Firmwares

SE302

Samuel TARDIEU
samuel.tardieu@telecom-paris.fr
Septembre 2019

Qu'est-ce qu'un *firmware* ?

On appelle généralement **firmware** (ou **micrologiciel**) le code qui s'interface avec le matériel d'un système, embarqué ou non, comme par exemple :

- sur PC, le BIOS (*basic input/output system*) ;
- sur PC, les chargeurs lancés par UEFI (*unified extensible firmware interface*) ;
- sur un système embarqué, le code applicatif.

Certains utiliseront d'autres définitions :

- le code qui se trouve en ROM/flash par opposition au code chargé depuis un disque (même SSD) ou le réseau ;
- tout code chargé systématiquement au démarrage de l'appareil et qui n'a pas vocation à changer souvent.

Firmware et mise à jour

- Un firmware qui ne peut pas être mis à jour ne permet pas *a priori* la correction de bugs logiciels ou les évolutions.
- Cette absence de mise à jour peut être voulue (Yubikey).
- Certains firmwares chargent et utilisent des tables en RAM permettant de dérouter à l'exécution certaines fonctionalités (cartouche Basic du Thomson TO7 par exemple) et d'en corriger les bugs.
- Un bug critique nécessite un retour de l'appareil en usine pour mettre à jour le firmware en utilisant des équipements spécialisés si la mise à jour sur le terrain n'est pas possible.

Mise à jour douloureuses

En 2015 :

- Des bugs sont trouvés dans le firmware des voiture Jeep permettant d'en prendre le contrôle à distance. 1,4 millions de voiture sont rappelées pour une mise à jour.
- Toyota a rappelé 625.000 voitures Prius hybrides dont les moteurs pouvaient s'arrêter subitement.
- Jaguar Land Rover a rappelé 65.000 voitures dont les portes étaient susceptibles de se déverouiller spontanément.
- Ford a rappelé 433.000 voitures qui avaient un risque de ne pas pouvoir être arrêtées même en en retirant la clé.

En 2016, General Motors a rappelé plus de 4 millions de voiture dont les airbags et tenseurs de ceintures risquaient de ne pas se déclencher.

Procédés de mise à jour

- La mise à jour du firmware peut nécessiter une connexion (USB par exemple) et une reprogrammation de certaines zones de stockage (`fastboot` et `adb` sur Android).
- La mise à jour peut se faire *over the air* (OTA), après une sollicitation de l'utilisateur, une validation de l'utilisateur ou sans demande de l'utilisateur.
- Par abus de langage, on parle de mise à jour OTA pour toute mise à jour à distance initiée par l'appareil même lorsqu'une connexion physique existe (set-top-box par exemple).

Risque des mises à jour sur le terrain

La mise à jour sur le terrain (physique ou OTA) comprend des risques :

- possibilité de rendre l'appareil inutilisable (on parle de *briquer* l'appareil) ;
- possibilité de charger un firmware non autorisé, révélant des secrets, ajoutant/débloquant des fonctionalités non inclues à l'origine ou permettant l'accès à des zones normalement interdites par convention avec des tiers (DRM) ;
- risque pour l'utilisateur mal informé de charger un firmware malveillant ;
- possibilité pour des tiers d'installer un firmware malveillant (surveillance, renseignement économique).

Un ou plusieurs firmwares ?

Plusieurs firmwares peuvent être installés à un moment donné sur le même appareil. Par exemple, sur Android, on trouve généralement :

- le système Android lui-même ;
- le *recovery*, qui permet des manipulations scriptées du contenu de la mémoire flash en utilisant les systèmes de fichier de l'appareil, la manipulation de la table de partitions, le formattage d'une partition ;
- le *bootloader*, qui permet de reprogrammer la mémoire flash, notamment la partition contenant le *recovery* ;

Parfois un firmware d'urgence permet de réinstaller un *bootloader* fonctionnel depuis une zone de mémoire immuable en cas d'écrasement ou de dysfonctionnement de celui-ci (Freebox power cycle $\times$ 5).

Des firmwares plus discrets

- Deux firmwares supplémentaires (au moins) se trouvent dans tous les téléphones : le modem (exécuté par un processeur auxiliaire et souvent un DSP, systématiquement propriétaire) et la carte SIM (processeur + firmware + application).
- Des commandes peuvent être envoyées à travers le réseau GSM à la carte SIM.
- La carte SIM peut envoyer des commandes au modem.
- Le modem est directement connecté à certains périphériques (radio, GPS, micro, WiFi, BlueTooth), et à travers une interface au système principal.

Il est possible d'accéder à ces périphériques (radio, GPS, micro, WiFi, BlueTooth) depuis des commandes envoyées par le réseau GSM.

Des firmwares spécialisés

Certains éléments sont séparés du processeur principal et possèdent leur propre firmware pour des raisons de sécurité. Exemple du Titan M dans les Google Pixel 3 (octobre 2018) :

- circuit dédié en charge de la sécurité ;
- seul détenteur des secrets de l'utilisateur, seul capable de vérifier qu'un mot de passe est correct avant d'effectuer certaines opérations de déchiffrage et de signature ;
- force à attendre en cas d'authentification incorrecte ;
- n'accepte que des firmwares signés, et **en présence du mot de passe de l'utilisateur** ;
- attend un appui physique sur un des boutons auxquels il est relié électriquement avant d'effectuer certaines opérations d'authentification (FIDO2).

