College of Information Studies

University of Maryland Hornbake Library Building College Park, MD 20742-4345

Virtualization

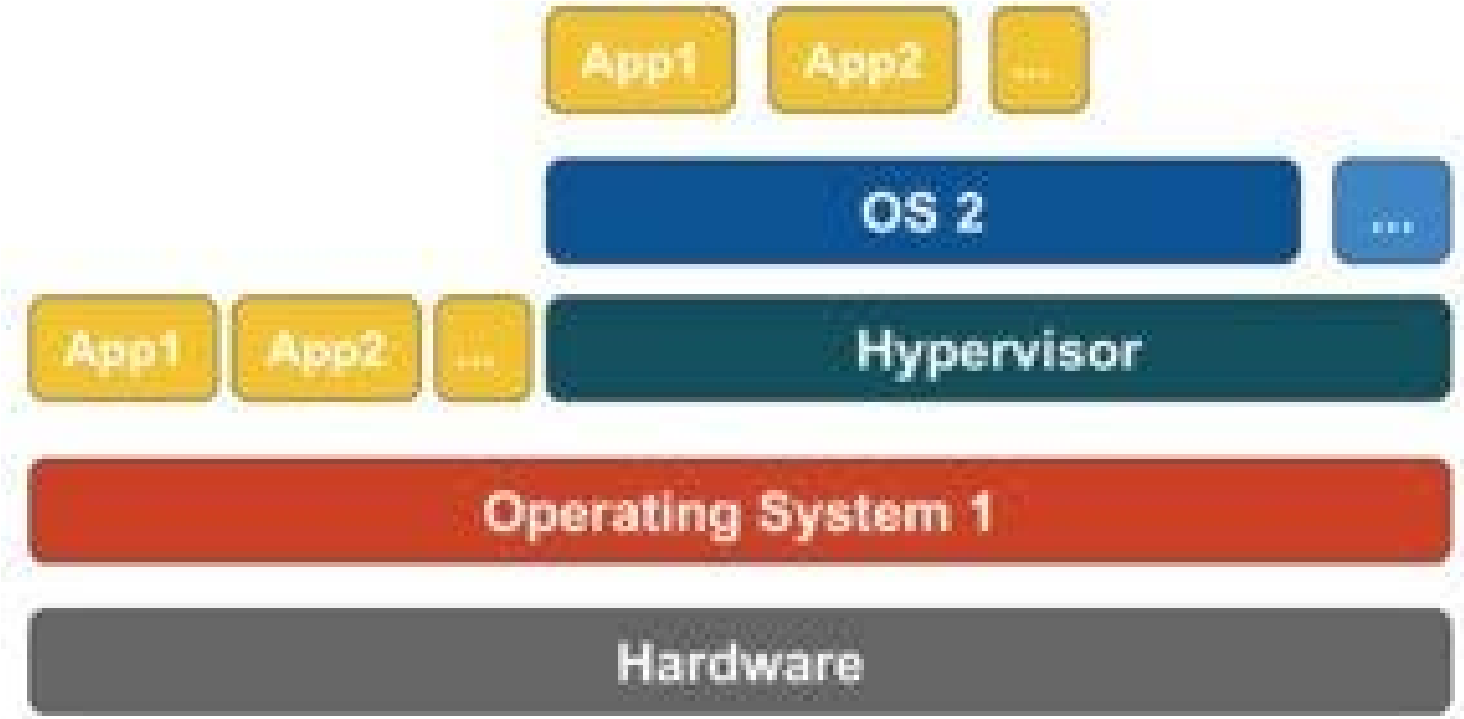
Session 8

