

TD – Flux d'information

Exercice 1: Considérons le programme suivant :

```
x : integer class S;
y,z : integer class C;
t : integer class U;
y := 2; z := 3;
x := y+z ;
if ( y<5 ) then t := 4;
    else t := 3;
```

où les classes de sécurité sont dans l'ordre $S > C > U$.

Est-ce que le flux d'information est correcte ?

Exercice 2: Considérons maintenant le programme suivant, où les premières lignes sont des déclarations de fonctions, avec leurs équations de classes de sécurité (qui sont dans l'ordre $S > C$) :

```
procedure read_string(out a : string);           // ∅
procedure create_file(a: string, out b: file);   // a <= b
procedure file_not_empty(a: file; out b: boolean ); // a <= b
procedure write_file(a: integer; out b: file);   // a <= b
x : file class S;
y : file class C;
t : string class C;
b : boolean ;
read_string(t);
create_file(t,x);
file_not_empty(x,b);
if ( b ) then write_file(2,y);
    else write_file(3,y);
```

1. Quelle est la classe du booléan b ?
 2. Est-ce que le flux d'information est correcte ?
-

Exercice 3: Un autre programme à analyser, sur le treillis de classes de sécurité $H > L$:

```
procedure division(a: integer; out b: integer){
  c: integer;
  c := a;
  while ( (c>1) || (c<-1) ) do {
    c:= c/2;
  }
  b := c;
}
procedure read_high_integer(out a) // a >= H
procedure write_low_integer(out a) // a <= L

main(){
  x : integer class H;
  y : integer class L;
  write_low_integer(2);
  read_high_integer(x);
  division(x,y);
  write_low_integer(y);
}
```

1. Est-ce que le programme est correct d.p.d.v. du flux d'information ?
 2. Est-ce qu'avec un appel `division(x,x)` (à la place de l'appel `division(x,y)`) le programme serait correct ? Discuter aussi du point de vue du principe de la non-interférence.
-

Exercice 4: Considérons le programme suivant :

```
1.  a := 2a+b;
2.  do {
3.    c := 2d;
4.    b := b-c;
5.    while (a<=2) {
6.      b := b+d;
7.      c := b-c;
    }
8.    c := 2d;
9.    d := 2b-c-1;
    }
10. while (c<2)
11.  d := b+d;
12.  a := 2b+d;
13.  printf(a);
```

Construire la tranche de programme qui correspond au critère (13, a).
