WEBSAND: Sicurezza incorporata per un'esperienza online più sicura

Un gruppo di ricercatori dell'UE ha ideato un quadro di sicurezza innovativo che garantisce agli utenti e agli sviluppatori del web una maggiore protezione contro gli attacchi informatici.

Ottobre è il mese europeo della sicurezza informatica e i cittadini dell'UE sono sempre più consapevoli dell'importanza della sicurezza online. Si stima che la criminalità informatica costi all'economia europea decine di miliardi di euro ogni anno, soprattutto a causa del furto di dati di carte di credito, che vengono poi venduti sul mercato nero.

Uno dei progetti finanziati dall'UE per combattere la criminalità informatica è denominato WEBSAND ("Server-driven Outbound Web-application Sandboxing"), il quale ha creato nuovi strumenti per rendere i sistemi più resistenti agli attacchi degli hacker.

Gli informatici di WEBSAND hanno costruito soluzioni basate su "sandbox", ovvero meccanismi restrittivi che separano i sistemi di server nonché i flussi di informazioni (tra i server e i browser degli utenti) dai codici inaffidabili.

SISTEMARE IL WEB

"Il principale successo di WEBSAND è stato di mostrare agli sviluppatori come fare della sicurezza una parte integrante del sistema, piuttosto che una cosa aggiunta in seguito", ha spiegato il coordinatore, il dott. Martin Johns .

Il web è notevolmente cambiato dal 1990, quando veniva usato come strumento statico per la fornitura di documenti. Ormai è diventato un ambiente multisorgente in tempo reale, che costringe gli sviluppatori ad aggiungere la sicurezza ai sistemi,

anziché farne parte integrante del modello client/server. WEBSAND è stato creato per cercare di cambiare proprio questo.

"Ci siamo proposti un obiettivo deliberatamente ambizioso sin dall'inizio del progetto. Abbiamo pensato: "Cerchiamo di sistemare il web". E in qualche modo ci siamo riusciti. Abbiamo costruito un sacco di soluzioni direttamente dalla parte del server, le quali rafforzano la sicurezza richiesta per alcune aree".

L'obiettivo era di mettere lo sviluppatore al posto di guida, assumendo un approccio alla sicurezza orientato al server e costruendo un quadro modulare e facile da usare, che permettesse anche agli sviluppatori con un'esperienza limitata nel campo della sicurezza di costruire applicazioni sicure per default.

Inoltre, WEBSAND ha sviluppato una serie di estensioni del browser per gli utenti finali, tra cui CSFIRE , che è invisibile agli utenti nel senso che cerca di non interferire con la funzionalità delle applicazioni che stanno usando – che sia un programma di email, Facebook, Google o un convertitore di valuta, per esempio – mentre li protegge in modo trasparente dagli attacchi in rete.

Gli scienziati di WEBSAND hanno anche studiato e ideato soluzioni per alcuni dei problemi fondamentali del web.

Hanno progettato un'aggiunta leggera alla parte del cliente dei browser che previene gli attacchi DNS Rebinding, un metodo comune e frequente di estrarre informazioni da un server senza che l'host se ne accorga. Una leggera espansione della "same origin policy" del server elimina questo rischio.

Hanno anche proposto un modo diverso di autenticare le password, implementando un nuovo sistema di richiesta e risposta che ha origine nel server anziché nel browser.

Adesso i partner principali del progetto – le aziende tedesche SAP e Siemens , l'Università di Lovanio in Belgio e l'Università di Chalmers in Svezia – stanno lavorando con gli organismi internazionali di normazione internet, W3C e IETF, per convincere le aziende di browser ad adottare la tecnologia di WEBSAND. Aderiscono anche all'organizzazione no profit OWASP (Open Web Application Security Project) e stanno promuovendo i loro risultati attraverso gruppi di utenti e incontri.

"Alla SAP e alla Siemens usiamo la tecnologia di WEBSAND per rendere più sicuri i nostri prodotti, ma ovviamente un web sicuro in partenza sarebbe un vantaggio", ha detto il dott. Johns. "La sicurezza è molto costosa e un web più sicuro permetterebbe alle aziende di destinare più risorse alla funzionalità".

WEBSAND, che è durato da ottobre 2010 ad aprile 2014, era composto da cinque partner di tre paesi e ha ricevuto un finanziamento di 3,2 milioni di euro dal 7° PQ.

Collegamento al sito web del progetto

Progetti correlati

ARCHIVED

Server-driven Outbound Web-application Sandboxing

WEBSAND

25 Maggio 2022

PROGETTO

Questo articolo è contenuto in...

RIVISTA RESEARCH*EU

L'idrogeno potrebbe rivoluzionare il nostro modo di vivere?

Ultimo aggiornamento: 27 Ottobre 2014

Permalink: https://cordis.europa.eu/article/id/149101-websand-inbuilt-security-for-a-safer-web-experience/it