# The arms race between programs and users

devblogs.microsoft.com/oldnewthing/20040216-00

February 16, 2004

Raymond Chen

There is a constant struggle between people who write programs and the people who actually use them. For example, you often see questions like, “How do I make my program so the user can’t kill it?” Now, imagine if there were a way to do this. Ask yourself, “What would the world be like if this were possible?” Well, then there would be some program, say, xyz.exe, that is unkillable. Now suppose you’re the user. There’s this program xyz.exe that has gone haywire, so you want to exit it. But it won’t let you exit. So you try to kill it, but you can’t kill it either. This is just one of several arms races that you can imagine.

- “I don’t want anybody to kill my process.” vs. “How do I kill this runaway process?”
- “I want to shove this critical dialog in the user’s face.” vs. “How do I stop programs from stealing focus?”
- “I don’t want anybody to delete this file.” vs. “How do I delete this file that refuses to be deleted?”
- “How do I prevent this program from showing up in Task Manager?” vs. “How can I see all the programs that are running on my computer?”

Eventually you have to decide which side wins, and Windows has decided to **keep users in control of their own programs and data**, and **keep administrators in control of their own computer**. So users can kill any process they want (given sufficient privileges), they can stop any program from stealing focus, and they can delete any file they want (again, given sufficient privileges). Programs can try to make themselves more difficult to kill (deny PROCESS_TERMINATE access, deny PROCESS_CREATE_THREAD access so people can’t CreateRemoteThread(EndProcess), deny PROCESS_VM_WRITE so people can’t scribble into your stack and make you doublefault, deny PROCESS_SUSPEND_RESUME so they can’t suspend you), but eventually you just can’t stop them from, say, elevating to Debug privilege, debugging your process, and moving EIP to “ExitProcess”. Notice that you can kill CSRSS.EXE and WINLOGON.EXE if you like. Your computer will get very angry at you, but you can do it. (Save you work first!)

Another useful question to ask yourself: “What’s to prevent a virus from doing the same thing?” If there were a way to do these things, then a virus could take advantage of them and make itself invisible to Task Manager, undeletable, and unkillable. Clearly you don’t want

that, do you?

Raymond Chen

**Follow**