

GCN Magazine Exposes Microsoft's Ad Hoc Review

Two articles published in today's Government Computer News (GCN) Magazine are the first known press articles to expose Microsoft's Ad Hoc Review as the potential culprit behind the recent rash of Tracked Changes incidents appearing in the news. Other articles have typically blamed the users for failing to turn off this well known feature. Today's GCN articles acknowledge the presence of the Ad Hoc Review and Outlook's ability to enable the Ad Hoc Review and Tracked Changes automatically without any warning to the user.

The first article by Patience Wait talks about recent Government guidance for redacting information that will be released to the public. NSA told Patience that, "Improper redaction of electronic documents has been a growing area of concern in the information assurance community."

http://www.gcn.com/25_4/news/38286-1.html

Joab Jackson's technical article points out that Meta data is only one part of a much larger problem of hidden data in electronic documents. Embedded objects and special features can obscure information from view, but the information is still in the document and can be recovered. The SRS Document Detective product excels in both reviewing and sanitizing this type of hidden data, which is not handled very well by other commercial Meta data products.

http://www.gcn.com/25_4/tech-report/38253-1.html

SRS Technologies did provide detailed technical information for both of these articles, and we do expect to consult on future articles on electronic document security. The SRS Program Manager for Electronic Document Security began warning the Government about this threat over five years ago, and, since that time, he has amassed a considerable body of knowledge regarding that threat and ways to eliminate it. We are pleased to see his research and expertise acknowledged by the press.

DD Redaction Tool follows NSA Guidance

SRS Technologies included a Word redaction tool in Document Detective version 1.1 (released on 27 November 2005) that closely follows the recent guidance from the National Security Agency's (NSA) Systems and Network Attack Center (SNAC) published on 13 December 2005. The NSA procedure is a time consuming and tedious manual process, while the Document Detective procedure is automated. Use the link below to obtain a copy of the NSA Redaction Guidance.

<http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/vtechrep/I333-TR-015R-2005.PDF>

We added a new button to the Document Detective toolbar that is automatically installed into the Word Application. In Word, simply select the text or image that you want to redact and click on the redact button. You will be prompted to save the current file so Document Detective can create a new, redacted copy of the file. Microsoft also provides a free redaction tool which appears to be more functional than Document Detective, but the Microsoft tool does not redact images and the text redaction is flawed. Microsoft's redaction tool does not obscure the length of the words in the redacted text, so the text can be recovered using standard cryptographic techniques.

Of course, we used Document Detective to review the NSA redaction policy. The dates in the Meta data indicate that the document was ported to PDF on 10 Jan 2006, and then modified again on 20 Jan 2006. We were not able to determine what was modified.

xap:ModifyDate='2006-01-20T09:05:43-05:00'
xap:CreateDate='2006-01-10T11:15:26Z'
xap:MetadataDate='2006-01-20T09:05:43-05:00'

We do have some additional recommendations that were not included in the NSA guidance. The NSA process for removing Meta data works well, but Microsoft Word will automatically create new Meta data in the new document, and this data could also be sensitive. Each document also needs to be checked carefully for hidden objects and text that could port into the PDF document. We recommend using the Document Detective flattening tool to remove these hidden objects and text before porting the document to PDF. Finally, PDF documents should not be edited after the port. Editors leave fragments and fingerprints behind that can be recovered. If you need to make changes, go back to the original document, make the changes, and then port it to PDF again.

Vioxx Lawsuits Exacerbated by Tracked Changes

David Ewalt reported in the December edition of Forbes online magazine that the Merck pharmaceutical company was the victim of hidden data in electronic documents. Citing the *New England Journal of Medicine* (NEJM), he said, "that before Merck submitted a major study to the *Journal* for publication in 2000, information linking Vioxx to an increased risk of heart attacks was deleted from the document."

He goes on to say that, "According to Dr. Gregory Curfman, an executive editor at the *Journal*, the NEJM determined data had been deleted by turning on a feature in Microsoft Word called "Track Changes," which keeps a record of what's been added and removed to a document, and allows users to add notes to the text. It's commonly used by groups of people who are sharing a document, since it allows them to make changes to each other's work, without permanently deleting or altering the original document."

http://www.forbes.com/2005/12/13/microsoft-word-merck_cx_de_1214word_print.html

This could be another example of the Microsoft Ad Hoc Review running out of control. It is very possible that no one at Merck enabled the Tracked Changes feature intentionally and then forgot to turn it off. All they had to do was email the document using Outlook XP, and Microsoft would have automatically enabled the Ad Hoc Review, which automatically enables Tracked Changes without any warning. If no one knows the Ad Hoc Review has been enabled, then no one would suspect that Tracked Changes was enabled.

Hit Send and Regret

"A poorly constituted e-mail sent on Melbourne Cup Day this week saw Westpac's full-year profit results potentially exposed before being finalised and lodged with the Australian Stock Exchange (ASX). The revelation forced the institution to bring forward its results announcement to 4pm (AEDT) on Wednesday after halting trading of its shares two hours earlier in response to rumours the results were being distributed through the market. The corporate watchdog has launched an investigation."

Iain Ferguson, ZDNet Australia, November 04, 2005

http://www.zdnet.com.au/news/communications/soa/Hit_send_and_regret_it/0,2000061791,39220866,00.htm

This was a case of an improperly redacted spreadsheet. The sensitive information was covered with the usual black boxes, but it wasn't difficult to recover the information. There was no indication that the Tracked Changes or Ad Hoc Review contributed to this incident.

There are many considerations when reviewing and redacting a document, and attempting to do all of these checks manually without the aid of a tool like Document Detective is dangerous. Document Detective performs hundreds of checks that would be nearly impossible without an automated process.

The additional time required to review an electronic document before you hit the send button may seem like an unnecessary burden, but the cost of not performing that review could be costly or even catastrophic.

Document Detective Version 1.2 Release Planned

The next release of Document Detective, version 1.2, is scheduled for 20 March 2006. This release includes enhanced PDF detection capabilities, including an ability to recover deleted text and deleted pages. We have also added new folders to get the annotations, thumbnails, bookmarks, Meta data and fonts out of the unused objects collection. That greatly reduces the number of unused objects and makes this a useful collection to review.

Based on suggestions from NSA, we have added font parameter checks to our Microsoft Word review tool. Document Detective checks for a number of font characteristics that could obscure text in the original document. Because we do not use the original document font parameters to display the text in our interface, the text is never obscured in Document Detective. The only difference is that now Document Detective warns you if these conditions exist.

The Microsoft Word flattening tool can now identify certain geometry problems, such as objects off the page, and delete them. The geometry check is not done in the review tool because Microsoft Word does not have a consistent geometry. Word documents are repaginated when the document is opened. The repagination depends on the default printer, the version of Word being used, and other local settings. As a result, the carefully arranged geometry on one computer could be entirely different on another computer. This would cause problems if different users were reviewing the same document on different computers, because the results could be different.

A new hanging indent repair tool can identify and repair a condition that could allow text to appear outside the visible boundary of the page. This condition usually occurs when a Word Perfect document has been ported to Microsoft Word.

Our integration with Microsoft Outlook is going well, and the Outlook plug-in should be included in the next release. The plug-in will warn the user if dangerous security settings, such as the Ad Hoc Review, exist when attaching documents. The plug-in will also offer to flatten or review documents attached to email addressed outside a user configurable security zone.

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 a list of articles and information regarding EDS, including previous editions of this newsletter, please visit:

<http://www.stg.srs.com/eds/>

For information about Document Detective electronic document review and sanitization toolkit, please visit:

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

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 2006 SRS Technologies