INST 346

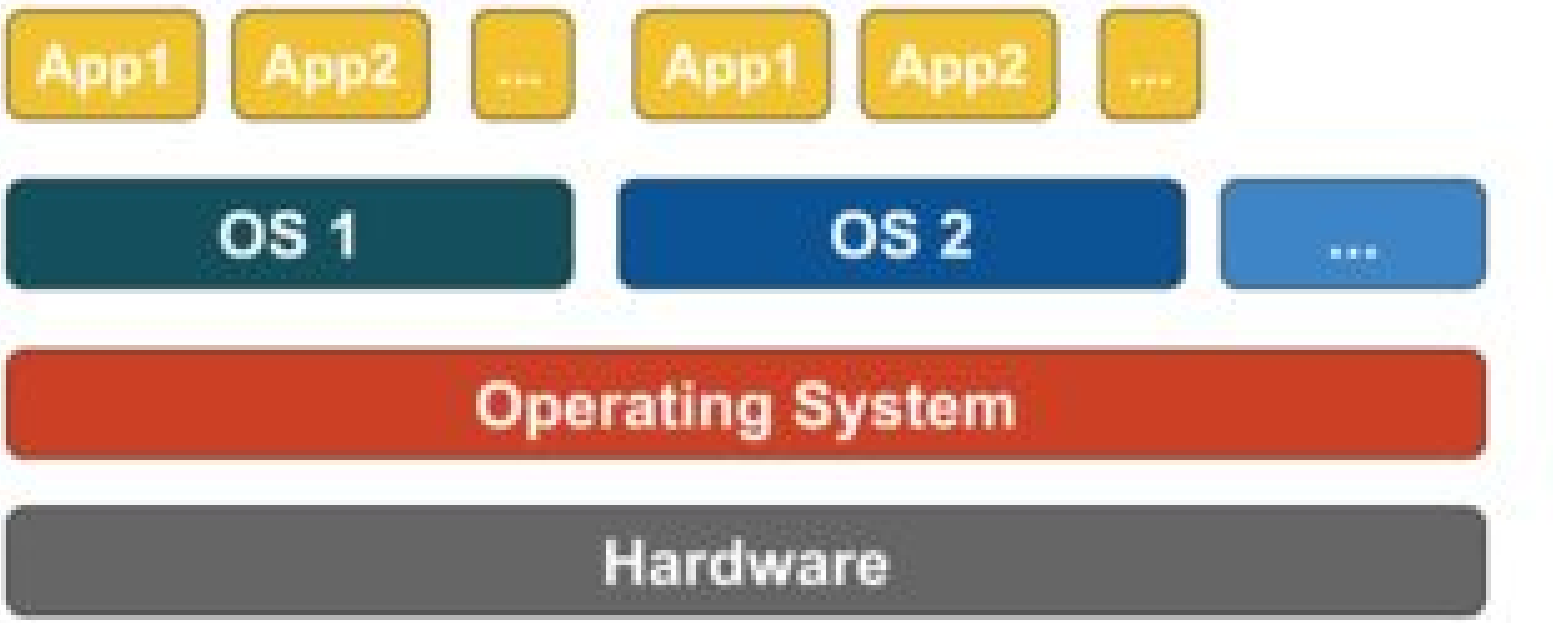
Software Stack

- Application Program (“App”)
- API
- Runtime environment
- Operating System
- BIOS
- Hardware drivers
- Microcode

