# Computer Security

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

May 18, 2011

## 1 IFC and Entropy

Consider the following statement:

**if** $(x = 1) \wedge (y = 1)$ **then** $z := 1$

where $x$ and $y$ can each be 0 or 1, with both values equally likely, and $z$ is initially 0.

1. Compute the equivocation $H(X|Z')$.
2. Compute the equivocation $H(Y|Z')$.

## 2 IFC and Entropy

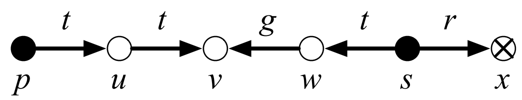
Let $x$ be an integer variable in the range $[0, 2^{64} - 1]$, with all values equally likely. Write a program that transfers $x$ to $y$ using implicit flows. Compare the running time of your program with the running time of the trivial program `y:=x`.

## 3 Execution-based IFC

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 $\underline{x} = high$, $\underline{y} = low$, $\underline{z} = high$, and $\underline{pc}$ is initially *low*. Is the execution secure?

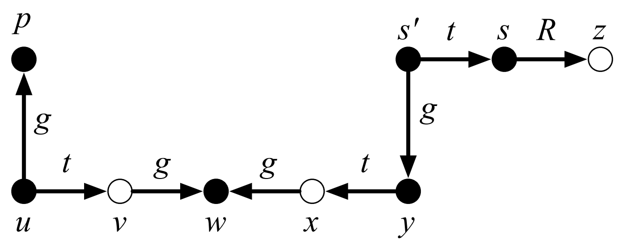
## 4 Take-Grant protection model

Give a sequence of commands showing how the right $r \to x$ can be transferred over the bridge connecting $p$ and $s$ in the following graph:




## 5 Take-Grant protection model

Let $G_0$ be the protection graph:




1. Give a sequence of rule applications showing *can.share*$(R, z, p, G_0)$ is true.
2. Is *can.share*$(t, s', p, G_0)$ true? Why or why not?
3. Show *can.steal*$(R, z, p, G_0)$ is true and list the conspirators.