# 基于安全本体的协同报警分析研究

徐 慧[1] 肖 敏[2] 肖德宝[1]
(华中师范大学计算机网络与通信研究所 武汉 430079)[1]
(重庆邮电大学计算机科学与技术学院 重庆 400065)[2]

**摘 要** 用户的网络管理需要建立一种新型的综合网络安全管理解决方案,即统一网络安全管理。关注其中的一个关键功能——协同报警分析,在把握现有研究方向的基础上,提出一个网络安全报警分析基本框架。现今存在的主要问题在于如何保证安全报警的环境资产信息、背景知识与攻击知识的统一表达。目前,针对这一问题仍缺乏一个实践可行的有效方法,这将直接影响到统一网络安全管理的最终实现。在协同报警分析过程中引入CIM模式扩展的OWL+SWRL安全本体来统一表达信息与知识,并提出一个极具潜力的方法用以完善现有协同报警分析技术,作为实现统一网络安全管理的重要步骤。

**关键词** 网络安全,报警分析,协同,安全本体
**中图法分类号** TP393.08 **文献标识码** A

## Collaborative Alert Analysis Based on Security Ontology

XU Hui[1] XIAO Min[2] XIAO De-bao[1]
(Institute of Computer Network and Communication, Huazhong Normal University, Wuhan 430079, China)[1]
(College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)[2]

**Abstract** Network users need a new integrated solution for network security management, or in other words, unified network security management. This paper discussed collaborative alert analysis, which is one of its key functionalities, and based on a sufficient understanding of research direction, a basic network security alert analysis model was then provided. As for collaborative alert analysis, the main problem is how to guarantee unified representation of context information, background knowledge and attack knowledge for security alerts. And the fact is that, a practical and efficient approach is still lacking these days, which influents the realization of unified network security management. This paper introduced the use of security ontology by means of OWL+SWRL based on CIM Schema for unified representation of information and knowledge, and aimed at proposing a promising approach to improve existing collaborative alert analysis techniques as an important stage to realize unified network security management.

**Keywords** Network security, Alert analysis, Collaboration, Security ontology

## 1 引言

作为网络安全监控的重要工具,入侵检测系统(Intrusion Detection System, IDS)根据检测机制,被分为两类——异常检测系统和误用检测系统,但它们存在3点明显的不足:(1)报警率非常高,短时间内的大量报警使得管理员根本不能充分地进行报警分析、弄清楚报警的实际意义和采取合适的响应行动;(2)误报率很高,传统的IDS产品倾向于避免漏报,所以容忍一定程度的误报;(3)检测混合攻击的能力非常有限。产生这3点不足的根本原因在于IDS检测机制具有弱的环境意识且主要集中检测低层次的单个行动并独立地报警,缺乏与其它的网络安全机制和网络管理工具之间的协同,忽略了这些单个行动之间的空间与时间上的逻辑联系以及行动与具体环境之间的联系。也就是说,传统IDS的检测机制具有细粒度、孤立性和弱的环境意识等缺点。

为了克服现今IDS报警分析技术中存在的问题和局限,顺应网络安全管理的统一化趋势,有两种技术被众多的实践从业者和学院研究者所提倡:

· 协同(Collaboration)。协同体现在不同的IDS之间,IDS和其它的安全机制(如漏洞扫描、防火墙等)之间,IDS和其它的网络管理工具之间。人们希望通过协同实现对网络安全的统一和全面的管理。

· 关联(Correlation)。下层的协同依靠上层的数据分析技术来实现。这种数据分析技术主要是将来自于各个协同对象的数据信息进行关联分析以得出由单一的信息无法得到的结果。通称这类技术为关联技术。以IDS报警为中心,关联

到稿日期:2008-06-30 本文受湖北省科技攻关重大项目(2004AA103A01),武汉市科技攻关计划项目(200710421130)资助。
徐 慧(1983-),女,博士生,CCF学生会员,主要研究方向为网络管理与网络安全,E-mail:xuhui_1004@hotmail.com;肖 敏(1971-),女,博士,讲师,主要研究方向为网络安全与应用数学;肖德宝(1945-),男,教授,博士生导师,CCF会员,主要研究方向为计算机网络与通信技术等。

