集成安全分析的模型驱动软件开发方法研究

陈 峰[1,2] 李伟华[1] 房鼎益[2] 陈晓江[2]

(西北工业大学计算机学院 西安 710072)[1] (西北大学 西安 710069)[2]

摘 要 提出了一种集成安全分析的软件设计与开发新方法,该方法以MDA为基础框架,使用UMLsec建立软件安全属性的平台无关模型,使得在软件设计的早期就能够囊括更多的安全需求,从而降低后期开发的风险与成本,提高软件的复用性。

关键词 安全分析,模型驱动架构,UML安全扩展

中图法分类号 TP311 **文献标识码** A

Research on Integration of Safety Analysis in Model-driven Software Development

CHEN Feng[1,2] LI Wei-hua[1] FANG Ding-yi[2] CHEN Xiao-jiang[2]

(School of Computer Science and Technology, Northwestern Polytechnical University, Xi'an 710072, China)[1]

(Northwest University, Xi'an 710069, China)[2]

Abstract This paper proposed a new method aiming at integrating the safety analysis in software design and development. Model Driven Architecture is used for the basic framework. By making use of UML extension, UMLsec modeled the Platform Independent Model of software security, which achieved more security requirements in the initial stage of the system design cycle. This approach reduces the risk and the cost of software development and improves the reusability.

Keywords Safety analysis, MDA, UMLsec

1 引言

软件质量的提高一直是开发过程中面临的一个重要而棘手的问题。近年来,随着计算机应用范围的迅速扩大,软件系统开始广泛地应用于工业控制、航天航空、医疗设备、银行、交通等领域。计算机及其软件虽然改善了人们的生活水平与工作条件,但也更加直接地关系到人们的生命、财产与人类的生存环境的安危,因此对软件质量提出了一个新的要求,即安全性[1]。系统安全性设计的不足将会成为重大软件事故的隐患。

MDA(Model Driven Architecture,模型驱动架构)[2]是OMG(The Object Management Group,国际对象管理组织)提出的软件开发过程中的模型组织管理框架,它试图准确地建立模型与模型之间、模型与系统之间的关系,使模型在系统开发过程中起到实质性的作用。模型驱动的软件开发过程中,系统的业务模型和实现技术相分离,业务模型具有持久价值,但是目前在该方法的使用中并未很好地解决安全属性的建模问题。

针对上述具体问题,文献[3]给出了一种通过创建安全对象以及故障树分析评估进行安全分析的模型驱动软件开发方法;文献[4]介绍了基于模型的安全工程,采用UMLsec描述安全特性,但在该方法中并未对各个阶段所包含的不同信息的模型进行有效划分,降低了模型的重用性与灵活性。本文提出了一种集成安全分析的模型驱动软件开发方法,并实现了相应的支持工具,从而有效地解决了以上问题。

本文阐述了在模型驱动软件开发方法中加入安全性描述与建模的重要意义。第2节着重分析了软件安全性的设计;第3节详细讨论了集成安全分析的模型驱动的软件开发方法及其应用;最后对本文工作进行了总结。

2 软件安全性设计

软件安全性分析旨在保证程序在所设计的运行环境中不会引起(或可以容忍的小概率引起)或诱发对人员、设备的危害。它是一种系统性的分析,应在研发过程的早期进行。从开发方法上讲,它涉及软件开发的全过程和各种方法,包括软件工程、形式化方法、容错技术、测试技术等,要求与具备不同领域知识背景的专家合作,从系统的角度考察软件。软件生存周期的各个阶段,包括需求分析、规约、设计、编码、测试、维护,都应当为所能达到的安全性提供证据。这些证据应形成相互衔接的、完整的链条,作为独立部分加以保存,以便分析

到稿日期:2008-12-22 返修日期:2009-03-02 本文受陕西省自然科学基础研究计划项目(2007F38),陕西省教育厅自然科学专项(08jk445),陕西省自然科学基金(2007F06),陕西省教育厅产业化示范项目(08JC01),陕西省国际科技合作重点项目(2006KW-21)资助。

