Global Information Assurance Certification Paper

Adobe Acrobat Security:
Not Just a Bunch of Mud and Straw Bricks!

By

Joseph Richmeyer

SANS GSEC Practical
Option #1
Version 1.4b

December 8, 2003

Table of Contents

Abstract

The purpose of this document is to examine the security features and vulnerabilities of the Adobe Acrobat program. As you probably already know, the PDF (Portable Document Format) format originated by Adobe has become the de facto standard for document portability. What you may not know is there are a lot of security related options for your PDF documents. In addition to the common security features found in most software applications, I will examine some of the lesser known security features available in Acrobat. Lastly, I will cover some of the recent security vulnerabilities found in Adobe Acrobat line of products and how to mitigate these risks. The main focus of this paper will be Adobe's latest version for Windows named Acrobat 6.0. However, comparisons to previous versions will be made as needed. I encourage the reader to have a PDF document open while reviewing this paper. If you do not have the latest version of Adobe Acrobat Reader (now simply called Adobe Reader), you can download this free of charge from the following Adobe web site: http://www.adobe.com/support/downloads/main.html

Adobe Acrobat –Then & Now

Adobe Systems Inc., founded in 1982, first released Adobe Acrobat in 1993. To date, over a half a billion copies of Acrobat Reader have been distributed worldwide.[1] The PDF format has many advantages such as compatibility, reduced file size and the ability to retain the exact look of the original document. Remember the major snafu when Microsoft Word 97 documents were unreadable by previous versions of Microsoft Word?[2] The PDF format solves this type of file format problem and other document incompatibility issues that can be caused by different operating systems, different software programs, printer drivers, etc.

The Adobe Acrobat 6 Family of products comes in four versions: Reader, Elements, Standard and Professional. The Adobe Reader program is available for free at numerous web sites (see hyperlink above). This version basically allows you to read a PDF file. To create a PDF file, you need to have the Elements, Standard or Professional versions of Acrobat. These three versions are not free, but do give increased functionality and allow use of the security features described in this document.

The Elements version is designed for corporations and must be purchased at the minimum quantity of one thousand units. The Standard version, which has more functionality than the Elements version but not as much as the Professional version, is designed for the average user who wants simple ways to quickly create PDF documents. The Professional version contains all available advanced features such as forms and is designed for the power user. As with most software versions, more functionality means more dollars out of your pocket.

Document Security

Viewing Security Settings in a PDF Document

In this section, I will demonstrate how to quickly show the security settings of a document. There are four ways to show the security settings of a document. These methods work regardless of which version of Acrobat you are using. First, the *long* way to view the security settings is:

- Click once on the **File** menu
- Select the **Document Properties…** menu option
- Click on the **Security** option in the left hand pane

The Document Properties window will show the current security settings and the corresponding restrictions set in the right hand pane. The second way to get the security settings window is to click the **Secure** button on the menu bar. This button looks like a yellow padlock. (Please see the red arrow pointing downward in Figure 1) The third way to see the security dialog box is to click on the right-pointing arrow directly above the vertical scroll bar and select the "**Document Properties…**" option from the pop up menu and then select Security in the left hand pane. (Please see the left-pointing blue arrow in Figure 1 for details.)