技术被分为两个方面：

① 资产关联。将 IDS 报警与相关的网络、主机、漏洞扫描、防火墙、防病毒等的信息(即背景知识)进行关联分析。这种分析主要是利用被监控环境的信息对 IDS 的报警的可信度和严重级别进行评估，增强 IDS 的环境意识，减少误报，也称之为一级关联或报警评估(Alert Evaluation)。这些背景知识来自于网络管理工具和其它的安全管理机制。因此，资产关联实现了 IDS 与被监控环境中的这些管理工具之间的协同。

② 报警关联。将来自于多个 IDS 的报警进行时间或空间上的关联，根据攻击情景将多个细粒度的报警综合成元报警，实现对攻击的全面描述，使管理员易于对报警进行分析和响应，也称之为二级关联或报警相关(Alert Correlation)。报警关联能在保证检测率的情况下大大降低报警率，抑制报警洪泛。时间上的报警关联主要是关联对具有因果关系的互为前提和结果的攻击的报警，空间上的报警关联则主要是关联具有一定相似度的攻击(如同源、同目的攻击等)的报警。

从这一角度来看，协同报警分析一般可以划分为 3 个阶段：报警聚合、报警评估和报警相关。然而，现今存在的主要问题在于如何保证安全报警的环境资产信息、背景知识与攻击知识的统一表达。本文针对这一问题，并结合当前数据模型与信息模型通过语义模型完善的发展趋势，引入安全本体作为信息与知识统一表达的基础，继而提出基于安全本体的协同报警分析方法。

## 2 协同报警分析基本框架

图 1 给出了统一网络安全管理环境下协同报警分析的基本框架。

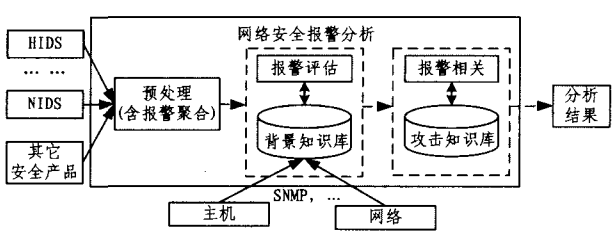


图 1 协同报警分析的基本框架

如图 1 所示，网络安全报警分析以经过预处理的 IDS 报警为中心，而后续处理过程则主要通过包含报警评估与报警相关的两级关联分析模式实现，最终将得到分析结果交由上层处理，以保证协同的具体实施。这里，预处理部分主要完成报警数据在语法和语义方面的标准化(如第 3 部分将要提到的 IDMEF 格式)与报警聚合(Alert Aggregation，将不同类型 IDS 和其它安全产品针对同一安全事件产生的大量相同或在相似度允许范围内的报警合并成一个报警)。而在报警分析技术的实际应用研究过程中，报警聚合技术常常与报警相关技术联系在一起，这是因为两者的目标是一致的，都是为了实现报警信息融合。

值得注意的是，在实现过程中为了保证最大程度地利用报警的环境资产信息，需要网络与主机数据采集技术的支持，例如综合网络管理技术。这样，从多数据源得到的信息(包括各类安全信息以及各种环境资产信息两方面)本身表达格式多种多样，且与背景知识、攻击知识的表达方式也不尽相同，所以有必要实现网络安全状态和状态变化的方式与规则的统一表达，即保证网络安全信息与知识表达的通用性，以便真正达到协同分析的表达需求。

## 3 安全本体的引入

信息和知识的表达是为了方便各种报警分析技术的实现，特别是对于报警信息和攻击知识的表达要适用于所有的分析技术。但在不同的分析技术中可能需要不同方面的特征信息，比如聚集中只用到与聚集轴对应的特征信息。而现有的表示方法往往集中研究攻击知识的表达方式，并没有尝试实现攻击知识与背景知识这两种表达方式的统一，更不用提与多数据源得到的信息表达方式的统一。如何保证网络安全协同报警分析技术中信息与知识的统一表示，是决定其效果的关键因素，也一直是研究的难点。

入侵检测消息交换格式(Intrusion Detection Message Exchange Format，IDMEF)[1]作为 IETF 制定的一个标准草案，主要用于表达报警之间的关系，这一目标正是由于报警关联分析的需求而产生的，但 IDMEF 主要用于统一 IDS 报警信息格式。而安全本体(Security Ontology，SO)[2]作为基于标准的容器，则更有利于信息与知识的统一表示，是未来网络安全协同报警分析技术研究中一个极有希望的发展方向。

