Journal of Computer Security 20 (2012) 635–636
DOI 10.3233/JCS-2012-0445
IOS Press

Preface

Central to the challenge of making computers secure is the very theory of computer security. A full understanding of computer security is lacking, and it is difficult to rigorously enforce even the models we do understand. Shedding light on the theory of computer security is the focus of the *IEEE Computer Security Foundations Symposium (CSF)*, an annual conference for computer security researchers. CSF covers all theoretical aspects of computer security, including formal models and verification methods. The 2010 conference was the 23rd in the series. We invited the authors of some of the excellent papers appearing in that conference to submit expanded versions to the *Journal of Computer Security*. Based on a full peer review process, just three of these submissions were judged ready to be accepted to this special issue featuring some of the high-quality work ongoing in the theory of computer security.

In "Required information release", Stephen Chong introduces a new kind of policy for information security. Previous models of information security have focused on preventing release of information and on defining conditions in which information *may* be released. Chong identifies real-world situations in which applications are *required* to release some information and develops a formal theory for describing this information security property.

Computer systems rely on increasingly complex authorization mechanisms to control access to resources. In many cases the policies controlling access may be confidential. A danger is that an adversary may learn about these policies by probing them through access attempts. Moritz Becker's paper "Information flow in trust management systems" studies what information can be learned about policies by probing attacks in a credential-based authorization system, showing connections to but also differences from prior work on information flow security.

Computerized voting systems are increasingly important. But they are also uniquely demanding from the computer security standpoint, because they must balance multiple security objectives that are in tension with each other. One of the most challenging security goals is coercion resistance, which prevents vote buying and coerced voting. In "A game-based definition of coercion resistance and its applications", Ralf Küsters, Tomasz Truderung and Andreas Vogt present a new way to quantitatively characterize coercion resistance, and show that some well-known voting systems are not as coercion resistant as we might like.

We would like to thank the many people who helped make this special issue possible. These include the external reviewers, who put many hours into reviewing submitted papers, and provided many thoughtful suggestions. The *JCS* Editors-in-Chief, John Mitchell and Pierangela Samarati, provided guidance through the process. We also thank Kim Willems and others at IOS Press who put the Special Issue together.

We hope that you will enjoy this collection of excellent papers and find them as interesting and thought-provoking as we have.

Andrew Myers and Michael Backes
Guest Editors