

CS 6V81-002: Quiz 14 Solutions

March 24, 2008

1. The Jif/Split system enforces which security policies (excluding those already enforced by Java)? (circle all that apply)

- (a) memory and control-flow safety
- (b) data integrity**
- (c) data confidentiality**
- (d) data availability

Memory and control-flow safety are already enforced by Java. Jif/Split adds integrity labels to JFlow's confidentiality labeling scheme, so (b) and (c) are both correct. Availability is not enforced since deadlocks are still possible in type-correct Jif/Split code.

2. Suppose x is a low-confidentiality, low-integrity variable; and suppose y is a high-confidentiality, high-integrity variable. When compiling code “`if (x>0) y=y+1`” which of the following are true? (circle all that apply)

- (a) Jif rejects due to a confidentiality violation
- (b) Jif rejects due to an integrity violation**
- (c) the confidentiality of y gets downgraded
- (d) the integrity of y gets downgraded**

If x and y 's integrity labels are programmer-specified, then the type-checker rejects due to an integrity violation. If the labels are being inferred by the type-checker, y gets downgraded to low-integrity.

3. Suppose Alice owns v and does not trust Bob to read it, but Bob later endorses v . What must Jif/split implement in order to handle this situation? (circle one)

- (a) robust declassification operators
- (b) secure hash replication**
- (c) global frame ID's
- (d) a secure control-flow interface

This is a case where a principal (in this case Bob) trusts a variable's integrity but lacks permission to read it. In such cases, secure hash replication allows Bob to verify v by reading its hash without learning its actual value.

4. The `lgoto` protocol is required when... (circle one)

- (a) transferring control from a high-confidentiality host to a low-confidentiality host
- (b) transferring control from a low-confidentiality host to a high-confidentiality host
- (c) transferring control from a high-integrity host to a low-integrity host
- (d) transferring control from a low-integrity host to a high-integrity host**

5. Add a label to the following Jif/split variable declaration to indicate that principal p allows only q to read x , and p and q both trust the integrity of x .

```
int{p:q;*:p,q} x;
```