



Server-driven Outbound Web-application Sandboxing
FP7-ICT-2009-5, Project No. 256964

<https://www.websand.eu>

Deliverable D6.1 (M42)

Dissemination plan

Abstract

This dissemination plan reports on the dissemination activities of WebSand. In particular, dissemination via publications, participation at academic and industrial events, training and community transfer are described.

Deliverable details

Deliverable version: *v3.0*

Date of delivery: *30.04.2014*

Editors: *Lieven Desmet and Frank Piessens*

Classification: *public*

Due on: *M42*

Total pages: *40*

List of Contributors:

Bastian Braun, Jorge Cuellar, Lieven Desmet, Martin Johns, Peng Liu, Frank Piessens, Joachim Posega, Andrei Sabelfeld, David Sands, Phu Phung, Jan Wolff

Project details

Start date: *October 01, 2010*

Project Coordinator: *Martin Johns*

Partners: *SAP, Siemens, CHALMERS, KUL, UNI PASSAU*

Duration: *42 months*



Document revision history

	Responsible	Date
Initial revision (M12)	Lieven Desmet	September 29th, 2011
Review	Martin Johns	September 30th, 2011
Final version (M12)	Lieven Desmet	September 30th, 2011
Initial revision (M24)	Lieven Desmet	September 24th, 2012
Review	Walter Tighzert	September 24th, 2012
Final version (M24)	Lieven Desmet	September 25th, 2012
Initial revision (M42)	Lieven Desmet	April 28th, 2014
Review	Martin Johns	April 29th, 2014
Final version (M42)	Lieven Desmet	April 30th, 2014

Contents

1	Introduction	4
2	Publications	4
3	Events	14
3.1	WebSand organized events	14
3.2	Participation in national and international events	15
4	Training	22
4.1	Industrial and academic training	22
4.2	Academic courses and theses	23
5	Community transfer and communication	27
5.1	OWASP, ENISA and W3C	27
5.2	Collaboration with other projects	29
5.3	WebSand portal	31
5.4	Communication	31

1 Introduction

This dissemination plan reports on the dissemination activities during the full lifespan of WebSand. In particular, dissemination via publications (Section 2), participation at academic and industrial events (Section 3), training (Section 4) and community transfer and communication (Section 5) are described.

2 Publications

The results of the WebSand project have been disseminated by participating in international conferences and workshops in the areas of software security and software engineering.

As part of the dissemination activities in WebSand, research results have been presented and published at major conferences and high-profile workshops in this area, such as the European Symposium on Research in Computer Security (ESORICS), the IEEE Computer Security Foundations Symposium (CSF), the Annual Computer Security Applications Conference (ACSAC), the European Symposium on Programming (ESOP), the ACM Symposium on Applied Computing (SAC), the Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), the ACM Symposium on Information, Computer and Communications Security (AsiaCCS), the ACM Conference on Computer and Communications Security (CCS), the International Symposium on Research in Attacks, Intrusions and Defenses (RAID), the IFIP International Conference on Formal Techniques for Distributed Systems (FMOODS/FORTE), the Workshop on Web 2.0 Security and Privacy (W2SP), the USENIX Workshop on Offensive Technologies (WOOT), the ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS).

The full list of WebSand publications are enumerated on the next pages.

Type	Venue	Publication	Partner(s)
Conference	NordSec 2010	Filippo Del Tedesco, Alejandro Russo, David Sands, Implementing erasure policies using taint analysis, 15th Nordic Conference in Secure IT Systems, LNCS, October 2010 [31]	CHALMERS
Conference	NordSec 2010	Philippe De Ryck, Maarten Decat, Lieven Desmet, Frank Piessens, and Wouter Joosen. Security of Web Mashups: a Survey. To appear in Proceedings of the 15th Nordic Conference in Secure IT Systems (NordSec 2010), LNCS. Springer Verlag, October 2010 [23]	KUL
Conference	NordSec 2010	Jonas Magazinius, Phu H. Phung, and David Sands. Safe wrappers and sane policies for self-protecting JavaScript. In Tuomas Aura, editor, The 15th Nordic Conference in Secure IT Systems, LNCS. Springer Verlag, October 2010 [58]	CHALMERS
Conference	GI Sicherheit 2010	Michael Schrank, Bastian Braun, Martin Johns, Joachim Posegga. Session Fixation - the Forgotten Vulnerability?, in 5th conference on "Sicherheit, Schutz und Zuverlassigkeit" (GI Sicherheit 2010), Lecture Notes in Informatics (LNI), October 2010 [72]	UNI PASSAU, SAP
Conference	ICISS 2010	Arnar Birgisson, Alejandro Russo, Andrei Sabelfeld, Unifying Facets of Information Integrity, International Conference on Information Systems Security (ICISS), Gandhinagar, India, December 2010, LNCS, Springer-Verlag [7]	CHALMERS
Conference	ESSoS 2011	Nick Nikiforakis, Wannes Meert, Yves Younan, Martin Johns and Wouter Joosen. SessionShield: Lightweight Protection against Session Hijacking. Proceedings of the 3rd International Symposium on Engineering Secure Software and Systems (ESSoS 2011), Madrid, Spain [66]	KUL, SAP
Report		Natalia Bielova, Dominique Devriese, Fabio Massacci, Frank Piessens, Reactive non-interference for the browser: extended version, Technical Report (CW Reports), volume CW602, Department of Computer Science, K.U.Leuven, February 2011 [6]	KUL
Conference	SAC 2011	Martin Johns, Bastian Braun, Michael Schrank, Joachim Posegga, 26th ACM Symposium on Applied Computing (SAC 2011), Security Track, March 2011 [45]	SAP, UNI PASSAU
Conference	SECTEST'11	Martin Johns, Moritz Jodeit. Scanstud: A Methodology for Systematic, Fine-grained Evaluation of Static Analysis Tools, in Second International Workshop on Security Testing (SECTEST'11), March 2011 [42]	SAP
Conference	ESOP 2011	S. Hunt, David Sands, From exponential to polynomial-time security typing via principal types, Programming Languages and Systems, 20th European Symposium on Programming, ESOP 2011 [41]	CHALMERS
Conference	EuroSec 2011	Nick Nikiforakis, Wouter Joosen, Martin Johns, Abusing locality in shared web hosting, European Workshop on System Security, Austria, 10 April 2011 [63]	SAP, KUL

Type	Venue	Publication	Partner(s)
Conference	W2SP 2011	Sebastian Lekies, Martin Johns, Walter Tighzert. The State of the Cross-domain Nation, in 5th workshop on Web 2.0 Security and Privacy (W2SP 2011), May, 2011 [53]	SAP
Conference	PLAS 2011	Willard Rafnsson, Andrei Sabelfeld, Limiting Information Leakage in Event-based Communication, ACM SIGPLAN Workshop on Programming Languages and Analysis for Security, San Jose, CA, June 2011 [68]	CHALMERS
Conference	PLAS 2011	Arnar Birgisson, Alejandro Russo, Andrei Sabelfeld, Capabilities for information flow, ACM SIGPLAN Workshop on Programming Languages and Analysis for Security, San Jose, CA, June 2011 [9]	CHALMERS
Conference	CSF 2011	Heiko Mantel, David Sands and Hemming Sudbrock. Assumptions and Guarantees for Compositional Noninterference, In Proceedings of the 24th IEEE Computer Security Foundations Symposium. IEEE Computer Society, 2011 [61]	CHALMERS
Conference	DIMVA 2011	Martin Johns, Sebastian Lekies. Biting the Hand That Serves You: A closer look at client-side Flash proxies for cross-domain requests, in Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2011), LNCS, Springer Verlag, July, 2011 [46]	SAP
Conference	NSS 2011	Natalia Bielova, Dominique Devriese, Fabio Massacci, Frank Piessens, Reactive non-interference for a browser model, Proceedings of the 5th International Conference on Network and System Security (NSS 2011), Milan, Italy, 6-8 September 2011 [5]	KUL
Conference	ESORICS 2011	Philippe De Ryck, Lieven Desmet, Wouter Joosen, Frank Piessens, Automatic and precise client-side protection against CSRF attacks, European Symposium on Research in Computer Security (ESORICS 2011), Lecture Notes in Computer Science, volume 6879, pages 100-116, Leuven, Belgium, 12-14 September 2011 [24]	KUL
Conference	ESORICS 2011	Arnar Birgisson, Andrei Sabelfeld, Multi-run security, European Symposium on Research in Computer Security (ESORICS), Leuven, Belgium, September 2011 [10]	CHALMERS
Conference	ACSAC 2011	Steven Van Acker, Philippe De Ryck, Lieven Desmet, Frank Piessens, Wouter Joosen, WebJail: Least-privilege integration of third-party components in web mashups, ACSAC, Orlando, Florida, USA, 5-9 December 2011 [75]	KUL
Conference	APLAS 2011	Jonas Magazinius, Aslan Askarov, Andrei Sabelfeld, Decentralized Delimited Release, Asian Symposium on Programming Languages and Systems (APLAS), Kenting, Taiwan, December 2011 [3]	CHALMERS