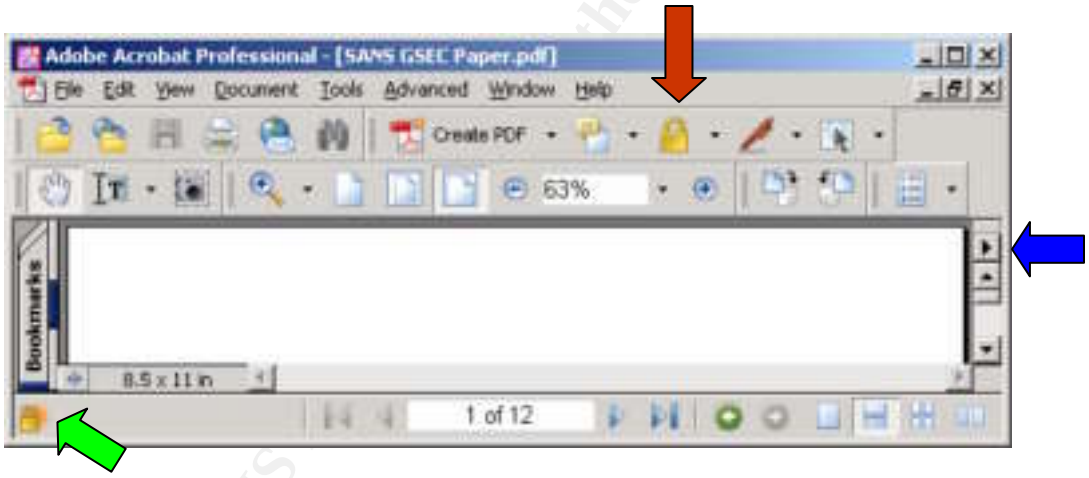

Figure 1

The fourth and fastest way to view the security settings is to look for the small gold padlock in the lower left hand corner. (Please see the diagonally pointing green arrow in Figure 1 for details.) If you do not see a padlock in this section, there are no security settings on the document. If there is a gold padlock, right-click this icon and select the "**Document Security…**" pop up option.

Now that you know how to view the security settings of a PDF document, let us look at how to set some of these options that I have whetted your appetite with.

Setting Security Options in a PDF Document

In order to set any of the security features in a PDF document, you must be running either the Elements, Standard or Professional version of Acrobat. There are three security settings available for your documents:

- No Security
- Password Security
- Certificate Security

Let us take a look at each of these options in depth.

No Security – This is the default setting for a newly created PDF file. There is a common misconception that the contents of a PDF document can not be changed. Not only is this wrong, but it could have dangerous consequences. This setting allows anyone with the Elements, Standard or Professional versions of Acrobat to change the contents of the document. Simply use the Acrobat's *Touchup Text* tool to make whatever changes are desired. For example, in a yearly report of a major company with the default No Security setting, you could easily change the line "*We expect to meet our financial goals next quarter...*" to "*We **do not** expect to meet our financial goals next quarter…*" PDF documents that originate from scanned sources are not immune from changes either. You could use the *Paper Capture* command to convert sections of the scanned image to text and then make changes with the *Touchup Text* tool.

Password Security – Although the title of this section seems uncomplicated, this is where things can get a little confusing. There are two types of document passwords: Document Open and Permission. The Document Open and Permission passwords are: case sensitive, must be different, and either one can be used to open the document. Also, the following characters may not be used in either password: ! @ # $ % ^ & * , | \ ; <.[3] It is critical to note that Password Security is dependent on the compatibility level chosen. The three compatibility levels are:

- Acrobat 3.0 or later (40-bit RC4 encryption)
- Acrobat 5.0 or later (128-bit RC4 encryption)
- Acrobat 6.0 or later (128-bit RC4 encryption)

The first thing you must decide is what compatibility level to select for your document. There are two perspectives in determining which compatibility level to use: security and user-version. In the security perspective, the compatibility level is chosen by the encryption level or restrictions needed. For example, if your document requires 128-bit RC4 encryption, then you can not use the "Acrobat 3.0 or later" compatibility level since it uses 40-bit RC4 encryption.

In the user-version perspective, the target audience of your document determines the compatibility level chosen. If you do not know which version of Acrobat Reader your audience has, then you should select the "Acrobat 3.0 or later" compatibility level. However, if you know your intended audience is

exclusively using Adobe Reader (version 6), then you should choose the "Acrobat 6.0 or later" compatibility level. The higher compatibility level selected, the more secure the document will be and the greater number of available document restrictions can be set.

Document Open Password - This password, as the name implies, is designed to allow a person to open a document via a previously defined password. However, just because they can open the document does not necessarily mean they can make changes to or even print the document. These restrictions, also known as permissions, are covered in the next paragraph. If you set a Document Open password, you probably will want to set a Permission password. If you do not, a reader could remove the Document Open password set in your document.

Permission Password - This password allows you to set specific items of what can and can not be done to the document. It also protects the Document Open password. In previous versions of Acrobat this was know as the Master password.[4] The Permission password can be used independently of the Document Open password. The number of restriction options available depends on compatibility level chosen in the Document Security window.

