软件可信评估综述*

周　剑，张明新
（常熟理工学院，江苏 常熟 215000）

摘　要：软件可信评估是近年来计算机科学的一个新的研究热点和难点，对软件可信评估的研究有助于促进软件产业的振兴与发展。首先分析了软件可信评估的必要性；然后对可信评估的研究现状进行综述，主要包括体现可信的属性特征和软件可信等级的定义、软件可信评估模型、软件可信评估实现方案四个方面；同时分析了目前可信评估中存在的不足以及造成这些不足的根本原因；最后指出了可信评估的未来发展趋势。

关键词：软件可信；可信属性；可信等级；可信证据；可信评估
中图分类号：TP311　　**文献标志码**：A　　**文章编号**：1001-3695(2012)10-3609-05
doi:10.3969/j.issn.1001-3695.2012.10.003

Survey on trustworthy software evaluation

ZHOU Jian, ZHANG Ming-xin
(*Changshu Institute of Technology*, *Changshu Jiangsu* 215000, *China*)

Abstract: In recent years, software trustworthy evaluation is a new hot research and a tough job in the field of computer science. It contributes to promoting the rejuvenation and development of the software industry through the research of software trustworthy evaluation. Firstly, this paper analyzed the necessity of the software trustworthy evaluation, and then, it summarized the research statue of which mainly included presenting the following four aspects: the credible attributive character, the definition of the credible level of software, the model of software trustworthy evaluation, the implementation plan of software trustworthy evaluation. And at the same time, it also analyzed the insufficient of software trustworthy evaluation in present and the reasons for these insufficient. Finally, it pointed out the trend of software trustworthy evaluation in the future.

Key words: software trustworthy; trustworthy attribute; trustworthy class; trustworthy evidences; trustworthy evaluation

0　引言

当前，以通信、存储和计算为核心的信息基础设施已经渗透到政治、经济、军事、文化和社会生活的各个层面，软件作为信息基础设施的灵魂，在信息社会中发挥着至关重要的作用。日趋庞大的软件需求愈来愈多，复杂度愈来愈高，可用性要求愈来愈强，软件系统却愈来愈脆弱，常常发生各种各样的问题，并对人们的工作生活带来不利的影响，甚至造成巨大的损失[1,2]。例如：1996 年 6 月，软件失效导致欧洲 Ariane 五型火箭首发失败；2003 年 8 月，美国电力检测与控制管理系统的软件失效造成美国东北部大面积停电；2006 年，我国中航信离港系统发生三次软件故障，造成近百个机场值机系统瘫痪……人们发现软件并不总是可以完全信任的，其行为和结果并不完全符合人们的预期，因此，人们对软件的正确性、可靠性、安全性、可生存性等“可信”属性给予了高度关注，这就是所谓的软件可信性问题。

构造可信软件已成为现代软件技术发展和应用的重要趋势和必然选择[1,3]。随着软件规模越来越大，导致软件的开发、集成和维护工作越来越复杂，目前的可信软件构造和可信性度量与评测方法严重缺乏，使得软件产品在推出时就含有很多已知或未知的缺陷，对软件系统的安全可靠运行构成了不同程度的威胁，使得可信问题变得更加突出。

从可信软件的生产和应用的需求出发，软件开发过程中所集成的服务、构件和架构等软件资源以及所开发完成的软件系统是否可信、可信的程度如何，都将成为人们关注的重要问题，而如何确定一个软件是否可信以及如何度量软件的可信程度，则是软件可信评估的主要研究内容[4~6]。

1　软件可信评估中相关的定义

1.1　软件可信的定义

对软件进行可信评估，首先要明确软件可信的内涵，可信计算从出现到现今的发展，已经有三十多年的历史，经历了不同的发展阶段，研究的内容和重点在不断地演变。本世纪初，这一概念还没有形成一个被广泛接受的、良好形式化的定义，可称为 dependability[1,4,7~9]、trustworthiness[2,3,6,10]、high confidence[5,11,12]。

