In Containers We Trust? Building Trust In Containerized Environments

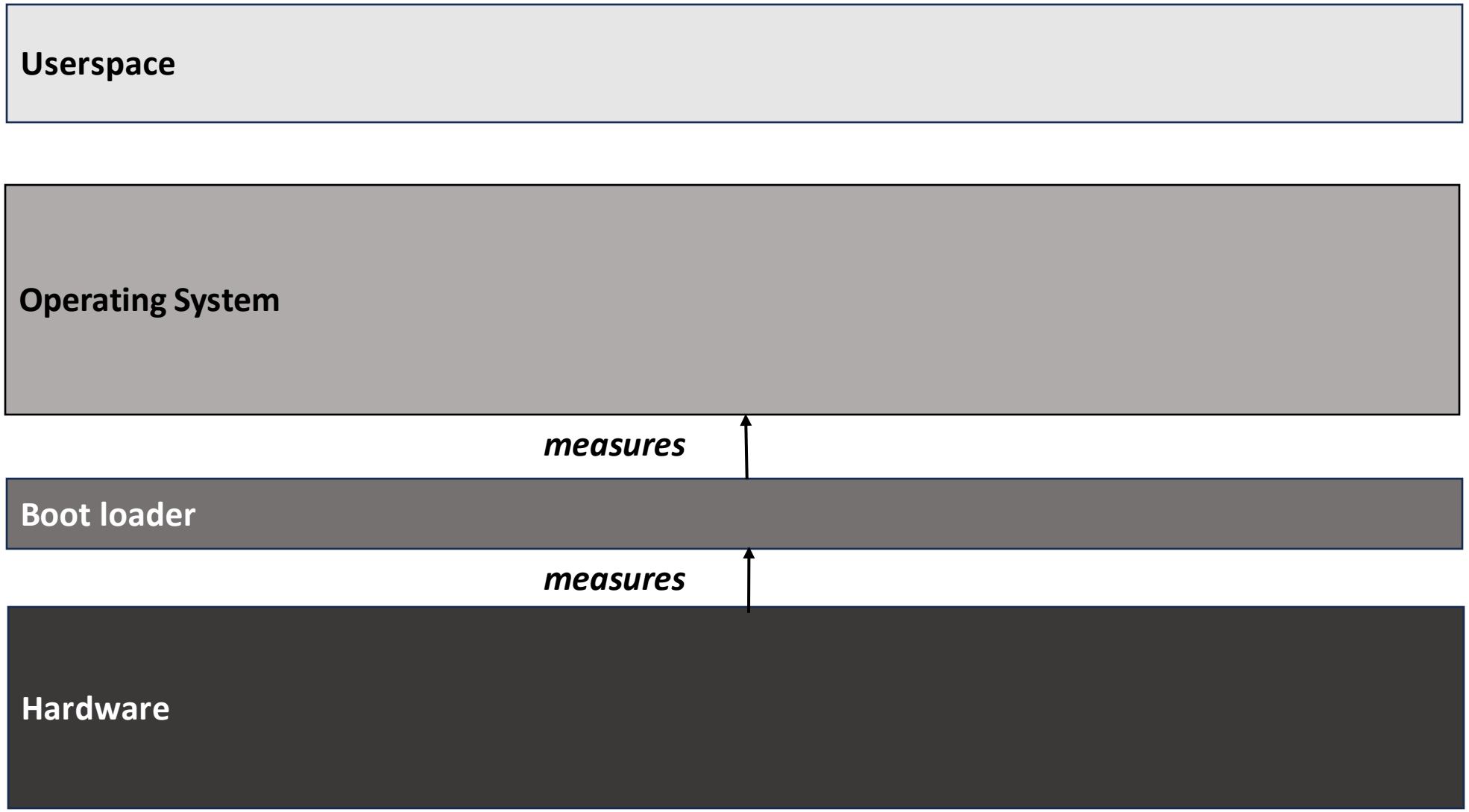
Avery Blanchard[1], Gheorghe Almasi[2], James Bottomley[2] and Hubertus Franke[2]

