给出了具体的实现方案和评估工具 CoCoFlow.

面向商用成品 COTS 的选择:文献[43]提出了一种基于产品领域的间接选取方法,并在一个在线贸易系统中加以应用,结果表明,该方法比传统的直接选取方法更有效.文献[44]提出了一种软件功能需求驱动的评估和选择 COTS 构件的方法,首先将功能需求分解到每一个模块,再基于每一个模块识别出候选的构件,根据给定的评估模板对构件的可用性、易用性进行评估,最后求解构件给定成本约束下的最优组合.文献[15]提出一种基于差异分析的构件评估方法,通过分析构件与需求在功能性上的差异度选择构件.

对于开源软件的评估有若干主要的评估模型和方法,如 OSMM[45](open source maturity model)、QSOS[46](qualification and selection of open source software)、OpenBRR[47](open business readiness rating)等.这些评估模型和方法总体思路比较类似,首先定义质量属性模型(包含若干属性/子属性),其次收集原始评估数据并获得度量,依据一个计算模型(如乘权求和)由度量计算出属性.这里,以 OpenBRR 为例作一说明:OpenBRR 是由 Carnegie Mellon Silicon Valley Center 与 Intel 等公司联合发起的,采用了 12 个开源软件的属性分类(categories),如功能、质量、性能、支持度、社区、文档等,通过采集规范化的度量,计算获得每个分类,最终将所有分类乘权求和得到最终的 BRR 分级.总体上,这些评估模型和方法兼顾了通用性和开源软件的部分特点(如支持度、社区).但由于其属性模型扁平化,且计算模型相对简单,标度多采用离散的分级(如 1~5 级),使其对于其他较为复杂的软件和领域的适用性有所不足.

文献[48]通过可信证据的成熟度计算可信属性的可满足性,并根据可满足性裁剪软件可信属性,然后,基于该可信属性对 CPS 系统进行建模与评估.文献[49]研究了作战仿真系统的可信性,结合实际建立了一套可信性评估指标体系,提出了专家权重定量计算方法.文献[50]在综合分析电力系统的特点和可信需求后,从系统构建、实施过程管理、可信评估和可信证明这 4 个方面对如何构建可信的电力系统进行了研究.文献[51]针对作战飞机的任务效能评估问题,提出了自己的解决方案.文献[52]研究 Web 服务的可信性问题,从可用性、可靠性和安全性这 3 个方面对 Web 服务的可信性进行评估,给出了具体评估标准和算法.文献[53]针对开源构件可信性进行了评估.文献[54]在分布式数据库服务器系统 DDSS(distributed database server system)中引入可信机制,通过建立多层次信任链结构,改进存取控制方式,加强客户端角色管理、认证机制等技术,一定程度上提高了 DDSS 系统的可信性.文献[55]提出了适用于无线传感网络的可信评估模型.文献[56]给出了评估工作流型软件产品可信性的关键指标.文献[57]引入相关度的概念来评估面向服务的工作流的性能.文献[58]提出了使用形式化验证技术来验证时序安全属性,以提高医疗设备软件的可信性.

可见,针对特定领域的可信评估呈现出明显多样性的特征.即添加了特定领域的知识,并采纳了定制的度量和决策标准等,使之更专有、更具体,但不易迁移使用.

3.3 可信评估工具

软件可信评估工具对于可信评估的实施至关重要,然而,由于可信评估面临的应用领域众多,关注的质量属性侧重点不同,评价的标准变化,证据收集困难等,使得工具的实现具有一定的难度.