为了得出一个可接受的软件可信性的定义，在 1989 年进行了近六个月的广泛争辩和讨论。出现这种困难的局面是因为许多已存在的组织以不同的方式使用可信性(trustworthiness)这个名词。例如，美国国家计算机安全中心(NCSC)曾经在它的 TCSEC 系统安全方面推出了一个标准，导致许多程序员、工程师和管理者习惯于对可信的认知仅仅局限于安全方面。

收稿日期：2012-04-08；**修回日期**：2012-05-12　　**基金项目**：国家自然科学基金资助项目(61173130)

作者简介：周剑(1981-)，男，江苏常熟人，讲师，硕士，主要研究方向为软件方法学、数据挖掘与知识发现(jzhou1650@163.com)；张明新(1962-)，男，教授，博导，中国计算机学会、电子学会高级会员，甘肃省计算机学会理事，主要研究方向为智能化控制系统、图形图像和视频信息检索、智能信息处理、数据挖掘与知识发现.

另一方面,20 世纪 80 年代末 90 年代初,一些研究成果开始出现,如 Parnas[8] 把“可信性”一词用到不同的方法当中。他们反而关注于在软件开发和维护周期中为了尽可能地减少错误所使用的软件工程技术的程度,如增强测试(enhanced testing)、检查(reviews)和审查(inspection)。安全很少被提到或者根本不提。

TSM[13] 决定考虑安全和软件工程这两者来定义软件可信,即软件满足其一系列需求的可信赖程度。1992 年 Laprie[14] 把恶意代码和入侵等有意缺陷与偶然缺陷并列,丰富了可信性的内涵,并在其著作[15] 中对可信性进行了系统的阐述。

国家“863”重点项目“高可信软件生产工具及集成环境”所提出的软件可信分级规范(TRUSTIE-STC)[7,16] 分析软件系统的行为和用户的期望,得到如下的定义:如果一个软件系统的行为总是与用户预期的行为和结果相一致,则称该软件可信。概括这些定义,软件可信具有两大特点:

a)可信性的最终评估是一个软件可信赖度,这就与参与软件可信评估的个人或者组织的决策有关,具有一定的主观性。

b)软件的可信性与软件需求和用户期望有关,这些需求可能包括功能性的需求和非功能性的需求。

1.2 体现软件可信的属性特征

软件可信属性是软件(客体)获得用户(主体)对其行为实现预期目标的能力信任程度的客观依据。主体通过客体所具有一组表达其可信属性的客观能力事实,从而信任客体的行为能够实现其设定的目标。因此,若软件可信,则意味着软件拥有了一系列与软件可信属性相关的能力;反过来,若软件具有了一系列与软件可信属性相关的能力,则可以相信该软件能达到其预设目标[3]。文献[1,5,6]分别介绍了软件可信属性。

本文中,软件可信属性采用文献[16]的定义,即软件可信属性包括可用性(availability)、可靠性(reliability)、安全性(security)、实时性(real time)、可维护性(maintainability)和可生存性(survivability)。上述每个特性又由若干子特性构成,这些属性构成了软件可信属性模型,如图 1 所示。

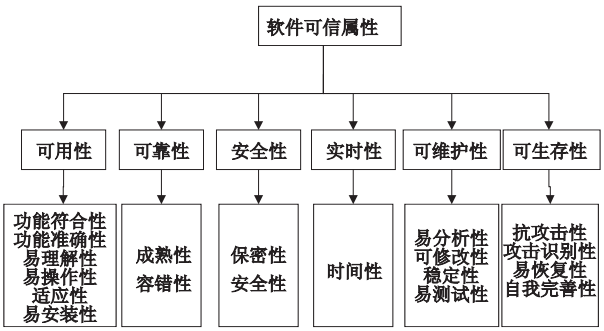

图1 软件可信属性模型

1.3 软件可信证据

软件可信性是主体(用户)的主观感受,软件可信评估是对这种主观感受以分级的方式进行客观表达,是依据软件对可信属性的满足程度进行分级的。而对某种可信属性满足程度的确定,需要依据特定的证据进行。软件所具有的能够反映其某种可信属性的数据、文档或其他信息,称为软件可信证据。一种可信属性可能通过多个可信证据从不同的角度反映出来。一个软件所有可信证据的集合以某种结构进行组织后,就构成了软件可信证据模型,Trustie 小组提出了一种可信证据模型[16],如图 2 所示。

