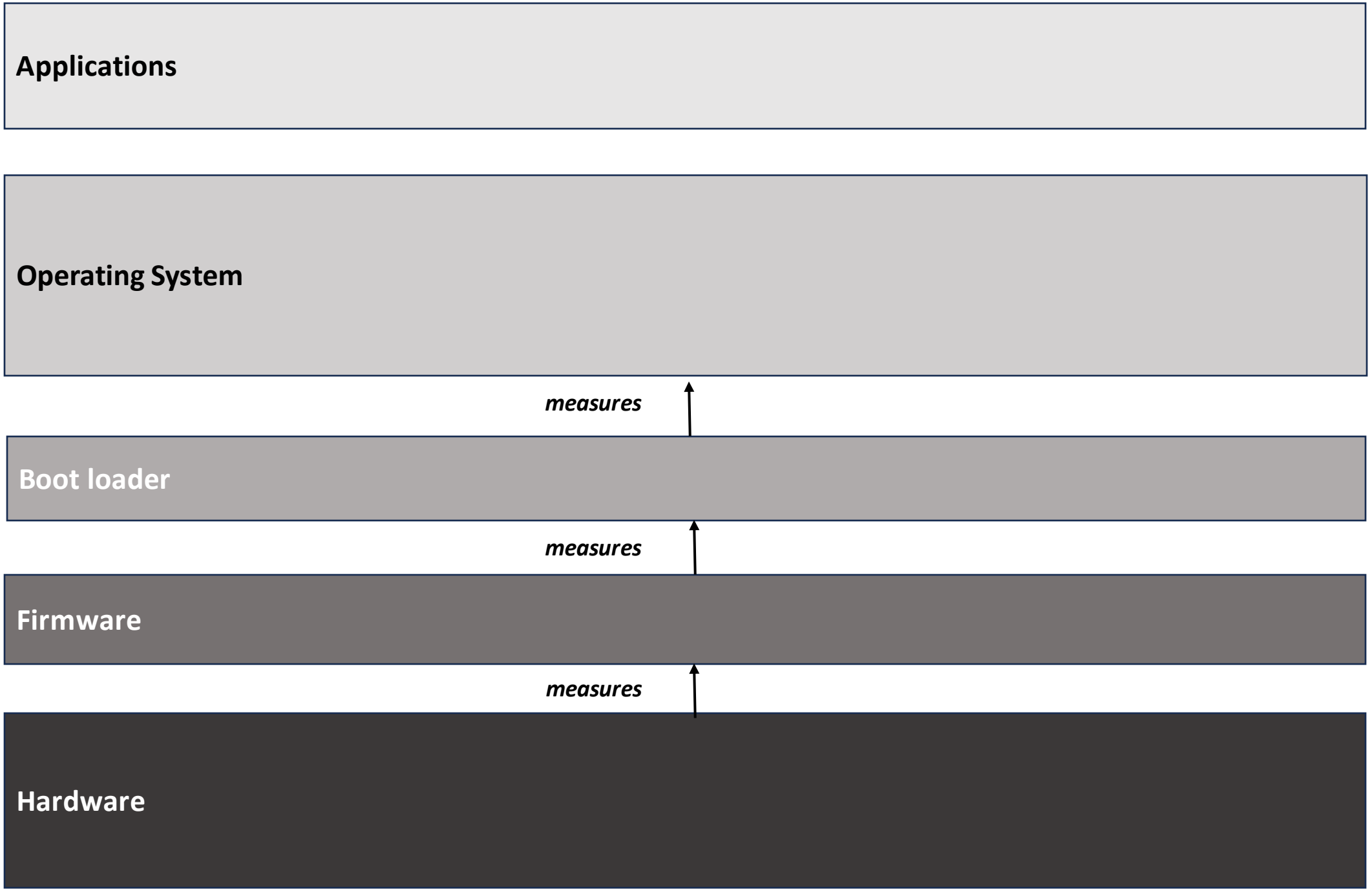
In Containers We Trust? Building Trust In Containerized Environments