文献[40]设计并实现了一个基于 Java 的软件可信评估工具 SPATRUME,采用针对文献[38]改进的属性度量值计算模型,具有通用性,可能的不足之处在于缺乏证据信息以及属性度量值与证据的关联关系.北京航空航天大学设计并实现了“可信软件结构及代码的审查和综合评估及支持工具”[26],具有比较完整的软件质量(在代码及结构方面)分析与度量功能以及初始的可信评估能力,但并未深入关注评估.北京大学开发了软件资源库[16],可针对软件系统、构件、服务进行发布、检索,并管理可信证据,另外还包括可信分级的描述以及软件可信评估功能.软件可信评估过程包括发布者提供证据信息,交由专家人工评定可信级别.软件资源库系统可以辅助软件可信评估,但并不提供评估定制功能,且专家评定具有一定的主观性,对可信分级与证据间的关联关系表达有一定的欠缺.南京航空航天大学设计并实现了“软件可信评估管理工具”[27],该工具提供了可信评估元建模能力,因此是领域无关的,可提供完整的评估定制能力,并可根据领域特性定制属性模型和证据模型,并依据分级体系自动生成评估结果.另外,该工具还实现了与北京大学资源库系统的连接,实现了两个系统中资源信息、证据包的数据交换.上述工具主要适用于通用领域或应用场景,具有较为普遍的通用性,并在一定程度上具备经过定制

用于特定领域的能力.

文献[28]在提出可信度层次评估过程模型的基础上,设计实现了一个针对仿真系统的可信评估工具HIT-CET.文献[29−31]均针对业务流程管理系统(BPMS),实现了软件可信评估的管理工具.其中,文献[29]提出了一个完整的领域构件可信评估体系,并在此基础上实现了领域构件可信评估系统的开发;文献[30]提出了可信指标体系、评估过程模型及算法模型,并设计实现了适用于BPMS软件可信评估的管理工具;文献[31]提出了一种在管理设置阶段对过程设计的创建和评价提供指导的启发式方法.上述工具主要适用于特定的领域或应用场景,具有较强的针对性.

4 结束语

安全攸关软件的可信性关乎生命安全和财产保全,因此,相应的软件可信评估至关重要.软件可信评估从主观和客观两个方面度量软件的质量,对软件生产和应用有着重要的意义.本文重点关注软件可信评估的管理,综合分析、对比了目前可信评估的研究现状,从相关标准、评估涉及的模型(包括质量属性模型、证据模型、分级规范等)以及软件工具支持等方面综述了软件可信评估研究工作.

总体上看,软件可信评估取得了大量研究成果,在理论(模型和框架)上分两个层面展开,第 1 层是具有通用性、领域无关的模型/元模型,第2层是在前一层的基础上,对通用模型/元模型进行定制或实例化,以满足不同领域、不同软件形态、不同使用环境的实际需求.此外,针对理论成果开发出相应的工具,用于辅助实际的软件可信评估过程管理,为研制出高可信软件提供技术保障和支持.

未来主要关注的发展方向包括:如何将可信评估向更专有的领域、更特定的应用去发展,并适用于不同软件形态和不同的运行环境;如何表示可信证据/可信属性在软件工程的各阶段(从需求到设计、编码、测试、维护)之间的追踪关系,以及它们对于可信标准的依从性.

致谢 在此,我们向对本文工作给予支持和提出宝贵建议的同行表示感谢.尤其要感谢在国家863计划“高可信软件生产工具及集成环境”专题中有课题合作的北京大学计算机科学技术系赵俊峰、张伟副教授、复旦大学计算机科学技术学院的赵文耘教授、彭鑫副教授.感谢南京航空航天大学计算机学院钱巨副教授、刘春勇、洪宏、彭焕峰等同志对可信评估工具开发付出的努力.另外,还要感谢神州数码信息系统有限公司的徐拥军执行总监,他们对于评估工具的应用案例提出了很多宝贵的意见.

References:

[1] Athalye P, Maksimovic D, Erickson R. High-Performance front-end converter for avionics applications. IEEE Trans. on Aerospace and Electronic Systems, 2003,39(2):462−470. [doi: 10.1109/TAES.2003.1207258]

[2] Final Report on the accident flight AF 447 Rio de Janeiro-Paris. BEA, 2012. http://www.bea.aero/docspa/2009/f-cp090601.en/pdf/f-cp090601.en.pdf

[3] Wu WH, Kelly T. Safety tactics for software architecture design. In: Proc. of the 28th Annual Int’l Computer Software and Applications Conf. 2004. [doi: 10.1109/CMPSAC.2004.1342860]

[4] NSTC. Research challenges in high confidence systems. In: Proc. of the Committee on Computing, Information and Communications Workshop. 1997. http://www.hpcc.gov/pubs/hcs-Aug97/intro.html

[5] Gates B. Trustworthy computing. 2002. http://www.wired.com/2002/01/bill-gates-trustworthy-computing/

[6] TCG. Specification architecture overview specification. Revision 1.4.2nd, 2007.

