Guest Editorial: Emerging Software Reliability and System Security Technologies

Fang-Yie Leu[1] and A Min Tjoa[2*]
[1] *Computer Science Department, Tunghai University, Taiwan*
leufy@thu.edu.tw
[2] *Vienna University of Technology, A-1040 Vienna, Austria*
amin@ifs.tuwien.ac.at

Due to the quick development of mobile, ubiquitous, cloud, network and communication systems and applications, many computer and communication systems, wired or wireless, have been proposed to provide their users (human or other systems) with different services. However, hackers may anytime and anywhere attack these systems for stealing a company's business secrets or a person's credit card information, penetrating a system to show the achievement of their professional skills, preventing a system from providing its normal operations just for fun, etc. Also, a software system cannot be perfectly developed. So sometimes it may fail or out of services. To prevent a system from being attacked or intruded, we need various security mechanisms to protect our systems and the information delivered between/among them. To realize the probability of a system, we have to derive its reliability model and predict when it may fail. Then we can do something in advance. That is why information security and system reliability models have been important issues in recent computer and communication research. They are also the reasons why this special issue is created.

This special issue collects six papers that discuss different aspects of software reliability and system security technologies. Most of them are selected from those submitted to and presented in the 8th International Conference on Availability, Reliability and Security (ARES 2013)[1]. Their focuses are mainly on how to prevent a system from being attacked, and what the reliability model of a software system is.

- The first article "Reliability Prediction for Component-based Software Systems with Architectural-level Fault Tolerance Mechanisms" [1] presents a novel extension built upon the core model of a recent component-based reliability prediction approach to offer an explicit and flexible definition of reliability-relevant behavioral aspects (i.e. error detection and error handling) of fault tolerance mechanisms, and the evaluation of their reliability impact in the dependence of the whole system architecture and usage profile. This approach is validated in two case studies, by modeling the reliability, conducting reliability predictions and sensitivity analyses, and demonstrating its ability to support design decisions.

- The second article "Supporting Common Criteria Security Analysis with Problem Frames" [2] proposed a threat analysis method to improve the Common Criteria threat analysis and the derivation of security objectives based upon an attacker model, which considers different attacker types that threaten only specific parts of a system. The authors also provided tool support for checking consistency and the completeness of the specified software systems using OCL expressions and illustrate the method with the development of a smart metering gateway system.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 5, number: 1, pp. 1-3
*Lead Guest Editor
[1] ARES 2013 was held in Regensburg, Germany on September 2-6, 2013. `http://www.ares-conference.eu/ares2013/`

- The next article "Plausibilistic Entropy and Anonymity" [3] detailed side-by-side comparison between plausibilistic entropy and Shannon entropy, and underlined a promising level of compatibility between them. At the end, the author presents the vision on how to define a measure for anonymity based on plausibilistic entropy and how such a definition can be employed to serve practical purposes.
- In the fourth paper "Analyzing Android's Full Disk Encryption Feature" [4], the authors gave a structured analysis of the software-based encryption method of Android 4.0, and presented a tool named EvilDroid to show that with physical access to an encrypted smartphone only (i.e., without user level privileges), the Android system partition can be subverted with keylogging. Additionally, as it was exemplary shown by attacks against Galaxy Nexus devices in 2012, Android-driven ARM devices are vulnerable to cold boot attacks. This paper demonstrated that Android's software encryption can be improved to withstand cold boot attacks by performing AES entirely on the CPU without RAM and then the cold boot attacks on encryption keys can be defeated.
- The fifth article "Enforcing Reputation Constraints on Business Process Workflows" [5] contributed to solve the problem of how to calculate service and service provider reputation values of a cloud system by defining a model which calculates service reputation levels with a BPEL-based business workflow. These reputation levels are used to control the execution of the workflow based on service-level agreement constraints provided by the users. The main contributions of this article are presenting a formal meaning for BPEL processes, which is constrained by reputation requirements from the users, and then demonstrating that these requirements can be enforced using a reference architecture with a case scenario from the domain of distributed map processing.
- The last paper "A New Certficateless Blind Signature Scheme" [6] proposed a new efficient provably secure certificateless blind signature scheme, the security of which can be proven to be equivalent to solving computational Diffie-Hellman (CDH) and chosen-target CDH problem in the random oracle model.