现有管理信息定义语言，在语义表达方面能力都较弱，无法满足统一网络安全管理中报警分析的协同目标，而本体的应用使得在语义层面上解决管理数据模型的融合问题成为可能。万维网联盟(World Wide Web Consortium，W3C)组织提出的 Web 本体语言 OWL[3]是目前普遍使用的本体语言，它本身可扩展性强，并且具有诸如 UML 等通用建模语言的表达能力，而模型的文本表示则更为简单。

事实上，目前数据模型与信息模型正在通过语义模型完善，以保证用于管理领域的概念含义与它们之间已存在的关系能够实现形式化[4]，如图 2 所示。

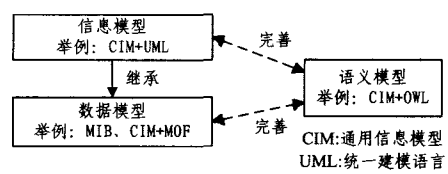


图 2 数据模型、信息模型与语义模型的关系

在网络安全协同报警分析技术的研究过程中，可以考虑结合基于本体的安全管理流程[2]统一网络安全信息与知识表示方式，以便支持信息抽取与决策。这样，在协同报警分析技术中，便可以融合本体方法，以实现复杂网络安全管理环境下信息与知识的统一表示。笔者认为，对于协同报警分析而言，信息与知识统一表达的基础便是一个安全本体 SO。

## 4 安全本体的构建

协同报警分析中基于本体的信息和知识的统一表达的关键在于定义一个安全本体 SO，以便通过使用来自于多源信息的安全知识实现可重用安全知识的互操作性、聚合与推理。

### 4.1 构建方法概述

应用于协同报警分析的安全本体构建将基于信息、知识与安全管理领域的知名模型与标准。

首先基于广泛采纳的管理领域标准，将 DMTF 组织提出的通用信息模型 CIM 标准作为一个容器用于定义 IS 中安全

相关的信息。接着，通过定义一个通用 SO，即使用本体语义来丰富这个 CIM 扩展，以支持知识共享与重用。SO 的定义是一个详细描述协同报警分析细节的本体。CIM 在本方法中是具有优势的，这是因为在特定条件下，这个模型可以被映射成结构化的语义网规范，例如 OWL。

这个 SO 是由带有本体语义的 CIM 扩展模式所定义的，用于为安全管理信息建模。另外，它与可继承的 CIM 概念相联接，能够访问其它 CIM-OWL 本体。这个 SO 用于作为 IS 安全需求("What"部分)的容器，这些安全需求是从可用的信息资源中提取的。为了实现这一目标，采用以下的"三步走"策略[2]。

① 概念层次建模；

② 以扩展的形式联接 CIM；

③ 在 OWL 中实现安全本体 SO。

### 4.2 概念层次建模

由于本体开发目前还没有一个标准化的方法[5]，这里依据文献[6]中描述的本体设计协作方法实现所需安全本体的构建。该安全本体用于满足协同报警分析技术实现过程中信息和知识的统一表达需求，其逻辑模型如图 3 所示。

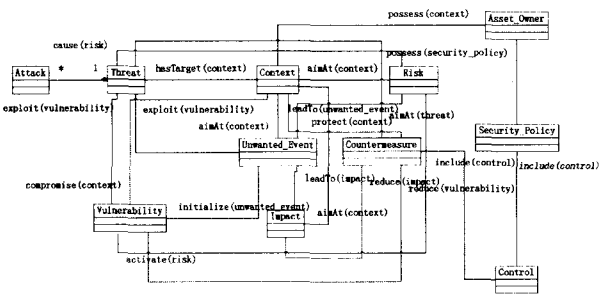


图 3 安全本体的逻辑模型

在图 3 所示的逻辑模型中，安全本体构建的核心概念在于 Context(环境资产信息)、Asset_Owner(资产所有者)、Vulnerability(漏洞)、Threat(威胁)和 Countermeasure(防御措施)。更进一步说，一个 Asset_Owner 拥有一个 Context，而该 Context 反过来又因 Vulnerability 而容易受到 Threat 的安全危机。从另一个角度看，可能由多个 Attack(攻击)造成的某个 Threat 的目标在于 Context，并试图利用 Context 的 Vulnerability 来达到这一目的。另外，利用 Vulnerability 将导致一个 Unwanted_Event(意外事件)的发生，该 Unwanted_Event 将具有一定的 Impact(影响)。在这种情况下，Countermeasure 通过使用 Control(控制)的方式减少 Threat 的 Impact。最终，Security_Policy(安全策略)将 Control 以规则的形式封装成由 Asset_Owner 所拥有的一个可管理的安全体系结构。

