On Compositional Information Flow Aware Refinement

Christoph Baumann
Mads Dam
Roberto Guanciale
Hamed Nemati

CSF 2021
Modular verification based on refinement

---

But relationship between Info flow security and refinement is troubled.

J. McLean: A general theory of composition for a class of "possibilistic" properties
Modular verification based on refinement

But relationship between Info flow security and refinement is troubled.

J. McLean: A general theory of composition for a class of "possibilistic" properties
Well-formed refinement ↓

↓ is a simulation that

- can reduce non-determinism
- can add new variable that introduce discriminating power (e.g. cache state, time)
Semantic justification in terms of the knowledge an observer gains

Given a run $\square$, ignorance $\square = \text{all runs that are observational equivalent (\sim)}$

A. Askarov and S. Chong: Learning is change in knowledge: Knowledge-based security for dynamic policies
Ignorance - Knowledge

- Semantic justification in terms of the knowledge an observer gains
- Given a run \[ \square \], ignorance \[ \square \] = all runs that are observational equivalent (~)

A. Askarov and S. Chong: Learning is change in knowledge: Knowledge-based security for dynamic policies
Ignorance Preserving Refinement (IPR)

\[ a \downarrow c \Rightarrow \Diamond a = \Diamond c \uparrow \]

C. Morgan, “The Shadow Knows: Refinement and security in sequential programs”
Ignorance Preserving Refinement (IPR)

\[ a \downarrow c \text{ implies that } \llbracket a \rrbracket^a = \llbracket c \rrbracket^c \uparrow \]

C. Morgan, “The Shadow Knows: Refinement and security in sequential programs”
Ignorance Preserving Refinement (IPR)

\[ \mathcal{a} \downarrow \mathcal{c} \] implies that \( \mathcal{a}^{\downarrow} = \mathcal{c}^{\uparrow} \)

covers the intentional leakage of abstract secret information (e.g. pwd check) and data refinement
Ignorance Preserving Refinement (IPR)

\[ a \downarrow^c \text{ implies that } a^a = c^\uparrow \]

covers the intentional leakage of \textit{abstract} secret information (e.g. pwd check) and data refinement
Compositionality
Compositionality
Relational Refinement

${P} \downarrow {Q}$ is a relational refinement iff
Relational Refinement

\[ \{P\} \downarrow \{Q\} \text{ is a relational refinement iff} \]

\begin{figure}
\centering
\begin{tikzpicture}
  \node (a1) at (0,0) {a1};
  \node (a2) at (0,-2) {a2};
  \node (c1) at (0,-4) {c1};
  \node (P) at (0,-6) {P};

  \draw[->] (a1) -- (a2);
  \draw[->] (a2) -- (c1);
  \draw[->] (c1) -- (P);
\end{tikzpicture}
\end{figure}
Relational Refinement

\( \{P\} \downarrow \{Q\} \) is a relational refinement iff
Relational Refinement

\[ \{P\} \downarrow \{Q\} \text{ is a relational refinement iff} \]
Relational Refinement

\{P\} \Downarrow \{Q\} is a relational refinement iff
Relational Refinement

\[
\{P\} \Downarrow \{Q\} \text{ is a relational refinement iff}
\]
Relational Refinement

If \( \{P\} \downarrow \{Q\} \) is a relational refinement the it is an IPR

If \( \{P\} \downarrow_1 \{Q\} \) and \( \{Q\} \downarrow_2 \{R\} \) are relational refinements then

\( \{P\} \downarrow_1 : \downarrow_2 \{R\} \) is a relational refinement
In the paper

- Two example applications:
  - SMC addition
  - Oblivious RAM
- Vertical composition
- Related work