Deliverable D6.1
Dissemination plan

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

Deliverable details
Deliverable version: v0.1  Classification: public
Date of delivery: 30.09.2011  Due on: M12
Editors: Lieven Desmet and Frank Piessens  Total pages: 18

List of Contributors:
Bastian Braun, Jorge Cuellar, Lieven Desmet, Martin Johns, Peng Liu,
Frank Piessens, Joachim Posegga, Andrei Sabelfeld, David Sands, Jan Wolff

Project details
Start date: October 01, 2010  Duration: 36 months
Project Coordinator: Martin Johns
Partners: SAP, Siemens, CHALMERS, KUL, UNI PASSAU
# Contents

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

This dissemination plan reports on the dissemination activities of the first year of WebSand, and planned upcoming activities. 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 are being disseminated by participating in international conferences and workshops in the areas of software security and software engineering.

During the first project year, results have been presented and published in major conferences and high-profile workshops in this area, such as the European Symposium on Research in Computer Security (ESORICS), the International Symposium on Engineering Secure Software and Systems (ESSoS), 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 Workshop on Web 2.0 Security and Privacy (W2SP), the ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS).

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

We intend to continue the current publication strategy for year two and three, and target scientific journals and major conferences in this field, including Journal of Computer Security, ESORICS, ACM CCS, IEEE Symposium on Security and Privacy, USENIX Security Symposium, WWW, ESSoS, ICSE, ECOOP, OOPSLA, IEEE Computer Security Foundations Symposium, Annual Computer Security Applications Conference.
<table>
<thead>
<tr>
<th>Type</th>
<th>Venue</th>
<th>Publication</th>
<th>Partner(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Venue</td>
<td>Publication</td>
<td>Partner(s)</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
</tbody>
</table>
3 Events

3.1 WebSand organized events

WebSand organizes a yearly event to bring together researchers in the web application community and disseminate results of the WebSand project. The first and third event are foreseen to be a closed workshop, whereas the second event is planned as an open workshop.

The first event has been organized by Chalmers on 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.

The full program looked as follows:

- A survey of Session Fixation vulnerabilities and a thorough solution (Bastian Braun)
- A client-side approach to session fixation & session hijacking (Nick Nikiforakis)
- The state of the cross-domain nation, a survey (Walter Tighzert)
- Vulnerabilities in SAML Single-Sign-On (Jorge Cuellar)
- Invited talk: Language-Based Isolation of Untrusted JavaScript (Sergio Maffeis, Imperial College, UK)
- Information-flow Control in WebSand (Andrei Sabelfeld)
- A Lattice-based Approach to Mashup Security (Jonas Magazinius)
- Capabilities for Information Flow (Arnar Birgisson)
- Secure Multi-Execution (Lieven Desmet)
- Limiting Information Leakage in Event-based Communication (Willard Rafnsson)
- Invited talk: Site security policies from a practical perspective (CSP, XFO, HSTS) - Will new HTTP-Headers Save Us (John Wilander, OWASP Sweden)
• Towards a Browser Feedback for Multiple TLS Certificate Verifications (Bastian Braun)

• Enforcing Policies for Web Mashups in Secure EcmaScript 5 (Phu H. Phung)

• WebJail: Intra-origin sandboxing (Lieven Desmet)

For the second WebSand event, a 5-day Dagstuhl seminar on “Web Application Security” (Seminar no. 12401) has been scheduled for 1-5 October 2012. The Dagstuhl seminar can host approximately 60 international participants, and will be organized by three WebSand leaders (Lieven Desmet, Martin Johns and Andrei Sabelfeld) and Ben Livshits (Microsoft Research, US).

