Homework 6

1. Access-control logic includes formulas of the form

   $$P \textit{ says } F$$

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

2. The informal meaning of the formula P *controls* F is 'P is entitled to do F'. Give a definition for this formula in terms of *says*.

3. Assume an access control logic with security levels, say top secret (*TS*), secret (*S*) and public (*P*), with

   $$slev(\textit{P}) < slev(\textit{S}) < slev(\textit{TS})$$

   (a) Modify the formula

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

   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

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

   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 $slev(\textit{S}) < slev(\textit{TS})$. Assume further the substitution rules

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

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

   Let Γ be the set containing the following six formulas

$slev(\mathit{S}) < slev(\mathit{TS})$
$slev(\mathit{Agent}) = \mathit{TS}$
$slev(\mathit{File}_1) = \mathit{S}$
$slev(\mathit{File}_2) = \mathit{TS}$
$\forall O.\ slev(O) < slev(\mathit{Agent}) \Rightarrow (\mathit{Agent\ controls\ Permitted}(O, \mathit{read}))$
$\forall O.\ slev(O) = slev(\mathit{Agent}) \Rightarrow (\mathit{Agent\ controls\ Permitted}(O, \mathit{read}))$

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

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