10 things you really wished you had known about PDF Security, but they didn't tell you!

Is the PDF security software you are looking to purchase really secure? If the PDF security software you are evaluating can be simply broken then you might as well save your money. What PDF security vendors are not telling you about their products and solutions, and what questions you should be asking.

Think carefully about the tool that is used to render your PDF to the screen. Are there published cracks for it, or is the implementation insecure?

All PDF password protected documents can have their passwords removed by PDF password recovery software. Once the password has been removed the user can do what they like with the PDF document. Password removal or 'recovery' programs are freely available on the Internet and cost as little as $10 to purchase.

If you type in "PDF password remover" in Google it returns 825,000 results. Top of the list is http://www.a-pdf.com/security/restrictions_remover.htm which charges $9.99 and offers to remove the password and restrictions in a few seconds.

Go and check that password recovery expert companies like Elcomsoft don't list the program you are rendering in their 'password recovery' list. Basically it means that they have found a way in, and for a small fee, so can anyone else. So if you are protecting a $6k bucks file and the crack costs $50 then you figure it out for yourself.

Don't be fooled by companies that have been around for a while or are affiliated with big names. Dimitry Sklyarov, a cryptanalyst from Elcomsoft says:

"FileOpen was chosen as an Adobe 'security partner', which leads me to wonder how closely Adobe examines the cryptography used by its partners. The code can be broken instantly. FileOpen software, puts key information in the encrypted document, which is sort of like leaving your car with the keys in the ignition. Surprisingly, many of it's users seem to be scientific and technical journals."

"The $197 Ebook Pro e-book protection software is advertised as *100% burglarproof* and claims a list of Fortune 500 companies as its customers. The software "encrypts" e-books by mixing each byte of the text with a constant byte. This is a technique so weak that it probably shouldn't even be called cryptography."

The latest information on poor PDF security implementations and PDF flaws can be found here.

Does your PDF security supplier have a background in content security or are you purchasing from a one man band or affiliate scheme?

A lot of companies out there claim their products are secure yet use weak encryption or don't publish their security mechanisms. The majority have no data or content security experience. A lot of ebook 'security' software on the market is affiliate software that is re-branded for different organizations to sell as their own. If the company you are considering does not demonstrate any security credentials, then ask yourself whether you can really be certain that your content will be kept secure - you might want to look elsewhere.

Be careful about arguments that plug-ins are a lot safer than executable programs.

Because a plug-in inherits all the power and authority of the program it is loaded into, then you have to be just as confident about the provenance of the plug-in as you do about an executable. But your testing could be a whole lot harder because you can't evaluate a plug-in unless you load it into its host program and then you don't know if you are observing the actions of the plug-in or the host.

Make sure that people absolutely cannot load their own plug-ins into the master program. Because if they can, then they can get around the security that is being applied. Plug-ins run on the honor system. But, unfortunately, it seems that whilst people love honor, they love money more.

Plug-ins are exe files that need Windows administration rights to install. There are therefore no benefits of using plug-ins against standalone viewers - only disadvantages.

Plug-ins can also conflict with each other. There is no verification system in the host program that sorts out conflicts and reports lack of interoperability. Even Microsoft Windows does a better job of identifying ahead of time when systems simply won't 'plug and play' than the plug-in system. The approach to plug-ins is load and go. And it is down to the person installing the plug-in to sort out if there are any conflicts between the plug-ins they already have and the new one they are trying to introduce.

Read more information on PDF Security plug-in vulnerabilites here.

Zero footprint solutions (no plug-ins or downloads).

Anyone claiming to offer a zero footprint PDF security solution (no software to download) is selling you snake oil.

If no plug-in or standalone viewer is required then what you are getting is PDF password protection. The decryption key MUST be sent in the protected file, and therefore is easily compromized by the standard PDF password removal software freely available on the Internet. PDF editing software can then remove what is left of the 'protection'.

Apart from being easily compromized, the weakness of zero footprint solutions is that they cannot control print screen, printing controls, virtual environments, and so on because they have nothing to do it with. Also, they cannot verify if they are running properly, compromized by a plug-in to Acrobat, or control dates/times, numbers of views, prints, and so on.

Companies selling zero footprint solutions often quote the DMCA (Digital Millennium Copyright Act) for protection of your PDF documents (telling your users they must not remove the security) but that is not offering you any real protection at all. You might want to ask yourself why you would pay more for something that offers you no additional protection to the PDF password security that comes as standard with your PDF creation and editing software.

Does your PDF Security provider force you to use technology that puts users computers at risk?

If the PDF security solution you choose uses technology such as javascript to mask pages or provide communication with a licensing server then you might want to consider the legal implications very carefully.

