You can't even trust the identity of the calling executable

devblogs.microsoft.com/oldnewthing/20060203-00

February 3, 2006

Raymond Chen

A while back, I demonstrated that you can't trust the return address. What's more, you can't even trust the identity of the calling executable. I've seen requests from people who say, "I want to check whether I'm being called from MYAPP.EXE. I'm going to make a security decision based on the result." Although you can do this, all it does is give you more rope.

Even if you are convinced that you're being called from the expected application, you aren't any safer. An attacker can inject code into that process (say, via a global hook) and you will foolishly trust it. In the same way that you shouldn't trust who you're talking to on the phone based solely on the caller ID. Somebody could have broken into the caller's house and made the call from that phone.

Raymond Chen

Follow