Computer Security

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

May 22, 2012

Question 1: Information flow control and entropy

Consider the following statement:

```
1  if x > k then y := 1
```

where x has the probability distribution:

$$p_i = \begin{cases} \frac{1}{2} & x = 0 \\ \frac{1}{4} & x = 1 \\ \frac{1}{4} & x = 2 \end{cases}$$

and y is initially 0.

1. Compute the entropy $H(X)$.
2. Compute the equivocation $H(X|Y')$ for $k = 0$ and $k = 1$.

Question 2: Information flow control and entropy

Consider the following statement:

```
1  if (x = 1) ∧ (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 $H(Y|Z')$.

Question 3: Information flow control and entropy

Let x be an integer variable in the range $[0, 2^{64} - 1]$, with all values equally likely. Write a program (in pseudocode) 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`.

Question 4: Assembly indirect information flow

Let x be a memory location holding a 64 Bit value, with all values equally likely. Write an Assembly program that transfers the value in x to another memory location y using implicit flows.

Question 5: Upper and lower bounds

Consider the lattice in Figure 5.1. (*Cryptography and data security - Dorothy Elizabeth Robling Denning, Addison-Wesley 1982*). What class corresponds to each of the following?

1. $A \bigoplus B$, $A \bigotimes B$
2. $B \bigoplus I$, $B \bigotimes I$
3. $B \bigoplus C$, $B \bigotimes C$
4. $A \bigoplus C \bigoplus D$, $A \bigotimes C \bigotimes D$
5. $A \bigoplus B \bigoplus D$, $A \bigotimes B \bigotimes D$