1 Duke University
2 IBM Research

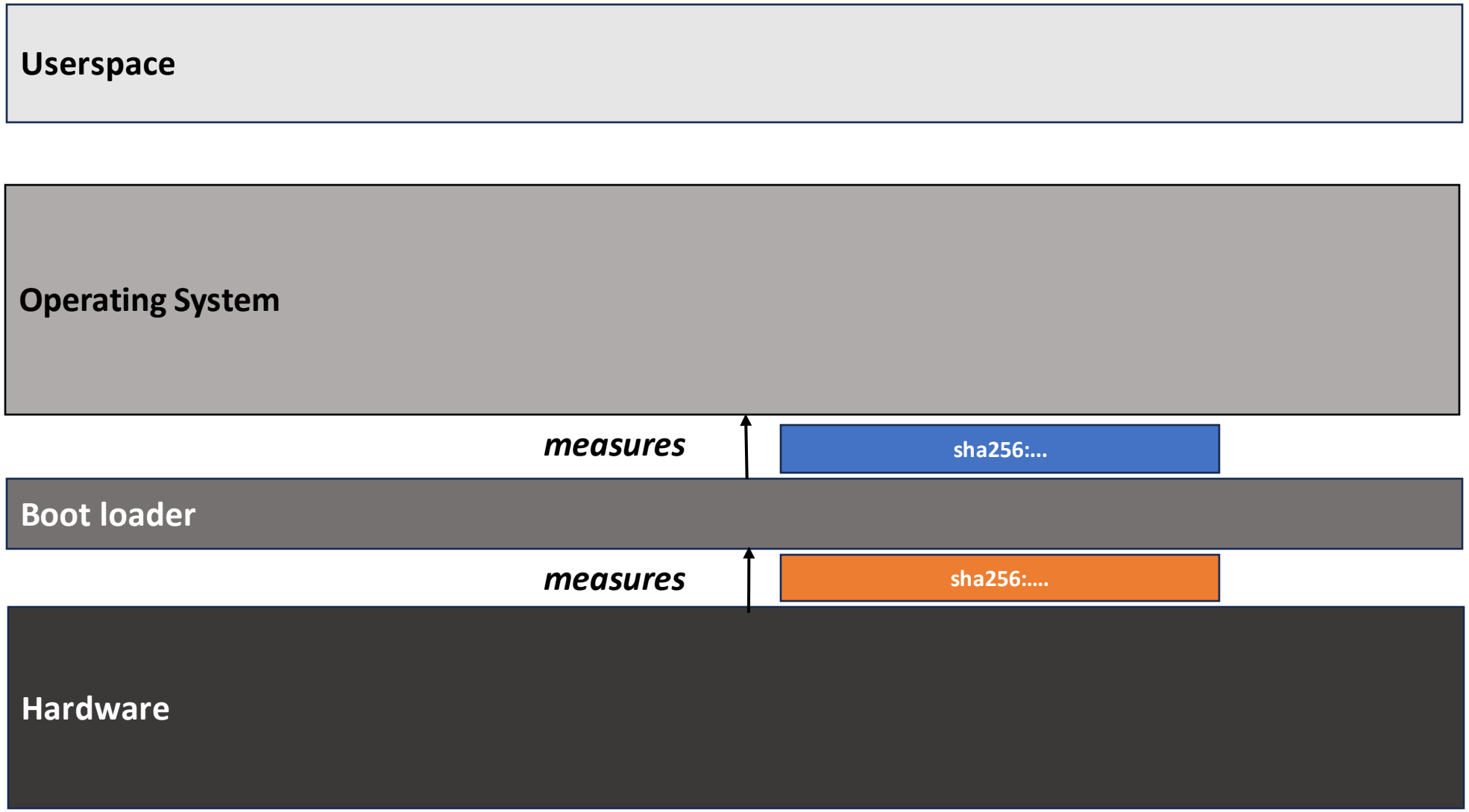
November 13th, 2023

Containers are ubiquitous and blindly trusted…

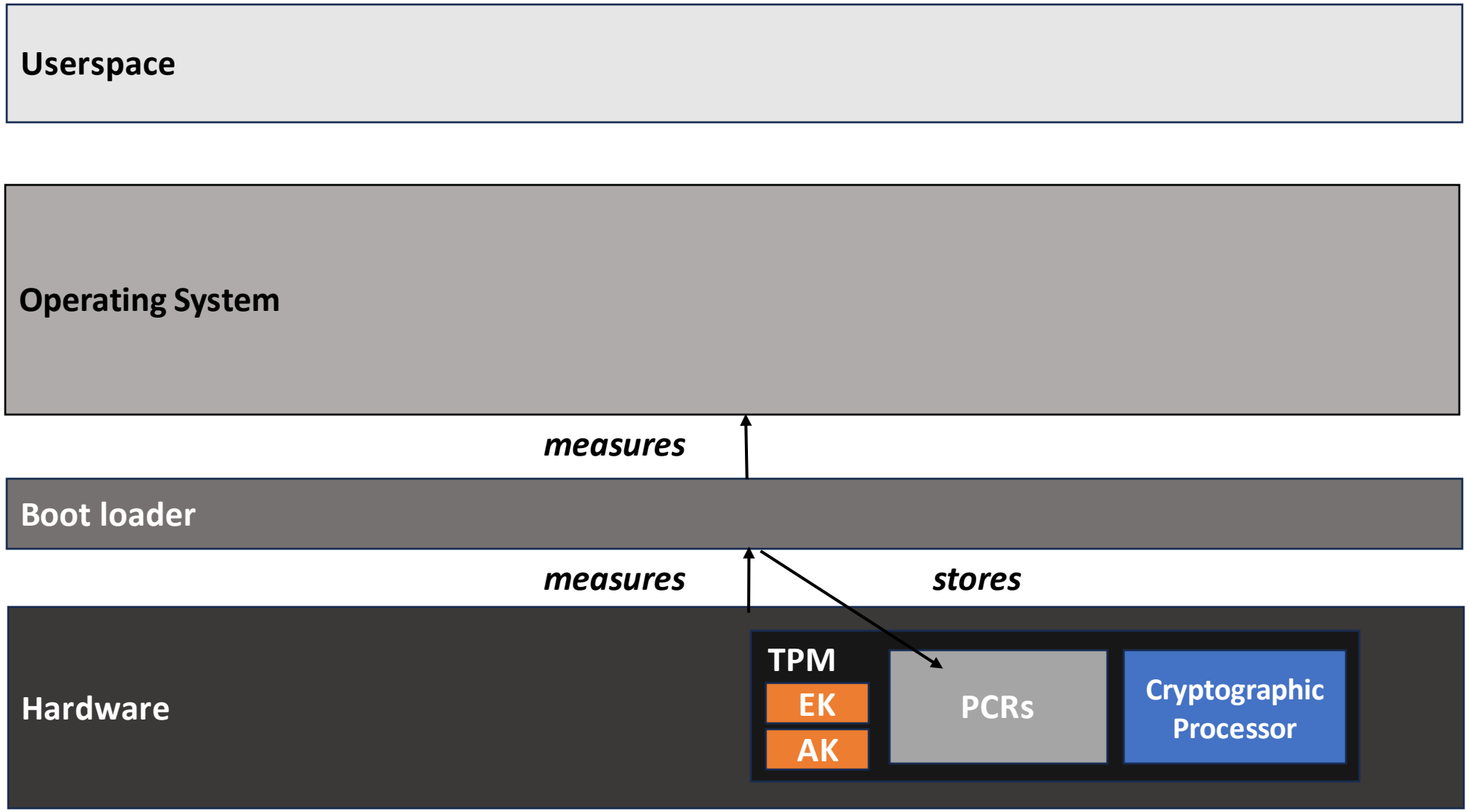
Defining Trust: Measurement

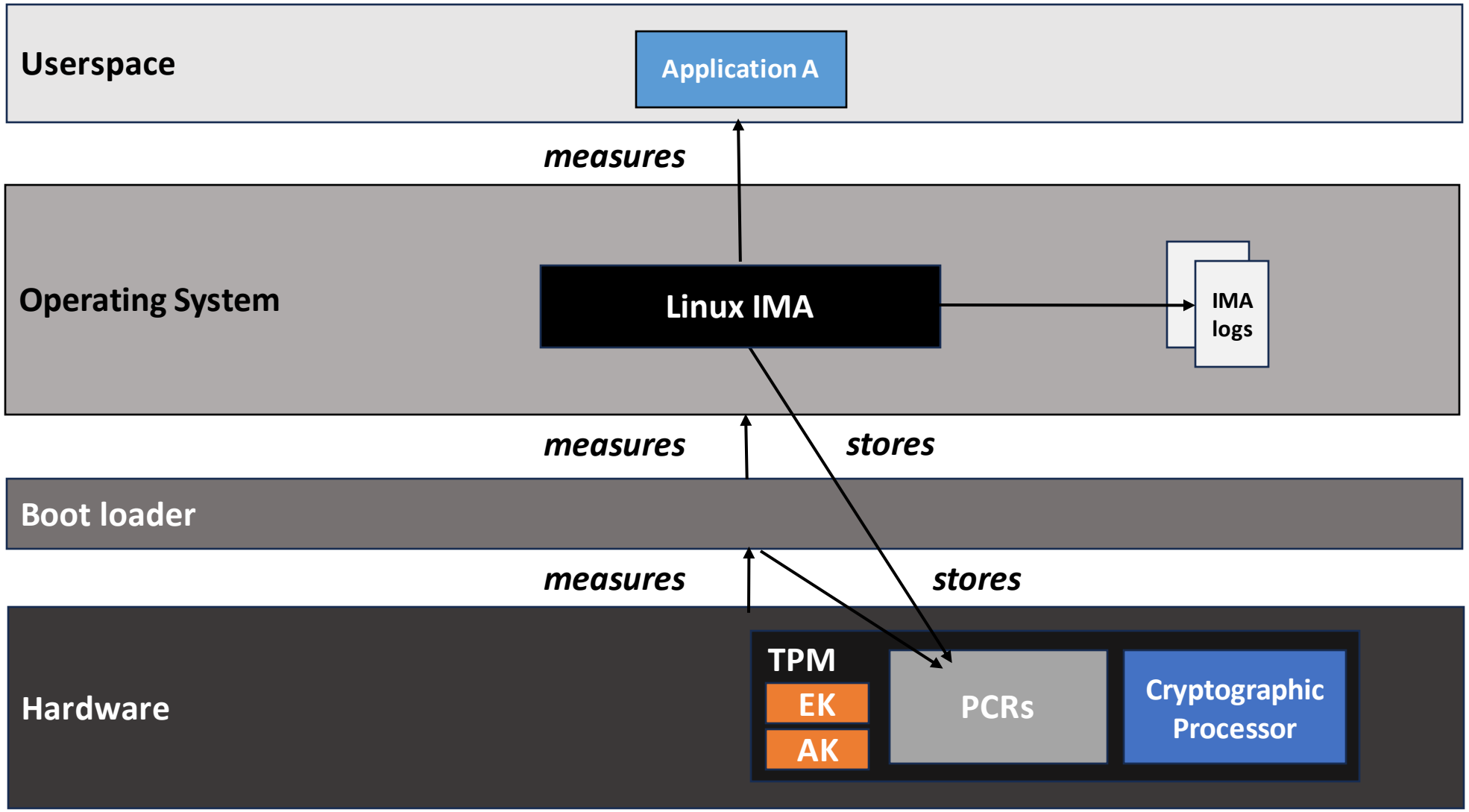


Defining Trust: Measurement

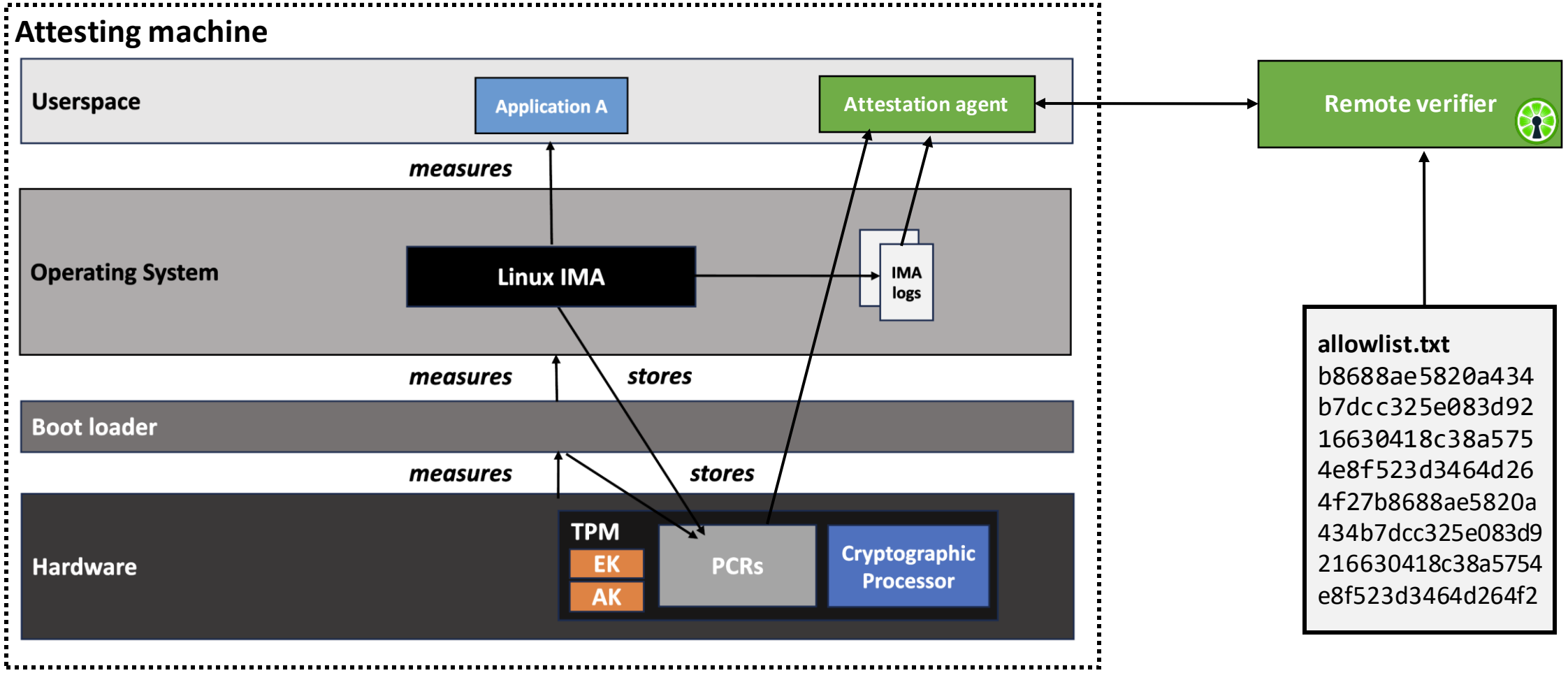


Building Trust from Hardware

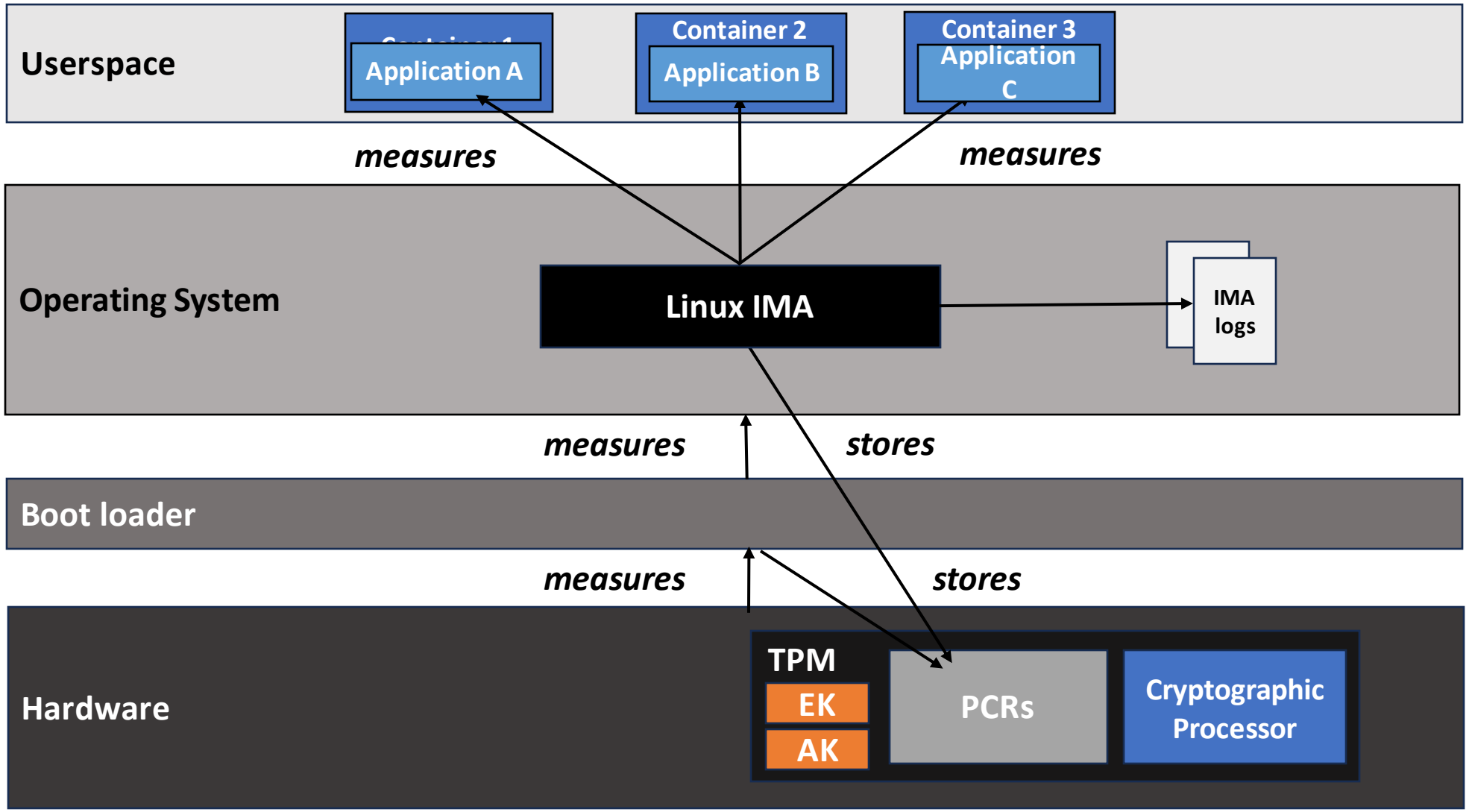



Userspace
Application A
measures
Operating System
Linux IMA
IMA logs
measures
stores
Boot loader
measures
stores
Hardware
TPM
EK
AK
PCRs
Cryptographic Processor

