Learn Clickjacking 2.0 attack method

British security expert - Paul Stone demonstrated a completely new attack method of clickjacking attack ...

***TipsMake.com* - At the hacker conference - Black Hat Europe just ended in Barcelona, ??the British security expert - Paul Stone demonstrated a completely new attack method of clickjacking attack** .

Clickjacking involves a web page that is prepared manually by automatically inserting an iFrame 'stealth' module under the action of the mouse cursor. When users work on a certain website, they are actually interacting with another website with components controlled through iFrame.

Stone's presentation does not limit the number of clicks, can fill in text and form values, read text that is being opened in the victim's browser or other source sites. At the same time, Stone also takes full advantage of the drag-and-drop capabilities, provided by the API, which are now available in most current browsers like Internet Explorer, Firefox, Chrome and Safari. In addition to "assigning" a victim to a controlled object, Stone also demonstrates the ability to "control" the user to drag any object, a text string from a window or a form. available on 1 'invisible' module.

This can be explained as follows, users log into a social page or a certain website, when opening a website from

this source page through a built-in hidden frame, of course people use does not know this existence. In Stone's opinion, the policy of operating in the same source of browsers does not show much of the counter-action in this situation, and the components in that site will automatically be converted from any site to The site is built on the user's 'unintentional' action. Using this method, Stone can circumvent the restrictions to prevent tampering with similar requests to cross-site.

In contrast, the drag-and-drop feature is also used to copy content from the user's window to the attacker's work window. Also according to Stone, this can be used to access the website's HTML code, including ID functions or token identification strings. And through this mechanism, the attacker will easily insert other control functions. Such attacks are becoming more sophisticated when Java and Javascript are embedded in the system. Also, according to Stone, Java's drag-and-drop API is more powerful than the browser. Taking advantage of this, attackers will divide and mark text as text by dragging and dropping content with a single click. When combining this feature with other attack methods via Javascript, it is possible to place drag and drop commands at any time, even if the mouse pointer has not moved to the location specified by the Java applet. or when the victim does not press and hold the left mouse button.

Besides, Java also supports faster form fill feature. Instead of waiting for each action to click on the victim, the attacker can complete the content form in a single operation. ' *Spraying* ', the brief method of this method, can work in Windows and Mac OS X platforms, but cannot be applied to Linux.

However, these types of attacks can be blocked by trusted web server systems, when sending the request with " ***X-FRAME-OPTIONS: DENY*** " to the header of a browser, any thing This will protect and allow the website to display in a single frame. However, only the latest browser versions such as Internet Explorer 8, Safari 4 and Chrome 2 are able to 'notice' this option, maybe Mozilla Firefox will be equipped with this feature for a while. time is not far away. Stone also points out that, for large or very large websites like facebook.com, googlemail.com and twitter.com, it has been able to fight clickjacking, but besides that, according to the reviews. Other security experts, mobile or smartphone versions of these browsers have also been optimized to the highest level to avoid the risk of clickjacking attacks.

Recently, Stone has provided tools to help developers understand more about the mechanism of clickjacking. This tool illustrates the full process and implementation modules of clickjacking attack mechanisms, including classic and modern ways.