CS161 Fall 2026 — Introduction to Computer Security — Homework 6

Complete the following practice isolation question at by the end of the day on Friday, November 20. Please submit it to Gradescope once you are finished.

After the deadline, we'll release the solutions and a self-response form. Review the solutions, then submit the form to evaluate how you did.

Your grade is based solely on completing both the practice question and the self-response form, regardless of whether your answer is correct. The point of this homework is to prepare is to help you prepare for the final, so please don't use AI!

Q1 *Isolation: Blip Functions™* **(6 points)**

CodaBot is evaluating Blip Functions™, a platform where customers upload code that is run on shared servers on demand.

Design 1: The server is a single process. Each customer's code runs as its own thread inside that process. While running, each customer's code keeps its customer's request data on the single shared process heap.

Q1.1 (1 point) Select all that are true.

- ☐ One customer's code can read another customer's request data.
- ☐ One customer's code can modify another customer's request data.
- ☐ Each customer's code can prevent another customer's code from completing.
- ◯ None of the above

Design 2: Each invocation now runs in its own Linux process under a unique, non-root UID. Nothing else changes. Each function writes scratch files to a shared `/tmp` directory. Files are readable by everyone but writable only by their owner, and customers can't delete each other's files.

Q1.2 (1 point) Select all that are true.

- ☐ One customer's code can read another customer's scratch files.
- ☐ One customer's code can modify another customer's scratch files.
- ☐ One customer's code can slow down other customers' code.
- ◯ None of the above

This content is protected and may not be shared, uploaded, or distributed.

Q1.3 (1 point) Blip changes each code's scratch space to a private directory that only that code's customer's can access. Which of the following is most easily exploited?

- ◯ Customers can read other users' scratch files.
- ◯ Customers can modify other users' scratch files.
- ◯ Customers can read other users' process memory.
- ◯ Customers can exhaust shared resources.

Design 3: Blip moves each customer's code into its own virtual machine. All VMs run on the same physical host, managed by a hypervisor.

Q1.4 (1 point) Select all that are true.

- ☐ A bug in the hypervisor could break isolation between customers.
- ☐ A customer must trust the guest OS in other customers' VMs for their own data to stay private.
- ☐ Two VMs cannot learn anything about each other through shared hardware.
- ◯ None of the above

Share links: A customer can generate an unguessable share link for their function. Anyone who has the link can invoke the function. The platform checks only the link, not who is calling.

Q1.5 (1 point) Select all that apply.

- ◯ Capability-based access control is in place.
- ◯ Mandatory Access Control is in place.
- ◯ Discretionary Access Control is in place.
- ◯ Roles-based Access Control is in place.

Q1.6 (1 point) In 10 words or fewer, give one security drawback of share links compared to a per-user access list.

This content is protected and may not be shared, uploaded, or distributed.