Mike Nelson – SV article

VMware Fusion Security – Things To Watch Out For

If you are either new to VMware Fusion or an old pro at it, there are some things you should be aware of and thinking about when it comes to security, both for the Virtual Guest, the Host, and your own sanity.

While some of these security components have been around for a while now through several versions, it is also not just limited to VMware's product but also Parallel's and any other Type 2 Hypervisor. This is due mainly to customer's asking for and getting new features that open or create new security vulnerability points in these Type 2 Hypervisors. There is basically one thing to keep in mind on the topic of security and Type 2 Hypervisors: The nature of Type 2 requires a Host OS. What does this mean in the big picture? It means a larger attack surface than just a single OS. It also means that many different types of "sharing" between the Guest and Host OS's are available and some even enabled by default.

When I first upgraded to Fusion version 4, I was somewhat surprised, from a security standpoint, by some of the options that are enabled by default. One of the big ones was Bluetooth being enabled in the Guest OS and Bluetooth Sharing enabled between the Guest and the Host. Now, before I met up with some really, really smart folks at a security conference a few years back and was taught the hard way about how easy it really is to hack into Bluetooth, I probably would not have given this another thought. Since the Host and Guest are "sharing" the Bluetooth connections to say, a nearby hackers Bluetooth device, they can both be compromised easily. For this reason alone, I believe that this is something that should be, by default, disabled.

Along with Bluetooth, there is also the ability to "share" other devices and services, like USB devices and Folders. The actual sharing of these devices in itself shouldn't really be a big security concern, but it's what could be on these USB devices and in these shared folders that should be the concern. As an example, while it is widely known that the OSX operating system has much less viruses and malware written to attack it as compared to the Windows OS, what if the USB device was compromised, or a rogue command file was executed from a shared folder, that allowed for an ambiguous type of infection that could cause trouble for either OS? If that happens, you have possibly just infected both the Guest and the Host and probably have a lot of cleanup to do.

While on the topic of shared folders, it also important to remember that these folders are not always "local" folders, but could be shares on your company or home network. If the shared folders are in fact on a network, you have just increased your attack surface to an exponential amount. More times that I wish to recall, I have run into folks who decide, for whatever reason, that the share they create should have "Everyone" with "Full Control". And, of course this share has personal, financial, or sentimental items in it, right? Be sure to lock down any shares that you enable in Fusion between the Host and the Guest, both at the file level and at the Fusion preferences level.

One new feature of Fusion is the ability to "encrypt" a Guest using a password. The issue I have with this encryption is two-fold. First, the encryption method is the older 128bit AES encryption. I don't quite understand why this was put into this new release when the much more secure 256bit AES has been available for some time. Second, the Guest files (or "package" in OS X terms) is only encrypted while the Guest is powered off. Now, while some may ask why you would need a Guest to be encrypted while it is in use, think of it this way – what if you merely "suspend" or "pause" a Guest? Since the guest is technically still in an active state (i.e. opened), then the Guest, including both disk and memory, is not encrypted in this state and is vulnerable.

For any new Fusion users out there, you may also notice that you get to decide between two separate downloads when you purchase the product, one being with McAfee's Security Suite and one without. I personally highly recommend that you download and use the one without and here's two reasons why. First of all, in all my experience with McAfee's line of products, from the Enterprise to the home user, their products are cumbersome, bloated, and difficult to manage and remove. I much prefer to use a product that is much more elegant, easy to administer, control, and remove. I have found in my trials, and you mileage and opinions may vary, that Microsoft's Security Essentials does some really good basic protection, while ESET's NOD32 products are very easy to manage and control. Secondly, while it is somewhat nice to have this option "pre-bundled" with a product, it is also only limited time activation, with all the nagging to purchase it before it runs out. Although it may not be in this case with the relationship between VMware and McAfee, in other products that carry these "bundles", the two vendors have made an monetary agreement based on the number of units that are renewed after the nagging, thus allowing the other to keep the overall cost of the product down.

The last thing I will hit on in this topic is a change made since the release of 4.0 in the post 4.01 release. "Mirrored" folders are now enabled by default in 4.01, and are specifically the Downloads and Movies folders on your Mac's hard drive. In my opinion, while a convenience to most, this is just another means to provide cross-OS infection and increases the overall attack surface of the Host and Guest. It probably won't take long for someone to exploit that.

While I am a huge fan of Fusion and use it every day, whether at home or at the office, and I.T. security is in my professional blood so I am always looking to see what's open and what's not. If Fusion users are educated on how to turn some of these default options off from the start, and not make their machines more vulnerable, everyone could enjoy some rest and relaxation instead of rebuilding machine after machine when disaster strikes.