陈 峰(1978-),男,博士生,助理研究员,主要研究方向为软件安全、信息安全,E-mail:xdcf@nwu.edu.cn;李伟华(1951-),男,教授,博士生导师,主要研究方向为信息安全;房鼎益(1959-),男,教授,博士生导师,CCF会员,主要研究方向为网络监测、信息安全;陈晓江(1973-),男,博士,讲师,主要研究方向为网络应用、网络安全。

和检查。涉及到安全性需求的通用软件系统以及安全性至关重要的软件系统，应考虑使用更为严格的过程管理以及形式化的设计与开发方法。

对于安全性关键软件，从系统的设计人员到开发人员均能将其安全属性的实现视为头等任务；而对于通用应用软件，开发者往往会忽视系统的安全性，从而引发故障。例如，某些权威部门网站在一些关键时刻所发布的信息如果被恶意篡改，将会导致不良的社会影响；涉及私密信息的软件系统，如果不对访问权限、数据安全性加以控制，同样会产生大量问题。

MDA 作为一种新的系统开发方法能够实现将安全性设计贯穿于整个软件开发过程的目标，它强调通过建模行为的驱动，完成系统需求分析、架构设计、构建、测试、部署和运行维护工作。根据模型中是否包含与平台技术相关的信息以及不同的抽象层次，定义了 CIM（Computation Independent Model，计算独立模型）、PIM（Platform Independent Model，平台独立模型）、PSM（Platform Specific Model，平台相关模型）和 ISM（Implementation Specific Model，实现相关模型）。CIM 类似于通常所说的业务模型和用例模型，是一个抽象层次较高、独立于任何实现技术的系统模型；PIM 类似于系统分析模型，处于中间抽象层次，关注系统的整个架构实现，但却忽略掉与平台相关的部分；PSM 则与设计模型相像，包含了具体平台的特定实现技术。MDA 方法通过模型技术提高软件开发效率，有效地集成各种跨平台的应用，增强软件的可移植性。将软件的安全性设计加入到建模过程中并制定相应的转换规则，可使模型驱动的开发方法能够创造出高质量的、安全的软件系统，同时具备使用 MDA 开发的诸多优势。

3 集成安全分析的模型驱动软件开发方法（SAM-DA）

在软件设计过程中，时刻要有安全性观念。编写安全软件的更好方法是从一开始就将安全性设计到系统之中[3]。从诸多案例中已体会到这一点，在设计之初并没有考虑安全因素，随后只有通过添加安全性功能部件来解决存在的隐患。

3.1 集成安全分析的模型驱动架构

MDA 方法从系统需求出发，通过建立不同阶段的模型以及应用模型转换技术，实现了软件的自动化生成。然而，在使用 UML 对系统进行建模的过程中，现有的 UML2.0 所提供的基本模型无法对其安全属性进行恰当的描述。为了突出安全性在软件设计与开发中的重要性，结合 MDA 的设计方法，本文提出了集成安全分析的模型驱动架构，如图 1 所示。中间的虚线框中显示了基于模型驱动架构的软件开发过程，即首先建立系统的业务模型，将其转换为平台无关模型之后再转换为平台相关模型，最后产生系统的实现相关模型。右侧的虚线框中显示了对软件设计过程所要添加的安全分析，即首先领域专家通过对系统安全性评估，得出所涉及领域的安全特征描述（该描述可用自然语言表示），同时生成系统的安全特征说明文档。安全特征作为系统需求的一部分，划分为性能描述与功能描述。将性能描述直接添加为系统业务模型的一部分，并转换为左侧虚线框中显示的安全性能测试用例。功能描述通过 UMLsec[4]（UML 安全扩展）建模后加入到平台无关模型中。

