The Sierra Conjecture

ou tout ce que vous voulez savoir sur le GateKeeper sans jamais oser le demander

Karim Haddad
IRCAM,
repmus

16 janvier 2018

1 Introduction

1.1 Avant-propos

Toutes ces informations reposent sur Sierra et non High-sierra[1]. La plupart de celles-ci sont issues du net et sont testées sur une machine virtuelle Sierra.

1.2 Gatekeeper

Gatekeeper est une nouvelle fonction apparue dans l'OS d'Apple à partir de la version OS X 10.8, Mountain Lion, un outil pensé pour la sécurité des utilisateurs. Or, au fur et à mesure cet outil est devenu, entre autre, un outil de contrôle d'installation des "packages" d'applications venant de Apple (Apple-store), ou signées numériquement par un identifiant de développeur Apple,

À l'origine, Gatekeeper dispose de trois options :

— Autorisation d'installation d'application venant exclusivement du Mac Apple Store
— Autorisation d'installation d'application venant de Mac Apple Store et développeurs identifiés
— Autorisation d'installation de toute application signée ou non signée

Figure 1.1: Dialogue Gatekeeper de Mountain Lion

1. je ne dispose pas de machine high sierra.

À partir de Sierra, Apple ne propose plus la troisième option. Il n'est plus possible de la choisir à travers l'interface graphique du dialog :

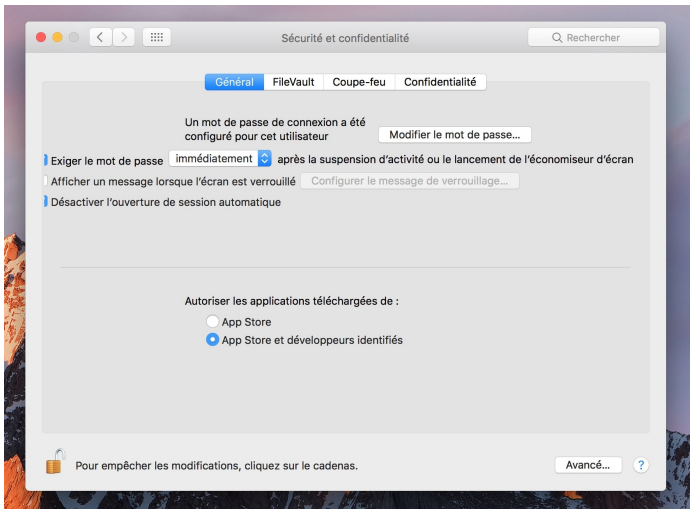

Figure 1.2: Dialogue Gatekeeper de Sierra

Avec la dernière mise-à-jour de Sierra, Gatekeeper est encore plus bridé. Pour l'activer, il faut être un utilisateur "expert". *"Une ligne de commande devrait toutefois permettre de retrouver le réglage que l'on avait auparavant dans l'interface d'OS X. De fait, ce que Sierra retire, c'est surtout l'option affichée et facile à activer. Les utilisateurs avancés qui souhaiteront ouvrir n'importe quelle application pourront toujours le faire, mais ce sera un frein de plus pour le grand public. Apple incite de plus en plus les développeurs à certifier leurs logiciels, ce qui est payant."* [1]

1.3 La Apple Policy

Sur le site apple.com, nous pouvons lire sous la rubrique **Gatekeeper sécurise le téléchargement des apps.** :

Gatekeeper s'assure que vous n'installez pas de logiciels malveillants par mégarde lorsque vous téléchargez des apps sur votre Mac. Le Mac App Store est encore l'endroit le plus sûr pour télécharger des apps. Apple passe chaque app en revue avant qu'elle soit acceptée par le Store. Et si une app présente le moindre problème, elle peut être retirée rapidement. Gatekeeper sécurise également tous vos téléchargements de logiciels sur Internet, quelle que soit leur provenance. Apple fournit aux développeurs un Developer ID unique qui leur permet de signer numériquement leurs apps. Grâce à

