Le Chatelier's Principle in action: Administrative overrides

devblogs.microsoft.com/oldnewthing/20140422-00

April 22, 2014

Raymond Chen

Today we have another example of Le Chatelier's Principle as interpreted by John Gall: Every system resists its proper functioning. There was a video card manufacturer which was using the `AppInit_DLLs` key so that they could inject their DLL into every process. I have no idea why. Perhaps to get a nice bonus. In Windows Vista, the `AppInit_DLLs` registry key was deactivated for both engineering and security reasons. Oh no! Undeterred, the video card manufacturer issued an update to their driver so that in addition to adding themselves to `AppInit_DLLs`, they also set the administrative override switch that re-enabled the feature. Boom, they probably got a second bonus for that.

Another lesson from this story is that if you provide an administrative override to restore earlier behavior, then you never really removed the earlier behavior. Since installers run with administrator privileges, they can go ahead and flip the setting that is intended to be set only by system administrators.

Raymond Chen

Follow