Acrobat allows for 40-bit or 128-bit RC4 encryption in the compatibility levels. Additional permissions are available if you use the latest version of Acrobat and its corresponding compatibility level. You should encourage your audience to freely upgrade to version 6 of Adobe Reader as it is well known that 40-bit encryption can be easily cracked in today's computing environment.[5] Note, this author has never engaged in any cracking of any Adobe product as he does not want to end up in a similar fate as Dmitry Sklyarov. In 2001, Mr. Sklyarov was arrested and spent time in jail for presenting a paper on cracking the encryption routine used in the Adobe Ebook product.[6]

Here is a table showing the differences of compatibility levels:

Permission	Acrobat 3.0 or later (40-bit RC4)	Acrobat 5.0 or later (128-bit RC4)	Acrobat 6.0 or later (128-bit RC4)
No printing allowed	X	X	X
Printing allowed – 150 DPI (dots per inch)		X	X
Printing allowed –high resolution	X	X	X
No changes allowed	X	X	X
Filling in forms & signing	X	X	
Commenting, filling in forms and signing	X	X	X
Any change allowed except extracting pages	X	X	X

Enable copying of text, images and other content and access for the visually impaired (screen readers)	X	X	X
Copying of text, images and other content		X	X
Inserting, deleting and rotating pages		X	X
Enable plain text metadata			X

Password Security Summary

1. Determine the compatibility level of your document. Which perspective has a higher priority: security or user-version?
2. Determine if your document needs to be password protected. If the answer is yes, then set a Document Open password and a Permissions password.
3. Determine what permissions you want set on the document. Recall, the permissions available are dependent on the compatibility level. Set these options and select a good Permissions password. This will also protect the Document Open password.
4. Save and close the document so the new security settings will be set.

Certificate Security

In general, a digital certificate validates your digital credentials and contains information used to safeguard data. The topic of digital certificates is very complex and beyond the scope of this paper. Related to digital certificates is the subject of digital signatures. Per SANS, a digital signature is "a hash of a message that uniquely identifies the sender of the message and proves the message hasn't changed since transmission."[7] Adobe Acrobat extends the functionality of the digital signature to include version control. You can revert back to the point in time to see the document exactly as it was when the digital signature was added. You can also do a comparison between signed versions of the same document.

In a PDF document, a digital signature can be hidden or visible, but will always appear in the signature tab. Note, in previous versions "tabs" were referred to as "palettes".[8] If a digital signature is visible in the document, it can contain graphics, text, and even a picture of you. If the Signature tab is not visible, you can easily display this tab by clicking the **View** menu and selecting the **Navigation** tabs menu option. This will present a variety of tabs for use in your document, please select the Signature tab.

There are three methods to access a digital ID, they are:

- Default Certificate Security

- Windows Certificate Security
- Third-party Options

Let us briefly look at each of these options:

Default Certificate Security – This option enables you to create and select a password for your protected digital ID file. Basically, you are the Certifying Authority for your digital ID. To create your digital ID using the Default Certificate method, do the following:

1. Click on the **Document** menu and select the **Security** menu option
2. Click on the "**Display Restrictions and Security…**" menu option
3. In the "Security Method" drop-down box near the top, select the "**Certificate Security**" option.
4. In the "Certificate Security – Choose Method" window, select the "**Default Certificate Security**" option.
5. Click the **OK** button
6. On the next window, click the "**New Digital ID File…**" button
7. On the next window, click the **Continue** button
8. On the next screen there is a lot of information to be filled out such as your name (which will appear on the digital signature, which key algorithm to use (1024-bit RSA or 2048 bit RSA), email address…
9. Enter a password and confirm it for this digital ID (6 characters minimum)
10. Save the file, it will have an *.pfx extension.

You now have a digital ID that can be used to digitally sign or encrypt your documents. Be sure to back up this file, preferably on removable media. It is important to protect this removable media in case the system used to create the digital ID experiences an unrecoverable failure. If this digital ID is lost, you may not be able to access some of your documents.

Windows Certificate Security – This option uses an existing Windows digital ID as opposed to creating a new one like we did in the Default Certificate Security approach. An advantage to this is that you do not have to use a password because the Windows logon process protects access to your Windows digital ID. Additional information on using digital certificates with Windows can be found at: http://www.microsoft.com/technet/security/topics/crypto/Certs.asp

Third-Party Solutions – There are a variety of third-party solutions that will work with Adobe Acrobat in providing a digital ID and other security related functions. These solutions are implemented as plug-ins and often add customized menu options. For additional information on third-party products that deal with digital certificates and document control, please see the following web site: http://partners.adobe.com/asn/developer/security/index.jsp

Miscellaneous Security Features:

