Project Report

**Introduction:**

Windows users usually find some ads popping up on their screen. In most of cases the users cannot find out which program pushed such ads and hence they cannot remove the ads permanently. Many malwares sneak into computers like the Ads software. The file system of Windows allows all software to get access to most of files in disk (although there is restriction according each user), which give the malwares chance to hide in you disk.

This project aims to make a virtual file system that forces all file operation to be signed by software. I believe that such file system could help developers to think about how to stop malware by enforcing digital signature on files and operation.

**Assumption:**

In order to develop the possibility of such design, following assumption is made in this project:

1. All software must get permission from this system service if they want to get access to files in system.
2. All software will sign the files after operating files, with the private key assigned by the system service.

**Design:**

The software is designed as a system service, it would authorize and keep record of all file operation made by software, hence it should have following functionalities:

1. Assign private to software
2. Authorize file operation of software that has effective private key
3. Deny file operation of software without has effective private key
4. Help users control effective private keys
5. Scan file system to ensure each software sign the files correctly

Considering about its working scenario, the system service should have following features:

1. Low resource consumption.
2. Has absolute control over file access

A flow diagram is included in the end of this report that introduce the logic of this system service.

**Implementation:**

Following modules are required for this whole project to run:

1. Monitor:
   1. Monitor changes to file system and keep a log for any changes. (Finished)
   2. Process file operation request.
2. Digital Signature:
   1. Generate private key for software to provide file operation permission. (Finished)
   2. Verify request made by software by verifying signature (Finished)
3. API:
   1. Allow software to request a private key
   2. Allow software to request a file operation
   3. Allow software to deactivate a private key

The project can be found in following GitHub repository:

<https://github.com/Deliangus/SignEnfoceFile>

**Difficulties:**

Enforcing signature aims to let users know all software that has gained access to a file. Obviously, the signature must become part of the file so that the file itself explained its history. However, making the signature an appendix of the file is not practical because the signature can be modified in this way. So, the signature must be protected by signature itself, which results in a looping. I haven’t figure out how to process such logic loop.

**Conclusion:**

In order to make this system works, system developers need to force all software developers to register their software (locally to their system only or globally to some certificate authorization), which many of them have been doing this for decades.

However, this system is not practical on Windows as Windows system has been supporting software that are developed in last century. And applying this service to Windows might cause many old software to stop working.

From other point of view, this methodology could help in building a critical zone that all files are encrypted in system. By creating such critical zone, the users can control the access to content of files (although not controlling access to the file).