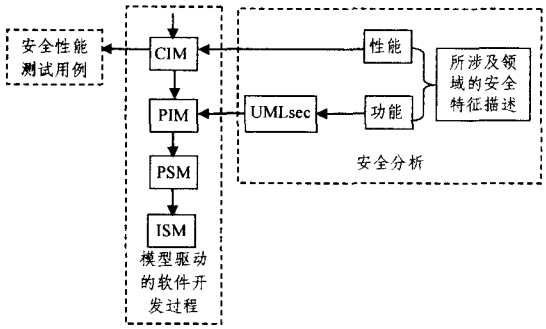

图 1 集成安全分析的模型驱动架构

3.2 安全属性建模

软件安全特征的功能性描述根据不同应用领域的不同侧重点，通过添加相应的 profile 文件，实现不同的安全分析策略。基本原理如图 2 所示：(1)使用 UML 建立系统未包含安全属性的平台无关模型；(2)将该模型保存为 xml 文件；(3)选定预先定义的 xml 格式的 profile 文件，该文件对不同图形所能添加的构造型进行了约束；(4)通过菜单选项向 UML 模型中的图件添加 profile 文件中的构造型；(5)添加后的文件保存为 xml 格式，工具通过可视化机制将其显示为使用 UML 表示的包含安全属性的 PIM。

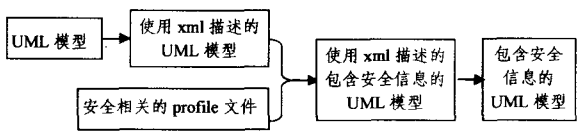

图 2 安全属性的添加过程

3.2.1 安全类型的划分

在核能、航空、铁路、航天、石油、化工、医疗仪器等领域，应用着大量安全性关键软件，其安全特性与使用环境紧密相关。而通用应用软件的安全问题主要针对信息安全的部分内容，即主要针对数据库安全、访问控制、加密与鉴别等应用层面的安全。本文所提出的集成安全分析的模型驱动架构也主要应用于通用应用软件安全性的讨论。

3.2.2 基于安全分析的 UML 扩展

UML 是一种通用的可视化建模语言，适用于各种软件开发方法、软件生命周期的各个阶段。尽管它已经提供了丰富的建模元素和符号，可满足大多数情况下对系统的建模需要，但在对软件安全进行建模时，一些构件不能与标准 UML 建模元素一一对应，因此必须对 UML 进行扩展，其 3 种核心扩展机制包括构造型、标记值和约束。构造型是一种修饰，允许为建模元素定义新的语义。标记值是可以与建模元素相关联的键值对，允许在建模元素上“标注”任何值。约束是定义模型外形的规则，可表示为任何形式的文本，或者用更正式的对象约束语言表示。

UML 安全扩展“UMLsec”是基于 UML 标准扩展机制的一个 UML profile，通过在 UML 元模型中增加安全相关的构造型、标记值、约束等建模元素，来表达安全属性的语义和系统需求与约束。但目前 UMLsec 主要是基于计算机网络环境定义的，将其用于不同应用领域的安全分析中还需要进行相应的扩展。主要扩展点在于在 UMLsec 的元素中增加相关领域的定义，使其能够更明确、更有针对性地表达不同业务领域的特点，同时描述最基本的安全需求，例如数据保密性和

完整性；领域相关的安全知识；允许考虑不同的威胁场景，此场景取决于对手的实例；允许包含重要的安全概念；允许加入安全机制，例如访问控制权限等[5,6]。

3.2.3 UMLsec 设计

通过 UML 活动图对软件系统的安全控制流进行建模，顺序图用来表示安全关键的交互，状态图则能够建立保护对象安全性的模型，而部署图实现了物理安全性需求。根据 UML2.0 中各类模型的特性，针对软件安全属性，设计了以下构造型。

