Computer Security

Prof. Dr.-Ing. Volker Roth
Freie Universität Berlin

June 6, 2012

Please note that your submission will not be accepted without the properly signed Academic Integrity agreement.

Academic Integrity

We each certify that this submission is our own original work and that we have due acknowledged any work of others.

_____

Date, signature, name in block letters

_____

Date, signature, name in block letters

_____

Date, signature, name in block letters

Question 1: Execution-based information flow control

Trace the execution of the procedure *copy1* on the single accumulator machine (see Denning's book, Figure 5.8 and Table 5.2) for both $x = 0$ and $x = 1$ when $\underline{\text{x}} =$ *high*, $\underline{\text{y}} =$ *low*, $\underline{\text{z}} =$ *high*, and $\underline{\text{pc}}$ is initially *low*. Is the execution secure?

Question 2: Information flow control certification

Draw the syntax tree showing how the certification mechanism of Section 5.4.3 in Denning's book verifies the flows in the following statement:

```
1  while a > 0 do begin
2    a := a − x;
3    b := a ∗ y
4  end.
```

Question 3: Information flow control certification

Following the approach in Section 5.4.2 of Denning's book, give security conditions for a `case` statement:

```
1  case a of
2    v1: S1
3    v2: S2
4    ⋮
5    vn: Sn
6  end.
```

where a is a variable and $v_1, \ldots, v_n$ are values.