GateKeeper in Principle

GateKeeper is a program designed to continuously monitor the operation of your Macintosh, watching for operations that are commonly carried out by viruses as they attempt to spread. When GateKeeper detects an infection attempt it will automatically stop it, almost before it's started.

This type of monitoring and protection is possible because viruses generally depend on a small group of operations which they use in somewhat unusual ways. Of course, if detecting virus operations was really as straightforward as all that, everyone would be doing it. The fact is there's a catch. Not a big one, but a catch just the same:

A few perfectly normal programs
carry out some of the same basic operations that viruses do.
(For very different reasons, of course.)

GateKeeper deals with these "false-alarms" by allowing you to tell it what virus-like operations any given program should be *allowed* to carry out. You tell GateKeeper just once, then forget about it – everything's automatic from then on.

GateKeeper restricts two basic *classes* of operations:

1. Operations on information *about* files that contain programs. These are known as "File" operations.

2. Operations on the components of programs stored *within* files. These are known as "Resource" (usually abreviated as just "Res") operations.

Within each class of operation there are three *variants*:

1. The file being operated on is the file containing the currently running program, i.e. the program is operating on itself. This is known as an operation of type "Self."

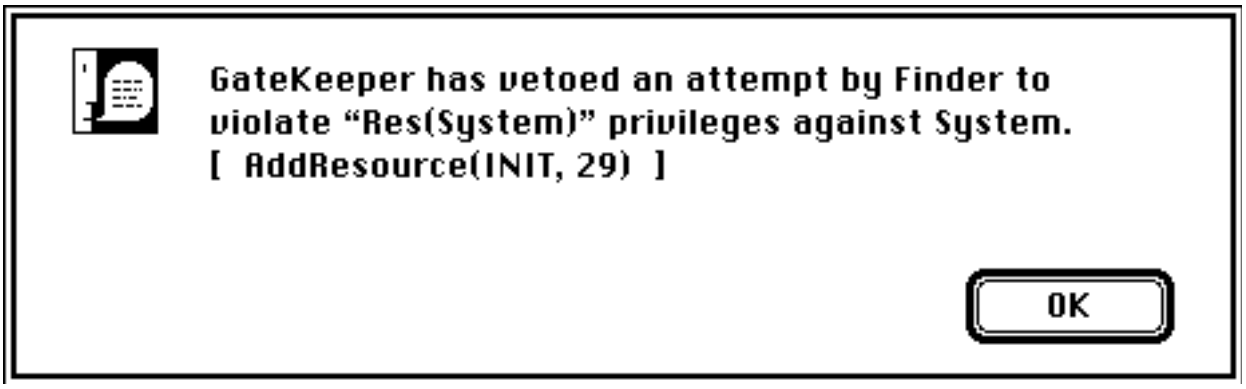
2. The file being operated on is the System file. This is known as an operation of type "System" (usually abreviated as "Sys").

3. The file being operated on is some other file, i.e. the program isn't operating on itself (case 1) and it isn't operating on the System file (case 2), either. This is known as an operation of type "Other."

With these two basic classes of virus operations, each of which has three variants, we see that there are a total of six separate operations that GateKeeper has to watch for.

If this doesn't mean anything to you, don't worry. It's helpful to understand what these different operations do, but it's certainly not required. Just understand that there are two classes of operations monitored by GateKeeper, "File" and "Res," and that there are just three variations within those two classes, "Self," "System" and "Other." You don't have to memorize this, or do anything else of the sort, but you should be aware of it.

GateKeeper in Practice



When push comes to shove, this is GateKeeper. A suspicious operation has been stopped and you’ve been notified of the fact.

This alert tells you what program appears to have been responsible for the suspicious operation (Finder), what privilege the program attempted to violate (Res(System)), and who the intended victim was (the System file). For the technical and the curious, it also includes in brackets the name of the actual ROM operation that was blocked (AddResource) and what it’s immediate intent was (to add a resource of type INIT with an ID number of 29).