Building Trust in Remote Environments



Container Present a Gap in Trust and Integrity



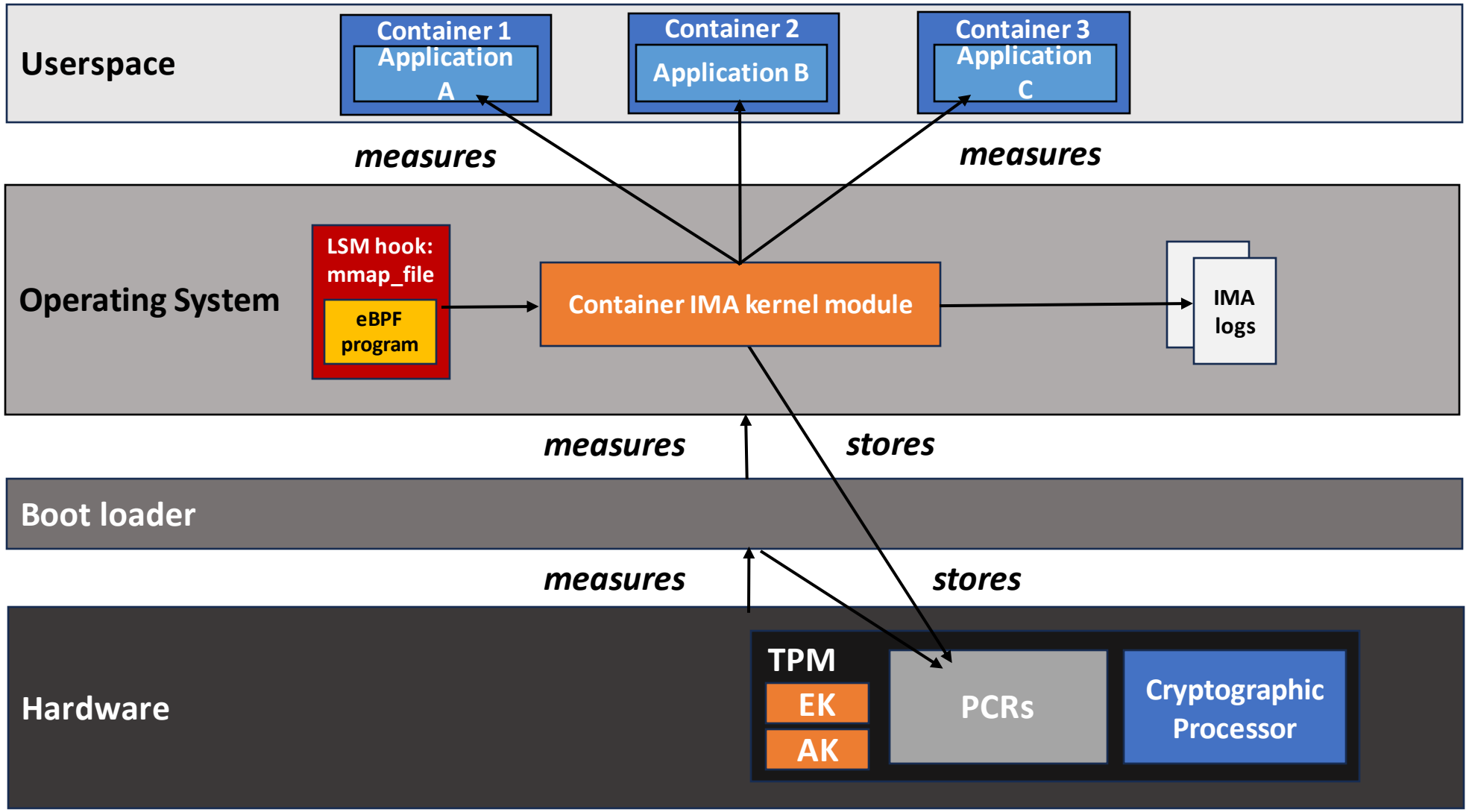
The Need for Namespace Support

```
[avery@fedora ~]$ sudo tail -n 20 /sys/kernel/security/integrity/ima/ascii_runtime_measurements
10 240d3f5bb871c7540d5fa91a7a9b0e616ff34b37 ima-ng sha256:06757b36daadb8228df0031496c2e9f3e16b1e2fe9cf5935756b9e4d0a315cff /usr/lib64/security/pam_motd.so
10 2d6ae2a41111b8ef8ac131d03891e1795de64b02 ima-ng sha256:7a935fb9c4735483548f79c218ee0c549a0412beba1079c9d58ab361956f8762 /usr/bin/id
10 526280709ef5c30d1d295d329573d606a5a14508 ima-ng sha256:604c924cd216b077739d5cc7668b4c917c3c784bff30c03454dd5fa4337da6af /usr/bin/hostnamectl
10 4431b8f9ded554c13422329d704d4bc335e3a656 ima-ng sha256:b91c10cb140a1593b37fba2dcab5cddf53c8e2c5104980b2ed7a1b42b7aa7d1b /usr/libexec/grepconf.sh
10 df4fc4579582f97fb2b26501acbaed387be07865 ima-ng sha256:14a956e5ca7f5c6353c1c402e540ee90681139f480730a3ae2cec90979a06426 /usr/bin/dircolors
10 884bdeca3d357b2d4a1841579acb4dca707a69be ima-ng sha256:a392c3fb23c8f6dc6ea60686e6bea7d7ba02b801feed60d48a15f708e5d45227 /usr/bin/tr
10 4eee461a1cc8acd0de77681f3b40dd61810c6d59 ima-ng sha256:2385b88763aa30afbbb883f9d4986eeae930565f0359136bb9c2db455a5936d7 /usr/bin/locale
10 6e3d31be5ce90f101a51f9c3cd4ff1028b8e2aa9 ima-ng sha256:998d3149a3da2f8b7e25dca9939527344e8cd72a3592d91a5f7565e94205ba9a /usr/bin/basename
10 4fbf9276e099a3595ed92f7f645e84490a20421f ima-ng sha256:a6bcff83842822258a65d7f192b5b7614ad84eadb7b8798856242218e32965e4 /usr/bin/sudo
10 f023c1f61dcaa830c9ae16ff76e9820851a3233f ima-ng sha256:52168dda87781f2ae7d141558d6f2bf0d22a9d984dd3e7d7e4d3f10dbc78505b /usr/libexec/sudo/libsudo_util.so.0.0.
10 7be972007b6c71eb9da55f3df38419f8d2866dd6 ima-ng sha256:f5133e9455f155edcec2a715f6bf4eae41937da7ef73536ea0123f4544535924 /usr/libexec/sudo/sudoers.so
10 c462d2c296c96946edc1659ded465c87d09c03c7 ima-ng sha256:96243a67c64c1de805f2a0da43232f1ba9ae44447c0fc84863aaed2d6ef0de0e /usr/lib64/security/pam_fprintd.so
10 dafe26ca42d945a6807199624fe3e12eda7c5266 ima-ng sha256:b98ecafe49699d4eb55789efd4e8f1d9208622da4972af761eb19fad93d90162 /usr/bin/docker
10 5fb55ea1517fb800aea13744cf6f8b9b366ebf0d ima-ng sha256:0efb18f93ab7c680ba28ba9bc50c3fabed9fa49d22e18a76b381039cfd01d4cf /usr/bin/containerd-shim-runc-v2
10 5c4f7bddfc3988228ca9d50629d524b4dacb1454 ima-ng sha256:d3f7d10e296e5c626ea78539cb38cd8dffd043bea3627da35ce3b20c0ac68014 /hello
10 1844bd922c570347569afc8ca2551b0c26302661 ima-ng sha256:8a56e729fd7764215090c1a02781c465ddf534a50b602f76b3cc33c19e013bbd /usr/bin/tail
10 bfc24c544fc3f85107c65e69856f43cc54ef72b4 ima-ng sha256:415a5f6f063d6b6c0183947708651e5424b3c38d68357fd23103ad7c56a2a3cf /usr/lib64/ld-linux-x86-64.so.2
10 7393b51a9384e4254a9c8df419309a41fac0d5f5 ima-ng sha256:9f2e4d479a9a7d7e27e639701da4ffbcfb8ff40512b5c676ac42801058847c28 /usr/lib64/libc.so.6
10 60776682416701d59dc629e089d78c6e5b09c9a5 ima-ng sha256:9f4a5f1f38860c5479da080378a632636d818675b3f19849a4c43fe5242beadc /usr/bin/locale
10 39e08422189f153283aafba2fa32240fb2149177 ima-ng sha256:d91502c3a044c776ae0c9b799b59df4fb1901aa84dcb4c26c4dcbe55cf5951be /usr/bin/sha256sum
[avery@fedora ~]$
```

Which of these measurements are from a container?

