CERIAS

the center for education and research in information assurance and security

Mandatory Access Control for Experiments with Malware

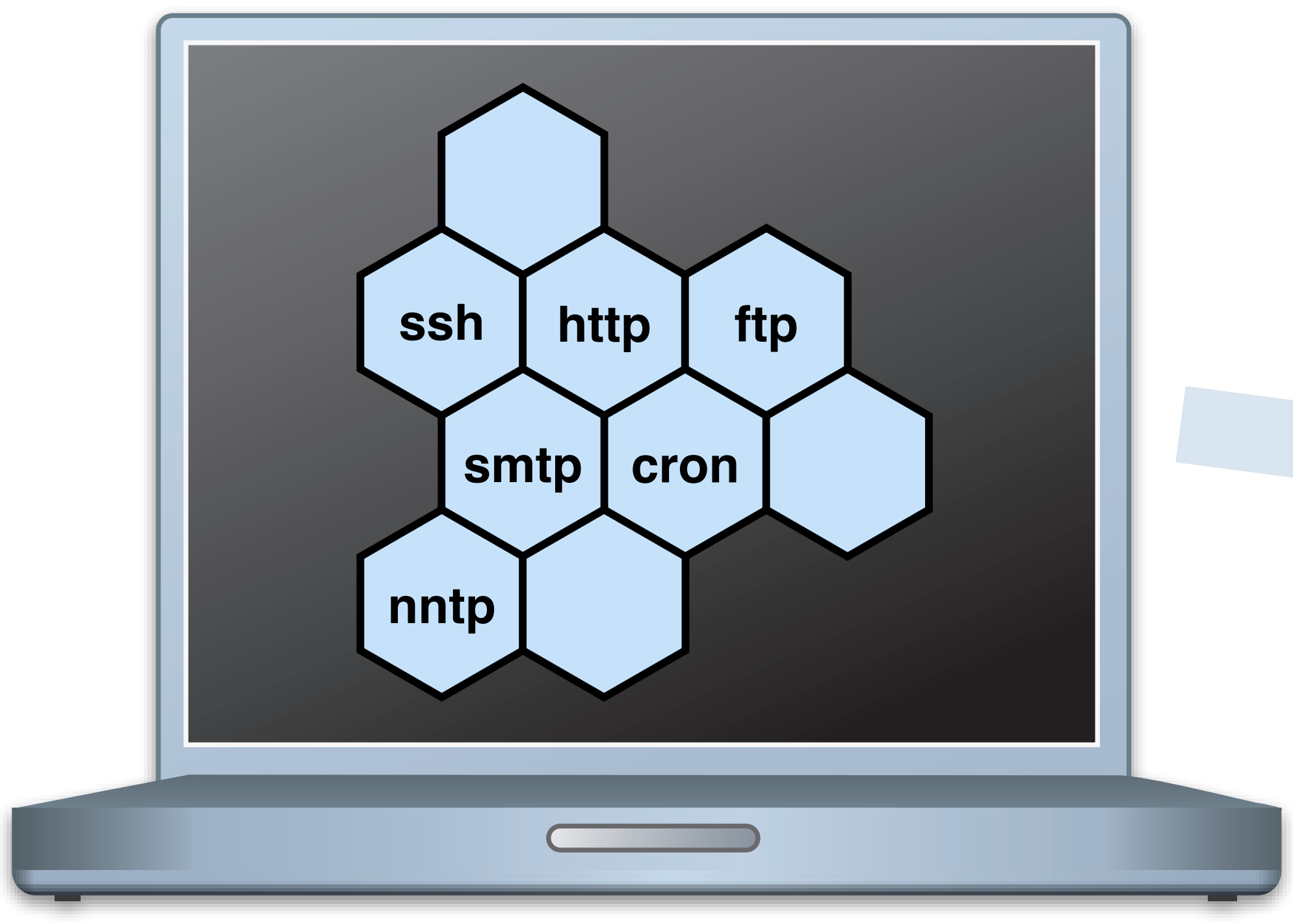
Jacques Thomas, Pascal Meunier, Patrick Eugster, Jan Vitek
{jthomas, pmeunier, p, jv}@cs.purdue.edu