Certifying a Document

When saving a document as a "Certified Document", you attest to the contents and decide what changes are allowed that will retain the documents certified status. This is all done via your certifying signature. Click on the **File** menu and select the "**Save as Certified Document…**" menu option. There are three options to choose from. You can disallow all changes, allow only forms to be filled in or allow comments to be added & forms to be filled in. You can also decide if you want the certification shown on the document. Lastly, select which digital ID you want to use to certify the document. Once the document is correctly certified, a blue ribbon will appear in the lower left hand corner of the Acrobat window. You can click on this icon to get additional information about the certification. If unauthorized changes are made, the certifying signature is now invalid and a message window will appear indicating this.[9]

Trusted Documents

Acrobat allows you to create a list of trusted documents and authors. All documents and authors not specifically added to the Trusted list are considered non-trusted. Using the Trust Manager feature, you can specifically set what security functions are allowed for trusted and non-trusted documents. This includes: displaying security permissions, whether the document can open other files or launch applications, allow multimedia clips to be played, use a specific media player and other options. To get to the Trust Manager, click on the **Edit** menu and select the **Preferences…** menu option. In the left hand pane, choose **Trust Manager** and the options noted above will appear on the right hand pane. Be careful not to click on the "Reset List of Trusted Documents and Authors" button as this will remove all of your previous entries.

PDF as a Container

Don't want to pay for client-based encryption software, use Acrobat instead! Acrobat has the ability to embed files of any type into an existing PDF document.[10] You can insert any file via the "**File Attachments…**" menu option of the **Documents** menu. After the file is inserted, use either the password or certificate security option which will encrypt the entire document, including the attachment. The encrypted PDF document can now be safely delivered to the recipient via email, posted on a web page, etc.

Extending Adobe Security

There are many possibilities available with the extension-able Acrobat architecture. In addition to digital certificates and password security, Acrobat can integrate with several technologies such as smart cards, biometric readers, USB keys…for greater protection of private keys and enhanced document control. All

versions of Acrobat 6 have support for the Microsoft CryptoAPI which allow a variety of crypto service providers the ability to interface with Acrobat.[11]

Adobe Acrobat Vulnerabilities

Like any software product, Acrobat has its share of vulnerabilities that must be dealt with. Again, it is a common misconception that PDF documents are safe and can not contain any malware. Acrobat can run JavaScript code and can be set to run automatically when the document opens. This author predicts that PDF files will unfortunately be a future target of hackers. Here are some of the latest Acrobat vulnerabilities and mitigation strategies involved in dealing with these.

SVG Viewer Vulnerabilities

In October 2003, three vulnerabilities with the Adobe Scalable Vector Graphics viewer (SVG) were announced to the public.[12] The SVG viewer is widely used with several popular browsers such as Internet Explorer, MSN explorer, AOL browser and others. The SVG viewer is a plug-in for a browser that enables XML creation and control of vendor graphics. Specifically, these vulnerabilities allow an Active Scripting bypass, local and remote file viewing and cross-domain & zone access. An attacker who exploits these vulnerabilities could view files on the victims system, redirect URLs and execute code of choice on the system!

The version of the affected SVG viewer is 3.0. It is important to note that proof of concept code has been released for all of the SVG Viewer vulnerabilities. Adobe has released a free upgrade which corrects all of the vulnerabilities. This upgrade can be found at: http://www.adobe.com/svg/viewer/install/mainframed.html. If you are running a vulnerable version of the SVG viewer, it is recommended that you install the patch as soon as possible.

Acrobat Plug-in Vulnerability

In March 2003, and later updated in July 2003, a vulnerability was announced concerning the Adobe Acrobat plug-in functionality.[13] Acrobat does not properly authenticate plug-ins such that a forged digital signature (within the plug-in) could be used to alter the document or perform other malicious actions.

Here is the scenario of how an attack could occur. An attacker gets an Adobe plug-in with a valid signature. The attacker modifies the contents of the plug-in except for the header which contains the critical signature information. Thus, the attacker has a valid plug-in header and his malicious code as the content. He can then email the plug-in to a victim or make the plug-in available on a website.

This vulnerability affects Acrobat (Reader & Full) versions: 4.0.0, 4.0.0.5, 4.0.0.5C, 4.0.5.a, 5.0.0 and 5.0.5. The Acrobat version 6 family of products is not affected. No exploits that target this weakness are known at the time of this writing. Please do not let this last piece of information lull you into a false sense of security. If a vulnerability exists, there is probably a hacker out there trying to

figure out the exploit. The only course of action to correct this situation is to upgrade to version 6 line of Acrobat products.

