Engineer develops browser-based analysis framework observer

November 19 2019

Professor Wei Meng. Credit: The Chinese University of Hong Kong

Malicious third-party advertisers or hackers expose web users to a security threat by injecting malicious JavaScript code to intercept user clicks and trick them into visiting untrusted web content. To investigate the problem of click interception, the research team led by Professor

Wei Meng of the Department of Computer Science and Engineering, Faculty of Engineering, The Chinese University of Hong Kong (CUHK) developed a browser-based analysis framework—Observer, which is able to detect three different techniques for intercepting web user clicks.

The research result has been published in USENIX Security Symposium 2019 (USENIX Security '19), one of the top academic conferences in computer security. The research team will release the source code of the framework publicly to help web browsers detect malicious click interceptions and alert users about the malicious behaviour to protect them from being exposed to malicious content.

A click is the prominent way that users interact with content on the World Wide Web (WWW). Attackers therefore aim to intercept genuine user clicks to either launch ad click frauds by fabricating ad click traffic, or to send malicious commands to another website on behalf of the user (e.g., to force the user to download malwares). Previous researches mainly considered one type of click interceptions in the cross-origin settings via iframes, i.e., clickjacking, that is usually launched by malicious first-party websites. This does not comprehensively represent various click interceptions that can be launched by third-party JavaScript code.

To address this research gap, Professor Wei Meng and his Ph.D. student Mingxue Zhang of the Department of Computer Science and Engineering developed an analysis framework—Observer based on the Google Chromium browser, to systematically record and analyse various click interceptions on the Web. Using Observer, they analysed Alexa top 250K websites, and detected 437 third-party scripts that intercept user clicks on 613 popular websites, which in total receive around 43 million visits on a daily basis. In particular, though click interception, these scripts could trick users into visiting 3,251 untrusted unique uniform resource locators (URLs) controlled by third parties. Over 36% of them

were related to online advertising. Further, some click interception URLs led users to malicious content such as scamwares. This demonstrates that click interception has become an emerging threat to web users.

The research identified three categories of click interception techniques: (1) modifying the destination URL of hyperlinks to lead users to malicious websites upon clicks; (2) adding click event listeners to manipulate user clicks; (3) visual deception, for example, by creating web content that is visually similar to first-party content, or displaying transparent elements on top of the web page. The former will trick users into clicking the third-party element, and the latter enables the transparent elements to capture all user clicks on the first-party content. Consequently, the users can be led to a page controlled by the attackers.

It is acknowledged that web behaviour caused by third-party JavaScript code is difficult to record and analyse. Observers detect third-party click interceptions by extending the browser to collect the behaviour at runtime and thoroughly analysing the click-related behaviour. The system is of great significance in protecting web users from such security threats. Professor Wei Meng thinks the root cause of click interception might be the privilege abuse by third-party web developers, who intercept user clicks for monetisation via committing ad click fraud. He said, "We will make our implementation publicly available. The browser vendors can design defense mechanisms against click interception accordingly. For example, they can show security warnings to users to prevent them from accessing potentially malicious web pages. This can help build a more secure web ecosystem."

Provided by Chinese University of Hong Kong

Citation: Engineer develops browser-based analysis framework observer (2019, November 19)