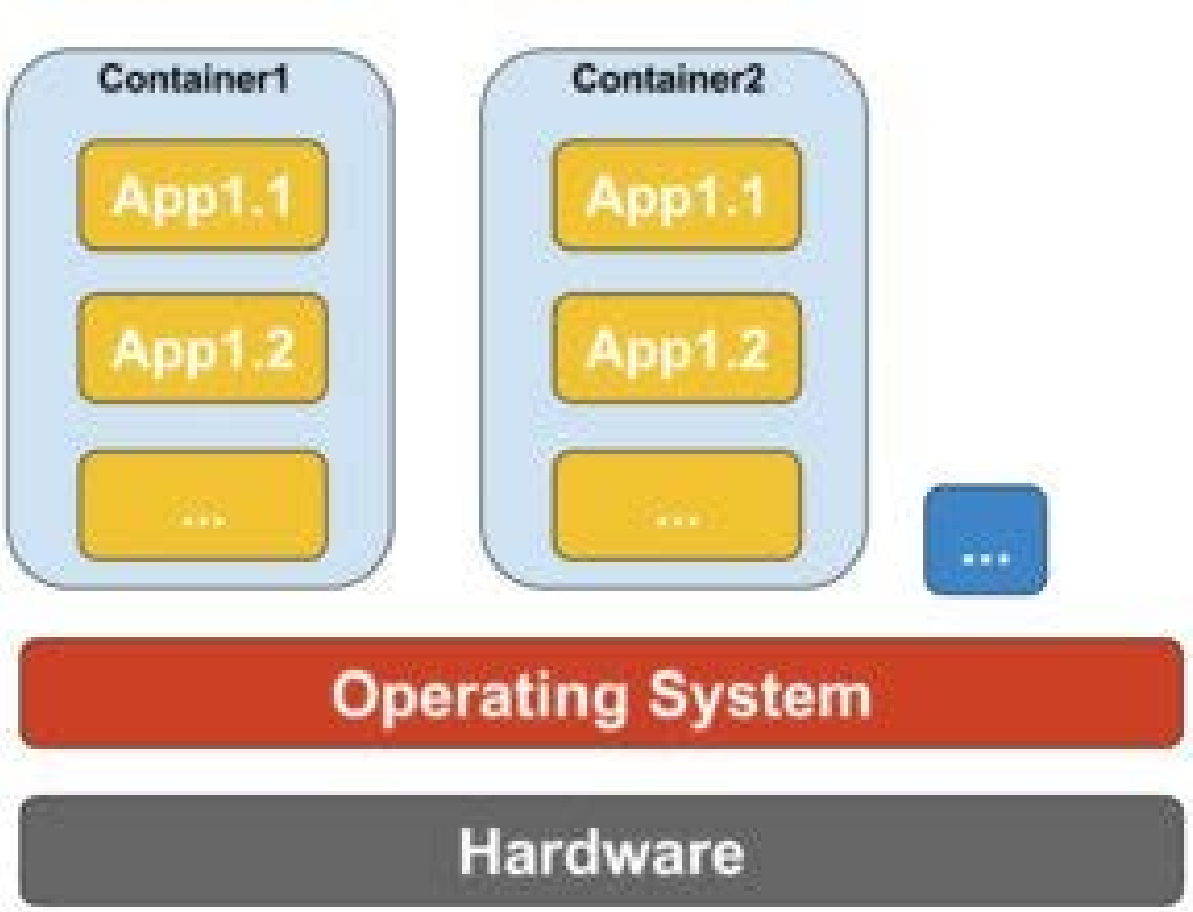
Emulation


App1
App2
...
OS 2
...
App1
App2
...
Hypervisor
Operating System 1
Hardware

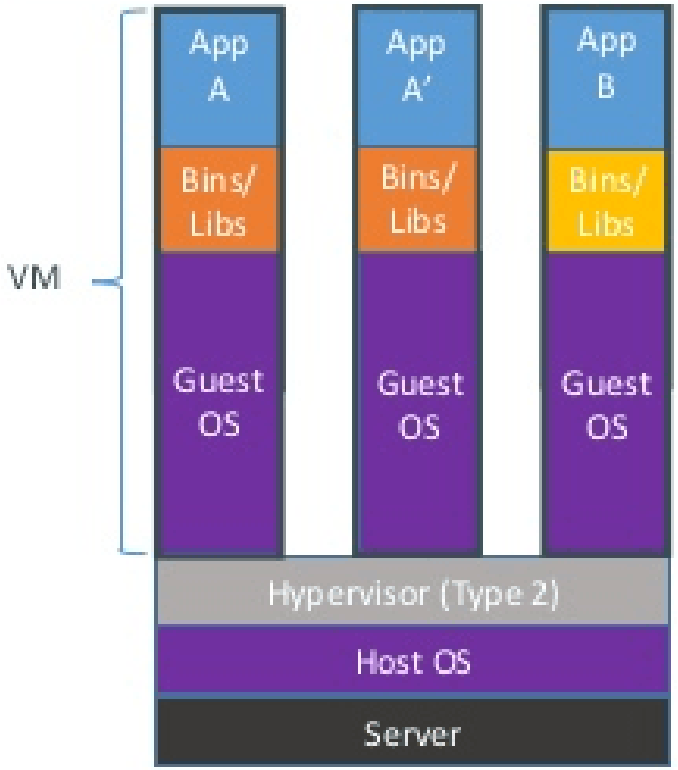
Paravirtualization



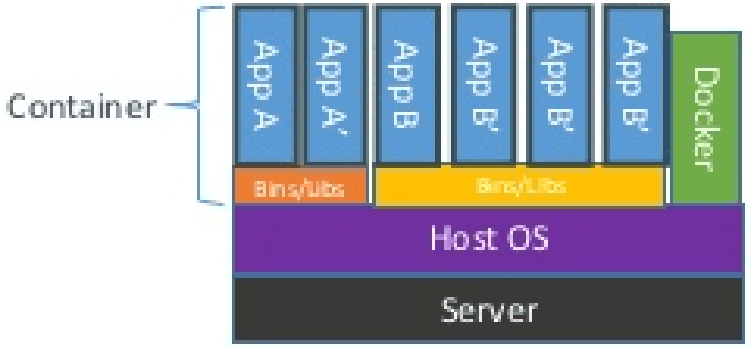
