Journal of Computer Security 20 (2012) 1
DOI 10.3233/JCS-2011-0438
IOS Press

Preface

This issue of the *Journal of Computer Security* contains three papers that originally appeared at the *Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (ARSPA-WITS'10)*. The workshop was held on March 27–28, 2010, in Paphos, Cyprus, and affiliated with ETAPS 2010. The workshop brought together researchers interested in developing and applying formal techniques in the development of security-related applications.

The three papers in this issue are significant extensions of the workshop papers, and were reviewed according to the normal *Journal of Computer Security* procedures.

The first paper, "Quantitative information flow in interactive systems", by Mário Alvim, Miguel Andrés and Catuscia Palamidessi, considers information flow in a system where secrets and observables alternate during the computation. The authors show that if secrets can depend on the observables, then the system cannot be modelled validly by a classical information-theoretic channel. Instead, they show that this setting corresponds to the notion of channels with memory and feedback. Finally, they show that the channel capacity is a continuous function of a pseudometric based on the Kantorovich metric.

The second paper, "Iterative enforcement by suppression: Towards practical enforcement theories", by Nataliia Bielova and Fabio Massacci, considers run-time security enforcement mechanisms. Such mechanisms aim to suppress bad behaviours of a monitored system (i.e., behaviours that do not satisfy the security policy) while not changing good behaviours. The authors observe that when a system does have a bad behaviour, there may be many ways of suppressing it, some of which may be more desirable than others. They define a notion of *"better" enforcement*, based on the number of elements from the original execution that should be suppressed in order to obtain a legal execution. They then propose a new class of enforcement mechanism, which they show is better than the previously proposed longest-valid-prefix mechanism.

The final paper, "Modular plans for secure service composition", by Gabriele Costa, Pierpaolo Degano and Fabio Martinelli, considers service networks built from open services, i.e. services with unknown components. The authors model services in a variant of the λ-calculus; compliance of a service to a local policy is established by model checking a safe abstraction of the service obtained from a type-and-effect system. The authors describe *orchestration plans*, which drives the execution at run-time, mapping requests to services. Finally, they define a composition strategy for safely synthesizing a global orchestration plan.

Alessandro Armando
Gavin Lowe