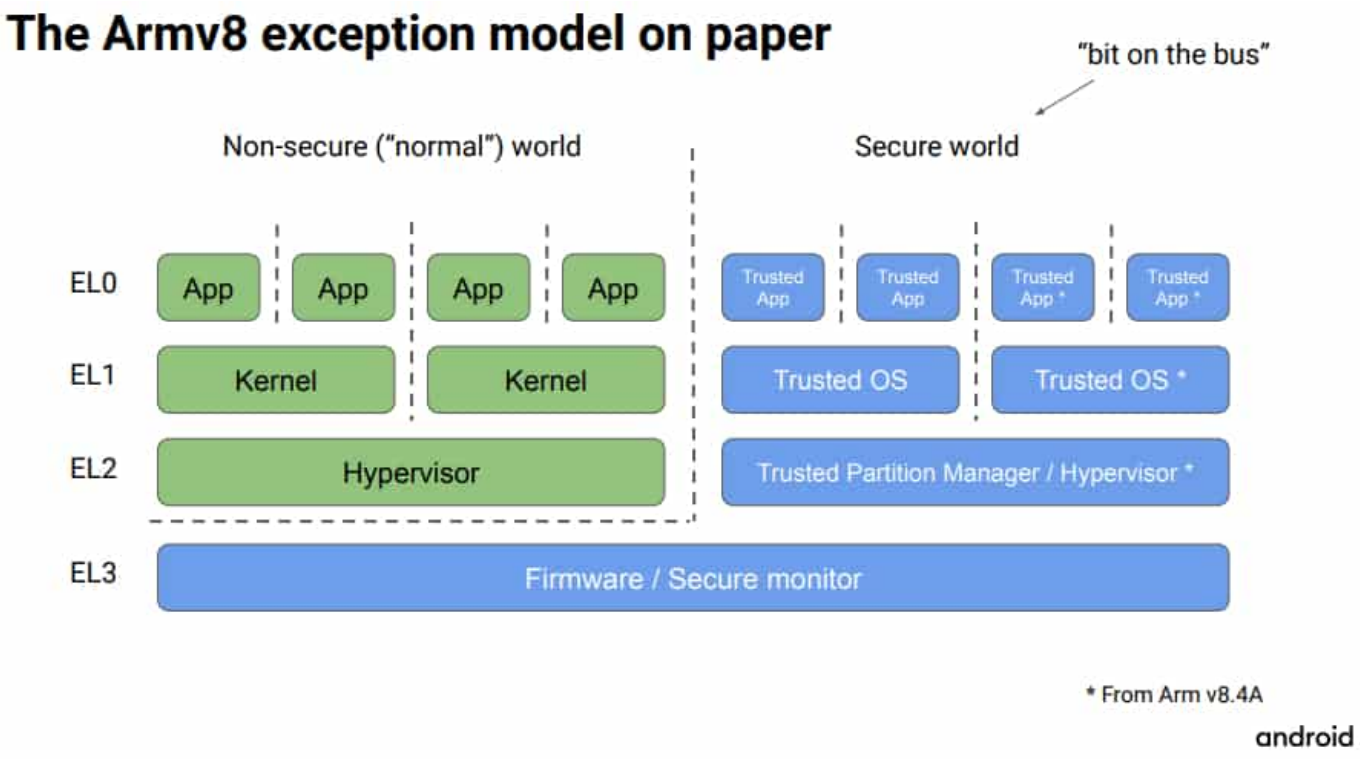
Microdroid : un nouvel entrant dans la stratégie virtualisation de Google

Comment Microdroid va-t-il s'imbriquer dans la stratégie de Google ? Le nom* vient d'apparaître dans une série de *commits* sur le projet AOSP. Il fait référence à une version allégée d'Android basée sur une GSI (image système générique) et destinée à un usage dans des VM.

Il est tentant d'établir un lien avec les travaux que le groupe américain mène pour porter KVM (hyperviseur du noyau Linux) sur Android.
Une présentation faite dans le cadre du KVM Forum 2020 – et dont sont issues les illustrations ci-dessous – résume la situation. Dans les grandes lignes, il s'agit d'adapter l'hyperviseur pour proposer une alternative au modèle d'exceptions d'Armv8.

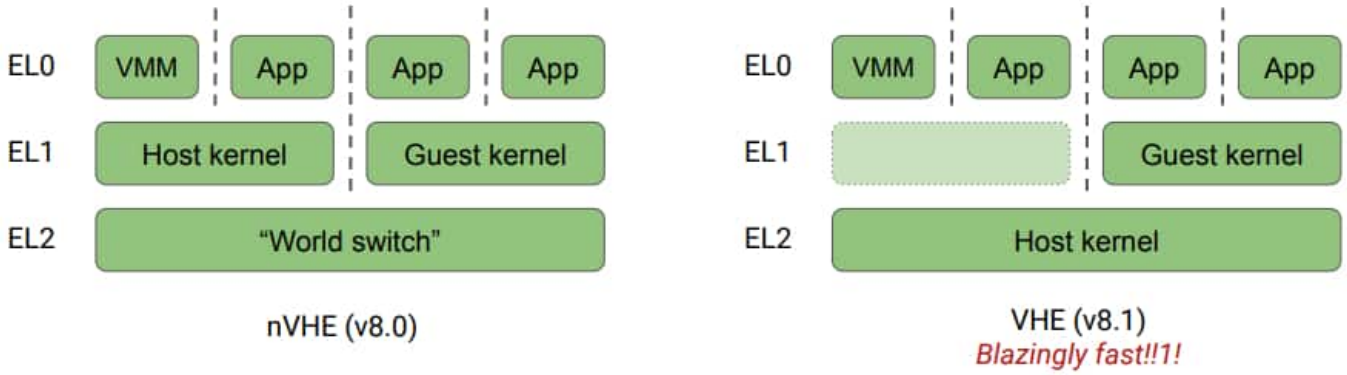
Ce modèle implique, d'une part, quatre niveaux de privilèges : utilisateur (EL0, le plus bas), OS (EL1), hyperviseur (EL2) et *firmware* (EL3). Et de l'autre, deux environnements : le code « non sécurisé » et le code « de confiance ». Le premier est ouvert au second, indépendamment des niveaux de privilèges. Un OS « de confiance » peut par exemple accéder à la mémoire d'un hyperviseur « non sécurisé ».