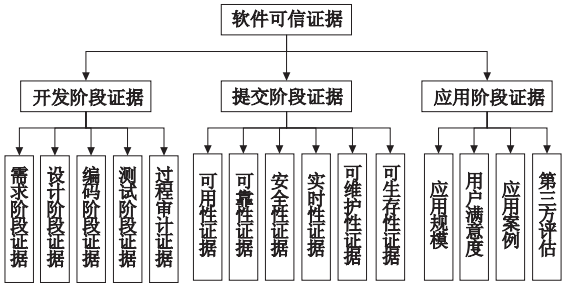

图2 可信证据模型

软件开发阶段的证据是在软件开发中的需求分析、设计以及编码与测试等过程中能够提供的与保障软件可信性相关的一系列证据;软件提交阶段的可信证据是指从软件实体可以获取的可信证据,也称为软件实体证据,这些证据集中体现在软件可信属性模型中的各个特性上,主要通过自动化分析、测试和验证工具,以及人工分析和评估等手段获得;应用阶段证据是在软件实际使用过程中形成的与软件可信性相关的证据。

1.4 软件可信等级的定义

软件可信评估最终的结果是通过可信等级来反映软件可信度的,软件的可信等级是一个有序递进的组合。目前主要的研究成果有:

a)TRUSTIE-STC[16] 基于用户对软件所期望的可信属性的满意程度把软件可信性划分为六个等级:第 0 级(未知级)、第 1 级(可用级)、第 2 级(证实级)、第 3 级(实用级)、第 4 级(评估级)、第 5 级(证明级);并对定义了每个等级的具体内涵,给软件可信评估提供了依据。相对以往软件可信评估中“可信”或者“不可信”的结论更加具体化,针对不同的应用需求用户可以选择不同可信级别的软件。

b)Amoroso 等人[17] 基于软件过程与软件可信规范符合程度,把软件的可信性划分为六个等级:T_0(untrusted)、T_1(minimal trust)、T_2(moderate trust)、T_3(improved trust)、T_4(protected trust)、T_5(trusted)。这种可信等级的划分主要依赖于软件开发过程是否遵循可信规范,从开发过程的角度来对软件可信等级进行划分。

软件可信等级的划分进一步明确了软件可信性的内涵,对软件可信性的评估提供了依据。以上这些定义用非形式化的语言对软件可信的内涵和属性进行了描述,软件的可信评估受软件可信定义和相关属性而驱动的。

软件的可信评估由三部分组成,如图 3 所示。软件可信等级对软件可信级别进行划分,并对每一可信级别的含义进行定义,不同级别表示具有不同程度的可信性。软件可信等级依赖于软件可信属性,软件的可信属性是根据特定的应用需求而确定的,依赖于软件可信证据,每一个可信属性可能有多个可信证据支持。

2 软件可信评估方法

1989 年以来,发达国家的政府组织、跨国公司、大型科研机构逐步认识到可信软件研究的巨大价值和应用前景,开始从不同角度、不同出发点研究与软件可信评估相关的问题,如对可靠性、可用性、安全性和生存性等能够体现软件可信的属性特征进行了必要的研究。可靠性(reliability)[18~20] 关注在规定

的条件和时间间隔内,软件能正常运行的概率;可用性(availability)[21~24]则关注软件在某一时刻所能提供有效功能的程度;安全性(safety)[25~27]则关注软件无论是否完成其预定功能,不会导致意外事故的概率。早期研究软件可信是对单维可信属性进行分析、测试和验证的。但是随着软件应用环境越来越复杂,在评估一个软件的可信性时,需要综合考虑多维可信属性。对于这些属性,并不是一视同仁的。各属性的重要程度取决于系统的应用需求、设计和开发成本、外在环境等多方面的因素。因此,对可信性的度量和评价实际上一个综合评价的过程。