Enabling Container Attestation: A Preliminary Approach

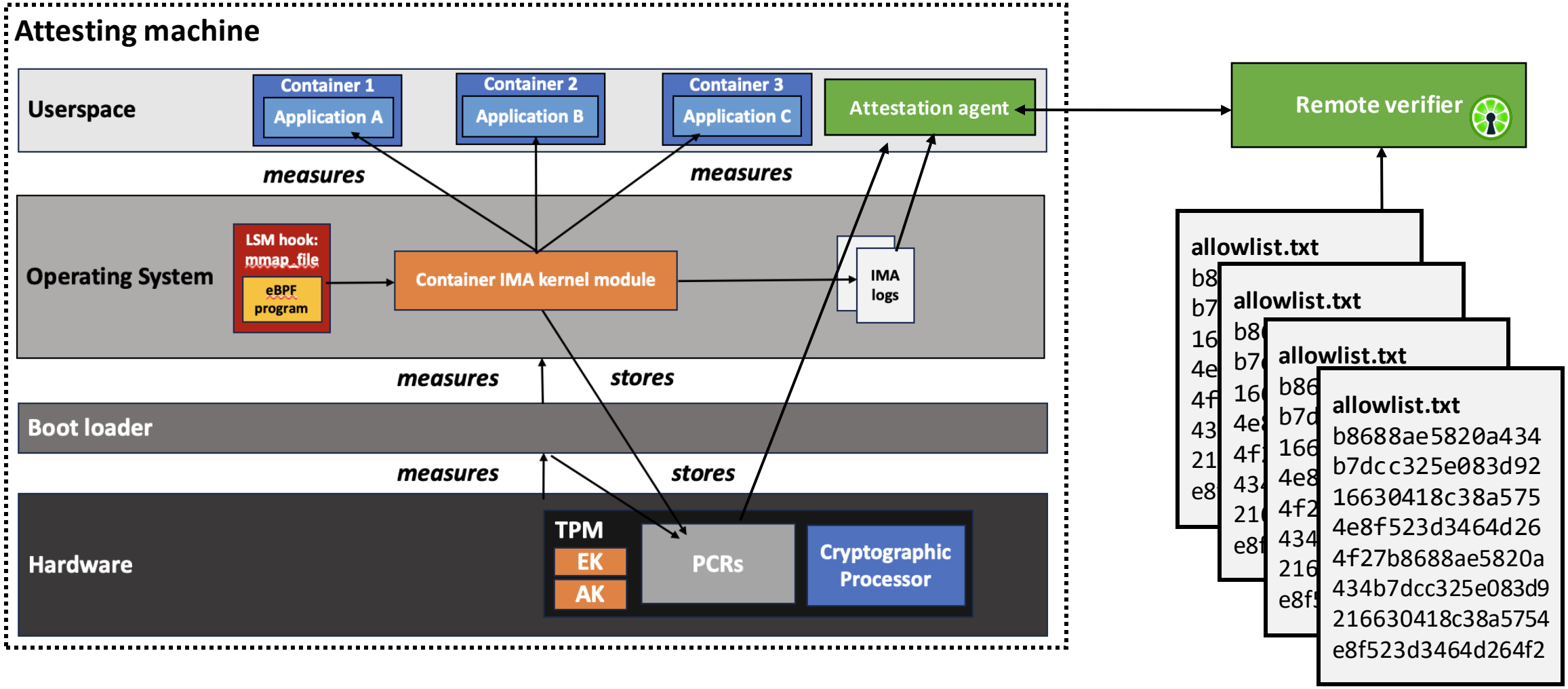
Extending Linux IMA to Containers



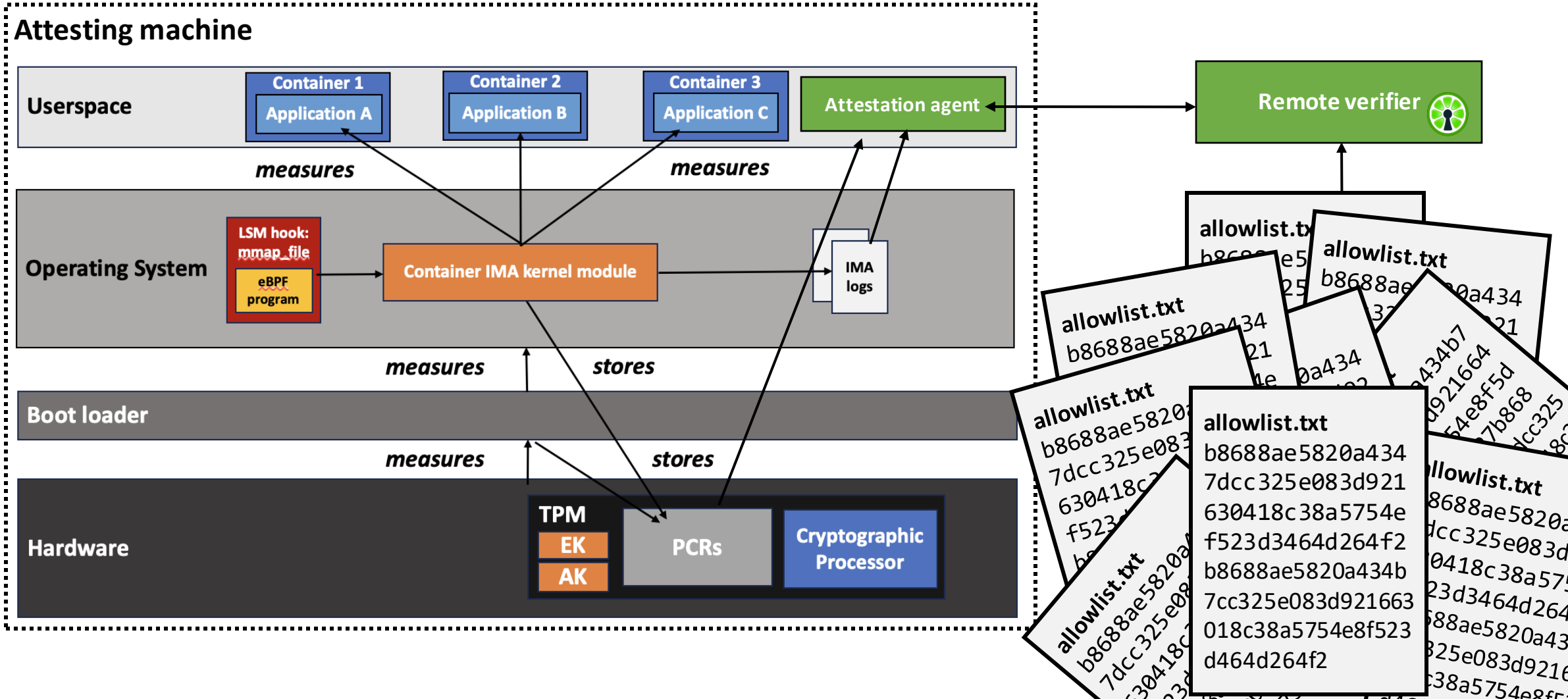
Logging Namespaces File Integrity Measurements

```
[[avery@fedora container-ima]$ sudo tail -n 25 /sys/kernel/security/ima/ascii_runtime_measurements
11 56c23fc8baf7155d5e50797c55b0a0436eb4f1e0 ima-ng sha256:5353978a6cc92dad314d0ef0bfbdec1f84241b77aa12b06aba221893fee8c728 4026532423:/usr/lib64/libpcre2-8.so.0.11.2
11 cf5f9b53ad9292dd5759fcccc49a643442deb583 ima-ng sha256:0b50ab927bd942ef6a7434e16f8819caedcdbfc5445176a7eba6990d2cb2e233 4026532423:/usr/lib64/libcap-ng.so.0.0.0
10 5fb55ea1517fb800aea13744cf6f8b9b366ebf0d ima-ng sha256:0efb18f93ab7c680ba28ba9bc50c3fabed9fa49d22e18a76b381039cfd01d4cf /usr/bin/containerd-shim-runc-v2
10 5c4f7bddfc3988228ca9d50629d524b4dacb1454 ima-ng sha256:d3f7d10e296e5c626ea78539cb38cd8dffd043bea3627da35ce3b20c0ac68014 /hello
11 eec36e004d3dd397484f9302bfc209b5e98a91b7 ima-ng sha256:aa15dcbe503ee00f9f72924e8bea3b0c9bd42ca5205c40e70dde9d7c963e56e0 4026532981:/hello
11 f6422a7bd7c8cdab8de4130492ecc3b88918447a ima-ng sha256:0458c4bf9471e7b2083b4fc1d3f8b7632b2b2fe1f54fbaa2b43d8b37b1e53690 4026532896:/usr/bin/bash
11 bf122367ae1321e9d50a35a9578fd9c78f6af526 ima-ng sha256:21d54feee92cd42390a9fa151f8950813ecd5eaf8607b3e353aa4742a3cff08d 4026532896:/usr/lib64/ld-linux-x86-64.so.2
10 bfc24c544fc3f85107c65e69856f43cc54ef72b4 ima-ng sha256:415a5f6f063d6b6c0183947708651e5424b3c38d68357fd23103ad7c56a2a3cf /usr/lib64/ld-linux-x86-64.so.2
11 828866f89825ac2b847c97b5189a74ba38151729 ima-ng sha256:8046a139aa8590f8004da1319b64c09194596dd5a0abf59020a8568e9b6d61f1 4026532896:/usr/lib64/libtinfo.so.6.4
11 c79143cc2fc5bf4780b9a35a02acaad81e9a28f7 ima-ng sha256:be13ff2194f060dff73c96f317d16e3a2c380ba3beedc1b485af866b3b7e4729 4026532896:/usr/lib64/libc.so.6
10 7393b51a9384e4254a9c8df419309a41fac0d5f5 ima-ng sha256:9f2e4d479a9a7d7e27e639701da4ffbcfb8ff40512b5c676ac42801058847c28 /usr/lib64/libc.so.6
11 3f81e07160ed9c5a0306d04070f222e73e25f405 ima-ng sha256:e5fef662f3f426b94c10d288a7ce06caa14bea7b2452976232b8d20b99d3c61e 4026532896:/usr/bin/grep
11 35d240dbf1f63cef20c3a374c2f02055da7477e0 ima-ng sha256:5353978a6cc92dad314d0ef0bfbdec1f84241b77aa12b06aba221893fee8c728 4026532896:/usr/lib64/libpcre2-8.so.0.11.2
11 509eed1e60450cacb7a50135b0b5bad68bfdbea4 ima-ng sha256:696e58e522641b5e1392f8927f1ec6da7dc2227ff224f9341bf795108603f9d2 4026532896:/usr/bin/dircolors
10 60776682416701d59dc629e089d78c6e5b09c9a5 ima-ng sha256:9f4a5f1f38860c5479da080378a632636d818675b3f19849a4c43fe5242beadc /usr/bin/locale
11 a8644b70da2f5c21375daf0282b54ba14a664475 ima-ng sha256:e9d92cd921a0aff13e408f1a2584d1d1bf6d6e385e4587ed315750de2e3a4afd 4026532896:/usr/bin/locale
11 244db78d5a27491ff64dd2e4151504d87f5dab8e ima-ng sha256:f67b8429b6c88aed90d42f0ae5c10cbd0db870999f07f9ab64b81920557cf243 4026532896:/usr/bin/sed
11 9b1628bd57965c0e533792d7387d7aed7f325c7b ima-ng sha256:2bc581d5f250e8cc107293dc20146c5ca4c284542fe2a710ddd7a86d18922689 4026532896:/usr/lib64/libacl.so.1.1.2301
11 4f95cb7d1f8eeea324de0daf4f991ae7f4d8d5e9 ima-ng sha256:f60ce3ddcc706168ed8af61c585782e841e242d3053132bfd60e01f9980b776a 4026532896:/usr/lib64/libselinux.so.1
11 930798123fa89441440093cd8f9f1226a07a6e63 ima-ng sha256:29bd22f15758028d3a11ed853b9fb93156cc19915fdb844b73e3075d3ce6510b 4026532896:/usr/lib64/libattr.so.1.1.2501
10 39e08422189f153283aafba2fa32240fb2149177 ima-ng sha256:d91502c3a044c776ae0c9b799b59df4fb1901aa84dcb4c26c4dcbe55cf5951be /usr/bin/sha256sum
11 07d6e54b15a424d098754beb53826dc4302e47cb ima-ng sha256:45c8aa2c7fbac7881cc7edd30d12e4584ce83ad4733d03d80eaf1a53a3b555e5 4026532896:/usr/bin/sha256sum
11 e55e3e1e1b707e9b0a7833dae9ef518f9cdf5d86 ima-ng sha256:a034c7cb9eaa990a1e71ff0b72b689b5a311de8117a1bdf8191cce5f6157fce7 4026532896:/usr/lib64/libcrypto.so.3.0.9
11 c4c94f9689565e866c0fd79e53da7ca46f3deb7b ima-ng sha256:d6c93839cc0e7c29fab74d08bfda639ce776c594ac77a4704160bd5069b9a7e8 4026532896:/usr/lib64/libz.so.1.2.13
10 1844bd922c570347569afc8ca2551b0c26302661 ima-ng sha256:8a56e729fd7764215090c1a02781c465ddf534a50b602f76b3cc33c19e013bbd /usr/bin/tail
[avery@fedora container-ima]$
```

