Full credit is given to the above companies including the OS that this PDF file was generated!

Rocky Enterprise Linux 9.2 Manual Pages on command 'systemd-measure.1'

$ man systemd-measure.1

SYSTEMD-MEASURE(1) systemd-measure SYSTEMD-MEASURE(1)

NAME

systemd-measure - Pre-calculate and sign expected TPM2 PCR values for booted unified kernel images

SYNOPSIS

/usr/lib/systemd/systemd-measure [OPTIONS...]

DESCRIPTION

Note: this command is experimental for now. While it is likely to become a regular component of systemd, it might still change in behaviour and interface.

systemd-measure is a tool that may be used to pre-calculate and sign the expected TPM2 PCR 11 values that should be seen when a unified Linux kernel image based on systemd-stub(7) is booted up. It accepts paths to the ELF kernel image file, initrd image file, devicetree file, kernel command line file, os-release(5) file, boot splash file, and TPM2 PCR PEM public key file that make up the unified kernel image, and determines the PCR values expected to be in place after booting the image. Calculation starts with a zero-initialized PCR 11, and is executed in a fashion compatible with what systemd-stub does at boot.

The result may optionally be signed cryptographically, to allow TPM2 policies that can only be unlocked if a certain set of kernels is booted, for which such a PCR signature can be provided.

COMMANDS

The following commands are understood:

status

This is the default command if none is specified. This queries the local system's TPM2 PCR 11+12+13 values and displays them. The data is written in a similar format as the calculate command below, and may be used to quickly compare expectation with reality.

calculate

Pre-calculate the expected values seen in PCR register 11 after boot-up of a unified kernel image consisting of the components specified with --linux=, --osrel=, --cmdline=, --initrd=, --splash=, --dtb=, --pcrpkey= see below. Only --linux= is mandatory. (Alternatively, specify --current to use the current values of PCR register 11 instead.)

sign

As with the calculate command, pre-calculate the expected value seen in TPM2 PCR register 11 after boot-up of a unified kernel image. Then, cryptographically sign the resulting values with the private/public key pair (RSA) configured via --private-key= and --public-key=. This will write a JSON object to standard output that contains signatures for all specified PCR banks (see --pcr-bank=) below, which may be used to unlock encrypted credentials (see systemd-creds(1)) or LUKS volumes (see systemd-cryptsetup@.service(8)). This allows binding secrets to a set of kernels for which such PCR 11 signatures can be provided.

Note that a TPM2 device must be available for this signing to take place, even though the result is not tied to any TPM2 device or its state.

OPTIONS

The following options are understood:

--linux=PATH, --osrel=PATH, --cmdline=PATH, --initrd=PATH,

--splash=PATH, --dtb=PATH, --pcrpkey=PATH

When used with the calculate or sign verb, configures the files to read the unified kernel image components from. Each option corresponds with the equally named section in the unified kernel PE file. The --linux= switch expects the path to the ELF kernel file that the unified PE kernel will wrap. All switches except --linux= are optional. Each option may be used at most once.

--current

When used with the calculate or sign verb, takes the PCR 11 values currently in effect for the system (which should typically reflect the hashes of the currently booted kernel). This can be used in place of --linux= and the other switches listed above.

--bank=DIGEST

Controls the PCR banks to pre-calculate the PCR values for ? in case calculate or sign is invoked ?, or the banks to show in the status output. May be used more then once to specify multiple banks. If not specified, defaults to the four banks "sha1", "sha256", "sha384", "sha512".

--private-key=PATH, --public-key=PATH

These switches take paths to a pair of PEM encoded RSA key files, for use with the sign command.

Note the difference between the --pcrpkey= and --public-key= switches. The former selects the data to include in the ".pcrpkey" PE section of the unified kernel image, the latter picks the public key of the key pair used to sign the resulting PCR 11 values. The former is the key that the booted system will likely use to lock disk and credential encryption to, the latter is the key used for unlocking such resources again. Hence, typically the same PEM key should be supplied in both cases.

If the --public-key= is not specified but --private-key= is specified the public key is automatically derived from the private key.

--tpm2-device=PATH

Controls which TPM2 device to use. Expects a device node path referring to the TPM2 chip (e.g. /dev/tpmrm0). Alternatively the special value "auto" may be specified, in order to automatically determine the device node of a suitable TPM2 device (of which there must be exactly one). The special value "list" may be used to enumerate all suitable TPM2 devices currently discovered.

--phase=PHASE

Controls which boot phases to calculate expected PCR 11 values for. This takes a series of colon-separated strings that encode boot "paths" for entering a specific phase of the boot process. Each of the specified strings is measured by the systemd-pcrphase-initrd.service and systemd-pcrphase.service(8) into PCR 11 during different milestones of the boot process. This switch may be specified multiple times to calculate PCR values for multiple boot phases at once. If not used defaults to "enter-initrd", "enter-initrd:leave-initrd", "enter-initrd:leave-initrd:sysinit", "enter-initrd:leave-initrd:sysinit:ready", i.e. calculates expected PCR values for the boot phase in the initrd, during early boot, during later boot, and during system runtime, but excluding the phases before the initrd or when shutting down. This setting is honoured both by calculate and sign. When used with the latter it's particularly useful for generating PCR signatures that can only be used for unlocking resources during specific parts of the boot process.