Type	Venue	Publication	Partner(s)
Conference	Sicherheit 2012	Sebastian Lekies, Walter Tighertz, Martin Johns: Towards stateless, client-side driven Cross-Site Request Forgery protection for Web applications, in in 5th conference on "Sicherheit, Schutz und Zuverlassigkeit" (GI Sicherheit 2012), Lecture Notes in Informatics (LNI), March 2012 [56]	SAP
Conference	SAC 2012	Jorge Cuellar, Martin Ochoa, Ruben Rios, Indistinguishable regions in geographic privacy, 27th ACM Symposium on Applied Computing (SAC 2011), Security Track, March 26-30 2012 [19]	SIEMENS
Journal	DuD	Martin Johns: HTML5-Security - Sicherer Umgang mit den neuen JavaScript APIs. In Datenschutz und Datensicherheit, 36(4): 231-235, April 2012 [43]	SAP
Report		Philippe De Ryck, Lieven Desmet, Frank Piessens, Wouter Joosen, A security analysis of emerging web standards - Extended version, Technical Report (CW Reports), volume CW622, Department of Computer Science, KU Leuven, May 2012 [26]	KUL
Conference	AsiaCCS 2012	Steven Van Acker, Nick Nikiforakis, Lieven Desmet, Wouter Joosen, Frank Piessens, FlashOver: Automated discovery of cross-site scripting vulnerabilities in rich internet applications, AsiaCCS, Seoul, 2-4 May 2012 [76]	KUL
Conference	W2SP 2012	Sebastian Lekies and Martin Johns: Lightweight Integrity Protection for Web Storage Content Caching. In 6th Workshop on Web 2.0 Security and Privacy (W2SP 2012), May 2012 [52]	SAP
Conference	JSTools '12	Phu H. Phung, Lieven Desmet, A two-tier sandbox architecture for untrusted JavaScript, Proceedings of the Workshop on JavaScript Tools (JSTools '12), pages 1-10, Beijing, China, 13 June 2012 [67]	CHALMERS, KUL
Conference	DAIS 2012	Philippe De Ryck, Nick Nikiforakis, Lieven Desmet, Frank Piessens, Wouter Joosen, Serene: Self-reliant client-side protection against session fixation, 12th IFIP International Conference on Distributed Applications and Interoperable Systems, pages 59-72, Stockholm, Sweden, 13-15 June 2012 [30]	KUL
Conference	FMOODS/ FORTE 2012	Gilles Barthe, Juan Manuel Crespo, Dominique Devriese, Frank Piessens, Exequiel Rivas, Secure multi-execution through static program transformation, Formal Techniques for Distributed Systems (FMOODS/FORTE 2012), volume 7273, pages 186-202, Stockholm, 13-16 June 2012 [4]	KUL

Type	Venue	Publication	Partner(s)
Conference	CSF 2012	Daniel Hedlin, Andrei Sabelfeld, Information-Flow Security for a Core of JavaScript, Proceedings of the IEEE Computer Security Foundations Symposium, Harvard University, Cambridge MA, June 25-27, 2012. IEEE Computer Society Press. [40]	CHALMERS
Conference	CSF 2012	Willard Rafnsson, Daniel Hedlin, Andrei Sabelfeld, Securing Interactive Programs, Proceedings of the IEEE Computer Security Foundations Symposium, Harvard University, Cambridge MA, June 25-27, 2012. IEEE Computer Society Press. [69]	CHALMERS
Conference	SECURITY	Philippe De Ryck, Lieven Desmet, Frank Piessens, Wouter Joosen, A security analysis of emerging web standards - HTML5 and friends, from specification to implementation, Proceedings of the International Conference on Security and Cryptography (SECURITY), pages 257-262, Rome, Italy, 24-27 July 2012 [27]	KUL
Journal	DuD	Bastian Braun, Patrick Gemein, Benedikt Höfling, Michael Marc Maisch, Alexander Seidl, Angriffe auf OpenID und ihre strafrechtliche Bewertung - Cross-Site-Request-Forgery, Phishing und Clickjacking im Fokus, Datenschutz und Datensicherheit - DuD, Volume 36, Number 7 (2012), pp. 502-509 [11]	UNI PASSAU
Conference	WOOT 2012	Sebastian Lekies, Mario Heiderich, Dennis Appelt, Thorsten Holz, and Martin Johns: On the fragility and limitations of current Browser-provided Clickjacking protection schemes, in 6th USENIX Workshop on Offensive Technologies (WOOT '12), August 2012 [51]	SAP
Conference	MobiWIS 2012	Hong-Linh Truong, Phu H. Phung, Schahram Dustdar, Governing Bot-as-a-Service in Sustainability Platforms - Issues and Approaches, Proceedings of the 9th International Conference on Mobile Web Information Systems (MobiWIS), August 27-29, 2012, Niagara Falls, Ontario, Canada, Elsevier. [74]	CHALMERS
Conference	TrustBus 2012	Martin Johns, Joachim Posegga: WebSand: Server-Driven Outbound Web-Application Sandboxing. Trust, Privacy and Security in Digital Business (TrustBus 2012), September 2012 [50]	UNI PASSAU, SAP
Conference	TrustBus 2012	Bastian Braun, Stefan Kucher, Martin Johns, Joachim Posegga, A User-level Authentication Scheme to Mitigate Web Session-Based Vulnerabilities, Proceedings of 9th International Conference on Trust, Privacy & Security in Digital Business (TrustBus 2012), Lecture Notes in Computer Science, 2012, Volume 7449/2012, pp. 17-29 [16]	UNI PASSAU, SAP

Type	Venue	Publication	Partner(s)
Conference	ESORICS 2012	Arnar Birgisson, Daniel Hedin, Andrei Sabelfeld, Boosting the Permissiveness of Dynamic Information-Flow Tracking by Testing, Proceedings of the European Symposium on Research in Computer Security (ESORICS), Pisa, Italy, September 2012, LNCS, Springer-Verlag. [8]	CHALMERS
Conference	RAID 2012	Sebastian Lekies, Nick Nikiforakis, Walter Tighertz, Frank Piessens, and Martin Johns: DEMACRO: Defense against Malicious Cross-domain Requests. In 15th International Symposium on Research in Attacks, Intrusions and Defenses (RAID'12), September 2012 [54]	SAP, KUL
Journal	ITRB	Ermano Geuer, Einwilligung in Cookieempfang durch Browsereinstellungen?, Schlussfolgerungen aus einer Auslegung der gesetzlichen Regelung in Österreich (Consent into the reception of cookies through browser settings?, Conclusion of the interpretation of Austrian legislation), ITRB 2012, 206 [35]	UNI PASSAU
Conference	CCS 2012	Nick Nikiforakis, Luca Invernizzi, Alexandros Kapravelos, Steven Van Acker, Wouter Joosen, Christopher Kruegel, Frank Piessens, Giovanni Vigna, You are what you include: Large-scale evaluation of remote JavaScript inclusions, Proceedings of the 19th ACM conference on Computer and Communications Security (CCS 2012), Raleigh, NC, USA, 16-18 October 2012 [62]	KUL
Conference	CCS 2012	Willem De Groef, Dominique Devriese, Nick Nikiforakis, Frank Piessens, FlowFox: a web browser with flexible and precise information flow control, Proceedings of the 19th ACM conference on Computer and Communications Security (CCS 2012), Raleigh, NC, USA, 16-18 October 2012 [20]	KUL
Journal	AnwZert	Ermano Geuer, Der Cookie-Guide der britischen Internationalen Handelskammer (The Cookie Guide of the british ICC), AnwZert ITR 15/2012, Anm. 2 [34]	UNI PASSAU
Journal	AnwZert	Ermano Geuer, Keine Rechtssicherheit bei Safe Harbor-Selbstzertifizierungen (No legal certainty in case of Safe Harbor self certification), AnwZert ITR 16/2012, Anm. 2 [36]	UNI PASSAU
Journal	COSE	Jonas Magazinius, Alejandro Russo, Andrei Sabelfeld, On-the-fly Inlining of Dynamic Security Monitors, Computers & Security, Elsevier, October 2012. [60]	CHALMERS

Type	Venue	Publication	Partner(s)
Conference	ACSAC 2012	Pieter Agten, Steven Van Acker, Yoran Brondsema, Phu H. Phung, Lieven Desmet, Frank Piessens, JSand: Complete client-side sandboxing of third-party JavaScript without browser modifications, Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC 2012), pages 1-10, Orlando, Florida, USA, 3-7 December 2012 [2]	KUL
Conference	ACSAC 2012	BetterAuth: Web Authentication Revisited, in 28th Annual Computer Security Applications Conference (ACSAC '12) [49]	SAP, UNI PASSAU
Journal	TDSC	Willard Rafnsson, Keiko Nakata, Andrei Sabelfeld, Securing Class Initialization in Java-like Languages, IEEE Transactions on Dependable and Secure Computing, IEEE Computer Society Press, January 2013. [70]	CHALMERS
Conference	ESSoS 2013	Bastian Braun, Patrick Gemein, Hans P. Reiser, and Joachim Posegga. Control-Flow Integrity in Web Applications. In International Symposium on Engineering Secure Software and Systems (ESSoS 2013), Lecture Notes in Computer Science (LNCS), Springer, 2013. [12]	UNI PASSAU
Book chapter	IGI global	Willem De Groef, Dominique Devriese, Tom Reynaert, Frank Piessens, Security and privacy of online social network applications, Social Network Engineering for Secure Web Data and Services, pages 206-221, 2013 [22]	KUL
Conference	AsiaCCS 2013	Philippe De Ryck, Nick Nikiforakis, Lieven Desmet, Wouter Joosen, TabShots: Client-side detection of tabnabbing attacks, Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security (AsiaCCS), pages 447-455, Hangzhou, China, 8-10 May 2013 [29]	KUL
Conference	IEEE Security & Privacy	Nick Nikiforakis, Alexandros Kapravelos, Wouter Joosen, Christopher Kruegel, Frank Piessens, Giovanni Vigna, Cookieless monster: Exploring the ecosystem of web-based device fingerprinting, Proceedings of the 34th IEEE Symposium on Security & Privacy, pages 541-555, San Francisco, 19-22 May 2013 [64]	KUL
Conference	PLAS 2013	Per Hallgren, Daniel Mauritzson, Andrei Sabelfeld, GlassTube: A Lightweight Approach to Web Application Integrity, Proceedings of ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS), Seattle, WA, June 2013. [38]	CHALMERS
Conference	CSF 2013	Willard Rafnsson, Andrei Sabelfeld, Secure Multi-Execution: Fine-grained, Declassification-aware, and Transparent, Proceedings of ACM IEEE Computer Security Foundations Symposium (CSF), New Orleans, LA, June 2013. [71]	CHALMERS