Adobe for example recommend that you disable javascript in Adobe Reader due to the fact that it is unsafe - it is regularly used by hackers to gain access to computers. Other major security companies are telling companies to stop using Adode Reader all together. More information on these vulnerabilities can be found at PDF security flaws.

If the technology you use therefore forces users to use unsafe methods that expose their computers to risk, where does the responsibility lie if compromize occurs?

If you decide to allow printing, make sure that your PDF security system can make sure the printing is to a real printer.

There are any number of printer drivers (including those supplied by Microsoft) that can transfer a printout to a file, or, even better, a PDF file directly. If your PDF security solution can't spot a real printer from a fake then you have a problem.

7 Be aware that there are systems and services that, for operational reasons, are perfectly valid, but they act in a way that can compromise DRM controls.

Facilities like Citrix or Windows Terminal Server allow the implementation of a license on a single PC to be replicated across an entire installation. So a company can purchase just one copy of your protected document (ebook, report, etc.) and use it on every computer in their organization. Make sure you check if the DRM supplier can control these environments, because if they can't then you do not have the DRM control that you first thought.

8 Have you looked into watermarking capabilities as a way of both establishing your ownership or a means of identifying who is pirating your IPR?

The ability to display dynamic watermarks is especially important when allowing users to print documents as it can be used to identify the source if photocopies of your document are distributed to others. The ability to position watermarks anywhere on the page is equally important if you want to use them as an effective deterrent.

Be sure to check that your PDF security supplier does not require you to make a new encrypted copy of the information you are selling each time you sell to a new customer. Encrypting a file is an expensive CPU operation, not to mention the problems of having to maintain (or be able to create on the fly) encrypted copies for individual users. Look for a solution that encrypts just the once and can identify customers dynamically (ability to show the users name, email address, company name, etc.) rather than you having to put in place a system that does the job.

Note that watermarks applied to password protected PDF documents are useless because if a password remover is used to remove the protection, the watermarking overlay can be easily removed...

9 Does your PDF security provider prevent screen grabbers?

There are many popular programs available on the Internet, such as Snagit, or photo processing programs, that provide the ability to capture the screen image and save it as a file, or, even, OCR it and save the result! Be aware that plug-in systems are totally dependent upon what the host program is willing to do, because they are not in charge of the environment.

If the PDF security provider you are looking at only prevents Windows print screen then you might want to look elsewhere.

10 Do not choose solutions that involve you in having to set up complex codes and encryption keys.

Any PDF security solution worth its salt should keep the complexity of how it achieves your business objectives transparent from both you and your customers. After all, what is the point of buying a solution and then spending a fortune on internal (or, worse still, consultant led) implementation if you don't have to do that?

Balancing security against usability

If you want to talk about security for PDF documents then you have to understand what you are trying to achieve.

It is all about objectives. How difficult to do want to make it for the IPR pirate to do their job? How feasible is it that you can stop them in their tracks? At the baseline, does the security stop screen print or copy and paste? These are the simplest attacks to allow pirating of documents. So does the system that you have selected actually stop these features on demand? Be aware that proper security controls should allow you to switch this control on or off, not just off.

It's a commonly held view that security systems are difficult to set up, and the more secure you want them to be the harder they are to use. It's also wrong.

LockLizard have made full use of their significant background in the design of easy-to-use systems, and in the implementation of encryption and security technologies, to provide realistic, granular and effective PDF document protection and document management controls.

PDF Password Protection

Common weaknesses in most PDF protection products are to rely upon passwords being distributed by document publishers to those authorized to use them. Apart from the obvious problems that passwords can be given away, there are a plethora of password recovery or cracking tools available on the Internet to remove passwords or reveal what they are.

The LockLizard approach is to license the relationship between the document publisher and customer, and automatically establish and verify authorizations on a document by document basis. No access control information travels with the documents, no passwords are given to users, and users have no means of entering passwords. Access control information is negotiated cryptographically and the user (or any other attacker) cannot become involved in the process or

capture any secret information.

So the commonest methods of **attacking protected PDF documents** - through attacking passwords, **have been prevented**.

PDF Plug-ins and Plug-Outs

A common approach to rendering PDF documents is to use the Adobe viewer, operating either as a plug-in (the security company provides add-on code that links into hooks provided by Adobe) or as a plug-out (where the security company puts a shell around Adobe and manipulates their interfaces). **These have a number of weaknesses.**

Plug-ins are notorious for failing to interact cleanly because there is no certification process by which their interoperation can be tested. From a security standpoint there is little or nothing to stop people from creating plug-ins that compromise system security, and using them to bypass other plug-in controls. Plug-ins are normally run on an 'honor' system, which is fine except that there is no honor among thieves! For further information see PDF plug-in vulnerabilities.

