Journal of Computer Security 23 (2015) 539–540
DOI 10.3233/JCS-150537
IOS Press

Editorial

Special issue on security and high performance computing systems

Luca Spalazzi [a] and Luca Viganò [b,*]

[a] *Dipartimento di Ingegneria dell'Informazione, Università Politecnica delle Marche, Via Brecce Bianche, I-60131 Ancona, Italy*
E-mail: spalazzi@dii.univpm.it
[b] *Department of Informatics, King's College London, Strand, London WC2R 2LS, UK*
E-mail: luca.vigano@kcl.ac.uk

1. Introduction

Providing high performance computing and security is a challenging task. On the one hand, Internet, operating systems and distributed environments currently suffer from poor security support and cannot resist common attacks. On the other hand, adding security measures typically degrades performance. The relationships between security and high performance computing systems thus raise a number of problems and challenges such as the following ones:

(1) How to enforce security requirements in high performance computing systems. For instance, which kind of obfuscation techniques can enforce privacy in a cloud storage, or how grid security can be verified at design-time (formal verification) or at run-time (run-time verification). In this case, safety properties can also be addressed, such as availability and fault tolerance for high performance computing systems.
(2) How to use high performance computing systems to solve security problems. For instance, a grid computation can break an encryption code, and a cluster can support high performance intrusion detection or a distributed formal verification system. More generally, this topic addresses every efficient use of a high performance computing systems to improve security.
(3) The tradeoffs between maintaining high performance and achieving security in computing systems and solutions to balance the two objectives. In all these directions, various formal analyses, as well as performance analyses or monitoring techniques can be conducted to show the efficiency of a security infrastructure.

*Corresponding author: Luca Viganò, Department of Informatics, King's College London, Strand, London WC2R 2LS, UK. E-mail: luca.vigano@kcl.ac.uk.

This special issue is the result of a selection of the papers that were submitted to an open call for submissions from academia and industry tackling challenges such as the above ones and presenting novel research on all theoretical and practical aspects of computer and network security (with practical relevance to the construction, evaluation, application, or operation of secure systems), as well as case studies and implementation experiences. After a thorough reviewing, four papers were selected for publication:

- "Design and performance analysis of efficient KECCAK tree hashing on GPU architectures", by Sonia Lopez Alarcon, Jason Lowden and Marcin Lukowiak. This work focuses on the hashing algorithm Keccak. In particular, the authors present an efficient implementation of this algorithm using a GPU. Furthermore, they analyse how parameter configuration impacts performances.
- "Service security and privacy as a socio-technical problem (Literature review, analysis methodology and challenge domains)", by Giampaolo Bella, Paul Curzon and Gabriele Lenzini. This work focuses on security and privacy for service computing. It proposes a new design methodology considering service security and privacy from a socio-technical perspective that combines formal methods and empirical methods.
- "Brandt's fully private auction protocol revisited", by Jannik Dreier, Jean-Guillaume Dumas and Pascal Lafourcade. This work focuses on electronic auctions. In particular, the authors formally analyse Brandt's Fully Private Auction Protocol, show that this protocol is vulnerable to attacks by dishonest bidders, and suggest some countermeasures to address the discovered flaws. This work is related to high performance computing in two ways: auctions are used in grid computing to establish optimal scheduling, and the authors propose a high performance implementation of Brandt's protocol.
- "Measuring and estimating power consumption in Android to support energy-based intrusion detection", by Alessio Merlo, Mauro Migliardi and Paolo Fontanelli. This work focuses on intrusion detection for mobile devices. In particular, the authors propose a power-consumption-based measurement methodology for the identification of security threats to Android based mobile devices.

Given the high number and quality of the papers submitted in response to our call, we had to be very selective. We thank the authors of all accepted papers and of all those submitted papers that were not selected for this special issue. We also thank the reviewers who made the selection work possible: Marco Baldi, Guido Bertoni, Roberto Carbone, Mauro Conti, Matteo Cristani, Paolo Giorgini, Dieter Hutter, Steve Kremer, Sam Malek, Jean Emerson Martina, Marius Minea, Sebastian Mödersheim, Jukka Nurminen, Serena Ponta, Jaime Ramos, Jun Pang, Massimiliano Sala, Suriadi Suriadi, Ruggero Sussella. Finally, we thank Andrew Myers and Pierangela Samarati, the Editors-in-Chief of this journal, for their support and for making this issue possible.