[7] Wang HM, Tang YB, Yin G, Li L. Credible mechanism of Internet software. Science in China-Series E: Information Sciences, 2006,36(10):1156−1169 (in Chinese with English abstract).

[8] ISO/IEC 15408-1:2009. Information technology-security techniques-evaluation criteria for IT security. Part1: Introduction and General Model, 2009.

[9] ISO/IEC 25010:2011: Systems and software engineering—Systems and software quality requirements and evaluation (SQuaRE)—System and software quality models. 2011.

[10] Avizienis A, Laprie JC, Randell B, Landwehr C. Basic concepts and taxonomy of dependable and secure computing. IEEE Trans. on Dependable and Secure Computing, 2004,1(1):11−33. [doi: 10.1109/TDSC.2004.2]

[11] Lin C, Peng XH. Research on trustworthy networks. Chinese Journal of Computers, 2005,28(5):751−758 (in Chinese with English abstract).

[12] Wang HM, Yin G. Evolution of software trustworthiness in the network age. Communication of China Computer Federation, 2010,6(2):28−34 (in Chinese with English abstract).

[13] Fan XG, Chu WK, Zhang FM. Surveys of software safety. Computer Science, 2011,38(5):8−13 (in Chinese with English abstract).

[14] Liu K, Shan ZG, Wang J, He JF, Zhang ZT, Qin YW. Overview on major research plan of trustworthy software. Bulletin of National Natural Science Foundation of China, 2008,22(3):145−151 (in Chinese with English abstract).

[15] Mei H. Software credibility: Internet brings challenges. China Computer Federation, 2010,6(2):20−27 (in Chinese with English abstract).

[16] Cai SB, Zou YZ, Shao LS, Xie B, Shao WZ. Framework supporting software assets evaluation on trustworthiness. Ruan Jian Xue Bao/Journal of Software, 2010,21(2):359−372 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3786.htm [doi: 10.3724/SP.J.1001.2010.03786]

[17] Yang SL, Ding S, Chu W. Trustworthy software evaluation using utility based evidence theory. Journal of Computer Research and Development, 2009,46(7):1152−1159 (in Chinese with English abstract).

[18] Liu XD, Lang B, Xie B, Wang HM. Software trustworthiness classification specification (TRUSTIE-STC V 2.0). In: High Confidence Software Production Tools and Integrated Environment Technical Documentation. 2009. http://www.doc88.com/p-3008711993507.html

[19] Lu G, Wang HM, Mao XG. A cognitive-based evidence model for software trustworthiness evalution. Journal of Nanjing University (Natural Sciences), 2010,46(4):456−463 (in Chinese with English abstract).

[20] Ding XL, Wang HM, Wang YY, Lu G. Verification oriented trustworthiness evidence and trustworthiness evaluation of software. Journal of Frontiers of Computer Science and Technology, 2010,4(1):46−53 (in Chinese with English abstract).

[21] Voas J. Trusted software's holy Grail. Software Quality Journal, 2003,11(1):9−17. [doi: 10.1023/A:1023679926998]

[22] Ding S, Yang SL. Research on evaluation index system of trusted software. In: Proc. of the 4th Int'l Conf. on WiCOM. 2008. 1−4. [doi: 10.1109/WiCom.2008.1869]

[23] Amoroso E, Taylor C, Watson J, Weiss J. A process-oriented methodology for assessing and improving software trustworthiness. In: Proc. of the 2nd ACM Conf. on Computer and Communications Security. New York: ACM, 1994. 39−50. [doi: 10.1145/191177.191188]

[24] Qian HB, Yan HH, Zhang ML,Yang HY, He ZT, Zhu XJ. A test-oriented software measurement and evaluation method. China, CN200910082587.4, 2009 (in Chinese).

