

## **Problems with Adobe Acrobat 8 Redaction Feature**

Adobe's latest version of Acrobat Professional now includes a redaction feature, but should you trust it? Not according to Duff Johnson's PDF Perspective, a PDF and Acrobat discussion blog for end-users, CIOs and developers. Johnson obtained much of his information from Mark Gavin, the founder and CTO of Appligent. Appligent makes a PDF redaction product called Redax. Gavin points to the opaque regions Adobe inserts where the information has supposedly been redacted as one potential problem. Gavin says that the opaque regions prevent the user from detecting the improperly redacted information.

SRS has observed that earlier versions of Adobe Acrobat, including version 7, flashes a message across the status bar at the bottom of the application window that indicates that unused objects are being removed when the document is saved. Reviewing the document with our Document Detective review tool shows that the unused objects are still in the file. We have successfully recovered deleted and modified text, deleted images, and even old Metadata from PDF documents edited with Adobe Professional.

So what about Redax and other PDF redaction tools? SRS has not done any extensive testing of these products, but our cursory testing did not bode well. Several products use encryption to prevent easy access to the results, and Document Detective does not yet support encryption. We did notice that the redacted file sizes were larger than the original. This could be attributed to different encoding schemes, but until we can prove a redaction tool actually removes the information from the file, we won't recommend any of them.

We do not recommend editing or redacting PDF documents. The best option is to edit or redact the document in its original format and then port it to PDF again. If you don't have access to the original document, find a program to convert the PDF document into another format, such as Microsoft Word. If the original format is a Microsoft Office format, then use Document Detective to redact the document before converting it to PDF. We also recommend scanning the new PDF document with Document Detective to detect any anomalies that may have occurred during the conversion.

<http://www.acrobatusers.com/blogs/duffjohnson/2006/11/16/cut-it-out-redacting-with-acrobat-8/>

-----

## **ABA Rules Metadata Admissible in Court**

The San Diego Business Journal reports that the American Bar Association has made a decision regarding meta data in electronic document. Michelle Mowad reports that, "Attorneys receiving electronic documents are free to use so-called "metadata" and other information embedded in those documents." The ABA's Standing Committee on Ethics and Professional Responsibility said that such hidden information is "free game" and can be used in litigation.

The article cites two examples of recent meta data exposures in her article. "Google recently inadvertently leaked financial projections and the U.S. Justice Department revealed Social Security numbers through metadata," According to Mowad.

Unfortunately, Mowad ends her article with the usual recommendation to us a PDF document to eliminate hidden data problems. SRS has demonstrated that this is a myth. PDF documents can contain a lot of hidden data, and a lot of hidden data ports from the original document into the new PDF document. Documents must be properly sanitized using a tool like Document Detective before they are converted into a PDF document; otherwise, hidden data will remain hidden in the new PDF document.

[http://www.sdbj.com/industry\\_article.asp?aID=060269.9113936.1395680.299919.377934.850&aID2=107351](http://www.sdbj.com/industry_article.asp?aID=060269.9113936.1395680.299919.377934.850&aID2=107351)

-----

### **Hacker Discovers Adobe PDF Back Doors**

Microsoft Office documents have been plagued with problems recently such as the zero-day attack for Word, but Microsoft is not alone. eWeek magazine reported recently that a hacker has discovered back doors in Adobe's popular PDF file. The article cites two back door attacks including malicious link that is accessed by the targets browser when the PDF file is opened, and an attack that can query databases on the targets computer. David Kierznowski, a penetration testing expert specializing in Web application testing, claims that there are at least seven more attacks that would allow an attacker to launch malicious software.

This article demonstrates once again that Adobe PDF is not a safe file format as is commonly believed. The Adobe specification is 1,236 pages long. It is extremely functional, but all those wonderful features lead to technical vulnerabilities like unintentionally hidden data and malicious software. Document Detective can not prevent these features from being abused by an attacker, but it can prevent you from inadvertently exposing sensitive information hidden by these very functional documents.

<http://www.eweek.com/article2/0,1759,2016606,00.asp>

-----

### **Document Detective Version 2.1 Released**

SRS announced the release of Document Detective version 2.1 on Monday, 5 February 2007. A formal announcement will be made to the press later this month. This new version includes a number of new features including an integrated thumbnail view of graphical objects and a graphical depiction of the objects location in the same window with the objects properties. This eliminates the need to switch between the Properties View and the Object View when reviewing an electronic document. The Object View, now called the Shape View, is still available for close-up, detailed examinations of graphic objects. This release also includes a built-in Review Checklist to lead you through our recommended review process. This process is designed to meet the US Government's criteria for reviewing potentially classified material for downgrading. No process will eliminate the risks inherent to sharing electronic documents, but a conscientious application of our Review Checklist will reduce that risk to an acceptable level.

Other improvements include a streamlined Flatten Document process. You can configure the process to minimize the number of dialogs displayed. You can even configure the process to skip all dialogs, making it a true one-button fix for most common document security problems. We also changed the regular expression library and provided a way for you to enter your own regular expressions. This lets you minimize the number of false positives such as "Secret Agent," "Secret Service," and "Secret Releasable" when searching for the keyword SECRET, and you can locate structured data such as social security numbers easily. Developing good regular expressions is an art, so we retained our original capability enter simple text strings. These strings are automatically converted into regular expressions by Document Detective.

For a longer list of changes and a screen shot of the new interface, please visit:

<http://www.stg.srs.com/eds/docdet/support/DD21Annouce.htm>

You can also request a free 30-day evaluation copy of the software from this web page. Our export control officer will not allow us to provide an open download link, so you will have to submit a request using our website. We will email you a download link as soon as we have validated your request. The information provided on this form will not be used for any other purpose.

SRS Technologies is committed to continuing research and product development. While no process or procedure is perfect, Document Detective is the best available solution for reviewing and sanitizing electronic documents, especially when National Security Information is at stake.

Please feel free to forward this message to anyone you believe would benefit from this information.

-----

This newsletter is dedicated to raising awareness about the Desktop Publishing Threat to Information Security and to disseminating information that will help mitigate these risks. Our newsletter is published aperiodically when there is news to report. We will not clutter your inbox with idle chatter when there is nothing significant or useful to say. This newsletter is available free of charge. Subscriptions are at the discretion of SRS Technologies.

Suggestions and comments are always welcome. If you do not wish to receive this newsletter, please e-mail us and we will gladly remove you from the list. All EDS-related correspondence should be sent to [rhackett@srs.com](mailto:rhackett@srs.com)

For information about Document Detective electronic document review and sanitization toolkit, please visit:  
<http://www.docdet.com/>

For a list of articles and information regarding EDS, including previous editions of this newsletter, please visit the Document Detective website and click on "The Threat."

To subscribe or unsubscribe from this newsletter, send email to:  
[rhackett@srs.com](mailto:rhackett@srs.com)

SRS Technologies  
Systems Solutions Division  
500 Discovery Drive  
Huntsville, AL 35806  
Copyright 2006 SRS Technologies