Containerization



Containers vs. VMs



Containers are isolated, but share OS and, where appropriate, bins/libraries



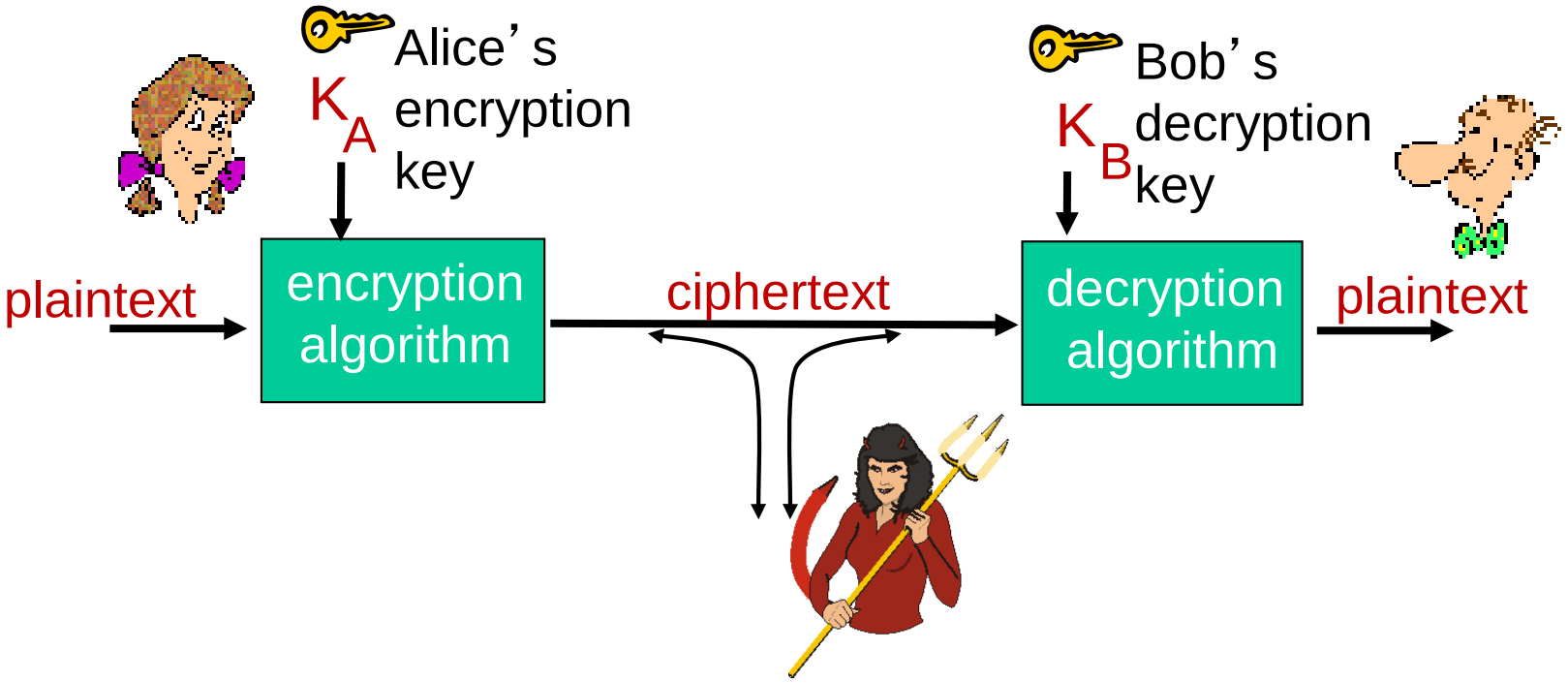
docker

Other “Virtualizations”

