Editorial

Antonio F. Gómez Skarmeta

Departamento de Ingeniería de la Información y las Comunicaciones,
University of Murcia,
Campus de Espinardo s/n, Murcia, 30100, Spain
E-mail: skarmeta@um.es

Most of critical activities that rely on networked communication and information systems (CIS) are highly interconnected. CIS performance could be jeopardised by incidents of various kinds. Within Europe a special attention within the research community and the European Union framework program has been put in a look for a multi-disciplinary approach to leverage their dependability by an alliance of three approaches:

- Modelling and simulation: by means of innovative approaches and tools to design, model, simulate, and plan critical infrastructures to dramatically improve their resilience.
- Detection: integrates various detection mechanisms to ensure fast detection of severe incidents but also to detect complex ones based on a combination of seemingly unrelated events, or on an abnormal behaviour.
- Response: provides frameworks for computer-aided counter-measures initiatives to respond in a quick and appropriate way to a large range of incidents to mitigate the threats to the dependability and rapidly thwarts the problem. CIS re-configuration is the utmost mechanism for their survivability.

Within this context the DESEREC FP6 project funded by the European Commission has proposed a workshop under the umbrella of the SECURWARE2008 conference, under the title DEPEND 2008: Dependability in Complex Systems and Applications, where 16 papers were presented providing experiences and results coming from different R&D projects like the ones in the EC 6th framework program, but also from other research activities. Two of them have been selected as representative of the results presented in that workshop, and will help to provide an innovative vision for researchers working in this area.

Aime, Pomi and Vallini introduced a methodology and associated techniques for automating the selection and configuration of dependability controls in large information systems. The process starts from a service-level representation of the target dependability requirements and computes a set of per-device abstract configurations to be used with remote system management suites like Microsoft SMS or IBM Tivoli. The methodology inspires to well-established practices from information risk analysis, and pushes forward their level of formalisation and automation. This is achieved by defining an ontology for information dependability controls and configurations. The configuration synthesis is rule-based, where rules are defined as transformations over the elements of the ontology.

Finally Martínez Pérez et al. designed a multi-layer architecture to detect complex attacks by correlating isolated alerts into attack scenarios which are composed of several

single steps that any attacker could execute. This architecture gives system administrators the ability of detecting this sort of attacks without adding new detection rules to the underlying IDSes when possible variations of the same attack arise. In this sense, two probabilistic values are calculated in runtime for pointing out which is the confidence level that the system has in detecting each of these attacks. A complete performance measurement study is also described in detail to demonstrate the feasibility in the implantation of this architecture in real environments.

We would like to thank all the authors and reviewers for their contributions and devoted efforts. Thanks are also due to the Editor-in-Chief Dr. Francesco Flammini, for hosting this special issue.