Orc Secure Information Flow Notes

Adrian Quark

January 31, 2009

1 Publication Predicate

pub is a decision procedure for finding the set of publications of an expression given a context for variables, i.e. $pub : Expression \to Context \to \{Publication\}$. $Context = Variable \to Publication$. $Publication = (Predicate, Predicate)$ where the first is a predicate denoting the value published and the second a predicate which holds iff the value was published.

$$
\begin{aligned}
pub\ [\texttt{\~{}}x]\ E &= \{(\neg v, c)\} \\
&\quad \text{where } (v, c) = E(x) \\
pub\ [x\ \texttt{||}\ y]\ E &= \{(v \vee v', c \wedge c')\} \\
&\quad \text{where } (v, c) = E(x), (v', c') = E(y) \\
pub\ [x\ \texttt{\&\&}\ y]\ E &= \{(v \wedge v', c \wedge c')\} \\
&\quad \text{where } (v, c) = E(x), (v', c') = E(y) \\
pub\ [\texttt{if}(x)]\ E &= \{(\texttt{signal}, v \wedge c)\} \\
&\quad \text{where } (v, c) = E(x) \\
pub\ [M(x)]\ E &= \{(?, ? \wedge c)\} \\
&\quad \text{where } (\_, c) = E(x) \\
pub\ [f(x)]\ E &= pub\ g\ (E + f : (?, \texttt{false}) + y : E(x)) \\
&\quad \text{where } [\texttt{def}\ \ f(y) = g] \\
pub\ [f\ \texttt{>x>}\ g]\ E &= \{vc' | vc' \leftarrow pub\ g\ (E + x : vc), vc \leftarrow pub\ f\ E\} \\
pub\ [g\ \texttt{<x<}\ f]\ E &= \{vc' | vc' \leftarrow pub\ g\ (E + x : vc), vc \leftarrow pub\ f\ E\} \\
pub\ [f\ \texttt{|}\ g]\ E &= (pub\ f\ E) \cup (pub\ g\ E) \\
pub\ [f\ \texttt{;}\ g]\ E &= fp \cup \{(v', c' \wedge (\neg c)) \mid (\_, c) \leftarrow fp, (v', c') \leftarrow gp\} \\
&\quad \text{where } fp = (pub\ f\ E), gp = (pub\ g\ E)
\end{aligned}
\tag{1}
$$