COMP9152 Assignment 5
Due: Wed, June 4

May 23, 2008

FHMV: 6.11, 6.12, 6.13, 6.19, plus the following problems:

Consider the semantic model for intransitive noninterference. Let $X \subseteq D$ be a set of security domains, and let $\pi : A^* \times \mathit{Prop} \to \{0, 1\}$ interpret the atomic propositions *Prop* at sequences of actions of a system M. Given a sequence of actions $\alpha \in A^*$, write $\alpha|X$ for the subsequence of all actions a with $dom(a) \in X$.

Define the variant D^*_G of the notion of distributed knowledge, with semantics given by $M, \pi, \alpha \models D^*_G\phi$ if $M, \pi, \alpha' \models \phi$ for all for all α' such that $\alpha|G = \alpha'|G$ and $\mathtt{view}_u(\alpha) = \mathtt{view}_u(\alpha')$ for all $u \in G$.

Say that a proposition p *depends only on* X if for all sequences of actions $\alpha, \alpha' \in A^*$, if $\alpha|X = \alpha'|X$ then $M, \pi, \alpha \models p$ iff $M, \pi, \alpha' \models p$.

1. Prove the following generalization of the claim that TA-security correctly solves the problem identified with IP-security.

   Suppose that a system M is TA-secure with respect to a nonintereference relation $\rightarrowtail$ that does not have any cycles, let $u \in D$ be a domain, and let p depend only on $D \setminus u$. Let $I = \{v \in D \mid v \neq u,\ v \rightarrowtail u\}$ be the set of daomins that may interfere with u.

   Then for all $\alpha \in A^*$ if $M, \pi, \alpha \models K_u p$ then $M, \pi, \alpha, \models D^*_I p$,

2. Does this hold if we use the usual notion of distributed knowledge instead of D^*_G?