M2 CySec **Ensimag & UGA**

Software Security course

Lab session on Frama-C

First, have a look to the Frama-C introduction slides ...

To run Frama-C on the Ensimag machines you should firts use the following command:

```
source /matieres/WMM9MO73/opam_profile.sh
```

The main frama-c commands we are going to use are the following:

`frama-c-gui -rte xxx.c` (RTE, showing potential runtime errors)
or
`frama-c-gui -rte -eva xxx.c` (to run RTE and EVA analysis)
or
`frama-c-gui -rte -eva -wp xxx.c` (to run RTE, VSA and WP analysis)

Your are not required to provide a « report », but questions on value analysis and (dynamic) symbolic execution will be part of the final exam … !
(so don't hesitate to ask if something is unclear for you).

1) Demo files for Frama-C

demo_1 :
run RTE
run RTE and VSA to see dead code detection (highlighted in red)

demo_2 : (with some constrained input values)
run RTE
run RTE and VSA (here one assertion is not discharged)

demo_3 : (with more constrained input values)
run RTE
run RTE and VSA (all assertions are discharged)

2) Exercices with Frama-C

Look at the comments inside each provided file in order to know how to process it …

exo_1:
- Generate RTE
- Run a VSA analysis (using intervals) by hand. Is the runtime error discharged ?
- Use value to see that it works fine (good example of widening/narrowing operators !)
- What happens if you replace the constant N by 1000 , 1001?

exo_2 and exo_21 :
illustrates interval computations on arithmetic expressions,
which may produce false positives ...
one assertion not discharged by VSA (needs Wp !)

exo_3:
- Generate RTE
- Does the error occur at runtime ?
- Use value to see that a valid assertion is not discharged (false positive)
  Why is it not discharged ?
- Try to discharge it using WP … (providing a suitable loop invariant)

exo_4: generalize exo_3
needs to introduce by hand an auxiliary assertion to get rid of the false positive
This extra assertion can be proved using Wp

3) Application to the Grub example

Try to use Frama-C in order to retrieve the vulnerabilities present in the code ...