D, (x,a_1) \in u_1^I \wedge \cdots \wedge (x,a_n) \in u_n^I \wedge (a_1, \cdots, a_n) \in P^D\}$

$(\forall u_1, \cdots, u_n.P)^I = \{x \in \Delta^I \mid \exists a_1, \cdots, a_n \in \Delta^D, (x,a_1) \in u_1^I \wedge \cdots \wedge (x,a_n) \in u_n^I \rightarrow (a_1, \cdots, a_n) \in P^D$

一个 $ALCO(D)$ 的知识库 KB（Knowledge Base，KB），$K=(T,A)$，包含两种不同类型的信息 TBox 和 ABox。其中 TBox（Terminological Box）为术语部分，包含领域原子概念、角色及描述领域的词汇，包含描述知识库基本框架的最基本的推理操作包含关系。包含关系引导了子概念和上层概念的分层，如知识库 KB 中有 C 和 D 两个概念，概念 C 包含于概念 D（C 是比 D 更具体的概念）可以记为 $C \sqsubseteq D$，当且仅当对所有的解释 I 都有 $C^I \sqsubseteq D^I$ 成立。概念 C, D 是等价的当且仅当 C, D 互包含 $C \sqsubseteq D, D \sqsubseteq C$，记为 $C \equiv D$；ABox（Aassertional Box）为断言部分，包含使用领域的词汇断言有关个体的事实，即个体的实例断言和关系断言，如对于一个解释 I，称个体 x（$x \in \Delta^I$）是概念 C 的实例，当且仅当 $x \in C^I$。

3 基于 CBR 和 DL 的网络安全应急响应系统框架

网络安全应急响应可以分为应急的准备、检测和分析，抑制、根除和恢复以及应急后的事件剖析等几个阶段。不同的组织如 FIRST、CERT/CC[3]、APCERT 及不同的文献[3-9,14]对于列举的这些步骤可能会有不同，然而不管步骤是怎样，它们都包含相同的成分和相同的目标去有效地响应安全事件。如图 2 的系统框架图中安全事件应急响应部分显示了应急响应的各个不同的阶段，下面开始更深层地描述这些阶段。

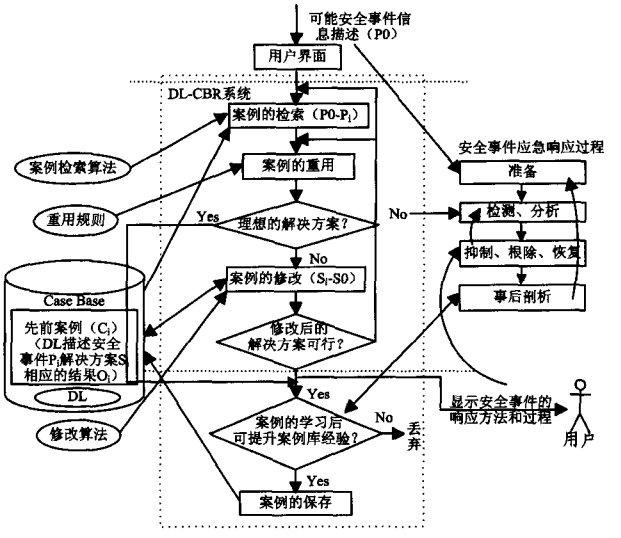

图 2 系统的总体运行图

准备阶段：包含使组织具有能够进行应急响应的能力和为预防安全事件确保系统、网络、应用安全而做的准备。这一阶段主要是准备在响应的过程中可能需要的一些通讯设备，以及检测和分析事件用的软硬件工具和资源。这些工具和资源包括备份的存储介质、加密和解密软件、安全补丁、联系信息等。

检测和分析阶段：证实事件是否为安全事件和对安全事件进行全面分析。很明显，如果不是安全事件，就无需进行应急响应。事件的检测有几种共同的方法识别潜在的事件：入侵检测和预防系统发送预警；杀毒软件显示恶意软件被检测；当具体事件发生时，许多自动工具频繁扫描审计日志和发送预警和警告；终端用户报告他们的问题，如他们不能访问网络上的资源。当然接收到这些信息并不意味着潜在的安全事件已经发生，入侵检测防御系统经常会给出错误的预警，而中断用户倾向于简单的用户的出错，因此需要调查分析决定它们是否是安全事件。当被确定为安全事件后，还需结合安全事件未来潜在的影响和受影响资源的重要性，决定事件响应的顺序，制定策略，对于重要资源和可能造成重大影响的事件进行优先处理。

抑制、根除和恢复阶段：抑制和减少安全事件的影响和危

害，完全将事件根除，使系统返回正常状态。一个有效的应急响应的最初的目标是限制事件的影响范围。抑制，很重要的一部分是做决策（例如，关闭某个服务或系统、不连接有线或无线网络、修改防火墙规则和路由器的过滤规则等）。事件的抑制策略措施会根据事件的类型、事件处于的环境有所不同，同时在处理有些事件和制定策略时需权衡可能存在的风险。在事件被抑制以后，接下来需要进一步地根除，根除事件的组件，如删除恶意代码和使用户的账户不能用等。对恶意代码或行为进行分析，找出事件根源，明确相应的补救措施并彻底清除。当然也可以在事件被抑制之后，在能够识别真正攻击者的情况下，向攻击者发动攻击。有些事件可能需要调查，需要追究一些法律责任，需保存保护必要的证据，恢复受影响的系统和网络设备至正常的状态，加固系统，防止类似的事件再次发生。一般应急响应的恢复涉及恢复系统、数据、程序和服务。恢复过程会因不同的组织机构而异，不同组织对于受侵害的系统的不同可信度要求，需要不同级别的担保。另外，不同的操作系统恢复过程必然有所不同。恢复系统，根据需要重新安装受感染的系统，在重装系统之前保存数据，使用户改变密码。如果有口令被嗅探，需根据攻击者获得的访问权限，要求不同级别的密码进行更改。如果是攻击者获得了超级用户的访问权限，那么需要一次性完整地强制性地修改所有密码。确保防病毒保护和入侵检测运行，确保系统的补丁被完全安装好，加固网络的外围设备安全；最后要去掉在短期的抑制过程中的中间防御措施。

