

5 October 2007

By: Marius Oiaga, Technology News Editor



Windows Vista
Editions
Microsoft

Microsoft: Top Vista Mitigations Are Not Security Features = No Guarantees for Users

There is value, but no guarantee

If you believe that User Account Control, PatchGuard (Kernel Patch Protection) and Mandatory Driver Signing introduced in Windows Vista are security mitigations, then you might want to know that you are wrong. But don't be disappointed, some of Microsoft's own people tend to think that the features enumerated above are in fact security related when that is not the case. Microsoft Technical fellow Mark Russinovich explained that a number of top Windows Vista mitigations provide absolutely no security guarantee to end users. "There's a number of misconceptions about a number of features in Windows that are perceived to be, and maybe even overly hyped as being security related. And people's expectations, and this can be everybody, I see even people at Microsoft that work in security that have this conception about these things and believe that we are making guarantees about them. And I can see how disturbed they are when I'm conversing with them and it comes out that we're not making guarantees and there's ways for malware to cross these boundaries, that they think they're there. A great example is User Account Control elevation in Windows Vista," Russinovich explained. The fact of the matter is that Microsoft's position, expressed through the voice of Russinovich was that UAC in Vista is in no way a security boundary. But in addition to the UAC, Russinovich enumerated additional technologies that are in no way security boundaries. Kernel Patch Protection (PatchGuard); Mandatory Driver Signing and Protected Mode in Internet Explorer 7 in Windows Vista also cannot be considered security boundaries. But just because Microsoft is not willing to make any guarantees to users about their features does not mean that they do not deliver some kind of value. "Either they are providing value directly now, and it might not be security it might be liability, or they are providing defense in depth. And this is the same case as for the anti-virus. There's ways around the anti-virus, but they are defense in depth, they have security value, there is no guarantee about them. There are some things that we wish would be security boundaries, such as User Account Control. Well why are they not boundaries? Because of application compatibility, for example. Or the cost of making a boundary is so high that we believe that true value to the end user doesn't justify that enormous cost, which might include application incompatibility, might include even a worst user experience people consider they have with user account control."