Logics in Security **Winter 2014**

Homework for Module 3

Instructor: Deepak Garg
dg@mpi-sws.org

TA: Iulia Bolosteanu
iulia_mb@mpi-sws.org

Release date: 13.12.2014 *Due date: 20.12.2014*

General instructions: Attempt all questions. Submit your homework via email to both the instructor and the TA before midnight on the due date. The LaTeX source for this homework will be provided to help you typeset. You can also typeset using any other means, including simple ASCII.

Problem 3-1 ($2 + 3 + 1 + 2 + 2 = 10$ points)

Authorization policies in SecPAL. Saarland University, `UnivSaarland`, has bachelors students, graduate students and professors, all of whom need access to a specific door in the university. `UnivSaarland` uses SecPAL to manage the door's authorization system. Let the predicate "x has access" mean that principal x has access to this door. Saarland University has created credentials that establish the following judgments:

`UnivSaarland` says x has access if x is a bachelors student
`UnivSaarland` says x has access if x is a graduate student
`UnivSaarland` says x has access if x is a professor

A. Assume that `Alice` is a bachelors student and `Bob` is a professor, so the following judgments hold:

`UnivSaarland` says `Alice` is a bachelors student
`UnivSaarland` says `Bob` is a professor

What judgment in SecPAL corresponds to the informal assertion "Alice can access the door"? Write down a proof using the rules of SecPAL (paragraph "Semantics" in Section 3 of the paper) that establishes this judgment. Now do the same for Bob instead of Alice.

B. `UnivSaarland` gives every professor the right to decide who is a graduate student (this makes sense because graduate students are usually associated with a professor). Accordingly, `UnivSaarland` issues the following credential:

`UnivSaarland` says x can say$_\infty$ y is a graduate student if x is a professor (1)

`Bob` decides to take `Charlie` as a graduate student, so `Bob` issues the following credential:

`Bob` says `Charlie` is a graduate student

Write a formal SecPAL proof to show that `Charlie` is allowed access to the university's door.

C. Professor `Bob` wants to delegate administrative responsibility to his student `Charlie`. Accordingly, he wants to issue a credential that will allow `Charlie` to state who is a graduate student. What SecPAL judgment would this credential establish?

D. `Charlie` decides to misuse the authority he received from Professor `Bob` in the previous step. He decides to designate his wife `Mary` a graduate student so that she can access the university's door (`Mary` is not really a graduate student). `Charlie` issues the credential:

`Charlie` says `Mary` is a graduate student

Write a SecPAL proof to show that `Mary` has access to the the university's door.

E. Clearly, something has gone wrong. One way to fix this problem is for `UnivSaarland` to delegate to `Bob` the right to decide graduate students but *without* allowing him to delegate this right further. What credential should `UnivSaarland` have issued in place of credential (1) of step B in order to ensure this property? Explain why with this revised credential (and keeping all other credentials the same) `Mary` will *not* get access to the university's door.

Problem 3-2 ($2.5 \times 4 = 10$ points)

Intuitionistic logic. Construct proofs of the following judgments in intuitionistic logic. The proof rules are listed in Figure 1 for your reference. Note that the judgment $\vdash \varphi$ is an abbreviation for $\emptyset \vdash \varphi$. Further, $\neg\varphi$ is an abbreviation for $\varphi \supset \bot$.

a. $\vdash A \supset (B \supset (A \wedge B))$

b. $\vdash (A \supset B) \supset ((A \supset \neg B) \supset \neg A)$

c. $\vdash (\neg\neg(A \supset B)) \supset (A \supset \neg\neg B)$

d. $\vdash \neg\neg(\neg\neg A \supset A)$

Problem 3-3 (0 points)

This is a practice exercise to help you understand reduction semantics better. If you turn in a solution, we will check it to provide you feedback, but not for points. We strongly encourage you to solve this exercise before the lecture on Wednesday, December 17, 2014.

