Chaque processus possède un niveau d'intégrité mais aussi le processus enfant qui hérite du niveau d'intégrité du processus l'ayant "enfanté". Ces niveaux d'intégrité sont appelés *Integrity access Levels* ou IL.

Signalons que le niveau d'intégrité est associé à la SACL et non à la DACL.

Un processus ne peut interagir avec un niveau d'intégrité possédant des privilèges plus élevés. Les API (*Application Programming Interface*) échoueront à partir d'un processus possédant un niveau d'intégrité faible quand il sera utilisé contre un processus d'un niveau d'intégrité plus élevé. Ceci étant fait pour éviter les risques d'attaques ou d'intrusions malveillantes.

Les entrées du Registre peuvent seulement être écrites à partir d'un processus possédant un fort niveau d'intégrité. C'est pourquoi Internet Explorer (processus d'intégrité faible) ne vous permet d'écrire que dans des portions congrues de l'Explorateur ou du Registre Windows.

Les niveaux d'intégrité sont les suivants :

- **High (haut)** : correspond aux privilèges système d'administrateur. Ce niveau de privilèges vous donne le droit d'écrire dans le répertoire \Program Files et la branche du Registre HKEY_LOCAL_MACHINE.
- **Medium (moyen)** : correspond au niveau Utilisateur. Ce niveau de privilèges vous donne le droit d'écrire dans votre répertoire d'utilisateur et la branche du Registre HKEY_CURRENT_USER.
- **Low (faible)** : ce niveau ne vous permet que d'écrire dans les zones sans niveau de privilèges comme la clé HKEY_CURRENT_USER\Software\LowRegistry ou les répertoires nommés LOW et qui sont présents dans l'Explorateur Windows. Par ailleurs, une fonctionnalité appelée "Interface utilisateur d'isolation des privilèges" (*User Interface Privilege Isolation* ou UIPI) vient renforcer ce dispositif et ce afin de prévenir les attaques de type "Escalade des privilèges".

Windows 8 a ajouté aux niveaux d'intégrité précédents le niveau d'isolation **AppContainer**, également présent dans Windows 10. Ce niveau d'isolation est celui utilisé par défaut pour l'exécution des applications Windows Store.

3. L'élévation de privilèges

Certaines opérations ne sont pas adaptées à l'utilisation des listes de contrôle d'accès. Imaginons qu'un utilisateur ait besoin de sauvegarder un ensemble de fichiers, il est beaucoup plus simple de lui accorder le privilège de sauvegarde quelles que soient les permissions NTFS attachées aux fichiers plutôt que de modifier un à un le masque des permissions de chacune des ressources auxquelles il peut accéder. Un processus peut recevoir une élévation de privilèges dans les circonstances suivantes :

- Si l'application est une plate-forme d'installation comme Windows Installer ou Install Shield.
- Si l'application possède une entrée dans la couche de compatibilité des applications ou la base de données de compatibilité des applications.

Dans le premier cas, une entrée sera présente dans cette arborescence du Registre : HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store.