论文标题

Static analysis for efficient hybrid information-flow control

Scott Moore
School of Engineering and Applied Sciences
Harvard University
Cambridge, MA, USA
sdmoore@fas.harvard.edu

Stephen Chong
School of Engineering and Applied Sciences
Harvard University
Cambridge, MA, USA
chong@seas.harvard.edu

研究动机&背景

本文的动机和背景是探索使用静态分析来提高混合信息流监控器的效率。 作者的目标是提供精确、强大的信息安全保证，同时减少监视器相关的运行时开销。

本文提出了静态分析和动态机制的组合来实现这一目标，并讨论了如何使用静态分析以两种方式使混合信息流监视器更加高效：确定监视器何时停止跟踪某些变量的安全等级，并通过导出充分的条件将广泛的内存抽象合理地合并到信息流监视器中。 这允许内存抽象可以在效率和精度之间提供适当权衡。

本文主要基于 Russo 和 Sabelfeld 先前工作的简单命令式语言和混合信息流监视器

解决问题

本文解决了混合信息流监视器中运行时开销过高的问题，同时仍然提供相同的安全保证。 此外，本文还探讨了信息流监视器内存抽象的精度和效率之间的权衡。

主要方法

通过一个类型系统

两点格 Γ(x)="⊥ or T"

T 表示被不再追踪的变量影响

$$\frac{\tau = \bigsqcup_{x \in \mathbf{vars}(e)} \Gamma(x)}{\Gamma \vdash e : \tau} \qquad \frac{\Gamma \vdash e : \tau}{pc \vdash \Gamma\,\{x := e\}\,\Gamma[x \mapsto pc \sqcup \tau]}$$

$$\frac{\Gamma \vdash e : \bot}{\bot \vdash \Gamma\,\{\mathsf{output}_\ell(e)\}\,\Gamma} \qquad \frac{pc \vdash \Gamma\,\{t_1\}\,\Gamma' \quad pc \vdash \Gamma'\,\{t_2\}\,\Gamma''}{pc \vdash \Gamma\,\{t_1; t_2\}\,\Gamma''}$$

$$\frac{\Gamma \vdash e : \tau \qquad pc \sqcup \tau \vdash \Gamma\,\{c_i\}\,\Gamma_i \qquad \Gamma_i \sqsubseteq \Gamma' \qquad i = 1, 2}{pc \vdash \Gamma\,\{\mathsf{if}\ e\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2\}\,\Gamma'}$$

$$\frac{\Gamma \sqsubseteq \Gamma' \qquad \Gamma' \vdash e : \tau \qquad pc \sqcup \tau \vdash \Gamma'\,\{c\}\,\Gamma'' \qquad \Gamma'' \sqsubseteq \Gamma'}{pc \vdash \Gamma\,\{\mathsf{while}\ e\ \mathsf{do}\ c\}\,\Gamma'}$$

$$\frac{}{pc \vdash \Gamma\,\{\mathsf{skip}\}\,\Gamma} \qquad \frac{}{pc \vdash \Gamma\,\{\mathsf{stop}\}\,\Gamma} \qquad \frac{}{pc \vdash \Gamma\,\{\mathsf{end}\}\,\Gamma}$$

M_{perf} - M_{RS} 基础上的改进

$$\frac{X \subseteq \mathrm{dom}(\gamma') \qquad \langle \gamma, \sigma \rangle \xrightarrow[\mathrm{M_{RS}}]{\alpha, t', m}_{\beta} \langle \gamma', \sigma' \rangle \qquad \bot \vdash \overline{\bot}[X \mapsto \top]\,\{t'\}\,\Gamma}{\langle \gamma, \sigma \rangle \xrightarrow[\mathrm{M_{PERF}}]{\alpha, t', m}_{\beta} \langle \gamma' \setminus X, \sigma' \rangle}$$

X的求解：

principal typing problem
Hunt and Sands's polynomial-time algorithm

内存抽象

将原先命令式语言扩展，支持动态内存和一级的指针

$$
\begin{array}{lrll}
\text{Values} & v & ::= & \ldots \mid r \\
\text{Expressions} & e & ::= & \ldots \mid *e \\
\text{Commands} & c & ::= & \ldots \mid x := \mathsf{new}(e) \mid e_1 \leftarrow e_2
\end{array}
$$

$$
\frac{e, m \Downarrow r \qquad m(r) = v}{*e, m \Downarrow v}
$$

$$
\frac{e, m \Downarrow v \qquad r \notin \mathrm{dom}(m)}{\langle x := \mathsf{new}(e), m\rangle \xrightarrow{\mathrm{new}(x,e,r)} \langle \mathsf{stop}, m[x \mapsto r][r \mapsto v]\rangle}
$$

$$
\frac{e_1, m \Downarrow r \qquad e_2, m \Downarrow v}{\langle e_1 \leftarrow e_2, m\rangle \xrightarrow{\mathrm{store}(e_1,e_2,r)} \langle \mathsf{stop}, m[r \mapsto v]\rangle}
$$

M_{mem} :

NEW

$$
\frac{\begin{array}{c} A = \mathit{points\text{-}to}(x, r) \\ \ell = \mathit{lev}(e, \gamma, m) \sqcup \mathit{lev}(\sigma) \\ \gamma'(s) = \begin{cases} \ell \sqcup \gamma(s) & s \in A \\ \gamma(s) & \text{otherwise} \end{cases} \end{array}}{\langle \gamma, \sigma\rangle \xrightarrow[\mathrm{M_{MEM}}]{\mathrm{new}(x,e,r),t,m} \langle \gamma'[x \mapsto \mathit{lev}(\sigma)], \sigma\rangle}
$$

STORE

$$
\frac{\begin{array}{c} A = \mathit{points\text{-}to}(e_1, r) \\ \ell = \mathit{lev}(e_1, \gamma, m) \sqcup \mathit{lev}(e_2, \gamma, m) \sqcup \mathit{lev}(\sigma) \\ \gamma'(s) = \begin{cases} \ell \sqcup \gamma(s) & a \in A \\ \gamma(s) & \text{otherwise} \end{cases} \end{array}}{\langle \gamma, \sigma\rangle \xrightarrow[\mathrm{M_{MEM}}]{\mathrm{store}(e_1,e_2,r),t,m} \langle \gamma', \sigma\rangle}
$$

$$\textsc{Branch}\quad \frac{lev(e,\gamma,m) \sqcup lev(\sigma) = \ell}{\langle \gamma, \sigma \rangle \xrightarrow[\mathrm{M_{MEM}}]{\mathrm{branch}(e,c),t,m} \langle \gamma, (\ell, \textsc{Analyze}(c,m,\gamma,\ell)) : \sigma \rangle}$$

$$lev(e,\gamma,m) = \left(\bigsqcup_{x \in \mathrm{dom}(\gamma) \cap \mathrm{vars}(e)} \gamma(x) \right) \sqcup \bigsqcup_{a \in \mathrm{dom}(\gamma) \cap A} \gamma(a)$$

where

$$A = \bigcup \{ points\text{-}to(e', r) \mid *e' \text{ appears in } e \wedge (e', m \Downarrow r) \}.$$

优缺点

1. 背景介绍很充分
2. 抽象很充分

缺点：

1. 没有实际的evaluation

对自己工作的启发

1. 在抽象层次上，本文抽象层次较高，可以学习本文的抽象方法
2. 信息流追踪的方法可以应用到任何和外部交互的场景下，可以考虑系统层面的信息流安全问题