### 4.3 CIM 扩展的 OWL 定义

为了实现本体语言与 CIM 元模型的整合，利用文献[7]中描述的方法将后者转换成一个由 OWL-DL 定义的本体。根据网络安全协同报警分析的实际需要，这里只需要转换 CIM_ManagedElement 概念。利用 Protégé OWL 编辑器工具(选择 OWL 的描述逻辑 OWL-DL 作为编辑本体的方式)，同时依据已经得到的概念模型(如图 3 所示)，并结合 OWL-DL 语言的语法规则，实现所需安全本体的构建。

通过安装开源画图工具 GraphViz，并在 Protégé OWL 编辑器的 OWLViz 设置中指定正确的 DOT application 路径，便可以在 Protégé OWL 编辑器的基础上直接得到 OWL 类的关系图。由于篇幅的关系，图 4 仅给出构建的安全本体 OWL 类关系局部图。

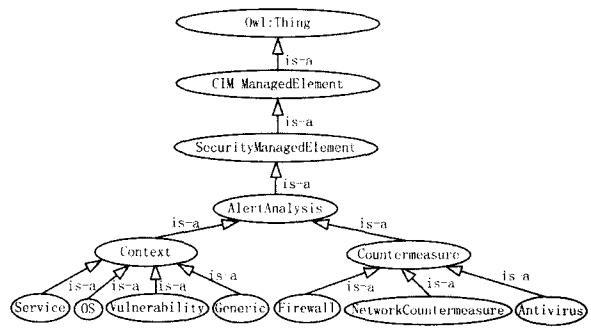


图 4 利用 Protégé OWL 编辑器构建的安全本体 OWL 类关系局部图

对于网络安全报警而言，每一个环境资产 Context 与特定的威胁 Threat 有关，并能通过一系列防御措施 Countermeasure 缓解。从这一点出发，在图 4 的基础上，表 1 与表 2 分别对所构建的安全本体中的环境资产类型与防御措施类型作进一步的说明。

表 1 网络安全报警环境资产类型列表

| 报警环境资产类型 | 说明 |
|---|---|
| 漏洞 | 漏洞指的是系统中存在的安全缺陷，而漏洞扫描的结果实际上是对系统安全性能的一个评估。作为一个重要的环境资产，漏洞信息主要用于判断报警的重要性。典型的信息源为 Nessus 脚本、Bugtraq 漏洞库与 CVE 目录。 |
| 操作系统 | 操作系统本身存在的漏洞极有可能威胁网络安全。例如，IIS Exploit 攻击针对的是 Linux 操作系统，而并非 Windows 操作系统。 |
| 服务 | 一般说来，服务的端口号、协议和版本信息与网络安全威胁是密切相关的。 |
| 其它信息 | 主要包括网络流量、主机上运行的用户、进程等信息，可通过综合网络管理平台工具动态获取。 |

表 2 网络安全报警防御措施类型列表

| 报警防御措施类型 | 说明 |
|---|---|
| 防火墙 | 经过报警分析识别出攻击后的响应策略是维护系统安全性与完整性的关键。IDS 与防火墙的联动是其中的一个重要措施，旨在实现自动响应。 |
| 防病毒 | 作为报警分析后的防御措施，防病毒软件应与 IDS、防火墙等相互协调形成一整套解决方案，这才是更为有效的网络安全管理手段。 |
| 网络防御措施 | 从全局的角度制定网络安全策略，并说明控制意图，在此基础上，定义具体的防御行为。 |

## 5 SWRL 关联规则定义

报警评估作为一级关联分析，主要用于减少误报率，并在此基础上，实施二级关联分析——报警相关，构造攻击场景，这就需要在安全本体中定义关联规则。规则的定义在网络安全协同报警分析技术中也是非常重要的，而 OWL 本体语言在描述关联规则的能力上明显不足。虽然 OWL 中定义了公理和约束，但这些都只是对类或属性进行约束，不能定义规则，也不能进行推导，因此有必要采用 SWRL 语言[8]来定义这些规则。

