Privilege separation in browser architectures

Michele Bugliesi Stefano Calzavara Enrico Steffinlongo

May 31, 2014

Abstract

In many software systems as modern web browsers the user and his sensitive data often interact with the untrusted outer world. This scenario can pose a serious threat to the user's private data and gives new relevance to an old story in computer science: providing controlled access to untrusted components, while preserving usability and ease of interaction. To address the threats of untrusted components, modern web browsers propose privilege-separated architectures, which isolate components that manage critical tasks and data from components which handle untrusted inputs. The former components are given strong permissions, possibly coinciding with the full set of permissions granted to the user, while the untrusted components are granted only limited privileges, to limit possible malicious behaviours: all the interactions between trusted and untrusted components is handled via message passing. In this thesis we introduce a formal semantics for privilege-separated architectures and we provide a general definition of privilege separation: we discuss how different privilege-separated architectures can be evaluated in our framework, identifying how different security threats can be avoided, mitigated or disregarded. Specifically, we evaluate in detail the existing Google Chrome Extension Architecture in our formal model and we discuss how its design can mitigate serious security risks, with only limited impact on the user experience.

Contents

Chapter 1

Motivation

1.1 Privilege separation

1.2 Privilege escalation attacks

1.3 Chrome extension architecture overview

Chrome by Google, as all actual-days browsers, provides a powerful extension framework. This gives to developers a huge architecture made explicitly to extend the core browser potentiality in order to build small programs that enhance user-experience. In Chrome web store there are a lot of extensions with very various behaviors like security enhancers, theme changers, organizers or other utilities, multimedia visualizer, games and others. For example, AdBlock is an extension made to block all ads on websites; ShareMeNot "protects the user against being tracked from third-party social media buttons while still allowing it to use them"[1]. As we can notice extensions have different purposes, and many of them has to interact with web pages. This creates a very large attack surface for attackers and is a big threat for the user. Moreover many extensions are written by developers that are not security experts so, even if their behavior is not malign, the bugs that can appear in them can be easily exploited by attackers. Google Chrome extension architecture adopt a composition of the privilege-separated approach. As deeply discussed in [2] the actual Google Chrome extension framework is based on privilege separation, least privilege and strong isolation.

1.4 Chrome extension architecture weaknesses

1.5 Proposal

Chapter 2

Background

2.1 Chrome extension architecture details

2.2 Flow logic

Chapter 3

Formalization

3.1 Threat Model

3.2 Calculus

3.3 Safety properties

3.4 Analysis specification

3.4.1 Abstract succinct

Abstract cache	$\hat{C}$	:	$\mathcal{L} \to \hat{V}$
Abstract variable environment	$\hat{\Gamma}$	:	$\mathcal{V} \to \hat{V}$
Abstract memory	$\hat{\mu}$	:	$\mathcal{L} \times \mathcal{P} \to \hat{V}$
Abstract permission cache	$\hat{P}$	:	$\mathcal{L} \to \mathcal{P}$