• 针对用户安全：构造型《access》对用户基本信息进行控制与验证，防止对软件系统的非法攻击与恶意访问。

• 针对访问权限控制：构造型《privilege》对被访问的类、对象、信息设定权限策略，约束信息可根据具体应用软件设计的实际情况制定。

• 针对敏感信息传输过程的加密与解密：构造型《encrypted》表示对传输过程中的敏感信息以及数据进行加密，该构造型可应用于顺序图所描述的交互行为；构造型《decrypted》表示对信息读取前进行解码。

• 针对数据库安全：构造型《data security》表示对数据安全性的说明，同时使用{secrecy, integrity, consistency}对数据保密性、完整性以及一致性进行约束。

UMLsec profile 构造规则如下：

1)经专家分析得出软件系统所涉及领域的安全特征 s-feature，s-feature＝{用户安全，访问权限，信息传输、数据库安全}，针对不同应用的需求可变更以上特征的划分。

2)给出各类特征包含的安全属性关键点 k-point，s-feature＝{k-point$_1$，k-point$_2$，…}，每个关键点对应一类构造型。

3)构造型 ST 可定义为一个五元组：ST＝{type，name，attribute，constrain，association}。其中，type＝{diagram | diagram∈UML2.0}，表明构造型的应用范围；name 表示构造型的名字，在命名时尽量贴近其代表的实际意义；attribute 描述了属性；constrain 指出了所属构造型的约束条件；association＝{(a-name，a-type)}，定义了所属构造型与其他构造型的关联关系，a-name 代表关联构造型名称，a-type 代表关联关系。

4)使用 xml 描述通过以上方法定义的构造型，完成 profile 文件。

UMLsec profile 构造完成之后，可根据实际应用的要求给出所包含构造型在 PSM 层具体实现细节的描述。

3.3 SAMDA 方法在软件开发中的应用

本节以典型的网上交易系统为例，说明如何使用 SAMDA 方法开发包含安全策略的应用软件。设计过程仅涵盖了部分通用性较高的系统用例，但并未对该方法的介绍造成影响。

网上交易系统通常包括用户登录、商品浏览、确认购买、网上支付等 4 个模块，如图 3 所示。该 4 部分可作为系统的基本需求，针对用户登录与网上支付还需附加额外的安全约束。在使用 SAMDA 方法进行设计与开发的过程中，用例图作为 CIM 表示系统业务，并可根据每个用例的实际意义给出其用例描述，以便向 PIM 转换；PIM 的建立需要使用到 UML2.0 中的类图、活动图、顺序图、状态图等。用户在使用该系统的过程中，浏览商品操作不需进行实名登录和身份确认，而其余操作均要在登录动作顺利完成后进行。图 4(a)显示了系统未对安全属性进行建模的顺序图，而图 5(a)则给出了添加安全信息后的顺序图。添加过程如下：(1)使用 xml 描述未包含安全信息的顺序图如图 4(b)所示，其给出了对应于图 4(a)顺序图的 xml 文件片段；(2)为顺序图中的对象、消息添加 profile 文件中相应的构造型《access》和《encrypted》，分别用以描述、验证用户登录基本信息、对支付账号进行加密等安全属性，图 6 显示了UMLsec profile文件的一部分，描述了可应用于顺序图的构造型《access》；(3)更新后的xml文件，如图 5(b)所示，可通过工具显示为包含安全信息的顺序图。

