Blog Post BACON

Motivation

BACON is a tool created to help optimize the workflow of securely using containers.
It gives an easy overview of the current state of the container host in regards to secure and measured boot.
It uses signed images to make sure the image wasn't tampered with upon pulling the image.
To prevent the user from starting containers of a high security level, when the host has been tampered with, BACON checks if the defined policies require measured boot and TDX to be attested and executes these attestations. Only should they be valid, the container will be started. In order to provide this functionality, a script is supplied.

Functionality

The script allows an easy interaction between signed images and their containers.
Only if multiple requirements are fulfilled the script will allow the user to interact with images and containers. Also we provide the ability to set a policy: High, Mid, Low. The user is only able to start a container if the policy-level of the container is the same or lower as the system policy. The policy can be set during startup or can also be changed later.
For this approach the Images need to have a label. Inside the Dockerfile you need to write

- LABEL policy="High"

to set the policy for the container to High.

The main script allows the user to interact with images and containers.

- Image options: List, Build, Push, Pull, Remove
- Container options: Show running containers, Start Container, Stop Container, Prune Container

The provided script first checks if multiple requirements are met:

- All the needed tools are installed (nerdctl, cosign, …)
- TDX guest driver is available
- Signing Keys are available
- Platform Configuration Registers (PCR) are not changed

Also there is an option to change the current set policy and get a sample TD Quote.

To accomplish this the script makes use of multiple programs:

- containerd
- nerdctl
- cosign
- tpm2-tools
- trustauthority-cli

Tools Used

Containerd

Containerd is used as the container runtime.

Nerdctl

Nerdctl is used as the CLI to manage the containers. It was chosen because it provides easy to use access to Cosign.

Cosign

Cosign is used to sign the images upon pushing them to a repository. It is used to verify the signature on pulling the image as well.

tpm2-tools

tpm2-tools is used to generate a quote of the tpm to help verify the measured boot status.

trustauthority-cli

trustauthority-cli is used to generate a quote of the tdx module in order to make attestation of the system integrity possible.

Limitations

BACON cannot prevent containers with a set policy to be started by the host that signed them, even when the policy is not met, when using a different tool.
It is designed to help the legitimate operator to enforce the proper security measures.

In order to verify Intel TDX quotes and use the remote attestation, an API Key to Intel Trust Authority is needed. At the moment this key is not given out to end users, therefore remote attestation of the TDX quote is not currently implemented. Should it be made available in the future, a function to generate the quote is already implemented.