Preface

Today, 25 years since its creation, the world-wide web has taken over the world as the global computing platform. The pace of development has been tremendous in the most recent years. A package of technologies, often referred to as Web 2.0, has revolutionized the web to move from a static client-server paradigm to a highly dynamic and interactive paradigm for computation by multiple servers and clients. The complexity of the web technology and the ever increasing reliance of the society on the web poses a grand challenge of securing the web.

Securing *web applications* calls for particular attention of security researchers. The power of web applications drives the evolution of the web, which makes *securing web applications* a critical goal. The Open Web Application Security Project (OWASP) is an example of a successful effort to consolidate the community of practitioners around the problem of web application security. Efforts are also taking place to consolidate the research community on this important problem. A notable recent event, Dagstuhl Seminar on web application security, which we organized at Schloss Dagstuhl, Germany, in October 2012, which was a successful step in this direction.

Another important step of consolidating research on web application security is this special issue: the focus of this special issue is *web application security*. Submitted articles were reviewed by referees according to the journal standards. As a result of the reviewing process, four excellent articles were selected for inclusion in the special issue. The articles address a landscape of security issues for web applications: from securing JavaScript and other executable content in the browser to securing cross-origin authorization protocols.

Two of the articles deal with securing JavaScript in the browser. The article by W. De Groef, D. Devriese, N. Nikiforakis, and F. Piessens presents FlowFox: a web browser with flexible and precise information flow control. FlowFox enforces fine-grained information-flow control for scripts in the browser. FlowFox is based on secure multi-execution, executing script multiple times - at different security levels with their inputs and outputs carefully synchronized.

The article by J. Gibbs Politz, S. Aristides Eliopoulos, A. Guha, S. Krishnamurthi presents ADsafety: Type-based verification of JavaScript sandboxing. The main contribution is a type system for JavaScript that guarantees sandboxing properties. The article demonstrates the effectiveness of the type system for the ADsafe subset of JavaScript.

The article by M. Heiderich, M. Niemietz, F. Schuster, T. Holz, and J.

Schwenk presents scriptless attacks: stealing the pie without touching the sill. This article explores malicious executable content beyond conventional malicious JavaScript, abusing Cascading Style Sheets (CSS) and Scalable Vector Graphics (SVG) features. It is striking how much can be done in a browser even when no scripts are allowed to run.

The article by C. Bansal, K. Bhargavan, and S.Maffeis studies discovering concrete attacks on website authorization by formal analysis. At the core of it is the WebSpy formalization that is used to model such protocols as OAuth 2.0 and identify previously unknown vulnerabilities in popular websites.

We wish to thank the authors for the hard work on submissions and the referees for their substantial and useful reviews.

Lieven Desmet
Katholieke Universiteit Leuven
Leuven, Belgium

Martin Johns
SAP Research
Karlsruhe, Germany

Benjamin Livshits
Microsoft Research
Redmond, USA

Andrei Sabelfeld
Chalmers University of Technology
Gothenburg, Sweden