事后剖析阶段：回顾事件和响应的整个过程，更新安全政策，加强防护，提高进一步的响应。主要考察此次应急响应是否合适，是否有需要改进的地方，应急响应的过程是否详细，是否覆盖了所有的情况。如何修改、改变可以阻止新的、类似的事情再次发生，安全政策是否需要更新。检查威胁造成的结果，评估事件带来的影响和损失，总结应急响应过程中可以学到的经验教训。

结合应急响应过程、CBR 和 DL，本文设计了一种智能的网络安全应急响应系统。该应急响应系统主要包含 2 个部分：一个是应急响应部分，另一个是 DL-CBR 部分，应急响应部分和 DL-CBR 部分相互作用解决应急响应问题。本文应用描述逻辑 $ALCO(D)$ 对应急响应领域知识进行了知识表示，模拟和建立了案例库，设计了相应的检索算法，执行了相应的基于案例的推理步骤，并用具体的实例阐述了其过程。图 2 显示了系统的总体运行过程。

当用户意识到自己可能遇到了安全事件，即可根据预先设定的用户界面选项，搜集尽可能多的关于安全事件的有用信息，将自己所遇到的安全情况（如事件发生的时间、受影响的资源、存在的现象等信息）填写到用户界面，系统结合输入的安全事件信息，调用应急响应事件库中的相关数据，将案例表示出来形成对当前所遇到事件的问题/事件的描述 P_0，同时应急响应过程也进入了安全事件的准备阶段，了解了事件的大致情况，做了一些必要工具和资源的准备。接着问题 P_0 就被送入 DL-CBR 循环的检索模块，系统根据设定的检索算法从案例库中检索、搜索先前问题的描述与目前问题最相似的问题描述 P_i，同时检索得到问题描述的解决方案 S_i 被作为起始点生成新问题的解 S_0。重用解决方案 S_i 生成新问题的解 S_0，评估解决方案的可行性。如果可行，那么就交给用户，用户遵循所给的解决方案处理安全事件。如果方案是不可行的，则还需要对解决方案进行修改，然后重复重用和修改的过程，直到最终生成合理的解决方案提供给用户。有时由于设置查询的问题信息不完整、与事实有偏离，还需添加或修改问题信息，而后重复案例的检索、重用、修改过程，直到最终生成合理的解决方案。$P_0-P_i-S_i-S_0$ 过程因为涉及到对事件的不断检测和分析也即为应急响应的检测和分析阶段。用户得到了合理的应急响应解决方案，就可执行相应的应急响应的抑制、根除和恢复过程，用户事后对事件剖析，选择性地保存案例，即完成了整个安全事件响应过程。

本文的系统是一个智能系统，将应急响应过程与 DL-CBR 系统一起融合能有效地解决网络安全事件。该系统在基本了解用户所面对的安全事件后，能智能地给出相应的解决方案，而该解决方案能够给应急响应决策者提供好的响应策略，减少了响应者响应安全事件的时间和错误率。

4 网络安全应急响应知识的表示

一个案例可以用一个三元组来表示，$CA=(P,S,O)$。其中，P(Problem)：用于描述网络安全事件发生的情况及问题；S(Solution)：描述对发生的安全事件(P)需采用的相应的响应方法或解决方案；O(Outcome)：说明对已发生的事件(P)采用相应的解决方案或响应方法(S)后所取得的效果。相应地，对于给定的案例库 CB(Case Base)，一个案例 CA_i 的 P_i，S_i，O_i 相应地表示问题的描述、解决方案和结果，所以 $CA_i \in CB, 0 \leqslant i \leqslant n$，$n$ 是案例库 CB 中案例的数量。

关于案例的表示形式，目前已经提出了许多种，主要可以分为 3 种：特征向量表示法、结构化表示法以及文本表示法。此外，针对专门的应用已经使用了一些特别的案例表示方法，如在设计和规划中，特征向量表示法采用的是属性-值对向量的方式表示案例，不能描述案例的内部结构；结构化表示方法可以描述案例的内部结构，主要包括基于框架的和基于对象的案例表示法。基于框架的表示法部分已经被描述逻辑形式化，领域知识可以利用分类分层整合；基于对象的表示方法类似于框架表示法，充分利用了面向对象的数据模型方法，如 is-a、part-of 关系、继承原则，将案例表示为对象的集合，将对象描述为属性-值对。文本表示法利用很弱的结构性对案例进行表示，这样容易捕获如故障报告或 FAQ 文本中的经验。案例的表示和相似性评估方法在检索时彼此密切相关，基于距离的相似性度量很容易应用于特征向量表示法中，与信息检索相关的技术就可以很容易地应用于文本表示法的案例表示中，而基于框架的案例表示通常需要密集型知识索引和匹配算法[15]。

网络安全应急响应是一个知识密集型的领域，对该领域知识的描述和表示，本文分别采用了结构化表示法中的描述逻辑刻画安全事件发生的情况（问题）和结果，而对于解决方案的描述则采用了文本形式。

安全事件的发生情况或问题(P)描述。一个事件的发生一般会涉及到事件的发生时间、地点、实施者、承受者、状态、事件造成的影响等信息，网络安全事件也不例外，如图 3 所示，对于安全事件的描述，也需描述安全事件的类型、事件发生和持续的时间、事件发生所在的组织机构、事件发生涉及的可能的攻击者信息、事件中受影响的资源及信息、事件造成的