Traditional approach: execute malware in a virtual machine (VM)

Problem 1: the malware attacks the VM and escapes

Solution 1: use Type Enforcement (TE) to confine the VM so that escaping the VM does not yield access to the host system

Problem 2: the malware modifies its behavior upon detection of the VM (virtualisation-aware malware)

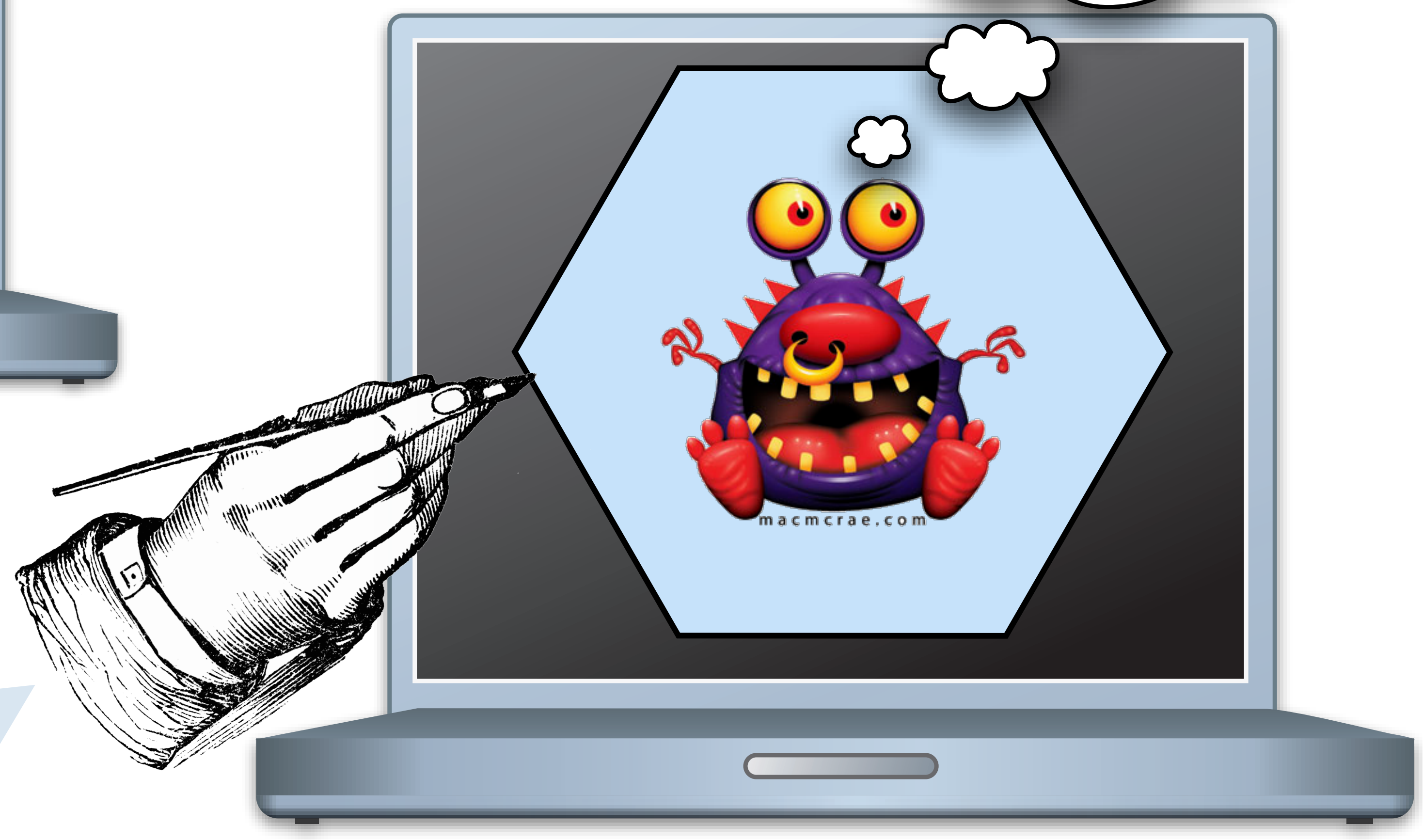


