Test 3 Sample questions

Virtualization

1. For system virtual machines, explain how virtual memory addresses are translated to physical addresses when (a) hardware supports EPT/NPT (extended/nested page tables) and (b) hardware only supports traditional (non-nested) page tables.

2. How does Intel VTx extending the traditional CPU execution privilege levels to support system virtual machines?

3. Compare different approaches for virtualizing I/O devices for virtual machines.


5. Which interface does a Process VM virtualize? Which interface does a System VM virtualize?

6. (a) How do Interpreters differ from Dynamic Binary Translators? (b) How do Binary Optimizers differ from Emulators?

7. What are the advantages and disadvantages of Classical System VMs compared to Para-virtualized VMs?

8. Give at least three mechanism(s) by which the highest privileged software, such as an operating system or a hypervisor, retains control over the CPU?

9. What is a co-designed virtual machine? Briefly describe and give an example.

10. What type of virtual machine (VM) is each of the following and why? Be as specific as possible. (a) Java Virtual Machine (JVM) (b) VMWare (c) Xen (d) Digital FX!32 (e) VirtualPC (f) (e) Transmeta Crusoe (Code Morphing)

11. Explain the difference between the concepts of full-virtualization and para-virtualization, giving at least one example of both virtualization techniques.

12. When you have design a system that does emulation, under what circumstances would you opt for Interpretation and when would you opt for Binary Translation? Justify your answer.

13. Compare the following terms with examples: (a) Monolithic kernels, (b) Micro-kernels, (c) Hypervisors.

14. (a) What is a shadow page table? How is it constructed and/or updated by the hypervisor? (b) What type of hardware virtualization support is needed to avoid constructing shadow page-tables in full-virtualization?
Live Migration of VMs

1. What constitutes “liveness” during live migration of virtual machines?
2. What are the key states transferred during live VM migration?
3. What are the metrics of performance in live migration of VMs?
4. How do different VM migration techniques work? How do they differ?
   1. Stop-and-copy
   2. Pure demand paging
   3. Post-copy
   4. Pre-copy
   5. Hybrid pre/post copy
5. What are the tradeoffs between different performance metrics when using each migration technique?
6. What are some optimization techniques you can use to speed up pre-copy? Post-copy? Both?
7. Under what situation would you use each migration technique?
8. What is dirty-page tracking? Why is it needed? How does it work? What are its overheads?
1. What is OS-level virtualization?
2. OS-level as opposed to what other levels?
3. How would you define the notion of isolation for any software or system component? What are the two (or more) extremes?
4. How does the isolation model for a processes differ from that for a system virtual machine?
5. How do containers improve upon process-level isolation model?
6. What are jails or sandboxes in the OS world? Why would you use them?
7. What are some key system resources that are virtualized by jails/containers/sandboxes?
8. Linux containers contain consist of two main components: Namespaces and CGroups. Explain the role of each.
1. Explain the three key principles of computer security?

2. Explain the basic security mechanisms supported by (a) the CPU execution hardware, (b) Memory management hardware and software, (c) File system. Assume that the machine uses x86 ISA.

3. What is authentication?

4. Describe different techniques to authenticate users.

5. What are some ways in which authentication mechanisms can be subverted?

6. What's a computer virus? What's a computer worm?

7. Explain a buffer overflow attack.

8. What is sandboxing? List two sandboxing mechanisms.

9. Explain Discretionary, Mandatory, and Role-based access control mechanisms.

10. Explain (a) trusted computing base (TCB) including why is it called “Trusted”, (b) Reference Monitor, and (c) relationship between TCB and reference monitor.

11. Explain the two key data access principles of multi-level security (MLS) systems (also called Mandatory Access Control).
System Design Techniques

1. When you “design” a computer system (hardware or software), what are some common goals that you may have as a designer?
2. What is meant by performance metric? What are resource constraints? How do the two interact? Give some examples.
3. What are some common examples of resources to consider when designing a computer system?
4. What is a “balanced” system? Why is balance important?
5. What are the different ways one can achieve balance? What are the goals of each approach?
6. Explain each of the following concepts and the tradeoffs it offers, with examples
   1. Multiplexing
   2. Pipelining and Parallelism
   3. Batching (versus multi-programming)
   4. Caching (or exploiting locality)
7. What is the “80/20 rule”? (Why is it not the “90/10 rule”?!?) Explain with examples.
8. Explain the notion of binding and indirection using virtual memory (or domain names or email aliases or something else) as an example.
9. What is the difference between abstraction and virtualization?
10. What are the benefits/drawbacks of hard state versus soft state design? Examples?
11. What is hysteresis? Explain with an example.
12. If you were to apply the principle of separating data plane and control plane to OS design, what OS components would you move out of the kernel to user space and why?