### 5.1 关联规则

从安全防护观点来看，入侵事件可以描述为能够引起入

侵行为的发生，或具有潜在入侵行为的一切活动、变化和事情。多个入侵事件可以组成入侵过程。大多数攻击不是孤立的，而是相关于一个攻击序列的不同阶段。早期阶段的活动是后期阶段活动的准备。如分布式拒绝服务(Distributed Denial of Service，DDoS)攻击，攻击者必须先在易受攻击的主机上安装 DDoS daemon 程序，然后才能指挥 daemons 发起攻击。也就是说，一个攻击者在实现其攻击目标之前必须先达到某个状态，而要达到这个状态通常要发起一些其它的攻击。一般地，一次完整的网络入侵过程可分为以下 7 个步骤[9]。

① 主机勘查：搜寻某一主机作为攻击的目标；

② 漏洞发现：找到目标主机上的安全漏洞；

③ 目标渗透：利用已经发现的目标主机的安全漏洞，获得非授权的访问权限；

④ 权限提升：获取目标主机上的特权权限；

⑤ 潜伏隐藏：掩盖活动行迹，以备下次进入目标主机；

⑥ 获取信息：获得或修改目标主机上的数据和信息；

⑦ 跳板攻击：利用已被控制的主机作为跳板，发动对其它目标主机的攻击。

一个成功的网络攻击往往由若干个处于不同阶段的入侵行为组成，较早发生的入侵行为为下一阶段的攻击做好准备，最后形成一个完整的网络攻击。再比如，一个易受攻击的服务的存在是一个远程缓存溢出攻击(Remote Buffer Overflow Attack)的前提，而这个攻击的一个结果是攻击者可以访问该主机。

换而言之，完成一个入侵需要一定的前提条件，同时它产生的结果也可能影响其它入侵行为。前提条件是指攻击成功的必要条件，而结果是攻击发生后可能产生的结果。利用 SWRL 语言定义规则来描述不同类型的攻击的前提和后果，并以此为基础，利用 SWRL 的推导机制将先发生的报警的结果与后发生的报警的前提进行匹配(可能是部分匹配)以实现报警之间的相关性分析。

### 5.2 SWRL 定义

下面通过一类典型的针对操作系统漏洞获取访问权限进而威胁系统安全的 DDoS 攻击的关联规则集实例对 SWRL 关联规则定义加以说明。

首先给出利用 SWRL 语法定义的其中一条关联规则(RDF 格式定义)：

```
〈swrl:Variable rdf:ID="x"〉
〈swrl:Variable rdf:ID="y"〉
〈swrl:Variable rdf:ID="z"〉
〈ruleml:imp〉
  〈ruleml:body rdf:parseType="Collection"〉
    〈swrl:classAtom〉
      〈swrl:classPredicate rdf:resource="#DestIPAddress"/〉
      〈swrl:argument1 rdf:resource="#x"/〉
    〈/swrl:classAtom〉
    〈swrl:classAtom〉
      〈swrl:classPredicate rdf:resource="#FTPService"/〉
      〈swrl:argument1 rdf:resource="#y"/〉
    〈/swrl:classAtom〉
    〈swrl:individualPropertyAtom〉
      〈swrl:propertyPredicate rdf:resource="#ExistFTPService"/〉
      〈swrl:argument1 rdf:resource="#x"/〉
      〈swrl:argument2 rdf:resource="#y"/〉
    〈/swrl:IndividualPropertyAtom〉
    〈swrl:classAtom〉
      〈swrl:classPredicate rdf:resource="#OS"/〉
      〈swrl:argument1 rdf:resource="#z"/〉
    〈/swrl:classAtom 〉
  〈/ruleml:body〉
  〈ruleml:head rdf:parseType="Collection"〉
    〈swrl:individualPropertyAtom〉
      〈swrl:propertyPredicate rdf:resource="#GainOSInfo"/〉
      〈swrl:argument1 rdf:resource="#x"/〉
      〈swrl:argument2 rdf:resource="#z"/〉
    〈/swrl:IndividualPropertyAtom〉
  〈/ruleml:head〉
〈/ruleml:imp〉
```