Type	Venue	Publication	Partner(s)
Conference	DIMVA 2013	Martin Johns. PreparedJS: Secure Script-Templates for JavaScript, in 10th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA '13), July 2013 [44]	SAP
Conference	OWASP AppSec	Philippe De Ryck, Lieven Desmet, Frank Piessens, Wouter Joosen, Improving the security of session management in web applications, OWASP AppSec EU, 20-23 August 2013 [28]	KUL
Conference	NordSec 2013	Bastian Braun, Christian v. Pollak, and Joachim Posegga. A Survey on Control-Flow Integrity Means in Web Application Frameworks. In 18th Nordic Conference on Secure IT Systems (NordSec 2013), 2013. [17]	UNI PASSAU
Conference	USENIX Sec 2013	Martin Johns, Sebastian Lekies, Ben Stock. Eradicating DNS Rebinding with the Extended Same-Origin Policy, in 22nd USENIX Security Symposium (USENIX Security '13), August 2013 [48]	SAP
Conference	RAID 2013	Martin Johns, Sebastian Lekies. Tamper-resistant LikeJacking Protection, in 16th International Symposium on Research in Attacks, Intrusions and Defenses (RAID'13), October 2013 [47]	SAP
Conference	CCS 2013	Güneş Acar, Marc Juarez, Nick Nikiforakis, Claudia Diaz, Seda Gürses, Frank Piessens, Bart Preneel, FPDetective: Dusting the web for fingerprinters, Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS 2013), pages 1129-1140, November 05-09, 2013 [1]	KUL
Conference	CCS 2013	Sebastian Lekies, Ben Stock, Martin Johns. 25 Million Flows Later - Large-scale Detection of DOM-based XSS, Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS 2013), pages 1129-1140, November 05-09, 2013 [55]	SAP
Conference	CCS 2013	Jonas Magazinius, Billy K. Rios, A. Sabelfeld, Polyglots: Crossing Origins by Crossing Formats, Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS 2013), November 05-09, 2013 [59]	CHALMERS
Conference	ISC 2013	Ping Chen, Nick Nikiforakis, Christophe Huygens, Lieven Desmet, A dangerous mix: Large-scale analysis of mixed-content websites, Proceedings of the Information Security Conference (ISC), Dallas, Texas, USA, 13-15 November 2013 [18]	KUL
Journal	JCS	Willem De Groef, Dominique Devriese, Nick Nikiforakis, Frank Piessens, Secure multi-execution of web scripts: Theory and practice, Journal of Computer Security, volume 22, issue 4, pages 469-509, 2014 [21]	KUL

Type	Venue	Publication	Partner(s)
Conference	ESSoS 2014	Jonas Magazinius, Daniel Hedin, Andrei Sabelfeld, Architectures for Inlining Security Monitors in Web Application, In Proceedings of the International Symposium on Engineering Secure Software and Systems (ESSoS), Munich, Germany, February 2014. [57]	CHALMERS
Conference	ACM CO-DASPY 2014	Bastian Braun, Johannes Kästler, Martin Johns, and Joachim Posegga. PhishSafe: Leveraging Modern JavaScript APIÅs for Transparent and Robust Protection. In Fourth ACM Conference on Data and Application Security and Privacy (ACM CODASPY 2014), 2014. [15]	UNI PASSAU, SAP
Conference	SAC 2014	Daniel Hedin, Arnar Birgisson, Luciano Bello, Andrei Sabelfeld, JSFlow: Tracking Information Flow in JavaScript and its APIs, In Proceedings of the ACM Symposium on Applied Computing (SAC), Gyeongju, Korea, March 2014. [39]	CHALMERS
Conference	WWW 2014	Nick Nikiforakis, Federico Maggi, Gianluca Stringhini, M Zubair Rafique, Wouter Joosen, Christopher Kruegel, Frank Piessens, Giovanni Vigna, Stefano Zanero, Stranger danger: Exploring the ecosystem of ad-based URL shortening services, Proceedings of the 23rd International World Wide Web Conference (WWW 2014), Seoul, Korea, 7-11 April 2014 [65]	KUL
Conference	AsiaCCS 2014	Steven Van Acker, Nick Nikiforakis, Lieven Desmet, Frank Piessens, Wouter Joosen, Monkey-in-the-browser: Malware and vulnerabilities in augmented browsing script markets, AsiaCCS 2014, Kyoto, Japan, 2-4 June 2014 [77]	KUL
Conference	AsiaCCS 2014	Ben Stock, Martin Johns. Protecting Users Against XSS-based Password Manager Abuse, AsiaCCS 2014, Kyoto, Japan, 2-4 June 2014 [73]	SAP
Conference	IFIP SEC 2014	Bastian Braun, Caspar Gries, Benedikt Putschku, and Joachim Posegga. Ghostrail: Ad Hoc Control-Flow Integrity for Web Applications. In 29th IFIP International Information Security and Privacy Conference (IFIP SEC 2014), 2014. [13]	UNI PASSAU
Conference	IFIP SEC 2014	Bastian Braun, Martin Johns, Johannes Kästler, and Joachim Posegga. A Trusted UI for the Mobile Web. In 29th IFIP International Information Security and Privacy Conference (IFIP SEC 2014), 2014. [14]	UNI PASSAU, SAP
Conference	CSF 2014	Mathy Vanhoef, Willem De Groef, Dominique Devriese, Frank Piessens, Tamara Rezk.Stateful Declassification Policies for Event-Driven Programs. Proceedings of the 27th Computer Security Foundations Symposium (CSF 2014), Vienna, Austria, 19-22 July 2014. [78]	KUL

Type	Venue	Publication	Partner(s)
Conference	TRUST 2014	Tom Van Goethem, Ping Chen, Nick Nikiforakis, Lieven Desmet, Wouter Joosen, Large-scale security analysis of the web: Challenges and Findings, 7th International Conference on Trust & Trustworthy Computing (TRUST 2014), Crete, Greece, 30 July - 2 August 2014 [37]	KUL

3 Events

3.1 WebSand organized events

WebSand organized a yearly event to bring together researchers in the web application community and disseminate results of the WebSand project.

The first event has been organized by Chalmers at 13-14 April 2011, and consisted of a 1,5 day workshop. This event brought researchers from the consortium and research peers together in an informal setting to present and discuss novel work in the context of WebSand. Apart from the consortium partners, external participants have been invited from KTH, Imperial College and OWASP Sweden. John Wilander (OWASP Sweden) and Sergio Maffeis (Imperial College, UK) gave invited talks.

For the second WebSand event, a 5-day Dagstuhl seminar on “Web Application Security” (Seminar no. 12401) has successfully been organized from 1 to 5 October 2012, by three WebSand leaders (Lieven Desmet, Martin Johns and Andrei Sabelfeld) and Ben Livshits (Microsoft Research, US).

The seminar brought 44 web security researchers together, coming from companies and research institutions across Europe and the US. The seminar had a well-filled program, with 3 keynotes, 28 research talks, and 15 5-minute talks. The topics that were presented and discussed during the seminar were closely themed around the technical challenges of the WebSand project. The full workshop report is available at [32].

As an important post-seminar dissemination activity, we launched a *special issue of the Journal of Computer Security (JCS)* dedicated to *Web Application Security*. The guest editors of the issue are the Web Application Security Dagstuhl seminar organizers, with three out of the four being WebSand affiliates. 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. We are happy to report that we have achieved high-quality processing of the submitted articles as well as their fast turn-around. The issue [33] has been recently finalized and already published by IOS Press.

The third event, the WASR 2013 workshop, has been co-organized with three other FP7 projects: NESSoS, STREWS and SPACIOS.

The First European workshop on Web Application Security Research¹ took place in Hamburg (Germany) on August 21st 2013, . To attract both

¹<http://2013.appsec.eu/wasr/>

researchers and practitioners, the workshop was co-located with the OWASP Research conference.

The workshop was a success with over 50 registered attendees, including representatives of all major browser vendors, people from the German Web economy (Xing, Zalando, BitPlaces) and members of the global OWASP board.

Members of the WebSand consortium gave the following WebSand related presentations at the workshop:

- Lieven Desmet (KU Leuven): “Server-driven sandboxing of JavaScript”
- Sebastian Lekies (SAP): “Large-scale Detection of DOM-based XSS”
- Ben Stock (SAP): “Eradicating DNS Rebinding with the Extended Same-Origin Policy”
- Jonas Magazinius (Chalmers): “Architectures for Inlining Security Monitors in Web Applications”
- Bastian Braun (Passau): “LogSec – A Smart Browser for Secure Web Sessions”
- Willem De Groef (KU Leuven): “Recent work on applications of SME on the server-side”

3.2 Participation in national and international events

The WebSand consortium partners have participated in various national and international academic conferences and industry events to disseminate results of the WebSand project as well as to network with peers from academia and industry.

The full list of participations in events is enumerated on the next pages.

