Editorial: Special Issue CISIS15-IGPL

The eight contributions selected in this special issue represent a collection of extended papers presented at the eighth International Conference on Computational Intelligence in Security for Information Systems (CISIS 2015) held in Burgos, Spain, in June 2015, and organized by the BISITE (University of Salamanca) and the GICAP (University of Burgos) research groups, together with the Technological Institute of Castilla y León.

CISIS aims 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, by Wójtowicz et al., an architecture and a protocol for secure and privacy-preserving smart space usage are proposed. It relies on a trusted party operating as a public service in the 'security infrastructure as a service' model. The proposed solution is designed to minimize the risk of users privacy violation from the side of service providers and attackers impersonating regular users, as well as the risk of violating privacy of users' payment patterns from the side of payment authorities.

Sanchez-Rola et al. analyze the current techniques for web-tracking as well as techniques for its detection and analysis, and countermeasures to prevent web tracking. Authors address this topic from a web-security research perspective, describing both web-tracking techniques and defences to bring understanding of the current state of the art in web tracking. Additionally, a better understanding of the landscape and the proper discussion of its implications and future research trends are also discussed.

The third contribution Ezpeleta et al. demonstrate that a classic spam model using online social network information can harvest a 7.62% of click-through rate. Email addresses are collected from the Internet, as well as complete email owner information (from their public social network profile), and the response of personalized spam sent to users according to their profile is analyzed. Results from typical spam and personalized spam are studied and compared.

Three Spanish smart card deployments intended to be used for eGovernment services are compared by Gayoso-Martínez et al. The contents and capabilities of such deployments for the authentication of users in public services are compared and contrasted with the already consolidated Spanish National Identity card.

In the fifth paper, by Sedano et al., Feature Selection based on Maximum Relevance Minimum Redundancy and evolutionary algorithms using a binary representation and a fitness function based on information correlation measures is applied for Android Malware characterization. The families of bad-intentioned Android apps are studied and the key features of such software that support their characterization are identified.

Nguyen et al. propose a new approach based on entropy-based clustering, and decision tree techniques in combination with bagging, to identify PNG data fragments which are the deflate-encoded fragments. Experiments on this deflate-encoded data detection showed high accuracy rates for the proposed combination of methods.

An extension of MOVICAB-IDS (a previously proposed Intrusion Detection System) is proposed by Sánchez et al. By incorporating clustering techniques to the original proposal, network flows are investigated, trying to identify different types of attacks. The analysed real-life data are analysed by

Vol. 25 No. 1, © The Author 2017. Published by Oxford University Press. All rights reserved.
For Permissions, please email: journals.permissions@oup.com
doi:10.1093/jigpal/jzw037

means of clustering and neural techniques, individually and in conjunction. Promising results are obtained, proving the validity of the proposed extension for the analysis of network flow data.

In the last paper, Kozik et al. address the problem of automated HTTP request structure analysis applied to web layer cyber attack detection. The discussed method combines payload tokenization technique and statistical analysis that allows describing the dynamic properties of text in between tokens. The proposed combination of multiple HTTP sequences clustering algorithm and classifier does not need any prior knowledge about protocols and APIs that use HTTP as a transportation layer.

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.

ÁLVARO HERRERO
University of Burgos, Burgos, Spain
E-mail: ahcosio@ubu.es

BRUNO BARUQUE
University of Burgos, Burgos, Spain
E-mail: bbaruque@ubu.es

JAVIER SEDANO
Technological Institute of Castilla y León, Burgos, Spain
E-mail: javier.sedano@itcl.es

HÉCTOR QUINTIÁN
Universidad de Salamanca, Salamanca, Spain
E-mail: hector.quintian@usal.es

EMILIO CORCHADO
Universidad de Salamanca, Salamanca, Spain
E-mail: escorchado@usal.es

Received 1 July 2016