Ultrablue : contrôle d'intégrité du démarrage d'un PC via Bluetooth

Ultrablue (User-friendly Lightweight TPM Remote Attestation over Bluetooth) est une solution permettant à des utilisateurs d'attester l'intégrité du démarrage de leur ordinateur à partir d'un téléphone. Elle se compose d'un serveur, qui s'exécute sur l'ordinateur et joue le rôle d'attesteur, et d'un client graphique, qui s'exécute sur un téléphone de confiance et joue le rôle de vérificateur.

Un cas d'usage typique est de vérifier l'intégrité de la chaîne démarrage avant d'entrer son mot de passe pour déverrouiller un ordinateur, afin d'éviter des attaques hors-ligne sur un PC portable laissé sans surveillance. Il est également possible d'utiliser Ultrablue en tant qu'outil de débogage du *measured boot*, par exemple après des mises-à-jour de *firmware* (BIOS/UEFI), ou encore comme second facteur pour le chiffrement du disque.

L'utilisation d'Ultrablue se fait en trois étapes :

1. **Enrôlement** : échange d'une clé pour chiffrer la communication par l'intermédiaire d'un QR Code et enregistrement de l'identité de la machine attestée et des mesures de référence dans le téléphone.
2. **Intégration au démarrage** dans l'*initramfs* (optionnel) : utilisation d'un secret retourné par le téléphone comme facteur de chiffrement du disque et lancement d'Ultrablue lors du démarrage de la machine pour permettre la récupération de ce secret.
3. **Attestation** : vérification de la concordances des mesures signées par le TPM avec les mesures de référence, affichage du résultat sur le téléphone et renvoi du secret de déchiffrement de disque le cas échéant.

Une machine virtuelle est fournie démontrant ces trois étapes, et son utilisation est détaillée ci-dessous.

Installation

Prérequis

Pour suivre ce tutoriel, il vous faut :

- un ordinateur utilisant une distribution Linux à jour (architecture `x86_64`), équipé d'une interface Bluetooth matérielle, et sur lequel vous avez les droits d'administration,
- un téléphone portable Android.

Le tutoriel a été testé sur Android 13 pour la partie client, et les distributions suivantes pour la partie serveur : Debian unstable, Kali, Fedora 37, Archlinux.

Android

Vous pourrez récupérer un paquet Android `ultrablue.apk` depuis la dernière page de release d'Ultrablue.

Copiez `ultrablue.apk` sur votre téléphone par la méthode de votre choix (USB, email, service de partage de fichier).

Ouvrez une application de gestion de fichiers et cliquez sur le fichier APK pour l'installer.

En fonction de votre version d'Android, il vous faudra accepter un certain nombre de messages d'avertissements pour autoriser l'installation depuis une source externe. N'oubliez pas de remettre ces options à leur valeur par défaut (ne pas autoriser) après avoir testé Ultrablue.

Notez que l'application Android est moins aboutie que l'application IOS présentée dans la démo SSTIC. Certaines fonctionnalités ne sont pas encore implémentées, notamment l'édition de politique de sécurité par sélection de PCRs et la visualisation du journal d'événements de démarrage.

IOS

Il n'est malheureusement pas possible d'installer une application IOS hors de l'Apple Store, et Ultrablue n'y a pas encore été publié. Toutefois, si vous possédez XCode et avez l'habitude de développer des applications IOS, vous pouvez recompiler une version du client à partir du code disponible sur la branche https://github.com/lfalkau/ultrablue/tree/ios-client (répertoires `src/clients/go-mobile` puis `src/clients/ios`).

Ordinateur

Les logiciels suivants doivent être installés pour pouvoir exécuter la machine virtuelle fournie :

- qemu, et plus précisément `qemu-system-x86_64` pour exécuter la machine virtuelle 64 bits.
- `swtpm`, pour émuler un TPM utilisé par la machine virtuelle.

```
### Installation
# Debian-like
$ sudo apt install qemu qemu-utils qemu-system-x86 qemu-system-gui
$ sudo apt install tpm-tools swtpm swtpm-tools
# Archlinux TODO

# Fedora
$ sudo dnf install qemu
$ sudo dnf install tpm2-tools swtpm swtpm-tools
```

Le serveur Ultrablue est déjà installé dans la machine virtuelle.