Traditional use of Type Enforcement (TE): confinement of system services

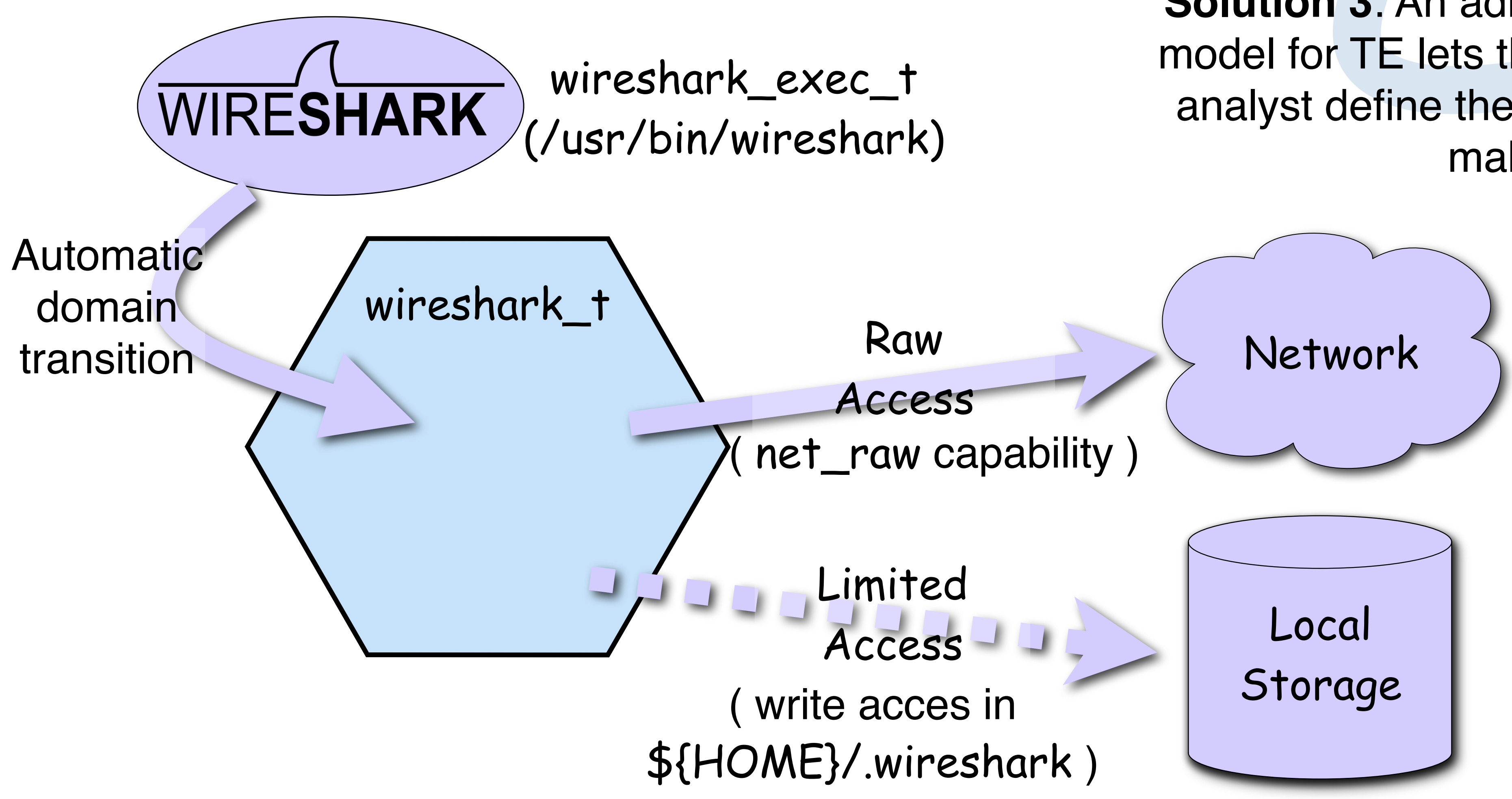
Problem 3: TE does not offer an administrative model to enable *controlled* runtime administration of the confinement

Solution 3: An administrative model for TE lets the malware analyst define the confinement of the malware

