

CS 6V81-002: Quiz 17 Solutions

April 2, 2008

1. The use of a type-safe, functional language helps insulate MELANGE against which of the following security vulnerabilities? (circle all that apply)

- (a) information leaks
- (b) buffer overflows**
- (c) denial of service due to slow runtime performance
- (d) denial of service due to program crashes**

Type-safety eliminates buffer overflow vulnerabilities and helps avoid crashes. The type-system isn't information-flow-based, so information leaks are still a possibility. Runtime performance was at a level achievable with an imperative language (though slightly faster than some existing imperative implementations).

2. Why did the authors write their network packet parsing code in MPL instead of OCaml? (circle all that apply)

- (a) The performance overhead imposed by OCaml's garbage collector was too high.
- (b) The MPL implementation was smaller than the OCaml implementation.**
- (c) The MPL compiler was able to eliminate more bounds checks than the OCaml compiler.**
- (d) OCaml does not support inherently unsafe system calls needed by a packet parsing implementation.

3. A *packet suspension* is... (circle one)

- (a) a randomized delay between packet-sends to avoid race conditions
- (b) a man-in-the-middle attack that delays (or prevents) packet delivery
- (c) a closure that delays writing data to a packet until it is needed**
- (d) a malformed ICMP packet used in denial of service attacks

4. What network latency was recorded for the MELANGE implementation of DNS compared to the BIND implementation? (circle one)

- (a) MELANGE was about 10% faster**
- (b) MELANGE was about the same speed
- (c) MELANGE was about 30% slower
- (d) MELANGE was about 83% slower

5. One disadvantage of *generative meta-programming* from a security perspective is that it adds what significant piece of code to the trusted computing base?

The MPL compiler must be trusted in addition to the OCaml compiler.