

## **Microsoft Office 12 with XML will not improve Information Security**

Microsoft recently announced that their next version of Microsoft Office (Version 12) will use XML as their default file format. Many people have asked if this will reduce the threat of hidden information in electronic documents. While there are some small security benefits, the new documents will still be a significant threat to information security.

First, consider that Microsoft made the same announcement about Microsoft Office 2003 (Version 11) two years ago. Office 2003 does not use XML by default.

Microsoft sells new software by adding new features and functions. If the functionality of the new software was identical to the old software, there would be no reason to upgrade. If they do switch, you can be sure that the new file format will be at least as functional as previous versions. Those features and functionality are the root of the hidden data problem.

If XML becomes the default file format, Microsoft is likely to use much of what is now the "Save as Webpage" feature. When you export a document to a webpage, Microsoft saves enough information to the new XML document to completely regenerate the original Microsoft formatted document. I proved this by recreating the original PowerPoint presentation used to create the DOD 101 Website. All I did was enter the URL into the PowerPoint Open File dialog. It took a few minutes to recreate the original 16 megabyte presentation, but it was complete with embedded objects (included some OLE objects) and Meta data. The only things lost in the transition from PowerPoint to XML back to PowerPoint were the document fragments. Fragments are the unused (deleted) sections of the document that are still contained in the file.

There is also the issue of legacy documents and applications. Everyone will not upgrade to the latest Office version at the same time. Many people are still using older versions of Office, like Office 2000 (Version 9) and Office 97 (Version 8). These older versions may not be compatible with the new file type. For example, I received several compatibility warning messages when trying to save a test document in Web Archive format from Office XP.

Finally, XML and HTML have been improperly considered "safe" file types. It is actually very easy to lose information in a highly formatted web page. Cascading style sheets, conditional links, embedded scripts, tables and other formatting features can obscure information, and few users have the expertise to dig through the "code" to find this data. The SRS Electronic Document Security threat presentation includes one simple example of a keyword that is virtually impossible to find.

So the bottom line is that even if Microsoft implements an XML based file format in Office 12, there will still be significant security issues that will need to be addressed. Document Detective already has an XML/HTML review capability built in, so it will be up to the challenge of reviewing and sanitizing Microsoft Office 12 documents quickly. If you already own a license for Document Detective, you will get the new Office 12 format parser as soon as it is available.

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](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 2005 SRS Technologies