[25] Mohamed A, Ruhe G, Eberlein A. COTS selection: Past, present, and future. In: Proc. of the 14th Annual IEEE Int'l Conf. and Workshops on the Engineering of Computer-Based Systems. 2007. 103−114. [doi: 10.1109/ECBS.2007.28]

[26] Liu C. Comprehensive review and assessment of the structure and code of trusted software and support tools. China Science and Technology Achievements, 2010,11(16):21−22 (in Chinese with English abstract).

[27] Shen GH, Huang ZQ, Qian J, Xu YJ, Hao J, Zhao WY, Peng X. Research on software trustworthiness evaluation model and its implementation. Journal of Frontiers of Computer Science & Technology, 211,5(6):553−561 (in Chinese with English abstract).

[28] Qin LG, Yang M, Fang K. Research on the simulation credibility evaluation assistant tool based on hierarchical evaluation. Computer Simulation, 2010,27(6):118−121 (in Chinese with English abstract).

[29] He JS. Research and implementation of BPM field component credible evaluation system [MS. Thesis]. Xi'an: Northwestern University, 2010 (in Chinese with English abstract).

[30] Yang J. Research and implementation of software credibility assessment tools [MS. Thesis]. Xi'an: Northwestern University, 2010 (in Chinese with English abstract).

[31] Van der Feesten I, Reijers HA, van der Aalst WMP. Evaluating workflow process designs using cohesion and coupling metrics. Computers in Industry, 2008,V01.59:420−437. [doi: 10.1016/j.compind.2007.12.007]

[32] Jiang R. A trustworthiness evaluation method for software architectures based on the principle of maximum entropy (POME) and the grey decision-making method (GDMM). Entropy, 2014,16(9):4818−4838. [doi: 10.3390/ e16094818]

[33] Wang HM, Tang YB, Yin G. Trustworthiness of internet-based software. Science in China-Series F: Information Sciences, 2006,49(6):759−773. [doi: 10.1007/s11432-006-2024-4]

[34] Viljanen L. Towards an ontology of trust. In: Proc. of the 2nd Int'l Conf. on Trust, Privacy and Security in Digital Business (TrustBus 2005). 2005,3592:175−184. [doi: 10.1007/11537878_18]

[35] Zhang LG, Zhang HG, Zhang F. The amount of credibility mechanism in turstede computing. Journal of Beijing University of Technology, 2010,36(5):586−591 (in Chinese with English abstract).

[36] Yuan L, Wang HM, Yin G, Shi DX, Mi HB. A role-based software credible assessment techniques. Journal of Beijing University of Technology, 2010,36(5):611−615 (in Chinese with English abstract).

[37] Zhang YJ, Zhang YM, Hai M. An evaluation model of software trustworthiness based on fuzzy comprehensive evaluation method. American Journal of Engineering and Technology Research, 2011,11(9):1145−1149.

[38] Tao HW, Chen YX. A metric model for trustworthiness of softwares. In: Proc. of the 2009 IEEE/WIC/ACM Int'l Conf. on Web Intelligence and Intelligent Agent Technology. 2009. 69−72. [doi: 10.1109/WI-IAT.2009.233]

[39] Liu YZ, Luo X, Xue K, Luo P. A metric model research based on attributes for trustworthiness of software. Computer Science and Application, 2012,2:121−125 (in Chinese with English abstract).

[40] Zhang LW, Zhou Y, Chen YX, Zhang M, Zhang JY. Stability of software trustworthiness measurements models. In: Proc. of the 7th Int'l Conf. on Software Security and Reliability Companion. 2013. 219−224. [doi: 10.1109/SERE-C.2013.23]

[41] Pedraza-Garcia G, Astudillo H, Correal D. Modeling software architecture process with a decision-making approach. The Jornadas Chilenas de Computación (JCC2014), 2014. http://www.jcc2014.ucm.cl/jornadas/WORKSHOP/WBPM%202014/WBPM-6.pdf

[42] Delgado A, Ruiz F, García-Rodríguez de Guzmán I, Piattini M. MINERVA: Model drIveN and sErvice oRiented framework for the continuous business process improVement and relAted tools. In: Dan A, Gittler F, Toumani F, eds. Proc. of the ICSOC/Service Wave 2009. LNCS 6275, 2010. 456−466. [doi: 10.1007/978-3-642-16132-2_43]

[43] Leilng KRPH, Leung HKN. On the efficiency of domain based COTS product selection method. Information and Software Technology, 2002,44:703−715. [doi: 10.1016/S0950-5849(02)00118-0]

[44] Sheng JF, Chen SQ, Wang B. Software requirements-driven COTS evaluation. Computer Engineering, 2005,(24):99−101 (in Chinese with English abstract).

