Principles of Computer Systems

December 17, 2024

This test has 16 questions totaling 100 points. You have 105 minutes to answer them. If you find yourself spending on any given question more minutes than the number of points attributed to it, you might consider moving on to the next question. The exam has 8 pages in total, including this one.

There is a mix of four kinds of questions:

- *ONE*: One-sentence answers related to a system or concept discussed in class. ONEs allow you to demonstrate your ability to identify, synthesize, and clearly state the essence of what you have learned.
- *OPAR*: One-paragraph answers related to a system or concept discussed. These are similar to ONEs, but with an opportunity to include more ample details and go in more depth.
- *BOE*: Back-of-the-envelope calculations that assess your ability to perform the quantitative reasoning that underlies intelligent design decisions.
- *MCQ*: Multiple-choice questions where you must check 1 or more of the 5 options provided. No justification is required, and nothing other than the checked boxes will be taken into account during grading. The MCQs efficiently test the breadth of your knowledge, covering many topics in a short amount of time.

Your answer to each question must be entirely within the box provided on the exam sheet. You have a few spare sheets at the end of the exam. Anything outside the boxes will be discarded prior to grading.

The exam takes place in room BC 01, and you must be physically present to take it. The exam is a written exam, and you need to use your own pen. The exam starts at 11:15 and ends at 13:00.

Rules:

- The exam is closed-book. You are allowed to bring with you one double-sided A4 cheat sheet with whatever information you want on it, in whatever font size you like.
- You are not permitted to interact with or receive or give any assistance for the exam except with/from the course staff.
- If you are noise-sensitive, you may wear ear plugs or ear muffs, but no electronic device is permitted (no headphones, no earbuds, no active noise-canceling device, etc.).

Read each question carefully. You need to provide a correct and complete answer to the *correct* question in order to receive full credit. A correct answer to a *wrong or misinterpreted* question will not earn credit. If you have any doubts, raise your hand, and the course staff will come to help.

SCIPER ☐☐☐☐☐☐

Question 1 (5 points)
One performance concern with the microkernel architecture is that the latency cost of IPC is too high. Where does this cost come from, and how does Liedtke address it in "On µ-Kernel Construction"?

(Answer in 1 sentence)

Question 2 (5 points)
The RON paper says that BGP "achieves scalability at the cost of fault tolerance." Name one mechanism that BGP uses to achieve scalability, then state how this mechanism helps scalability and how it hurts fault tolerance.

(*Answer in 1 sentence)*

Question 3 (5 points)
How does Twizzler enable regular applications to access persistent objects via 64-bit pointers?

(Answer in 1 sentence)

Question 4 **(4 points)**
Which of the following cache configurations could lead to aliasing problems (i.e., multiple virtual addresses mapping to the same physical address)?

(Circle all the correct options)

A. Virtually Indexed, Virtually Tagged (VIVT)
B. Virtually Indexed, Physically Tagged (VIPT)
C. Physically Indexed, Virtually Tagged (PIVT)
D. Physically Indexed, Physically Tagged (PIPT)
E. None of the above

Question 5 **(4 points)**
According to Popek & Goldberg's theorem, which of the following is true of an ISA for a conventional third-generation computer?

(Circle all the correct options)

A. If it has a sensitive instruction that is not privileged, a VMM cannot be constructed
B. If the ISA consists entirely of innocuous instructions, a VMM may be constructed
C. If all innocuous instructions trap in user mode, a VMM may be constructed
D. If behavior-sensitive instructions do not trap, it is not possible for the VMM to maintain control of all resources
E. None of the above

Question 6 **(4 points)**
PIPT caches are less prone to aliasing but can incur higher access latency compared to VIPT caches. Why?

(Circle all the correct options)

A. Because they require virtual-to-physical address translation before every access
B. Because they require larger page sizes for address mapping
C. Because they require complex hardware for virtual address translation
D. Because tags in PIPT caches slow down indexing more than in VIPT caches
E. None of the above

Question 7 **(4 points)**
What is a (potential) benefit of performing certain operations lazily in a system?

