

GUEST EDITORIAL PREFACE

Special Issue on CRiSIS 2012

Fabio Martinelli, Istituto di Informatica e Telematica - IIT National Research Council - C.N.R., Pisa, Italy

Jean-Louis Lanet, University of Limoges, Limoges, France

This special issue follows the footsteps of the CRiSIS 2012 conference (the *seventh International Conference on Risks and Security of Internet and Systems*), which was held in Cork, Ireland, 10-12 Oct. 2012. The meeting offered an effective forum for computer and network security researchers from industry, academia and government to meet, exchange ideas and present recent advances on Internet-related security threats and vulnerabilities, and on the solutions that are needed to counter them.

We have selected four papers representing some of the interesting issues that have been discussed during the conference for this special issue.

The work of Toumi et al. proposes a novel model of trust in the context of a multi-organization environment. The model views trust as a relation that involves situations (objects and actions) and time, and enables calculations which can transfer trust from organizations to users. The model also provides a way to compare and contrast various trust vectors with respect to a variety of trust policies.

The main idea in the paper presented by Ludinard et al. is to use program state invariants with Daikon for designing their IDS. The technique is based on the generation of invariants

relating values of variables at different execution time only during a given time-window. Their experiments demonstrate the effectiveness of their approach.

The paper presented by Kyrillidis et al. describes an infrastructure for e-voting based on the use of a tamperproof element, a smartcard which includes a web server for e-voting. They rely on the MNO's trusted SCWS administration protocols to transport the votes to the voting authority. It uses the "Prêt à Voter" e-voting system to have properties such as each people can verify if his vote has been correctly registered.

An interesting improvement of C. Estan and G. Varghese algorithm is proposed by Chabchoub et al., in order to detect so called vertical port scanning: several ports over a single destination address.

The main difficulty of detecting vertical port scans is counting a high number of distinct destination ports among many destination addresses. The paper proposes a modification of the original paper in order to cope with the additional difficulty of dealing with many destination addresses. The experimental results are quite impressive regarding the size of data and the accuracy of the detection.

We would like to kindly thank all the reviewers of the CRiSIS 2012 conference who challenged all the submitted papers in order to produce the final program but also this special issue. CRiSIS 2012 would not have been possible without the financial sponsorship from the Cork Constraint Computation Centre at University College Cork and the FP7 Network of

Excellence on Engineering Secure Future Internet Software Services and Systems (NESSOS).

Fabio Martinelli
Jean-Louis Lanet
Guest Editors
IJSSE