Journal of Universal Computer Science, vol. 22, no. 4 (2016), 453-458
submitted: 10/3/16, accepted: 25/3/16, appeared: 1/4/16 © J.UCS

Advanced Research on Software Security Design and Applications

J.UCS Special Issue

Shadi A. Aljawarneh
(Software Engineering Dept, CIT Faculty, Jordan University of Science and Technology
Irbid, Jordan
saaljawarneh@just.edu.jo)

Federica Cena
(University of Turin, Italy
cena@di.unito.it)

Abdelsalam Maatuk
(Benghazi University, Libya
abdelsalam.maatuk@uob.edu.ly)

1 Introduction

This special issue focuses on advanced research in the practical applications and the theoretical foundations of software security, through presentation of the most up-to-date advances and new directions of research in the field from various scholarly, professional, and practitioner perspectives. An interdisciplinary look at software security including engineering and business aspects, such issue covers and encourages high-quality research exposition.

The main mission of this special issue "Advanced Research on Software Security Design and Applications" is to be the premier and authoritative source for the most innovative scholarly and professional research and information pertaining to aspects of Software Security. Such issue presents advancements in the state-of-the-art, standards, and practices of software security, in an effort to identify emerging trends that will ultimately define the future of "the software security."

The objectives of this issue are multi-folds, including,

(1) Establish a significant channel of communication among software security researchers, engineers, practitioners and IT policy makers;

(2) Provide a space to publish and share the latest high quality research results in the area of software security;

(3) Promote and coordinate international collaboration in the standards of software security to meet the need to broaden the applicability and scope of the current and future research of software security.

This issue explores the foundations of software security. The important software vulnerabilities and attacks are considered that exploit them -- such as buffer overflows, SQL injection, and session hijacking -- and defenses are also considered

that prevent or mitigate these attacks, including advanced testing and program analysis techniques. Importantly, we take a "build security in" mentality, considering techniques at each phase of the development cycle that can be used to strengthen the security of software systems.

This special issue is intended for researchers and practitioners who are interested in issues that arise from using technologies of software security advancements. In addition, such issue is also targeted to anyone who wants to learn more about the software security research advancements in design and applications. Software security has become a hot topic in recent years and people at different levels in any organization need to understand security in different ways.

Topics are discussed in this issue include the following:

- Low-level, memory-based attacks
- Penetration testing, presenting an overview of goals, techniques, and tools of the trade
- Software Security Technologies & services
- Software Security Applications
- Software Security Architecture
- Software Security Standard
- Built-in security

2 Contributions of the special issue

The special issue got huge attention due to the fact that Software Security is a big topic in the field of Information Security and Security Vulnerabilities these days. Nevertheless a careful peer-review-process reduced the number of contributions to finally eight:

Paper 1: Analysis of Permission-based Security in Android through Policy Expert, Developer, and End User Perspectives by Ajay Kumar Jha and Woo Jin Lee.

This paper discussed one of the major operating system in smartphone industry, security in Android is paramount importance to end users. Android applications are published through Google Play Store, which is an official marketplace for Android. If we have to define the current security policy implemented by Google Play Store for publishing Android applications in one sentence then we can write it as “all are suspect but innocent until proven guilty.” It means an application does not have to go through rigorous security review to be accepted for publication. It is assumed that all the applications are benign which does not mean it will remain so in future. If any application is found doing suspicious activities then the application will be categorized as malicious and it will be removed from the Play Store. Though filtering of malicious applications is performed at Play Store, some malicious applications escape the filtering process. Thus, it becomes necessary to take strong security measures at other levels. Security in Android can be enforced at system and application levels. At system level Android uses sandboxing technique while at application level it uses permission. In this paper, the permission-based security

implemented has been analyzed in Android through three different perspectives – policy expert, developer, and end user.

Paper 2: A Novel Similar Temporal System Call Pattern Mining for Efficient Intrusion Detection by Vangipuram Radhakrishna**,** Puligadda V.Kumar and Vinjamuri Janaki.

In this paper, the major objective is to identify the intrusion using temporal pattern mining. The idea is to find normal temporal system call patterns and use these patterns to identify abnormal temporal system call patterns. For finding normal system call patterns, we use the concept of temporal association patterns. The reference sequence is used to obtain temporal association system call patterns satisfying specified dissimilarity threshold. To find similar (normal) temporal system call patterns, we apply our novel method which performs only a single database scan, reducing unnecessary extra overhead incurred when multiple scans are performed thus achieving space and time efficiency. The importance of the approach coins from the fact that this is first single database scans approach in the literature. To find if a given process is normal or abnormal, it is just sufficient to verify if there exists a temporal system call pattern, which is not similar to the reference system, call support sequence for specified threshold. This eliminates the need for finding decision rules by constructing decision table. The approach is efficient as it eliminates the need for finding decision rules (2n is usually very large for even small value of n) and thus aims at efficient dimensionality reduction as we consider only similar temporal system call sequence for deciding on intrusion.

Paper 3: Web Data Amalgamation for Security Engineering: Digital Forensic Investigation of Open Source Cloud by Asif Imran**,** Shadi Aljawarneh and Kazi Sakib**.**

This paper proposes a scheme that ensures Software Security and Security of Cloud provenance in a series of steps, the first of which involves binding the provenance journals with user-data from which those were derived. Next, mechanisms for merging provenance with unstructured web data for improved Security Intelligence (SI) is identified. Detection of attack models for nefarious malware activities in six Software as a Service (SaaS) applications running in real-life Cloud is taken as the research case and the performance of the proposed algorithms for those are analyzed. The Success Rates (SR) for melding the web data to secure provenance for the six specific SaaS applications are found to be 85.0554%, 96.7032%, 98.3871%, 93.9732%, 80.5000% and 84.9257% respectively. Hence, this paper proposes a framework for effectively ameliorating the current scheme of Cloud based Software Security, thereby achieving wider acceptance of open source Cloud.

