FMSP: Solution Attempt for exam 2021-07

Pizzaiolo

June 28, 2022

Preamble

Feel free to edit it to add more examples, fix mistakes, etc. If you do so, please update both the .tex and .pdf files. And obviously no guarantee for anything.

Problem 3: Information Flow

(a)

We have following examples:

$$\text{if } h > 1 \text{ then } \text{ skip } \text{ else } \text{ skip}$$

$$\text{while } h > 1 \text{ do } \text{ skip}$$

We let $\Gamma = \{h \colon H\}$

(i)

If example typechecks .

$$\dfrac{\dfrac{(1)}{\Gamma \vdash h > 1 \colon H} \quad \dfrac{}{\Gamma \vdash \text{ skip } : H \text{ cmd}}\,\text{SKIP} \quad \dfrac{}{\Gamma \vdash \text{ skip } : H \text{ cmd}}\,\text{SKIP}}{\Gamma \vdash \text{ if } h > 1 \text{ then } \text{ skip } \text{ else } \text{ skip } : H \text{ cmd}}\,\text{IF}$$

.

$$\dfrac{\dfrac{\Gamma(x) = Hvar}{\Gamma \vdash h \colon H}\,\text{R-VAL} \quad \dfrac{\dfrac{}{\Gamma \vdash 1 \colon L}\,\text{INT} \quad \dfrac{}{L \subseteq H}\,\text{BASE}}{\Gamma \vdash 1 \colon H}\,\text{SUBSUMPTION} \qquad > \in \{+, -, >, <}}{\dfrac{\Gamma \vdash h > 1 \colon H}{(1)}}\,\text{OP}$$

While example typechecks .

$$\dfrac{\dfrac{(1) \text{ - see if example}}{\Gamma \vdash h > 1 \colon H} \quad \dfrac{}{\Gamma \vdash \text{ skip } : H \text{ cmd}}\,\text{SKIP}}{\Gamma \vdash \text{ while } h > 1 \text{ do } \text{ skip } : H \text{ cmd}}\,\text{WHILE}$$

(ii)

They both don't typecheck, because we would need it to be a L cmd to use the IF/WHILE rule, however skip : H cmd (and we can't use subsumption for it)

(iii)

The if example is termination-sensitive non-interferent. It always terminates, thus the definition is essentially the same as for basic non-interference (which holds because it typechecks with the first rules). The attacker cannot gain information about high variables by ovserving low variables and the termination behavior.

The while example is not termination-sensitive non-interferent.

(b)

The only way a program does not terminate is, if it has a while loop. We want to prevent two cases: (1) a while loop has a high condition and (2) a while loop is entered based through an if based on a high condition.

We prevent (1), because the rule ...

We prevent (2), because the rule ...