Attesting Container File Integrity



Attesting Container File Integrity



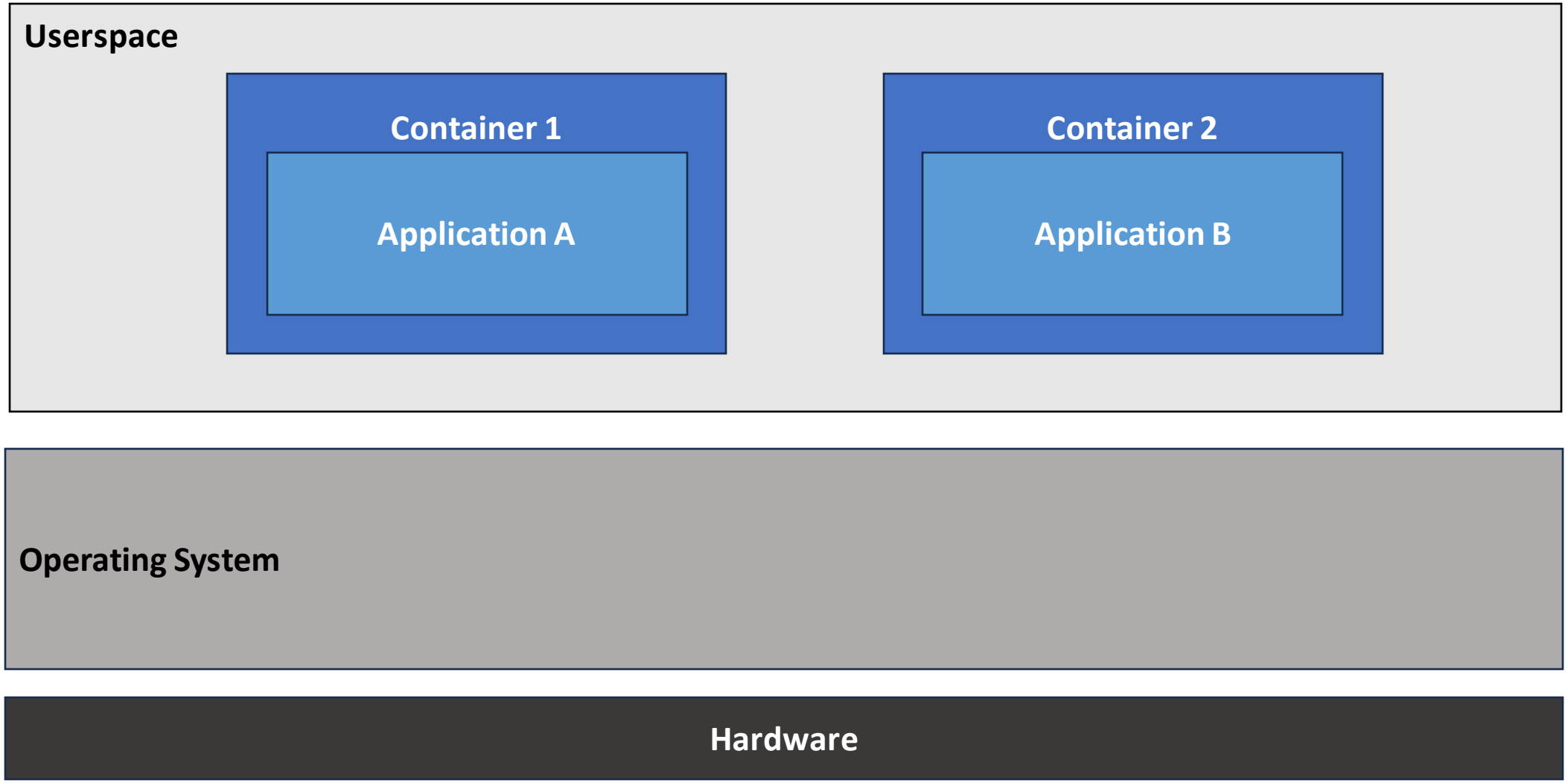
Measuring Container File Integrity

```
10 f19ce52e0da0a2489f15baa8eebae00c29893bae ima-ng sha256:5dd8d7e685866b396233d0dc983a09f7f63eb4e241e379f69519bfd22deefcdb /usr/lib64/libbz2.so.1.0.8
10 de0c5e24e84dd5e78e79458c1ceb99d671f67c8f ima-ng sha256:3410d3e62b520547a97fb1ff9bded715eca38a28c866e8132a832676d66c558e /usr/lib64/libnghttp2.so.14.24.1
10 4ac02b11498baf3d2a663d70b4d16f83df58bd7f ima-ng sha256:3ec4d2bcb756f8477882c5ec28b0956dc5a335e91b440659559ee515b0472fdd /usr/lib64/libidn2.so.0.3.8
10 760d7fb0c53c4f8560874c21e7e5b4365bcc1f09 ima-ng sha256:fba7bfb231f8f2ad531ab843ca090946419d4b4972736d7a515edf336d809f4b /usr/lib64/libssl.so.3.0.9
10 c2e4f9b0bdb893606dd9d61d508f01c3f9a0846b ima-ng sha256:3523bd98974ecee6d958b0e557ad52bd591aa099dafe62ca664382600e3db68c /usr/lib64/libgssapi_krb5.so.2.2
10 1df9265a6a92466bed049cb8bb80812a5e92cb85 ima-ng sha256:7effd55d6f158b886c62d4c1f4738f974b3dae504c7bd360c56011916210a921 /usr/lib64/libm.so.6
10 078db92ba0cee0474087f55799a52f4a87c9496d ima-ng sha256:db95a1c4936a1be7f27669a29a974cb68504971781bdd2a5618d8d9f6dc531f8 /usr/lib64/libblkid.so.1.1.0
10 4697e26e4681c7d1568ed7f75e1600809e593237 ima-ng sha256:4d1428559f9627cf1cce31495db93a262ab30e54be3a4eceafb0fe89d42d71d8 /usr/lib64/libassuan.so.0.8.6
10 a7f09075709b6924869864539ed76350d33c366e7 ima-ng sha256:d4238c8a4c739036ed1ad0e950f86e6aaaca679db7dbc0ba04599596ccc3b25c /usr/lib64/libattr.so.1.1.2501
10 aa43747cc18a68ef0eeb1ebd84fedc24f5d57534 ima-ng sha256:321fae59626e3cffa040fa043bdff3b2ef018c53e0dce4f5d9d0a0bd4c2173b6 /usr/lib64/libunistring.so.2.2.0
10 61d5dd8f7710786523b261a7400ec44c686e2db2 ima-ng sha256:4a4401c516ef79cddc3b5d89766af3bea303e1a6c5f370f62ff74e0d1b64a28d /usr/lib64/libkrb5.so.3.3
10 f903c2f116700d40565531f5dbf802c8ff52091f ima-ng sha256:8c79c9b0f1f2820e81cdd766ef6944671bc06b5cab0bdf8a10e6da22fb845197 /usr/lib64/libk5crypto.so.3.1
10 3e14e5a997dfaf76602e5041f15acdaebae53e54 ima-ng sha256:08ee3c1b277f3e6edc8a94bd413e1af56bec557a487128d155340aca8e2c3922 /usr/lib64/libcom_err.so.2.1
10 95f846e7589eec0a996d288bbe8c14f7560ea654 ima-ng sha256:652a3e29fd7926c40a0089213eacba824d80bfaf47ed06986c53ddd50640c93a /usr/lib64/libkrb5support.so.0.1
10 360289da11f86c21a1e9de27e98a5980f70061c4 ima-ng sha256:22eec95384753b88f0e6660bfdc04ff74bc5aae828f873acca6cbe048e83fef8 /usr/lib64/libkeyutils.so.1.9
10 1345ebcb46c75e717ddbc96eff95e7c5060f8ee5 ima-ng sha256:78a6e7fa6c4c0d6e0fb590e0414df9be58da8bcaf58c77e0ac6c17703d0de9e5 /usr/lib64/libresolv.so.2
10 e515c9be0f949784ca8fd4331e32f4b52afef045 ima-ng sha256:c1d57fabcfc43c8bcbd4ed59adc2d0dacc185c0cb9bb903f569acdf1885d7926 /usr/lib64/gio/modules/libgvfsdbus.so
10 b96efacb26e96fcf71892ec4c0ac0518d203f284 ima-ng sha256:343a0693d3c6bd17c4c782a5cf147fb5216e1ac1c2a8eb6c96eed6cab2da6912 /usr/lib64/gvfs/libgvfscommon.so
10 33d7c05fdaf8479b4fae7e2f3058b6e99ce77d9e ima-ng sha256:21de2fd6e029b6d2b087fe03dbd30c7d61e825b41135ec7d93a5d0d3172bb285 /usr/lib/systemd/system-generators/anaconda-generator
10 54f1e6d5fb1b847a067a291bdd58070ae2131e21 ima-ng sha256:492e61ea7479b08a47b632195594b790dda24f2249841d3f8603ca1f8927087d /usr/lib/systemd/system-generators/kdump-dep-generator.sh
10 22ac0619c5489d0ed381e518dfbdb1db537d38d7 ima-ng sha256:ec486e169b4cb8995b10d56dfc191ff70b1d1d271f8a041db7a400ca92dcfabb /usr/lib/systemd/system-generators/nfs-server-generator
10 a84259c30b2df5eac6845a93e4036f386ebf8049 ima-ng sha256:1a6a9335c6a7067dd7c6345f18d95a6c3fb91bb7f027437c9079e496d227012b /usr/lib/systemd/system-generators/selinux-autorelabel-generator.sh
10 071aec4d5a167f249b01f0015858c6294318a01be ima-ng sha256:b9a432f6a4d053510bd6e281710d46d6f0260faaaa7af7f6fe5ce091f1688291 /usr/lib/systemd/system-generators/ostree-system-generator
10 740e483bcecf7652f47c24634478b8c8b07b5398 ima-ng sha256:a1608e1ab5fdd098648adb7b6b2fba558122ba4444e68867280ea4f62446a70b /usr/lib/systemd/system-generators/systemd-bless-boot-generator
10 975ec82997c41041c614b8fa6527960179be56ea ima-ng sha256:d05f2a0f18cea107c0a8b5f77cd8401837051dfc9045f31a380ed6cdddd3276e /usr/lib/systemd/system-generators/rpc-pipefs-generator
10 fe5e080182f8faec7a6d7570d28fcb5a7a4f9ea8 ima-ng sha256:87c3105cc36da795291f36df7affa897dcf61ca57e5647d321fe588fac051af0 /usr/lib/systemd/system-generators/systemd-debug-generator
10 5ebbaaa31944d55d1dd3db6354bd2fd8cfe63416 ima-ng sha256:cd824dbd7a823ac1d1f91d4c5f56ad2030bb00bf4a1362451297cbe9376a9de1 /usr/lib/systemd/system-generators/systemd-cryptsetup-generator
10 279c5ee1949f48c07395687d28dc26c571f59608 ima-ng sha256:0f9104065fd0aa4fa462041ec32a640cdc0f5d6017d90c804b6db66dbc2d6f1c /usr/lib/systemd/system-generators/systemd-hibernate-resume-generator
10 2909f59284da197a759dc7f46ca8b3b51d2b58da ima-ng sha256:3f6af7b9d46bda2b4f014bbe5c2221d6cd58244cd0252c62f3a98b4ae2022dbd /usr/lib/systemd/system-generators/systemd-gpt-auto-generator
10 d01b83941c9af8364b9afafe6c29a3565bcdde72 ima-ng sha256:3dc8f7c38572221ca1129f7a9f9768301a6492eb42bdcb39c866decaad8f8c1f /usr/bin/readlink
10 fcbe7939ba91c4d9c0ac2f1d4bae82b0d78e5f61 ima-ng sha256:85d73578754e4890aa85947e7e2822d3c807036746de9c86c486ae95e4bcddc2 /usr/lib/systemd/system-generators/systemd-rc-local-generator
10 2273e955e4f88388c2b94cc76a43f01e8ae44d57 ima-ng sha256:4b2db6a69545edf20593cd54b32848c36ca91ea153e58a9b80d1554c4a887e41 /usr/lib/systemd/system-generators/systemd-run-generator
10 52fb939e621a529e62213b2ca04a95a9d5abf75a ima-ng sha256:e35d38299b2290 8dff103e475832074cd4ebc80a8da37d80968c9f79450f1de4 /usr/lib/systemd/system-generators/systemd-system-update-generator
10 3e927b8d4450d9ae31dc50ebfd1612e4f51da7fe ima-ng sha256:f4e587935ad3dc682330bd5c32990f478d18b7ba4e77a6b56761d46f16f4a7b0 /usr/lib/systemd/system-generators/systemd-integritysetup-generator
10 c79e1d6ac7536e246756c43c8c251dc83afa9419 ima-ng sha256:d578d8cd56840cd7526541fd5b9dbcd510036fc93376178ce9c05f98fb879a2e /usr/lib/systemd/system-generators/systemd-getty-generator
10 936f70da9aee5165dd13d1570ace77e264241ef2 ima-ng sha256:0b9d518bd8b553925f15d1488c9468657ab1b04b8a417abfdc76bfbeeb98ccb1 /usr/lib/systemd/system-generators/systemd-fstab-generator
10 af939763dc587f80308d1d4fcf1f792ac085d599 ima-ng sha256:86bd42b539dd1069b51977fbaf8029efee3877bd62a02a08debe88e00e393258 /usr/lib/systemd/system-generators/systemd-sysv-generator
10 039c5232df349667b77e7742ce6aa93e45e1e52b ima-ng sha256:17284881fc812d2bfb695ec8384d037ce0cb730cee80ef6ced981da4d390e444 /usr/bin/sed
10 ef908858ff79d2a864db3ced9df8be18da322eca ima-ng sha256:5420d20c19624c38903ace2393bc9a7ba75bc690b49e79f66f9122f7680958b1 /usr/bin/grep
10 dd8895d5194987502ca9609dcec448f5c713dfcb ima-ng sha256:a8acfbf9edae0019a839a5de8f1e3c343fae2e6608886fc143597d15e925823a /usr/lib/systemd/system-generators/systemd-veritysetup-generator
10 61e0185f3738e8237a667ece59f1c44418f65b89 ima-ng sha256:571d6e8da3464f806791cfb389ff1182807ecdccf30a4138659f6ce96090eda9 /usr/lib/systemd/system-generators/zram-generator
10 873ff40780c659eefe79cc7bed3c1a7a23c4f766 ima-ng sha256:842034a0d1665ee2c1c8dfa8fc2e16067709ee26e1e69b21f2616fae2731a6e8 /usr/sbin/selinuxenabled
10 31890f0e704d132e3cd0578b79e8437252d206ca ima-ng sha256:eb0bf4d851c6e5cf0030bb97b8a41ddf52df8bee2fb9ee581c0bcdc9acccd9c9 /usr/bin/systemd-detect-virt
10 1fcc3d607bbf2cd6fe670b4796774511fd51d71e ima-ng sha256:c7eebdaef03a516e43e284f44da0cf8aec402905ac2c97617559759 89dcbb9004 /usr/libexec/podman/quadlet
10 abab36c9821e0d7b046a6dc3397cd59d2de69a5c ima-ng sha256:a8acfbf9edae0019a839a5de8f1e3c343fae2e6608886fc143597d15e925823a /usr/lib64/systemd/libsystemd-shared-253.12-1.fc38.so
10 710f7249b054c981c34e02d3d7d320e4eb3a40c0 ima-ng sha256:17aeab8a2b3bfc4e57ac450b66158d85fb525b73a3a1c8f1fe4db7b7be0459bb /usr/lib64/libcrypt.so.2.0.0
10 243031444074321f4c557fa03e5e8ebb00715df8 ima-ng sha256:8b91c3d1c6d27191bbde709c9f81fd64d3acab19049507583abec49d39e215c9 /usr/lib64/libkmod.so.2.4.0
10 aafa4c29b11a80bc181a8f3b02ca34da0c9cce5f ima-ng sha256:cc40739415b9109b7f6b2193b0c3c84d56b59176869d2e60fb2a777a74240d41 /usr/lib64/libpam.so.0.85.1
10 89cb792bd03c49528b56d0a8418a5ea4d75a8e08 ima-ng sha256:c2280ca9a7853570b839cd9f2e30df63fd344a35b77f4bcabbf89087c1f7b98c /usr/lib64/libaudit.so.1.0.0
10 6ff1675208e3a4f643bfb8eb4874e32c0351c0fc ima-ng sha256:5f0e460f25e7e6a857e9e3f2cf74644b649209bbee1baf1f1b11f6c79d0e6365 /usr/lib64/libeconf.so.0.5.2
10 23b4f599e66927dfe7801aad5dcea8e5af3573a0 ima-ng sha256:d3bac50325bef88378e138f603a259ea4e77faa8e43c21cec0bbe39d41e1735b /usr/lib64/libcap-ng.so.0.0.0
10 4430bf2a5456c0a69d2b682da33b8363f11eaa89 ima-ng sha256:800bdca7f739b5e7e3b1df029735f87b1af3adbf075b866611791 5ef5ffabd0b /usr/bin/kmod
10 63e61f470104e6e34004e39f79aedda113b4eef9 ima-ng sha256:ac8efce2afaab784c382bc7ec3843c023e3aa60bcd57467bbce3691a21eda24c /usr/bin/mount
10 63893a9fc78769e7802fd39dd591a55c4d075449 ima-ng sha256:ae48ad71be2071b1c733f69535d6fa6cb04bc244a45640443c8fe1f33cd6595e /usr/sbin/lvm
10 7ef9ef2721854e1fba7ca2b1f2a5cab0529c4b16 ima-ng sha256:1dc0767e798781e246c7cc5d133949ae4afa215b094b7529fb769b13eb50023f /usr/lib64/libdevmapper-event.so.1.02
10 fb979f67cedec4053d5520e67680f4e984691c54 ima-ng sha256:00111d55bab4cd740fa3c7aacd698ddbf48ad5a69c875a31564fc3ef4a54d874 /usr/lib64/libedit.so.0.0.70
10 c235d684439a3c45e7ebbf8be2c8ed615a623e33 ima-ng sha256:40c3345b07ce53ef46568f68cfe7a2217605417e22288dcb58708b00706d3587 /usr/lib64/libaio.so.1.0.1
10 16005cd756de1428750a5c8d41bcf8e4b6a2b5d9 ima-ng sha256:b82ff53b1ef8213d002ae2822a3716bfcdaaee13f960f3c4d68b11e5d0795444 /usr/lib64/libudev.so.1.7.6
10 d4922949c5017301ed32d8c0bdff5475d65c9be8 ima-ng sha256:17727fcedfd7b3f70d0bd200db0092d93cb95d04b1660c58fc5e4264e1004845 /usr/lib64/libdevmapper.so.1.02
10 f03afd99496878dbf331623d6ba96b702e2e824b ima-ng sha256:48d871f0b4c8401601b1445ae9d521c2b49f7904d94a2b4cb2051634eeff44ba /usr/lib/systemd/systemd-modules-load
10 aeeb62e66b65326b981d75959d5cdd9123253052 ima-ng sha256:de751a2f2b37d9b3cf88eaa90cc8f1e9f3321ea71af4f77001c18589c7ecae8b /usr/lib/systemd/systemd-network-generator
10 ae9acbd636167ae47954126470a30fe74e1596b8 ima-ng sha256:eae68291348b18e238f1e22090d2cf71c91e2e0c27e3659ce53e9a67df3e200a /usr/lib/systemd/systemd-remount-fs
10 eea54318ef43cb71ebf24f8733a8588df6672e87 ima-ng sha256:b08edfc8f0265ff8b5f7f083bdd043afec74c2d05a410777a7bc10fad7bd578b /usr/lib/systemd/systemd-journald
10 7e3eae16176c6b46371417e1bbd5f3d14b28fa85 ima-ng sha256:0c19c6b193783a3cd2176209d9c843a16515c2b2fa8d8a07b36af83174474728 /usr/bin/udevadm
10 fc18f31a1f16965dcb03a30f0647a0087fb8fef9 ima-ng sha256:3ea07ae8b0b3c1e049966ee6ef4fce3ee8adce3511d2345281746823 6e0320e1 /usr/bin/journalctl
10 543326dd16276be31b2758d5bbf3f948d2286a17 ima-ng sha256:702c2fd4d7602531cd329bf87d3f6a1fa444732e1e14797fd5d9ef47d851976b /usr/lib/systemd/systemd-random-seed
10 b70f14e85bfe5f59994115c7fa786eb1e335f8f8 ima-ng sha256:5464dbe48ee75a20beeb65c1eae5e28b77d7d3b2ead319bf214f827d2c0064b2 /usr/lib/systemd/systemd-sysctl
```

