

## SCO Group and Alcatel Meta Data Examples

The SCO Group, famous for their recent lawsuit against IBM for releasing proprietary code into the Linux development environment, is the most recent example of the dangers of hidden data in electronic documents. Stephen Shankland and Scott Ard from CNet News reported the incident in a 4 March 2004 article entitled, "Document Shows SCO Prepped Lawsuit Against BofA." This article contains a fairly detailed description of the document's history and makes interesting reading. Read this article online at:

[http://news.com.com/2100-7344\\_3-5170073.html](http://news.com.com/2100-7344_3-5170073.html)

The article also claims that Microsoft Office 2003 addresses this problem and provides a feature to permanently remove hidden data. While MSO 2003 did add some new functionality, it still falls far short of what is needed, especially when protecting National Security Information. SRS has completed our analysis of MSO 2003, and we plan to release our results to this newsletter later this year.

The article also mentions a recent marketing study that was conducted by the Vanson Bourne firm entitled, "The cost of sharing." This was a commercial study, and was apparently funded by Workshare, a British company that is developing Meta data removal software. This study reports the following:

- 90% of documents in circulation began as something else, but 68% of respondents were not aware of that metadata -- hidden information within Microsoft Word files showing document amendments and author histories -- may still exist in the their document.
- 70% of companies have people external to the company contributing to document content, increasing security and information management risks.
- Two-thirds of companies engage in document collaboration with up to five people. The study also revealed that most collaborative groups are constantly changing, precluding consistent processes for collaboration. These collaboration challenges, among others, can lead to significant productivity losses, increased risk of missed deadlines, and impaired information security from hidden document metadata.

These are alarming statistics! Based on my personal experience in the military, I believe the Government situation is even worse. A link to the Workshare press release is provided below, but this is not an endorsement of their product. SRS has reviewed four commercial Meta data removal tools and the new Microsoft Remove Hidden Data plug-in, and none meet the rigorous Government requirements for sanitizing and reviewing electronic documents.

[http://www.workshare.net/news/ne\\_pressreleases\\_single.asp?pressID=81](http://www.workshare.net/news/ne_pressreleases_single.asp?pressID=81)

We have one more tidbit to report. This story is several years old, but the lessons are still pertinent. In April 2001, Nick Johnson published an article entitled, "Alcatel [Expletive Deleted]"

Up Bigtime,” in an online publication called *Morons in the News*. Again, the author shows in graphic detail how an international company embarrassed themselves using Microsoft Word.

<http://web.morons.org/article.jsp?sectionid=1&id=188>

SRS continues to make progress in our program to build the first electronic document sanitization and review system that was designed from the ground up to meet all of the U. S. Government’s statutory and regulatory requirements for protecting National Security Information. Unfortunately, we are still short of the full funding necessary to complete the project and field a system. More Government support is needed to make this system a reality before a serious incident occurs. Because of the nature of this hidden data threat, serious incidents may have occurred already, and we may never know if our adversaries are exploiting our vulnerability in this area.

Our business plan for developing solutions to this problem has always been one of soliciting contributions from many Government organizations so no one organization is saddled with the entire bill. In essence, we seek distributed contributions toward a system that will benefit all who need to transfer electronic documents across security boundaries.

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](mailto: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](mailto:rhackett@stg.srs.com)

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

Copyright 2004 SRS Technologies