Keymaster Solo Help

There's always a balance between security and utility. A line in the sand. Secure systems are unusable if they can't be used. Apple crossed that line long ago.

We can speculate forever as to why Apple did this, but it's pointless. What's necessary, on the other hand, is to make our own systems usable again. Keymaster Solo is an attempt to achieve that goal.

It's nigh on impossible to explain what's going on without getting into technical details and explaining what seems to be behind it all.

So let's just throw it out there, you either deal with it or run away. And then we'll explain what you do to make your Apple system usable again.

Apple's overall plan

Apple's overall plan is to completely co-opt all independent software development on this platform. They want an egregious (obscene) 'piece of the pie' for every software product sold. They want 30%. Plus they want independent software developers to pay them an application fee of $100. And that $100 must be paid every year, or else the products are removed.

The 'spin' is that Apple will make sure you're safe.

Supposedly because there are so many evil 'players' out there. Lurking, as it were, behind every corner.

That's the first lie.

Apple are in collaboration with acknowledged security experts ('hackers') who can find flaws in Apple's code (sometimes lots of them) but these flaws are obscure and rarely if ever pop up on anyone's radar. They normally do not affect any users.

Apple use this equation to engender fear, uncertainty, and doubt - 'FUD'. (FUD is considered a very unethical marketing technique.) Once they have you on the 'FUD' thing, they can move onto 'phase two'.

But let it be pointed out, already at this early stage in the presentation, that Apple's OS X is one of the most secure systems in the world - as things already stand. Apple's OS X is a Unix system, and there are light years between Microsoft's Windows and everything else in the world. And that 'everything else' is mostly Unix. Apple's OS X is a Unix, and thereby eminently safe. And here you have Apple gambling on you not knowing this.

So Apple tell you - and remind you again and again, through ordinary use - that you are insecure, that bad things will happen, and it's only Apple who can protect you. (Yes, this is classic 'protection racket' tactics - are you getting it?)

All this is done to you so that you accept their totalitarian regime on your own computer.

How they do it

People don't have to register with Google to share software on Android. They don't have to pay Google a fee. Google won't be asking for a commission on sales either.

But with Apple?

Apple found it possible to completely close down their mobile platforms from the start. These were new platforms that did not already have a legacy of millions of software products.

But when it comes to their existing computer platforms, Apple couldn't do this. They therefore invented a scheme they call 'Gatekeeper'. Gatekeeper is not a single application, or computer program, or even a single computer process - it's Apple's attempt to virtually accomplish what they've already done on their mobile platforms.

This Gatekeeper system is not without its shortcomings, its flaws, its technical 'holes'.

Apple's goal is to control all access to your computer. Not as a firewall would do, but in a more suspect

manner. Apple's systems want to 'flag' every one of your attempts to download anything, from anywhere, for any reason. They flag these attempts by slapping a so-called 'extended attribute' on the files you download. This extended attribute is Apple's 'quarantine' flag.

At this point in time, nothing much has happened to you or your system. What happens next will happen as soon as you attempt to interact with your download. At this point, Apple's 'launch services' will kick in.

Apple's launch services are a long-standing part of their computer systems that have been retooled for Gatekeeper.

Once Apple's launch services have seen your download, by you attempting to interact with it, by opening it, for example, Apple will place that file into a dedicated 'realm' so it is tracked (and controlled) wherever it goes. And a special set of rules will kick in.

The first and most crucial rule is that your download must be approved by Apple. Apple signify that your download is 'approved' by attaching a cryptographic seal. This is considered unethical by many in the computer science community. Your download will not run on your computer if it's been detected by Apple's launch service and if it doesn't have Apple's

cryptographic seal.

Of course, to obtain this cryptographic seal, independent software developers have to first pay Apple $100 to even be considered, then pass Apple's stringent and oftentimes whimsical tests to be approved. Apple control what software you can run on your own personal property. Apple's criteria include not exposing holes or weaknesses or shortcomings in their own products. If you have a product that is superior to Apple's own, odds are it will not be approved. At the end of the day, Apple will shut out any product they don't like. They have complete control.

Once you interact with your download, Apple's launch services will place it in their Gatekeeper system. Please note that there are a great many standard applications, utilities, and tools that needed to be rewritten to make this happen. For example, Apple's Archive Utility will automatically propagate the 'quarantine' flag to every file it unzips for you so that all of them are put into their Gatekeeper system.

But remember: this is all for your own good! (You do believe that, don't you?)

Apple users see no evil here. They have Apple's App Store icon on their desktop. They just click away and can browse through so many software titles. What they of course do not see is what's happening behind

the scenes.

What you can do about it

It's not exactly practical to rewire Apple's entire system to remove the Gatekeeper constraints. These constraints are a constant pain for developers who find it increasingly difficult to carry out routine operations on their systems. But this not something Apple will worry about - there is simply too much money in it. In broad brush strokes, Apple's increase in annual revenues is measured in the billions - not for their doing anything to make your systems better, but simply for making most users live within their Gatekeeper system - within their 'walled garden'.

The weakness in Apple's diabolical system is in flagging your downloads. If Apple's launch services do not detect the 'quarantine' flag on the files you access, they must of needs assume your files are already resident on your system and thereby approved.

The key, therefore, is to get at your downloads before Apple's Gatekeeper does. And that's where Rixstep's Keymaster comes in.

Rixstep's Keymaster technology (yes all these terms come from the movie 'Ghostbusters') comes in many forms and is the result of significant research (with a number of additional utilities available to registered

users).

The Keymaster applications work in one of two ways up front for you. The one way is to come into action when a download has been detected. The other way is to regularly check your download locations and purge Apple's 'quarantine' flag when found.

For reasons that have to do with a programming error in Apple's own system code, the latter method is used here for Keymaster Solo.

Keymaster Solo

Keymaster Solo is a trimmed-down version of Rixstep's Keymaster application. It will monitor any of your standard 'user area' folders - Applications, Desktop, Documents, Downloads, Library, Movies, Music, Pictures, Public, and Sites. Operations on these folders are recursive. When Keymaster Solo looks at your Library folder, for example, it will look for the 'quarantine' flag in both the Library folder and all its files, as well as in all subfolders and files.

Keymaster Solo will run at regular intervals. Should you detect any lingering quarantine flag in your system, merely stop and start Keymaster Solo again. That should do it.

Please consult Keymaster Solo Documentation on the Help menu for more information.