[45] Golden B. Succeeding with Open Source. Reading: Addison-Wesley Professional, 2004.

[46] Semeteys R, Pilot O, Baudrillard L, Le Bouder G, Pinkhardt W. Qualification and selection of open source software (QSOS), Version 2.0. Technical Report, Atos Origin, 2013.

[47] OpenBRR. Business Readiness Rating for Open Source. A Proposed Open Standard to Facilitate Assessment and Adoption of Open Source Software, Request for Comments, 2005.

[48] Rong M. A model for CPS software system trustworthiness evaluation based on attributes classifying. In: Proc. of the 8th Int'l Conf. on Computer Science & Education (ICCSE 2013). 2013. 1309−1314. [doi: 10.1109/ICCSE.2013.6554124]

[49] Tang JB. Research on credibility of warfare simulation system [Ph.D. Thesis]. Changsha: University of Defense Technology, 2009 (in Chinese with English abstract).

[50] Bao T, Liu SF, Wang XY. Research on a trusted construction method for electric power production management system. Acta Electronica Sinica, 2010,38(9):2166−2171 (in Chinese with English abstract).

[51] Zhang JK, Cheng L, Huang J, Wu Z. Mission-Based operational effectiveness evaluation model of combat aircraft. Journal of Beijing University of Aeronautics and Astronautics, 2005,31(12):1279−1283 (in Chinese with English abstract).

[52] Wang XL, Wang HW. Requirements for trust evaluation of Web services. Computer Systems & Applications, 2009,(4):36−39 (in Chinese with English abstract).

[53] Palviainen IM. Trustworthiness evaluation and testing of open source components. In: Proc. of the 7th Int'l Conf. on Quality Software (QSIC 2007). 2007. [doi: 10.1109/QSIC.2007.4385514]

[54] Tian JF, Xiao B, Ma XX, Wang ZX. The trust model and its analysis in TDDSS. Journal of Computer Research and Development, 2007,44(4):598−605 (in Chinese with English abstract). [doi: 10.1360/crad20070408]

[55] Hur J, Lee Y, Yoon H, Choi D, Jin S. Trust evaluation model for wireless sensor networks. Advanced Communication Technology, 2005,491−496. [doi: 10.1109/ICACT.2005.245914]

[56] Perez M, Rojas T. Evaluation of workflow-type software products: A case study. Information and Software Technology, 2000,V01.42:489−502. [doi: 10.1016/S0950-5849(00)00093-8]

[57] Liu B, Fan YS. Service-Oriented workflow performance evaluation and correlation analysis for key performance indicators. Computer Integrated Manufacturing Systems, 2008,14(1):160−165 (in Chinese with English abstract).

[58] Li CX, Raghunathan A, Jha NK. Improving the trustworthiness of medical device software with formal verification methods. Embedded Systems Letters, 2013,5(3):50−53. [doi: 10.1109/LES.2013.2276434]

附中文参考文献:

[7] 王怀民,唐扬斌,尹刚,李磊.互联网软件的可信机理.中国科学(E 辑),2006,36(10):1156−1169.

[11] 林闯.可信网络研究.计算机学报,2005,28(5):751−758.

[12] 王怀民,尹刚.网络时代的软件可信演化.中国计算机学会通讯,2010,6(2):28−34.

[13] 樊晓光,褚文奎,张凤鸣.软件安全性研究综述.计算机科学,2011,38(5):8−13.

[14] 刘克,单志广,王戟,何积丰,张兆田,秦玉文.“可信软件基础研究”重大研究计划综述.中国科学基金,2008,22(3):145–151.

[15] 梅宏.软件可信性:互联网带来的挑战.中国计算机学会通讯,2010,6(2):20–27.

