In Containers We Trust? Building Trust In Containerized Environments
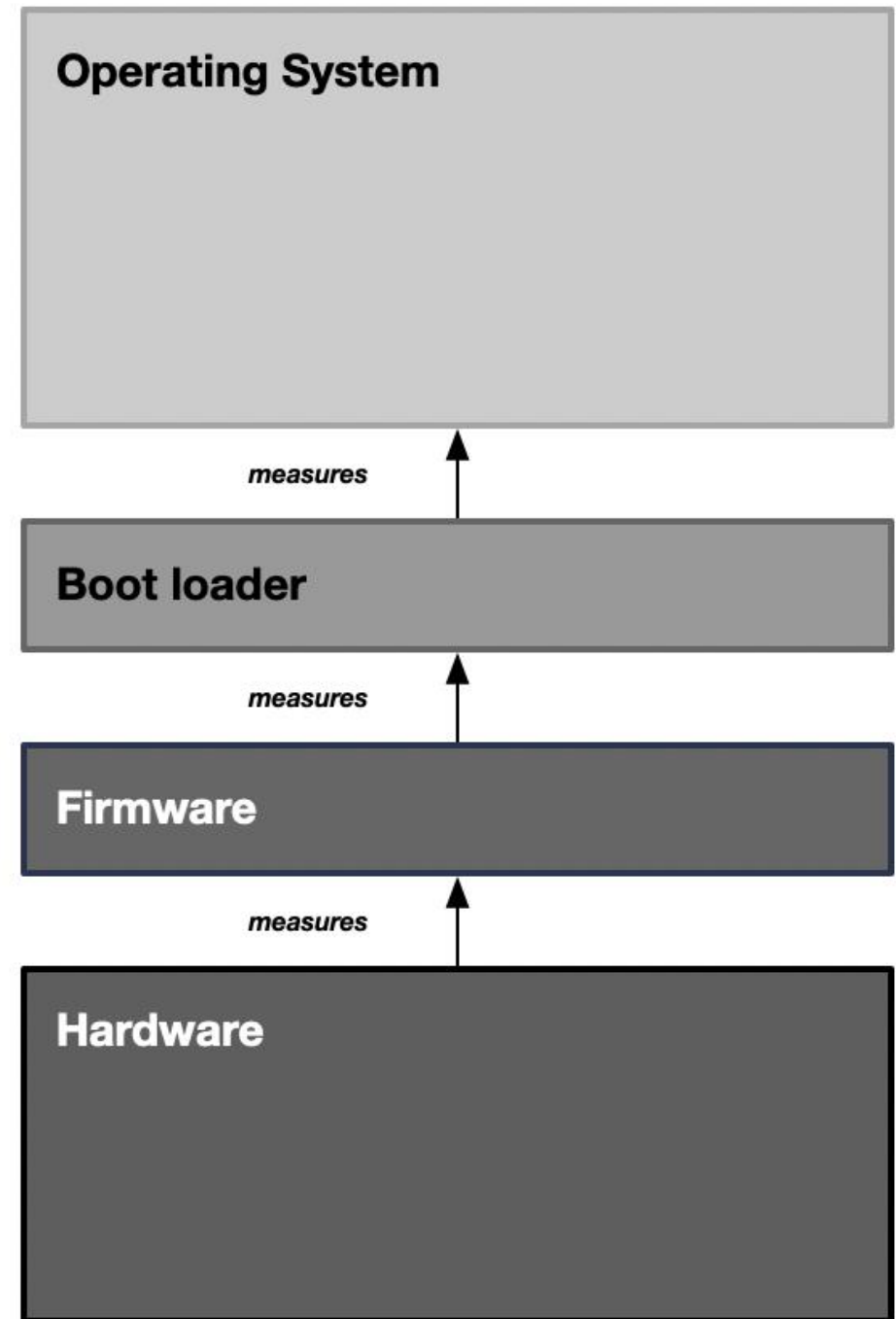
Avery Blanchard[1], Gheorghe Almasi[2], James