= =

Protected eBooks for Dummies

By William Kent

= =

William, being the founder of what we know as copy protection for use on the Internet, is undoubtedly the most informed authority on copy protection and DRM solutions. Having been there to witness the advent of every new scheme and its eventual demise, and the fateful endings of new startups trying to cash in on DRM hype…

Ken Douglas (Addmine Reviews)

Introduction

Writing eBooks, whether for fiction, documentation or for tutorials can be intensive work and as a living, the author needs to be paid to survive… to live another day and publish more. So forwarding to others to use for free is robbing the author of his livelihood, and a despicable practice that needs to be kept in check.

Piracy of media is a most popular hobby and in some countries it's a national pastime where the public can openly shop and purchase pirated music, books and software. The penalties for such piracy, even in countries where Copyright has been reformed, are not a strong enough deterrent and thanks to the public thirst for whatever can be obtained for free, copy protection can seem like a futile battle.

For authors an alternative is to distribute eBooks that can be opened and read only by those who pay for the privilege, providing samples prior to purchase and then delivering the complete book only after payment. While this might sound a viable solution, it doesn't prevent anyone from forwarding a copy of their eBook to others, and at worse, an author's first sale could end up being mass distributed via a share network.

Restricting access to use digital media, is often referred to as "digital rights management" (DRM) where a method is used to restrict or limit the use of digital media which can include inbuilt mechanisms to check its surrounding environment before allowing a user access to its content. DRM can be applied to a vast variety of digital products including both software and hardware, however the main topic of interest for this article is "eBooks".

At this point it should be noted that the document protection discussed in this article is orientated towards secure protection that doesn't leave gaping security holes as a result of making compromises to protect from anything but the majority of Internet users.

For example, why we haven't chosen ePub or other common e-reader formats is because they cannot be protected in any way that can remain secure. If you want to publish for portable readers and tablets, forget about reading the rest of this document because the e-reader merchandise being peddled today is intended to be appealing but no consideration has been given to protect the media it displays. In fact all that can be guaranteed will be a high sales turnover as they are improved and replaced to overcome their shortcomings, most of which are related to the very design features that make them popular. Even LCD screens generate heat and the ongoing drain of batteries, especially those of high power to limited mass ratios, will have very short life cycle… nice to touch and feel maybe, but eventually useless and a chore to keep powered.

Nor are the solutions discussed here intended for use on any iPad, iPhone, iToys, iGadgets, PlayStation, X-Box or any other device intended for amusement only, and you can include Mac computers in that list. 95% of all internet users are using Windows and why the remaining 5% want to be difficult, different, rebellious or stray sheep should not be an author's worry at all, so concentrate on more important issues like good content.

Copy Protection Requirements

Encryption

Encryption is the first and foremost consideration because it is encryption that provides the core for protection of a document. If your document is provided in it's original format (editable text) then you cannot prevent access However if it's encrypted then they will not be able to access its content without a key to decrypt (unlock) it.

A decryption key is the secret phrase that holds the key to an encryption, without which a document cannot be decrypted and opened.

Encryption Strength

There is a trend to promote security applications by citing encryption processes of high reputation as a guarantee that they will be most secure. However there are many different types of encryption processes that will provide protection secure from the most powerful intelligence resources in the world today, providing that they are cleverly deployed. As for most of what is claimed to be secure, the end user and especially the novice has no means to verify anything, leaving software vendors to get away with pretence when in fact what they are really doing is exposing the first clue of where a hacker should begin. It really doesn't matter what encryption process is used if either the document or the reader can be easily pulled apart to extract their secrets and decryption key. Yes it is possible to use secure encryption that would not be decrypted without using all of the computers at NASA for such a time that the cost would far exceed the value of what can be attained by at least a hundredfold, and that's what this article is about… the solutions that are most effective.

Password Protection

Password protection is like a decryption key, because it is the pass phrase used for unlocking an encrypted document, however it may not be the decryption key itself, because a document can be unlocked to provide access for reading, however it may not necessarily enable access to the original text version for extraction of any parts or whole.

Read Only Document

Providing a read only view without providing the original text in such a form that can be easily copied is the aim of most document protection applications, and their varying degrees of success is directly attributable to two (2) things, which is the format of the document file and the reader which is used to open and display the document's contents.

Generic Readers

A generic reader is one designed to be as user friendly as possible, supported on as many different types of computers as possible and able to open and display common document formats. A typical example for eBooks is one that can open a variety of eBook formats.

General eBook Formats

Although there are quite a few different eBook file formats, they generally all have one thing in common, and that is that they manage to be portable and accessible by a large variety of readers because they are all basically simple text, and while there may have been some form of protection in place such as encryption requiring a key to open them, the unlock key can be found inside the document file.

