Habilitando el arranque seguro en Slackware

En el hardware basado en la Interfaz de firmware extensible unificada (UEFI), un sistema puede operar en modo de arranque seguro. En el modo de arranque seguro, solo los binarios EFI (es decir, los gestores de arranque, los cargadores de arranque) en los que el propietario de la plataforma confía, ya sea explícitamente o mediante una cadena de confianza, pueden ejecutarse en el momento del arranque. Esto evita que los binarios y sistemas operativos no autorizados de EFI se ejecuten en su sistema, lo que puede mejorar la seguridad.

Este artículo te enseñará:

- Acerca de las claves de arranque seguro y las bases de datos de firmas
- Cómo registrar claves de arranque seguro mientras se inicia en Slackware
- Cómo firmar archivos binarios de EFI para su uso en el modo de arranque seguro.

Asegúrese de que puede encontrar y manipular la configuración de arranque seguro con el firmware UEFI de su sistema. De esa manera, si comete un error, simplemente puede desactivar el Arranque seguro para tener nuevamente un sistema de arranque.

Una vez que haya cambiado sus claves de arranque seguro, haya firmado sus binarios de EFI y haya probado que el arranque seguro está funcionando, debe almacenar sus claves privadas en un lugar seguro hasta que las claves sean requeridas nuevamente. Cualquier persona con acceso a sus claves privadas puede pasar por alto la protección que ofrece el arranque seguro.

Claves de arranque seguro y bases de datos de firmas

Se utilizan dos tipos de claves de arranque seguro para crear relaciones de confianza:

- Clave de la plataforma: esto establece la relación de confianza entre el propietario de la plataforma y el firmware de la plataforma. El firmware UEFI solo puede almacenar una clave de plataforma. La clave pública se almacena en la variable de arranque seguro PK . Esta clave permite al propietario de la plataforma manipular todas las claves de arranque seguro y las bases de datos de firmas.
- Key Exchange Key: establece la relación de confianza entre el sistema operativo y el firmware de la plataforma. El firmware UEFI puede almacenar múltiples claves de intercambio de claves. Las claves públicas se almacenan en la variable de arranque seguro “KEK”. Key Exchange Keys solo permite que el sistema operativo manipule las bases de datos de firmas.

Hay dos bases de datos de firmas para autorizar binarios de EFI:

- Base de datos de firmas prohibidas: almacena hashes y claves de firma públicas de binarios EFI prohibidos. Esto utiliza la variable de arranque seguro dbx . Los binarios EFI con hashes presentes en esta base de datos o firmas que pueden autenticarse con una clave de firma almacenada en la base de datos tienen prohibido cargarse.

- Base de datos de firmas autorizada: almacena hashes y claves de firma públicas de binarios de EFI de confianza. Esto utiliza la variable de arranque seguro `db` . Los binarios EFI con hashes presentes en esta base de datos o firmas que pueden autenticarse usando una clave de firma almacenada en la base de datos pueden ejecutarse si no hay coincidencias con ninguna entrada en la base de datos de firmas prohibidas.

Requisitos

Necesitarás el paquete efitools and sbsigntools antes de que empieces. En Slackbuilds están disponibled http://slackbuilds.org.

Si aún no tiene su propia clave de plataforma inscrita en el firmware UEFI, el howto asume que tiene desactivado el arranque seguro y que ha borrado la variable `PK` en el firmware UEFI.

Inscripción de claves de inicio seguro y entradas de base de datos de firmas

Si no tiene un par de claves de plataforma existentes y un par de claves de firma binaria EFI, el método más sencillo para crear los pares de claves sería crear claves autofirmadas. Se recomienda crear pares de claves RSA de 2048 bits que usen el algoritmo de firma sha256RSA. Para generar claves autofirmadas con las propiedades recomendadas, ejecute:

```
openssl req -new -x509 -newkey rsa:2048 -subj "/CN=Platform Key Common
Name/" \
        -keyout PK.priv -out PK.pub -days 3650 -nodes -sha256
openssl req -new -x509 -newkey rsa:2048 -subj "/CN=EFI Binary Signing Key
Common Name/" \
        -keyout db.priv -out db.pub -days 3650 -nodes -sha256
```

que crea claves privadas con la extensión `.priv` y certificados de clave pública con la extensión `.pub` . Es posible que desee ajustar el período de validez de la clave y elegir un Nombre común (CN) diferente para ayudar a distinguir sus claves.

No es necesario crear o usar su propia clave de intercambio de clave, ya que está destinada a ser utilizada por los sistemas operativos. Sin embargo, a continuación se proporcionan las instrucciones de Key Exchange Key para que sepa cómo inscribir las Key Exchange Keys para los sistemas operativos que lo requieren.

Para preparar una nueva Clave de plataforma para escribir en la variable `PK` :

1. Inserte la clave de plataforma pública en una lista de firmas EFI:

   ```
   cert-to-efi-sig-list -g owner_guid PK.pub PK.esl
   ```

   reemplazando `owner_guid` con un GUID hexadecimal en el formato

`12345678-1234-1234-123456789abc` . El GUID del propietario debe ser el mismo para todas las claves que posea. Si un sistema operativo no puede agregar una firma a una base de datos de firmas debido a la falta de recursos, puede eliminar una firma con un GUID propietario asociado con el sistema operativo.

