The Old New Thing

The way to stop people from copying files to a folder is to use NTFS security, not to block drag/drop

26 Aug 2009 10:00 AM | 19

A customer wanted to prevent users from copying files to certain locations, and they did it by hooking functions like `SHFileOperation` and failing the operation if the parameters were not to its liking. The customer found that the hooks stopped working in Windows Vista because Explorer in Windows Vista uses the new `IFileOperation` COM interface instead of using the old `SHFileOperation` function. The customer wanted assistance in getting their hook working again so they could prevent users from copying files to directories they wanted to block.

Well, first of all, arbitrary function hooking is not supported by any version of Windows, so the customer was already in unsupported territory right off the bat. (There are some components which have an infrastructure for hooks, such as file system filter drivers or Winsock Layered Service Providers.)

Second, attempting to hook `SHFileOperation` to prevent the user from copying files into specific directories is looking at the problem at the wrong level, similar to the people who want to block drag/drop when what they really want to block is accidental drag/drop. If you block copying files via drag/drop in Explorer, that won't stop the user from copying files by other means, or by doing the "poor man's copy" by opening the document from the source location and doing a *Save As* to create a duplicate in the destination.

If you want to prevent the user from copying files to a directory, use the NTFS security model. Withhold *Create files* permission in the folder, and users will be blocked from copying files into the directory in Explorer, Notepad, or any other program.

Related: Shell policy is not the same as security.

Blog - Comment List MSDN TechNet

Comments

Peter
26 Aug 2009 10:33 AM
#

For goodness sake, don't create new Layered Service Providers! It's really hard to write one correctly, and when you make a bad one, it causes many, many customer issues (like, "I can't connect to the internet")

Heck, Layered Service Providers cause enough problems that there's knowledge base articles on how to reset your Winsock catalog (It turns out the command to use is "netsh winsock reset")(but don't just run it to see what it does -- some Layered Service Providers are essential)

The "Windows Filtering Platform" provides much of the same functionality without the danger to your customers. Many companies that used to provide Layered Service Providers have switched to the Windows Filtering Platform.

> [*Thanks for the tip (since I'm not an expert in the field). Though I find it interesting that people can't even get the documented API hooking method right; imagine how hard it is to get the undocumented version working... -Raymond*]

John Topley
26 Aug 2009 11:50 AM
#

That's really funny. It puts me in mind of the Maginot Line.

DWalker
26 Aug 2009 12:41 PM
#

Policy is not the same as security, except maybe for the set of policies called Local Security Policy...

Alexandre Grigoriev
26 Aug 2009 1:32 PM
#

What's sad is that this exercise in futility is repeated all over again and again. You see these questions all the time in the forums.

Daniel Colascione
26 Aug 2009 1:43 PM
#

Peter, it seems as if LSPs get more use from Malware than they do from legitimate software developers.

Erzengel
26 Aug 2009 2:18 PM
#

To me this is one of those "restating the obvious", and more proof to what I said earlier: Just because it's obvious doesn't mean people realize it.

If you want to prevent copying and creating files, why not do the obvious and revoke creation permission? Because to them, it's not obvious, and they think, "Hmm, may a shell hook?" and then go off on that tangent without ever thinking that there is an optimal solution.

Gabe
26 Aug 2009 3:09 PM
#

The difficult problem here is that they wanted to prevent *certain* files from being copied. That's incredibly hard to do (like the Halting Problem).

Hooking drag-n-drop to accomplish this is like hooking right-click on a web page to prevent people from "downloading your copyrighted images".

Michael Stum
26 Aug 2009 6:43 PM
#

I know nothing about the history, but as they have written it before Windows Vista, I might think that maybe they used FAT32 at the time, thus permissions wouldn't work.

That doesn't make arbitrary unsupported hooking any better, but it may reduce their sentence from death penalty to lifelong imprisonment instead.

arnshea
26 Aug 2009 7:22 PM
#

What if you don't know that the file copy shouldn't be allowed until it's attempted? Or if the user should be allowed to copy anything into the folder *except* certain files? Granted the hook won't cover other copying methods but if you're only concerned about casual/easy copying...

I can't help but wonder if it's time to take a step back and re-think the data persistence model. If there are files that shouldn't be copied by the user should the user be able to see them at all?

Miral
26 Aug 2009 9:35 PM
#

Yeah, they might have wanted to have some kind of smart filtering on it (you can copy these things, but not these other things; this application however can do whatever it wants on your behalf). The NTFS security model isn't capable of doing that sort of thing; you need some kind of hook somewhere.

Yuhong Bao
26 Aug 2009 9:40 PM
#

Reminds me of my comment from <http://blogs.msdn.com/oldnewthing/archive/2008/09/10/8938051.aspx>:

"Yep, don't reinvent the wheel. NT already has auditing and security features, use them."

Cheong
27 Aug 2009 3:15 AM
#

[sarcasm]

Rules / policies are made to be broken.

Your suggestion eliminates the need to define penalties for copying files to those folders.

[/sarcasm]

Alexandre Grigoriev
27 Aug 2009 10:33 AM
#

The only solution to the problem of information isolation is to separate runtime environment and/or security context for protected and unprotected information. When you run in a context where you can read classified information, you should not be able to write to unprotected storage. And vice versa.

> [*How do you prevent somebody from taking a digital picture of the monitor? -Raymond*]

Alexandre Grigoriev
27 Aug 2009 10:55 AM
#

[How do you prevent somebody from taking a digital picture of the monitor? -Raymond]

This is the ultimate question. But not all information to be protected has graphical or human-readable representation. And usually the amount of it takes many many screens.

In the end, the purpose of the exercise is to make a accidental information leak impossible, and make a data theft difficult to the point when such attempts can be detected by external (non-computer) means, such as observation.

arnshea
27 Aug 2009 1:32 PM
#

Ooooo, Raymond threw "side channel" into the mix! All kinds of bets are off once you've got a telescope and a reflective surface http://www.sciam.com/article.cfm?id=hackers-can-steal-from-reflections ...

PhilW
28 Aug 2009 3:59 PM
#

There's an aphorism that goes something like:

"If all you have is a hammer, then every problem starts looking like a nail". To a room full of developers this looks like something that needs solving with code.

anonymous
28 Aug 2009 5:12 PM
#

"...Though I find it interesting that people can't even get the documented API hooking method right;..."

All the issues I encountered with Layered Service Providers were a result of two layered providers conflicting with each other.

The API that installs a layered provider asks the developer of the provider to build a stack of providers starting with a base provider. When no other provider is present this is not problem, but when a stack with a layered provider is already present in the system the developer has to decide where in that stack to put his layered provider. Without knowing anything about the other providers there's no way to know what is the right order.

kingofgames999
31 Aug 2009 3:00 PM
#

[How do you prevent somebody from taking a digital picture of the monitor? -Raymond]

[Sarcasm]

You only allow the information to be accessed from inside your building, Ban digital camera's or any other device that can take a photo in a corporate policy. Search all employees when entering your building. for extra security have guards monitoring employee's actions at all times.

[/Sarcasm]

Me
1 Sep 2009 2:37 PM
#

>>for extra security have guards monitoring employee's actions at all times.<<

Yes, and then security guards can take out recorded videos of the information they were supposed to save instead of see.