Vous pourrez récupérer une archive `ultrablue-vm.tar.bz2` (libellée "Ultrablue testbed (VM)") utilisable pour ce tutoriel depuis la dernière page de release d'Ultrablue.

```
# Préparation d'un répertoire de travail dédié
mkdir -p ~/tuto/SSTIC-2023/Ultrablue
cd ~/tuto/SSTIC-2023/Ultrablue

# Récupération de l'archive - le lien sera mis à jour pour la conférence
wget https://github.com/ANSSI-FR/ultrablue/releases/download/fosdem-2023/ultrablue-vm.tar.bz
# TODO: download sig and gpg check
tar xjf ultrablue-vm.tar.bz2
cd ultrablue-vm
```

Tutoriel

L'archive `ultrablue-vm.tar.bz2` mentionnée préalablement contient les éléments suivants :

- un script `run-demo.sh` pour configurer et lancer la machine virtuelle,
- les images des partitions nécessaires à la machine virtuelle (`OVMF_CODE.secboot.fd` et `OVMF_VARS.fd` pour la flash BIOS/UEFI, `ultrablue.raw` pour le disque).

La machine virtuelle est configurée pour démarrer en émulant un mode *secure boot* et elle dispose d'un disque chiffré.

`/!\ IMPORTANT!`Les clés de chiffrement du disque sont protégées par défaut par la phrase de passe `passphrase`.

La machine virtuelle a accès au périphériques Bluetooth physiques de l'hôte pour communiquer avec l'extérieur. En revanche, le TPM utilisé n'est pas celui de l'hôte, mais une émulation logicielle opérée par `swtpm` (dont l'état est stocké dans `/tmp/emulated_tpm/ultrablue`).

Lancez la machine virtuelle dans un terminal :

```
$ ./run-demo.sh
```

Le script utilise `sudo` pour exécuter `qemu` avec les privilèges administrateur[1].

`/!\ IMPORTANT!` Si vous êtes bloqué à n'importe quel moment dans le tutoriel, il est possible d'arrêter la machine virtuelle en invoquant la combinaison de touches `ctrl-a x`.

[1] Il est possible d'éditer le script pour supprimer l'usage de `sudo` mais cela nécessite (1) que l'utilisateur courant soit membre d'un groupe ayant accès à KVM (typiquement le groupe `kvm`), et (2) d'avoir configuré une règle udev autorisant `qemu` à monter l'interface Bluetooth physique dans la machine virtuelle (https://unix.stackexchange.com/a/637428). Nous avons préféré simplifier l'usage en sacrifiant la réduction de privilèges.

Lorsque le système le demande, entrez la phrase de passe pour déchiffrer le disque : `passphrase`

Une fois que la machine virtuelle a démarré, vous êtes automatiquement connecté en tant que `root`.

Enrôlement

Nous voulons tout d'abord enrôler la machine auprès de notre application mobile Ultrablue.

Attention : il est important de n'exécuter cette procédure qu'une seule fois avant de passer aux sections suivantes, pour des raisons détaillées ci-dessous. Si vous avez lancé plusieurs enrôlements ou attestations de suite, redémarrez la machine virtuelle pour recommencer le processus à zéro.

Lancez la commande suivante dans la machine virtuelle, ce qui devrait afficher un QR Code à l'écran :

```
ultrablue-server --enroll --pcr-extend
```

Le QR code contient l'identifiant MAC de l'interface Bluetooth utilisée par Ultrablue, ainsi qu'une clé AES-GCM pour chiffrer les échanges avec le téléphone.

Ouvrez l'application Ultrablue sur le téléphone. Cliquez sur `+` en haut à droite de l'écran pour ajoutez un nouvel appareil, donnez les autorisations pour utiliser l'appareil photo et scannez le QR Code. Donnez ensuite les autorisation de localisation (indispensable sous Android pour pouvoir utiliser le Bluetooth Low Energy). L'enrôlement devrait se terminer avec succès de part et d'autre, ajoutant un appareil à la liste des machines enregistrées dans l'interface Android. Vous pouvez renommer cet appareil pour lui donner un nom plus mémorable (par exemple "VM SSTIC").