2. Firmando la lista de firmas EFI. En el modo de configuración (arranque seguro desactivado), la mitad privada de la clave insertada debe firmar la lista de firmas. En el modo Usuario (inicio seguro activado), la clave privada de la clave de la plataforma actual debe firmar la lista de firmas:

```
sign-efi-sig-list -k PK.priv -c PK.pub PK PK.esl PK.signed
```

Se aplica un procedimiento similar para preparar una clave de intercambio de claves o una entrada de la base de datos de firmas para escribir en las variables KEK , `db` o `dbx` . Las claves de intercambio de claves deben estar firmadas por la mitad privada de la clave de plataforma:

```
cert-to-efi-sig-list -g owner_guid KEK.pub KEK.esl
sign-efi-sig-list -a -k PK.priv -c PK.pub KEK KEK.esl KEK.signed
```

Y las entradas de la base de datos de firmas deben estar firmadas por la mitad privada de la Clave de la plataforma o cualquiera de las Claves de intercambio de claves:

```
cert-to-efi-sig-list -g owner_guid db.pub db.esl
sign-efi-sig-list -a -k PK.priv -c PK.pub db db.esl db.signed
```

Tenga en cuenta que la opción `-a` se usó para preparar una escritura anexa.

Para actualizar las variables de arranque seguro debe tener privilegios de raíz. Necesitará cargar el módulo del kernel efivarfs y montar el sistema de archivos efivarfs de antemano si aún no se ha resuelto:

```
modprobe efivarfs
mount -t efivarfs efivarfs /sys/firmware/efi/efivars
```

Para registrar la Clave de la Plataforma, ejecute:

```
efi-updatevar -f PK.esl.signed PK
```

Si el sistema estaba en modo de configuración, ahora estará en modo de usuario.

Para agregar claves a las variables KEK , `db` o `dbx` , ejecute (según corresponda):

```
efi-updatevar -a -f KEK.signed KEK
```

```
efi-updatevar -a -f db.signed db
```

```
efi-updatevar -a -f dbx.signed dbx
```

Puede verificar que sus claves se hayan inscrito correctamente usando `efi-readvar` .

Firma Binarios EFI

Mi recomendación (en el momento de escribir esto) es que use un administrador de arranque con un kernel de stub de EFI, o que arranque directamente un kernel de stub de EFI. ELILO, efilinux y syslinux (y posiblemente GRUB, pero no estoy seguro) permitirán que se ejecuten núcleos sin firmar (o al menos lo hace en mi hardware y VM), lo que anula el propósito de arranque seguro. Si sigue mi recomendación, asegúrese de firmar su kernel cada vez que lo cambie.

Deberá firmar todos los archivos binarios de EFI, hasta e incluyendo su cargador de arranque y/o el núcleo de stub de EFI. Para firmar un binario, ejecute:

```
sbsign --key db.priv --cert db.pub --output signed_binary.efi binary.efi
```

Un ejemplo de cómo agregar una entrada de kernel stub EFI usando efibootmgr es:

```
efibootmgr -c -L SlackSecureBoot -l '\EFI\Slackware\vmlinuz-signed.efi' -u
'root=/dev/sda3'
```

Si ve “” warning: gap in section table “” cuando firma un binario EFI (consulte a continuación), es probable que el binario no funcione en el modo de arranque seguro. Esta advertencia aparece para los binarios de EFI creados contra versiones anteriores de la biblioteca gnu-efi. Si planea usar ELILO, deberá volver a compilarlo usted mismo, la versión que se incluye con Slackware no funcionará.

```
warning: gap in section table:
    .text   : 0x00000400 - 0x00017c00,
    .reloc  : 0x00017ca1 - 0x000180a1,
warning: gap in section table:
    .reloc  : 0x00017ca1 - 0x000180a1,
    .data   : 0x00018000 - 0x00033000,
gaps in the section table may result in different checksums
warning: data remaining[225792 vs 242346]: gaps between PE/COFF
sections?
```

Deshabilitando el arranque seguro

Si desea eliminar todas las claves de inicio seguro y volver al modo de configuración, la forma más sencilla de hacerlo es firmar un archivo vacío con su clave de plataforma y escribir el archivo firmado en todas las variables de inicio seguro:

```
touch empty
sign-efi-sig-list -k PK.priv -c PK.pub PK empty empty.signed
efi-updatevar -f empty.signed PK
efi-updatevar -f empty.signed KEK
```

```
efi-updatevar -f empty.signed db
efi-updatevar -f empty.signed dbx
```

Dual / Multi-booting con Windows

Si Windows es una de sus opciones de arranque, necesitará los certificados KEK y db de Microsoft. Los certificados se pueden encontrar en https://technet.microsoft.com/en-us/library/dn747883.aspx y tendrá que convertirse del formato DER al formato PEM:

```
openssl x509 -in certificate.der -inform DER -out certificate.pem
```

Las instrucciones que se proporcionaron anteriormente se pueden utilizar para inscribir los certificados. El GUID propietario que debe usar para las claves de Microsoft es 77fa9abd-0359-4d32-bd60-28f4e78f784b.

Sources

- Originally written by turtleli

More information can be found at:

- http://uefi.org
- http://www.rodsbooks.com/efi-bootloaders/secureboot.html
- http://blog.hansenpartnership.com/
- https://technet.microsoft.com/en-us/library/dn747883.aspx

howtos, security, secure boot, uefi, author turtleli