cet identifiant, Gatekeeper peut bloquer les apps conçues par des développeurs malveillants et s'assurer que les apps n'ont pas été falsifiées. Et il peut protéger votre Mac en empêchant l'installation d'apps conçues par des développeurs inconnus, qui ne sont pas identifiés par un Developer ID.
Gatekeeper vous procure davantage de contrôle sur ce que vous installez. Gatekeeper vous offre deux options de sécurité. L'option par défaut vous permet de télécharger des apps du Mac App Store et d'autres sources signées au moyen d'un identifiant Apple. L'autre option consiste à installer exclusivement les apps provenant du Mac App Store, la source de téléchargement la plus sûre pour votre Mac. Lorsqu'une app ne porte pas de signature numérique, Gatekeeper empêche son installation et vous informe qu'elle ne provient pas d'un développeur approuvé. Néanmoins, si vous êtes certain que l'app est fiable, vous pouvez manuellement passer outre Gatekeeper en faisant un Contrôle + clic sur l'app pour l'ouvrir.[2]

2 “How-to”

2.1 Déverrouillage du Gatekeeper sous Mountain Lion OSX 10.8

Pour les OS Mountain Lion et Lion, la procédure de déverrouillage d’autorisation d’installation des logiciels est bien simple :

1. Ouvrir Menu Apple > Préférences Système > Sécurité et confidentialité > Onglet Général.
2. Cliquer sur le cadenas. Il vous sera demandé votre mot de passe d’administrateur.
3. Choisir « N’importe où ».

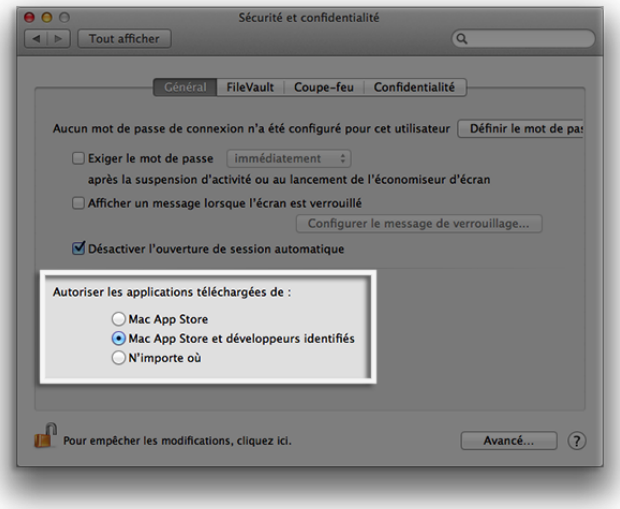

Figure 2.1: Sécurité et confidentialité

Remarque : sous OS X Lion 10.7.5, Gatekeeper est réglé par défaut sur « N’importe où »

2.2 Système "D" - Sierra

À partir des OS Sierra, la procédure est plutôt réservée aux utilisateurs expert. Dans cette section on guidera l'utilisateur expert afin de contourner la limitation du contrôle d'installation Apple sur Sierra.

1. Allez dans le Finder, Applications et sous Utilitaires lancez le Terminal Mac.
2. Entrez ou copiez-collez la ligne de commande suivante puis la touche Entrée et votre mot de passe administrateur :
   sudo spctl -master-disable

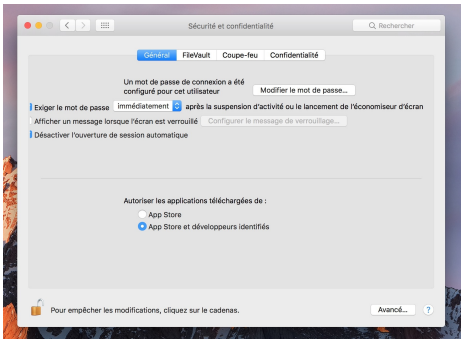

Figure 2.2: Terminal commande disable

Retournez dans les Préférences Système, Sécurité et confidentialité et sous l'onglet Général. Vous constatez maintenant que sous Autoriser les applications téléchargées de :, l'option « N'importe où » est de retour ! Il suffit de déverrouiller le cadenas en bas à gauche à l'aide de votre mot de passe administrateur et de cocher la case « N'importe où » comme on l'a déjà décrit plus haut 2.1. Désormais toutes les apps s'ouvriront sous macOS Sierra (10.12), celles de l'App Store, celles de développeurs identifiés et toutes les autres (UnrarX, Transmission, uTorrent...).