Bottomley[2] and Hubertus Franke[2]
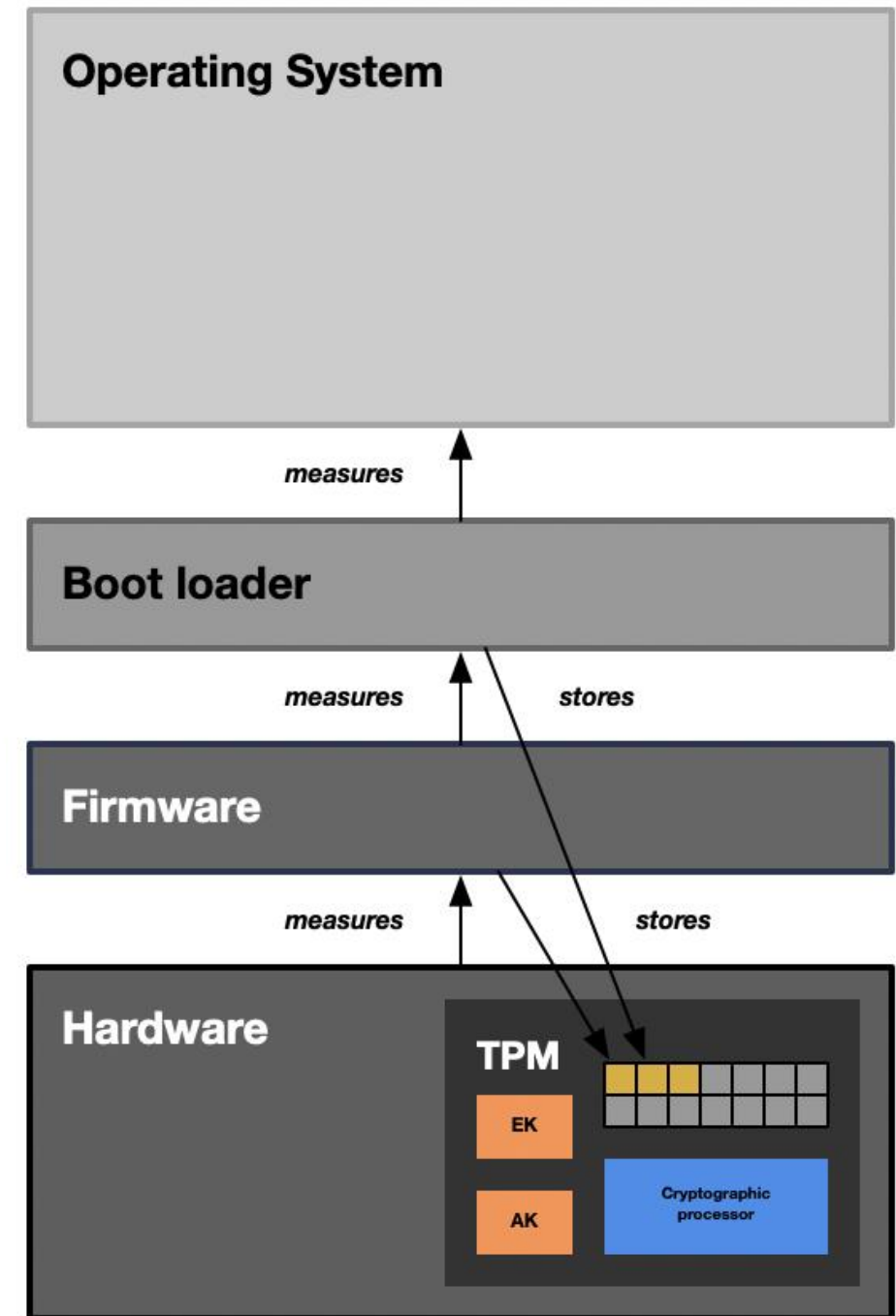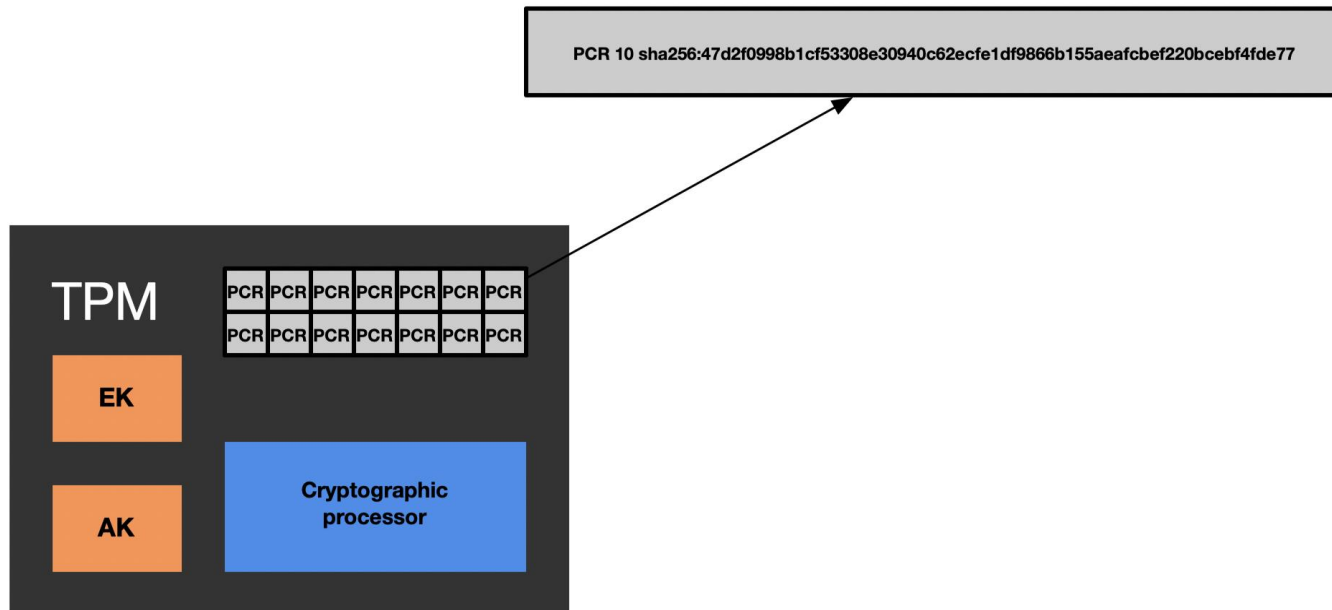
1 Duke University
2 IBM Research

