

## Homework 6

1. Access-control logic includes formulas of the form

$$P \text{ says } F$$

where  $P$  is a principal and  $F$  a formula. Give two inference rules of access-control logic involving *says*.

2. (Removed) Was already used in HW 5
3. Assume an access control logic with security levels, say top secret ( $TS$ ), secret ( $S$ ) and public ( $P$ ), with

$$slev(P) < slev(S) < slev(TS)$$

- (a) Modify the formula

$$P \text{ controls Permitted}(O, \text{write})$$

using security levels so that it satisfies the *write rule* from the *Bell-LaPadula* access policy. Do the same again, but satisfy the *write rule* from the *Biba* access policy.

- (b) Modify the formula

$$P \text{ controls Permitted}(O, \text{read})$$

using security levels so that it satisfies the *read rule* from the *Bell-LaPadula* access policy. Do the same again, but satisfy the *read rule* from the *Biba* access policy.

4. Assume two security levels  $S$  and  $TS$ , which are ordered so that  $slev(S) < slev(TS)$ . Assume further the substitution rules

$$\frac{\Gamma \vdash slev(P) = l_1 \quad \Gamma \vdash slev(Q) = l_2 \quad \Gamma \vdash l_1 < l_2}{\Gamma \vdash slev(P) < slev(Q)}$$

$$\frac{\Gamma \vdash slev(P) = l \quad \Gamma \vdash slev(Q) = l}{\Gamma \vdash slev(P) = slev(Q)}$$

Let  $\Gamma$  be the set containing the following six formulas

$$slev(S) < slev(TS)$$

$$slev(\text{Agent}) = slev(TS)$$

$$slev(\text{File}_1) = slev(S)$$

$$slev(\text{File}_2) = slev(TS)$$

$$\forall O. slev(O) < slev(\text{Agent}) \Rightarrow (\text{Agent controls Permitted}(O, \text{read}))$$

$$\forall O. slev(O) = slev(\text{Agent}) \Rightarrow (\text{Agent controls Permitted}(O, \text{read}))$$

Using the inference rules of access-control logic and the substitution rules shown above, give proofs for the two judgements

$$\Gamma \vdash (\textit{Agent says Permitted}(\textit{File}_1, \textit{read})) \Rightarrow \textit{Permitted}(\textit{File}_1, \textit{read})$$
$$\Gamma \vdash (\textit{Agent says Permitted}(\textit{File}_2, \textit{read})) \Rightarrow \textit{Permitted}(\textit{File}_2, \textit{read})$$