Event name	Participation	Date	Location	Partner(s)
ISSE 2010: GI Sicherheit	Academic dissemination of research results [72]	05/10/2010 - 07/10/2010	Berlin, Germany	UNI PASSAU
TU Darmstadt	Colloquium / invited talks	14/10/2010	Darmstadt, Germany	CHALMERS
it-sa 2010	Participation at academia/industry event	19/10/2010-21/10/2010	Nuremberg, Germany	SIEMENS
OWASP AppSec Germany 2010	Participation at industry event	20/10/2010	Nuremberg, Germany	SIEMENS
Nordsec 2010	Academic dissemination of research results [23, 31, 58]	27/10/2010 - 30/10/2010	Espoo, Finland	KUL, CHALMERS
NWPT 2010	Academic dissemination of research results	10/11/2011 - 12/11/2011	Turku, Finland	CHALMERS
Future Internet Week	Booth at industry event with WebSand PR	15/12/2010 - 16/12/2010	Ghent, Belgium	KUL
ICISS 2010	Academic dissemination of research results [7]	15/12/2010 - 19/12/2010	Gandhinagar, India	CHALMERS
OOP2011, Security Track	Participation at industry event	24/01/2011-28/01/2011	Munich, Germany	SIEMENS
ESSoS 2011	Academic dissemination of research results [66]	09/02/2011 - 10/02/2011	Madrid, Spain	KUL
EICT Conference: IT-Sicherheit: "Vertrauen, Datenschutz, Sicherheit und Innovation"	Presentation at academia/industry event	10/02/2011	Berlin, Germany	UNI PASSAU
ACM SAC 2011	Academic dissemination of research results [45]	21/03/2011 - 24/03/2011	Taichung, Taiwan	UNI PASSAU
InfoSecurity Belgium	Booth at industry event with WebSand PR	23/03/2011 - 24/03/2011	Brussels, Belgium	KUL
ICST 2011, SECTEST Workshop	Academic dissemination of research results [42]	25/03/2011	Berlin, Germany	SAP
European Symposium on Programming (ESOP 2011)	Academic dissemination of research results [41]	26/03/2011 - 03/04/2011	Saarbrücken, Germany	CHALMERS

Event name	Participation	Date	Location	Partner(s)
European Workshop on System Security	Academic dissemination of research results [63]	10/04/2011	Salzburg, Austria	KUL
OWASP Sweden Chapter Meeting	Industrial dissemination of WebSand results	14/04/2011	Göteborg, Sweden	All partners
KULeuven	Colloquium / invited talks	10/05/2011	Leuven, Belgium	CHALMERS
W2SP 2011	Academic dissemination of research results [53]	26/05/2011	Oakland, California, USA	SAP
Stanford University	Colloquium / invited talks	03/06/2011	Palo Alto, USA	CHALMERS
PLAS 2011	Academic dissemination of research results [68, 9]	05/06/2011	San Jose, California, USA	CHALMERS
OWASP AppSec EU 2011	Participation at industry event	09/06/2011 - 10/06/2011	Dublin, Ireland	KUL
IEEE Computer Security Foundations Symposium (CSF 2011)	Academic dissemination of research results [61]	27/06/2011 - 29/06/2011	Cernay, France	CHALMERS
Summer School on Network and Information Security (NIS'11)	WebSand poster presentation	27/06/2011 - 01/07/2011	Crete, Greece	KUL, UNI PASSAU
IT-Speicher Regensburg: Mobile Applikationen in Breitbandnetzen	Booth at industry event with WebSand PR	28/06/2011	Regensburg, Germany	UNI PASSAU
DIMVA 2011	Academic dissemination of research results [46]	07/07/2011 - 08/07/2011	Amsterdam, The Netherlands	SAP
Harvard University	Colloquium / invited talks	31/08/2011	Boston, USA	CHALMERS
ESORICS 2011	Academic dissemination of research results [24, 10]	12/09/2011 - 14/09/2011	Leuven, Belgium	KUL, CHALMERS
BruCON 2011	Participation at academia/industry event	19/09/2011-20/09/2011	Brussel, Belgium	KUL
MyPhd 2011	Presentation at academic event	19/09/2011 - 21/09/2011	Erlangen, Germany	UNI PASSAU
Google Doctoral Fellowship Forum	Poster presentation	20/09/2011	Zurich, Switzerland	CHALMERS

Event name	Participation	Date	Location	Partner(s)
iMinds 2011	Booth at industry event with WebSand PR	13/10/2011	Ghent, Belgium	KUL
German Testing Day 2011	Presentation at academia/industry event	09/11/2011	Frankfurt, Germany	SAP
German OWASP Day 2011	Academic dissemination of research results [53, 54]	17/11/2011	Munich	SAP
OWASP BeNeLux Day 2011	Presentation at academia/industry event	01-02/12/2011	University of Luxembourg (Luxembourg)	KUL
APLAS 2011	Academic dissemination of research results [3]	05-07/12/2011	Kenting, Taiwan	CHALMERS
ACSAC 2011	Academic dissemination of research results [75]	05-09/12/2011	Orlando, Florida, USA	KUL
DFN Workshop	Presentation at academia/industry event	22/02/2012	Hamburg, Germany	SAP
GI Sicherheit 2012	Academic dissemination of research results [56]	7-9/03/2012	Darmstadt, Germany	SAP
AsiaCCS 2012	Academic dissemination of research results [76]	02-04/05/2012	Seoul, South Korea	KUL
OWASP Sweden 2012	Participation at industry event	14/05/2012	Stockholm, Sweden	CHALMERS
Caro Workshop 2012	Academic dissemination of research results [51]	14-15/05/2012	Munich, Germany	SAP
W2SP 2012	Academic dissemination of research results [52]	24/05/2012	San Francisco, CA, USA	SAP
IRISA/INRIA	Colloquium / invited talks	1/06/2012	Rennes, France	CHALMERS
JSTools'12	Academic dissemination of research results [67]	13/06/2012	Beijing, China	CHALMERS
DAIS 2012	Academic dissemination of research results [30]	13-15/06/2012	Stockholm, Sweden	KUL
Stevens Institute of Technology	Colloquium / invited talks	21/06/2012	Hoboken, NJ, USA	CHALMERS

Event name	Participation	Date	Location	Partner(s)
CSF 2012	Academic dissemination of research results [69, 40]	25-27/06/2012	Cambridge, MA, USA	CHALMERS
SECURITY 2012	Academic dissemination of research results [27]	24-27/07/2012	Rome, Italy	KUL
WOOT 2012	Academic dissemination of research results [51]	06/08/2012	Remond, OR, USA	SAP
MobiWIS 2012	Academic dissemination of research results [74]	26-28/08/2012	Ontario, Canada	CHALMERS
University of Illinois at Chicago	Colloquium / invited talks	31/08/2012	Chicago, IL, USA	CHALMERS
TrustBus 2012	Academic dissemination of research results [16]	04-06/09/2012	Vienna, Austria	UNI PASSAU
ESORICS 2012	Academic dissemination of research results [8]	10-13/09/2012	Pisa, Italy	CHALMERS
OWASP Belgium Chapter	Presentation at academia/industry event	12/09/2012	Leuven, Belgium	KUL
RAID 2012	Academic dissemination of research results [54]	12-15/09/2012	Amsterdam, Netherlands	SAP
BruCON 2012	Participation at academia/industry event	26/09/2012-27/09/2012	Ghent, Belgium	KUL
MyPhd 2012	Presentation at academic event	27/09/2012 - 28/09/2012	Bochum, Germany	UNI PASSAU, SAP
Dagstuhl "Web Application Security" 12401	Presentation at academia/industry event	01-05 October 2012	Wadern, Germany	ALL
CCS 2012	Academic dissemination of research results [62, 20]	16-18 October 2012	Raleigh, NC, USA	KUL
ERIC 2012	Presentation at academia/industry event	23+24 October 2012	Barcelona, Spain	SAP
iMinds The Conference	Booth at industry event with WebSand PR	06-08 November 2012	Ghent, Belgium	KUL

Event name	Participation	Date	Location	Partner(s)
OWASP BeNeLux Day 2012	Presentation at academia/industry event	29 November 2013	Leuven, Belgium	KUL
ACSAC 2012	Academic dissemination of research results [2, 49]	3-7 December 2012	Orlando, Florida, USA	KUL, SAP
ESSoS 2013	Academic dissemination of research results [12]	27 February - 1 March 2013	Paris (Rocquencourt), France	UNI PASSAU
AsiaCCS 2013	Academic dissemination of research results [29]	8-10 May 2013	Hangzhou, China	KUL
IEEE Security & Privacy	Academic dissemination of research results [64]	19-22 May 2013	San Francisco, USA	KUL
OWASP Tour EU 2014	Presentation at academia/industry event	20-22 June 2013	Lisbon, Portugal	KUL
ACM PLAS 2013	Presentation at academia/industry event	June 2013	Seattle, WA	CHALMERS
IEEE CSF 2013	Presentation at academia/industry event	June 2013	New Orleans, LA	CHALMERS
DIMVA 2013	Academic dissemination of research results [44]	18+19 July 2013	Berlin, Germany	SAP
USENIX Security	Academic dissemination of research results [48]	14-16 August 2013	Washington, D.C, USA	SAP
WASR workshop	Presentation at academia/industry event	21 August 2013	Hamburg, Germany	ALL
OWASP AppSec	Academic dissemination of research results [28]	20-23 August 2013	Hamburg, Germany	KUL, Passau, SAP
NordSec 2013	Academic dissemination of research results [17]	18-21 October 2013	Ilulissat, Greenland	UNI PASSAU

Event name	Participation	Date	Location	Partner(s)
RAID 2013	Academic dissemination of research results [47]	23-25 October 2013	St. Lucia	SAP
RSA Europe 2013	Presentation at academia/industry event	29.10.-01.11.2013	Amsterdam, the Netherlands	SAP
CCS 2013	Academic dissemination of research results [1, 55, 59]	5-9 November 2013	Berlin, Germany	KUL, SAP, CHALMERS
ISC 2013	Academic dissemination of research results [18]	13-15 November 2013	Dallas, Texas, USA	KUL
OWASP BeNeLux Day 2013	Presentation at academia/industry event	29 November 2013	Amsterdam, Netherlands	KUL
ESSoS 2014	Presentation at academic event-Magazinius+:ESSoS14	26-28.02.2014	Munich, Germany	SAP, CHALMERS
ACM CODASPY 2014	Academic dissemination of research results [15]	3-5 March 2014	San Antonio, TX, USA	UNI PASSAU, SAP
ACM SAC 2014	Academic dissemination of research results [39]	March 2014	Gyeongju, Korea,	CHALMERS
WWW 2014	Academic dissemination of research results [65]	7-11 April 2014	Seoul, Korea	KUL

4 Training

4.1 Industrial and academic training

The outcome of the WebSand project is being disseminated and taught via various training activities. This includes academic tutorials, summer schools, industrial training courses, and demos at industrial events.