影响、事件进行的状态及已采取的解决安全事件的措施。

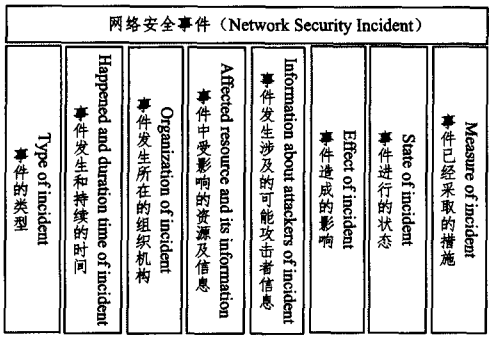

图 3　安全事件的组成部分

网络安全事件的类型(Type)。网络安全事件的种类、发生方式很多,且层出不穷,根据文献[3,4]可以把网络安全事件分为以下几类:恶意代码事件、拒绝服务攻击事件、未授权访问事件、不当使用事件及它们之间的组合引发的复合型事件。对于已发生的安全事件,为确定最适当的响应策略,首先需考虑安全事件的性质和类型,例如对资源的破坏、未授权使用、拒绝服务等;不同的攻击类型对应于不同的响应策略[16]。拒绝服务攻击由于不涉及实际的入侵,因此是一些最容易响应且最难预防的安全事件。对资源的未授权使用通常是内部人以不适当的方式使用自己的计算机,因此响应时更多地考虑内部因素。

图 4、图 5 分别表示了部分的不同种类安全事件的层次关系和一些预定义的概念。图 4 对事件的类型进行了划分,图 5 中,TBox 包含了预先定义的概念,定义了病毒、蠕虫、DDoS 型事件之间的层次关系,以及病毒、蠕虫型事件的概念,如病毒型事件是一种存在程序能够自我复制、能通过传播媒介(如:局域网、可移动设备)传播且需要触发条件传播的事件等。在 ABox 中包含了描述个体的概念和原子概念。

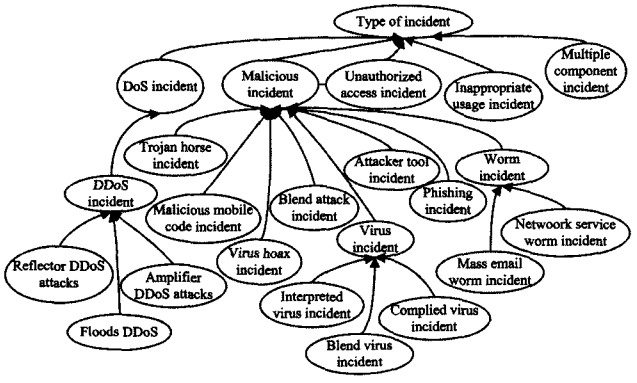

图 4　安全事件类型层次关系图

TBox

Virus incident ⊒0 Complied virus incident ⊔ Interpreted virus incident ⊔ Blend virus incident

Blend virus incident = Complied virus incident ⊓ Interpreted virus incident

Compiled virus incident ⊒File infector virus incident ⊔ Boot sector virus incident ⊔ Multipartite virus incident

Worm incident ⊒Network service worm incident ⊔ Mass email worm incident

Virus incident == ∃ Program. (Self－replicate ⊓ ∃ has transmission method. Transmission method)

…

ABox

Virus incident (p1), Complied virus incident (p2), Network service worm incident(t1), has transmission method(p1, m1)

图 5　安全事件类型预定义概念

事件发生和持续的时间(Time):由于技术的进步,安全事件被设计实现的功能越来越强大,事件覆盖的范围和领域也越来越广,产生的效果也越来越复杂。每当一种新的安全事件出现后,通常此类安全事件的防御水平都会有所提高,那么旧的方式引发的安全事件在未来新的环境下可能是没有效果的。考虑时间的因素,可以使我们关联到最近的安全事件,方便更好地找出与发生事件更相近相似的事件。另外,在进行应急响应时,安全事件持续的时间越久,事件造成的影响范围也越广,存在的可能危险也就越大,那么进行响应的事件也越紧迫。

事件发生所在的组织机构(Organization):事件发生在不同的机构部门,则个人普通主机的处理方式和侧重点是不同的。如商业机构和政府部门的安全事件处理方式就会不同,响应金融机构的安全事件时要考虑商业的连续性和金钱损失,而响应政府部门的安全事件更多考虑造成的名誉和机密数据的损失。所以,为了进行良好的响应,本文考虑了事件发生的组织机构,可能的组织机构有政府机关、商业机构、军事机构、医疗机构、科研教育机构、网络服务机构、互联网企业和组织等。

可能的攻击者的信息(Information about attackers of incident):如攻击者的 IP 地址,可能使用的攻击通信协议、端口等,这些信息有助于应急响应,如追踪攻击者,关闭被攻击的通道来阻止攻击。

事件中受影响的资源及其信息(Affected resource and its information):事件中受影响的不同资源(防火墙、Web 服务器、网络连接、用户工作站和应用等)对一个组织或个人来说有着不同的意义。根据不同资源的不同关键作用,处理事件的优先级将是不同的,重要的资源和潜在的具有重大技术影响的事件要最先处理。这些资源及其信息包括受害主机、连接的网络和网络服务、网络设备及其信息。其中,受害主机的信息包括主机的功能作用、主机的数量、操作系统类型、被攻击主机系统、安全工具、应用、服务、硬件存在被攻击异常情况和现象。主机的功能包括作为客户机还是服务器;被侵害的操作系统的类型包括 windows、linux、android 等;被攻击主机系统、安全工具、应用、服务、硬件存在被攻击及其异常信息和现象,其中安全工具为诸如杀毒软件、基于主机和网络的 IDPS(入侵检测防御系统)、反垃圾邮件软件、反间谍软件等保护计算机的安全防卫工具。被攻击时不正常现象,如:杀毒软件检测到并预警主机感染了蠕虫病毒,某种应用多次登录失败并来自一个不熟悉的远程登录系统,主机系统突然变慢,弹出可疑内容的邮件或窗口,来自操作系统、服务或应用的审计记录的日志发现攻击记录等。连接的网络和网络服务信息包括网络不能连接,只能连接特定的网址,网络的流量异常等;网络设备的信息如路由器、交换机等的运行异常信息。