图 5 给出了使用 Protégé SWRLTab 工具编辑该 DDoS 攻击关联规则集的 SWRL Editor 视图。

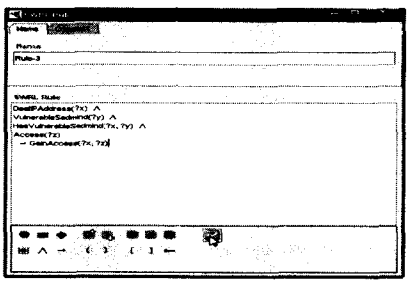

图 5 利用 Protégé SWRLTab 工具编辑 DDoS 攻击关联规则集的 SWRL Editor 视图

如图 5 所示，使用 Protégé SWRLTab 工具可以直接编辑得到以下这些 SWRL 规则，并生成 XML 格式的本体表现形式：

DestAddress(? x) ∧ FTPService(? y) ∧ ExistFTPService(? x,? y) ∧ OS(? z)

⇒ GainOSInfo(? x,? z)

DestAddress(? x) ∧ OSSolaris(? y) ∧ GainOSInfo(? x,? y) ∧ VunerableSadmind(? z)

⇒HasVunerableSadmind(? x,? z)

DestAddress(? x) ∧ VunerableSadmind (? y) ∧ HasVunerableSadmind(? x,? y) ∧ Access(? z)

( GainAccess(? x,? z)

… …

由此可见，利用 Protégé OWL 编辑器的 SWRLTab 工具可以直接生成这些关联规则的语法定义，并应用于报警评估后的报警相关中，最终实现关联分析，生成攻击场景图。

**结束语** 本文引入了安全本体作为网络安全信息与知识的统一表示的基础，以确保协同报警分析效果，并重点探讨了用于协同报警分析的安全本体构建问题，该本体的构建基于 CIM 扩展模式、OWL 语言与 SWRL 语言等信息、知识与安全管理领域的知名模型与标准。

总而言之，借助于 Protégé OWL 编辑器及其相关工具，并依据 CIM 扩展模式，定义 OWL+SWRL 本体，可以实现应用于协同报警分析技术中的安全本体构建。

(下转第 157 页)

些任务，及随机增加一些任务），得到 Model'，然后再根据 Model'成多条工作流实例，作为新增日志。(3)调用改进后的更新算法进行测试。下面是一个执行例子。新增日志记录了 1000 条流程记录。$\sigma$ 取值 0.1。首先，读入已有模型，再读入新增日志信息。模型更新结果如图 3 所示。在新增日志中，新增了任务 H 及 I，而缺少了任务 C 及 F。由于任务 C 被指定要求保留在模型中，故在新增模型中仍然保留，而任务 F 则被去掉。

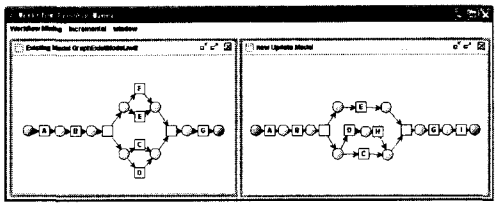

图 3 Workflow Process Miner 增量挖掘模型更新图例

**结束语** 工作流流程挖掘，能从系统日志记录中挖掘系统任务的执行时序关系，以工作流模型的形式向模型设计者反馈工作流流程的真正执行状态。目前很多研究仅针对一份日志信息进行挖掘处理，而关于增量挖掘方面的研究却不多。文献[8]提出一种利用新增日志更新已有模型的算法。但是，该算法没有考虑到已有模型中某些任务可能被取消的情况。本文在该算法的基础上提出了一种改进方法：对于原有模型中已存在的、在新增日志中未被执行过的任务，通过流程设计者的先验知识及任务在总记录数中出现的频率，判断该任务是否被取消。最后，通过模拟实验验证该方法的可行性。但是，对于未被指定为模型中必须存在的任务，在通过其出现频率判断其是否应保留在模型中的步骤上，仍存在一定缺陷：对于处于选择结构的任务，由于流程不一定执行其选择分支，故该任务被执行的频率低于其余流程中必须要执行的任务的频率。这样，对于不同的任务，有不同的阈值 $\sigma$。下一步的工作，将结合任务在模型中所处的结构，动态选取其阈值。