In particular, the WebSand consortium has been active in two industrial training courses (SecAppDev and COSIC course), in three summer schools (Marktoberdorf Summer School 2011, Microsoft Research Summer School 2011, and FOSAD 2013), in two academic courses/seminar series (Formal Aspects in Security and Formal Methods and Security seminar series) and has given a demo on CsFire at the Future Internet Week and at iMinds.

- CsFire demo at Future Internet Week, 15/12/2010 - 16/12/2010, ICC, Ghent, Belgium (by Lieven Desmet)
- Secure Application Development Course (SecAppDev), 28/02/2011 - 04/03/2011, Groot Begijnhof, Leuven, Belgium (Training on advanced web application security by Lieven Desmet)
- International Course on Computer Security and Cryptography (COSIC Course), 14/06/2011 - 17/06/2011, Leuven (BE) (Session on enforcing security policies on untrusted software by Frank Piessens)
- Microsoft Research Summer School 2011: Software Engineering and Verification, 17/07/2011 - 27/07/2011, Moscow, Russia (Lectures on Language-based Security by Andrei Sabelfeld)
- Marktoberdorf Summer School 2011: Tools for Analysis and Verification of Software Safety and Security, 02/08/2011 - 14/08/2011, Bayrischzell, Germany (Lectures on Information-Flow Security by Andrei Sabelfeld)
- CsFire demo at iMinds, 13/10/2011, ICC, Ghent, Belgium (by Lieven Desmet)
- Formal Aspects in Security, 26/10/2011, Aalborg University, Denmark (Intensive course on Security Policies and Language-based Enforcement by Andrei Sabelfeld)
- Secure Application Development Course (SecAppDev), 05/03/2012 - 09/03/2012, Groot Begijnhof, Leuven, Belgium (Training on HTML5 Security by Philippe De Ryck)

- Formal Methods and Security seminar series at IRISA, Rennes, France (11/05/2012 by Frank Piessens & 01/06/2012 by Andrei Sabelfeld)
- Secure Application Development Course (SecAppDev), 4-8/03/2013, Groot Begijnhof, Leuven, Belgium (Training on Client-side security policies by Lieven Desmet, training on Sandboxing JavaScript by Steven Van Acker and Nick Nikiforakis)
- 13th International School on Foundations of Security Analysis and Design (FOSAD 2013), 2-7 September 2013, University Residential Center of Bertinoro, Italy (Information flow control for the web by Frank Piessens)
- Secure Application Development Course (SecAppDev), 10-14/02/2014, Groot Begijnhof, Leuven, Belgium (Training on Recent web security technologies by Lieven Desmet, training on The Web's security model by Philippe De Ryck, training on Browser fingerprinting by Nick Nikiforakis)
- B-CENTRE Web Security Training, 28/03/2014, Leuven, Belgium (Full day industrial training on Web Security by Philippe De Ryck, Lieven Desmet and Jef Mariën)
- 14th International School on Foundations of Security Analysis and Design (FOSAD 2014), 1-6 September 2014, University Residential Center of Bertinoro, Italy (From theory to practice of information flow control by Andrei Sabelfeld)

4.2 Academic courses and theses

In addition, partners of the WebSand consortium are continuously updating their course material to include new findings from the WebSand project, and are supervising students with their master or PhD thesis in the scope of WebSand-related research topics.

The following courses given in the past three years have been influenced by the WebSand project:

- Web Application Security Lab (given at Karlsruhe Institute of Technology by SAP)
- Datensicherheit (Computer Security) (BSc level lecture given at DHBW Karlsruhe by SAP)
- Secure Software Development (KULeuven, MSc level course)

- Language-based security course (Chalmers, MSc level course)
- Real-life Security (Passau, MSc level seminar)
- Security Unleashed (Passau, MSc level seminar)
- Software Sicherheit (Software Security) (jointly conducted by Uni Passau and Siemens, MSc level course)
- Sicherheits-Infrastrukturen (Security Infrastructures) (Passau, MSc level practical course)
- Software-Sicherheit (Software Security) (Passau, MSc level practical course)
- Selected Topics in Systems Security (MSc level course given at the Technical University of Munich by Siemens)
- Formal Methods for Security Assurance (MSc level lecture given at the University of Malaga by Siemens)

Over the past three years, the following theses have been supervised in scope of the WebSand research topics:

- Client-Side Cross-Domain Requests in the Web browser: Techniques, Policies and Security Pitfalls (Master thesis, Sebastian Lekies, 2011)
- Protecting mobile browsers against cross-site request forgery (Master thesis, Maarten Lambert, 2011)
- Improving session security in web applications (Master thesis, Bram Bonné, 2011) *This thesis was awarded with the Luciad Master Thesis price 2011*
- Information Flow Security for JavaScript Web Applications through Secure Multi-Execution (Master thesis, Willem De Groef, 2011)
- Dynamic enforcement of decentralized security policies (Licentiate thesis, Jonas Magazinius, 2011)
- Controlling Dependencies for Security and Privacy (Licentiate thesis, Arnar Birgisson, 2011)
- Practical, Flexible Programming with Information Flow Control (PhD thesis, Niklas Broberg, 2011)

- Lightweight Enforcement of Fine-Grained Security Policies for Untrusted Software (PhD thesis, Phu H. Phung, 2011)
- Implementation of a Stateful HTTP Reverse Proxy by Caspar Gries (Master thesis, Caspar Gries, 2011)
- Securing Session Management with Focus on the Session Fixation Attack (Master thesis, Michael Schrank, 2010)
- Techniques to Isolate and Partially Deactivate JavaScript in Browsers (Diploma thesis, Mathias Wagner, 2010)
- Enhanced Privacy in Social Application Platforms (Master thesis, Tom Reynaert, 2012) *This thesis was awarded with the Alcatel-Lucent Master Thesis price 2012*
- A modular web crawler for conducting security experiments (Master thesis, Frederik Nijs, 2012)
- Secure integration of JavaScript advertisements using Secure ECMAScript (Master thesis, Lynsey Hens and Brenda Lissens, 2012)
- Autonomous client-side protection of web sessions (Master thesis, Joeri Ledegen, 2012)
- Narcissus-based security architecture for JavaScript (Master thesis, Andy Debrouwer and Sam Segers, 2012)
- GlassTube: A Lightweight Approach to Web Application Integrity (Master thesis, Per Hallgren and Daniel Mauritzson, 2012)
- Information Erasure: An Information-Flow Approach to Semantics and Enforcement (Licentiate thesis, Filippo Del Tedesco, 2011)
- Tracking Information Flows in Interactive and Object-Oriented Programs (Licentiate thesis, Willard Rafnsson, 2012)
- Entwicklung eines Assessment-Tools für HTML5 Sicherheitseigenschaften und aufkommende Bedrohungen für die Websicherheit (Master thesis, Dennis Applet, 2012)
- Implementierung eines Kontrollfluss-Integritäts-Monitors zur Integration in existierende Web-Applikationen (Master thesis, Patrick Gemein, 2012)

- Identity Theft in the Internet – Attack Vectors and Countermeasures (Master thesis, Wolfgang Frankenberger, 2014)
- Mitigating Impersonation Attacks on Web Authentication Using Device Pinning and Authorized Actions (Master thesis, Johannes Koestler, 2014)
- WebHackArena: An automated framework for evaluating client-side web defenses (Master thesis, Leendert Dommicent and Jorn Van Look , 2014)
- Comparative study of implementation strategies for WebJail (Master thesis, Alard Geukens and Jelle Van Regenmortel, 2014)
- Efficient JavaScript sandboxing using JSand (Master thesis, Koen Wellens, 2014)
- Server-driven policies for a secure information flow enhanced browser (Master thesis, Pieter Van Riet, 2014)
- Protection against Cross-Site Request Forgery at the client- and server-side (Master thesis, Pieter Hiele, 2014)
- Towards a Secure Web: Critical Vulnerabilities and Client-Side Countermeasures (PhD Thesis, Nick Nikiforakis, 30 August 2013)
- Information-Flow Tracking for Dynamic Languages (Licentiate thesis, Luciano Bello, October 2013)
- Securing the mashed up web (PhD thesis, Jonas Magazinius, 1 November 2013)
- Tracking Dependencies for Security and Privacy (PhD thesis, Arnar Birgisson, 25 November 2013)
- Functional Techniques for Representing and Specifying Software (PhD Thesis, Dominique Devriese, 23 January 2014)
- Information Flow in Databases for Free (Master thesis, Daniel Schoepe, 28 April 2014)
- Securing Interactive Systems (PhD thesis, Willard Rafnsson, 29 April 2014)

5 Community transfer and communication

5.1 OWASP, ENISA and W3C

The WebSand consortium has closely collaborated with the OWASP community. John Wilander of OWASP Sweden gave an invited talk at the first WebSand workshop, and WebSand partners have been involved in multiple local chapter meetings, workshop, have attended the OWASP AppSec EU 2011 conference in Dublin and the OWASP AppSec EU 2013 in Hamburg, and are the initiators of the Gothenburg chapter.

