Le contrôle de compte d'utilisateur

Windows Vista a introduit un nouveau concept de sécurité appelé UAP ou *User Account Protection* (en français, contrôle de compte d'utilisateur). D'autres termes sont utilisés : *Least-Privilege User Accounts* ou *Limited User Accounts* (LUA). Ce concept, désormais appelé UAC (*User Account Control*), a été conservé et amélioré dans Windows 7 puis dans Windows 8 et finalement dans Windows 10, pour qu'il apparaisse moins contraignant pour l'utilisateur. Cette fonctionnalité permet de limiter le champ d'action des logiciels malveillants.

Les utilisateurs créés par Windows ont le statut d'administrateur protégé, c'est-à-dire que la fonctionnalité UAC est activée pour ces comptes. Ce n'est pas le cas du compte Administrateur qui désigne le compte intégré au système d'exploitation mais qui, par défaut, est désactivé.

Quand un utilisateur a le droit d'interagir sans restriction avec le système, il peut installer une application, écrire dans la branche du registre HKEY_LOCAL_MACHINE, installer des périphériques, démarrer des services, etc.

En mode protégé, tous les processus initiés par un administrateur sont lancés avec un minimum de privilèges. Si, par exemple, vous ouvrez un programme à partir du menu **Démarrer**, l'application va s'exécuter dans un contexte restreint avec les mêmes privilèges que ceux qui vous ont déjà été accordés.

Si l'application requiert pour pouvoir s'exécuter convenablement, des privilèges élevés, il faudra, dans ce cas, que le compte d'administrateur puisse exécuter le processus de manière non restrictive. Le processus hérite alors des nombreux avantages accordés par cette élévation de privilèges (*Over The Shoulder* (OTS) *elevation*). Quand un programme nécessite de s'exécuter en mode d'élévation de privilèges, une boîte de dialogue vous en avertit. Il n'y a donc pas, par défaut, de possibilité d'élever les privilèges accordés à une application sans le consentement éclairé de l'utilisateur. Nous allons voir dans la suite de cette section qu'il est désormais possible, dans Windows, de désactiver la demande de confirmation du processus d'élévation de privilèges.

Notez toutefois que le service reste actif même lorsque vous sélectionnez le paramètre le moins sécurisé pour cette fonction.

1. Les comptes d'utilisateurs

À chaque fois que vous ouvrez une session d'utilisateur, un jeton d'accès (*token*) vous est attribué. Ce jeton d'accès dresse la liste des privilèges dont vous disposez et énumère les ressources auxquelles vous accédez ou tentez d'accéder. Chaque ressource disponible sur le système possède une liste de contrôle d'accès (DACL) qui tient la liste des utilisateurs et des services pouvant l'atteindre, ainsi que le niveau de permission qu'ils possèdent.

Par défaut, les administrateurs reçoivent deux jetons d'accès :

- Un jeton en tant qu'administrateur.
- Un jeton en tant qu'utilisateur standard et c'est ce dernier qui est attribué par défaut.

Lors de l'élévation d'un processus, un utilisateur reçoit les mêmes privilèges que ceux de l'administrateur. En d'autres termes, il obtient le même jeton d'accès. Le mécanisme qui vous permet de passer d'une identité à l'autre est appelé *Admin Approval Mode* (AAM).

2. Les niveaux d'intégrité

Le contrôle d'intégrité (MIC ou *Mandatory Integrity Control*) est un autre mécanisme apparu sous Vista. Il est contrôlé par une liste de contrôle d'accès ACE dans la liste système de contrôle d'accès (SACL) de tout objet "sécurisable" (clé du Registre, fichier, processus, etc.).