Guest Editorial: Special Issue on Computer and Communications Security

This special issue contains extended versions of articles selected from the program of the 13th ACM Conference on Computer and Communications Security (CCS'06), which took place October 30 to November 3, 2006 in Alexandria, Virginia (USA). This annual conference is a leading international forum for information security researchers, practitioners, developers, and users to explore cutting-edge ideas and results, and to exchange techniques, tools, and experiences. Its mission is to promote and share novel research from academia, government, and industry covering all theoretical and practical aspects of computer security, as well as case studies and implementation experiences. The selected articles represent the broad scope of the conference, covering topics such as enforcement of security and privacy properties, detection of bugs and exploits, and understanding and preventing attacks that make use of current Web and e-mail infrastructures.

The articles in this special issue were invited for submission from the 38 articles presented at CCS'06 (which in turn were selected from 256 articles submitted to the conference). The submissions to the special issue were required to contain at least 25% new material beyond the conference articles. All the journal submissions went through an additional thorough review process to further ensure their quality. (The journal editor-in-chief was not involved in the decision-making process for the article of which he is a coauthor.)

The first article, "Enforcing Safety and Consistency Constraints in Policy-Based Authorization Systems" by Adam J. Lee and Marianne Winslett, addresses the issue of view consistency in policy-based authorization systems. The article provides algorithms that achieve consistency and safety, and also highlights design tradeoffs among such algorithms. In their article, "Data Collection with Self-Enforcing Privacy," Philippe Golle, Frank McSherry, and Ilya Mironov demonstrate cryptographic protocols that allow polls to be conducted in such a way that any leakage of private data by the pollster can be detected.

Cadar et al.'s article "EXE: Automatically Generating Inputs of Death" describes a bug-finding tool that automatically finds software bugs along with test cases that trigger them. In "Fast and Black-box Exploit Detection and Signature Generation for Commodity Software," Wang et al. introduce packet vaccines as a way to protect against software control-flow hijacking. Their method does not require access to the source code, so it works well even with commodity software.

In “Puppetnets: Misusing Web Browsers as a Distributed Attack Infrastructure,” Antonatos et al. demonstrate that an attacker can use existing Web languages, protocols, and security policies to create powerful botnet-like attack infrastructures. They also describe several partial countermeasures to reduce the effectiveness of such attacks. Finally, in their article “Thwarting E-mail Spam Laundering,” Mengjun Xie, Heng Yin, and Haining Wang discuss ways to detect and suppress proxy-based spam activities—which are an enabling factor in the current spam epidemic—close to their sources.

We are thankful to all who contributed to this special issue: the referees for their helpful and insightful comments, the authors for their hard work and their patience, and Editor-in-Chief Michael Reiter for his encouragement and support.

—REBECCA N. WRIGHT
SABRINA DE CAPITANI DI VIMERCATI
Guest Editors