For further details about PCR boot phases, see systemd-pcrphase.service(8).

--json=MODE

Shows output formatted as JSON. Expects one of "short" (for the shortest possible output without any redundant whitespace or line breaks), "pretty" (for a pretty version of the same, with indentation and line breaks) or "off" (to turn off JSON output, the default).

--no-pager

Do not pipe output into a pager.

-h, --help

Print a short help text and exit.

--version

Print a short version string and exit.

EXAMPLES

Example 1. Generate a unified kernel image, and calculate the expected TPM PCR 11 value

```
# objcopy \
    --add-section .linux=vmlinux --change-section-vma .linux=0x2000000 \
    --add-section .osrel=os-release.txt --change-section-vma .osrel=0x20000 \
    --add-section .cmdline=cmdline.txt --change-section-vma .cmdline=0x30000 \
    --add-section .initrd=initrd.cpio --change-section-vma .initrd=0x3000000 \
    --add-section .splash=splash.bmp --change-section-vma .splash=0x100000 \
    --add-section .dtb=devicetree.dtb --change-section-vma .dtb=0x40000 \
    /usr/lib/systemd/boot/efi/linuxx64.efi.stub \
    foo.efi
# systemd-measure calculate \
     --linux=vmlinux \
     --osrel=os-release.txt \
     --cmdline=cmdline.txt \
     --initrd=initrd.cpio \
     --splash=splash.bmp \
     --dtb=devicetree.dtb
11:sha1=d775a7b4482450ac77e03ee19bda90bd792d6ec7
11:sha256=bc6170f9ce28eb051ab465cd62be8cf63985276766cf9faf527ffefb66f45651

11:sha384=1cf67dff4757e61e5a73d2a21a6694d668629bbc3761747d493f7f49ad720be02fd07263e1f93061243aec599d1ee
4b4
```

```
11:sha512=8e79acd3ddbbc8282e98091849c3530f996303c8ac8e87a3b2378b71c8b3a6e86d5c4f41ecea9e1517090c3e8ec0c714821032038f525f744960bcd082d937da
```

Example 2. Generate a private/public key pair, and a unified kernel image, and a TPM PCR 11 signature for it, and embed the signature and the public key in the image

```
# openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out tpm2-pcr-private.pem
# openssl rsa -pubout -in tpm2-pcr-private.pem -out tpm2-pcr-public.pem
# systemd-measure sign \
     --linux=vmlinux \
     --osrel=os-release.txt \
     --cmdline=cmdline.txt \
     --initrd=initrd.cpio \
     --splash=splash.bmp \
     --dtb=devicetree.dtb \
     --pcrpkey=tpm2-pcr-public.pem \
     --bank=sha1 \
     --bank=sha256 \
     --private-key=tpm2-pcr-private.pem \
     --public-key=tpm2-pcr-public.pem > tpm2-pcr-signature.json
# objcopy \
    --add-section .linux=vmlinux --change-section-vma .linux=0x2000000 \
    --add-section .osrel=os-release.txt --change-section-vma .osrel=0x20000 \
    --add-section .cmdline=cmdline.txt --change-section-vma .cmdline=0x30000 \
    --add-section .initrd=initrd.cpio --change-section-vma .initrd=0x3000000 \
    --add-section .splash=splash.bmp --change-section-vma .splash=0x100000 \
    --add-section .dtb=devicetree.dtb --change-section-vma .dtb=0x40000 \
    --add-section .pcrsig=tpm2-pcr-signature.json --change-section-vma .splash=0x80000 \
    --add-section .pcrpkey=tpm2-pcr-public.pem --change-section-vma .splash=0x90000 \
    /usr/lib/systemd/boot/efi/linuxx64.efi.stub \
    foo.efi
```

Later on, enroll the signed PCR policy on a LUKS volume:

```
# systemd-cryptenroll --tpm2-device=auto --tpm2-public-key=tpm2-pcr-public.pem --tpm2-signature=tpm2-pcr-signature.json /dev/sda5
```

And then unlock the device with the signature:

```
# /usr/lib/systemd/systemd-cryptsetup attach myvolume /dev/sda5 - tpm2-device=auto,tpm2-signature=/path/to/tpm2-pcr-signature.json
```

Note that when the generated unified kernel image foo.efi is booted the signature and public key files will be placed at locations systemd-cryptenroll and systemd-cryptsetup will look for anyway, and thus these paths do not actually need to be specified.

EXIT STATUS

On success, 0 is returned, a non-zero failure code otherwise.

SEE ALSO

systemd(1), systemd-stub(7), objcopy(1), systemd-creds(1), systemd-cryptsetup@.service(8), systemd-pcrphase.service(1)