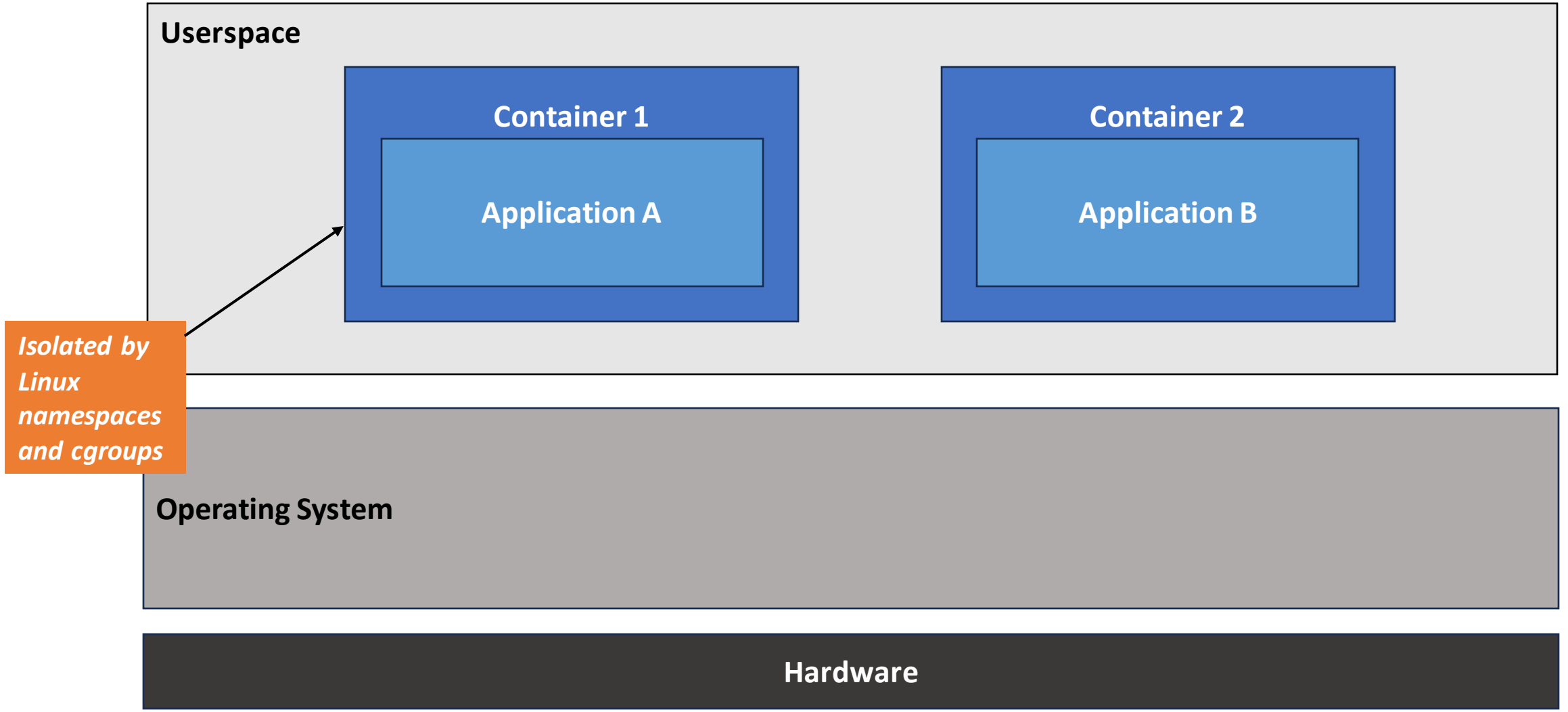
The addition of these namespaced measurements adds to an already large log…