$$
\begin{array}{ll}
[\mathit{PE\text{-}Val}] & (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} c : \hat{v} \text{ iff } \{d_c\} \subseteq \hat{v} \\
[\mathit{PE\text{-}Var}] & (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} x : \hat{v} \text{ iff } \hat{\Gamma}(x) \subseteq \hat{v} \\
[\mathit{PE\text{-}Lambda}] & (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} \lambda x.e : \hat{v} \text{ iff } \{\lambda x.e\} \subseteq \hat{v} \\
[\mathit{PE\text{-}Obj}] & (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} \{\overrightarrow{str_i : e_i}\} : \hat{v} \gg \rho \text{ iff} \\
 & \quad \forall i : (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_i : \hat{v}_i \gg \rho_i \wedge \\
 & \quad\quad \{\overrightarrow{str_i : \hat{v}_i}\} \subseteq \hat{v} \wedge \\
 & \quad\quad \rho_i \sqsubseteq \rho \\
[\mathit{PE\text{-}Let}] & (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} \textbf{let } \overrightarrow{x_i = e_i} \textbf{ in } e' : \hat{v} \gg \rho \text{ iff} \\
 & \quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e' : \hat{v} \gg \rho' \wedge \\
 & \quad \rho' \sqsubseteq \rho \wedge \\
 & \quad \forall i : \\
 & \quad\quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_i : \hat{v}_i \gg \rho_i \wedge \\
 & \quad\quad \hat{v}_i \subseteq \hat{\Gamma}(x_i) \wedge \\
 & \quad\quad \rho_i \sqsubseteq \rho \\
[\mathit{PE\text{-}App}] & (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_1\, e_2 : \hat{v} \gg \rho \text{ iff} \\
 & \quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_1 : \hat{v}_1 \gg \rho_1 \wedge \\
 & \quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_2 : \hat{v}_2 \gg \rho_2 \wedge \\
 & \quad \rho_1 \sqsubseteq \rho \wedge \\
 & \quad \rho_2 \sqsubseteq \rho \wedge \\
 & \quad \forall (\lambda x.e_0) \in \hat{v}_1 : \\
 & \quad\quad \hat{v}_2 \subseteq \hat{\Gamma}(x) \wedge \\
 & \quad\quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_0 : \hat{v}_0 \gg \rho_0 \wedge \\
 & \quad\quad \rho_0 \sqsubseteq \rho \wedge \\
 & \quad\quad \hat{v}_0 \subseteq \hat{v} \\
[\mathit{PE\text{-}Op}] & (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} op(\overrightarrow{e_i}) : \hat{v} \gg \rho \text{ iff} \\
 & \quad \forall i : \\
 & \quad\quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_i : \hat{v}_i \gg \rho_i \wedge \\
 & \quad\quad \rho_i \sqsubseteq \rho \wedge \\
 & \quad \widehat{op}(\overrightarrow{\hat{v}_i}) \subseteq \hat{v} \\
[\mathit{PE\text{-}Cond}] & (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} \textbf{if } (e_0) \ \{\ e_1\ \} \textbf{ else } \{\ e_2\ \} : \hat{v} \gg \rho \text{ iff} \\
 & \quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_0 : \hat{v}_0 \gg \rho_0 \wedge \\
 & \quad \rho_0 \sqsubseteq \rho \wedge \\
 & \quad \widehat{\textbf{true}} \in \hat{v}_0 \Rightarrow \\
 & \quad\quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_1 : \hat{v}_1 \gg \rho_1 \wedge \hat{v}_1 \subseteq \hat{v} \wedge \rho_1 \sqsubseteq \rho \wedge \\
 & \quad \widehat{\textbf{false}} \in \hat{v}_0 \Rightarrow \\
 & \quad\quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_2 : \hat{v}_2 \gg \rho_2 \wedge \hat{v}_2 \subseteq \hat{v} \wedge \rho_2 \sqsubseteq \rho \\
[\mathit{PE\text{-}While}] & (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} \textbf{while } (e_1) \ \{\ e_2\ \} : \hat{v} \gg \rho \text{ iff} \\
 & \quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_1 : \hat{v}_1 \gg \rho_1 \wedge \\
 & \quad \rho_1 \sqsubseteq \rho \wedge \\
 & \quad \widehat{\textbf{true}} \in \hat{v}_1 \Rightarrow \\
 & \quad\quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_2 : \hat{v}_2 \gg \rho_2 \wedge \hat{v}_2 \subseteq \hat{v} \wedge \rho_2 \sqsubseteq \rho \wedge \\
 & \quad \widehat{\textbf{false}} \in \hat{v}_1 \Rightarrow \\
 & \quad\quad \widehat{\textbf{undefined}} \subseteq \hat{v} \\
[\mathit{PE\text{-}GetField}] & (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_1[e_2] : \hat{v} \gg \rho \text{ iff} \\
 & \quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_1 : \hat{v}_1 \gg \rho_1 \wedge \\
 & \quad \rho_1 \sqsubseteq \rho \wedge \\
 & \quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_2 : \hat{v}_2 \gg \rho_2 \wedge \\
 & \quad \rho_2 \sqsubseteq \rho \wedge \\
 & \quad \widehat{get}(\hat{v}_1, \hat{v}_2) \subseteq \hat{v}
\end{array}
$$