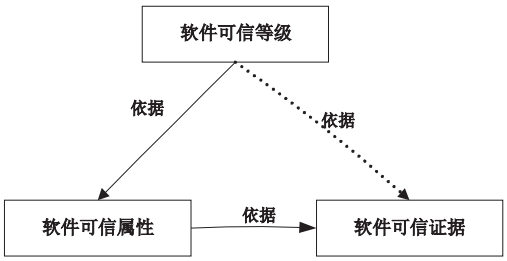

图3　软件可信评估模型

目前,软件可信综合评估主要有两种方法,即面向软件产品(software product)的评估和面向软件过程(software process)的评估。前者是通过分析和测试软件产品,把这些分析和测试的结果作为软件可信评估的证据,最终评估软件的可信度;后者是在软件整个生命周期内,通过分析软件开发过程是否遵循可信规约来评定软件的可信度。

2.1　面向软件产品的评估

现如今,人们所说的软件产品不再仅仅包括源代码和可执行程序,还应包括软件开发过程中相应的文档、状态报告、用户手册等[28~30]。这就要求面向软件产品的评估不仅仅测试软件源代码和软件功能,还要对软件产品中的其他内容进行分析和测试。

目前,面向软件产品的评估主要从分析软件产品属性和软件产品行为两个角度来进行评估。

2.1.1　基于软件产品的可信属性进行评估

基于软件产品的可信属性评估原理[31,32],首先分析软件的需求,获得软件所关注的可信属性;其次利用测试分析工具对软件产品进行测试和分析,获得大量直接有用的信息作为软件可信的证据,如代码测试、功能测试、可靠性分析等;最终融合大量的证据来评估软件的可信度。其模型如图 4 所示。

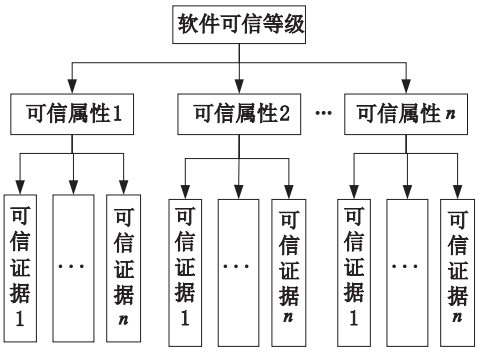

图4　基于软件产品可信属性的评估模型

在这方面的主要研究成果有

Voas[9]提出的软件可信根据功能需求的不同,它可以分成以下子属性,即可靠性(R)、性能(P)、容错性(F)、安全性(Sa)、机密性(Se)、可用性(A)、可测试性(T)和可维护性(M);他还强调了软件的可信性度量和评价实际是一个综合评价的过程,可以用下式表示:

$$Q = aR + bP + cF + dSa + eSe + gT + fA + hM$$

其中:Q 表示一个软件的可信性,a、b、c、d、e、f、g、h 表示软件可信属性的权重,此权重是由设计人员或最终用户根据应用需求等因素而作出的权衡。对各属性的强调强度与侧重点的不同直接影响到系统的可信性。然而当各属性彼此之间相互依附或者相互矛盾时,用此方法就很难准确地度量软件的可信性了。

Ding 等人[33]参照 Voas 提出的可信评估方法,设计出获得可信属性权重的 OWG 算法,该算法的主要思想是聚合多个专家意见来得到属性的权重信息,实质是一个专家评估系统。

杨仕平等人[8]在高可信软件的防危性评估研究一文中,在分析安全关键软件防危性测评的必要性基础上,提出了适合于评估关键软件防危性的评估指标,给出了防危性评估指标与可靠性评估指标之间的关系,总结了四种传统测评方法评估高防危性需求软件的局限性,研究了基于重要性采样及压力测试技术测评高防危性软件的可行性。该方法从软件安全性和可靠性这两点出发,对软件可信性进行评估。该方法适合于高防危性软件的评估。