In this case the operation being stopped was an attempt by the INIT 29 virus to implant itself in a Macintosh’s System file. But what if you didn’t know about the INIT 29 virus? How would you determine whether or not this was an operation that should have been permitted?

Unfortunately, there’s no perfect method. The first thing to do is check the list of programs known to require privileges in the GateKeeper Release Notes. If the Release Notes don’t help there are a few rules of thumb that take care of most situations, so, when in doubt, ask yourself the following questions:

Does the program modify, create, install, decode, recover or restore applications or system documents? If so, it’ll need some type of File privilege.

- All file manipulation, disk/file backup and recovery software will require File(Other) privileges in order to do restore operations.

  Examples: Finder, DiskFit, Symantec Tools, HFS Recover, MacTools, Scanner, Floppy Recover, HD TuneUp, File Splitter.

- Communications programs and related utilities require File(Other) privileges when decoding downloaded applications and system files.

  Examples: StuffIt, PackIt, BinHex, VersaTerm, MacTerminal, Red Ryder, AppleLink, NCSA Telnet, etc.

Does the program modify, create, install or delete resources that contain programs? If so, it’ll need some type of Res privilege. Some of the most common examples of resources that contain programs are desk accessories, FKEYs, and HyperCard’s XCMDs and XFCNs.

- Installer and Updater applications almost always require Res(Other) and/or Res(System) privileges and are likely to require similar File privileges. However, since these

applications are used infrequently, they shouldn't be granted any privileges. Just place GateKeeper in Override mode (after using your favorite anti-virus disk scanning utility to verify that the items to be installed are free of viruses) while you perform the installation.

Examples: Apple's Installer, PageMaker Installer.

- Resource manipulation utilities generally need Res(Other) privileges and will need Res(System) privileges if they are used to modify the System file. The exact privileges they require will depend on what you use these utilities for.

  Examples: Font/DA Mover, FKey Manager, ResEdit, ResCopier stack, RMaker, Rez.

- Development systems (i.e. programming languages) require File(Other) and Res(Other) privileges in order to build virtually all projects.

  Examples: THINK C, THINK Pascal and Apple's MPW.

- Some Startup Documents (INITs) and Control Panel documents (cdevs) will require Res(Self) privileges while they are loading during system startup. A very few of these items may also need Res(Sys) privileges, but you're encouraged to be suspicious in these situations.

  Examples: Tops, Møire, Clock Adjust, TOM√INT.

- All applications that use the MacinTalk speech synthesis system require Res(Other) privileges. This is silly, but there's nothing I can do about it.

If none of these cases seem to fit your situation, or you're just not sure, check with others who might have relevant knowledge – users group's can be good places to find such people.

