CS 513 Homework 4: Authorization Policies (Appendix)

A *proof tree* is a set of applications of inference rules, arranged as a tree with a goal at the root. The *goal* is the formula being proved. The leaves of the tree (at the top) must be true formulas that require no more applications of inference rules.

The following proof tree shows that the program

$$\mathsf{if}\ l == 0\ \mathsf{then}\ h = 1\ \mathsf{else}\ l = 1$$

is secure, using the inference rules given in lecture. The tree also uses an inference rule immediately below each leaf to show the reasoning about the max operator applied to labels.

$$\dfrac{\dfrac{D = L}{D = \max(\underline{l == 0}, L)} \quad \dfrac{\dfrac{L \leq H}{\max(\underline{1}, D) \leq \underline{h}}}{h = 1\ \mathbf{sif}\ \underline{pc} = D} \quad \dfrac{\dfrac{L \leq L}{\max(\underline{1}, D) \leq \underline{l}}}{l = 1\ \mathbf{sif}\ \underline{pc} = D}}{\mathsf{if}\ l == 0\ \mathsf{then}\ h = 1\ \mathsf{else}\ l = 1\ \mathbf{sif}\ \underline{pc} = L}$$