杨善林等人[31]提出了一种基于效用和证据理论的可信软件评估方法。该方法首先设计了一个需求驱动的可信指标树动态构造模型——开放式可信指标数据库和指标树生成算法;利用专家给出的效用值构造效用函数来对软件的可信指标进行度量;最后利用 Dempster 合成规则对可信证据进行合成。该方法改变了以往从单一可信属性[15,17,18,21,34,35]来对软件进行评估,而是通过分析应用需求获得软件关注的可信属性,具有很大的灵活性。

基于软件可信属性的评估目前也仅是处于实验阶段,还有很多亟待解决的问题:

a)如何从软件需求映射到软件的可信属性。

b)软件可信属性对软件可信的影响程度不一样,如何权衡这些属性。当这些属性相互依附或相互矛盾时,又如何去权衡。

c)软件可信证据如何映射到软件可信属性上。可信证据对可信属性的影响也是不一样的,如何去权衡,如何去合成这些可信证据,可信证据本身具有不确定性,在可信评估当中如何去体现。

2.1.2　基于软件产品的行为进行评估

基于软件产品行为进行评估的原理:首先根据 TCG 对可信性的定义以及动作、行为定义,将软件用途中所规定的动作,即用户使用此软件的目的进行分解,得到由动作组成的软件可信路径图;然后根据软件的实际运行过程进行分解,得到由动作组成的软件实际行为路径图;最后将实际运行的软件行为与软件可信行为进行拟合度分析来对软件可信性进行度量。

王慧强等人[19]提出一种基于 Pi 演算和拟合度分析的自律软件可信性度量方法,改变了以往从软件可信属性这个角度来度量软件的可信性,根据 Pi 演算工具分别对行为路径上的动作进行形式化的描述,最后将实际运行的软件行为与软件可信行为进行拟合度分析,根据自律软件可信性度量算法对软件可信性进行度量。软件的行为路径如图 5 所示。

2.2　面向软件过程的评估

基于软件产品评估的最大好处就是能过通过测试获得支

持软件可信度的大量证据。其最大的问题是:在软件测试过程中,由于有些软件缺陷隐藏得比较深而被忽略,这将直接影响软件可信评估的可靠性。然而,面向过程的可信评估是在软件的整个生命周期内对不同阶段进行可信性度量,最终来确定软件的可信度。

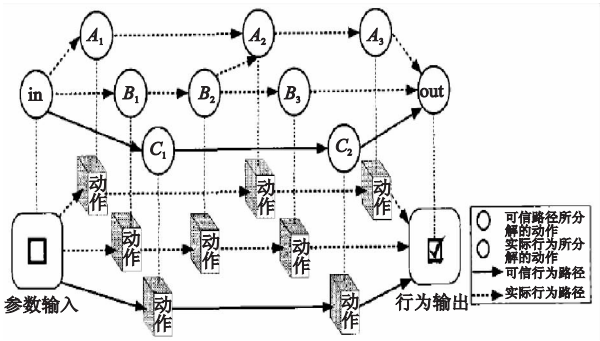

图5 软件行为所对应的软件可信行为路径和实际运行行为路径

目前主要的研究成果有:

Amoroso 等人[17]提出一种面向过程的软件可信评估方法,他们首先制定了软件开发过程中的 44 个可信规约(principle),然后通过分析软件在开发过程遵循或违背了哪些规约来度量软件的可信度。该方法最大的好处就是通过分析可信规范的匹配度降低了可信评估过程中主观因素的影响,但是仍然存在很多的问题:软件可信等级与可信规约符合度的映射关系很难确定;它们要求可信规约之间相互独立,但是实际情况很难做到这一点,规约之间具有一点的依附关系;可信规约对软件可信度的影响不同,可信规范的权重问题很难确定,可能存在一个关键的可信规范对软件的可信度影响特别大。