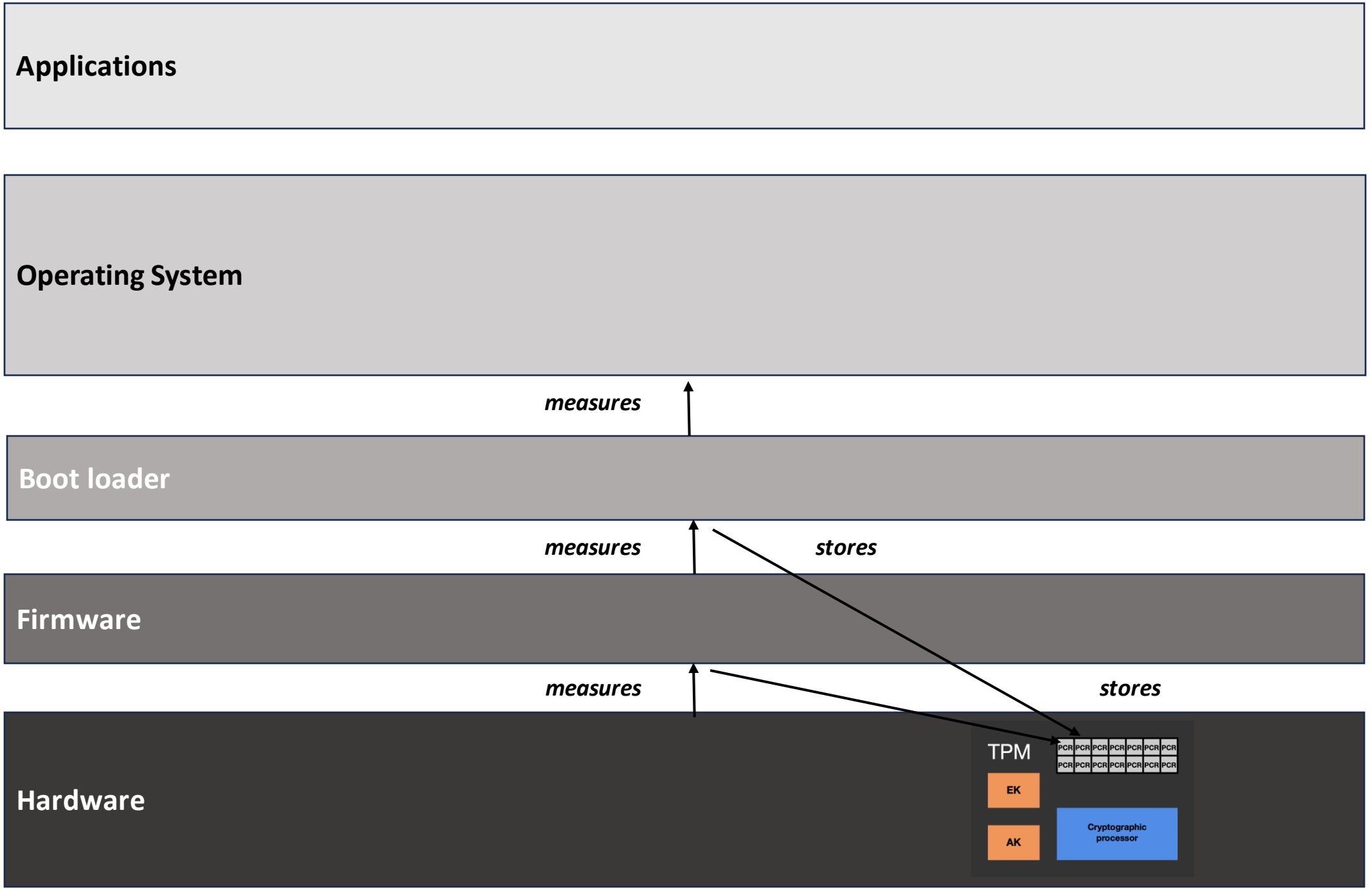
Avery Blanchard[1], Gheorghe Almasi[2], James Bottomley[2] and Hubertus Franke[2]