事件造成的影响(Effect):主要考虑安全事件对受害者造成的影响,包括:金钱的损失、名誉的损害、数据的丢失、敏感资料的泄露,客户信息的泄露、信息的破坏、资源盗用等。

事件进行的状态(State):事件发生的状态不同,采取的响应措施也不同,有些攻击会有一些征兆,这时事件可能还没发生,我们进行的响应就是预防阻止事件的发生。有些事件可能已经在不知情的情况下发生了,那么组织或个人就要快速缓解风险和事件带来的影响,将安全事件解决,使系统恢复正常的状态。

已采取的解决安全事件的措施(Measure):在遇到安全事件之后,可能已经采取了一些措施响应安全事件,比如不连接网络、关闭了受病毒感染的主机等,考虑这些是因为已采取的措施会对事件的处理产生影响。

具备刻画网络安全事件必备的要素之后,就可以使用经 $ALCO(D)$ 刻画后的知识库中的一些预定义概念对事件进行刻画。根据上文提到的知识,部分网络安全事件(P)预定义的概念如图 6 所示。

A incident = ∃ has type of incident. Type of incident ⊓ ∃ has happened time of incident. = h year ⊓ ∃ has duration time of incident. = f hour ⊓ ∃ has organization of incident. Organization ⊓ ∃ has information about attackers of incident. Information about attacker ⊓ ∃ has affected resource of incident. Affected resource ⊓ ∃ has state of incident. State of incident ⊓ ∃ has effect of incident. Effect of incident ⊓ ∃ has taken measure of incident. Measure of incident

Organization ⊒ (Commercial organization ⊔ Government ⊔ Education ⊔ Network service provider ⊔ military establishment)

Effect of Incident ⊒ {money loss, fame compromise, important data lost}

State of incident ⊒ {finished, ongoing, unhappened, unknown}

Measure of incident ⊒ {close the affected host, disconnected network}

Information about attacker ⊒ {attacker'IP address, attacker'port number, attacker'used protocol}

Affected resource ⊒ (Affected host ⊔ Affected network ⊔ Affected network device).

Affected host ⊒ (∃ has type of host OS. Type of host OS ⊓ ∃ has host function. Host function ⊓ ∃ has host number. = m tai ⊓ ∃ has abnormal sign. (System of host ⊔ Application of host ⊔ Hardware of host))

Type of host OS ⊒ windows ⊔ linux ⊔ unix ⊔ android ⊔ ios

Host function ⊒ (client ⊔ server)

Server ⊒ (FTP server ⊔ Web server ⊔ Data server ⊔ Mail server)

System of host ⊒ System service of host

Application of host ⊒ Security tool of host

System of host ⊒ ∃ has abnormal sign. System sign of host

Hardware of host ⊒ ∃ has abnormal sign. Hardware sign of host

System sign of host ⊒ {system instability、system crash}

Hardware sign of host ⊒ {keyboard unavailable, loudspeaker with strange sound}

(其中 h, f, m 均为自然数)

图 6 预定义的概念

安全事件解决方案(S)的描述。描述了应对具体安全事件进行应急响应的全过程,包括针应急响应前的准备,应急响应过程中对安全事件的检测、分析、制约、根除、恢复,响应后的事件的剖析和后期维护(详细可见本文的第 3 节,应急响应的过程)。这部分的描述主要采用了文本的形式。

处理安全事件所取得的结果(O)描述。这里的结果可以是好的结果,也可以是坏的结果。好的结果,说明解决方案良好,可以采纳;坏的结果,说明解决方案不合适,用于吸取教训。这部分的描述也采用了描述逻辑 $ALCO(D)$ 描述。

网络安全事件应急响应的案例 CA_i 的具体表示,用一个案例说明如下:

2010 年极虎病毒感染某商业机构,该病毒类似于 Qvod 播放器图标,能够利用 IE 极光 0day 漏洞、网页挂马、局域网弱口令、移动设备传播,感染 Win XP、Win 7 系统客户机 20 台。中毒后,杀毒软件失效,系统明显变慢,CPU 占用极高,频繁读写磁盘,硬盘灯狂闪;exe 文件被感染,IE 主页异常,进程中莫名出现 rar. exe 和 ping. exe 且无法结束。网络连接和网络设备运行正常。该事件造成该组织商业运作变慢,部分业务搁置和间接经济损失。

安全事件的问题描述(P_i):

Tiger virus incident = ∃ has type of incident. (∃ Program. (Self-Replicate ⊓ Self-propagation ⊓ ∃ has transmission method. (LAN weak password ⊔ mobile memory media ⊔ web Trojan ⊔ {affected exe file}) ⊓ {IE Aurora 0day vulnerability}) ⊓ ∃ has happened time of incident. = 2010 year ⊓ ∃ has organization of incident. Commercial organization ⊓ ∃ has affected resource of incident. (∃ has type of host OS. ({win7} ⊔ {win xp}) ⊓ ∃ has host number. = 20 tai ⊓ ∃ has function of host. Client ⊓ ∃ has abnormal sign. ({antivirus software with virus warn} ⊓ {antivirus software unavailable} ⊓ {CPU usage high} ⊓ {exe file infected} ⊓ {system slowdown} ⊓ {hard disk light blink fast} ⊓ {IE abnormal} ⊓ {process rar. exe and ping. exe cannot close})) ⊓ ∃ has state of incident. {ongoing} ⊓ ∃ has effect of incident. {money loss}.