Li 等人[36]提出软件整体的可信性取决于软件整个生命周期中各个阶段的可信性,因此提出了一种在软件生命周期中基于不信任因素(distrustable factors)的可信评估模型,如图 6 所示。

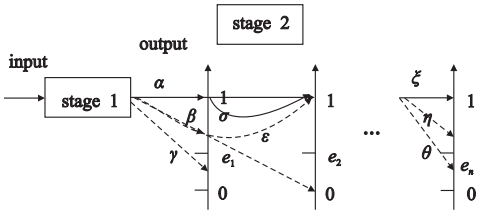

图6 基于软件过程的可信模型

该方法技术方案为:从软件开发第一个阶段(需求分析阶段)进行可信性的评估,每一个阶段的可信度作为下一个阶段的可信性评估的输入,最终评定软件的可信性。

钱红兵等人[37]提出了一种面向测试过程的软件可信评估方法。该方法从管理阶段可信、过程阶段可信以及软件最终产品可信三维角度来度量和评估软件的可信性,最终利用 Dempster 合成公式对可信指标进行合并,最终得到软件的可信性评估指标。

3 软件可信评估研究存在的不足

尽管经过可信评估人员不懈努力,使得软件可信评估从最初的萌芽逐步发展起来并取得了相当的成果,但是从软件可信评估的实际应用状况来看,还处在探索阶段,还远未达到人们所期待的普及状态,在实际应用当中可操作性差。产生这种状况的原因主要有以下几点:

a)缺乏相应的规范和标准,即缺乏对软件可信性度量的统一定义和准确说明。现有软件可信性评估方法的评估结果大多是一个 0 和 1 之间的值或可信/不可信的简单定论,该结果与软件可信度之间的关系是不精确且不统一的。

b)目前很多可信评估的研究都是单独分析软件可信属性,之后再简单地组合在一起的。然而可信属性相互之间是有关系的,Hasselbring 等人[38]把可信属性之间的关系分为两种:a)内在关系,即属性之间相互影响,比如病毒攻击被认为是软件安全的威胁,实质上它们攻击的是软件的可用性,因此,安全可以认为是软件可用的一部分;b)外在关系,即软件属性之间有时会产生相互冲突,比如追求软件的高安全性或者高可靠性会影响软件实时性,这个时候可靠性和实时性之间的关系就是外在关系。

c)在软件可信评估中所用到的软件可信证据不充分,缺少一种方法或者技术来获得和度量能够反映某种软件可信属性的可信证据。软件可信评估是一个动态的过程,随着软件可信证据增多,软件可信度趋于稳定。因此,充分的软件可信证据能够更加真实可靠地证明软件的可信性。

d)软件可信评估缺少对不确定信息的处理,有的软件的可信证据具有模糊性,如用户对软件的评价。虽然在有些研究成果中用到了 DS 证据理论来处理不确定信息,但却没有考虑证据之间的冲突问题和证据本身的可信性问题。

4 软件可信评估面临的挑战

为了对软件实体的可信状态进行客观的判断,软件的可信评估需要解决以下问题:

a)建立可信软件评估的技术标准或规范,对软件可信性以及软件的可信等级进行明确定义,为软件可信评估提供依据。

b)对软件可信性建模,对于可信软件,需要考虑包括可用性、可靠性、安全性等诸多属性的综合度量空间,形成对软件可信性的科学理解,以定量的方式给出可信性建模的系统方法论。

c)研究多维可信属性的多尺度量化指标系统、获取、度量和评估机制及测评体系;同时要研究可信属性之间的交互关系及可能涌现的特征,包括多个属性/综合属性的局部/全部相容与失配情况。