- Data Virtualization
  - Session 34
- Network Virtualization
  - Not this semester

Getahead: Encryption

The language of cryptography

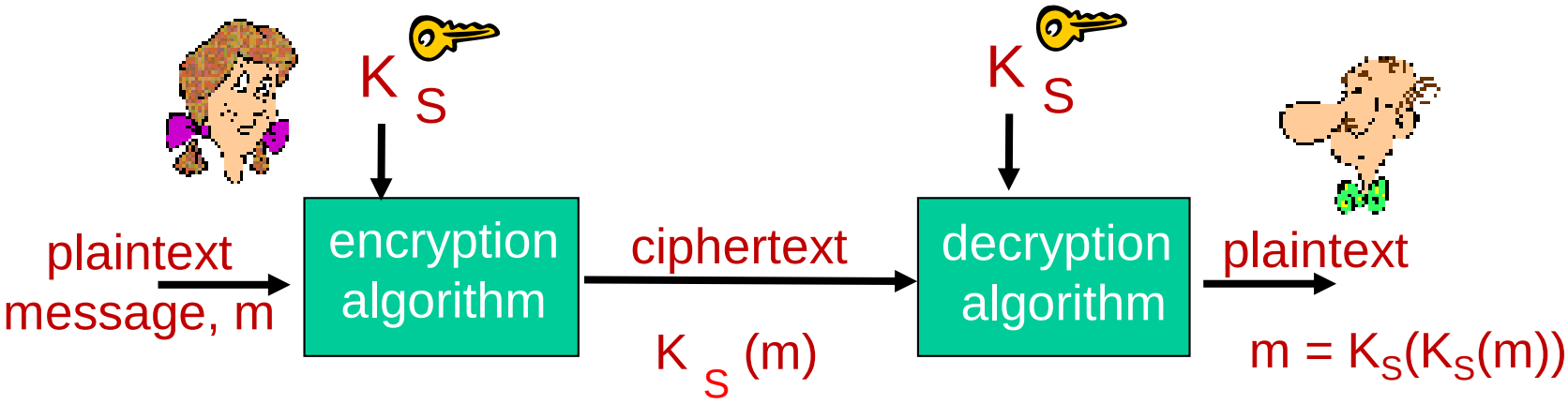


m plaintext message

$K_A(m)$ ciphertext, encrypted with key K_A

$m = K_B(K_A(m))$

Symmetric key cryptography



symmetric key crypto: Bob and Alice share same (symmetric) key: K_S

- e.g., key is knowing substitution pattern in mono alphabetic substitution cipher

Simple encryption scheme

substitution cipher: substituting one thing for another

- monoalphabetic cipher: substitute one letter for another

e.g.: **Plaintext: bob. i love you. alice**
ciphertext: nkn. s gktc wky. mgsbc

Encryption key: mapping from set of 26 letters to set of 26 letters

Stream and Block Ciphers

- n substitution ciphers, $M_1, M_2, \ldots, M_n$
- cycling pattern:
  - e.g., n=4: M_1, M_3, M_4, M_3, M_2; M_1, M_3, M_4, M_3, M_2; ..
  - random initialization
- for each new plaintext symbol, use subsequent substitution pattern in cyclic pattern
  - dog: d from M_1, o from M_3, g from M_4

Encryption key: n substitution ciphers, and cyclic pattern

AES: Advanced Encryption Standard

- symmetric-key NIST standard, replaced DES (Nov 2001)
- processes data in 128 bit blocks
- 128, 192, or 256 bit keys
- brute force decryption (try each key) taking 1 sec on DES, takes 149 trillion years for AES

Before You Go

On a sheet of paper, answer the following (ungraded) question (no names, please):

What was the muddiest point in today's class?