

CS 6V81-002: Quiz 2 Solutions

January 23, 2008

1. Software Fault Isolation (SFI) implements which of the following security policies (circle all that apply)?
 - (a) Rewritten code never throws a seg-fault interrupt due to an illegal memory reference.
 - (b) Rewritten code never branches to an address outside its fault domain.**
 - (c) Rewritten code is immune to buffer overflow attacks.
 - (d) Rewritten code never performs a system call except via trusted code inserted by the rewriter.**
2. Complete each of the following sentences by circling the word that makes it a valid reason to implement SFI as described in the paper:
 - (a) Context-switch overhead on the system is **high**.
 - (b) Interprocess communication is **frequent**.
 - (c) The system architecture has a **large** register set.
 - (d) The code is **static**.
3. A difference between *segment matching* and *sandboxing* is... (circle one)
 - (a) Sandboxing requires fewer dedicated registers.
 - (b) Sandboxing protects against infinite loops.
 - (c) Segment matching incurs lower runtime overhead.
 - (d) Segment matching gives better error messages.**
4. To enforce the policy that some fault domains may invoke a certain system call whereas others may not, one should implement...
 - (a) guard zones
 - (b) arbitration code**
 - (c) lazy pointer swizzling
 - (d) branch prediction
5. The SFI implementation described in the paper rewrites all store instructions so that they use the same dedicated register to reference memory. Why?

I decided this question was too vague, so I didn't count it in your scores. What I was looking for was something like this: *By using the same dedicated register for all store instructions, we can merely restrict assignments to that one register to enforce the policy (instead of trying to guard all possible control flows to dangerous instructions).*