d)研究软件可信证据模型,包括软件可信证据的获取和度量方法的研究、软件可信证据如何映射到可信属性的研究以及软件可信证据融合技术的研究。

e)软件可信性的动态演化特征的研究,随着软件可信证据的增多,软件的可信性趋于稳定。

5 结束语

软件的使用已渗透到经济民生和国防军事等重要部门,人们对软件安全的依赖程度越来越高,因而对于其可信性的要求也越来越高。软件可信性度量已引起了学术和产业界的高度关注,可信评估经过近几年的研究与发展,在一些关键技术上取得了进展和突破,出现了一些软件可信评估原型系统。通过对软件可信评估研究现状的分析,可以得出以下结论:

a)总的来说,软件可信性评估研究还处于初期探索阶段,还没有形成具有普遍适用性的基础理论体系。无论是学术界还是产业界,对可信评估方法的认识还没有统一,缺乏切实可行的可信评估规范和标准。

b)软件可信评估是个复杂的综合过程,软件可信属性、可信证据等还需要进一步深入的研究。

参考文献:

[1] 陈火旺. 高可信软件工程技术[J]. 电子学报,2003,31(12A):1933-1938.

[2] SIEWIOREK D,杨孝宗. 可信计算的产业趋势和研究[J]. 计算机学报,2007,30(10):1645-1661.

[3] 闵应骅. 可信系统与网络[J]. 计算机工程与科学,2001,23(5):21-23.

[4] 周明天,谭良. 可信计算及其进展[J]. 电子科技大学学报,2006,35(4):686-697.

[5] 林闯,彭雪海. 可信网络研究[J]. 计算机学报,2005,28(5):751-758.

[6] 熊光泽,常政威,桑楠. 可信计算发展综述[J]. 计算机应用,2009,29(4):1001-1010.

[7] IMMONEN A, PALVIAINEN M. Trustworthiness evaluation and testing of open source components[C]//Proc of the 7th International Conference on Quality Software. 2007:361-321.

[8] 杨仕平,熊光泽,桑楠,等. 可信软件的防危性评估研究[J] 计算机工程与设计,2004,25(2):161-165.

[9] VOAS J. Trusted software's holy grail[J]. Software Quality Journal,2003,11(1):9-17.

[10] HUA Zhong-sheng, GONG Ben-gang, XU Xiao-yan. A DS-AHP approach for multi-attribute decision making problem with incomplete information[J]. Expert Systems with Applications,2008,34(3):2221-2227.

[11] 刘克,单志广,王戟,等. 可信软件基础研究重大研究计划综述[J]. 中国科学基金,2008,22(3):145-151.

[12] ZENG Jin, SUN Hai-long, LIU Xu-dong, *et al*. Dynamic evolution mechanism for trustworthy software based on service composition[J]. Journal of Software,2010,21(2): 261-276.

[13] WANG Hai-min, LIU Xu-dong, XIE Bing. Software trustworthiness classification specification(TRUSTIE-STC V 2.0)[EB/OL]. (2009). http://www.trustie.net/clinks/trustiecriterion.jsp.

[14] ALGIRDAS A, JEAN-CLAUDE L, BRIAN R, *et al*. Basic concepts and taxonomy of dependable and secure computing[J]. IEEE Trans on Dependable and Secure Computing,2004,1(1):11-13.

[15] WANG Huai-min, TANG Yang-bin, YIN Gang, *et al*. Trustworthiness of Internet-based software[J]. Science in China Series F: Information Sciences,2006,49(6):759-773.

[16] Trustie Group. A trustworthy software production environment for large scale software resource sharing and cooperative development [EB/OL]. (2008). http://www.trustie.org.

[17] AMOROSO E, TAYLOR C, WATSON J, *et al*. A process-oriented methodology for assessing and improving software trustworthiness [C]//Proc of the 2nd ACM Conference on Computer and Communications Security. New York: ACM,1994:39-50.

[18] YANG Shi-ping, XIONG Guang-ze, SANG Nan, *et al*. Research on safety evaluation of high dependable software[J]. Computer Engineering and Design,2004,25(2):161-165,169.

