

# CS 6V81-002: Quiz 5 Solutions

February 6, 2008

1. For each of the following tasks, write a  $P$  next to those that are performed by the code-producer, and write a  $C$  next to those that are performed by the code-consumer. If a task is performed by both code-producer and code-consumer, write both a  $P$  and a  $C$  on that line.

P compiling binaries from source code    C proof validation

C precondition generation                      PC negotiating a security policy

PC verification condition generation        P annotation generation

P proof generation

2. A difference between an actual DEC Alpha processor and the simulation of it performed by a PCC abstract machine is (circle all that apply)...

(a) **the abstract machine does not return an error when an unsafe memory operation fails**

(b) **the abstract machine does not model pipelining**

(c) arithmetic overflow is not permitted by the abstract machine

(d) **the abstract machine does not support runtime code generation**

3. PCC packet filters performed better than those of SFI or SPIN because the runtime overhead caused by runtime security checks inserted by the PCC system was only...

(a) 50%

(b) 30%

(c) 10%

(d) **0%**

4. The authors report a high startup cost for their PCC packet filter application primarily due to...

(a) verification condition generation

(b) **proof validation**

(c) locality issues related to proof size

(d) the omission of certain code optimizations from their prototype compiler

5. What mathematical operation do the authors denote using the symbol  $\oplus$  throughout the paper?

*two's complement, 64-bit addition* (I included this question because the paper contained numerous discussions of how arithmetic overflow was modeled by the abstract machine, proof rules, and proof of soundness. If you understood any of those discussions, you know what  $\oplus$  denoted in those discussions.)