Lors de cette première connexion, la machine transmet au téléphone un journal des mesures effectuées (ou *TPM eventlog*, qui contient les événements de la chaîne de démarrage tels que le BIOS, le *bootloader*, le noyau et leurs configurations), ainsi que des condensats de ces derniers signés par la puce TPM de l'ordinateur (ou *quote*, qui permet de valider les événements contenus dans le journal). Le téléphone stocke ces condensats pour pouvoir vérifier lors des attestations futures que la chaîne de démarrage n'a pas été altérée. Le téléphone génère également un secret qu'il transmet à l'ordinateur, afin d'être utilisé comme facteur de déchiffrement du disque. Ce secret est alors passé par le serveur Ultrablue au TPM pour être intégré à la valeur courant du registre PCR 9.

Cette dernière étape est la raison pour laquelle il ne faut exécuter l'enrôlement qu'une seule fois : si plusieurs enrôlements successifs sont réalisés, c'est la concaténation de tous les condensats qui sera ajoutée au PCR 9, rendant le déchiffrement du disque impossible au prochain démarrage.

La communication entre le téléphone et l'ordinateur est chiffrée par AES-GCM.

Sur l'ordinateur, la clé de chiffrement scellée à l'aide du TPM est stockée dans `/etc/ultrablue` (ce qui rend impossible son déchiffrement en dehors de la machine si le fichier venait à être exfiltré).

Configuration d'Ultrablue pour déchiffrer le disque au démarrage

Exécutez à présent la commande suivante :

```
systemd-cryptenroll --tpm2-device=auto --tpm2-pcrs=9 \
  /dev/$(lsblk -lf|grep crypto_LUKS|cut -f1)
```

Cette commande utilise le contenu du PCR 9 comme facteur pour sceller les clés de chiffrement du disque. Ainsi, lors du démarrage suivant, il suffira que le TPM contienne la même valeur dans le PCR 9 pour que le disque soit déchiffré automatiquement. Si la valeur est incorrecte, la phrase de passe sera demandée en solution de repli.

Il ne nous reste plus qu'à installer Ultrablue dans l'initrd de la machine pour lancer une procédure d'attestation tôt au démarrage, avant le déchiffrement du disque, afin de désceller le secret LUKS. Ce tutoriel utilise le générateur d'initrd `dracut`, pour lequel nous avons écrit des modules de configuration afin d'y intégrer Ultrablue :

```
dracut --add "crypt ultrablue" --force $(find /efi -name initrd) --verbose
```

Notez que cette commande, ainsi que la précédente, doivent être exécutées à chaque fois qu'un nouveau téléphone est enrôlé : `systemd-cryptenroll` pour ajouter le secret à la liste des PCRs. Bien que cela soit techniquement possible, `systemd-cryptenroll` ne sait pas combiner plusieurs tokens LUKS TPM, l'ajout d'un nouveau supprime les anciens. On ne peut donc pas enrôler plusieurs téléphones simultanément à l'heure actuelle.

Attestation au démarrage

Vous pouvez à présent redémarrer la machine virtuelle :

```
reboot
```

Au redémarrage, attendez qu'Ultrablue soit lancé et affiche :

```
INFO[0000] Start advertising
```

Vous disposez alors d'une minute pour réussir une procédure d'attestation distante. En cas d'échec ou de délai expiré, la phrase de passe (`passphrase`) sera demandée.

Ouvrez l'application Ultrablue sur Android et cliquez sur le symbole triangulaire "lecture".

Le téléphone envoie alors le journal d'événement et la *quote* au téléphone via la connexion Bluetooth chiffrée. Si la *quote* est conforme à celle du précédent démarrage et que les signatures sont correctes, le téléphone envoie le secret à

l'ordinateur, qui l'ajoute au PCR 9. Le disque peut alors être déverrouillé sans avoir à entrer de phrase de passe.

Vous pouvez éteindre la machine virtuelle à l'aide de la commande `poweroff`.