

AT&T Leaks Sensitive Info in NSA Suit

AT&T is the latest victim of improperly redacted electronic documents. *C|Net News* reports that an Adobe Portable Document Format (PDF) document filed by AT&T's attorneys was improperly redacted, allowing the redacted information to be recovered. The 25-page document responded to allegations from the Electronic Freedom Foundation (EFF) that AT&T had a secret room at one of their switching facilities in San Francisco to support an unlawful National Security Agency surveillance program. Roughly one and a half pages of text are covered with black strips that attempt to conceal information, but the data is easily recovered. Simply select the text tool in Adobe Acrobat, drag it through the redacted text, copy the text and paste it into a Word document. The text and the formatting can be recovered using this technique.

The Meta data of this document reveals that it was originally a Microsoft Word document that was ported to PDF using Adobe Acrobat PDFMaker 7.0. The SRS Document Detective electronic document review and sanitization toolkit includes a redaction tool that could have saved AT&T from this embarrassing incident. The Document Detective redaction tool is easy to use and exceeds the recommendations set forth in the NSA's recently published guidance on data redaction. We also recommend using the Document Detective PDF review tool to verify the redacted document prior to releasing it. In this case, the Document Detective review tool clearly showed that the redacted data was still in the document.

http://news.com.com/AT38T+leaks+sensitive+info+in+NSA+suit/2100-1028_3-6077353.html

Another Dept of Justice Redaction Blunder

A few years ago, the Department of Justice published a heavily redacted report on hiring practices, but the redacted text was easily recovered. Now the DOJ has repeated the error in a brief filed in a grand jury investigation of steroid use in professional baseball. The New York Times reported that about 8 of the 51 pages in the report were electronically blacked out. Simply copying the redacted text and pasting it into a word processing document or a text document is all that is needed to recover the redacted text.

This inadvertent revelation is ironic because the grand jury is investigating potential Government leaks in the case, and is seeking to force two San Francisco Chronicle reporters to testify regarding their sources. SRS was not able to obtain an original copy of the filing, so we have not analyzed the document for other security problems.

<http://www.nytimes.com/2006/06/23/us/23leak.html?ex=1152072000&en=6c01613f173f4190&ei=5070>

Sharing Information, but not too much

In a *Homeland Security Today* magazine (www.HSToday.us) article on information sharing, Hank Hogan points out the dangers of embedded data and metadata in both government and commercial documents, as well as a solution in SRS' highly touted Document Detective. He goes on to say that not only static documents are a risk, but also dynamic data streams such as email and web documents. Hogan's article relies heavily on expert information obtained from SRS Technologies, and he mentions some of the examples of hidden data issues we discovered.

Hogan, Hank, "Sharing information, but not too much," *Homeland Security Today*, Vol. 3, No. 6, (<http://www.hstoday.us>), June 2006, pg 56-7.

Hide and Go Seek with Writer Content

We are often asked if other applications like Word Perfect and Open Office have serious hidden data issues like Microsoft Office. The answer is a resounding YES. All formatted data has the capability to obscure information unintentionally. The more formatting options that are available--the more likely some data will be obscured. Even "text" files like HTML and XML are so highly formatted that a user could inadvertently hide (or lose) information. Many people incorrectly assume that open document formats, such as the OpenDocument standard or Microsoft new XML based Office 2007 formats, will eliminate the hidden data threat. A recent article in the *LINUX Journal* illustrates how information can be obscured in an OpenOffice document.

In an article entitled, "Hide and Go Seek with Writer Content," Bruce Byfield shows how information can be embedded (hidden) in an OpenOffice.org document. He also explains how you can find that data, as well as why you may not be able to find it. The primary intent of this article is to show how to keep multiple documents synchronized using built-in features, but convenient features can sometimes have perilous results. Byfield walks the reader through three methods to hide data in the document, with reasoning for which to use when, and for what types of purposes. Mr. Byfield then ends the article with some very important workarounds for deficiencies in what he portrays as the best solution.

<http://www.linuxjournal.com/article/9053>

Network Computing Review

George Hulme published his review of Document Detective in the May 2nd edition of *Network Computing* magazine. In his half page article, Hulme talks about finding sensitive data in embedded spreadsheets in both Word and PowerPoint documents he received via email by using Document Detective. The documents also contained names and email addresses of various reviewers. In one case, he found that a seemingly benign chart in a Word document contained customer names and average profit margins for several product categories -- information the originator did not intend to share.

<http://www.networkcomputing.com/channels/personaltechnology/showArticle.jhtml;jsessionid=3342LKBDJ5YDMQSNDBECKHSCJUMKJVN?articleID=187002259>

Version 2.1

SRS continues to improve Document Detective, and we anticipate releasing version 2.1 in early September. This version will integrate with Microsoft Outlook to provide more seamless protection for the most significant electronic document security issue--email attachments. Document Detective will warn users if attachments are being sent to addresses outside a specified "trusted" domains list, and the user will have the option of flattening those documents before the email is sent. The Flatten Document process is being streamlined to make it easier to use.

The batch processor will also be improved in this release. The "Server Busy" dialog has been a significant impediment to batch processing because it is coming from the Microsoft Automation layer, which is outside of the control of Document Detective. We have found a way to detect and to work around this issue, which will make batch processing more robust and feasible. The batch processor output will be improved to include counters for keywords, embedded OLE objects, and other warnings, which can be used to assign risk scores to documents. This would give users the ability to identify and segregate high risk documents.

Document Detective is now listed on Version Tracker (<http://www.versiontracker.com>). Go to the Version Tracker website and search for Document Detective. New releases will be announced on Version

Tracker, and existing customers will be notified by email when new releases are available. Customers with existing version 2.0 licenses can upgrade to version 2.1 at no charge.

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@stg.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

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