

CS 6V81-002: Quiz 3 Solutions

January 28, 2008

1. A *chunk* as defined in the PittSFieId system is...
 - (a) an area of the data segment reserved for the control stack
 - (b) a sequence of atomic instructions aligned on a power-of-two address boundary**
 - (c) a sequence of high-order bits common to all legal memory addresses in the fault domain
 - (d) the series of guard instructions in-lined just before each unsafe operation
2. Which of the following are design goals satisfied by the PittSFieId verifier (circle all that apply)?
 - (a) it accepts all programs that satisfy the security policy and rejects all programs that violate the security policy
 - (b) it has a smaller implementation than the rewriter**
 - (c) it has a worst-case runtime that is linear in the size of the code being verified**
 - (d) it emits a proof of correctness that is machine-checkable
3. The machine-checkable proof of correctness for the PittSFieId rewriter was written in
 - (a) NuPRL
 - (b) LF
 - (c) Twelf
 - (d) ACL2**
4. The `%ebp` register on x86 is traditionally reserved for holding...
 - (a) the segment address
 - (b) the stack pointer
 - (c) the frame pointer**
 - (d) the status flags
5. The PittSFieId rewriter chooses virtual memory addresses such that the high-order bits of every legal memory address consist of all 0's except for a single 1. It also creates a non-writable "zero-tag segment". How do these two implementation details together result in improved runtime efficiency?

This allows potentially dangerous memory operations to be guarded by a single AND instruction instead of an AND and an OR instruction.