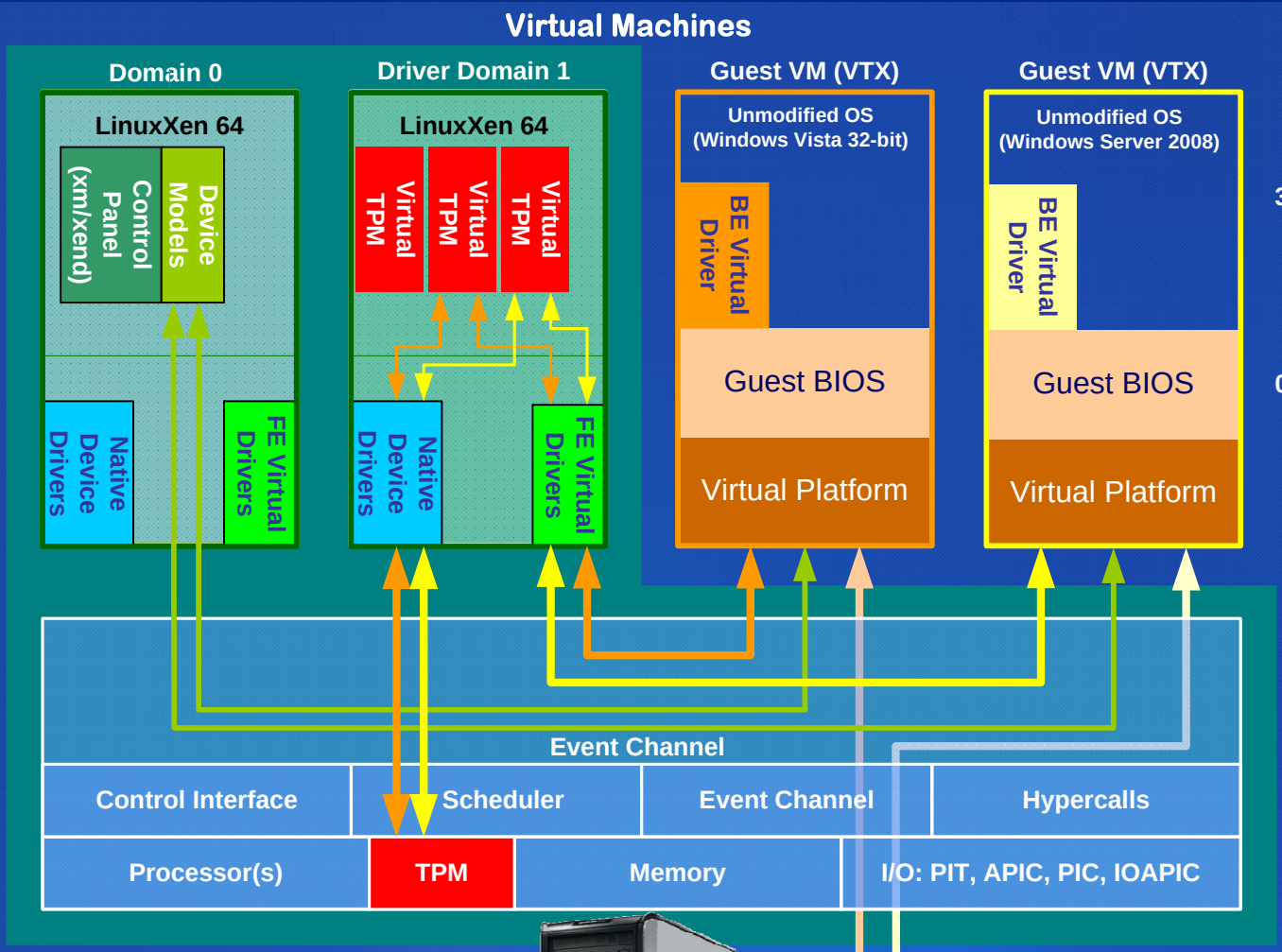
Identifying Trusted Virtual Machines

John Krautheim, Cyber Defense Lab — Advisors: Dhananjay Phatak, Alan Sherman



Xen – open source hypervisor

Provides powerful, efficient, and secure para-virtualization and full hardware virtualization

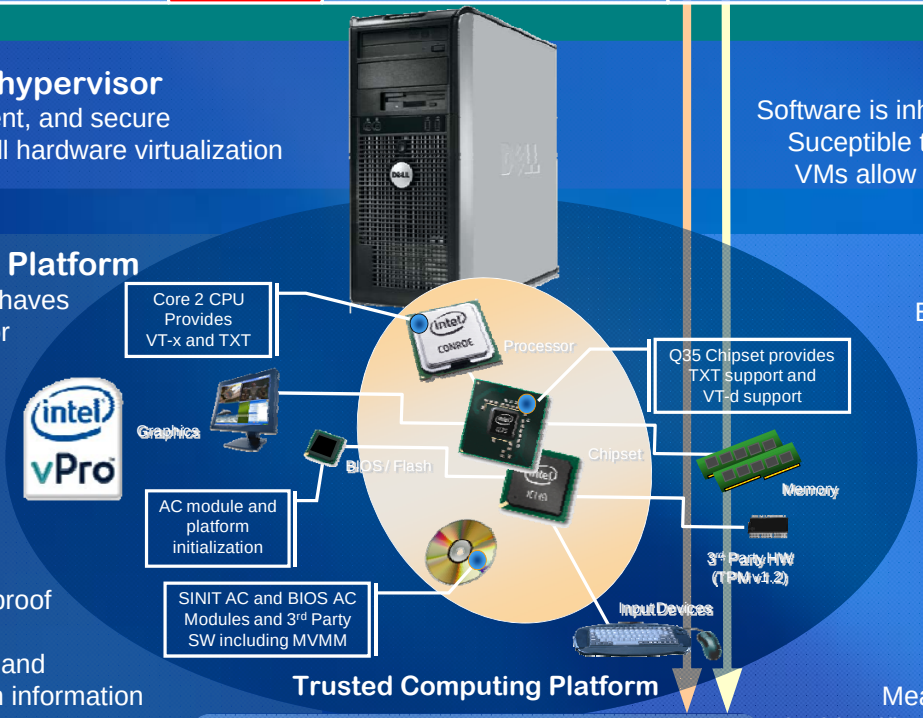
The Problem

Software is inherently not trustworthy
Suceptible to attacks and malware
VMs allow subversion of licensing

Trusted Computing Platform

Trusted if and only if it behaves in an expected manner for an intended purpose

Hardware can be trusted because it is immutable



Trusted Platform Module (TPM)

Cryptographic & Tamperproof
Provides "Root of Trust"
for system measurement and reporting for configuration information

Trusted Execution Technology

(Intel TXT) Provides hardware enforcement of security policy to ensure proper code is executed

The Solution

Employ virtualized TPM to enable trusted measurement of VM

Create unique identity through measurement of system parameters

"Lift" the trust from the hardware level to the virtual machine

Measurement sent to PDP for identification and authentication

Hardware enforcement assures proper virtual environment is executing, with no additional "malware," thus the VM is trusted

Attestation

Policy Decision Point (PDP) makes decision to trust based on identity report signed by vTPM

UMBC