Administrivia

- I've listed reading for today, but really it's optional (though interesting!).
- If you're behind on homework: I'll still accept all homeworks (for reduced credit unless you have an extracurricular reason for being late in which case remind me when you turn something in), as long as you haven't looked at a solution. However, there will be a "not accepted past" deadline during finals week. Specifics TBA by e-mail soon.

Slide 1

Minute Essay From Last Lecture Pretty much everyone agreed that people in general seem to prefer features to security (sometimes — though not always — including themselves). Several people thought most computer users aren't even aware of the possible risks. "I think people tend to think that they are smart enough that they don't need to worry about security." (!) Heard on the phone with a support person a while back: With regard to identity theft, there are two categories of people: those who have been victims, and those who haven't — yet. Sadly probably true!

Homework 6 Essays

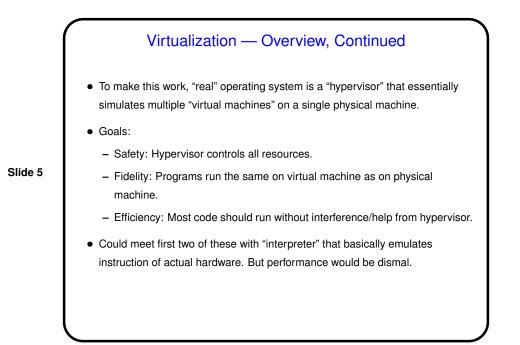
 Most people found the problems relatively easy, though not all. A few thought they were hard, and several found the last problem especially hard. (I thought it was a not-too-tough extension of the previous problem, but apparently several of you didn't agree!)

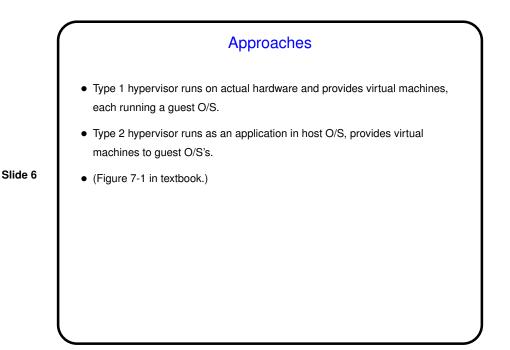
Slide 3

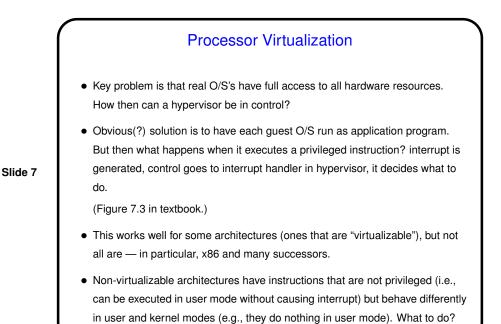
- Several people mentioned finding the calculations and/or results interesting.
- A few people mentioned finding the question about permissions interesting.

Virtualization — Overview

- Process abstraction allows multiple applications to run concurrently on the same hardware, isolating them from each other to some extent.
- Virtualization takes that a step(?) further and allows multiple operating systems to run concurrently on the same hardware, isolating them from each other.
- Attractive for many reasons, most of them related to usefulness of seeming to have more computers than you actually have (e.g., run many different operating systems without having many computers).
- Idea is far from new goes back to the mainframe days (VM/370 mentioned early in the semester) — but has recently become very popular, especially for providing computing services "in the cloud". Trinity's ITS also seems to be moving toward use of virtual machines for servers.

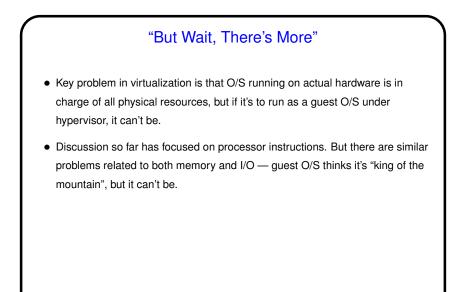


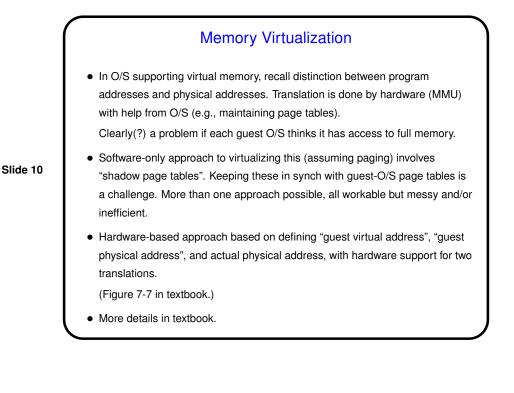


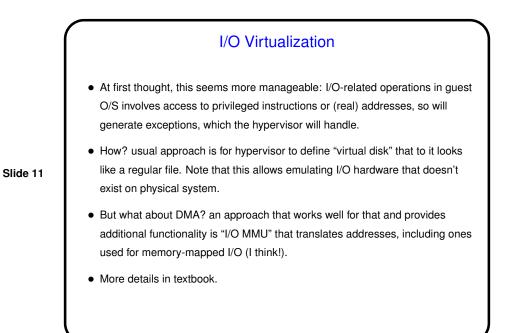


"Virtualizing the Unvirtualizable"

- One approach: "Binary translation", in which guest O/S is translated during execution in a way that replaces so-called "sensitive" instructions (ones that behave differently in user and kernel modes) with calls to hypervisor. Sounds very inefficient, but in practice apparently works well. More details in textbook.
- Another approach: "Paravirtualization", in which guest O/S is revised so that any operations normally requiring kernel mode are replaced with "hypervisor calls" (analogous to "supervisor calls" in application programs). Of course(?), then you have an O/S that no longer runs on actual hardware.







Minute Essay
• Have you used virtualization? (VMware, VirtualBox, cloud-based virtual
machines, ...)