Paper 4: Feature Selection for Black Hole Attacks by Muneer Bani Yassein**,** Yaser Khamayseh and Mai AbuJazoh.

This paper proposes a new dataset (BDD dataset) for black hole intrusion detection systems which contributes to detect the black hole nodes in MANET. The proposed dataset contains a set of essential features to build an efficient learning model where these features are selected carefully using one of the feature selection techniques

which is information gain technique.J48 decision tree, Naïve Bayes (NB) and Sequential Minimal Optimization (SMO) classifiers are learned using training data of BDD dataset and the performance of these classifiers is evaluated using a learning machine tool Weka 3.7.11. The obtained performance results indicate that using the proposed dataset features succeeded in build an efficient learning model to train the previous classifiers to detect the black hole attack.

Paper 5: An Empirical Investigation of Security Vulnerabilities within Web Applications by Ibrahim Abunadi and Mamdouh.
Existing vulnerability prediction models use process or product metrics and machine learning techniques to identify vulnerable software components. Cross-project vulnerability prediction plays a significant role in appraising the most likely vulnerable software components, specifically for new or inactive projects. Little effort has been spent to deliver clear guidelines on how to choose the training data for project vulnerability prediction. In this work, we present an empirical study aiming at clarifying how useful cross-project prediction techniques are in predicting software vulnerabilities. Our study employs the classification provided by different machine learning techniques to improve the detection of vulnerable components. The prediction performance of five well-known classifiers have been compared. The study is conducted on a publicly available dataset of several PHP open-source web applications in the context of cross-project vulnerability prediction, which represents one of the main challenges in the vulnerability prediction field.

Paper 6: Secure Channel coding schemes based on Algebraic-Geometric Codes over Hermitian Curves by Omar A. Alzubi, Thomas M. Chen, Jafar A. Alzubi , Hasan Rashaideh and Nijad Al-Najdawi.
Algebraic-Geometric (AG) codes are new paradigm in coding theory with promising performance improvements and diverse applications in point to point communications services and system security. AG codes offer several advantages over state- of-the art Reed-Solomon (RS) codes. Algebraic-Geometric Codes are proposed and implemented in this paper. The design, construction and implementation are investigated and a software platform has been developed. Simulation results are presented for the first time showing significant performance improvements of AG codes over RS codes using different modulation schemes. The superiority in error correcting and security of AG codes over RS codes has been demonstrated clearly when Rayleigh fading channel is used. Also the results show an obvious improvement when using higher modulation schemes, namely 16QAM and 64QAM.

Paper 7: On the Analysis and Detection of Mobile Botnet Applications by Ahmad Karim, Rosli, Muhammad Khurram Khan, Aisha Siddiqa and Kim-Kwang Raymond Choo.
In this article, a static analysis approach, DeDroid, is proposed to investigate botnet-specific properties that can be used to detect mobile applications with botnet intensions. Initially, we identify critical features by observing code behavior of the few known malware binaries having C&C features. Then, the identified features with the malicious and benign applications of Drebin dataset have compared. The results

show against the comparative analysis that, Drebin dataset has 35% malicious applications, which qualify as botnets. Upon closer examination, 90% of the potential botnets are confirmed as botnets. Similarly, for comparative analysis against benign applications having C&C features, DeDroid has achieved adequate detection accuracy. In addition, DeDroid has achieved high accuracy with negligible false positive rate while making decision for state-of-the-art malicious applications.

Paper 8: An Approach for Intrusion Detection Using Novel Gaussian Based Kernel Function by Gunupudi Rajesh Kumar and Nimmala Mangathayaru and Gugulothu Narsimha. In this paper the major objective is to design and analyze the suitability of Gaussian similarity measure for intrusion detection. The objective is to use this as a distance measure to find the distance between any two data samples of training set such as DARPA Data Set, KDD Data Set. This major objective is to use this measure as a distance metric when applying k-means algorithm. The novelty of this approach is making use of the proposed distance function as part of k-means algorithm so as to obtain disjoint clusters. This is followed by a case study, which demonstrates the process of Intrusion Detection. The proposed similarity has fixed upper and lower bounds.

3 Program Committee

We express our gratitude to the program committee for their valuable work on reviewing all contributions and giving detailed feedback. Thank you for your expertise:

Anna Goy, Universita' di Torino, Italy
Ryan K. L. Ko, HP Labs Singapore, Singapore
Maik A. Lindner, SAP Research, UK
Shiyong Lu, Wayne State University, USA
Yuzhong Sun, Chinese Academy of Science, China
Ray Walshe, Irish Centre for Cloud Computing and Commerce, Ireland
Sanjay P. Ahuja, University of North Florida, USA
Junaid Arshad, University of Leeds, UK
Juan Caceres, Telefónica Investigación y Desarrollo, Spain
Jeffrey Chang, London South Bank University, UK
Kamal Dahbur, NYIT, Jordan
Ravindra Dastikop, SDMCET, India
Sam Goundar, Victoria University of Wellington, New Zealand & KYS International College, Melaka - Malaysia
Sofyan Hayajneh, Isra University, Jordan
Sayed Amir Hoseini, Iran Telecommunication Research Center, Iran
Gregory Katsaros, National Technical University of Athens, Greece
Mariam Kiran, University of Sheffield, UK
Anirban Kundu, Kuang-Chi Institute of Advanced Technology, China
Sarat Maharana, MVJ College of Engineering, Bangalore, India
Manisha Malhorta, Maharishi Markandeshwar University, India