解决方案(S_i):

对尚未感染的主机,禁止使用连接过受感染主机的可移动介质;使用漏洞扫描工具,检查主机是否有 IE 极光零日漏洞,如果有漏洞,则从 windows 操作系统供应商的官网下载安全补丁,将漏洞修补;将重要文件备份到安全的可移动介质;检查杀毒软件,升级更新杀毒软件病毒库标志,合理地配置杀毒软件,开启实时监控防护;提高安全意识,不再点击具有可疑恶意代码的网站。

将受感染的 20 台主机从局域网等网络上隔离出来;将重要的文件备份到安全空白移动介质;重新启动主机,将旧的杀毒软件卸载,安装最新的其他杀毒软件,全面查杀系统;如果主机查杀成功,检查异常现象消失后,确保系统安全再正常使用。如果查杀不成功,将准备好的 Win XP 和 Win 7 系统安装盘,重装系统。重装后安装主流正版的杀毒软件,并及时升级;全面查杀整个磁盘,查找可疑的文件,待异常现象完全消失后,确保主机的安全后再接入网络,正常使用。

类似事件的安全防范:安装主流杀毒软件,及时更新病毒库并打开监护防护;及时更新软件,安装漏洞等安全补丁;将机器上重要的文件备份到移动存储硬盘内;不使用诱人的软件,尽量到官网下载软件。不点击不良的网站,健康上网。

事件的结果(O_i):∃ has outcome of incident response. {success}

从上可以看出,描述逻辑具有强大的描述能力,在刻画网络安全事件时,具有清晰的语义,能够刻画案例的内部结构,可刻画更多、更全面的知识,能够更有力地贴近人的思维和表达模式,这是其他的表示法如属性-值对、单一对象的特征描

述所不能企及的，而这些对以后案例的检索和修改也是非常有效的。

5 网络安全事件 DL-CBR 系统

5.1 网络安全事件案例的检索

当新的网络安全事件出现，DL-CBR 系统从案例库中检索相似的安全事件案例。案例的检索是 CBR 设计中的一个关键阶段，也是 CBR 系统的重要部分。在案例的检索中，相似度通常都被使用，相似度越接近于 1 说明案例间的相似程度越高。案例检索的质量直接影响得到的案例的相关度，影响到是否能够产生合适问题的解决方案。关于案例相似度的计算，根据不同的应用，不同的案例表示有许多不同的度量方法。Cunningham[17]概括性地给出了 CBR 领域的不同应用和表示的主流相似性度量方法。Sánchez-Ruiz 等人[18,19]先后提出了基于概念空间和基于合取查询空间的描述逻辑概念、个体之间相似性度量方法。Amailef 等人[20]利用本体构造案例库中案例的属性方便信息的抽取，根据灾难应急领域案例的不同属性的特点如数值型、区间型、字符型将它们分割，分别给出了它们不同的相似性度量方法。

在前人的基础上，本文使用描述逻辑 $ALCO(D)$ 表示了案例，本节将进一步给出一种基于细化算子和细化图的案例间的相似性度量方法来度量网络安全事件之间的相似性。现简要介绍细化算子和文中涉及的相关概念(在文献[21,22]可以对细化算子进行更进一步的了解)。细化算子可以由拟序集进行定义。拟序集是$(S,\leqslant)$对，S 是一个集合，$\leqslant$是 S 中的元素之间的二元关系，S 具有自反性和可传递性。如果 $a\leqslant b$ 且 $b\leqslant a$，那么 $a\approx b$，即 a 和 b 等价。细化算子的定义如下：向下细化算子 ρ 是一个关于拟序集$(S,\leqslant)$的函数，$\forall a\in S$：$\rho(a)\subseteq\{b\in S\mid b\leqslant a\}$；向上细化算子 γ 是一个关于拟序集$(S,\leqslant)$的函数，$\forall a\in S$；$\gamma(a)\subseteq\{b\in S\mid a\leqslant b\}$。向下细化算子通常生成更“小”的 S 中的元素(在本文中意味着更具体的含义)，相反地，向上细化算子意味着生成更“大”的元素(在本文中即为更普遍的含义)。通常需要考虑算子的下列特性：

—细化算子是局部有限的，如果 $\forall a\in S$；$\rho(a)$是有限的；

—向下细化算子 ρ 是完备的，如果 $\forall a,b\in S\mid a\leqslant b$；$a\in\rho^*(b)$；

—向上细化算子 γ 是完备的，如果 $\forall a,b\in S\mid a\leqslant b$；$b\in\gamma^*(a)$；

—细化算子是合理的，当 $\forall a,b\in S\mid$；$b\in\rho(a)\Rightarrow a\not\approx b$。

这里 ρ^* 表示细化算子的传递闭包。直观上看，局部有限意味着细化算子是可计算的；完备性意味着我们可以通过细化 a 和有序关系$\leqslant$生成与给定 a 元素相关的 S 中的任意元素(除了那些可能与 a 相等的)；合理性意味着细化算子不可能与存在经过细化 a 元素后还与给定元素 a 相等的情况。

最小公共包含(Least Common Subsumer，LCS)给定概念 $C_1,\cdots,C_n$ 集合的最小公共包含是另一个概念 $C=LCS(C_1,\cdots,C_n)$，则有 $\forall_{i=1,\cdots,n}\ C_i\sqsubseteq C$ 对其他任意的概念 C' 存在 $\forall_{i=1,\cdots,n}\ C_i\sqsubseteq C'$，则 $C\sqsubseteq C'$ 成立。

