11 Assignment (10+5 Points)

Hinweis:	Abgabe in $\{2, 3, 4\}$-er Gruppen.
Abgabe:	**08.07.2017, 23.59**
Email:	Betreff "[Compsec] Ex 11'
	(bitte nur .pdf oder .txt, kein .doc, .jpeg, etc)
	Source code: bitte inkl. `signify` Signatur

Exercise 37 (Information flow and entropy **(1+3 Points)**).
Consider the statement

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

and let X denote the random variable for x in this program and Y be the random variable for the resulting value of y. Let X have the probability distribution:

$$\Pr[X = x] = \begin{cases} \frac{1}{2} & x = 0 \\ \frac{1}{4} & x = 1 \\ \frac{1}{4} & x = 2 \end{cases}$$

and let y be initially 0.

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

Note: the (shannon) entropy $H(X)$ of a random variable X is defined as

$$H(X) := -\sum_{x \in \mathrm{Dom}(X)} \Pr[X = x] \cdot \log_2 (\Pr[X = x]),$$

where $\mathrm{Dom}(X)$ indicates the set of values that X may take, and the equivocation $H(X \mid Y)$ is defined as

$$H(X|Y) = \sum_{y \in \mathrm{Dom}(Y)} \Pr[Y = y] \cdot H(X \mid Y = y).$$

Exercise 38 (Information flow control (i) **(3 Points)**).
Following our approach in class, give security conditions for a **case** statement:

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

Exercise 39 (Information flow control (ii) (**3 Points**))**.**
Show line by line how the certification mechanism from class verifies the flows in the following statement:

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

Exercise 40 (Still more Hello World (**Bonus: 2+2 Points**))**.**
Consider the C program form exercise 31 again. Give an input string that does not crash this program and makes it

1. print `Hello World!` (not making use of the `hello` string already in this program) and does not contain any fixed addresses or NULL bytes
2. does make use of the buffer overflow vulnerability overwriting the return pointer in `foo` (may contain fixed addresses).

Notes: There is a `Makefile` in exercise40.tar.gz that makes testing a bit more convenient.

Exercise 41 (Keeping your systems secure (**Bonus: 1 Points**))**.**
Are there any new vulnerabilities for your Debian or OpenBSD system since last week (01.07.2016 at 23.59)? If so: state one, **name the programming mistake**, decide if you are affected or not, and report if there are any known work-arounds or patches.