Plug-outs, by comparison, are notoriously difficult to get working, and tend to be highly fragile. Even the slightest change in the application being plugged-out can render the entire security system unworkable, to the consternation of all users. And there is no incentive for the supplier of the application being plugged out to be helpful. Both approaches are also vulnerable to all the attacks against the underlying application since they cannot prevent them.

LockLizard has provided security by design. Using our own viewer completely prevents the problems of plug-ins/outs, and allows for a complete control over the environment that cannot be achieved by other approaches.

Zero footprint solutions

Zero footprint solutions sound brilliant - total security without doing anything! Of course if it were true then there would be no software or music piracy - and we all know that is not the case.

The fundamental weakness of these systems is that they MUST send the decryption/unscambling key with the protected document. So it can be easily found, and automatically removed. To be fair, the technique does reduce trivial copying by those who cannot be bothered to do some trivial Internet searching. But they are usually not the people you are trying to stop.

Without having anything implemented on the computer it is not possible to implement controls that can be enforced locally. So the most powerful security controls and techniques are not

available.

This approach leaves you largely relying on the DMCA (Digital Millennium Copyright Act) for protection of your PDF documents, always assuming you can afford the lawyers fees. Another good example of a zero footprint solution?

Risk Management and granular controls

Generally PDF security providers do not appear to have understood the need to be able to provide and support granular ranges of protection based upon the risk management stance of the publisher. There is little demonstrated thought about how controls are supposed to relate to each other, or to DRM as a specific method of Intellectual Property Rights management.

For instance, **allowing printing** introduces a risk that documents may be sent to file drivers, and then reprinted at will, or physically printed out, scanned and then brought back as uncontrolled documents. Different techniques may be used to resist these options, including the use of both **static and dynamic watermarking** to identify the user of the document or make it difficult to use scanning techniques and OCR to recreate documents. Omnia Romae cum pretio (Juvenal), or more literally, everything has a price.

LockLizard provide a comprehensive series of methods for helping publishers identify dynamically who is the source of printed copies, which can be augmented by OCR preventing or copy revealing where the security requirement is very high. The higher the strength of the controls, the more intense the demand on the computer hardware. But this is transparent to both publisher and user (unless the user tries to break the rules, of course).

Ease of use

But most important is the ease of use for both PDF document publishers and their authorized users.

For there to be realistic security, an applications program must be installed on the user's computer. So LockLizard minimize the need of the user becoming involved in entering codes, passwords or similar. The user establishes a single generic license with their publisher and LockLizard take care of all the document access permissions, monitoring, counts and so on without the need for any user or publisher intervention.

From the publisher's side, the publisher is presented with a small number of panels that step them cleanly through the protection process. They do not allocate codes or generate coding structures. They are not involved in PKI administration (under the hood LockLizard use that technology, but the way it was originally intended, without anyone having to get involved with it,

or understand it) and deal with questions that are business relevant – when is the document available from and to – how many prints are left – are thin client systems or similar environments forbidden – how often must the license be verified – and so on.

A quick look at screenshots of the protection dialog shows that choices offered to the publisher are obvious and logical – no use of mysterious codes such as 'enter -1 for unlimited' are required. LockLizard get the protection input from business people in their own language. Not exactly rocket science, but it shows the gulf between suppliers who can't even be bothered to understand their customers, and those who go the distance.

LockLizard customers clearly identify that they chose LockLizard as their supplier because it is the most cost effective and the easiest system to implement. It allows them to choose the level of controls that they believe are correct with respect to individual documents, and subsequently vary them in a meaningful way per customer.

So it is possible to have a high security system without making it impossible to use, but please don't tell the security experts since they might be out of a job.

LockLizard is used by a wide variety of industries to protect everything from financial and share trading information, accounting and investigation information, maps and charts, service manuals, sales and competitive analysis, training materials, proprietary designs, open tender documentation, membership and subscription information for both professional associations and financial services businesses, and so on.

About LockLizard

LockLizard is a DRM (digital rights management) company that specializes in document security and copy protection. We protect information with US Government strength encryption and drm controls to ensure complete protection against copyright piracy. Use our DRM software to stop copying, prevent printing, disable print screen, expire content, and instantly revoke access to information.

We provide copyright protection without the use of passwords to ensure maximum security and usability, and to protect information, documents and web content from unauthorized use and misuse no matter where it resides. Control who uses your content, what they can do with it, and how long they can use it for. http://www.locklizard.com