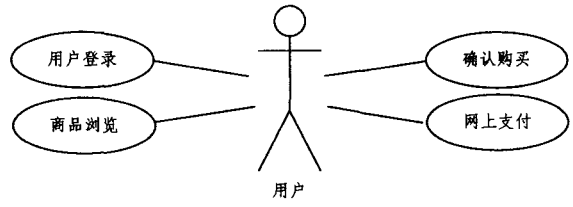

图 3 网上交易系统用例图

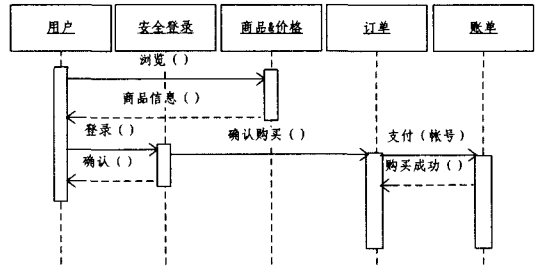

图 4(a) 网上交易系统未包含安全属性的顺序图(PIM)

```
<name>用户</name>
<lifeLine>
  <owner reference="../.."/>
  <activations>
      <uml.sequencediagram.model.ActivationModel>
       <ownerLine reference="../../.."/>
       <sourceConnections>
         <uml.sequencediagram.model. SyncMessageModel>
           <name>登录()</name>
           <source class="uml.sequencediagram.
           model.ActivationModel" reference="../../.."/>
           <target class="uml.sequencediagram.
           model.ActivationModel">
             <ownerLine>
               <owner>
                 <name>安全登录</name>  ……
</lifeLine>
```

图 4(b) 网上交易系统未包含安全属性顺序图的 xml 描述

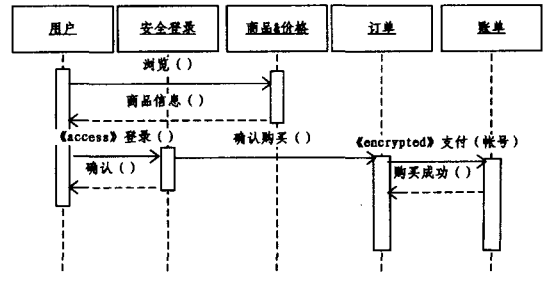

图 5(a) 网上交易系统包含安全属性的顺序图(PIM)

```
<profileURI>
  ......
</profileURI>
<profileName>UML.sec</profileName>
 <name>用户</name>
 ......
        <uml.sequencediagram.model.SyncMessageModel>
        // 顺序图同步消息模型
          <name>登录()</name>
          <stereoType>access</stereoType>
          ......
```

图 5(b)　网上交易系统包含安全属性顺序图的 xml 描述

```
......
<packagedElement xmi:type="uml:Stereotype"
xmi:id=" " name="access">
    <ownedAttribute xmi:id=" " name="base_
      Abstraction" association=" ">
      <type xmi:type="uml:Sequence" href="pathmap:// UML_
        METAMODELS/UML.metamodel. uml#Abstraction"/>
    </ownedAttribute>
</packagedElement> ......
```

图 6　UMLsec profile 文件片段

```
<uml.classdiagram.model.ClassModel>
        <name>access</name>
          <children>
            <uml.classdiagram.model.AttributeModel>
            // access类的属性
              <name>anonymous</name>
            // 确定访问方式：是否匿名访问
              <type>boolean</type>
            </uml.classdiagram.model.AttributeModel>
            <uml.classdiagram.model.OperationModel>
            // access类的操作
              <name>session</name>
            // 匿名访问：设置session失效时间
              <type>string</type>
              <name>name</name>
            // 实名访问：验证用户名、密码
              <type>string</type>
              <name>password</name>
              <type>string</type>
              <name>IP</name>
            // 记录访问者的IP地址
              <type>string</type>
            </uml.classdiagram.model.OperationModel>
          </children>
</uml.classdiagram.model.ClassModel>
```

