Computer Security

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

June 1, 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: Enforcement of security policies for computation

This task as is based on *Jones, A. K. and Lipton, R. J. 1975. The enforcement of security policies for computation* any needed information can be found there.

Given the following code of a program Q

```
1  if (x_1 = 1) and (x_2 = 1) then y := 1
```

- Sketch the basic flowchart of Q

- Construct the *surveillance protection mechanism M* for Q by applying the transformation rules (assume that execution time is not observable). Including the actual values of every $\underset{\sim}{v}$ and $\underset{\sim}{C}$.

- Show the execution path and output for the following security policies in M.

    - allow(2)

    - allow(1,2)

Question 2: Enforcement of security policies for computation

This task as is based on *Jones, A. K. and Lipton, R. J. 1975. The enforcement of security policies for computation* any needed information can be found there.

Given the following flowchart (page 204)
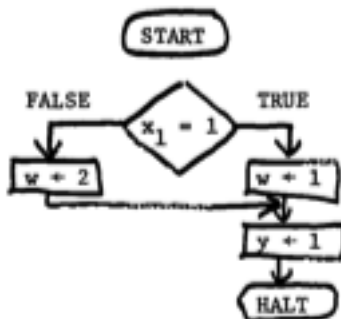
- Construct the corresponding *surveillance protection mechanism* (without observable running time).

- Explain why the protection mechanism is unable to detect that the assignment of y is independent of x_1. (Any answer longer than two sentences is considered false. You know what we mean by "sentence", right?)