There's only so much you can do to stop running code from simulating UI actions

devblogs.microsoft.com/oldnewthing/20110425-00

April 25, 2011

Raymond Chen

Commenter KiwiBlue asks whether Captcha-style tests were considered to prevent unsigned drivers from programmatically clicking the 'Install anyway' button. I'm sure somebody considered it, but Captcha has its own problems. "Type the (distorted) letters below"-type Captcha cannot be used by people with visual impairments, people who are dyslexic, or people who simply are not familiar with the Latin alphabet. (Believe it or not, the vast majority of people on the planet have a native language which does not use the Latin alphabet.) Using an audio captcha runs into the problem of different accents, letters whose readings vary (zee/zed anyone?), and computers without a sound card (like most servers). And yes, there are other types of Captchas (dog/cat, for example), but the strongest argument against Captcha is probably that it's just adding more locks to the front door while leaving the service entrance wide open. Once you make it computationally infeasible to programmatically solve the Captcha, unscrupulous driver vendors would simply inject a DLL into the "Install this unsigned driver?" process and patch the call to `DidUserAnswer-CaptchaCorrectly` so it always returns `TRUE`. Or even easier, just programmatically set the *Driver Signing Options* to *Install the software anyway*.

If somebody is running code with administrative privileges, then they already own your machine. Any roadblocks you put up they can find a way to drive over. The goal is not so much putting up stronger and stronger roadblocks (because eventually people will simply drive around them) but rather making it clear to the developer that what they're doing is driving around a roadblock.

Raymond Chen

Follow