Editorial

The papers included in this special issue represent a selection of extended contributions presented at the fourth International Conference on Computational Intelligence in Security for Information Systems, CISIS 2011 held in Torremolinos, Spain, June 8–10th, 2011, and organized by the BISITE and the GICAP research groups.

This special issue is then aimed at practitioners, researchers and post-graduate students who are engaged in developing and applying advanced intelligent systems principles to solving real-world problems. The papers are organized as follows.

In the first contribution by Laorden *et al.*, a novel approach is presented for spam filtering using, for the first time, Collective Classification algorithms. Their approach presents as a suitable approach to optimizing the classification of partially labelled data to overcome the amount of unclassified e-mails that are sent every day.

In this contribution by Bankovic *et al.*, a novel solution that detects and isolates attacks on reputation systems, in particular bad mouthing and ballot stuffing, impeding them at the same time to further spread their malicious activity. The approach is based on detecting outliers using clustering, in this case self-organizing maps. An important advantage of this approach is that there are no restrictions on training data, and thus there is no need for any data pre-processing.

This contribution by HaiThanh Nguyen *et al.* studies the GeFS measure for WAFs, conducting experiments on the publicly available ECML/PKDD-2007 data set. Since this data set does not target correct Web applications, it additionally generates a new CSIC-2010 data set. It analyses the statistical properties of both the data sets to provide more insights of their nature and quality. Subsequently, it determines appropriate instances of the GeFS measure for feature selection. It uses different classifiers to test the detection accuracies. The experiments show that it is possible to remove 63% of irrelevant and redundant features from the original data set, while keeping the detection accuracy of WAFs.

In this contribution by Roschke *et al.*, a novel correlation algorithm based on Attack Graphs (AG) is designed that is capable of detecting multiple attack scenarios for forensic and run time analysis. The algorithm uses advanced knowledge on the network infrastructure under surveillance, such as deployed software, existing vulnerabilities and network level connectivity of hosts. The algorithm can be parameterized to adjust the robustness and accuracy and ensure a high quality of the result. A formal model of the algorithm is presented and an implementation is tested to analyse the different parameters on a real set of alerts from a local network. To improve the speed of the algorithm, a multi-core version is proposed and a HMM-supported version can be used to further improve the quality. The parallel implementation is tested on a multi-core correlation platform, using CPUs and GPUs.

In this contribution by Aiello *et al.*, a novel approach to the analysis of DNS Tunneling Tools in terms of network impact and performance is proposed. In particular, the contribution is twofold: first, a comprehensive taxonomy of the current state-of-the-art DNS Tunneling tools is provided. Then, the impact of each tool on the performance of different network topologies is analysed using different traffic metrics.

In this contribution by Jaydip Sen, a secure and efficient searching protocol for unstructured peer-to peer networks has been proposed that utilizes topology adaptation by constructing an overlay of trusted peers where the neighbours are selected based on their trust ratings and content similarities.

doi:10.1093/jigpal/jzs039 Advance Access published 17 August 2012

While increasing the search efficiency by intelligently exploiting the formation of semantic community structures among the trustworthy peers, the protocol provides a highly reliable module for protecting the privacy of the users and data in the network. Simulation results have demonstrated the effectiveness of the protocol.

In this paper by J. Sedano *et al*., a mutation technique is proposed to test and evaluate the performance of a full range of classifier ensembles for Network Intrusion Detection when trying to recognize new attacks. The novel technique applies mutant operators that randomly modify the features of the captured network packets to generate situations that could not otherwise be provided to IDSs while learning. A comprehensive comparison of supervised classifiers and their ensembles is performed to assess their generalization capability. An example application of the proposed testing model is specially applied to the identification of network scans and related mutations.

In this contribution, by Durán *et al.,* two new group signature schemes are presented, whose security is based upon two Number Theory problems: Integer Factorization Problem (IFP) and Subgroup Discrete Logarithm Problem (SDLP). The protocol is detailed, the security of both proposals is analysed and their differences are presented as well. Group signature schemes are a special type of signatures allowing a user, belonging to a specific group of users, to sign a message in an anonymous way on behalf of the group. In general, these schemes need a Key Generation Center or a Trusted Third Party that collaborates in the protocol (to generate the keys and for other tasks) and is able to disclose the identity of the actual signer if necessary (to settle a dispute, e.g.).

This paper by J.A.M. Naranjo and L.G. Casado presents an up to date survey on the centralized secure multicast field. This area has recently experienced a dramatic evolution due to the appearance of new scenarios that differ from those traditionally considered. The best example is the widespread of infrastructureless ad-hoc networks, populated by mobile smart devices with low computational and energy resources. On the other hand, hierarchical access control infrastructures, which were not included on any survey so far, are also considered. Traditional general-purpose schemes, the most popular so far, are reviewed too. This editorial therefore arranges schemes into different categories according to their scenario of application. Comparisons and discussions are made within each category, and finally a unified view provides the reader with a wide and clear view of the whole field. Also, future challenges and research directions are presented.

In this contribution by Peinado and Ortiz, the cryptanalysis of a particular key refreshment scheme is presented. This scheme has been recently proposed by Naranjo *et al.,* in 2010, to be applied on multicast protocols. The theoretical foundation of this scheme is the extended Euclidean algorithm. However, the same Euclidean algorithm can be employed to exploit an important weakness. As a consequence, Peinado and Ortiz show that the key refreshment is not secure, describing several weaknesses and algorithms to obtain the private keys of the users. Furthermore, they apply a genetic algorithm to break the security of a practical implementation originally proposed by Naranjo *et al*.

In this contribution by Milan Marković and GoranĐorđević, a novel model of secure cross-border m-government online services based on secure JAVA mobile application and SOA-based platform is presented. The proposed model consists of additional external entities/servers, such as: PKI, XKMS, STS, UDDI and TSA servers. One example of this model is particularly emphasized: sending m-residence certificate request and obtaining m-residence certificate as a m-government's response. This scenario could serve as a secure model of any m-government online services consisting of sending some requests to the m-government platforms and obtaining responses as corresponding governmental electronic messages or documents. These scenarios are considered both in local and cross-border case where the borders could be either the borders between municipalities in the same country or the borders between different countries.

In the final contribution by Amato *et al.*, a semantic-based framework for textual data transformation is presented. They proposed different techniques aiming at analysing texts and automatically extracting relevant information; the main goal of this activity enables to structure documents and identify critical sections in unstructured documents and this allows a protection system to enforce proper security policies by means of fine-grain access control mechanisms.

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.

EMILIO CORCHADO
University of Salamanca,
Plaza de la Merced S/N,
37008 Salamanca, Spain
e-mail: escorchado@usal.es

ÁLVARO HERRERO
University of Burgos,
C/ Francisco de Vitoria S/N,
09006 – Burgos, Spain
e-mail: ahcosio@ubu.es

Received 28 May 2012