(Circle all the correct options)

A. Faster allocation of the needed resources
B. Reduction in unnecessary computation
C. Fewer cache misses
D. Predictable execution timing
E. None of the above

Question 8 **(4 points)**
What is a (potential) benefit of performing certain operations speculatively in a system?

(Circle all the correct options)

A. They guarantee correctness even in the presence of failures
B. They reduce resource usage by avoiding unnecessary computation and memory accesses
C. They eliminate the need for rollback mechanisms
D. They ensure better predictability of execution timing
E. The system can use otherwise-idle time to execute instructions before their dependencies are resolved

Question 9 **(4 points)**
How does knowing the "working set" of a process help?

(Circle all the correct options)

A. It identifies the total memory used by the process over its lifetime and enables pre-allocation
B. It determines the most frequently used data, optimizing cache allocation
C. It improves the process's CPU usage patterns
D. It provides a good estimate of the process's network bandwidth requirements
E. None of the above

Question 10 **(4 points)**
Which RAID level provides the highest write throughput for a given number of disks?

(Circle all the correct options)

A. RAID 0 (i.e., block-level striping without parity or mirroring)
B. RAID 1
C. RAID 5
D. RAID 4
E. RAID 10

Question 11 **(4 points)**
What is true of the Global Name Service (GNS)?

(Circle all the correct options)

A. It eliminates the need for caching on the endpoint
B. It provides a centralized point of control for all resources
C. It allows resources to be accessed using location-independent names
D. It simplifies the network protocol stack
E. None of the above

Question 12 (4 points)
Which of the following is true of a domain-specific hardware accelerator?

(Circle all the correct options)

A. It can be faster than a CPU because it can load and store more data per unit of time than a CPU
B. It can never be faster than a CPU if the PCIe latency is higher than the CPU's memory access latency
C. If it is "slower" than the CPU (i.e., performs the same operations slower than the CPU could), then there is no reason to use it
D. If it is "slower" than the CPU, we should improve its internal design to exploit more parallelism
E. None of the above

Question 13 (4 points)
According to the end-to-end argument, which functionality must be implemented solely at the application layer, not within the network?

(Circle all the correct options)

A. Error detection and correction
B. Packet forwarding and routing
C. Congestion control
D. Address resolution
E. None of the above

Question 14 (15 points)

You're building an operating system for devices with limited memory. The processor can provide paged virtual memory (VM) with a two-level hierarchical page table, or segments, or direct physical memory access. In order to decide whether you can afford the convenience of VM, compute the memory overhead of the VM option when fully mapping a 1-GiB address space.
Assume that virtual address (VA) size is 64 bits, physical address (PA) size is 48 bits, page size (PS) is 4 KiB, each page table entry (PTE) is 8 bytes wide, and a page table (PT) always fits in one memory page.

(*Write the answer in the small box below, and optionally provide your calculation to justify it.*)

Answer:
Calculation (optional):

Question 15 (15 points)

Consider N applications running on top of the Aegis exokernel, with each application having a working set of 32 distinct pages. The software-managed TLB can store 2048 entries. You are considering modifying Aegis to use an SSD or an NVRAM to cache TLB entries (instead of using DRAM, as Aegis did). You want the mean memory access latency to be ≤100 ns including access control.

Determine the value range of N for which using an SSD makes sense and the value range of N for which using an NVRAM makes.

Assume that memory accesses are served by DRAM (i.e., no caches), TLB lookups are instantaneous, and DRAM / NVRAM / SSD access latencies are 50 ns / 100 ns / 100 microsec respectively.

(*Write the answer in the small box below, and optionally provide your calculation to justify it.*)

Answer:
Calculation (optional):

Question 16 (15 points)

Suppose you want to allow any Internet end-system to specify a set of Autonomous Systems (ASes) that its outgoing traffic should not cross (if possible). At which layer(s) of the Internet stack would you implement the necessary functionality? Explain the trade-off(s).

(Answer in maximum 10 sentences)

– – – – – END OF EXAM – – – – –

(You can use the following pages for scratch notes. They will be discarded prior to grading.)