Acrobat Arbitrary Code Execution

In May 2003, a vulnerability in Acrobat's JavaScript parser was discovered that allows a malicious PDF document to execute arbitrary code on a system.[14] To exploit this vulnerability an attacker could create a PDF file that contains instructions to write code into the plug-ins folder. Note, code in the plug-ins folder is automatically executed when Acrobat is started. This malicious code could be used to modify files, delete files and be used as a launching pad for propagation of a worm.

Proof of concept code has been made available to the public. This vulnerability is only present in the full versions of Acrobat 5.0 & 5.5 ("reader" versions are not affected). There are two mitigation strategies for dealing this weakness. The first option is to upgrade to version 6 of Acrobat. The second option is to apply the patch from Adobe which can be found at:
http://www.adobe.com/support/downloads/detail.jsp?ftpID=2121

Acrobat 4.0 Buffer Overflow Vulnerability

In July 2000 it was discovered that the Acrobat 4.05 family of products (Acrobat Reader, Business Tools, Fill-in) have a buffer overflow vulnerability that could allow an attacker to insert malicious code of their choice into a PDF document. [15] Although this is a three-year old vulnerability, it is surprising the number of users (especially in the home arena) still running older versions of Acrobat. Thus, the author feels it is still pertinent to cover this issue.

To exploit this vulnerability, an attacker could insert a long string into a data field embedded in the PDF. This would overflow the buffer and allow the attacker to run code of choice which is inserted after the long string. There are two options to remove this vulnerability. First, upgrade to a later version of Acrobat. Second, install the "Update 2" patch which can be found at:
http://www.adobe.com/misc/pdfsecurity.html

Summary

Hopefully by now you have realized there are many untapped security options available in Acrobat that can protect the confidentiality, integrity and availability of your PDF documents. We covered how to view the security setting of a document, set a password required to open a document and how to apply specific restrictions depending on the level of encryption chosen. We also covered three choices in using digital certificates and some miscellaneous security features. Lastly, we covered four vulnerabilities in the line of Acrobat products that the security-minded user needs to be conscious of. The author hopes the reader is now aware of the basic and advanced security features of Adobe Acrobat and that it is *not just a bunch of mud and straw bricks*!

References

[1] Adobe Systems Inc. Acrobat Family
URL: http://www.adobe.com/products/acrobat/main.html

[2] Microsoft Corporation.
URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;q157666

[3] Baker, Donna; Carson, Tom. Adobe Acrobat 6 The Professional User's Guide. Berkeley: Apress. 2003.

[4] Adobe Staff. Adobe Acrobat 5.0 Classroom in a book. Berkeley: Adobe Press/PeachPit Press. 2001. P65-68

[5] Zeller, Tom. "Security Still Up in the Air". 5 February 2001.
URL: http://www.networkcomputing.com/1203/1203ws1.html

[6] Middleton, James. "Adobe Cracks under Hacker Pressure." 24 July 2001.
URL: http://www.pcmag.com/article2/0,4149,29210,00.asp

[7] Cole, Eric; Fossen, Jason; Northcutt, Stephen; Pomeranz, Hal. SANS Security Essentials with CISSP CBK Version 2.1. SANS Press, April 2003, Appendix A, page A-130

[8] Baker, Donna. Adobe Acrobat 5 The Professional User's Guide. Berkeley: Apress. 2002. P30-35

[9] Baker, Donna. The 100 Best Adobe Acrobat Tips & Tricks. Berkeley: Adobe Press. 2004. P287-289

[10] Adobe Systems Incorporated. "Protecting Electronic Documents with Adobe Security Solutions. 2003
URL: http://www.adobe.com/security/pdfs/acrobat_security_wp.pdf

[11] Adobe Systems Incorporated. "Document Security Drives Efficient Online Business Processing". 2003.
URL: http://www.adobe.com/financial/pdfs/doc_sec_sb.pdf

[12] GreyMagic Software. "Adobe SVG Viewer's Trio". 7 October 2003.
URL: http://www.greymagic.com/news/

[13] Harvilla, Jeffrey S and Cohen, Cory F. "Adobe Acrobat PDF viewers contain flaw when loading and verifying plug-ins". 108. 16 July 2003.
URL: http://www.kb.cert.org/vuls/id/549913

[14] Adobe Systems Incorporated. “Adobe Acrobat 5.0.5 Security, Accessibility, and Forms patch – English”. 30 April 2003.
URL: http://www.adobe.com/support/downloads/detail.jsp?ftpID=2121

[15] Adobe Systems Incorporated. “Security update”
URL: http://www.adobe.com/misc/pdfsecurity.html