Removing DRM from eBooks

One only needs to perform a web search on the topic of “remove DRM from eBook” to realize how superficial most document protection can be. Password protection and expiration are commonly used options, and for most uninformed authors those measures may remain to be adequate until the document really does become of interest. For anyone who really wants to extract the original content of these documents it couldn’t be easier, and if anyone doesn’t know how, all they have to do is look up “how” on the Internet.

Proprietary Readers

A proprietary reader is one that is not open source but specially designed to open special file types demarked as encrypted files. Ideally it will be one that cannot be decompiled to extract its secret encryption algorithms or the keys to work them.

Secure Readers

Similar to a proprietary reader, a secure reader will be specially designed throughout to open and preserve the integrity of specially encrypted document files which have been designed forward of a hacker’s mentality and how secure such a reader remains is how far forward its designer planned ahead and anticipated the resources available for exploitation, because it’s not so much the intelligence of a hacker that one has to worry about, but rather the collection of resources available to them.

Expiry Date Protection

Setting a date for a document to expire, after which it cannot be opened, is another method of preventing access and limiting redistribution because after that date the document will become unusable. So an author can regularly publish documents set to expire in a short period of time, thus limiting the number of potential threats. However expiry dates can be exploited quite easily where the date check relies on dates retrieved from the local computer (the user’s computer) because that clock can be turned back.

Time Server Checks

Where possible a much more secure solution for expiry date validation is using an independent time resource, such as an online timeserver, thus preventing a user from exploiting any document that has expired.

Copy Protection

Copy protection usually refers to the prevention of document copy by saving or copying the contents of a document while it is open. There are today many more references to "copy protection" in relation to disk and file copy prevention which are just too fanciful because nothing can prevent anyone from duplicating a file stored on disk. Preventing file copy is impossible, however it is possible to prevent the use of copies that have been forwarded to others, and that's by using DRM, which we have already introduced and will elaborate more on later.

Copy Techniques

The techniques (methods) available for copying the contents of a document while it is open are numerous. First you have the obvious technique of saving a copy of the document (save file as), then you can highlight text and by right mouse clicking for "Copy" and then "Paste" to place a copy into a document editor, or you can simply highlight and then mouse drag content such as text, images and other media to the desktop. Or if you know what the Printscreen button does, then you can click it to take a screen shot of the desktop (a view of what's on your screen) to paste into an image editor like Paint (which is installed on every Windows computer by default). If you don't know that you can do that using Printscreen and were stupid enough to pay for software to do the same thing, then you can use your "screen capture" software.

Remote Copying

These days there are applications that enable one to install a second operating system on the same computer. VMWare is popular on Windows and Parallels is commonly used on Mac computers to provide a "virtual" partition enabling one to install an operating system separate to the main OS. For example one can install Windows on a Mac, or install different versions of Windows, but as Apple would have it, the Mac operating system can only installed on an Apple computer. How remote computers are a problem for copy protection is that they can provide a view of protected content that is being displayed on another computer (albeit a virtual computer) and while that content may be copy protected on the computer displaying the content, whatever is protecting that content will not be running on the virtual computer thus enabling the capacity for screen shots to be taken from the virtual.

Printing Restrictions

Preventing copy by printing a document and the limitation of the number of copies printed (limiting print copies) is possible by a properly designed secure reader, however it cannot be maintained by local software alone. The reader software installed on a user's computer can either allow or disallow printing, but it cannot limit the number of copies in any way that cannot be exploited without integration with an online service. To limit the number of copies per user or document requires use of an online database that can record the usage and administer permission to print when still permitted… DRM control.

View Restrictions

It is not possible for reader software to do any more on its own that either allows or disallows access to view the contents of a document. To count the number of views of a document by a user and prevent further usage after a preset limit has been reached is possible but only by the integration with a DRM control, which independently monitors, records and administrates a user's permission to do so.

Access Rights

The rights, privileges or permissions to open a document and how that document can be used are known as "access rights". Simple readers can provide basic access rights such as whether you can open the document or not, which is governed by password or expiration control. Secure readers that support DRM can provide more control options.

Document Rights Management (DRM)

Some call it digital rights management, but for this article let's be more precise and call it document rights management because the guys at Wikipedia have compiled their definitions from research. Having not been there at the time they have to rely on hearsay, most of which was fabricated after the fact to support claims for ownership of patents and innovations. For example, while Wikipedia maintains that DRM has a long history, it is only in limited areas such as software protection that there was anything like DRM and at that time it was not known as DRM at all. The term "DRM" was coined very much later by wordsmiths and copywriters for advertising companies to promote new startups in the copy protection industry. Following the innovations of ArtistScope and their introduction of copy protection for web content, something that had always been deemed impossible, a wave of new companies and products emerged, funded by entrepreneurs milking the public share market.