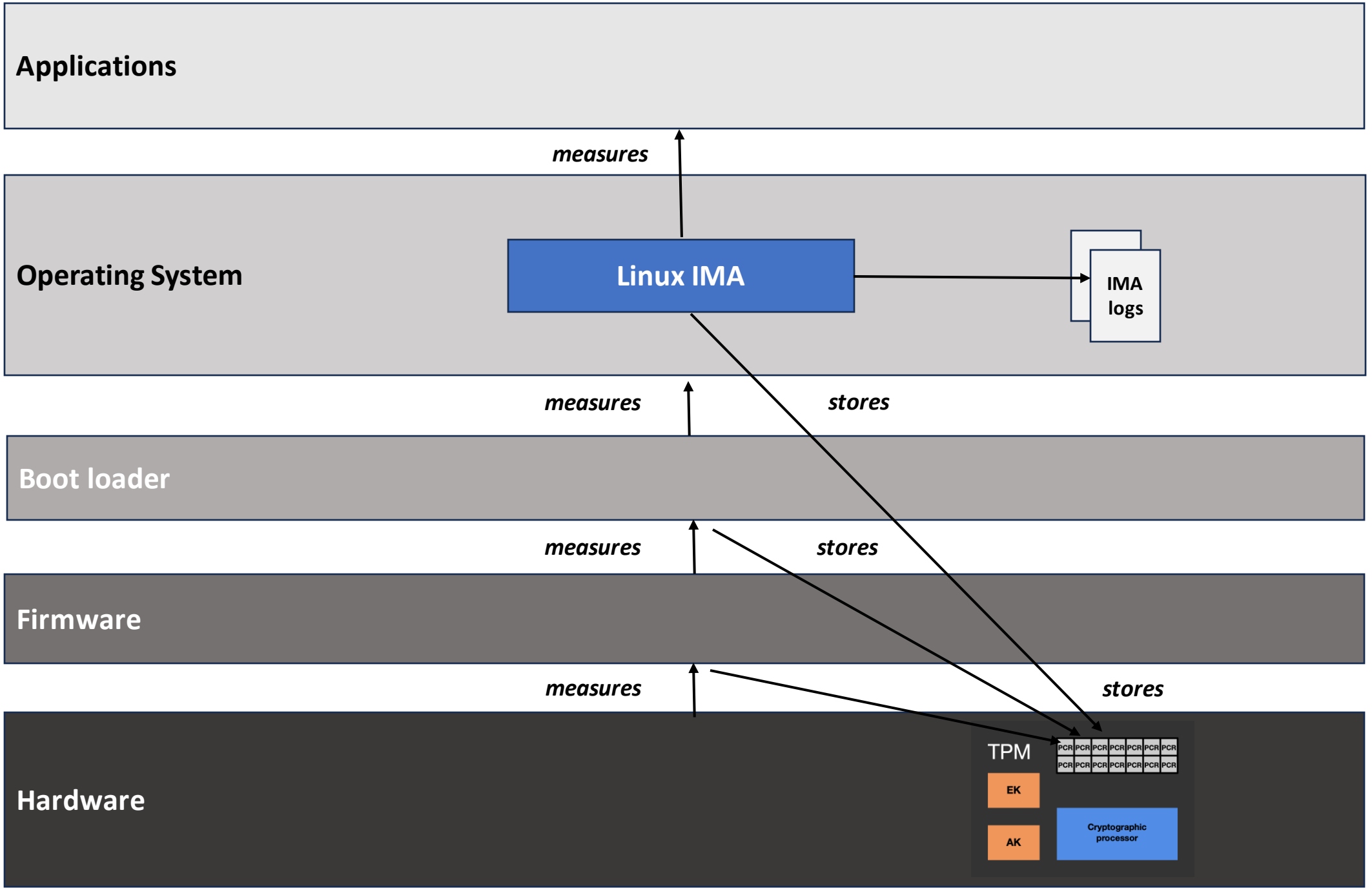
1 Duke University
2 IBM Research

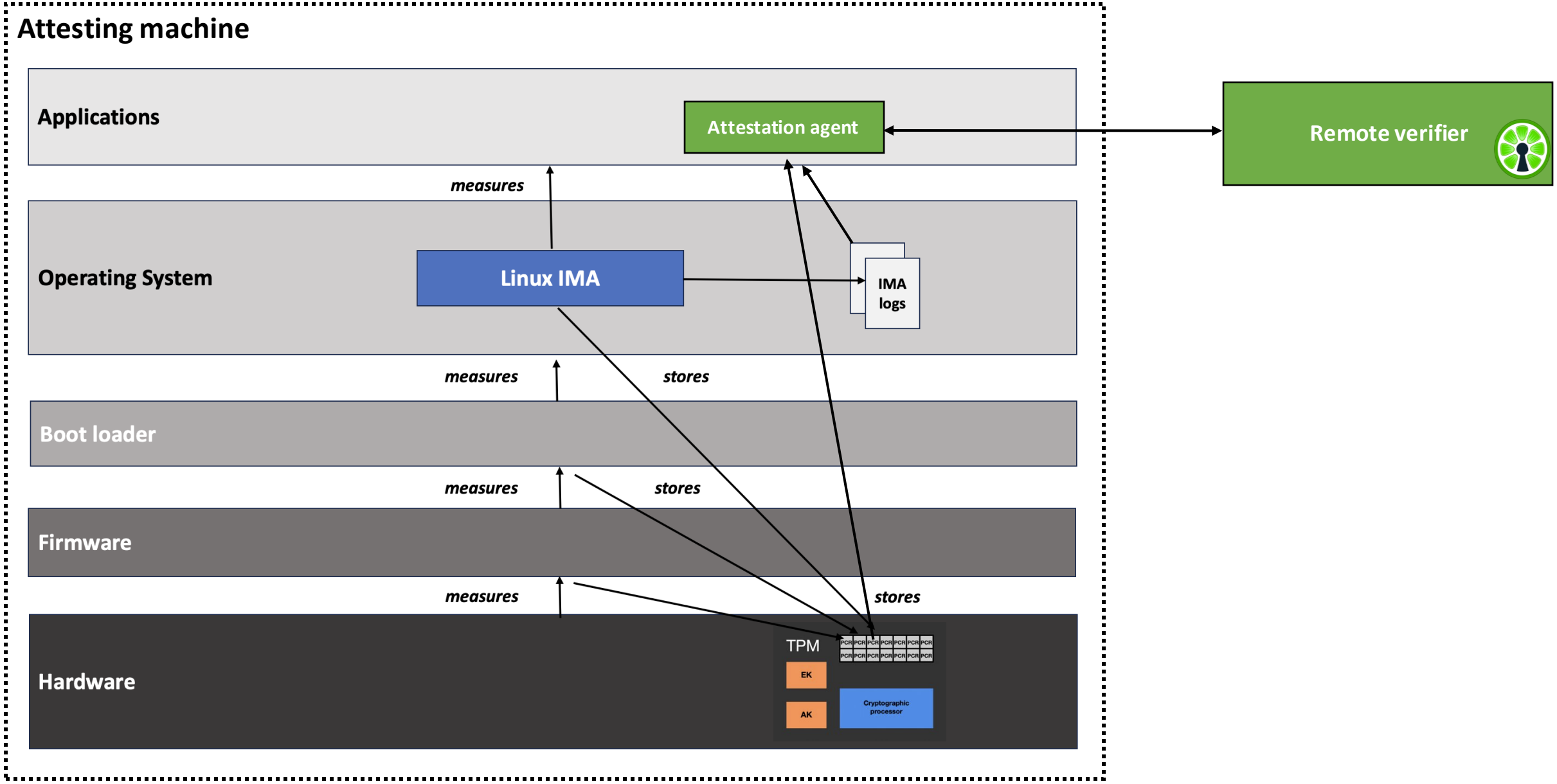
November 13th, 2023

Containers are ubiquitous and blindly trusted…


Applications
Operating System
measures
Boot loader
measures
Firmware
measures
Hardware


Applications
Operating System
measures
Boot loader
measures
stores
Firmware
measures
stores
Hardware
TPM
PCR PCR PCR PCR PCR PCR PCR
PCR PCR PCR PCR PCR PCR PCR
EK
AK
Cryptographic processor


Applications
measures
Operating System
Linux IMA
IMA logs
measures
stores
Boot loader
measures
stores
Firmware
measures
stores
Hardware
TPM
PCR PCR PCR PCR PCR PCR PCR
PCR PCR PCR PCR PCR PCR PCR
EK
AK
Cryptographic processor


Attesting machine
Applications
Attestation agent
Remote verifier
measures
Operating System
Linux IMA
IMA logs
measures
stores
Boot loader
measures
stores
Firmware
measures
stores
Hardware
TPM
PCR
EK
AK
Cryptographic processor