## 参 考 文 献


[1] 罗海滨，范玉顺，吴澄. 工作流技术综述[J]. 软件学报，2000，11(7)：899-907

[2] Aalst W M P, Weijters A J M M, Marster L. Workflow Mining: Discovering process models from event logs[J]. IEEE Transaction on Knowledge and Data Engineering, 2004, 16(9): 1128-1142

[3] Herbst J, Karagiannis K. Workflow Mining with InWoLvE[J]. Computers in Industry, 2004, 53(3): 245-264

[4] Silva R, Zhang J J, Shanahan J G. Probabilistic Workflow Mining [C]// Proceedings of the 11th ACM SIGKDD International Conference on Knowledge Discovery in Data Mining. 2005: 275-284

[5] Cook J E, Wolf A L. Discovering Models of Software Processes from Event-based Data[J]. ACM Transactions on Software Engineering and Methodology, 1998, 7(3): 215-249

[6] Maruster L, Weijters A J M M, van der Aalst W M P, et al. Process Mining: Discovering Direct Successors in Process Logs [C]// Proceedings of the 5th International Conference on Discovery Science. 2002: 364-373

[7] de Medeiros A K A, Weijters A J M M, van der Aalst W M P. Genetic Process Mining: An Experimental Evaluation[J]. Data Mining and Knowledge Discovery, 2007, 14: 245-304

[8] Sun Weixiang, Li Tao, Peng Wei, et al. Incremental Workflow Mining with Optional Patterns[C]// International Conference on Systems, Man and Cybernetics. 2006, 4: 2764-2771

[9] Kim K, Ellis C A. $\sigma$-Algorithm: Structured Workflow Process Mining Through Amalgamating Temporal Workcases[C]. Advances in Knowledge Discovery and Data Mining, LNCS. 2007, 4426: 119-130

[10] Kindler E, Rubin V, Schafer W. Incremental Workflow Mining for Process Flexibility[C]// The 7th Business Process Modeling, Development and Support. 2006


(上接第 107 页)

下一步的工作可以从以下两方面展开：

(1)实现用于协同报警分析技术中的安全本体的全面构建。本文给出了基于 CIM 扩展模式、OWL 语言与 SWRL 语言的安全本体标准化构建方法，但具体的构建过程是一项庞大的系统工程，需要了解和总结现阶段发生的所有攻击的关联规则，而且有必要考虑到扩展性的需求。

(2)研究如何应用构建的安全本体在关联分析的基础上实现安全设备间自动响应。本文引入的安全本体不仅定义了环境资产信息，还定义了防御措施信息。考虑在 OWL+SWRL 本体描述的基础上，通过定义 OWL-S 来规范一组用来描述服务的知识本体，而语义标记的使用将保证联动响应控制策略这类 Web 服务能够被人和机器理解。

## 参 考 文 献


[1] Debar H, Curry D, Feinstein B. The Intrusion Detection Message Exchange Format (IDMEF). RFC4765, 2007

[2] Tsoumas B, Gritzalis D. Towards an Ontology-based Security Management [A]// Proceeding of 20th International Conference on Advanced Information Networking and Applications [C]. Washington, DC: IEEE Press, 2006: 985-992

[3] Patel-Schneider P F, Hayes P, Horrocks I. OWL Web Ontology Language Semantics and Abstract Syntax. W3C Recommendation, 2004

[4] Pras A, et al. Key Research Challenges in Network Management [J]. IEEE Communications Magazine, 2007, 45(10): 104-110

[5] Noy N, McGuiness D. Ontology Development 101: A Guide to Creating Your First Ontology [R]. No. KSL-01-05. Palo Alto: Knowledge Systems, AI Laboratory, Stanford University, 2001

[6] Holsapple C, Joshi K. A Collaborative Approach to Ontology Design [J]. Communication of the ACM, 2002, 45(2): 42-47

[7] Quirolgico S, Assis A, Westerinen A, et al. Toward a Formal Common Information Model Ontology [A]// Bussler C, et al., eds. Web Information Systems - WISE 2004 Workshops, Lecture Note in Computer Science 3307 [C]. Berlin: Springer, 2004: 11-21

[8] Horrocks I, et al. SWRL: A Semantic Web Rule Language Combining OWL and RuleML. W3C Member Submission, 2004

[9] 卢继军，黄刘生，吴树峰. 基于攻击树的网络攻击建模方法[J]. 计算机工程与应用，2003，39(27)：160-163