ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ

ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΑΡΟΥΣΙΑΣΗ / ΕΞΕΤΑΣΗ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Καράμπελας Απόστολος - Παράσχος
Μεταπτυχιακός Φοιτητής

Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης

Επόπτης Μεταπτυχιακής Εργασίας: Επικ. Καθηγητής, Π. Πρατικάκης

Τετάρτη, 28 Ιουλίου 2021, ώρα 12:00 μ.μ.

Join Zoom Meeting
https://zoom.us/j/98977909394

"Αναπτύσσοντας μία απομονωμένη πλατφόρμα εντός περιηγητή για εφαρμογές ασφάλειας εναντίον κακόβουλων επεκτάσεων"

Περίληψη

Οι σύγχρονοι περιηγητές ιστού προσφέρουν στους προγραμματιστές μεγάλη ποικιλία ισχυρών δυνατοτήτων, επιτρέποντάς τους να μεταφέρουν τη λογική εφαρμογών ιστού προς τη μεριά των χρηστών ολο και περισσότερο. Αυτή η αλλαγή παραδείγματος στοχεύει στη βελτίωση της ποιότητας εμπειρίας των τελικών χρηστών, ελαχιστοποιώντας τις καθυστερήσεις δικτύου και αυξάνοντας την επεκτασιμότητα των υπηρεσιών Ιστού.

Στον πυρήνα αυτών των λειτουργιών βρίσκονται οι επεκτάσεις περιηγητών, οι οποίες έχουν πρόσβαση σε ένα πλούσιο σύνολο εργαλείων ώστε να μπορούν να ικανοποιήσουν ειδικές ανάγκες χρηστών, όπως την προσαρμογή του περιβάλλοντος διεπαφής χρήστη ή τον αποκλεισμό διαφημίσεων. Οι επεκτάσεις έχουν επίσης ευρεία υιοθέτηση στη βιομηχανία, έχοντας γίνει μια πολύ δημοφιλής επιλογή μεταξύ εταιρειών του διαδικτυακού οικοσυστήματος, για την ανάπτυξη και συντήρηση της λογικής των

υπηρεσιών τους στη μεριά του χρήστη. Δυστυχώς, κακόβουλοι παράγοντες εκμεταλλεύονται συχνά τις επεκτάσεις για να εκτελέσουν επιθέσεις τύπου Man-in-the-Browser, όπου αυτές λειτουργούν ως όχημα κατασκοπείας, ηλεκτρονικού ψαρέματος και απάτης εις βάρος απληροφόρητων χρηστών. Σε ορισμένες περιπτώσεις, η απόκτηση παράνομης πρόσβασης σε έναν προνομιούχο χρήστη δημιουργεί έναν πιο ισχυρό φορέα επίθεσης κατά της υπηρεσίας ή των πολυάριθμων χρηστών της.

Με αφορμή την έλλειψη αποτελεσματικών αντιμέτρων από τους κύριους προμηθευτές περιηγητών, αυτή η εργασία προτείνει το WRIT, ένα πρακτικό πλαίσιο κώδικα που επιτρέπει σε ιστότοπους και παρόχους υπηρεσιών διαδικτύου να προστατεύουν κρίσιμη λειτουργικότητα από κακόβουλες επεκτάσεις. Ο πρωταρχικός στόχος του WRIT είναι να δημιουργήσει και να διατηρήσει ένα αξιόπιστο περιβάλλον εκτέλεσης απομονωμένο τόσο από συμβατικό κώδικα στη μεριά του χρήστη όσο και από επεκτάσεις, όπου ευαίσθητος κώδικας μπορεί να αναπτυχθεί και να εκτελεστεί ασφαλώς. Στη συνέχεια, το WRIT παρέχει τα απαραίτητα εργαλεία για να επιβεβαιώσει την ακεραιότητα των εξερχόμενων αιτημάτων ιστού και να επαληθεύσει την αυθεντικότητά τους, διασφαλίζοντας ότι προκλήθηκαν από την ενέργεια ενός χρήστη και όχι από κακόβουλη επέκταση.

Αξιολογούμε τις ιδιότητες ασφαλείας του WRIT αναλύοντας τις πιθανές επιθέσεις που μπορεί να εκτελέσει μία επέκταση ενάντια στον κώδικα μιας υπηρεσίας ιστού και στο ίδιο το WRIT. Κάθε σενάριο επίθεσης εκτελείται και δοκιμάζεται ενάντια στο WRIT στην πράξη μέσω μιας μεμονωμένης προσαρμοσμένης επέκτασης. Πραγματοποιούμε επίσης μια αξιολόγηση απόδοσης δοκιμάζοντας την πρωτότυπη υλοποίηση του WRIT υπό διαφορετικές συνθήκες δικτύου. Τα πειραματικά μας αποτελέσματα δείχνουν ότι προσθέτει μία αμελητέα καθυστέρηση 7.29 ms σε ευαίσθητες ενέργειες που ενεργοποιούνται από χρήστες, όπως η δημοσίευση ενός μηνύματος σε κοινωνικά μέσα.

University of Crete

Computer Science Department

M.Sc. Thesis presentation / examination

Karampelas Apostolos- Parasxos

Master's Thesis Supervisor: Assistant Professor, P. Pratikakis

Wednesday, 28 July 2021, 12:00 p.m.

Join Zoom Meeting

https://zoom.us/j/98977909394

“Developing an isolated in-browser platform for security applications against malicious browser extensions”

Abstract

Modern web browsers offer developers a wide variety of powerful features, enabling them to push web application logic to the user side increasingly. This paradigm shift aims to improve end-user quality of experience by minimizing the latency and increasing the scalability of web services.

At the core of these features lie browser extensions, which have access to a rich set of tools so that they can satisfy unique user needs, like customizing the user interface or blocking ads. Extensions have also seen wide adoption in the industry, becoming a very popular avenue for companies in the web ecosystem to deploy and maintain the client side logic of their services. Unfortunately, malicious actors often exploit extensions to launch Man-in-the-Browser attacks, where they serve as a vehicle for spying, phishing and fraud at the expense of unknowing users. In some cases, compromising a privileged user opens up a more potent attack vector against the web service or its broad userbase.

Motivated by the lack of effective countermeasures by major browser vendors, this thesis proposes WRIT, a practical framework that enables websites and web service providers to protect critical functionality from malicious extension abuse. WRIT's primary objective is to establish and maintain a trusted execution environment isolated both from conventional client-sided code and extensions, where security-sensitive code can be deployed and run safely. WRIT then provides the necessary tools to attest the integrity of outgoing web requests and verify their authenticity, ensuring they were triggered by a user's action and not by a malicious extension.

We evaluate WRIT's security properties by analyzing the possible attacks extensions
can launch against a web service's client-sided code and WRIT itself. Each attack scenario is executed and tested against WRIT in practice through an individual custom extension. We also conduct a performance evaluation testing WRIT's prototype implementation under varying network conditions. Our experimental results show that it adds a negligible 7.29 ms latency to sensitive actions triggered by users, such as posting a message on social media.