Reduction semantics. Consider the following program p with the initial memory $\mu = \{x \mapsto 5; y \mapsto \mathit{false}; z \mapsto 2\}$:

```
x := 0;
if (y == true) then
   x := 1;
else
   while (z > 0) do
      x := x + 1;
      z := z − 1;
```

Specify the first four steps of the reduction of this program and the memory corresponding to the result of each of them. For the first and fourth steps of the reduction write down complete derivation trees following the rules of the reduction judgment. You may want to introduce names for parts of the program to abbreviate your proofs. The rules of the reduction judgment are shown in Figure 2 for your reference.

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\wedge\mathrm{I} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\wedge E_1 \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\wedge E_2$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\vee I_1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\vee I_2 \qquad \frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\vee E$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \supset B}\supset\mathrm{I} \qquad \frac{\Gamma \vdash A \supset B \qquad \Gamma \vdash A}{\Gamma \vdash B}\supset\mathrm{E} \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash A}\bot\mathrm{E} \qquad \frac{}{\Gamma \vdash \top}\top\mathrm{I}$$

Figure 1: Intuitionistic logic introduction and elimination rules.

Syntax:

Values	v	$::=$	$0 \mid 1 \mid 2 \ldots \mid \mathit{true} \mid \mathit{false}$
Expressions	e	$::=$	$v \mid \ell \mid e_1 + e_2 \mid e_1 - e_2 \mid e_1 == e_2 \mid e_1 > e_2$
Commands	p	$::=$	$\mathsf{skip} \mid \ell := e \mid p_1; p_2 \mid \mathsf{if}\ (e)\ \mathsf{then}\ p_1\ \mathsf{else}\ p_2 \mid \mathsf{while}\ (e)\ \mathsf{do}$

Semantic rules for expressions:

Note: For any connective o in $\{+, -, ==, >\}$, $\hat{o}$ denotes the underlying arithmetic operator.

$$\frac{}{\mu, v \Downarrow v} \qquad \frac{}{\mu, \ell \Downarrow \mu(\ell)} \qquad \frac{\mu, e_1 \Downarrow v_1 \qquad \mu, e_2 \Downarrow v_2 \qquad v_1 \hat{+} v_2 = v}{\mu, e_1 + e_2 \Downarrow \mu, v}$$

$$\frac{\mu, e_1 \Downarrow v_1 \qquad \mu, e_2 \Downarrow v_2 \qquad v_1 \hat{-} v_2 = v}{\mu, e_1 - e_2 \Downarrow \mu, v} \qquad \frac{\mu, e_1 \Downarrow v_1 \qquad \mu, e_2 \Downarrow v_2 \qquad (v_1 \hat{==} v_2) = v}{\mu, e_1 == e_2 \Downarrow \mu, v}$$

$$\frac{\mu, e_1 \Downarrow v_1 \qquad \mu, e_2 \Downarrow v_2 \qquad (v_1 \hat{>} v_2) = v}{\mu, e_1 > e_2 \Downarrow \mu, v}$$

Semantic rules for commands:

$$\frac{\mu, e \Downarrow v}{\mu, \ell := e \to \mu[\ell \mapsto v], \mathsf{skip}} \qquad \frac{\mu, p_1 \to \mu', p_1'}{\mu, p_1; p_2 \to \mu', p_1'; p_2} \qquad \frac{}{\mu, \mathsf{skip}; p \to \mu, p}$$

$$\frac{\mu, e \Downarrow \mathit{true}}{\mu, \mathsf{if}\ (e)\ \mathsf{then}\ p_1\ \mathsf{else}\ p_2 \to \mu, p_1} \qquad \frac{\mu, e \Downarrow \mathit{false}}{\mu, \mathsf{if}\ (e)\ \mathsf{then}\ p_1\ \mathsf{else}\ p_2 \to \mu, p_2}$$

$$\frac{\mu, e \Downarrow \mathit{true}}{\mu, \mathsf{while}\ (e)\ \mathsf{do}\ p \to \mu, p; \mathsf{while}\ (e)\ \mathsf{do}\ p} \qquad \frac{\mu, e \Downarrow \mathit{false}}{\mu, \mathsf{while}\ (e)\ \mathsf{do}\ p \to \mu, \mathsf{skip}}$$

Figure 2: Reduction semantics.