

# Adobe Acrobat™ Security Issues: The Open File Action and File Attachment Annotations

*By Carl Orthlieb, Engineering Manager, Acrobat Desktop*

Adobe Acrobat provides a variety of tools that give authors a rich environment to create hypertext links to pages within a PDF document, to other documents, and even to file types other than PDF. The annotation tools allow you to mark-up, comment on, and add attachments to PDF files. These features were added to Acrobat based on our customers' requirements to create documents that contain multimedia elements such as QuickTime movies or sound files or to create interactive "help" files. Our customers tend to be incredibly creative so we designed the features to be extremely flexible.

Generally, PDF files and the Acrobat viewers<sup>1</sup> are safe to use and are not prone to attacks by viruses. Unfortunately, there are several ways in which a malicious individual might create a PDF file that could cause mischief on the recipient's machine. Most of these cases fall into two classes: those using the Open File action and those using File Attachments.

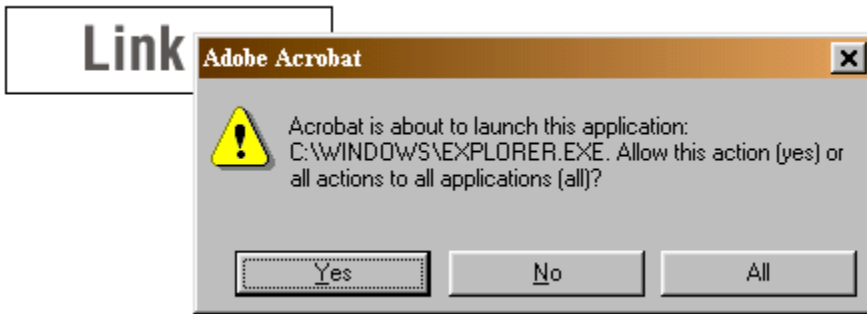
## Open File Actions:

Open File actions allow the author of the document to "launch" or invoke an external application on the user's machine. An Open File action can be attached to a bookmark, a link, a form field, or even to Page Open or Page Close events. This feature was designed for CD ROM publishers who want to include links to simulations and other example programs. Unscrupulous authors could create an Open File action that accesses a malicious executable that erases the users hard drive, sends system information to a web site, or any other detrimental action. It is necessary, however, that the end user's machine already have such a program installed **and** that it be in a known location. Most virus protection software will prevent rogue executables from installing on a user's system. It is unlikely that this will occur if a user's system is properly protected with a virus scanner.

There are, of course, safeguards built into Acrobat. Before opening an external file, Acrobat will display a warning dialog:

---

<sup>1</sup> Adobe Acrobat Reader and Adobe Acrobat 3.0 and 4.0

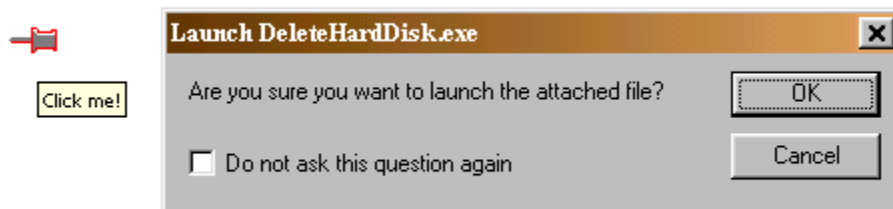


If the user clicks “Yes” then the launch will occur. If the user clicks “No” the application will not be run, if the user clicks “All” then the launch will occur and the warning dialog will never appear again for this application session.

