Homework #4

Due: March 14, 2023 **Points:** 100

Questions

1. (*30 points*) Consider again the algorithm in Figure 9–7. The power used is another side channel for most instantiations of this algorithm. Explain how this side channel works. How might you add sufficient noise to it to render it unusable?

2. (*20 points*) Let $L = (S_L, \leq_L)$ be a lattice. Define:

   (a) $S_{IL} = \{[a,b] \mid a,b \in S_L \land a \leq_L b\}$

   (b) $\leq_{IL} = \{([a_1,b_1],[a_2,b_2]) \mid a_1 \leq_L a_2 \land b_1 \leq_L b_2\}$

   (c) $lub_{IL}([a_1,b_1],[a_2,b_2]) = (lub_L(a_1,a_2), lub_L(b_1,b_2))$

   (d) $glb_{IL}([a_1,b_1],[a_2,b_2]) = (glb_L(a_1,a_2), glb_L(b_1,b_2))$

   Prove that the structure $IL = (S_{IL}, \leq_{IL})$ is a lattice.

3. (*30 points*) The following system call adds read permission for a process (*for_pid*) if the caller (*call_pid*) owns the file, and does nothing otherwise. (The operating system supplies $call_pid$; the caller supplies the two latter parameters.)

```
function addread(call_pid, for_pid: process_id; fid: file_id): integer;
begin
        if (call_pid = filelist[fid].owner) then
                addright(filelist[fid].access_control_list, for_pid, ”r”);
        result := (call_pid − filelist[fid].owner);
        return result
end.
```

   (a) Is the variable `result` directly or indirectly visible, or not visible?

   (b) Is the variable `filelist[fid].owner` directly or indirectly visible, or not visible?

   (c) Is the variable `filelist[fid].access_control` directly or indirectly visible, or not visible?

4. (*20 points*) Definition 19–2 defines assurance in terms of “confidence.” A vendor advertises that its system was connected to the Internet for three months, and no one was able to break into it. It claims that this means that the system cannot be broken into from any network.

   (a) Do you share the vendor’s confidence? Why or why not?

   (b) If a commercial evaluation service had monitored the testing of this system and confirmed that, despite numerous attempts, no attacker had succeeded in breaking into it, would your confidence in the vendor’s claim be increased, decreased, or left unchanged? Justify your answer.