Journal of Computer Security 17 (2009) 515
DOI 10.3233/JCS-2009-0396
IOS Press


# Introduction

The 18th meeting of the IEEE Computer Security Foundations Workshop, which has since become the IEEE Computer Security Foundations Symposium, was held in Aix-en-Provence in June 2005. The twenty presented papers were selected from 92 submissions. Expanded and revised versions of seven of these papers now appear in this issue of the *Journal of Computer Security*.

Two of these papers are devoted to those flows of information in a program that do not conform to a fixed traditional information flow policy. The paper by Sabelfeld and Sands provides a classification of a great deal of past work in this area – often referred to under the label "declassification" – and indeed has shaped many subsequent approaches to the problem. Boudol and Matos give a language-based approach to *local* information flow policies, i.e. policies based on partial orders of sensitivity that may vary from one syntactic region of a program to another.

The papers by Harrison and Hook, and by Clarkson, Myers and Schneider, are also related to information flow, but in different ways. The latter provides an epistemologically motivated view of the amount of information that flows to an adversary interacting with a program. The former provides a monad-based discipline for the development of kernels that respect information-flow policies.

Hofheinz, Müller-Quade and Unruh offer the most specifically cryptographic of these papers, focused on a foundational question in the reactive simulatability approach to protocol security. This is the question what "tractable execution" should mean when an adversary and an honest party may interact and make work for each other. Adão, Bana, Herzog and Scedrov relate cryptography to symbolic methods for analyzing security, showing the faithfulness of a symbolic model in cases that may involve key-cycles and partial disclosure. For instance, cryptography finds it difficult to disguise the length of a plaintext completely, and some forms of cryptography may disclose whether two messages were prepared using the same key.

Finally, Bartoletti, Degano and Ferrari discuss secure service-based computing, a form of distributed computation in which remote methods may be chosen according to the contract they promise to satisfy. The authors show how to ensure satisfaction of a global policy using this local, per-decision information.

This selection was intended to illustrate the range and rigor of current foundational work in information security. CSF has long served as meeting ground for this conversation.

Joshua D. Guttman
*Worcester Polytechnic Institute*