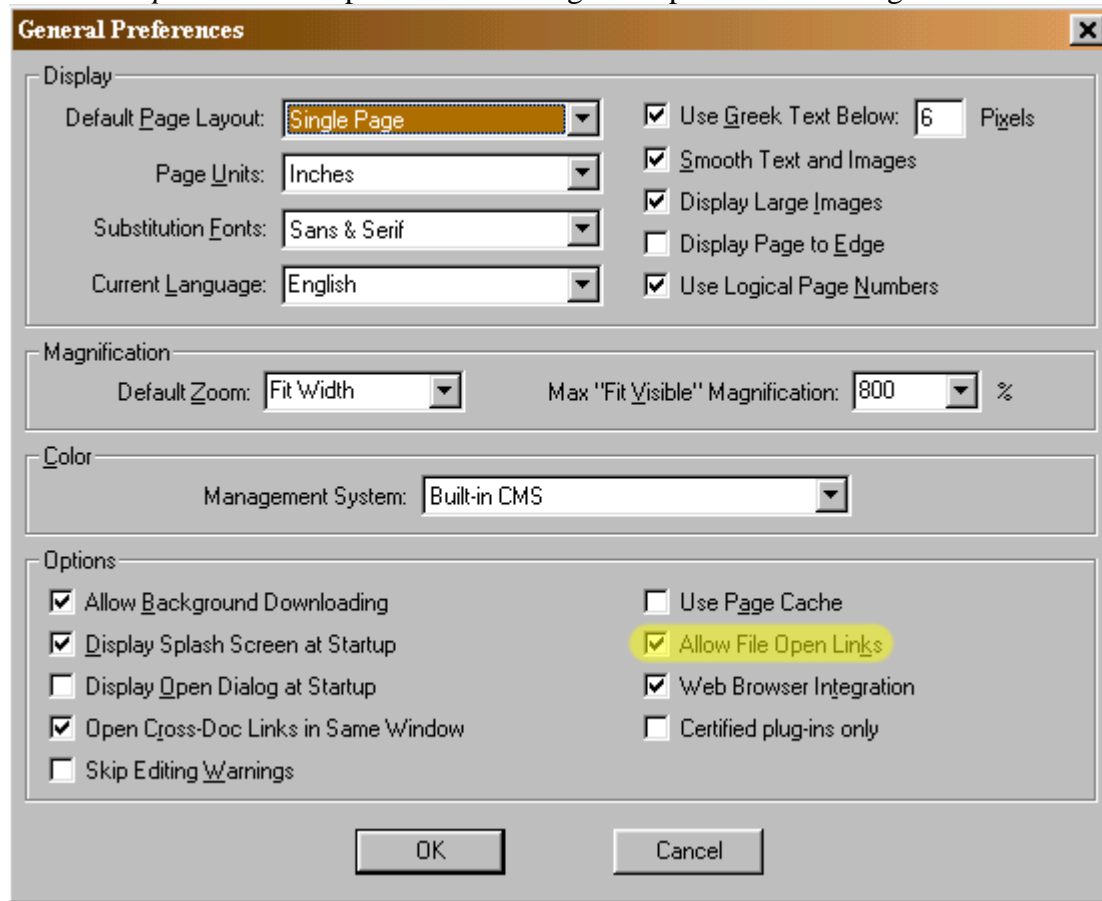
## File Attachments:

File attachments are actually files embedded within the PDF file, similar to attachments in email messages. File attachments are normally used during the authoring or mark-up and review process to attach auxiliary files to a PDF and package them up with the PDF for easy distribution. Just like email, rogue executables can be file attachments, which can make them potentially more dangerous than Open File actions.

Again, there are safeguards; before extracting and launching a file attachment, Acrobat displays the dialog shown below. If the user selects “OK” the application or file will open. If the user checks the box to “Do not ask this question again”, the warning will not be displayed until the preference to *Allow Open File Links* is reset (see below).



The user can also prevent both launch actions and file attachments from working by unchecking the *Allow Open File Links* preference in the general preferences dialog.



## ***System Administrator and IS Manager Options***

The Acrobat installer, on the Windows platform, is configurable. A system administrator or IS manager can customize the installer to have the *Allow File Open Links* preference turned off by default by modifying the ABCPY.ini file in the installer package.

```
Group1RegEntry1ParentKey=HKEY_CURRENT_USER
Group1RegEntry1Key=SOFTWARE\Adobe\Adobe Acrobat\4.0\AdobeViewer
Group1RegEntry1ValueName=AllowOpenFile
Group1RegEntry1ValueType=NUMBER
Group1RegEntry1ValueData=0
```

This still allows the naïve user to go into the General Preferences and remove the protection put in place by checking the *Allow File Open Links* check box.

For even greater security there is a hidden preference that makes this even more difficult to turn off:

```
Group1RegEntry1ParentKey=HKEY_CURRENT_USER  
Group1RegEntry1Key=SOFTWARE\Adobe\Adobe Acrobat\4.0\AdobeViewer  
Group1RegEntry1ValueName=SecureOpenFile  
Group1RegEntry1ValueType=NUMBER  
Group1RegEntry1ValueData=1
```

This registry entry overrides the user preference, even if the *Allow Open File Links* is checked, the user cannot launch external applications or open file attachments. However, a savvy user that has permission to edit the registry can remove the registry entry.

## **Conclusion**

The rich feature set of Acrobat allows authors an open and flexible tool to create documents that fit their specific needs. Unfortunately, this opens a door in which a malicious individual can create PDF files that may damage a recipient's computing environment. Acrobat displays a warning dialog to the user whenever an application is about to be launched. A user could, either through confusion, impatience, or inattention, dismiss this dialog and execute the offending application. A system administrator can pre-configure the installer to make the launch action or file attachment annotation effectively harmless.