Server-driven Outbound Web-application Sandboxing

From 2010-10-01 to 2014-03-31

Objective

Since its birth in 1990, the Web has evolved from a simple, stateless delivery mechanism for static hypertext documents to a fully-edged run-time environment for distributed, multi-party applications. Security becomes increasingly important in this context, but is typically only an afterthought in this process. The next wave, the Future Internet, will continue to rely on the same web application technology, while adopting more p2p and mashup-style approaches. Today’s server-centric solutions will give way to a rich and stateful client-centric paradigm with even less manageable security and even more severe threats to the web-based economy of the Future Internet. Data and services from multiple heterogeneous domains, aggregated both on the server-side and on an end-user’s client, demand for a novel, comprehensive security solution that increases the user’s trust into the technological infrastructure. WebSand tackles this demand by departing from the observation that security should be server-driven. Even though security preferences from end-users at the client-side have to be taken into account, only the service developers at the server-side have the necessary expertise and context information to define the policies to be enforced. Moreover, server-driven security can be deployed relatively easily, since much can be achieved without updating the client-side platform. The WebSand framework consists of four major building blocks: (1) a secure interaction model, that allows explicit and fine-grained control concerning incoming Web communication, (2) methods for secure end-to-end information flow control, to enforce confidentiality and integrity properties, (3) behavioral sandbox environments for secure client-side and server-side composition of multi-origin components, and (4) a declarative and expressive policy description mechanism that ties the individual components together into a unified security architecture spanning client and server.

Related information

Top Stories

- WEBSAND: In-built security for a safer web experience

Documents and Publications

- D 3.1
- D 6.1
- D 2.1
- D 1.3
Coordinator

SAP AG
Vincenz Priessnitz Strasse 1
76131 Karlsruhe
Germany
Administrative contact: Martin Johns
Tel.: +496227752547
Fax: +4962277844618
E-mail

Participants

KATHOLIEKE UNIVERSITEIT LEUVEN
Oude Markt
3000 LEUVEN
Belgium
Administrative contact: Tine Heylen
Tel.: +32 16 32 65 20
Fax: +32 16 32 65 15
E-mail

UNIVERSITAT PASSAU
Innstrasse
94032 PASSAU
Germany
Administrative contact: Sabine Wiendl
Tel.: +49 851 5091110
Fax: +49 851 5091102
E-mail

SIEMENS AKTIENGESELLSCHAFT
Wittelsbacherplatz
80333 MUNICHEN
Germany
Administrative contact: Jorge Cuellar
Tel.: +49 89 636 47585
Fax: +49 89 636 41166
E-mail

CHALMERS TEKNISKA HOEGSKOLA AB
- 41296 GOETEBORG
Sweden
Administrative contact: Eva Paulson
Tel.: +46 31 7723585
Fax: +46 31 165655
E-mail

Subjects

- D 4.1
- D 1.2