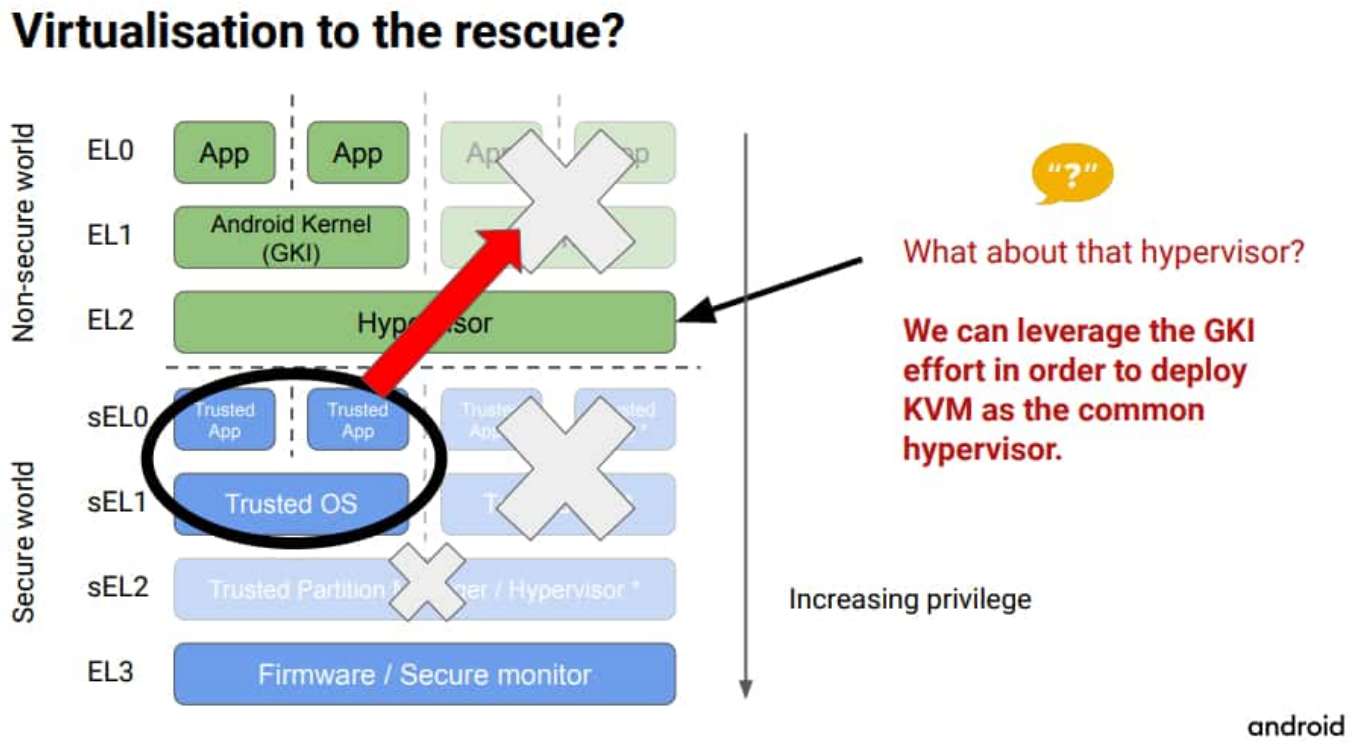
Mais le code dit « de confiance » l'est-il vraiment ? Des modules DRM aux bibliothèques de cryptographie, de nombreux composants sujets à caution s'exécutent dans cet environnement.
Pour en limiter l'impact potentiel, on peut envisager de les placer dans des VM isolées de l'OS et exécutées au même niveau de privilèges. Avec KVM pour jouer le rôle d'hyperviseur.

Microdroid, KVM… et crosvm

KVM peut tirer parti de la fonctionnalité VHE (Virtual Host Extensions), arrivée avec Armv8.1. Elle permet d'exécuter le noyau hôte en EL2 et les noyaux invités en EL1, sous forme de VM.
Cette approche induit la possibilité, pour l'hôte, d'accéder la mémoire des invités. Dans ce contexte, le projet d'adaptation de KVM se passe des VHE. Il met hôte et invités au même niveau (EL1) et fait intervenir un gestionnaire de VM, seul à bénéficier d'une pleine confiance (EL2).



Pour développer ce gestionnaire, on ne part pas de rien. On s'appuie en l'occurrence sur crosvm. Déjà inclus dans AOSP, il permet de faire tourner des applications Linux sur Chrome OS par l'intermédiaire d'une VM Debian (projet Crostini).



On surveillera d'éventuelles jonctions avec l'hyperviseur natif intégré au SoC Snapdragon 888 de Qualcomm. Voire avec le projet ARCVM, dans le cadre duquel Google cherche à étendre l'approche crosvm aux applications Android.

** On donne parfois le nom de « MicroDroid » aux employés de Microsoft.*

Illustration principale © Google