$$
\begin{array}{ll}
[\textit{PE-SetField}] & (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_0[e_1] = e2 : \hat{v} \gg \rho \text{ iff} \\
 & \quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_0 : \hat{v}_0 \gg \rho_0 \wedge \\
 & \quad \rho_0 \sqsubseteq \rho \wedge \\
 & \quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_1 : \hat{v}_1 \gg \rho_1 \wedge \\
 & \quad \rho_1 \sqsubseteq \rho \wedge \\
 & \quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_2 : \hat{v}_2 \gg \rho_2 \wedge \\
 & \quad \rho_2 \sqsubseteq \rho \wedge \\
 & \quad \widehat{set}(\hat{v}_0, \hat{v}_1, \hat{v}_2) \subseteq \hat{v} \\
[\textit{PE-DelField}] & (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} \textbf{delete } e_1[e_2] : \hat{v} \gg \rho \text{ iff} \\
 & \quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_1 : \hat{v}_1 \gg \rho_1 \wedge \\
 & \quad \rho_1 \sqsubseteq \rho \wedge \\
 & \quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_2 : \hat{v}_2 \gg \rho_2 \wedge \\
 & \quad \rho_2 \sqsubseteq \rho \wedge \\
 & \quad \widehat{del}(\hat{v}_1, \hat{v}_2) \subseteq \hat{v} \\
[\textit{PE-Ref}] & (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} \textbf{ref}_{r,\rho_r}\ e : \{r\} \gg \rho \text{ iff} \\
 & \quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e : \hat{v} \gg \rho \wedge \\
 & \quad \rho_r \sqsubseteq \rho_s \Rightarrow \hat{v} \subseteq \hat{\mu}(r, \rho_r) \\
[\textit{PE-DeRef}] & (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} \textbf{deref } e : \hat{v} \gg \rho \text{ iff} \\
 & \quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e : \hat{v}_1 \gg \rho_1 \wedge \\
 & \quad \rho_1 \sqsubseteq \rho \wedge \\
 & \quad \forall r \in \hat{v}_1 : \forall \rho_r \sqsubseteq \rho_s : \hat{\mu}(r, \rho_r) \subseteq \hat{v} \\
[\textit{PE-SetRef}] & (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_1 = e_2 : \hat{v} \gg \rho \text{ iff} \\
 & \quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e : \hat{v}_1 \gg \rho_1 \wedge \\
 & \quad \rho_1 \sqsubseteq \rho \wedge \\
 & \quad (\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_2 : \hat{v}_2 \gg \rho_2 \wedge \\
 & \quad \rho_2 \sqsubseteq \rho \wedge \\
 & \quad \forall r \in \hat{v}_1 : \forall \rho_r \sqsubseteq \rho_s : \\
 & \qquad \hat{v}_2 \subseteq \hat{\mu}(r, \rho_r) \wedge \\
 & \qquad \hat{v}_2 \subseteq \hat{v} \\
[\textit{PE-Send}] & \ldots \\
[\textit{PE-Err}] & \ldots \\
[\textit{PE-Exercise}] & \ldots
\end{array}
$$