Measuring Container Image Integrity in the Kernel

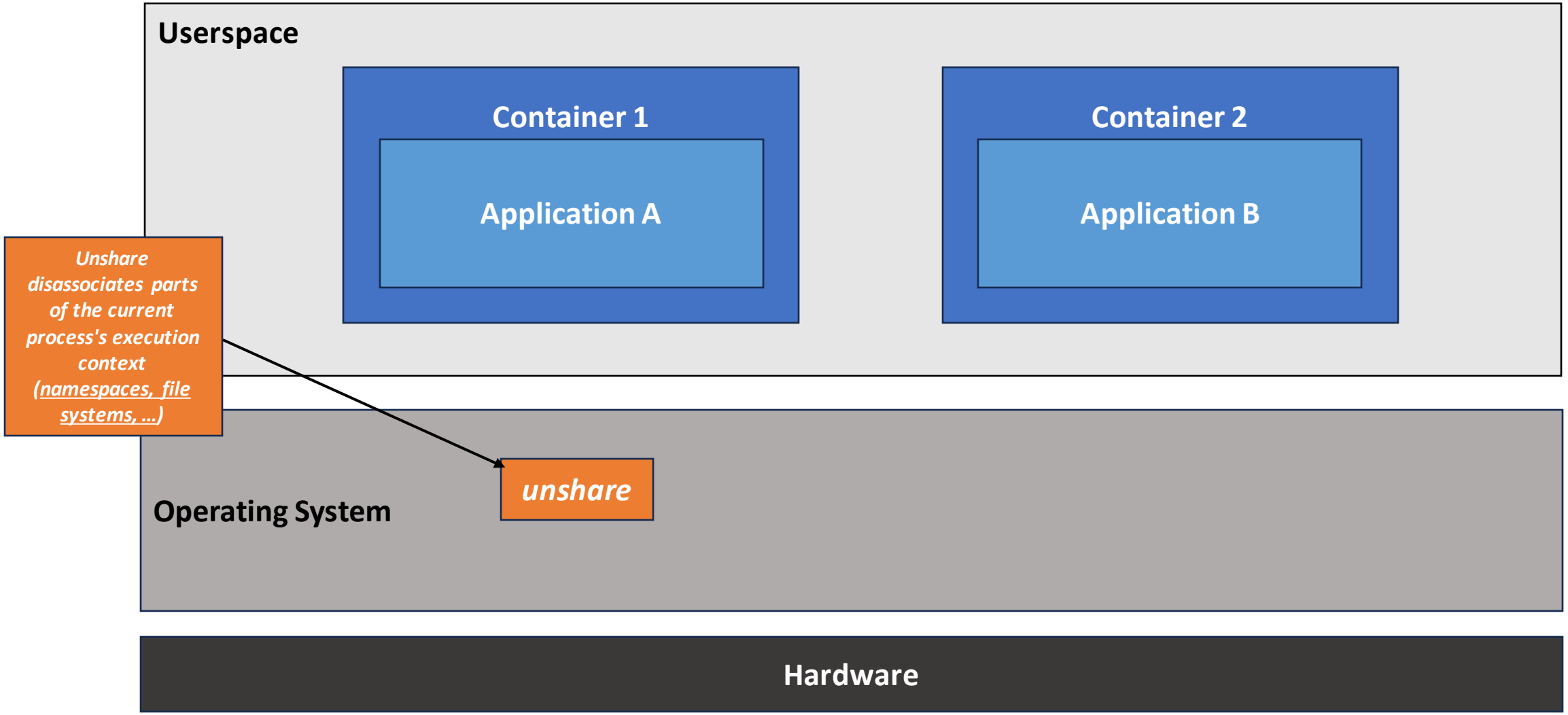
Container Image Integrity



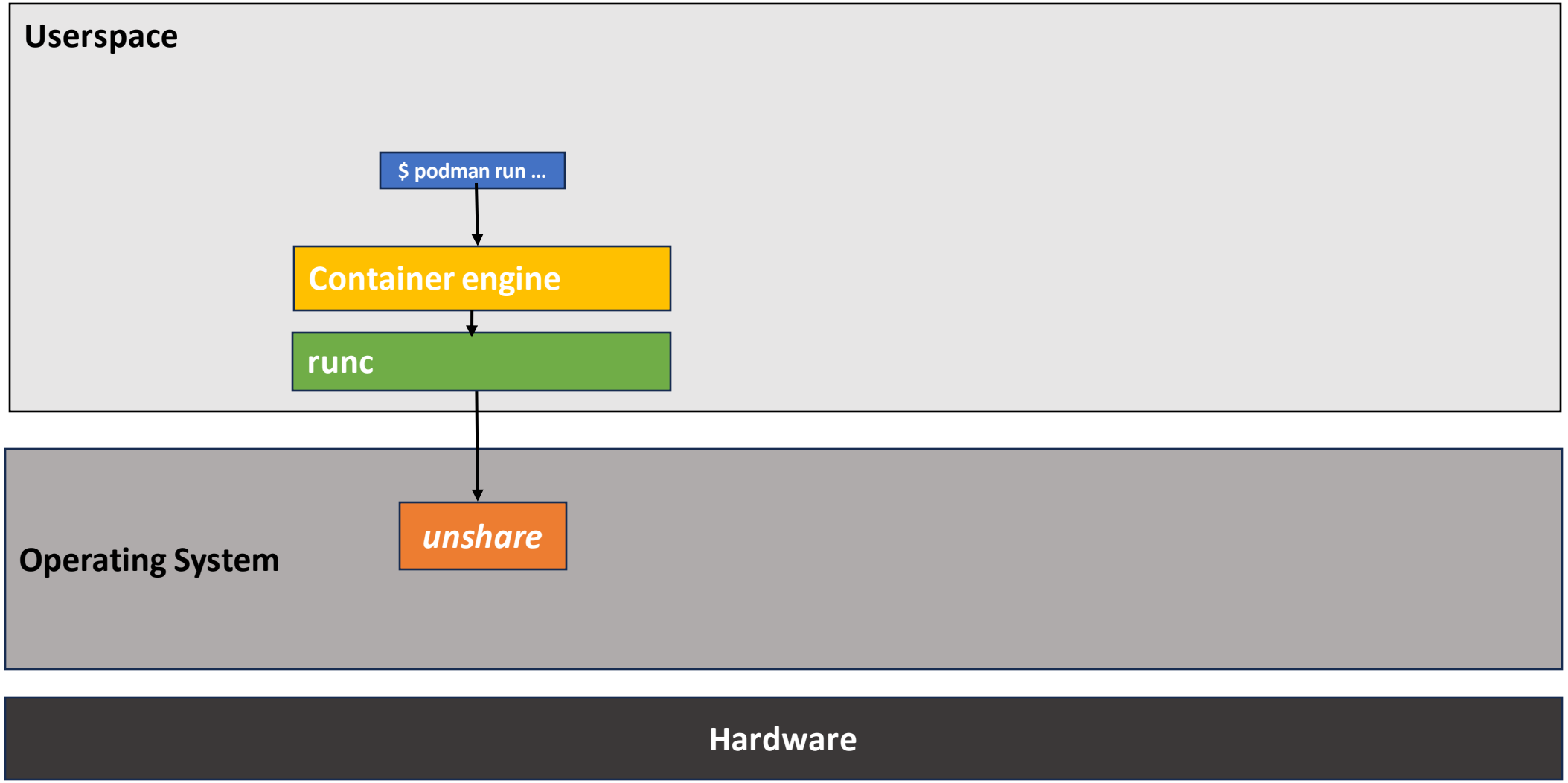
Container Image Integrity



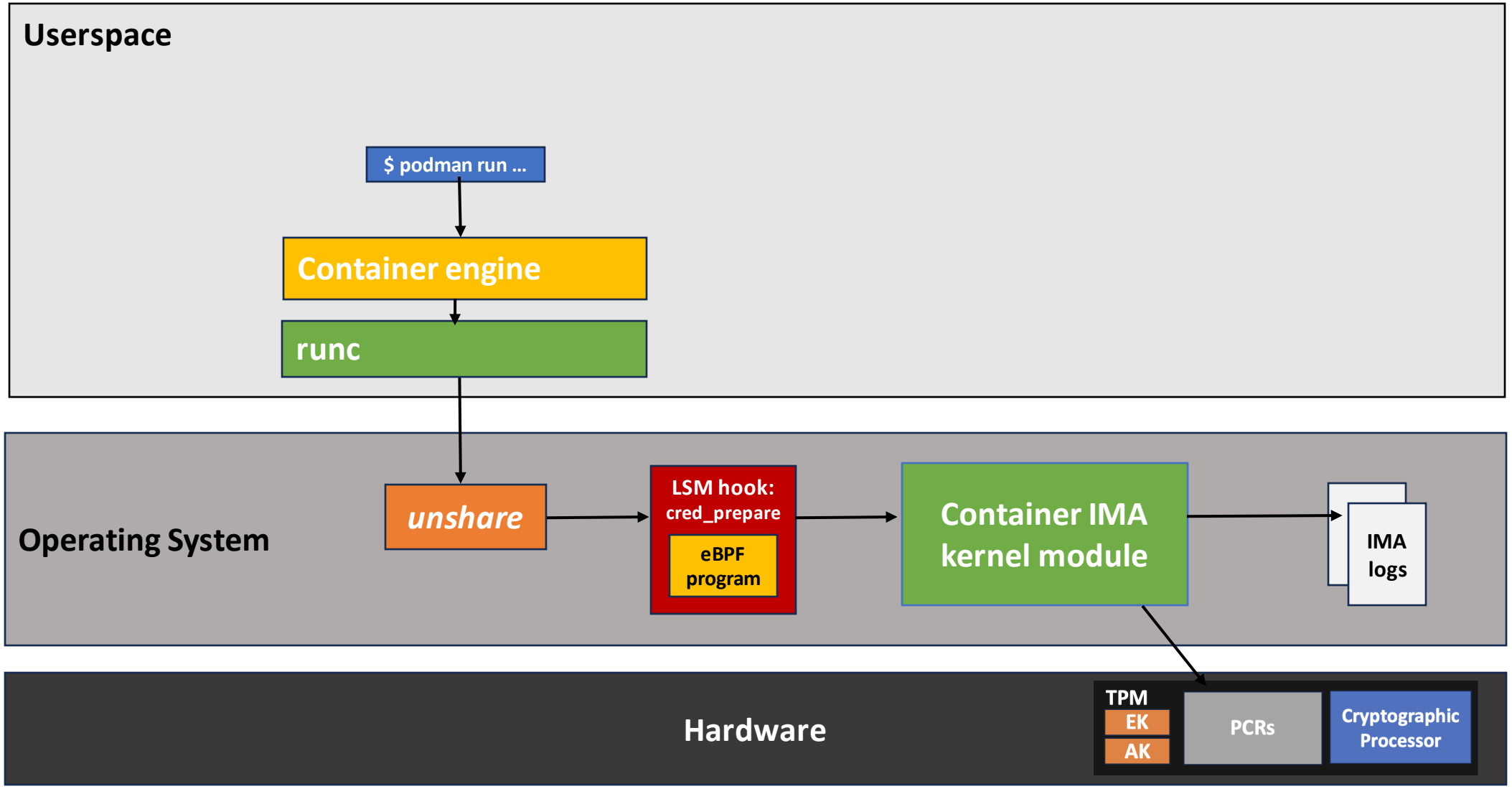
Container Image Integrity



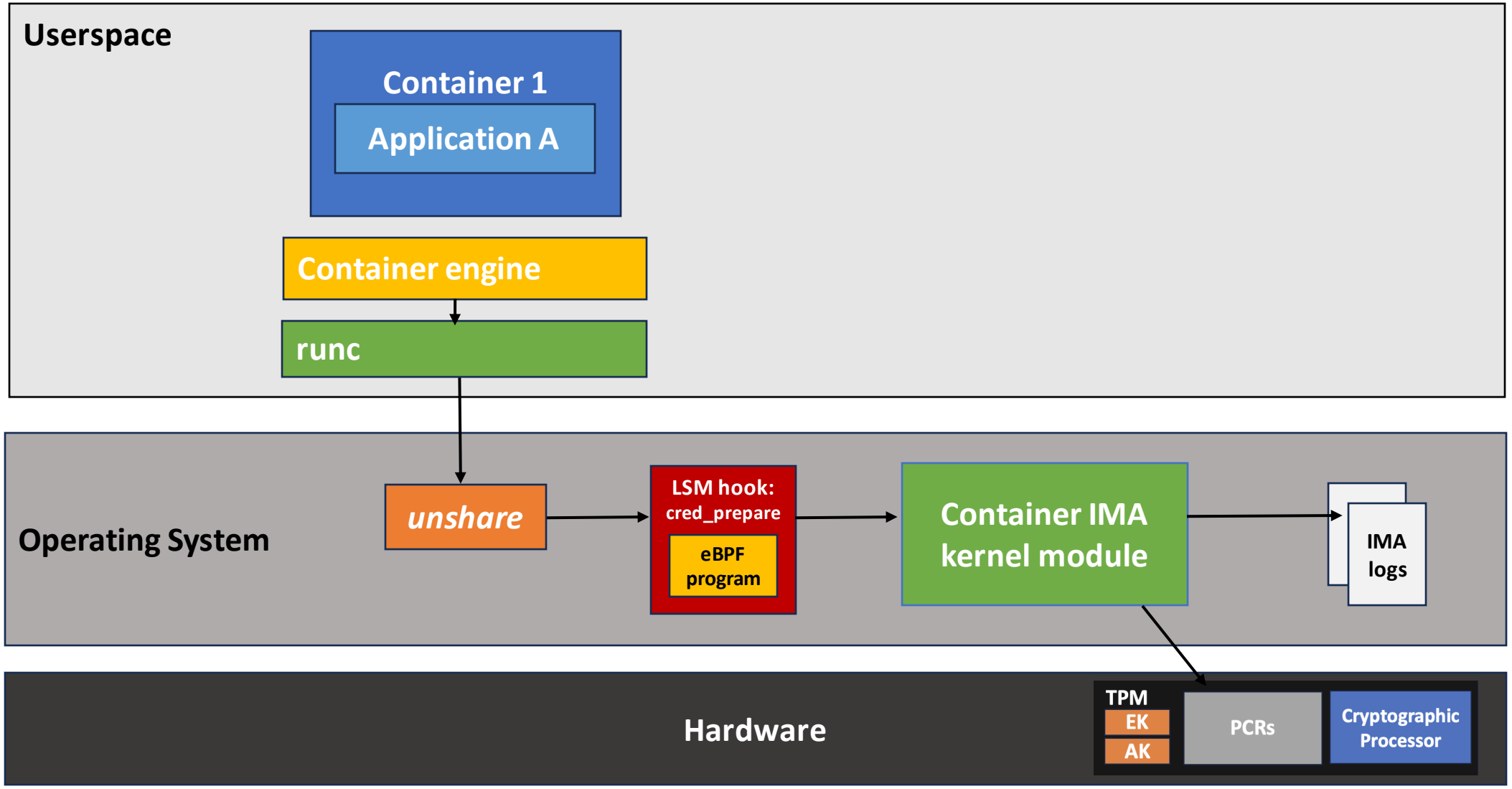
Container Image Integrity



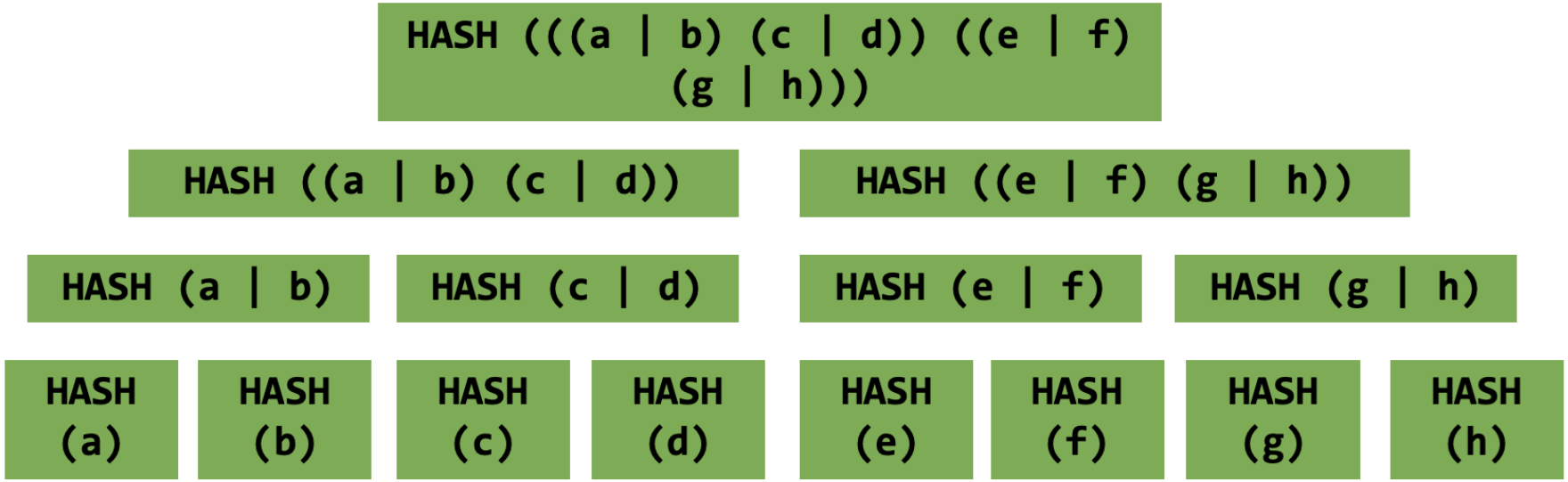
Container Image Integrity



Container Image Integrity



Constructing Container Image Digests



Extending the IMA log with Image Digests

```
[avery@fedora test]$ sudo tail -n 10 /sys/kernel/security/ima/ascii_runtime_measurements
10 100c21ea1a81be5b72a1fbc2034199a436ae5e5f ima-ng sha256:49c5fe0d8860aff1b178883d617c08fbe9b6989fe5ca20a7f306bbff22821c08 /usr/lib64/xtables/libxt_MARK.so
10 22b02541107a4fd14f28c6f4d21b0db74e984982 ima-ng sha256:f5299406dfecb8f4126ba82d896e4d890006d08d891d8809f73ee806203a44ba /usr/lib64/xtables/libxt_mark.so
10 8424ea6fd5f58ca3a7d06f9a4f06385fa2097d28 ima-ng sha256:a44a70b83f7ae8917dcf88f285827fc3e57ea8c65e6c4be75398e5083991b7d2 /usr/bin/conmon
10 fb3bd080ad9bccb8037900c2c81592afbc9a0b7f ima-ng sha256:177a5c84e9e020adf3b331f05929618caeeaa0e20aa194d24b6d26a3e7c2469f /usr/bin/crun
11 bb70f918156881c838d4b1cd7e36ec82c9409cd7 ima-ng sha256:af5570f5a1810b7af78caf4bc70a660f0df51e42baf91d4de5b2328de0e83dfc 4026532981
