

DSS Publishes Trusted Downloading Products List

The Defense Security Service (DSS) Industrial Security Program has published a Trusted Downloading Products List of evaluated products that includes the SRS Document Detective electronic document review and sanitization toolkit. The evaluation provides assurance that Document Detective performs according to SRS claims and documentation, and that it identifies embedded words and objects. The DSS list is for information only and is not an endorsement or recommendation for any product. For a copy of the DSS Trusted Downloading Products List, please visit:

http://www.dss.mil/search-dir/whatsnew/trusted_download_042705.doc

Pentagon Hacker Indictment Reveals Sensitive Data

A redacted PDF copy of the Pentagon hacker indictment included a complete list of the Pentagon, US Air Force and DOD server IP addresses that were hacked. This inadvertent disclosure could further compromise the integrity of those systems. Recovering the redacted material was easy with a copy of the free Adobe Acrobat reader. Simply use the text tool to copy the redacted text, and then paste it into any text editor. When the information is pasted into an RTF compatible editor, like Microsoft Word, the formatting is also recovered. PDF documents are not simple "printed" documents like most people believe. Documents must be properly sanitized before they are converted into PDF documents.

http://www.theregister.co.uk/2005/07/11/mckinnon_indictment_snafu/

PDF Plug-in Provides Tracking

A recent article in *PC Magazine* provides even more evidence of the complex nature of PDF documents. Don Fluckinger's article poses the question, "Are Your PDFs Spying on You?" The functionality of PDF documents can be extended with third party plug-in applications. The article begins by looking at a company called Remote Approach that provides a plug-in capable of tracking who has read documents under their control. According to Fluckinger, the software "can track who's e-mailing PDFs to whom and what they're reading—in real time." This obviously raises privacy issues. The software, called Map-Bot, does not access any user data on the computer, and it does not load "spyware," but the potential is obvious. The author laments that this "is the beginning of a movement that could chip away at PDFs' sterling rep, one document at a time." Like many people, the author appears to believe PDF documents are, or at least used to be, safe documents. PDF documents are very functional documents and have long posed a significant threat to information security. This is why SRS Technologies is adding a PDF scanner to our Document Detective electronic document review and sanitization toolkit.

<http://www.pcmag.com/article2/0,1759,1823029,00.asp>

Microsoft Word Redaction Tool

Microsoft recently announced a free plug-in redaction tool for Microsoft Word 2003 that can be downloaded from the Microsoft Website. Microsoft claims that the text redacted using this tool cannot be recovered. The tool does not provide a method for redacting other embedded objects, such as images, and the plug-in does not work for PowerPoint or Excel. SRS tested the Microsoft claims and found that they do indeed replace the redacted text with a single character (the vertical bar) with one notable exception. The spaces are not changed. While this does make recovering the information much more difficult, it may be possible to recover portions of the redacted text using cryptographic analysis. These seemingly benign spaces are needed to make the lines break in the same way they break in the original document. Because of redundancies in the English language, knowing word length and position provides useful information about the redacted text. The unredacted portions of the document also provide clues about the document structure, style and word usage that could aid in analyzing the redacted portions of

text. The difficulty involved in recovering the redacted text may be sufficient for protecting some private and sensitive information, but it may not be adequate for protecting National Security Information.

Document Detective Status

SRS Technologies is planning to release Document Detective version 1.0.4 in early October 2005. This version improves the document flattening process and allows you to control which objects get flattened in your document. Command line switches will allow the flattening and filtering process to be automated, and better integration with Word, PowerPoint and Excel will make Document Detective easier to use. You will be able to tell Document Detective which objects to delete or convert into safer image objects, and Document Detective will make the necessary changes to your document. Proper use of the flattening and filtering processes before a document review can reduce the complexity of the review to checking instances of keywords.

Version 1.1, scheduled for release in December, will include a PDF scanner. PDF documents are extremely complex. The open source PDF specification is over 1,200 pages long. In addition to text and images, PDF includes a very capable drawing feature, annotations (similar to Comments in Word), articles (similar to Text Boxes in Word), and other collaboration features. Multimedia files can be embedded into PDF documents, and PDF functionality can be extended using third party plug-ins (See article above). Few people realize the complexity of PDF documents and the threat they pose to Information Security. The Document Detective PDF scanner will resemble our Microsoft Word scanner. It will identify the presence of various constructions, and it will display the basic text from the PDF document. Future versions will expand Document Detective's ability to analyze the more complex and esoteric data embedded in PDF documents.

SRS Technologies is committed to continuing research and product development. While no process or procedure is perfect, we can assure you that 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 other Government personnel 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 to Government personnel and to certain contractors responsible for the generation and protection of National Security Information. Contractor 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@stg.srs.com.

For a list of articles and information regarding EDS, please visit our web page: <http://www.stg.srs.com/eds>.

To subscribe or unsubscribe from this newsletter, send email to: rhackett@stg.srs.com

SRS Technologies
Systems Technology Group
500 Discovery Drive
Huntsville, AL 35806
Copyright 2005 SRS Technologies