During the WebSand workshop and consortium meeting in April 2011 in Gothenburg, a first OWASP Sweden chapter meeting was held at Chalmers university with various speakers from within the WebSand consortium:

- Biting the Hand That Serves You: A closer look at client-side Flash proxies for cross-domain requests (Martin Johns)
- Abusing locality in shared Web hosting (Nick Nikiforakis)
- Tracking Information Flow in Web Applications (Andrei Sabelfeld)

This meeting in Gothenburg was a success with over 60 participants and shortly after a new local OWASP chapter was created in Gothenburg with a WebSand representative from Chalmers (Jonas Magazinius).

Members of the WebSand project were tightly involved in preparation and execution of the OWASP AppSec EU 2013 conference. Project coordinator Martin Johns (SAP) acted as program chair for the conferences research track and was part of the general organisation team. Furthermore, WebSand participants Lieven Desmet (KU Leuven), Nick Nikiforakis (KU Leuven), Bastian Braun (Passau), and Andrei Sabelfeld (Chalmers) served in the PC.

At the main event, the following talks were given at the conference by WebSand participants:

- Philippe De Ryck (KU Leuven): “Improving the Security of Session Management in Web Applications”
- Bastian Braun (Passau): “A Doorman for Your Home - Control-Flow Integrity Means in Web Frameworks”
- Ben Stock (SAP): “Eradicating DNS Rebinding with the Extended Same-Origin Policy”
- Nick Nikiforakis (KU Leuven): “Web Fingerprinting: How, Who, and Why?”

- Sebastian Lekies (SAP): “Clickjacking Protection Under Non-trivial Circumstances”
- Lieven Desmet (KU Leuven): “Sandboxing JavaScript”

Moreover, partners of the WebSand consortium have organized and/or participated in the following local OWASP chapter meetings:

- 19th OWASP 'Stammtisch' Meeting, 18/01/2011, Munich, Germany
- Belgium Chapter Meeting, 01/03/2011, Leuven, Belgium
- 21th OWASP 'Stammtisch' Meeting, 15/03/2011, Munich, Germany
- Sweden Chapter Meeting, 14/04/2011, Gothenburg, Sweden
- Belgium Chapter Meeting, 23/05/2011, Brussels, Belgium
- Belgium Chapter Meeting, 16/06/2011, Brussels, Belgium
- 26th OWASP 'Stammtisch' Meeting, 16/08/2011, Munich, Germany
- Gothenburg Chapter Meeting, 25/08/2011, Gothenburg, Sweden
- Sweden Chapter meeting, 3/11/2011, Gothenburg, Sweden
- German OWASP Day 2011, 17/11/2011, Munich, Germany
- OWASP BeNeLux Day 2011, 01-02/12/2011, University of Luxembourg, Luxembourg
- Belgium Chapter Meeting, 25/01/2012, Brussels, Belgium
- German Chapter meeting, 03/02/2012, Frankfurt, Germany
- Belgium Chapter Meeting, 06/03/2012, Leuven, Belgium
- Sweden Chapter meeting, 22/03/2012, Gothenburg, Sweden
- Sweden Chapter meeting, 14/05/2012, Stockholm, Sweden
- Belgium Chapter Meeting, 12/09/2012, Leuven, Belgium
- Belgium Chapter Meeting, 26/09/2012, Ghent, Belgium
- OWASP BeNeLux Day 2012, 29-30/11/2012, Leuven, Belgium

- Belgium Chapter Meeting, 5/03/2013, Leuven, Belgium
- Belgium Chapter Meeting, 6/06/2013, Leuven, Belgium
- Belgium Chapter Meeting, 8/10/2013, Diegem, Belgium
- OWASP BeNeLux Day 2013, 29/11/2013, Amsterdam, The Netherlands
- Belgium Chapter Meeting, 17/12/2013, Leuven, Belgium
- Belgium Chapter Meeting, 12/02/2014, Leuven, Belgium
- German Chapter Meeting, 14/03/2104, Frankfurt, Germany

In addition, partners of the WebSand consortium have initiated collaborations with the European Network and Information Security Agency (ENISA) and the World Wide Web Consortium (W3C). In particular, based on the expertise built up in WebSand, KULeuven was able to conduct a security analysis of next generation web standards [25], commissioned by ENISA. In follow-up, the results of this ENISA analysis have been followed up and discussed with W3C staff and on public mailinglists of W3C.

Furthermore, as a follow-up to the regular informal dissemination and exploitation interactions between the WebSand consortium and W3C and IETF, the FP7-project STREWS has been set up. This FP7 Coordination Action (CA) started on 1 October 2012, and will run for three years. The project will roll-out a European Roadmap for Research on Web Security, and brings together researchers from ERCIM/W3C, Trinity College Dublin, as well as WebSand partners SAP and KUL.

5.2 Collaboration with other projects

The WebSand project also fosters collaborations with other ongoing FP7 and non-EU projects.

FP7-ICT IP ANIKETOS With the ANIKETOS project, there is a continuous exchange on insecure code patterns with special attention on JavaScript. Moreover, the ANIKETOS project has been presented during the consortium meeting of 3-4 November 2010.

FP7-ICT IP HATS The theory of Secure-Multi Execution that is applied in WP3 has been developed in the HATS project. Moreover, the HATS project has been presented during the consortium meeting of 28-29 August 2012.

FP7-ICT IP MASTER The policies for Secure-Multi Execution and the executable model in FeatherWeight Firefox (as described in deliverable D3.1) have been developed in collaboration with the MASTER project. PhD student Nataliia Bielova (from the University of Trento) contributed to this work during a 3-month research visit at KULeuven.

FP7-ICT NoE NESSoS There are ongoing collaboration with the NES-SoS Network of Excellence on Engineering Secure Future Internet Software Services and Systems, in particular on the security of web environments. Moreover, in year 2 the collaboration of Siemens with NeSSoS participants in the topic of location privacy resulted in a joint publication (see Sect. 2). The WASR workshop was co-organized with NESSoS.

FP7-ICT STREP SPaCIoS The project SPaCIoS focusses on security testing and the development of testing tools. We strive to exploit synergies between the project by using some of the web services, which are part of the e-Health use case implementation, for testing within the SPaCIoS project. The WASR workshop was co-organized with SPaCIoS.

DFG PP RS3 The German Research Foundation Priority program “Reliably secure software systems *RS*³” focuses on the rigorous (formally based) development of secure software. Ongoing collaborations with projects participating in this priority program took place on the second year, in particular Siemens cooperated with the MoDelSec project of the TU Dortmund on the verification of information flow policies at the software design phase. Further collaborations are being explored.

US-NSF Secure Web Advertisements The project proposes to research, design, and implement protection systems for securing online web advertisements (ads) at three levels: end-user ad recipients, web page publishers, and ad distribution networks. The project is investigated by research groups at University of Illinois at Chicago, and University of Texas at Dallas.

FP7-ICT CA STREWS Based on the interactions between the WebSand consortium and W3C and IETF, the FP7-project STREWS has been set up. The project will roll-out a European Roadmap for Research on Web Security, and brings together researchers from ERCIM/W3C, Trinity College Dublin, as well as WebSand partners SAP and KUL. The WASR workshop was co-organized with STREWS.

5.3 WebSand portal

The WebSand portal (hosted at <https://www.websand.eu>) makes the results of WebSand easily available to a wide audience. The portal provides public access to white papers, publications and public deliverables of the project, such as reports and prototypes, and is regularly updated to reflect the actual state of the project.

5.4 Communication

At the launch of the project, the WebSand consortium has created external visibility to the project towards various media. In particular, a set of press releases has been distributed:

- WebSand Startup Press release, issued by University of Passau, 21 April 2011 ([http://www.uni-passau.de/921.html?&tx_ttnews\[tt_news\]=1344&tx_ttnews\[backPid\]=90&cHash=ae0eb41592ade5ddea7239218f42c154](http://www.uni-passau.de/921.html?&tx_ttnews[tt_news]=1344&tx_ttnews[backPid]=90&cHash=ae0eb41592ade5ddea7239218f42c154))
- Siemens ResearchNews, ‘Safe “Sandbox” for the Internet of the Future’, issued by Siemens AG, 01.05.2011 (http://www.siemens.com/innovation/en/news_events/ct_pressreleases/e_research_news/2011/e_22_resnews_1114_1.htm)

At the end of the project, Chalmers produced a popular-scientific 4-minute video for outreach to wider audiences about Chalmers’ research on securing information flow in web applications. (<http://vimeo.com/82206652>) At the time of the writing of this report, the video play count has nearly reached 2,000 times.

