21 January 2008

By: Marius Oiaga, Technology News Editor

Kicking Internet Explorer Security Up a Notch

Security and HTML frames (FRAMESETs and IFRAMEs)

IE7
Microsoft

Browsers are among the top exploited software products, as they provide the bridge between the users' machine and the Internet. And being one of the main vectors for attacks and exploits makes bulletproofing browsers a critical task in terms of delivering user protection. Microsoft's proprietary **Internet Explorer** browser, with its various iterations, currently accounts for the lion's share of the operating system market, with Mozilla's open source Firefox as the runner-up. IE's dominance was in fact more steep before the advent of Firefox. Bundled into Windows as a countermeasure to Netscape's near-monopoly on the browser market in the past decade, Internet Explorer developed a reputation as an insecure product.

And as IE's success in terms of audience ensured that it was the main target for attacks, **Firefox** grew in the background, dislodging audience away from IE. One of the aspects that contributed to drawing the public to the open source browser was the fact that it offered a much more secure product. This prompted Microsoft to come out with Internet Explorer 7, also focused on security. Still, the Redmond company's official position has also been that web developers share a responsibility to contribute to the end users' protection, as much as the browser maker. In this context, Eric Lawrence, IE Program Manager, revealed a method for securing HTML frames (FRAMESETs and IFRAMEs).

"HTML frames (FRAMESETs and IFRAMEs) are a feature of all modern web browsers that enable content from multiple pages to be displayed within a single view. Historically, frames were primarily used to enable partial page updates, where page navigation was contained in one frame, and page content was contained in another. Over time, use of frames expanded to include advertising, mashup, and AJAX scenarios. Today, the majority of popular websites use IFRAMEs for myriad reasons. From a security point of view, frames can help increase the security of web applications by creating isolation between content delivered from different sources," Lawrence explained.

But the Redmond company has proved again that it lives in a Microsoft-centric world. Lawrence came up with a rather simple solution to bulletproofing Frames, namely to add a "security restricted" attribute to each item. This detail will cause the browser to consider all content in such frames as belonging in the Restricted Sites Security Zone. However, the sole downside for web developers is that the attribute mentioned by Lawrence is rather proprietary. Yes, it has been around since the turn of the century, and it became a valid web site construction attribute with Internet Explorer 6, but at the same time it is still specific only to Internet Explorer.

"For frames rendered in Internet Explorer 6 and later, security can be further increased by setting the frame's SECURITY attribute to the value 'restricted'. Doing so causes Internet Explorer to treat the contents of the frame, regardless of their source, as content that should be rendered in the Restricted Sites Security Zone. Frames running in the Restricted Sites zone cannot run script, invoke ActiveX controls, redirect to other sites, and so on. This technique is particularly useful in cases where the frame's content cannot be assumed to be trustworthy (as in the case of web mail scenario above). However, it is important to understand that HTML frames are not a security panacea," Lawrence added.