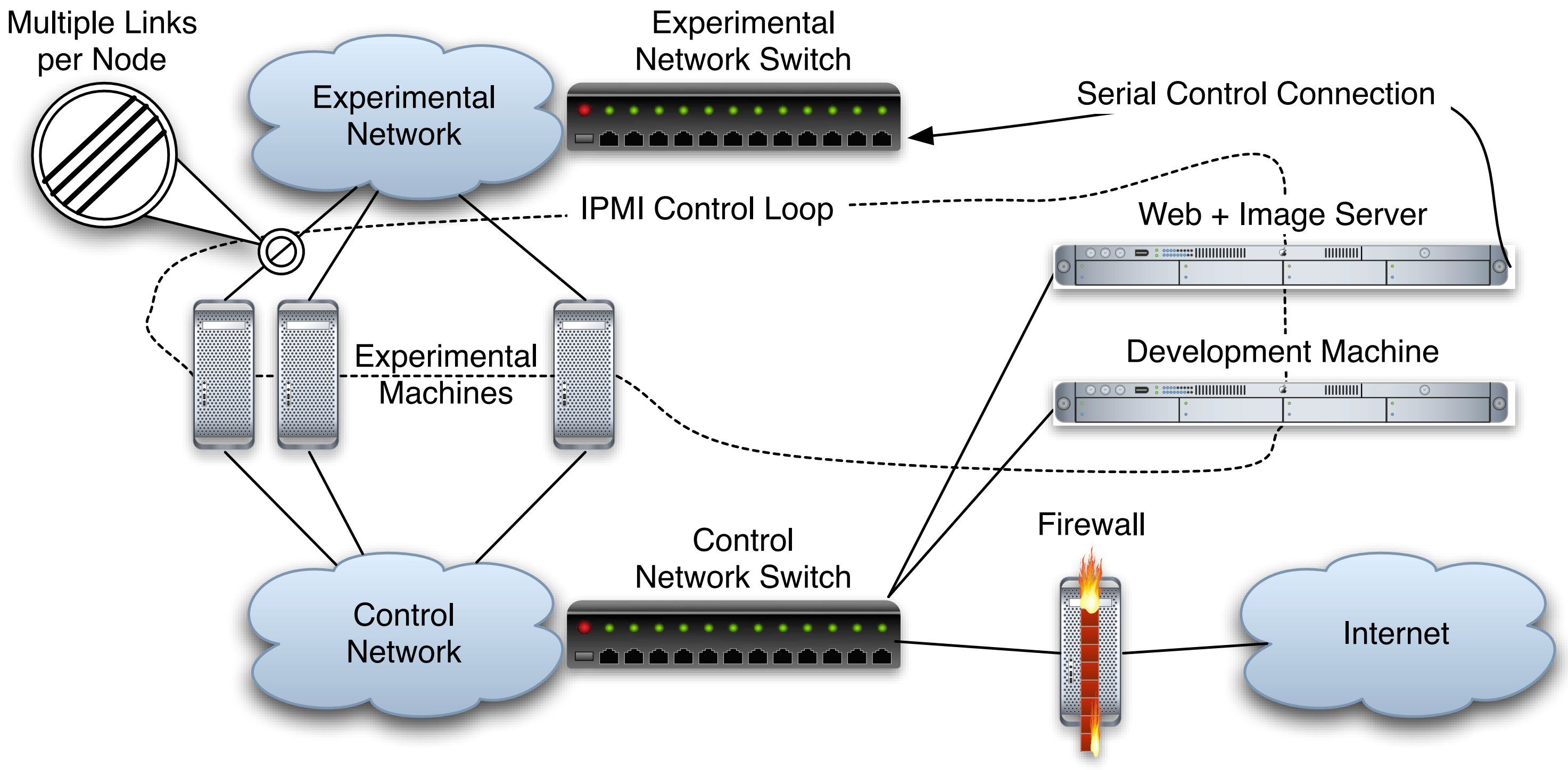
Solution 2: run the malware *directly* on the host OS; TE is used for confinement Even virtualization-aware malware can be analyzed



Simplified TE example for confining a protocol analyzer



The ReAssure testbed used for deployment



PURDUE
UNIVERSITY

CERIAS

Discovery Park
e-Enterprise Center