Journal of Computer and System Sciences 80 (2014) 902

Contents lists available at ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

Foreword

Special Issue: Dependable and Secure Computing

This special issue of *Journal of Computer and System Sciences* is devoted to papers on Dependable and Secure Computing based on DASC2011 – The 9th IEEE International Conference on Dependable, Autonomic and Secure Computing held in Sydney Australia from December 12–14, 2011.

As computer systems become increasingly large and complex, their Dependability and Security play critical role in achieving desirable results for complex science, engineering, and commercial applications. These systems often consist of heterogeneous software, hardware and network components of changing capacities, availability, and in varied contexts. They provide various computing services to large pools of users and applications. As such, they are often exposed to a large number of dangers such as accidental or deliberate faults, virus infections, malicious attacks, illegal intrusions, and natural disasters etc. As a result, too often computer systems fail, become compromised, or perform poorly and therefore undependable. Thus, it remains a challenge to design, analyze, evaluate, and improve the dependability and security for complex computing environments. As such, this special issue aims at presenting the latest developments, trends and research solutions of dependable and secure computing. The eight papers in this special issue offer a view from different perspectives on current research in the area.

The first paper proposes a message matching-based detection (MMBD) method where a smart mobile trusted module (MTM) is introduced to prevent the greedy behavior. The second paper proposes a trust enhanced distributed authorization architecture (TEDA) that provides a holistic framework for authorization taking into account the state of a user platform. The model encompasses the notions of 'hard' and 'soft' trust to determine whether a platform can be trusted for authorization. The third paper focuses on automatic adaptation of authorization assets (policies and user access rights) in order to manage federated authorization infrastructures, and then presents a Self-Adaptive Authorization Framework (SAAF) controller that is capable of managing policy based federated role/attribute access control authorization infrastructures. The fourth paper proposes to use a Connection Dependence Graph (CDG) representation of software control flow to construct a connection-based signature approach for detecting errors among component interactions. The fifth paper provides a deep survey about current threats in cyber security. Various threat issues have been identified and categorized. This paper would be a strategic guideline for researchers in the area. The sixth paper addresses security in G-Hadoop. The paper proposes a security framework. This security framework simplifies the users authentication and job submission process of the current G-Hadoop implementation with a single-sign-on approach. The seventh paper focuses on data privacy issue in big data applications on cloud. The paper analyzes the problem of individual top-down specialization and bottom-up generalization. Then, based on the problem, the paper develops a hybrid approach. The eighth paper uses side information to propose a semi-supervised approach for accurate traffic clustering. The experiment shows significant improvement on quality of resultant traffic clusters.

While the authors were invited to submit their papers to this special issue, all papers went through the standard refereeing procedures of this journal. We would like to thank the authors and referees for their help in making timely publication of this special issue possible. This issue could not have been produced without them.

Jinjun Chen
University of Technology Sydney,
PO Box 123, Broadway, NSW 2007, Australia

Jianxun Liu
Hunan University of Science and Technology,
Hunan 411201, China

24 June 2013
Available online 10 February 2014

http://dx.doi.org/10.1016/j.jcss.2014.02.009