对于网络安全事件案例的相似度量，我们假设案例 CA_1，CA_2 的问题描述部分分别为 $P_1\equiv C_1\sqcap C_2\sqcap\cdots\sqcap C_n$，$P_2\equiv D_1\sqcap D_2\sqcap\cdots\sqcap D_m$，其中 $C_i,D_j(i=1,\cdots,n;j=1,\cdots,m)$均为 $ALCO(D)$范式。于是案例 CA_1，CA_2 的相似性被定义为：

$$\mathrm{Sim}(CA_1,CA_2)=\alpha\cdot\mathrm{sim}_\rho(p_1,p_2)+(1-\alpha)\cdot\mathrm{sim}_c(con_F(C_i,D_j))(0\leqslant\alpha\leqslant1)\quad(1)$$

式中

$$\mathrm{sim}_\rho(p_1,p_2)=\frac{\lambda_1}{\lambda_1+\lambda_2+\lambda_3}\quad(2)$$

$$\lambda_1=\lambda(\top\xrightarrow{\rho}LCS(P_1,P_2))\quad(3)$$

$$\lambda_2=\lambda(LCS(P_1,P_2)\xrightarrow{\rho}C)\quad(4)$$

$$\lambda_3=\lambda(LCS(P_1,P_2)\xrightarrow{\rho}D)\quad(5)$$

由于案例中安全事件的问题表示部分 P 本质上就是概念的描述，式(2)计算出两个案例之间整体相似性 sim_ρ 部分，主要基于以下原理：首先，给定两个概念 C 和 D，$C\sqsubseteq D$，通过应用向下细化算子 ρ 有限次的细化 D 是可能到达 C 的，即 $C\in\rho^*(D)$。其次，细化算子应用到从 D 到达 C 的细化次数表明概念 C 比概念 D 更具体，换句话说，即为从 C 到达 D 的细化链的长度，可以记为 $\lambda(D\xrightarrow{\rho}C)$，也表明 C 中包含多少信息是 D 所没有包含的，也暗示了它们的相似性，长度越短，相似的程度越高。此外，$\lambda(\top\xrightarrow{\rho}C)$也测量着最具体概念$\top$到达 C 的距离和 C 中所包含的信息量。再者，给定两个概念，它们的最小公共包含是包含这两个概念的最具体概念。两个概念的 LCS 包含着它们所有的共享信息，共享的信息越多说明它们相似的程度越高。最后利用先前的 3 个观点，我们就可以计算两个概念之间 C 和 D 的相似性，即概念 C 和 D 的相似性可以由它们的 LCS 包含的信息量(即它们共享的信息量)除以 C 和 D 信息量的总和(公共的信息量加上每一个具体的信息量)来评估。

而 sim_c 的计算为两个案例之间的矫正相似性，用于计算案例表示中有型角色相同、有型论域为数值型时两个不同概念的相似性，如 ∃has happened time of incident. =2010 year 和 ∃has happened time of incident. =2009 year 之间的相似性。根据本文的需要，有型域 D 只使用了一个特征，即有型角色，一个谓词公式，考虑的对象即为 $\exists F.d$ 和 $\forall F.d$ 的情形。

在式(1)中

$$\mathrm{sim}_c(con_F(C_i,D_j))=\sum_{i=0}^{k}\omega_i\cdot\frac{|d_1-d_2|}{|\max-\min|}\quad(6)$$

k 为自然数，$0\leqslant\omega_i\leqslant1$，$\sum_{i=0}^{k}\omega_i=1$

其中，ω_i 为权重因子，k 为有型角色相同、有型论域为数值型概念的个数，若 $F.=d_1$，$F.=d_2$，则 max 和 min 为有型角色 F 下数据类型 d_1，d_2 的最大、最小值。

现有案例 CA_1，CA_2 的问题描述部分分别为 P_1，P_2，其中

P_1：

A tiger virus incident=∃has type of incident.(∃Program.(Self-replicate⊓Self-propagation⊓∃has transmission method.(LAN weak password⊔mobile memory media⊔web Trojan⊔{affected exe file})⊓{IE Aurora 0day vulnerability}))⊓∃has happened time of incident. =2010 year⊓∃has organization of incident. Commercial organization⊓∃has affected resource of incident.((∃has type of host OS.({win7}⊔{win xp})⊓∃has host number. =20 tai⊓∃has function of host. Client⊓∃has abnormal sign.({antivirus software with virus warn}⊓{antivirus software unavailable}⊓{CPU usage high}⊓{exe file infected}⊓{system slowdown}⊓{hard disk light blink fast}⊓{IE

abnormal}⊓{process rar. exe and ping. exe cannot close}))⊓∃has state of incident. {ongoing}⊓∃has effect of incident. {money loss}.

P_2:

A dummycom virus incident = ∃has type of incident. (∃Program. (Self-replicate⊓∃has transmission method. (LAN ARP attack⊔mobile memory media⊔{affected exe file})))⊓∃has happened time of incident. = 2009 year⊓∃has organization of incident. Education⊓∃has affected resource of incident. ((∃has type of host OS. {win xp})⊓∃has host number. =100 tai⊓∃has function of host. Client⊓∃has abnormal sign. ({exe file infected}⊓{system with blue screen and crash}⊓{antivirus software unavailable}⊓{two process lsass. exe and smss. exe cannot close}⊓{system time is distorted}⊓{hidden file cannot display}⊓{security tool website cannot access}⊓{system slowdown}))⊓∃(has state of incident. {ongoing}⊓∃has effect of incident. {important data lost}。

则它们的最小公共包含为:

$LCS(P_1, P_2)$ = ∃has type of incident. (∃Program. (Self-replicate⊓∃has transmission method. (LAN weakness⊔mobile memory media⊔{affected exe file})))⊓∃has organization of incident. Organization⊓∃has affected resource of incident. (∃has type of host OS. {win xp})⊓∃has function of host. Client⊓∃has abnormal sign. ({antivirus software unavailable}⊓{system slowdown}⊓{exe file infected})⊓∃has state of incident. {ongoing}⊓∃has effect of incident. Effect of incident.

