

IEEE Report on Meta Data

The Institute of Electrical and Electronics Engineers (IEEE) Computer Society has published an article by Simon Byers entitled, "Information Leakage Caused by Hidden Data in Published Documents" in their new *Security and Privacy* magazine. Simon Byers is a Senior Member of the AT&T Lab's Technical Staff. This article is important because it is a professional magazine for computer and software engineers, and it provides some statistics on the rate of hidden data occurrence in Word documents.

In his research, Mr. Byers uses an existing web crawler to collect Microsoft Word documents from the open Internet. The article reports collecting documents at a rate of approximately 1000 documents per hour using a cable modem. The "first" 100,000 documents took 16 gigabytes of disk space. The collection did not appear to be targeted at any particular organization.

Once the documents were downloaded, they were analyzed using open source tools. Several search algorithms are discussed, but the end results are extremely interesting. Approximately half of the 100,000 documents contained between 10 and 50 hidden words, one third contained 50 to 500 hidden words, and 10 percent contained over 500 hidden words. That's a whopping 93% incident rate of information being transmitted that is not intended for the recipient.

The article includes some suggestions for working around the problem, but those recommendations are far from adequate. While this is a very good article, it only addresses well-known Meta data issues. It does not address the other lesser known and often overlooked problems cited in SRS briefings and reports.

Unfortunately, this article is only available through IEEE's subscription services. You can obtain a copy through your library using the citation provided below. Before you go through a lot of trouble, I did locate an earlier version of the article that is available on the open Internet. That citation and a URL are also provided below.

Byers, Simon, "Information Leakage Caused by Hidden Data in Published Documents," IEEE Security & Privacy, Vol. 2, No. 2, pg 23-27, IEEE Computer Society, March/April 2004.

Byers, Simon, "Scalable Exploitation of, and Responses to Information Leakage Through Hidden Data in Published Documents," 3 April 2003. http://www.user-agent.org/word_docs.pdf

We have collected numerous additional articles that will be posted to the SRS EDS website as soon as we have reviewed them and determined their relevance to Electronic Document Security. The increasing number of articles indicates an increasing awareness of the problem, but there are still no credible solutions that will meet the Government's stringent requirements for protecting sensitive and classified information. While the U.S. Government and the DOD require a 100% reliable human review of all electronic documents crossing security boundaries, they have provided very little funding for programs and training to meet that requirement. There are numerous IT programs in the works to control access to information, but these programs make

assessing each document's content and assigning an appropriate security level the user's responsibility. SRS Technologies offers training that will allow Government/DOD employees to approach this task in a systematic, effective way, and we are developing software tools to assist in the review process. We have identified the need, and the solution is within our reach, but Government funding and support is needed to succeed.

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 2004 SRS Technologies