References

- [1] Güneş Acar, Marc Juarez, Nick Nikiforakis, Claudia Diaz, Seda Gürses, Frank Piessens, and Bart Preneel. Fpdetective: Dusting the web for fingerprinters. In *Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS 2013)*, pages 1129–1140. ACM, 2013.
- [2] Pieter Agten, Steven Van Acker, Yoran Brondsema, Phu H. Phung, Lieven Desmet, and Frank Piessens. Jsand: Complete client-side sandboxing of third-party javascript without browser modifications. In *Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC 2012)*, pages 1–10. ACM, December 2012.
- [3] A. Askarov, J. Magazinius, and A. Sabelfeld. Decentralized delimited release. In *Proceedings of the Asian Symposium on Programming Languages and Systems (APLAS)*. Springer-Verlag, 2011.
- [4] Gilles Barthe, Juan Manuel Crespo, Dominique Devriese, Frank Piessens, and Exequiel Rivas. Secure multi-execution through static program transformation. In *Formal Techniques for Distributed Systems (FMOODS/FORTE 2012)*, volume 7273, pages 186–202. Springer Berlin Heidelberg, June 2012.
- [5] Nataliia Bielova, Dominique Devriese, Fabio Massacci, and Frank Piessens. Reactive non-interference for a browser model. In *Proceedings of the 5th International Conference on Network and System Security (NSS 2011)*, September 2011.
- [6] Nataliia Bielova, Dominique Devriese, Fabio Massacci, and Frank Piessens. Reactive non-interference for the browser: extended version. CW Reports CW602, Department of Computer Science, K.U.Leuven, February 2011.
- [7] A. Birgisson, A. Russo, and A. Sabelfeld. Unifying facets of information integrity. In *Proceedings of the International Conference on Information Systems Security (ICISS)*. Springer-Verlag, 2010.
- [8] Arnar Birgisson, Daniel Hedin, and Andrei Sabelfeld. Boosting the permissiveness of dynamic information-flow tracking by testing. In *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, LNCS, Pisa, Italy, September 2012. Springer-Verlag.

- [9] Arnar Birgisson, Alejandro Russo, and Andrei Sabelfeld. Capabilities for information flow. In *ACM SIGPLAN Workshop on Programming Languages and Analysis for Security*, 2011.
- [10] Arnar Birgisson and Andrei Sabelfeld. Multi-run security. In Vijay Atluri and Claudia Diaz, editors, *Computer Security – ESORICS 2011*, volume 6879 of *Lecture Notes in Computer Science*, pages 372–391. Springer Berlin / Heidelberg, 2011.
- [11] Bastian Braun, Patrick Gemein, Benedikt Höfling, Michael Maisch, and Alexander Seidl. Angriffe auf OpenID und ihre strafrechtliche Bewertung. *Datenschutz und Datensicherheit - DuD*, 36:502–509, 2012. 10.1007/s11623-012-0168-5.
- [12] Bastian Braun, Patrick Gemein, Hans P. Reiser, and Joachim Posegga. Control-Flow Integrity in Web Applications. In *International Symposium on Engineering Secure Software and Systems (ESSoS 2013)*. Lecture Notes in Computer Science (LNCS), Springer, 2013.
- [13] Bastian Braun, Caspar Gries, Benedikt Petschkuhn, and Joachim Posegga. Ghostrail: Ad Hoc Control-Flow Integrity for Web Applications. In *29th IFIP International Information Security and Privacy Conference (IFIP SEC 2014)*, June 2014.
- [14] Bastian Braun, Martin Johns, Johannes Köstler, and Joachim Posegga. A Trusted UI for the Mobile Web. In *29th IFIP International Information Security and Privacy Conference (IFIP SEC 2014)*, June 2014.
- [15] Bastian Braun, Johannes Köstler, Martin Johns, and Joachim Posegga. PhishSafe: Leveraging Modern JavaScript APIs for Transparent and Robust Protection. In *Fourth ACM Conference on Data and Application Security and Privacy (ACM CODASPY 2014)*, 2014.
- [16] Bastian Braun, Stefan Kucher, Martin Johns, and Joachim Posegga. A User-Level Authentication Scheme to Mitigate Web Session-Based Vulnerabilities. In Simone Fischer-Hübner, Sokratis Katsikas, and Gerald Quirchmayr, editors, *Trust, Privacy and Security in Digital Business*, volume 7449 of *Lecture Notes in Computer Science*, pages 17–29. Springer Berlin / Heidelberg, 2012.
- [17] Bastian Braun, Christian v. Pollak, and Joachim Posegga. A Survey on Control-Flow Integrity Means in Web Application Frameworks. In *18th Nordic Conference on Secure IT Systems (NordSec 2013)*, 2013.

- [18] Ping Chen, Nick Nikiforakis, Christophe Huygens, and Lieven Desmet. A dangerous mix: Large-scale analysis of mixed-content websites. In *Proceedings of the Information Security Conference (ISC)*, November 2013.
- [19] Jorge Cuéllar, Martín Ochoa, and Ruben Rios. Indistinguishable regions in geographic privacy. In *Proceedings of the 2012 ACM Symposium on Applied Computing, SAC '12*, pages 1463–1469, New York, NY, USA, 2012. ACM.
- [20] Willem De Groef, Dominique Devriese, Nick Nikiforakis, and Frank Piessens. Flowfox: a web browser with flexible and precise information flow control. In *Proceedings of the 19th ACM conference on Computer and Communications Security (CCS 2012)*. ACM, 2012.
- [21] Willem De Groef, Dominique Devriese, Nick Nikiforakis, and Frank Piessens. Secure multi-execution of web scripts: Theory and practice. *Journal of Computer Security*, 22(4):469–509, 2014.
- [22] Willem De Groef, Dominique Devriese, Tom Reynaert, and Frank Piessens. Security and privacy of online social network applications. In *Social Network Engineering for Secure Web Data and Services*. IGI Global, 2013.
- [23] Philippe De Ryck, Maarten Decat, Lieven Desmet, Frank Piessens, and Wouter Joosen. Security of Web Mashups: a Survey. In *Proceedings of the 15th Nordic Conference in Secure IT Systems (NordSec 2010)*. Springer, 2010.
- [24] Philippe De Ryck, Lieven Desmet, Wouter Joosen, and Frank Piessens. Automatic and precise client-side protection against csrf attacks. In Vijay Atluri and Claudia Diaz, editors, *Computer Security - ESORICS 2011*, volume 6879 of *Lecture Notes in Computer Science*, pages 100–116. Springer Berlin / Heidelberg, 2011.
- [25] Philippe De Ryck, Lieven Desmet, Pieter Philippaerts, and Frank Piessens. A security analysis of next generation web standards. Technical report, G. Hogben and M. Dekker (Eds.), European Network and Information Security Agency (ENISA), July 2011.
- [26] Philippe De Ryck, Lieven Desmet, Frank Piessens, and Wouter Joosen. A security analysis of emerging web standards - extended version. CW Reports CW622, Department of Computer Science, KU Leuven, May 2012.

- [27] Philippe De Ryck, Lieven Desmet, Frank Piessens, and Wouter Joosen. A security analysis of emerging web standards - html5 and friends, from specification to implementation. In *Proceedings of the International Conference on Security and Cryptography (SECRYPT)*, pages 257–262. SciTePress, July 2012.
- [28] Philippe De Ryck, Lieven Desmet, Frank Piessens, and Wouter Joosen. Improving the security of session management in web applications. In *OWASP AppSec EU*, August 2013.
- [29] Philippe De Ryck, Nick Nikiforakis, Lieven Desmet, and Wouter Joosen. Tabshots: Client-side detection of tabnabbing attacks. In *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security (AsiaCCS)*, pages 447–455, May 2013.
- [30] Philippe De Ryck, Nick Nikiforakis, Lieven Desmet, Frank Piessens, and Wouter Joosen. Serene: Self-reliant client-side protection against session fixation. In *12th IFIP International Conference on Distributed Applications and Interoperable Systems*, pages 59–72. Springer-Verlag, June 2012.
- [31] Filippo Del Tedesco, Alejandro Russo, and David Sands. Implementing erasure policies using taint analysis. In Tuomas Aura, editor, *The 15th Nordic Conference in Secure IT Systems*, LNCS. Springer Verlag, October 2010.
- [32] Lieven Desmet, Martin Johns, Benjamin Livshits, and Andrei Sabelfeld. Web Application Security (Dagstuhl Seminar 12401). *Dagstuhl Reports*, 2(10):1–37, 2013.
- [33] Lieven Desmet, Martin Johns, Benjamin Livshits, and Andrei Sabelfeld. Special issue on web application security. In *Journal of Computer Security*. IOS Press, April 2014.
- [34] Ermano Geuer. Der cookie-guide der britischen internationalen handelskammer. *AnwZert ITR 15/2012, Anm. 2*, 2012. The Cookie Guide of the british ICC.
- [35] Ermano Geuer. Einwilligung in cookieempfang durch browsereinstellungen?, schlussfolgerungen aus einer auslegung der gesetzlichen regelung in österreich. *ITRB 2012, 206*, 2012. Consent into the reception of cookies through browser settings?, Conclusion of the interpretation of Austrian legislation.

