File Redirection for Restricted Processes

¡ Ensure that restricted processes, like MS Word sub-processes or Internet Explorer, will have access permissions for redirected data !

The Client Task

The client together with the Apriorit specialists develop a data security system that seamlessly redirects data to the hidden locations, encrypts them, and limits user actions. Administrator can configure rules for data processing.

Seamless redirection was on the agenda. The development team faced the issue when *.docx files downloaded from the Internet could not be opened by Microsoft Word 2010 while there were rules to redirect all new MS Office files to another secure location.

Brief research did not provide results while a quick bug resolution was required. So Apriorit research specialist started this task.

Research Task

The basic research request was to find out the cause of the issue. After preliminary research, the task was cleared out:

- To understand the specific of work with files downloaded from the Internet;
- To research in details the scheme of how MS Word creates temporary files;
- To provide the team with a recipe for fixing this issue.

Working On

First of all, the work with downloaded files was researched. When a file is downloaded from the Internet to the location within NTFS file system, OS adds one more file stream to it – so called “Zone.identifier”. When user opens such file in MS Word, the latter uses Zone.identifier to detect that this file was downloaded from the Internet and opens it in the protected mode with no editing permission. User can turn on editing manually and then MS Word re-opens the document in the standard mode.

The next step of research was about temporary file creation. Using specific system utilities, Apriorit specialist got the logs of all file operations performed by WinWord.exe at opening researched file. It was discovered that WinWord.exe creates a sub-process with Integrity Level = Low, so-called “restricted” process, which in its turn creates temporary files in the specific MS Office sub-folder.

The client’s solution includes file system mini-filter driver that, as was mentioned, seamlessly redirects all newly created files from the MS Office folders to another location. The researcher supposed that access permissions for the initial folder gave restricted processes possibility to write there, while the target location did not.

This hypothesis was checked by reconstructing the situation for testing folders, files, and processes for various combinations of actions and permission sets, and it was finally confirmed. These experiments also gave the details about security informations that had to be copied from initial location to the target folder so that the issue was resolved.

Results

Research took 3 man-days, and after that the team got the answer how to fix the issue. All works for researching and fixing the bug took a week, so the client had the new version pretty soon.

This issue and obtained solution were included to the Apriorit knowledge base: when you create a software that supposes file redirection, you should remember about the restricted processes and their specific needs to access data.

What’s next?

Get the **free estimation** of time and effort for your research task! Unlike many R&D service providers, we understand the specifics of research projects and completely rely on the professional skills of our specialists. So it won’t be just one phrase with the total sum and dead line.

Apriorit free research estimation pack includes:

- Basic task dropdown with the research approaches indicated;
- Each task-approach time & effort estimation supported by our broad research project experience;
- Prototype development estimation.

After we’ve received your request for proposal, usually it takes 2-7 business days to prepare the estimation for your task.

¡ So let’s start solution search right now with a zero-risk estimation stage !

All we need to start is a brief research task description sent to the info@apriorit.com with “RFP” mentioned in the subject.