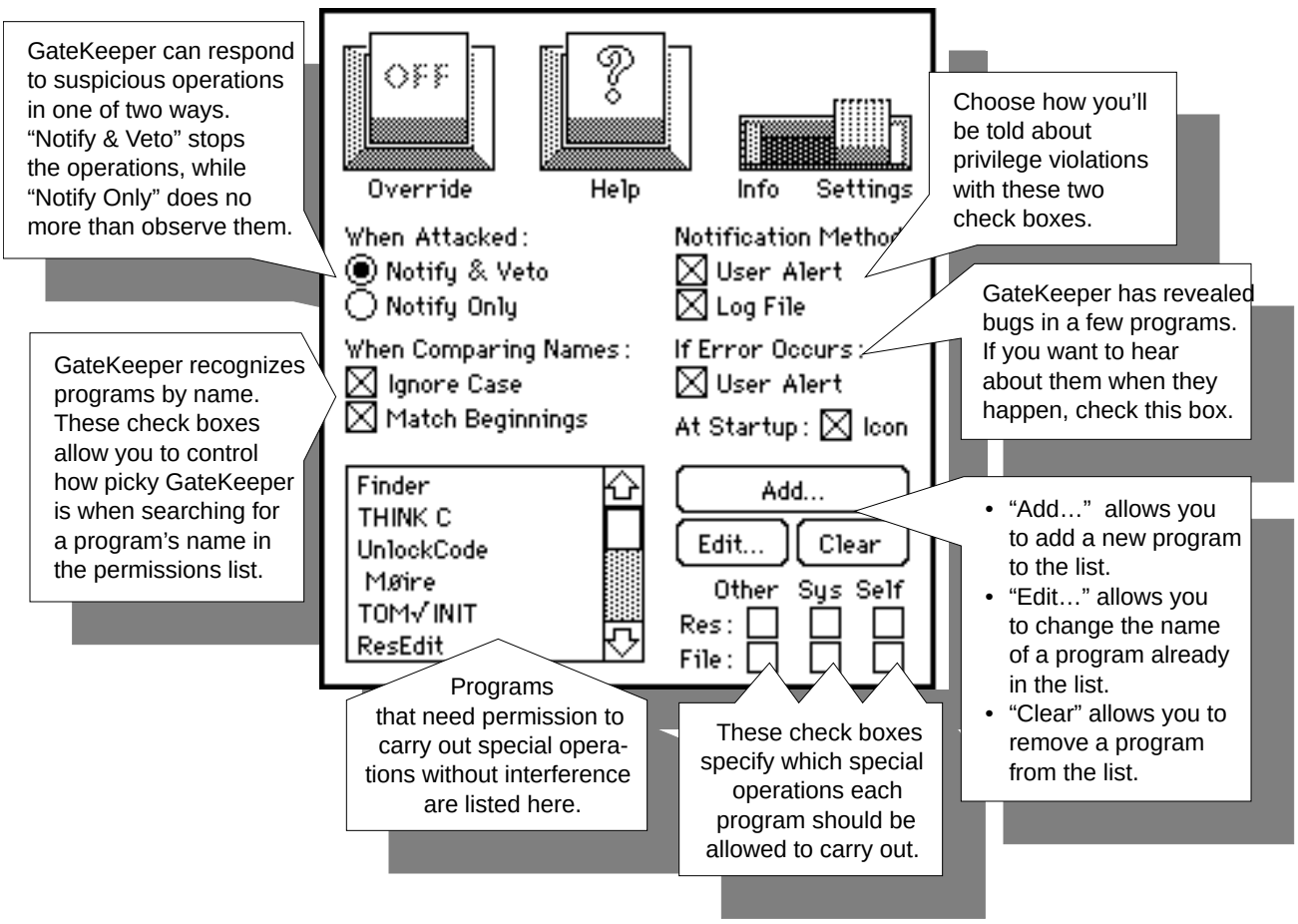
If none of the programs listed in the examples above sound very familiar to you, don't worry: most programs don't need any privileges.

NOTE: There's no way to grant desk accessories privileges, because it's difficult to distinguish between actions initiated by a DA and those initiated by the application the DA is being used within. If you must use a DA that needs privileges, use GateKeeper's Override mode or consider granting the privileges to the program(s) that the DA is most commonly used in. If you are using MultiFinder this program will be DA Handler. Caution should be exercised when considering granting privileges to the program(s) that a DA is used in since doing so entails a risk of opening an otherwise unnecessary door to viruses. This is due to the fact that the program will retain those privileges even when the DA is *not* in use.

Configuring GateKeeper

In order to begin configuring GateKeeper, click on the Info/Settings slide switch next to the Help button. It will slide over into the “Settings” position and a display like the one below will appear.

It is in this display that you define how GateKeeper operates. For example, does it stop suspicious operations, or just monitor them? Does it use alerts to tell you about suspicious operations or merely record them in the log file, or should it do *both*? Furthermore, it lets you answer questions like what programs and startup documents (INITs) should be allowed to carry out suspicious, i.e. virus-like, operations.



