Foundations and Tools for Client-Side Web Security

Résultats en bref

Renforcer la sécurité du web pour les utilisateurs quotidiens

De nouvelles méthodes d'identification des potentielles vulnérabilités des navigateurs web pourraient renforcer la résilience du monde numérique face à la multiplication des cyberattaques.

ÉCONOMIE NUMÉRIQUE

Les cyberattaques constituent une violation des droits de l'homme dont les conséquences peuvent être dévastatrices pour les individus et la société. «Ces attaques comprennent des logiciels rançonneurs qui exigent un paiement des utilisateurs et des entreprises», explique Matteo Maffei, coordinateur du projet Browsec, de TU Wien, en Autriche.

«Les cyberattaques ciblent également les infrastructures critiques, tandis que les hypertrucages (deepfakes), qui utilisent l'intelligence artificielle pour usurper l'identité d'une personne, peuvent tromper les victimes.»

Les pirates informatiques profitent souvent de l'utilisation intensive que nous faisons des navigateurs web. À mesure de leur évolution, ces navigateurs deviennent inévitablement vulnérables à des bogues critiques pour la sécurité qui peuvent être difficiles à détecter.

«Qui plus est, les normes de sécurité intégrées dans les navigateurs modernes ne

sont pas entièrement comprises», ajoute Matteo Maffei. «Les cyberattaques tentent d'exploiter non seulement les bogues de codage, mais également les failles logiques des normes Web elles-mêmes.»

Extensions de navigateur et techniques de vérification de code

L'objectif du projet Browsec, financé par le Conseil européen de la recherche, était de répondre à ces enjeux critiques. Pour ce faire, il a tout d'abord sécurisé le code du navigateur et, plus important encore, veillé à ce que les normes de sécurité du web fournissent aux développeurs et aux utilisateurs des garanties de sécurité rigoureuses.

«Notre recherche repose sur trois piliers fondamentaux», explique Matteo Maffei. «Tout d'abord, nous avons développé un modèle formel qui définit le comportement du navigateur et les interactions avec les sites web et les serveurs potentiellement hostiles.»

Ce modèle a permis à l'équipe de mener des tests rigoureux, de découvrir des interactions inattendues et de révéler de potentielles vulnérabilités.

«Nous avons ensuite reconnu que la mise à jour des navigateurs constituait un défi de taille», ajoute Matteo Maffei. «Pour y remédier, nous avons créé une technique automatisée qui formalise le comportement des navigateurs. Celle-ci a été réaffectée à l'analyse de la sécurité.»

L'équipe a ensuite développé des extensions de navigateur et des techniques de vérification du code, conçues pour appliquer collectivement des garanties de sécurité rigoureuses dans les applications web.

Normes web et sécurité des navigateurs modernes

Browsec a apporté une importante contribution aux normes web et à la sécurité des navigateurs modernes. Tout d'abord, les vulnérabilités découvertes dans le carde du projet ont été divulguées et corrigées depuis.

«Certaines de ces vulnérabilités découlent de problèmes conceptuels dans les cadres de développement web utilisés pour créer la quasi totalité des applications web», ajoute Matteo Maffei. «Notre travail a permis de résoudre ces questions.»

L'équipe a également découvert diverses incohérences et failles dans les normes web, qui ont été signalées aux organismes de normalisation. Enfin, le cadre

d’analyse de la sécurité des navigateurs du projet peut servir de base à l’étude des implications de sécurité des futures mises à jour des navigateurs.

La sécurité du web dès la conception

Grâce à Browsec, les développeurs web ont désormais accès à des bibliothèques qui leur permettent d’écrire un code plus sécurisé. Les fournisseurs disposent d’un cadre leur permettant de tester non seulement la fonctionnalité, mais également la sécurité de leurs navigateurs. En outre, les organismes de normalisation disposent désormais d’un cadre officiel d’évaluation de la sécurité des normes web.

«Browsec a eu un impact profond sur la sécurité de l’ensemble de la société numérique», souligne Matteo Maffei. «Notre cadre d’analyse sera mis à jour en tenant compte des changements, et nous entendons également réaliser une intégration plus étroite avec le processus de normalisation.»

Pour Matteo Maffei, l’un des principaux enseignements, et l’héritage durable de Browsec, est le fait que les méthodes formelles constituent un outil efficace et pratique pour assurer la sécurité du web.

«Les méthodes que nous avons développées se sont avérées efficaces non seulement pour identifier les bogues, mais également pour influencer le processus de normalisation», conclut-il. «Cela a rapproché le concept de “sécurité du web dès la conception” de la réalité.»

Mots-clés

Browsec, cyberattaques, numérique, navigateur web, ransomware, hypertrucages

Découvrir d’autres articles du même domaine d’application

Placer l’Europe à l’avant-garde de la révolution des supercalculateurs

Une technologie perturbatrice qui stimule la compétitivité des PME dans le secteur B2B

Donner à l'Europe une longueur d'avance en matière d'IA

Alice envoie des informations quantiques à Charlie

Informations projet

Browsec

N° de convention de subvention: 771527

Site Web du projet

DOI
10.3030/771527

Projet clôturé

Financé au titre de
EXCELLENT SCIENCE - European Research Council (ERC)

Coût total
€ 1 990 000,00

Contribution de l'UE
€ 1 990 000,00

Coordonné par

Date de signature de la CE
28 Mars 2018

TECHNISCHE UNIVERSITAET WIEN
Austria

Date de début
1 Juin 2018

Date de fin
30 Novembre 2024

Dernière mise à jour: 10 Avril 2025

Permalink: https://cordis.europa.eu/article/id/457695-enhancing-web-security-for-everyday-users/fr