[16] 蔡斯博,邹艳珍,邵凌霜,谢冰,邵维忠.一种支持软件资源可信评估的框架.软件学报,2010,21(2):359–372. http://www.jos.org.cn/1000-9825/3786.htm [doi: 10.3724/SP.J.1001.2010.03786]

[17] 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.计算机研究与发展,2009,46(7):1152–1159.

[18] 刘旭东,郎波,谢冰,毛晓光,王怀民.软件可信分级规范.版本 2.0,国家高技术研究发展计划(863)重点项目“高可信软件生产工具与集成环境”技术文档,TRUSTIE-STC V2.0,2009.

[19] 卢刚,王怀民,毛晓光.基于认知的软件可信评估证据模型.南京大学学报(自然科学),2010,46(4):456–463.

[20] 丁学雷,王怀民,王元元,卢刚.面向验证的软件可信证据与可信评估.计算机科学与探索,2010,4(1):46–53.

[24] 钱红兵,晏海华,张茂林,杨海燕,何智涛,朱小杰.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, 2009.

[26] 刘超.可信软件结构及代码的审查和综合评估及支持工具.中国科技成果,2010,11(16):21–22.

[27] 沈国华,黄志球,钱巨,徐拥军,郝进,赵文耘,彭鑫.软件可信评估模型及其工具实现.计算机科学与探索,2011,5(6):553–561.

[28] 秦立格,杨明,方可.仿真可信度评估辅助工具研究.计算机仿真,2010,27(6):118–121.

[29] 贺久松.BPM 领域构件可信评估系统的研究与实现[硕士学位论文].西安:西北大学,2010.

[30] 杨静.软件可信性评估工具的研究与实现[硕士学位论文].西安:西北大学,2010.

[35] 张立强,张焕国,张帆.可信计算中的可信度量机制.北京工业大学学报,2010,36(5):586–591.

[36] 袁霖,王怀民,尹刚,史殿习,米海波.基于角色的软件可信评估技术.北京工业大学学报,2010,36(5):611–615.

[39] 刘彦钊,罗峋,薛凯,罗平.一种基于属性划分的软件可信性度量模型研究.计算机科学与应用,2012,2:121–125.

[44] 盛津芳,陈松乔,王斌.软件功能需求驱动的商业构件评估.计算机工程,2005,(24):99–101.

[49] 唐见兵.作战仿真系统可信性研究[博士学位论文].长沙:国防科学技术大学,2009.

[50] 包铁,刘淑芬,王晓燕.电力生产管理系统的可信构造方法研究.电子学报,2010,38(9):2166–2171.

[51] 张建康,程龙,黄俊,武哲.基于任务的作战飞机效能评估模型.北京航空航天大学学报,2005,31(12):1279–1283.

[52] 王秀利,王宏伟.Web 服务可信评估要求.计算机系统应用,2009,(4):36–39.

[54] 田俊峰,肖冰,马晓雪,王子贤.TDDSS 中可信模型及其分析.计算机研究与发展,2007,44(4):598–605. [doi: 10.1360/crad20070408]

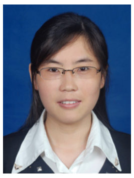
[57] 刘博,范玉顺.面向服务的工作流性能评价及指标相关度分析.计算机集成制造系统,2008,14(1):160–165.

沈国华(1976－),男,江苏丹阳人,博士,副教授,CCF 高级会员,主要研究领域为需求工程,软件可信评估,软件安全性.

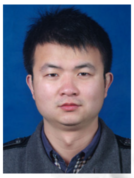
黄志球(1965－),男,博士,教授,博士生导师,CCF 杰出会员,主要研究领域为软件工程,形式化方法,隐私保护.

谢冰(1970－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为软件工程,形式化方法,分布式系统.

朱羿全(1990－),男,硕士,主要研究领域为软件安全性,Web 服务.



廖莉莉(1989－),女,硕士,主要研究领域为本体度量,语义 Web,描述逻辑.



王飞(1990－),男,硕士生,CCF 学生会员,主要研究领域为软件安全性,软件可追踪性.

刘银陵(1989－),男,硕士生,主要研究领域为软件安全性.

www.jos.org.cn

© 中国科学院软件研究所 http://www.jos.org.cn