November 13th, 2023

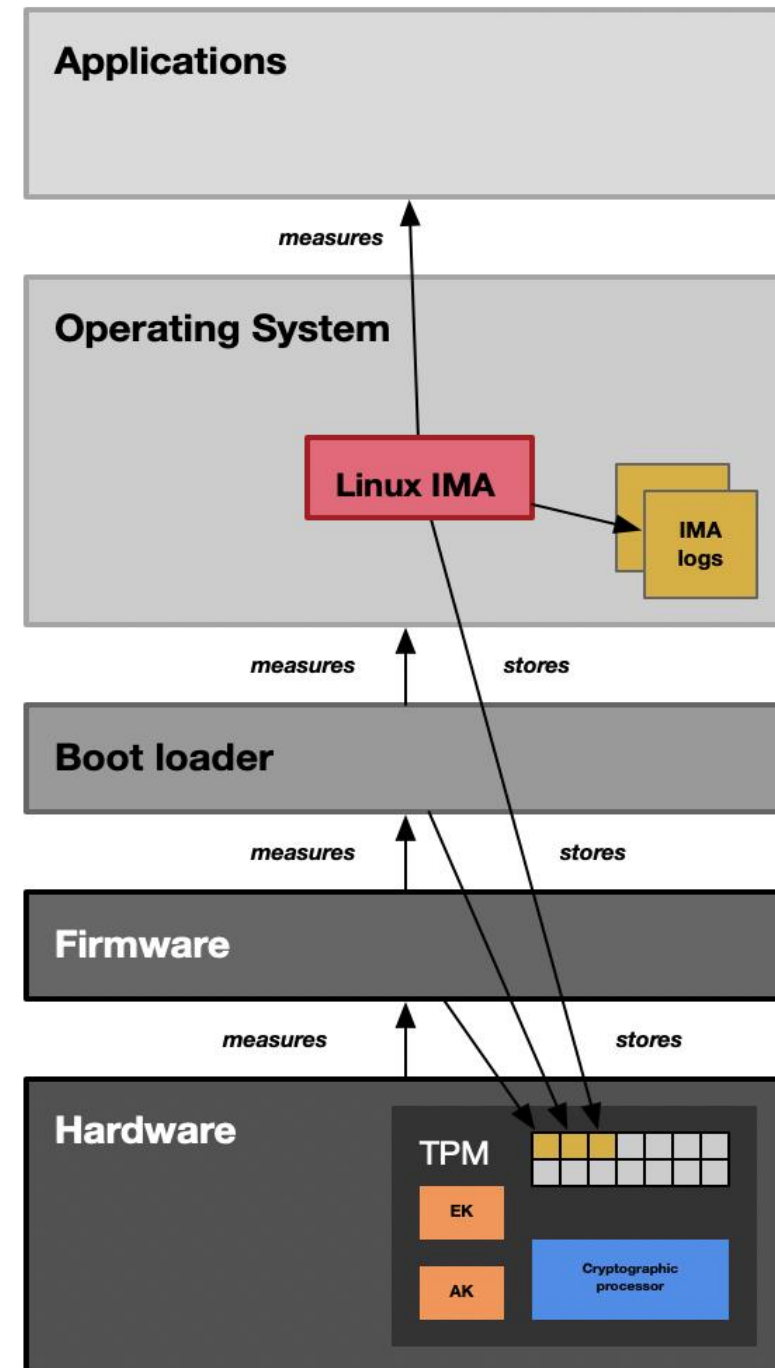Containers are ubiquitous and blindly trusted…

Measuring System Integrity

Operating System

↑ *measures*

Boot loader

↑ *measures*

Firmware

↑ *measures*

Hardware

Rooting Measurements in Trusted Hardware

Extending Integrity Measurements Through Runtime

Building Trust in Remote Environments