Override

If this option is on, GateKeeper provides no protection of any kind. Use this option when you just need to get GateKeeper out of the way for a little while. Just to make sure that GateKeeper is only out of the way for a *little* while, this option will automatically turn itself off after 30 minutes. GateKeeper will then resume normal operation.

Help

(Guess what this does....) GateKeeper includes a thorough on-line help facility which, in many cases, provides more detailed information than this help document. Clicking on this button will display the on-line help text. Click on the Help button again to dismiss the text.

The Privilege (or Permissions) List

This list displays the names of all of the programs that have been granted privileges to carry-out what would normally be considered suspicious (or special) operations. To its side are the controls that allow you to manipulate the privilege list.

Add. Use this button to add a new name to the privilege list. The standard "Open…" dialog box will appear, then you simply choose the program you wish to add to the list.

Edit. Click on this button in order to edit the name currently selected in the privilege list. A simple dialog box will appear in which you'll do the editing.

Clear. Click on this button in order to remove the currently selected name from the privilege list.

Res: Other Sys Self. Use these check boxes to specify which, if any, *resource* privileges any given program should receive.

File: Other Sys Self. Use these check boxes to specify which, if any, *file* privileges any given program should receive.

When Attacked

The "When Attacked" area lets you control how GateKeeper responds to suspicious operations (the term "attack" can be something of a misnomer here).

Notify & Veto. This is the mode in which you'll normally use GateKeeper. In this mode suspicious operations are vetoed before they can complete and you'll be notified in the manner of your choosing.

Notify Only. In this mode GateKeeper provides no protection. You will be notified in the manner of your choosing of any suspicious operations that occur, but the operations *will* take place, for better or for worse.

Notification Method

The "Notification Method" area allows you to specify in what manner GateKeeper will notify you of its actions.

User Alert. If this option is selected, each time a suspicious operation occurs an alert like the one shown at the start of the "GateKeeper in Practice" section will appear to tell you how GateKeeper dealt with the operation.

Note: This option will only be available if you are using System Software version 6.0 or better.

Log File. If this option is selected, a detailed record of each suspicious operation that occurs is written to a text file in your System Folder called "GateKeeper Log." Additional information such as when your system starts-up and shuts-down and when the Override mode is used is also written to the log file.

If Error Occurs

Some ill-behaved programs attempt operations that cause errors to occur within GateKeeper.

User Alerts. If this option is selected an alert will appear when these errors occur.

Note: This option will only be available if you are using System Software version 6.0 or better, *and* you have the *User Alert* option checked in the "Notification Method" area.

If the *Log File* option in the "Notification Method" area is checked, Internal Errors are automatically recorded in the Log File.

When Comparing Names

The “When Comparing Names” area lets you control how strict GateKeeper will be when it looks for a program’s name in the privilege list.

Ignore Case. If this option is selected GateKeeper will *not* distinguish between upper- and lower- case letters. This means that if you’ve granted privileges to a program named, for instance, “Font/DA Mover” but you run a copy of the program named “font/da mover” everything will be OK – GateKeeper will regard them as the same program and will give “font/da mover” the appropriate privileges. If this option were turned off, the names would not have been considered to match and “font/da mover” would not have receieved the privileges it requires.

Match Beginnings. If this option is selected GateKeeper will allow partial matches between names in the privilege list and program names. This means that if you’ve granted privileges to, once again, “Font/DA Mover” but you run a copy of the program named “Font/DA Mover 3.8” everything will be OK because the name in the privilege list was found at the beginning of the copy’s name – the extra characters at the end of the copy’s name (“ 3.8”) are ignored. If this option were turned off, the names would not have been considered to match and that would have been that.

At Startup

Icon. If this option is selected, GateKeeper’s icon will appear at the bottom of the Mac’s screen while the Mac is starting-up. This feature is purely an æsthetic one, and has no effect on the operation of GateKeeper – if you like seeing the GateKeeper icon while your Mac starts-up, select this option; if not, turn it off.