

Safe 'sandbox' for the internet of the future

May 13 2011



To better protect new Internet applications against hacker attacks and other types of manipulation, Siemens is taking part in the EU's WebSand research project. In cooperation with partner organizations SAP, the University of Passau (Germany), the Catholic University of Leuven (Belgium), and the Chalmers University of Technology (Sweden), Siemens will be working to develop technology that will help protect users who surf dynamic, interactive websites and to implement it in software over the next three years. The system will create a protected environment in which information can be used only in a controlled manner.

Social media services such as Facebook and Twitter are examples of how active content is becoming increasingly networked on the Web. So-called "mashups" combine content and functional elements from various

sources at a single website — for example Facebook’s “I like it” function or a map from Google Maps. Although users can’t immediately recognize mashups, they pose a number of risks, including unauthorized access to personal data or monitoring of surfing behavior.

The aim of the WebSand project is to make the composition of mashups more secure in order to protect users against the threat posed by the mashups’ active elements. The website providers often don’t control external content and can’t blindly trust it, which is why the researchers are looking for other ways to control the flow of information. To do this, the user is given a security module that can run all of the embedded applications in a secure mode. When a website is called up, potentially harmful program codes run in a “sandbox,” where they can’t cause any damage.

The IT security experts at [Siemens](#)’ central research unit Corporate Technology are contributing to the project their experience with a wide variety of applications. These applications include the company’s products for industrial automation, hospital information systems, and control centers for factories and power plants. The programs for these systems are already Web-based and subject to the same changes as all other Internet sites.

Source: Siemens

Citation: Safe 'sandbox' for the internet of the future (2011, May 13) retrieved 19 May 2024 from <https://phys.org/news/2011-05-safe-sandbox-internet-future.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.