Using FileOpen to Prevent Pass-Along of Emailed Documents

We frequently get requests from prospective licensees who ask if we can "prevent this document from being downloaded" or to "stop this document from being forwarded." These requests speak to the ongoing prevalence of email as a document distribution platform, and the relative ease with which unencrypted email attachments can be forwarded, saved locally, or uploaded to a third party site.

However, in the context of a rights-management application, when we talk about "preventing download" we can't literally mean "don't let the user download the file," because that's equivalent to "don't let the user view this file" -- all files that are displayed on a local computer have, necessarily, already been downloaded. Today's browsers and operating systems work that way: they download files to a local directory, or "cache", and then display the content from there. (It is possible to remove files from the cache once they have been displayed, and in fact the FileOpen client does this, but that is not the same as never downloading the file at all.)

So when we talk about "preventing download" what we really mean is "prevent the user from getting a usable copy of the file." What matters is not whether the user is able to download the file, but what the user can do with the file once it has been downloaded. Can it be opened? Can it be modified? Can it be opened by other users?

Likewise when we talk about "prevent forwarding" we can't literally mean "stop this user from right-clicking the email and selecting the option forward," because in order to do that we'd need to control that user's email application, and there are far too many email clients, on too many platforms, to be effectively controlled by any vendor. So what we mean has to be something like "if the user forwards this message, don't let the recipient open the attachment," or possibly "if the user forwards this message keep a record of who else opened the attachment." These, again, are actions that the FileOpen software can and does control.

The FileOpen Approach

A document owner using FileOpen's DRM tools typically begins by using the FileOpen Encryptor to batch-encrypt a set of documents, either locally on their desktop or on a server within their company's firewall. Local encryption is an important part of the FileOpen design: we don't think that unencrypted documents should leave the owner's

network, so we don't expect those files to be uploaded to our server. During the encryption process a set of identifiers and other metadata is generated for each file, and that metadata is uploaded to a server separately from the documents. If the FileOpen RightsManager™ solution is being used, the meta data is stored on FileOpen permissioning servers; if the document owner has licensed the FileOpen RightsServer™, the meta data is stored on the licensee's Web server.

The document owner now has a set of encrypted documents. With the RightsManager user interface, the owner can proceed to defining her list of authorized users (which can be email addresses), and the permission settings associated with those users. The document owner can impose a simple permission scheme if the access controls for all documents should be the same for all documents, or exercise a great deal of flexibility by organizing groups of users and documents with unique policies. For example you could create a Group that makes all Documents in it expire after six months, or after three views, etc.

Now it is time to deliver the secured documents to the authorized users, which may be delivered to the end user by any means (email, Web, CD-ROM, USB, etc.). In order for a user to open one of those documents, two additional elements are required: the user must have a copy of a supported viewing application, e.g. Adobe Reader or MSOffice, with the appropriate FileOpen plug-in or Add-in installed, and the user must obtain the permission of the document owner. The document owner can pre-authorize their users by sending them a customized registration document, which registers their device when it is launched. A user can also be authorized by providing their existing credentials to the owner's site (as a one-time requirement).

Pass-along, Prevented

So we can now revisit the preventing "download/forwarding" –what happens when an authorized user takes it upon himself to save a local copy of the document and then forward it to a friend using email or other means? The copy of the document shared by the user retains its encryption, so the unauthorized recipient will not be recognized by the server as an authorized user, and the device of that user will not be registered, so that request would be denied.

In the FileOpen design, the User's permissions to the document do not reside in the file. The permissions are obtained from the document owner's server in real-time, and are specific to that User's device. Permissions are not portable in any way that the user can control. There are ways in which an authorized User can request access from the document owner for additional Devices, but again these permissions can be explicitly granted only by the owner, and permissions will be locked to those devices as well.

Portability by Design

Any attempt to control the actual redistribution of documents in standard formats would be futile (after all, the "P" in PDF stands for "Portable." Fortunately, standard viewers such as Adobe Reader have been architected with security in mind, such that the FileOpen plug-in can control every aspect of whether a document can be viewed, for how long, etc. The primary goal, therefore, in protecting PDF or MSOffice files, is to exercise control over when and where and how the files are opened, not over how they are distributed. The core advantage of PDF is precisely that the files can be shipped around by many means to many destinations, retaining their integrity, like lockable containers for information. The encryption on the files ensures that they remain locked in transit, and the FileOpen client/server interaction ensures that the files are opened only by the authorized recipient.

That said, there are some business cases where allowing even the authorized user to obtain a copy of a file is not desirable, even if that file is encrypted and can only be opened with permission from the owner. With that in mind, we have developed the FileOpen WebViewer and the OPN document format on the assumption that files should not be portable, or downloadable, or usable out of the original context. In this scenario, document owners can email links to the location of an OPN file on their web site, where it can be viewed but not accessed locally. For more information on the FileOpen Viewer and OPN format, please visit http://www.fileopen.com/