[19] 王慧强,赵倩,吕宏武,等. 基于 Pi 演算和拟合度分析的自律软件可信性度量方法:中国,CN200910071286.1[P]. 2009-06-24.

[20] 丁学雷,王怀民,王元元,等. 面向验证的软件可信证据与可信评估[J]. 计算机科学与探索, 2010,4(1):52-58.

[21] JIANG Le-tian, XU Guo-zhi, YING Ren-dong, *et al*. Techniques of system reliability and availability analysis[J]. Telecommunication Engineering,2002,42(4):121-126.

[22] 杨静. 软件可信性评估工具的研究与实现[D]. 西安:西北大学,2009.

[23] LI Ning-hui, MITCHELL J C, WINSBOROUGH W H. Design of a role-based trust management framework[C]//Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society,2002:114-130.

[24] 李红霞. 软件可信度量研究初探[D]. 重庆:重庆大学,2005.

[25] BAO Tie, LIU Shu-fen, WANG Xiao-yan, *et al*. A software trustworthiness evaluation model based on level mode[J]. Communications in Computer and Information Science,2011,159(3):154-159.

[26] DU Rui-zhong, ZHANG Fang. A trust model based on check point behaviors risk evaluation [J]. Advanced Materials Research, 2101,403-408:2102-2106.

[27] SHI Li, YANG Shan-lin, LI Kai, *et al*. Developing an evaluation approach for software trustworthiness using combination weights and TOPSIS[J]. Journal of Software, 2012,7(3):532-543.

[28] ZHU Ming-xun, LUO Xin-xing, CHEN Xiao-hong, *et al*. A non-functional requirements tradeoff model[J]. Trustworthy Software, Information Sciences,2012,191(15):61-71.

[29] DING Shuai, MA Xi-jun, YANG Shan-lin. A software trustworthiness evaluation model using objective weight based evidential reasoning approach[J]. Knowledge and Information Systems,2011.

[30] IMMONEN A, NISKANEN A. A tool for reliability and availability prediction[C]//Proc of the 31st Euromicro Conference on Software Engineering and Advanced Applications. Washington DC: IEEE Computer Society. 2005:416-423.

[31] 杨善林,丁帅,褚伟. 一种基于效用和证据理论的可信软件评估方法[J]. 计算机研究与发展,2009,46(7):1152-1159.

[32] LIU Hao. Development and method of software availability [J]. Communications World,2005(14):46-46.

[33] DING Shuai, YANG Shan-lin. Research on evaluation index system of trusted software[C]//Proc of the 4th International Conference on WiCOM. 2008:1-4.

[34] BAO Tie, LIU Shu-fen, WANG Xiao-yan. Research on trustworthiness evaluation method for domain software based on actual evidence [J]. Chinese Journal of Electronics,2011,20(2):824-851.

[35] ZHANG Yue-jin, ZHANG Yan-mei, HAI Mo. An evaluation model of software trustworthiness based on fuzzy comprehensive evaluation method[J]. American Journal of Engineering and Technology Research,2011,11(9):1145-1149.

[36] LI Meng, ZHOU Xian-zhong, WANG Jian-jun, *et al*. A perspective of software trustworthiness based on distrustable factors[C]//Proc of IEEE International Conference on Networking, Sensing and Control. 2009:873-878.

[37] 钱红兵. 晏海华,张茂林,等. 一种面向测试过程的软件可信性度量与评估方法:中国,CN200910082587.4[P]. 2009-10-07.

[38] HASSELBRING W, REUSSNER R. Toward trustworthy software systems[J]. IEEE Computer,2006,29(4): 91-92.

[39] National Science and Technology Council(U.S). High confidence software and systems research needs[M]. [S.l.]: National Science Technology Council,2001:43.

[40] RAWASHDEH A, MATALKAH B. A new software quality model for evaluating COTS components[J]. Journal of Computer Science, 2006,2(4):373-381.

[41] JIANG Hai-miao. A study on software usability analysis and evaluate methods and tools[D]. Daliau: Dalian Maritime University,2004.