The Internet Explorer pop-up blocker follows guidelines, not rules

August 31, 2007

Raymond Chen

Here's a question that came in from a customer (paraphrased):

> Hello, we are developing an ASP.NET application and are running into problems with the pop-up blocker introduced in Windows XP Service Pack 2. Where can we get a full description of the rules that control whether a pop-up will be blocked so we can make sure our pop-ups are let through?

There is no full description because that would make the pop-up blocker useless. Suppose a formal description were available. Somebody studies the formal description and finds a loophole in the pop-up blocker and exploits it. (Indeed that is precisely what this customer is trying to do!) The browser team finds the same loophole and tries to plug it. The exploiter says, "Uh uh, according to your formal description, the XYZ technique avoids all the checks and therefore must not be blocked." A bug has become a feature. What you do have is a guiding principle: "Pop-ups are allowed if they were triggered by an explicit user input." For example, if the user clicks a button or link, you can display a pop-up in response to that click. React to the click when it is clicked. The click isn't a coupon you can save and then spend later. You have to do it when the click happens. Consequences of this guiding principle:

- Don't "forward" the click through redirects. Again, the browser won't necessarily make the connection between the redirect and the click.
- Don't set a timer and then display the pop-up later, because the browser won't necessarily make the connection between the call to `window.open` from your timer and the user click action from long ago. (Arguably, the user won't make the connection either!)

The point is, you get your chance when the click happens. If you blow it, then it's gone. If you are implementing an ActiveX control, you need to make sure to forward `QueryService` calls through your site chain so that when your control decides to perform a navigation, the navigation object can connect back to the web browser's pop-up blocker to determine whether the navigation should be allowed or blocked. In the future, new rules may be invented to plug additional holes in the current implementation, but the guiding principle

will still govern. Stick to the principles and you'll be fine. **Notes** I reiterate that the reason for not disclosing the "official rules" is *not* for security reasons. (Indeed the word "security" never appears in the article.) The reason is that making the rules official means that you can never change them. And the IE team wants to reserve the right to change the rules. Notice that the customer was looking for a *guarantee* that their pop-up algorithm will always be permitted in current and future versions of IE. In other words, they wanted a promise that the rules would never change. Some people have mentioned that Firefox has disclosed their rules for pop-up blockers. Has Firefox also promised never to change their rules? What happens if Firefox makes a change, and a site that used to be allowed is now blocked? Can the site sue Firefox for violating its own rules? You can find loopholes in even the simplest rules. "If the user physically clicks the mouse button over a link element that is enabled, visible, and all that good stuff, and the link is marked to open in a new window, then it will open in a new window." Sounds like a pretty fair rule, but are you willing to guarantee that this behavior will always be permitted in all future versions of the Web browser?

I'm glad you think so, because there's a loophole in that rule. But since you made the guarantee, you can't close the loophole.

Raymond Chen

Follow