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 are enumerated on the next pages.
<table>
<thead>
<tr>
<th>Event name</th>
<th>Participation</th>
<th>Date</th>
<th>Location</th>
<th>Partner(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISSE 2010: GI Sicherheit</td>
<td>Academic dissemination of research results [21]</td>
<td>05/10/2010 - 07/10/2010</td>
<td>Berlin, Germany</td>
<td>UNI PASSAU</td>
</tr>
<tr>
<td>TU Darmstadt</td>
<td>Colloquium / invited talks</td>
<td>14/10/2010</td>
<td>Darmstadt, Germany</td>
<td>CHALMERS</td>
</tr>
<tr>
<td>it-sa 2010</td>
<td>Participation at academia/industry event</td>
<td>19/10/2010-21/10/2010</td>
<td>Nuremberg, Germany</td>
<td>SIEMENS</td>
</tr>
<tr>
<td>OWASP AppSec Germany 2010</td>
<td>Participation at industry event</td>
<td>20/10/2010</td>
<td>Nuremberg, Germany</td>
<td>SIEMENS</td>
</tr>
<tr>
<td>Nordsec 2010</td>
<td>Academic dissemination of research results [7, 10, 16]</td>
<td>27/10/2010 - 30/10/2010</td>
<td>Espoo, Finland</td>
<td>KUL, CHALMERS</td>
</tr>
<tr>
<td>Future Internet Week</td>
<td>Boot at industry event with WebSand PR</td>
<td>15/12/2010 - 16/12/2010</td>
<td>Ghent, Belgium</td>
<td>KUL</td>
</tr>
<tr>
<td>OOP2011, Security Track</td>
<td>Participation at industry event</td>
<td>24/01/2011-28/01/2011</td>
<td>Munich, Germany</td>
<td>SIEMENS</td>
</tr>
<tr>
<td>ESSoS 2011</td>
<td>Academic dissemination of research results [19]</td>
<td>09/02/2011</td>
<td>Madrid, Spain</td>
<td>KUL</td>
</tr>
<tr>
<td>EICT Conference: IT-Sicherheit: “Vertrauen, Datenschutz, Sicherheit und Innovation”</td>
<td>Presentation at academia/industry event</td>
<td>10/02/2011</td>
<td>Berlin, Germany</td>
<td>UNI PASSAU</td>
</tr>
<tr>
<td>ACM SAC 2011</td>
<td>Academic dissemination of research results [13]</td>
<td>21/03/2011 - 24/03/2011</td>
<td>Taichung, Taiwan</td>
<td>UNI PASSAU</td>
</tr>
<tr>
<td>ICST 2011, SECTEST Workshop</td>
<td>Academic dissemination of research results [12]</td>
<td>25/03/2011</td>
<td>Berlin, Germany</td>
<td>SAP</td>
</tr>
<tr>
<td>Event name</td>
<td>Participation</td>
<td>Date</td>
<td>Location</td>
<td>Partner(s)</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>----------------------------------------------------</td>
<td>------------------------</td>
<td>-----------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>European Workshop on System Security</td>
<td>Academic dissemination of research results [18]</td>
<td>10/04/2011</td>
<td>Salzburg, Austria</td>
<td>KUL</td>
</tr>
<tr>
<td>OWASP Sweden Chapter Meeting</td>
<td>Industrial dissemination of WebSand results</td>
<td>14/04/2011</td>
<td>Gothenburg, Sweden</td>
<td>All partners</td>
</tr>
<tr>
<td>KULeuven</td>
<td>Colloquium / invited talks</td>
<td>10/05/2011</td>
<td>Leuven, Belgium</td>
<td>CHALMERS</td>
</tr>
<tr>
<td>W2SP 2011</td>
<td>Academic dissemination of research results [15]</td>
<td>26/05/2011</td>
<td>Oakland, California, USA</td>
<td>SAP</td>
</tr>
<tr>
<td>Stanford University</td>
<td>Colloquium / invited talks</td>
<td>03/06/2011</td>
<td>Palo Alto, USA</td>
<td>CHALMERS</td>
</tr>
<tr>
<td>W2SP 2011</td>
<td>Academic dissemination of research results [20, 5]</td>
<td>05/06/2011</td>
<td>San Jose, California, USA</td>
<td>CHALMERS</td>
</tr>
<tr>
<td>W2SP 2011</td>
<td>Participation at industry event</td>
<td>09/06/2011 - 10/06/2011</td>
<td>Dublin, Ireland</td>
<td>KUL</td>
</tr>
<tr>
<td>IT-Speicher Regensburg: Mobile Applikationen in Breitbandnetzen</td>
<td>Boot at industry event with WebSand PR</td>
<td>28/06/2011</td>
<td>Regensburg, Germany</td>
<td>UNI PASSAU</td>
</tr>
<tr>
<td>Harvard University</td>
<td>Colloquium / invited talks</td>
<td>31/08/2011</td>
<td>Boston, USA</td>
<td>CHALMERS</td>
</tr>
<tr>
<td>Google Doctoral Fellowship Forum</td>
<td>Poster presentation</td>
<td>20/09/2011</td>
<td>Zurich, Switzerland</td>
<td>CHALMERS</td>
</tr>
</tbody>
</table>
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 two summer schools (Marktoberdorf Summer School 2011 and Microsoft Research Summer School 2011), and has given a demo on CsFire at the Future Internet Week.

- CsFire demo at Future Internet Week, 15/12/2010 - 16/12/2010, ICC, Ghent, Belgium (by Lieven Desmet)
- Secure Application Development Course (SecAppDev), 28/02/2010 - 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)

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 year have been influenced by the WebSand project:

- Web Application Security Lab (given at Karlsruhe Institute of Technology 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)

Over the past year, the following thesissess has been supervised in scope of the WebSand research topics:

• 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
• Dynamic enforcement of decentralized security policies (Licentiate thesis, Jonas Magazinius, 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)
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 are at the basis 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).

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

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 [9], 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.

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.

**FP7-ICT IP HATS** The theory of Secure-Multi Execution that is applied in WP3 has been developed in the HATS project.

**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 Natalia 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 NESSoS Network of Excellence on Engineering Secure Future Internet Software Services and Systems, in particular on the security of web environments.

**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.

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:


References


