GUEST EDITORIAL PREFACE

Special Issue on CRiSIS'11

Frédéric Cuppens, Télécom Bretagne, Campus de Rennes, Cesson Sévigné, France

Simon N. Foley, Department of Computer Science, University College Cork, Cork, Ireland

The sixth International Conference on Risks and Security of Internet and Systems (CRiSIS) was held in Timisoara, Romania from September 26 to September 28, 2011. This yearly conference is technically co-sponsored by the IEEE Computer Society (Technical Committee on Security and Privacy) and offers valuable research contributions to the field of security in Internet-related applications, networks and systems. The conference was an overwhelming success with 11 full-length and 4 short papers accepted for presentation, an invited talk and two tutorials.

This special issue contains revised and extended versions of three papers that were presented at CRiSIS2011. The papers are representative of the conference theme: the development of efficient security systems that are resilient to attack. In particular, the selected papers consider cryptographic algorithm performance, replication schemes that help defend against attack and how trust measures can be used to help manage risk of attack.

Cryptographic hash functions are at the heart of many mechanisms that are used to secure the Internet and systems and it is important that these operations are carried out in an efficient manner. In *Performance improvements for SHA-3 finalists by exploiting microcontroller on-chip parallelism*, Pal-Stefan Murvay and Bogdan Groza consider how parallelism inherent in the algorithms of the SHA-3 finalists can be exploited in order to improve performance. A series of experiments are described that compare the implementation of SHA-2 and SHA-3 finalist algorithms on a micro-controller that is commonly used in the automotive industry. The results provide useful insights on the implementation of these algorithms and point to the parallelism potentially providing between 10% and 70% speedup, depending on the algorithm used.

The paper *Optimal Voting Strategy Against Rational Attacks* by Li Wang, Zheng Li and Shangping Ren continues this theme of security mechanism efficiency. Security mechanisms may use replication techniques as a means to provide resilience to attack and failure; the challenge is to devise schemes that minimize the voting overhead while ensuring maximal resilience. By considering the case whereby the system is composed of multiple clusters, each with the same number of replicas, the authors describe how to determine the optimal number of participating voters in each cluster in a manner that maximizes the number of surviving clusters.

Security risk management is an approach to monitoring the degree to which a system meets its security objectives, that is, the risk that it is not resilient to attack. In the paper, *Trust based interdependency weighting for on-line risk monitoring in interdependent critical infrastructures*, Filipe Caldeira and his co-authors describe an approach whereby measures of the trust relationships between different systems and their component are used to help determine overall degrees of security risk of the combined system. The approach is evaluated using a case study which considers the security risks in the interoperation of the separate, but inter-dependent, network infrastructure and computing grid that makes up Grid'5000.

The International Conference on Risks and Security of Internet and Systems provides an excellent venue for researchers to meet and to exchange ideas. We would like to thank the CRiSIS 2011 General Chair, local organizers, Programme Committee members and authors, without whom the conference would not have been possible.

Frédéric Cuppens
Simon N. Foley
Guest Editors
IJSSE

Frédéric Cuppens is a full professor at TELECOM Bretagne of Institut Mines-TELECOM and co-responsible of the CNRS LabSTICC SFIIS team on security, reliability and integrity of systems and information. He holds an engineering degree in computer science, a PhD and an HDR (Habilitation to supervise research). His research interests include formalization and deployment of security policies, access control to network and information systems, intrusion detection, reponse and counter-measures. He has published more than 150 technical papers in refereed journals and conference proceedings. He served as Programme Committee Chair of several conferences including ESORICS 2000, IFIP SEC 2004, SETOP 2008, CRISIS 2011, PST 2011 and DBSEC 2012.

Simon Foley is a Statutory Lecturer in Computer Science at University College Cork where he leads the security group based in the Cork Constraint Computation Centre. His research interests include distributed security, security modeling, security configuration, risk management and security psychology. Prior to his current appointment he was at Odyssey Research Associates NY and Cranfield IT Institute UK, and has held visiting positions at SRI International, Cambridge University and IBM. Dr. Foley currently serves on the Editorial Board of the Journal of Computer Security.