The DRM Front

For some time DRM providers have preferred to use techniques that are less obvious to their end-users which has resulted in poor performance when it comes to protecting media. DRM has been a new buzz word in the arts industry and while artists need and demand the right to protect their livelihood, they are grossly outnumbered by the public and malovents who wish to undermine those rights, demanding that they have the right to use and abuse the intellectual property of others, an attitude that is no more than selfish greed and one that will, if left unchecked, eventually result in there being no entertainment at all, at least none of any quality because it costs money to produce quality media and artists need to make a living.

DRM and Opposition

As already mentioned, DRM is not popular but one can rest assured that while it may be the artists that are painted as the criminals, the noise comes mostly from a much smaller group than what the trouble they cause might appear. As the author and owner of intellectual property it is you who has the right to decide how your product is delivered and by what terms, just as it is the right of the end-user to reject those terms by not using your product. Having agreed to your terms which you clearly define and the end-user having agreed to those terms prior to purchasing your document and again later prior to installing or opening the document, is in breach of contract by trying to remove your DRM or assist in the removal of your DRM by merely providing moral support to those who attempt to do so. Yet these malovents repeatedly agree to terms of use solely for the purpose and with the intent of breaching legal agreements that they made with authors, and these malovents have the audacity to assume that they have the right to do so. In the railway and outdoor advertising industries there are problem groups, some known as BUGUP which represent not a group but a mental state… bugger up (vandalize) anything and everything even at the cost of their own environment.

DRM and an Author's Rights

When one sells an item there is an agreement about the price. When one rents a property there is an agreement about the price and further terms come into the deal, such as how often rental payments are made and for how long the tenant has a right to use the property before re-evaluating the situation. Likewise an author has the right to determine how his property can be used, especially where conditions are in place by necessity because the end-user may not have respect for the International laws that already protect his intellectual property. If we could rely on the integrity of the shopper and end-user we wouldn't need storefronts, burglar alarms or the many police personnel who are mostly occupied with investigating thefts, burglary and fraud. Let's face it there are no honest people in this world because they will all cheat if (a) they know how, and (b) are confident about getting away with it. If you find this a hard pill to swallow, realize that the most popular software available today are programs for downloading pirated media, capturing online media and removing protection from media.

DRM Line of Defense

Choosing the right document protection solution can be an erroneous chore, especially when confronted by so many choices. For example if you perform a web search on “how to protect eBooks” you will be inundated by a variety of choices ranging from ‘sell your eBook through us so that we can make commission” to “pay for this program and end your unauthorized distribution worries”. Unfortunately, while there are a multitude of options provided by wanna-be speculators trying to cash in on eBook hype, not many of them will provide what you need. For example while a lot of them claim to be able to copy protect, what they are really talking about is password protection, which is not copy protection at all because while the document is open, it is exposed to numerous methods for copy and saving of both images and text.

Old DRM Techniques

DRM can be managed offline or online. DRM software makers desperate to be popular with their end users will prefer to provide solutions that can be used offline, without being connected to the Internet. Unfortunately having all components on the end-user’s computer exposes them to exploitation, and without any chance of recovery. Such techniques utilize registry keys and license files to store information pertinent to the user that can be checked and validated to ensure that the user has usage rights. Solutions that provide a license file from the point of purchase may not be creating a unique computer signature for the computer intended for use, which means that the whole solution including nay protected documents will be transferable for use by others.

New DRM Techniques

ArtistScope revolutionized document rights by looking at the security holes and then devising a solution that cannot be exploited. By utilizing machine locking, their DRM is not only most secure, but it also enables an author to have total control over user privileges and document permissions. Using ArtistScope DRM an author can change a user’s rights of access to a document or a document’s properties in relation to expiration and print limits with immediate effect even after that document has already been downloaded to the end-user’s computer. Other providers claimed that such a thing was impossible and in a fraudulent claim. The fact that the others in the industry took two (2) years to plagiarize and create similar solutions bears witness to the fact that most copy protection providers today are in fact IP thieves (intellectual property thieves) incapable of creating or innovating anything that hasn’t already been researched, developed and spelled out for them.

The Remedy

Ok, you are an author and you want to sell eBooks, but you also want to control just who can use those eBooks to ensure that you get paid and earn a living.

Possible Solutions

You need to be able to create the document, convert it to eBook, apply copy protection and DRM control, advertise online and take orders paid by credit card, and then manage your subscriptions.

