Editorial: SPECIAL ISSSUE CISIS14-IGPL

The ten contributions selected in this special issue represent a collection of extended papers presented at the seventh International Conference on Computational Intelligence in Security for Information Systems (CISIS 2014).

CISIS Conferences aim to offer a meeting opportunity for academic- and industry-related researchers belonging to the various, vast communities of Computational Intelligence, Information Security, and Data Mining. The need for intelligent, flexible behaviour by large, complex systems, especially in mission-critical domains, is intended to be the catalyst and the aggregation stimulus for the overall event.

In the first contribution, García-Ferreira *et al.* discuss the techniques used today for the search of patterns and vulnerabilities within the software to know what are the possible solutions to this issue. They examine the problem from the point of view of their algorithms and their effectiveness in finding bugs. Although there are similar surveys, none of them addresses the comparison of best static analysis algorithms against the best mathematical logic languages for model checking, two fields that are becoming very important in the search for errors in software.

Following, de-la-Peña-Sordo *et al.* propose a new method to detect trolling comments in social news websites. To this end, they extract a combination of statistical, syntactic, and opinion features from the user comments. Since this troll phenomenon is quite common in the web, they propose a novel experimental setup for anomaly detection method. They evaluate the approach with data from 'Menéame', a popular Spanish social news site, showing that the method developed can obtain high rates while minimizing the labelling task.

Next contribution, by Peiro *et al*. aim at the analysis and detection of stack-based information leaks to harden the security of the Linux kernel. They analyse the problem of kernel infoleaks, and examine the impact of infoleaks attacks on the security of the kernel. Then, a technique for detecting kernel-based infoleaks through static analysis is presented and evaluated by applying it to the Linux kernel.

In this paper, Borrego-Díaz *et al.* propose a method based on semantic techniques for both, analysing and specifying (meta)security requirements on protocols used for solving security incidents. This would allow specialist getting better documentation on their intangible knowledge about them.

In the following contribution, Peinado *et al.* study the different modes of operation of the linear feedback shift registers with dynamic feedback (DLFSR) structure and propose a general classification of the generators attending to the way in which the feedback is applied. A theoretical study of these modes of operation allows to identify the optimal ones. Recent DLFSR proposals are identified as particular elements of the classification proposed, and a new generic pseudorandom sequence generator, belonging to one of the optimal classes, is presented.

Andrysiak *et al.* present in the subsequent contribution a network anomaly detection system based on long memory statistical models. In order to determine whether the analysed time series are characterized by the long memory, they underwent tests with the use of the local Whittles estimator. The tests were performed over three diverse statistic approaches described as ARFIMA, A-FIGARCH and MIDAS. They propose to use statistical relationships between predicted and original network traffic to determine whether the examined trace is normal or attacked.

Vol. 24 No. 6, © The Author 2016. Published by Oxford University Press. All rights reserved.
For Permissions, please email: journals.permissions@oup.com
doi:10.1093/jigpal/jzw054

In next paper, Aiello *et al.* propose an innovative profiling system for DNS tunnels that is based on Principal Component Analysis and Mutual Information. Results from experiments conducted on a live network show that one of the introduced metric is able to characterize anomalies on small DNS servers, while the other behaves better on medium sized servers. Concerning DNS tunnelling attacks, the proposed approach reveals to be an efficient tool for traffic profiling in the presence of DNS tunnelling.

The aim of the next work, by Kühnel and Meyer, is to present a novel modification to the Android emulator in order to trick the mobile malware to think that it is being executed on an actual device. They also evaluate its previous model: Highly Space Efficient Blacklisting (HSEB) by applying HSEB to mobile malware initiated traffic, showing that HSEB can save up to 14.46% space when applied to IP-address blacklists.

In this contribution Merlo *et al.* extend and improve their previous work, where they modelled and analysed the energy savings enabled by aggressive intrusion detection, by introducing a new enhanced adaptive model that takes into full account the actual load of routers including what is due to forecasting errors.

In the final contribution, by Nuñez-Gonzalez *et al.*, a new global heuristic search method for Influence Maximization (IM) is proposed, providing a comparison over a collection of synthetic and real life graphs against other state-of-the-art heuristic search methods, namely Simulated Annealing, Genetic Algorithms, Harmony Search and the classical Greedy Search (GS) algorithm. The new method (IMH) competes with the GS algorithm getting the minimal IM-seed set whose influence spreads the largest amount of nodes, and also improves Greedy algorithm's time execution.

The guest editors wish to thank Professor Dov Gabbay (Editor-in-Chief of Logic Journal of the IGPL) for providing the opportunity to edit this special issue. We would also like to thank the referees who have critically evaluated the papers within the short time. Finally, we hope the reader will share our joy and find this special issue very useful.

Pablo García Bringas
DeustoTech Institute of Technology, University of Deusto, Bilbao, Spain
E-mail: pablo.garcia.bringas@deusto.es

Jorge de la Peña Sordo
DeustoTech Institute of Technology, University of Deusto, Bilbao, Spain
E-mail: jorge.delapenya@deusto.es

José Gaviria de la Puerta
DeustoTech Institute of Technology, University of Deusto, Bilbao, Spain
E-mail: jgaviria@deusto.es

Álvaro Herrero
University of Burgos, Burgos, Spain
E-mail: ahcosio@ubu.es

Héctor Quintián
University of Salamanca, Salamanca, Spain
E-mail: hector.quintian@usal.es

Emilio Corchado
University of Salamanca, Salamanca, Spain
E-mail: escorchado@usal.es

Received 1 July 2016