本文中相关系数 α 的取值为 0.98,ω_i 均为 0.5,则 $sim_p = \frac{24}{24+12+7} = 0.558$,案例 CA_1,CA_2 的相似度为 0.554。

为了验证所求算法的有效性,本文从国家互联网应急响应中心等机构收集了近 3 年比较典型性的 20 多个案例进行了相似性的度量,如图 7 所示,其中案例 1(CA_1)−7(CA_7)为病毒或蠕虫事件,案例 8(CA_8)−11(CA_{11})为移动恶意代码事件,案例 12(CA_{12})−14(CA_{14})为 DDoS 事件,案例 15(CA_{15})−17(CA_{17})为钓鱼网站或木马事件,案例 18(CA_{18})−20(CA_{20})为网页篡改事件。从图中可以看出,与飞客蠕虫安全事件相似度较高的事件都集中在案例 6(CA_6)−7(CA_7)之间,与 DDoS 安全事件相似度较高的事件都集中在案例 12(CA_{12})−14(CA_{14})之间,由此可以说明,该检索算法具有一定的辨识度,能够对不同的病毒、蠕虫和 DDoS 事件进行有效的区分,检索出与目标案例相匹配的安全事件案例,从而获得安全事件的解决方案,解决具体环境下的安全事件。

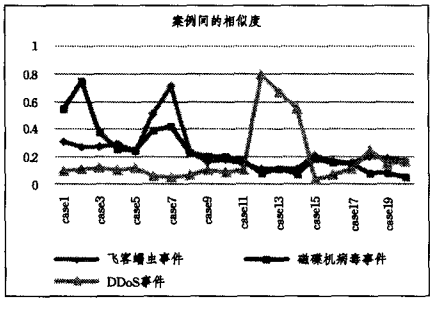

图 7 案例间的相似度

5.2 网络安全事件案例的重用和修改

案例的重用首先就是对检索到的相似性程度最高的案例进行直接重用,生成问题的初始解,但这往往会出现一些问题,生成的初始解在被评估之后不适用于目前的问题,所以还需对问题的初始解修改、评估得到最优解。案例的重用和修改有着密切的联系,这两个过程往往重复进行,直到评估生成最优解。案例的修改是一个将案例库检索到的最相似的案例转化为适合目前问题的合适解决方案的过程。已经有几种案例修正的方法被提出,这些主要可以分为 3 大类:替换修改、转换修改和生成修改[20]。其中,替换修改利用预定义的知识将旧的解决方案与新的问题需求矛盾、冲突的部分进行替换修改和更新。转换修改是将求解的问题转化成与之相关的问题,或者子问题求解后再修改得到解决方案。当检索到的案例的相似度很低,低于规定的阈值时,往往会采用生成修改的方法,直接由问题生成得到解决方案。本文主要采用替换修改的方法来对案例进行修改,具体方法和过程如下:首先假设源案例与目标问题案例是匹配的,那么它们将同时满足给定的知识库,然后通过描述逻辑概念的可满足性检测找出产生矛盾的概念,最后通过两个案例的最小公共包含逐一定位矛盾(需替换)的概念,替换修改或删除修改其中矛盾概念,直到矛盾消失完成修改。

5.3 网络安全事件案例的保存和维护

案例的保存需要保存的信息包括:解决安全事件的具体流程、未来响应类似安全事件需注意的地方、类似安全事件的防范方法以及利用该方法后响应的效果。保存案例时还需考虑,保存的案例是否能增加案例库的经验,丰富案例库,利于未来安全事件的解决,如若不能,就丢弃。案例的维护,是为了减少案例库案例的冗余,及时更新案例库,保证案例检索的效率和质量。案例的维护也需遵循删减的案例不会引起其他案例的变化,以及知识库中知识的减少;案例中更新的知识不会引起其他案例出现矛盾或错误等原则。

结束语 本文提出利用 DL-CBR 的方法实现网络安全应急响应,描述了 CBR 的主要过程及其在应急响应中的具体实现过程。考虑描述逻辑具有清晰的语义和能够提供相应的推理方法等特性,主要利用形式化的描述逻辑来表示案例,从而提供有效的方式分类和查询案例库。为了提升检索的整体效果,本文还设计了良好的基于细化算子和细化图的相似度匹配算法,以区分案例库中的不同案例,实验证明其具有良好的效果。对案例的修改方法和保存也做了详细的阐述。本文接下来还需要进一步开展的工作有:提升案例重用的过程,使用更有效的技术,比如结合失败的案例设计合理的案例重用、修改方法。

参 考 文 献

[1] Mitropoulos S, Dimitrios P, Christos D. On Incident Handling and Response: A state-of-the-art approach [J]. Computers & Security, 2006, 25(5): 351-370

[2] Danyliw R, Meijer J, Demchenko Y. RFC 5070: The Incident Object Description Exchange Format [OL]. http://www.ietf.org/rfc./rfc5070.txt

[3] Scarfone K, Grance T, Masone K. Computer security incident handling guide[J]. NIST Special Publication, 2008, 800(61): 38

[4] European Network Information Security Agency. Good practice guide for incident management [EB/OL]. [2013-12-09]. https://www.enisa.europa.eu/activities/cert/support/incident-management/files/good-practice-guide-for-incident-management

(下转第 163 页)

参 考 文 献

[1] Brewer D F C, Nash M J. The Chinese wall security policy[C]// Proceedings of the 1989 IEEE Symposium on Security and Privacy. Oakland, CA, USA, 1989. 206-214

[2] Lin T Y. Chinese wall security policy-an aggressive model[C]// Fifth Annual Computer Security Application Conference. Tucson, Arizona, USA, 1989: 282-289

