vTPM in Azure Confidential VMs

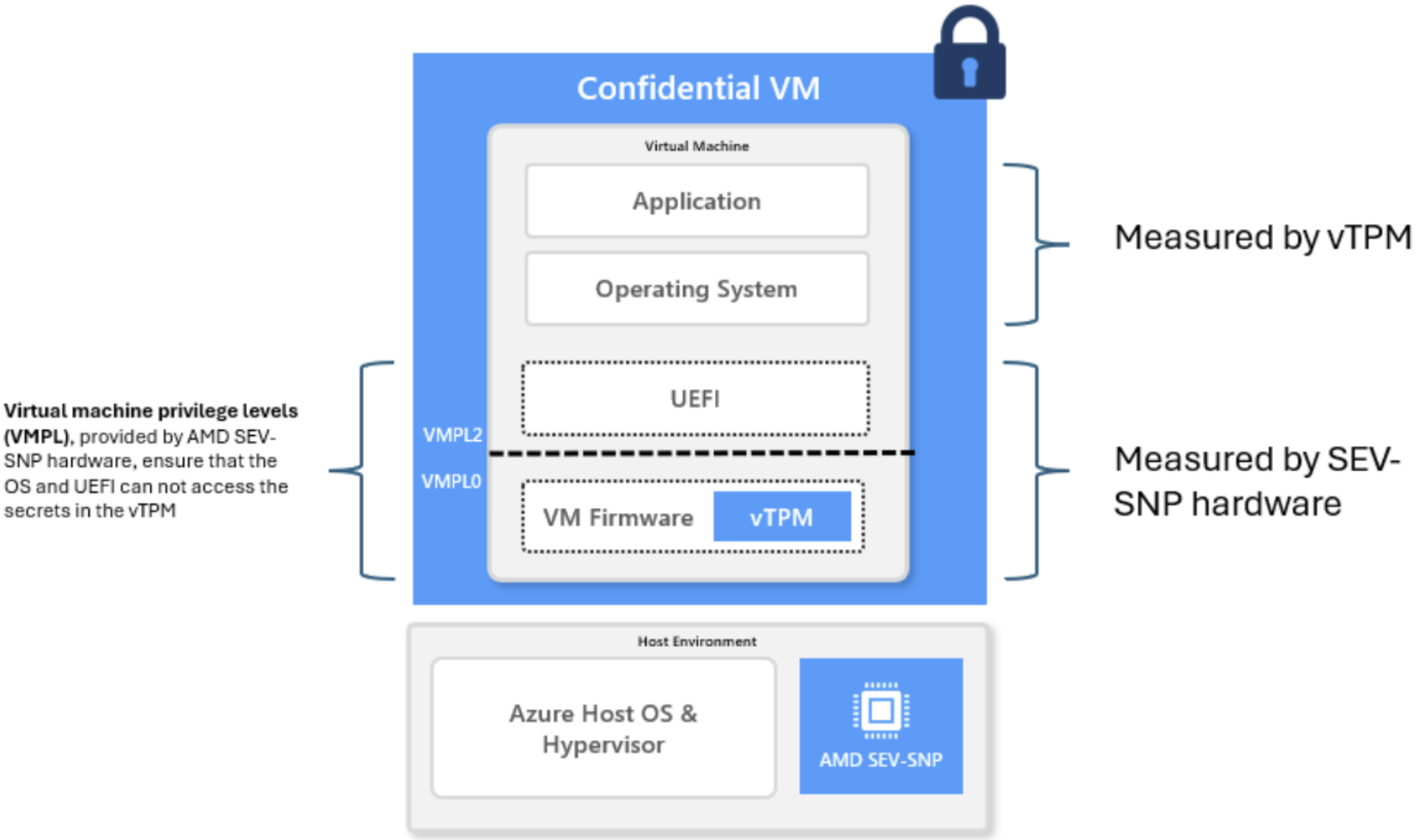
Muhammad Usama Sardar

TU Dresden, Germany

June 3, 2025

VM firmware should be OS & independently reproducible[1]

- Cannot check configs of vTPM, e.g., non-migratability of keys



[1] https://learn.microsoft.com/en-us/azure/confidential-computing/virtual-tpms-in-azure-confidential-vm