International Journal of Information Systems and Supply Chain Management
Volume 11 • Issue 1 • January-March 2018

Operation Refinement in Trusted Component Based on OR-Transition Colored Petri Net

Na Zhao, School of Software, Yunnan University, Kunming, China
Jin Xu, Yunnan University, Kunming, China
Xiucheng Yang, ICube Laboratory, University of Strasbourg, Strasbourg, France
Zhongwen Xie, School of Software, Yunnan University, Kunming, China
Yong Yu, School of Software, Yunnan University, Kunming, China
Jian Wang, Kunming University of Science and Technology, Kunming, China

ABSTRACT

The development and evolution of trusted software is the focus of attention in the fields of trusted software and software engineering at home and abroad. In view of its complexity and diversity, this article proceeds with component, which is the basic element of software architecture, and discusses the refinement of trusted component. Refine one of the operations and its local environment using OR-transition colored Petri net to achieve the purpose of gradual refinement.

KEYWORDS

Component Net, Petri Net, Refinement of Component, Trusted Component

INTRODUCTION

Microsoft defined software creditability in 2012, including security, confidentiality, reliability and integrity in business practices. Chen, Wang, and Dong (2003) regard software creditability as one or more of reliability, reliable security, confidential security, survivability, fault tolerance and instantaneity. Highly trusted software engineering is an important technology component for software creditability, in which formal methods based software technology will become the breakthrough and development trend.

Software engineering provides abstraction and refinement mechanism to handle the complexity of software. Refinement refers to adding more information in the software system model, which is conducive to the design and implementation of software system. Similarly, it is an important technique to construct hierarchical component model through abstraction or refinement in the process of modeling and designing software component.

Petri net is often used in software system modeling because of its rigorous mathematical expression and intuitive graphical representation. In previous work (Yu, Liu, Dai, & Zhao, 2009) we extended the Petri net to OR-transition colored Petri net as per relevant definition and principle of component such

DOI: 10.4018/IJISSCM.2018010103

that we can effectively make use of the transitions of it to represent the operations in the component. Based on the trusted component model of OR-transition colored Petri net, we build a hierarchical trusted component model by refining the operations in the trusted component.

RELATED WORK

In recent years, domestic and foreign research institutions and scholars have done many related works on trusted component from different perspectives.

There have been some works (Franco, Barbosa, & Zenha-Rela, 2013; Panwar & Garg, 2013; Zuo & Hu, 2009; Rathod & Parmar, 2012; and Wang & Chen, 2012) on the research of evaluation and evolution of trusted component. In five recent papers (Shafiu & Singh, 2016; Law, Verville, & Taskin, 2011; Brahimi, Seinturier, & Boufaida, 2009; Li, Li, & Wang, 2013; and Shanmugapriya & Suresh, 2012) the authors analyzed the reliability of component and discussed the trusted component modeling and algorithm efficiency.

Wang, Tang, Yin, & Li (2006) proposed a trusted concept model of Internet software for Internet virtual computing environment (iVCE), and the network software trusted guarantee system, which assembles identity creditability, capability creditability and behavior creditability. In addition, they argued that the online adjustment of environmental adaptability was an important part of credible evolution, thus proposed a component model that supports the fine-grained online adjustment of software environment adaptability (Ding, Wang, Shi, & Li, 2011).

The CLASP (Comprehensive, Lightweight Application Security Process) given in the literature (Secure Software, 2005) is best practice based on formal methods. The authors tried to build an activity-driven, role-based process component set to support the software development team incorporating security into the software development lifecycle in the early stages, the results of which demonstrated that the formal methods are effective to guarantee software security in combination with the software process. CbyC (Correctness by Construction) successfully combined formal methods into the software development process, and fully embodied the advantages of using formal methods to rigorously describe and verify security (Hall & Chapman, 2002; and Hall, 2002). Wehrmeister, Freitas, Pereira, & Wagner (2007) proposed DERAF framework based on aspect-oriented approach and RT-UML to introduce the attributes of software quality into the system in the early design phase. The SecureChange project team, funded by the European Union, studied the security evolution to ensure that the requirements of security, privacy, and reliability are satisfied after the evolution of the system (Secure Change project, 2009). Yang, Wang, & Li (2009) mainly studied the trusted software process management and risk modeling, and defined trusted attributes as functionality, reliability, security (including safety), usability, portability and maintainability. In addition, they referred process creditability as an indicator of measuring and improving software creditability, and proposed TPMF (Trustworthy Process Management Framework), a credible process management framework, to ensure software creditability by measuring and improving process creditability.

The important characteristics of trusted component evolution are discussed in (Yang & Zheng, 2013; and Jia & Zheng, 2012). Liu, Xu, & Cheung (2015), Chargo (2013) discussed the performance parameters in a trusted component model. And Chen (2012) described component and connector, and the relationship between them.

DEFINITION OF TRUSTED COMPONENT SUBNET

Definition 1

In the trusted component $C_t = <P_t, T_t, F_t, S_t, A_{Pt}, A_{Tt}, A_{Ft}, IP_t, OP_t>$, OR-transition colored Petri net $N_t=<P_t', T_t', F_t', S_t', A_{Pt}', A_{Tt}', A_{Ft}'>$ is the internal subnet of C_t, iff:

Agile Value Creation and Co-evolution in Global Supply Chains

Ali Alavizadeh, Reza Djavanshir, Mohammad J. Tarokh and Jaby Mohammed (2012). *Customer-Oriented Global Supply Chains: Concepts for Effective Management (pp. 94-111).*

www.igi-global.com/chapter/agile-value-creation-evolution-global/63775?camid=4v1a

Delivery Commitments in Stochastic Service Networks: Case of Automobile Service

Sandeep Dulluri and Ganesh Muthusamy (2013). *International Journal of Information Systems and Supply Chain Management (pp. 50-61).*

www.igi-global.com/article/delivery-commitments-in-stochastic-service-networks/80169?camid=4v1a