[3] Sobel A E K, Alves F J. A trace-based model of the Chinese wall security policy[C]// Proceedings of the 22nd National Information Systems Security Conference. Arlington, Virginia, USA, 1999. 231-240

[4] Sandhu R. A lattice interpretation of the Chinese wall policy [C]// Proc of the 15th NIST--NCSC National Computer Security Conference. Washington, USA, 1992: 329-339

[5] 何永忠,李晓峰,冯登国. RBAC 实施中国墙模型及其变种的研究[J]. 计算机研究与发展,2007,44(4):615-622

[6] 秦超,陈钟,段云所. Chinese wall 策略及其在多级安全环境中的扩展[J]. 北京大学学报,2002,138(3):369-374

[7] Foley S N. Building Chinese walls in standard unixTM[J]. Unix Computers and Security Journal, ACM, 1997, 16(6): 551-563

[8] 夏少君,魏玲玲. 一种基于中国墙策略的应用程序保护模型研究[C]//第 27 次全国计算机安全学术交流会论文集. 2012: 212-214

[9] 马俊,王志英,任江春,等. 一种实现数据主动泄漏防护的扩展中国墙模型[J]. 软件学报,2012,23(3):677-687

[10] 程戈,金海,邹德清,等. 基于动态联盟关系的中国墙模型研究[J]. 通信学报,2009,11:93-100

[11] Sailer R, Jaeger T, Valdez E. Building a MAC-based security architecture for the Xen open source hypervisor[C]// Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC2005). Miami, FL, USA, 2005: 276-285

[12] Mccune J, Berger S, Cacerres R. Shamon: a system for distributed mandatory access control[C]// Preceedings of the 22nd Annual Computer Security Applications Conference. Miami Beach, Florida, USA, 2006: 23-32

[13] 牛文生,李亚晖,张亚棣. 基于安全域隔离的嵌入式系统的访问控制机制研究[J]. 计算机科学,2013,40(Z6):320-322,326

[14] Katsuno Y, Watanabe Y, Furuichi S. Chinese wall process confinement for practical distributed coalitions[C]// Proceedings of the 12th ACM Symposium on Access Control Models and Technologies. NY, USA, 2007: 225-234

[15] Jaeger T, Sailer R, Sreenivasan Y. Managing the risk of covert information flows in virtual machine systems[C]// Proceedings of the 12th ACM Symposium on Access Control Models and Technologies. Sophia Antipolice, France, 2007: 81-90

(上接第 136 页)

[5] Ahmad A, Hadgkiss J, Ruighaver A B. Incident response teams-Challenges in supporting the organizational security function [J]. Computers & Security, 2012, 31(5): 643-652

[6] Gonzalez J W J J, Kossakowski K P, Wiik J. Limits to Effectiveness in Computer Security Incident Response Teams[C]// Proc. of Twenty Third International Conference of the System Dynamics Society. Boston, Massachusetts, 2005

[7] Hashemi S H, Babaeizadeh M, Nowruzi M, et al. A comprehensive semi-automated incident handling workflow[C]// Proc. of IEEE Symp on Sixth International Telecommunications (IST). 2012: 1065-1070

[8] Ping L, Haifeng Y, Guoqing M. An incident response decision support system based on CBR and ontology[C]// Proc. of the 2010 Int Conf on Computer Application and System Modeling (ICCASM). IEEE, 2010, 11: 337-340

[9] Nowruzi M, Jazi H H, Dehghan M, et al. A comprehensive classification of incident handling information[C]// Proc. of IEEE Symp on Sixth International Telecommunications (IST). 2012: 1071-1075

[10] 罗杰文,施智平,何清,等. 一种 CBR 与 RBR 相结合的快速预案生成系统[J]. 计算机研究与发展,2007,44(4):660-666

[11] Aamodt A, Plaza E. Case-based reasoning: Foundational issues, methodological variations, and system approaches [J]. AI communications, 1994, 7(1): 39-59

[12] Gómez-Albarrán M, González-Calero P A, Díaz-Agudo B, et al. Modelling the CBR Life Cycle Using Description Logics[M]. Case-Based Reasoning Research and Development. Springer Berlin Heidelberg, 1999: 147-161

[13] Zeghib Y, De Beuvron F Ç, Kullmann M. Using description logics for designing the case base in a hybrid approach for diagnosis integrating model and case-based reasoning[M]. Case-Based Reasoning Research and Development. Springer Berlin Heidelberg, 2001: 561-575

[14] 方滨兴. 建设网络应急体系保障网络空间安全[J]. 通讯学报,2002,23(5):4-8

[15] Bergmann R, Kolodner J, Plaza E. Representation in case-based reasoning[J]. The Knowledge Engineering Review, 2005, 20(3): 209-213

[16] 刘欣然. 一种新型网络攻击分类体系[J]. 通信学报,2006,27(2):160-167

[17] Cunningham P. A Taxonomy of Similarity Mechanisms for Case-Based Reasoning[J]. IEEE Trans on Knowledge and Data Engineering, 2009, 21(11): 1532-1543

[18] Sánchez-Ruiz A A, Ontañón S, González-Calero P A, et al. Measuring similarity in description logics using refinement operators[M]// Case-Based Reasoning Research and Development. Springer Berlin Heidelberg, 2011: 289-303

[19] Sánchez-Ruiz A A, Ontañón S, González-Calero P A, et al. Refinement-Based Similarity Measure over DL Conjunctive Queries [M] // Case-Based Reasoning Research and Development. Springer Berlin Heidelberg, 2013: 270-284

[20] 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

[21] Vander Laag P R J, Nienhuys-Cheng S H. Completeness and properness of refinement operators in inductive logic programming[J]. The Journal of Logic Programming, 1998, 34(3): 201-225

[22] Lehmann J, Hitzler P. Foundations of refinement operators for description logics[M]// Inductive Logic Programming. Springer Berlin Heidelberg, 2008: 161-174