图 7　《access》构造型对应的平台相关描述

得到系统集成安全性建模的 PIM 之后，可通过 XSLT (Extensible Stylesheet Language Transformations，扩展样式表转换语言)制定针对不同平台的转换规则，实现向 PSM 的转换，即将 PIM 中的安全属性映射到指定平台，最终使安全策略在所开发的软件中得以实现。为了使转换过程易实现、易操作、易修改，所有 PIM，PSM 均保存为 xml 文件。针对不同的应用系统，在相同的开发平台下，安全属性模型构建完成之后，可使用相同的转换策略实现安全属性模块。与传统建模方法相比，profile 文件对安全属性进行了有效的划分，明确了添加在每种图形之上的具体构造型，并使其具有指定的意义，作为模型转换的基础。图 7 给出了构造型《access》对应的 PSM 描述。为防止系统访问人数过载，需对匿名使用者设置访问时长，其限制可根据应用系统的类型及访问用户身份、数量的要求决定，在即将超时之前给予登录系统提示，直至会话关闭，同时匿名访问时，权限受到一定控制。而实名访问比较容易控制使用系统的用户数量上限。为防止恶意攻击，两种访问方式均需记录用户的 IP 地址。Profile 中的其他构造型以类似方法描述。

3.4　支持工具

为支持本文介绍的集成安全分析的模型驱动软件开发方法，在开源的 Eclipse 平台下开发了安全建模工具。该工具作为 Eclipse 插件使用，提供 UML 建模功能，并将模型保存为 xml 格式。在完成系统 PIM 模型建立之后，通过菜单加载 UMLsec profile。根据预先定义的 profile 文件可对相应的模型添加构造型，实现对软件安全性建模。

结束语　现代信息社会对计算机的依赖，主要表现为对软件的依赖。计算机软件已经成为信息基础设施中至关重要的环节。提高软件质量，保障软件安全性，具有巨大的社会价值和经济价值。

本文提出了一种集成安全分析的模型驱动软件开发方法，它采用 UML 安全扩展机制建立系统安全相关的平台无关模型，从而将软件的安全性分析提前到了设计的早期，实现了 MDA 方法中软件安全属性的建模，降低了后期开发的风险与成本。在进一步的工作中，需要深入研究不同应用领域软件系统存在的典型安全问题，设计出具有针对性的 UMLsec profile，并将该方法应用于更多的软件项目中。

参 考 文 献

[1] 周新蕾. 软件安全性分析技术及应用[J]. 质量与可靠性，2005(3)：37-40

[2] Miller J，Mukerji J，et al. Model driven architecture[EB/OL]. Ormsc/2001-07-01：Needham，Object Management Group，2001，1-31. http：//www.omg.org/cgi-bin/doc? ormsc/2001-07-01

[3] de Miguel M A，Briones J F，Silva J P，et al. Integration of safety analysis in model- driven software development[J]. IET Software，2008，2(3)：260-280

[4] Jürjens J，Munich T. UMLsec：Presenting the Profile[EB/OL]. http：//www.omg.org/news/meetings/workshops/DOCsec-2002_Proceedings/01-2_Juergens_UMLsec_Tutorial.pdf

[5] Jürjens J，Munich T. Secure Software Architecture Description using UML [EB/OL]. http：//wiki.lassy.uni.lu/tiki-download_file.php? fileId=165

[6] Best B，Jürjens J，Nuseibeh B. Model- based Security Engineering of Distributed Information Systems using UMLsec[C]// 29th International Conference on Software Engineering (ICSE 2007). Washington：IEEE，2007：581-590

(上接第 100 页)

[12] Kim Yong soo，Kim Sung-ihl. Fuzzy neural network model using a fuzzy learning vector quantization with the relative distance [C] //Proc of the 7th International Conference on Hybrid Intelligent Systems. Kaiserlautern，2007

[13] Behera L，Kumar S，Patnaik A. On adaptive learning rate that guarantees convergence in feedforward networks [J]. IEEE Transactions on Neural Networks，2006，17(5)：1116-1125

[14] Kuo Ming-jen，Lin Tsung-chih. Dynamical optimal training for behavioral modeling of nonlinear circuit elements based on radial basis function neural network[C] // Proc of the Asia-Pacific Symposium on Electromagnetic Compatibility and 19th International Zurich Symposium on Electromagnetic Compatibility. Singapore，2008

[15] Sh Hosseini，Ch Jutten. Maximun likelihood neural approximation in presence of additive colored noise[J]. IEEE Transactions on Neural Networks，2002，13(1)：117-131