Bootloader et signature

Le bootloader peut être chargé de vérifier l'intégrité de ce qui est chargé en mémoire ou programmé en mémoire flash :

- L'image programmée en mémoire flash peut être validée lors de l'écriture grâce à une signature cryptographique (cryptographie symétrique ou asymétrique).
- L'image chargée depuis la mémoire flash peut être elle aussi vérifiée avant l'exécution.
- Le bootloader peut essayer de valider sa propre image et s'arrêter s'il s'estime corrompu.

Dans certains cas, des obligations contractuelles obligent le fabricant à vérifier l'authenticité du firmware (solutions DRM des set-top-box).

Récupération OTA et installation

- Le chargement de la mise à jour peut être complet (en général compressé) ou partiel (différence par rapport à la version installée), continu (connexion réseau) ou opportuniste (petits paquets échangés).
- La mise à jour du bootloader (si nécessaire) peut se faire depuis le firmware en cours après vérification de l'intégrité et possiblement de la signature cryptographique.
- Possibilité de basculement atomique de l'ancien bootloader sur le nouveau par le changement d'un mot mémoire.
- Un redémarrage en mode bootloader finalise la mise à jour après vérification de l'intégrité et possiblement de la signature cryptographique.

Mise à jour OTA et partition A/B

Depuis Android 9, un système avec deux partition A/B peut être utilisé :

- L'ensemble *recovery* et système Android (noyau et applications préinstallées) est stocké dans une même partition.
- Il existe deux exemplaires de ce type de partition appelées *A* et *B*. À tout moment, une seule partition est active (par exemple *B*) et le bootloader démarre dessus.
- Lorsqu'une mise à jour est disponible, la partition active est copiée dans l'autre (ici de *B* vers *A*) et la mise à jour est appliquée sur *A*, pendant que le téléphone fonctionne normalement.
- Le bootloader est reconfiguré pour que *A* devienne la partition active lors du prochain redémarrage.

Vérification de la mise à jour

- Si le stockage le permet, présence de l'ancienne version du firmware et de la nouvelle en même temps sous forme exécutable.
- But : pouvoir revenir en arrière si le nouveau firmware ne parvient pas à redémarrer.
- Stockage en RAM d'un *magic number* demandant à booter sur la nouvelle version.
- Le bootloader vérifie cet emplacement, l'efface et éventuellement boote sur la nouvelle version à la place de la version configurée.
- À la fin de la phase de boot, écriture définitive de l'adresse du nouveau firmware dans la configuration du bootloader pour le conserver.

Versions signées et sécurité

Un firmware signé n'est pas une garantie de sécurité absolue :

- Si de la cryptographie symétrique est utilisée, la clé peut être trouvée sur l'appareil.
- Si de la cryptographie asymétrique est utilisée, la clé peut éventuellement être trouvée sur un serveur de développement.
- Si la clé est programmée, une perturbation du bus (ou de l'EEPROM ou de la flash contenant la clé) permet de la remplacer par une autre.
- De nombreux bootloaders permettent de charger une ancienne version (signée) du firmware contenant des bugs corrigés depuis.

Versions signées et bugs

Un firmware signé n'est pas une garantie d'absence de bugs :

- Certains jeux WII ont des débordements de buffer lors du chargement des sauvegardes mal formées : possibilité d'installer des programmes non autorisés *(homebrew channel)* en exploitant ces bugs.
- Certaines versions du firmware de la WII ont un débordement de buffer lors du chargement de "lettres" échangées entre WII signées avec l'adresse Mac de la console. Une lettre mal formée exploite ce bug et autorise le homebrew channel.

Vérification des signatures

- La signature doit être vérifiée au plus près de l'exécution.
- Les vérifications lors des étapes intermédiaires (chargement, programmation) ne servent qu'à éviter une erreur fatale plus tard.
- Les données sensibles (secrets) ne devraient être accessibles que par des firmwares spécialisés dans des zones réservées (*trust zone*) dont la reprogrammation efface le contenu des données.

Faire un firmware sécurisé est difficile

Source : Amazon

Amazon Dash Button v1 :

- pins du SWD accessibles $\Rightarrow$ pwned
- console série accessible $\Rightarrow$ pwned

On peut essayer d'améliorer : v2

La v2 a été renforcée :

- SWD désactivé $\Rightarrow$ bien
- console série inintéressante par défaut $\Rightarrow$ bien
- flash SPI avec copie du firmware, mais sans les secrets (flash interne uniquement) $\Rightarrow$ récupération du firmware
- chargement du firmware sur le même microcontrôleur $\Rightarrow$ analyse du firmware facilitée
- débordement de buffer identifié dans le protocole audio permettant de configurer la v1 et toujours présent $\Rightarrow$ construction d'un fichier audio exploitant le débordement de pile et dumpant les secrets sur le port série
- secrets accessibles et activation du SWD $\Rightarrow$ pwned

Conclusions

- Un firmware doit pouvoir être mis à jour sans renvoi de l'appareil.
- Une mise à jour ne devrait pas pouvoir briquer l'appareil sans possibilité de récupération automatique.
- Une mise à jour ne devrait jamais pouvoir briquer l'appareil sans possibilité de réparation par l'utilisateur.
- Des efforts importants doivent être mis pour sécuriser le firmware et les données de l'utilisateur.
- Il ne faut pas espérer que les protections du firmware préserveront l'intégrité du code qui tourne sur l'appareil dans tous les cas.