Although the articles selected in this special issue address several important aspects of emerging software reliability and system security Technologies, many security areas and software reliability models need to be intensively enhanced and developed, like how to effectively prevent *Denial of Services* and *Distributed Denial of Services* attacks, how to detect and avoid an insider attack, and the way to increase the reliability of a cloud system and its services, etc. We hope these threatens can be solved one by one and dependable software models can be further improved in the near future.

At last, we would like to extend our special thanks to Dr. Ilsun You who is the EiC of JoWUA as well as Ms. Yvonne Poul who is the guest editorial assistant for this special issue. Without their help, this special issue cannot be published on time.

Fang-Yie Leu and A Min Tjoa
Guest Editors
March 2014

References

[1] T.-T. Pham, F. Bonnet, and X. Défago, "Reliability Prediction for Component-based Software Systems with Architectural-level Fault Tolerance Mechanisms (Extended Version)," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 5, no. 1, pp. 4–36, March 2014.

[2] K. Beckers, M. Heisel, and D. Hatebur, "Supporting Common Criteria Security Analysis with Problem Frames," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 5, no. 1, pp. 37–63, March 2014.

[3] I. Goriac, "Plausibilistic Entropy and Anonymity," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 5, no. 1, pp. 64–83, March 2014.

[4] J. Götzfried and T. Müller, "Analysing Android's Full Disk Encryption Feature," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 5, no. 1, pp. 84–100, March 2014.

[5] B. Aziz and G. Hamilton, "Enforcing Reputation Constraints on Business Process Workflows," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 5, no. 1, pp. 101–121, March 2014.

[6] S. Jose, A. Gautam, and C. Pandurangan, "A New Certificateless Blind Signature Scheme," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 5, no. 1, pp. 122–141, March 2014.

Author Biography

Fang-Yie Leu received his BS, master and Ph.D. degrees all from National Taiwan University of Science and Technology, Taiwan, in 1983, 1986 and 1991, respectively, and another master degree from Knowledge Systems Institute, USA, in 1990. His research interests include wireless communication, network security, Grid applications and Chinese natural language processing. Between 1995 and 2001, he served as the chairman of his department. He is currently a workshop organizer of CWECS and MCNCS workshops, one of program committee and organizing committee members of several international workshops and conferences, a professor of TungHai University, Taiwan, one of the editorial board members of at least 7 journals and director of database and network security laboratory of the University. He has been the chief Judge of Computer Programming Category of National Professional Skill Competition for Disability, Ministry of labor, Taiwan and has published more than 160 peer reviewed articles in journals and conferences. He is also a member of IEEE Computer Society.

A Min Tjoa is is a full professor and director of the Institute of Software Technology and Interactive Systems at the Vienna University of Technology. He is currently also a Chairman of the Austrian National Competence Center for Security Research (COMET - SBA). He was visiting professor at the Universities of Zurich, Kyushu and Wroclaw (Poland), National Institute of Informatics (NII, Japan) and at the Technical Universities of Prague and Lausanne (Switzerland). From 1999 to 2003, he was the president of the Austrian Computer Society. Within IFIÜ he is member of the IFIP Board and Honorary Secretary of the IFIP Executive Committee and chairperson of the IFIP Working Group on Enterprise Information Systems (WG 8.9). In 2011 he received the Honorary Doctorate degree of the Czech Technical University in Prague and a Honorary Professor degree from the University of Hue (Vietnam). His current research focus areas are data warehousing, grid computing, semantic web, security, and personal information management systems. He is chairperson of the ASEA-UNINET University Network for the period 2013-2014. He has published more than 150 peer reviewed articles in journals and conferences. He is author and editor of more than 20 books.