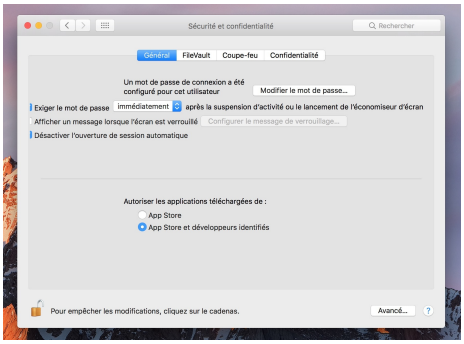

Figure 2.3: Dialogue déverrouillé

Pour retourner au niveau de sécurité initial de GateKeeper :

Ouvrir une fenêtre du Terminal et de taper littéralement la commande suivante :

sudo spctl -master-enable

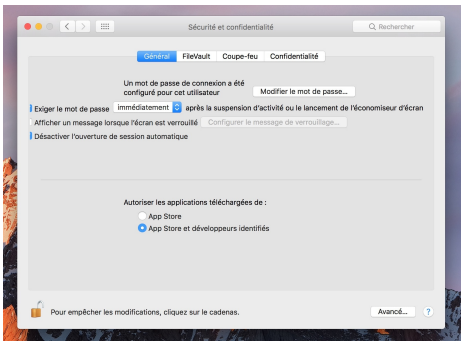

Figure 2.4: Terminal commande enable

Vos Préférences de sécurité ressembleront comme au départ, à la fenêtre ci-dessous :

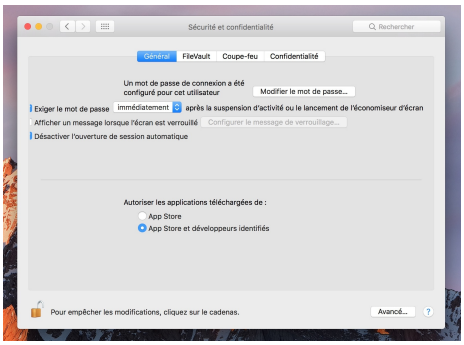

Figure 2.5: Dialogue vérouillé

2.3 Système “D” plus - Sierra

On peut faire face selon l’application à une réticence intempestive du OS qui nous contraint à répéter la manipulation vue plus haut à chaque lancement du logiciel. C’est le cas très probablement de High Sierra.Pour se faire il faudrait autoriser définitivement l’application en question sur sa propre machine. Attention, cette démarche est réservée aux utilisateurs experts et certainement pas aux novices.

1. Ouvrir un terminal
2. Saisir cette commande :
   spctl -add /Path/To/Application.app
   où Application.app est l’application en question.
3. Saisir le mot de passe de l’utilisateur ou utiliser sudo.

Pour enlever l’exception il faut utiliser cette ligne de commande :

1. Ouvrir un terminal
2. Saisir cette commande :
   spctl -remove /Path/To/Application.app
   où Application.app est l’application en question.
3. Saisir le mot de passe de l’utilisateur ou utiliser sudo.

2.4 Remarques

Pour toute remarque concernant ce documents, s’il vous plaît adresser vous à la liste des utilisateurs du forum : `http://forumnet.ircam.fr/user-groups/`.

Bibliographie

[1] N. Furno. Gatekeeper :sierra n'acceptera que les logiciels signés. https://www.macg.co/os-x/2016/06/gatekeeper-sierra-nacceptera-que-les-logiciels-signes-94565?page=2, 2016. [Online ; accessed 14-January-2018].

[2] A. Inc. La sécurité.directement intégrée. https://www.apple.com/fr/macos/security/, n/a. [Online ; accessed 14-January-2018].

[3] A. Inc. Os x : à propos de gatekeeper. https://support.apple.com/fr-fr/HT202491, n/a. [Online ; accessed 15-January-2018].