- [36] Ermano Geuer. Keine rechtssicherheit bei safe harbor-selbstzertifizierungen. *AnwZert ITR 16/2012, Anm. 2*, 2012. No legal certainty in case of Safe Harbor self certification.
- [37] Tom Van Goethem, Ping Chen, Nick Nikiforakis, Lieven Desmet, and Wouter Joosen. arge-scale security analysis of the web: Challenges and findings. In *Proceedings of the 7th International Conference on Trust & Trustworthy Computing (TRUST 2014)*, July 2014.
- [38] Per A. Hallgren, Daniel T. Mauritzson, and Andrei Sabelfeld. Glasstube: A lightweight approach to web application integrity. In *Proceedings of the Eighth ACM SIGPLAN Workshop on Programming Languages and Analysis for Security, PLAS '13*, pages 71–82, New York, NY, USA, 2013. ACM.
- [39] Daniel Hedin, Arnar Birgisson, Luciano Bello, and Andrei Sabelfeld. JSFlow: Tracking information flow in JavaScript and its APIs. In *Proc. 29th ACM Symposium on Applied Computing*, 2014.
- [40] Daniel Hedin and Andrei Sabelfeld. Information-flow security for a core of JavaScript. In *Proceedings of the IEEE Computer Security Foundations Symposium*, Harvard University, Cambridge MA, June 2012. IEEE Computer Society Press.
- [41] S. Hunt and David Sands. From exponential to polynomial-time security typing via principal types. In *Programming Languages and Systems. 20th European Symposium on Programming, ESOP 2011*, number 6602 in LNCS. Springer Verlag, 2011.
- [42] M. Johns and M. Jodeit. Scanstud: A methodology for systematic, fine-grained evaluation of static analysis tools. In *Software Testing, Verification and Validation Workshops (ICSTW), 2011 IEEE Fourth International Conference on*, pages 523 –530, march 2011.
- [43] Martin Johns. HTML5-Security - Sicherer Umgang mit den neuen JavaScript APIs. *Datenschutz und Datensicherheit - DuD*, 36(4):231–235, 2012.
- [44] Martin Johns. PreparedJS: Secure Script-Templates for JavaScript. In *10th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA '13)*, LNCS. Springer, July 2013.
- [45] Martin Johns, Bastian Braun, Michael Schrank, and Joachim Posegga. Reliable protection against session fixation attacks. In *Proceedings of*

- the 2011 ACM Symposium on Applied Computing, SAC '11*, pages 1531–1537, New York, NY, USA, 2011. ACM.
- [46] Martin Johns and Sebastian Lekies. Biting the hand that serves you: a closer look at client-side flash proxies for cross-domain requests. In *Proceedings of the 8th international conference on Detection of intrusions and malware, and vulnerability assessment, DIMVA'11*, pages 85–103, Berlin, Heidelberg, 2011. Springer-Verlag.
- [47] Martin Johns and Sebastian Lekies. Tamper-resistant LikeJacking Protection. In *16th International Symposium on Research in Attacks, Intrusions and Defenses (RAID'13)*, 2013.
- [48] Martin Johns, Sebastian Lekies, and Ben Stock. Eradicating DNS Rebinding with the Extended Same-Origin Policy. In *Proceedings of the 19th Usenix Security Symposium (Usenix Sec'13)*, 2013.
- [49] Martin Johns, Sebastin Lekies, Bastian Braun, and Benjamin Flesch. BetterAuth: Web Authentication Revisited. In *8th Annual Computer Security Applications Conference (ACSAC 2012)*, 2012.
- [50] Martin Johns and Joachim Posegga. Websand: Server-driven outbound web-application sandboxing. In Simone Fischer-Hübner, Sokratis K. Katsikas, and Gerald Quirchmayr, editors, *TrustBus*, volume 7449 of *Lecture Notes in Computer Science*, pages 216–217. Springer, 2012.
- [51] Sebastian Lekies, Mario Heiderich, Dennis Appelt, Thorsten Holz, and Martin Johns. On the fragility and limitations of current Browser-provided Clickjacking protection schemes. In *6th USENIX Workshop on Offensive Technologies (WOOT '12)*, August 2012.
- [52] Sebastian Lekies and Martin Johns. Lightweight Integrity Protection for Web Storage Content Caching. In *6th Workshop on Web 2.0 Security and Privacy (W2SP 2012)*, May 2012.
- [53] Sebastian Lekies, Martin Johns, and Walter Tighzert. The state of the cross-domain nation. In *Proceedings of the Workshop on Web 2.0 Security and Privacy*, May 2011.
- [54] Sebastian Lekies, Nick Nikiforakis, Walter Tighzert, Frank Piessens, and Martin Johns. DEMACRO: Defense against Malicious Cross-domain Requests. In *5th International Symposium on Research in Attacks, Intrusions and Defenses (RAID'12)*, 2012.

- [55] Sebastian Lekies, Ben Stock, and Martin Johns. 25 Million Flows Later - Large-scale Detection of DOM-based XSS. In *Proceedings of the 20th ACM Conference on Computer and Communication Security (CCS '13)*, 2013.
- [56] Sebastian Lekies, Walter Tighzert, and Martin Johns. Towards stateless, client-side driven Cross-Site Request Forgery protection for Web applications. In *5th conference on "Sicherheit, Schutz und Zuverlässigkeit" (GI Sicherheit 2012)*, Lecture Notes in Informatics (LNI), March 2012.
- [57] J. Magazinius, D. Hedin, and A. Sabelfeld. Architectures for inlining security monitors in web applications. In *ESSoS*, Lecture Notes in Computer Science. Springer, 2014.
- [58] Jonas Magazinius, Phu H. Phung, and David Sands. Safe wrappers and sane policies for self-protecting JavaScript. In Tuomas Aura, editor, *The 15th Nordic Conference in Secure IT Systems*, LNCS. Springer Verlag, October 2010.
- [59] Jonas Magazinius, Billy K. Rios, and Andrei Sabelfeld. Polyglots: crossing origins by crossing formats. In *ACM Conference on Computer and Communications Security*, pages 753–764, 2013.
- [60] Jonas Magazinius, Alejandro Russo, and Andrei Sabelfeld. On-the-fly inlining of dynamic security monitors. *Computers & Security*, October 2012.
- [61] H. Mantel, D. Sands, and H. Sudbrock. Assumptions and guarantees for compositional noninterference. In *Computer Security Foundations Symposium (CSF), 2011 IEEE 24th*, pages 218 –232, june 2011.
- [62] Nick Nikiforakis, Luca Invernizzi, Alexandros Kapravelos, Steven Van Acker, Wouter Joosen, Christopher Kruegel, Frank Piessens, and Giovanni Vigna. You are what you include: Large-scale evaluation of remote javascript inclusions. In *Proceedings of the 19th ACM conference on Computer and Communications Security (CCS 2012)*, October 2012.
- [63] Nick Nikiforakis, Wouter Joosen, and Martin Johns. Abusing locality in shared web hosting. In *Proceedings of the Fourth European Workshop on System Security, EUROSEC '11*, pages 2:1–2:7, New York, NY, USA, 2011. ACM.

- [64] Nick Nikiforakis, Alexandros Kapravelos, Wouter Joosen, Christopher Kruegel, Frank Piessens, and Giovanni Vigna. Cookieless monster: Exploring the ecosystem of web-based device fingerprinting. In *Proceedings of the 34th IEEE Symposium on Security & Privacy*, pages 541–555, May 2013.
- [65] Nick Nikiforakis, Federico Maggi, Gianluca Stringhini, M Zubair Rafique, Wouter Joosen, Christopher Kruegel, Frank Piessens, Giovanni Vigna, and Stefano Zanero. Stranger danger: Exploring the ecosystem of ad-based url shortening services. In *Proceedings of the 23rd International World Wide Web Conference (WWW 2014)*, April 2014.
- [66] Nick Nikiforakis, Wannes Meert, Yves Younan, Martin Johns, and Wouter Joosen. Sessionshield: Lightweight protection against session hijacking. In Ážlfar Erlingsson, Roel Wieringa, and Nicola Zannone, editors, *Engineering Secure Software and Systems*, volume 6542 of *Lecture Notes in Computer Science*, pages 87–100. Springer Berlin / Heidelberg, 2011.
- [67] Phu H. Phung and Lieven Desmet. A two-tier sandbox architecture for untrusted javascript. In *Proceedings of the Workshop on JavaScript Tools (JSTools '12)*, pages 1–10. ACM, June 2012.
- [68] W. Rafnsson and A. Sabelfeld. Limiting information leakage in event-based communication. In *ACM SIGPLAN Workshop on Programming Languages and Analysis for Security*, 2011.
- [69] Willard Rafnsson, Daniel Hedin, and Andrei Sabelfeld. Securing interactive programs. In *Proceedings of the IEEE Computer Security Foundations Symposium*, Harvard University, Cambridge MA, June 2012. IEEE Computer Society Press.
- [70] Willard Rafnsson, Keiko Nakata, and Andrei Sabelfeld. Securing class initialization in Java-like languages. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, January 2013.
- [71] Willard Rafnsson and Andrei Sabelfeld. Secure multi-execution: Fine-grained, declassification-aware, and transparent. In *CSF*, pages 33–48, June 2013.
- [72] Michael Schrank, Bastian Braun, Martin Johns, and Joachim Posegga. Session fixation – c the forgotten vulnerability? In *Sicherheit 2010: Sicherheit, Schutz und Zuverl?ssigkeit*, pages 341–352. Gesellschaft für Informatik, 2010.

- [73] Ben Stock and Martin Johns. Protecting Users Against XSS-based Password Manager Abuse. In *9th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2014)*, 2014.
- [74] Hong-Linh Truong, Phu H. Phung, and Schahram Dustdar. Governing bot-as-a-service in sustainability platforms – issues and approaches. *Procedia Computer Science*, 10(0):561 – 568, 2012. ANT 2012 and MobiWIS 2012.
- [75] Steven Van Acker, Philippe De Ryck, Lieven Desmet, Frank Piessens, and Wouter Joosen. Webjail: Least-privilege integration of third-party components in web mashups. In *ACSAC*, December 2011.
- [76] Steven Van Acker, Nick Nikiforakis, Lieven Desmet, Wouter Joosen, and Frank Piessens. Flashover: Automated discovery of cross-site scripting vulnerabilities in rich internet applications. In *AsiaCCS*, May 2012.
- [77] Steven Van Acker, Nick Nikiforakis, Lieven Desmet, Frank Piessens, and Wouter Joosen. Monkey-in-the-browser: Malware and vulnerabilities in augmented browsing script markets. In *ASIACCS*, June 2014.
- [78] Mathy Vanhoef, Willem De Groef, Dominique Devriese, Frank Piessens, and Tamara Rezk. Stateful declassification policies for event-driven programs. In *Proceedings of the 27th Computer Security Foundations Symposium (CSF 2014)*, Harvard University, Cambridge MA, May 2014. IEEE Computer Society Press.