1. Creating the document original

Here you can use almost any text editor at your disposal. You can use Notepad, Wordpad or Ms Word that comes with Microsoft Office. You can even create your pages as html by using a web page editor. In fact it doesn't matter what format your original is so long as you have the means to convert it to PDF. If you have Adobe Acrobat you can convert documents to PDF directly from MS Word. If you have another PDF conversion utility by all means use that one, however be warned that some editors like Open-Office can produce documents that when converted to PDF are not ideal, and by the time they have been encrypted for use as an eBook they can be totally illegible. So before commencing what can be a time consuming task (writing a book) perform some simple tests with the tools that you have to ensure that quality is maintained throughout the process.

2. Converting to PDF

PDF is chosen as the common file format because most document types can be converted to PDF and there is a multitude of tools available for PDF conversion. There is software for PDF conversions, and there are plugins to convert to PDF from most Microsoft applications and there are printer drivers. There is software available for free and there are also online services that provide free PDF conversions as demonstrations of their product that will convert your uploaded file and deliver it by email.

3. Protecting your eBook

The most secure solution for eBooks and PDF is undoubtedly the CopySafe PDF Protector because it not only provides the most robust and most secure copy protection from all methods of copy and save including Printscreen and screen capture, but it also provides the most secure DRM options as we have already discussed. The Protector can be downloaded and installed as a free trial, and the files that it protects can be uploaded to a DRM Portal for management of user privileges.

ArtistScope, the makers of CopySafe PDF, provide online DRM validation services for their users, and they also provide an Online eBook Store which provides everything from eBook protection to sales and distribution management..

4. Advertising your eBook

How you advertise your eBook is up to you and the options are unlimited. You can advertise and promote your eBook by placing ads online, getting reviews in the news and on online book review sites. However having a web presence is not only recommended, it is mandatory to provide a reference point for more information and purchase links.

Regardless of how you do advertise your prospective buyer needs to be able to find out more about the book, perhaps read an excerpt or summary and get an idea about what it's really about before deciding to purchase. Seeing a photo of a book cover, especially one designed to reflect the theme of the book, is a big plus. From that same page having a purchase link or button linking to an online order form is most recommended, because then there is no confusion and the treasure hunt is over… if they want to purchase they simply click on the "Buy" button and get on with it.

5. Processing sales from credit cards

There are quite a lot of eBook stores providing e-commerce services to facilitate sales, and some are just that, a credit card processing service that will charge commission to use their service per sale made. There are also many sites that provide shopping carts to list your product and process sales, and they too will charge commission for sales and most will also charge a fee to list your eBook in their shopping cart.

If you have your own web site you can easily do all of this yourself by establishing an account with PayPal and providing a link to a PayPal order form. Having been providing online credit card sales for longer than most, PayPal is a reliable and most sophisticated service that provides everything you need including sales records and the means to transfer your monies from PayPal to a bank account of your choice. If you are handy with web scripting you can also get your customers to return after a successful sale and record the sale for your own records.

Of course most sites providing shopping carts and sales services for eBooks will also be able to provide the sales records that you need. However there is one area in which most of these services are lacking and that's in the "after sales management" of your protected eBook. Sure there is some who claim to protect your eBook until delivered, but their solutions are simple and offer little protection beyond providing downloads for a limited time. Other than that they generally offer no copy protection of the document after delivery or any rights management to prevent forwarding to others.

6. Managing document delivery and user rights

A simple eBook sales service will send the purchaser an email with a download link. That download link might e monitored as far as tracking who uses it and from which IP (internet address) and it may expire in 48 hours after which the download will no longer be available. Now if you have read through this document and not skipped any parts, but still think that a simple download service is going to provide protection for your eBook, you had better start again.

The Ideal Solution

The ideal solution will be one that provides everything that you need, and one that provides everything that we have discussed, plus proper protection for your eBook. There is only one solution that fits this bill and it is a special all-in-one service designed by creative minds for creative people… and it's FREE!

The ArtistScope eBook Store

The ArtistScope eBook Store is the only service that provides everything that an eBook author needs to sell and distribute protected eBooks.

- ***Upload PDF and convert to eBook online***
- ***Create an advertising page and summary for each eBook***
- ***Upload an image to use for thumbnail and book cover art***
- ***Accept and process online orders that are commission free***
- ***Manage delivery of sold eBooks to purchasers***
- ***Keep in touch about updates and new editions by newsletter***
- ***Manage subscriptions and user rights to access your eBooks***
- ***Manage eBook properties and permissions***
- ***Monitor usage and statistics by user and eBook***

All of this is FREE to any author using CopySafe PDF to protect their eBooks.

Sponsorship for Authors

First time authors embarking on a new career as an author or simply testing the water may be entitled to sponsorship and assistance from ArtistScope. This sponsorship includes everything the author needs including a free account to use the ArtistScope DRM Portal thus qualifying an author as a CopySafe PDF user for a free listing in the online catalogue. More info can be found online at http://www.artistscope.com.au/shop/