10 dda2d30230967156079c9094625f9a5d4e9ef886 ima-ng sha256:35d39fd6ae35e28febd6b829ea9f087c899d70028d020d31cd5c25522883a32b /usr/local/bin/podman_hello_world
10 64f52333560ac9d817eec64e43f949b863a15354 ima-ng sha256:0c5d8d4dd08a0ca857b110b7f5a6cc8b7c1c3a0fec9346037cb88acf886e1276 /usr/bin/gnome-keyring-daemon
10 23f0a155865a6ff162f2a555d472773b6b7b4559 ima-ng sha256:7fce37dbd165263705166404531c6862bd4a32e58d5bb4c055985c50f20148ca /usr/lib64/libgcr-base-3.so.1.0.0
10 8a119453d4efd92900cf3b3fc0e69def819ded45 ima-ng sha256:5eab4b5c02b952faae652eadbc0d9940cf56cb2deca4d2c6e9bee81cfa377ff9 /usr/lib64/libgck-1.so.0.0.0
10 1844bd922c570347569afc8ca2551b0c26302661 ima-ng sha256:8a56e729fd7764215090c1a02781c465ddf534a50b602f76b3cc33c19e013bbd /usr/bin/tail
[avery@fedora test]$
```

Evaluating Measurement Overhead

- EVALS TODO

Demo Environment

- TODO

Enabling Container Integrity Verification

- Current image digests are dependent on images layers, manifest files, image ids, ...
- Kernel-verifiable digests need to be provided to extend the chain of trust from hardware up to each container instance

Building trust in containers through image integrity measurements leveraging trusted hardware.

avery.blanchard@duke.edu

https://github.com/avery-blanchard/container-ima
https://github.com/avery-blanchard/container-integrity-measurement

Duke UNIVERSITY

IBM