3.4.2 Compositional Verbose

$$
\begin{array}{ll}
[\textit{CV-Val}] & (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} (c)^{\ell} \text{ iff } \{d_c\} \subseteq \hat{C}(\ell) \\
[\textit{CV-Var}] & (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} (x)^{\ell} \text{ iff } \hat{\Gamma}(x) \subseteq \hat{C}(\ell) \\
[\textit{CV-Lambda}] & (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} (\lambda x.{e_0}^{\ell_0})^{\ell} \text{ iff} \\
 & \quad \{\lambda x.{e_0}^{\ell_0}\} \subseteq \hat{C}(\ell) \wedge \\
 & \quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_0}^{\ell_0} \\
[\textit{CV-Obj}] & (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} (\{\overrightarrow{str_i : {e_i}^{\ell_i}}\})^{\ell} \text{ iff} \\
 & \quad \forall i : \\
 & \quad\quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_i}^{\ell_i} \wedge \\
 & \quad\quad \hat{P}(\ell_i) \sqsubseteq \hat{P}(\ell) \wedge \\
 & \quad \{\overrightarrow{str_i : \hat{C}(\ell_i)}\} \subseteq \hat{C}_{\ell} \\
[\textit{CV-Let}] & (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} (\textbf{let } \overrightarrow{x_i = {e_i}^{\ell_i}} \textbf{ in } {e'}^{\ell'})^{\ell} \text{ iff} \\
 & \quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e'}^{\ell'} \wedge \\
 & \quad \hat{P}(\ell') \sqsubseteq \hat{P}(\ell) \wedge \\
 & \quad \hat{C}(\ell') \subseteq \hat{C}(\ell) \wedge \\
 & \quad \forall i : \\
 & \quad\quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_i}^{\ell_i} \wedge \\
 & \quad\quad \hat{C}(\ell_i) \subseteq \hat{\Gamma}(x_i) \wedge \\
 & \quad\quad \hat{P}(\ell_i) \sqsubseteq \hat{P}(\ell) \\
[\textit{CV-App}] & (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} ({e_1}^{\ell_1}\, {e_2}^{\ell_2})^{\ell} \text{ iff} \\
 & \quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_1}^{\ell_1} \wedge (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_2}^{\ell_2} \wedge \\
 & \quad \hat{P}(\ell_1) \sqsubseteq \hat{P}(\ell) \wedge \hat{P}(\ell_2) \sqsubseteq \hat{P}(\ell) \\
 & \quad \forall (\lambda x.{e_0}^{\ell_0}) \in \hat{C}(\ell_1) : \\
 & \quad\quad \hat{C}(\ell_2) \subseteq \hat{\Gamma}(x) \wedge \hat{C}(\ell_0) \subseteq \hat{C}(\ell) \wedge \\
 & \quad\quad \hat{P}(\ell_0) \sqsubseteq \hat{P}(\ell) \\
[\textit{CV-Op}] & (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} (op(\overrightarrow{{e_i}^{\ell_i}}))^{\ell} \text{ iff} \\
 & \quad \forall i : \\
 & \quad\quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_i}^{\ell_i} \wedge \\
 & \quad\quad \hat{P}(\ell_i) \sqsubseteq \hat{P}(\ell) \wedge \\
 & \quad \widehat{op}(\hat{C}(\ell_i)) \subseteq \hat{C}(\ell) \\
[\textit{CV-Cond}] & (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} (\textbf{if } ({e_0}^{\ell_0}) \ \{\ {e_1}^{\ell_1}\ \} \textbf{ else } \{\ {e_2}^{\ell_2}\ \})^{\ell} \text{ iff} \\
 & \quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_0}^{\ell_0} \wedge \\
 & \quad \hat{P}(\ell_0) \sqsubseteq \hat{P}(\ell) \wedge \\
 & \quad \widehat{\textbf{true}} \in \hat{C}(\ell_0) \Rightarrow \\
 & \quad\quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_1}^{\ell_1} \wedge \hat{C}(\ell_1) \subseteq \hat{C}(\ell) \wedge \\
 & \quad\quad \hat{P}(\ell_1) \sqsubseteq \hat{P}(\ell) \wedge \\
 & \quad \widehat{\textbf{false}} \in \hat{C}(\ell_0) \Rightarrow \\
 & \quad\quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_2}^{\ell_2} \wedge \hat{C}(\ell_2) \subseteq \hat{C}(\ell) \wedge \\
 & \quad\quad \hat{P}(\ell_2) \sqsubseteq \hat{P}(\ell) \\
[\textit{CV-While}] & (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} (\textbf{while } ({e_1}^{\ell_1}) \ \{\ {e_2}^{\ell_2}\ \})^{\ell} \text{ iff} \\
 & \quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_1}^{\ell_1} \wedge \\
 & \quad \hat{P}(\ell_1) \sqsubseteq \hat{P}(\ell) \wedge \\
 & \quad \widehat{\textbf{true}} \in \hat{C}(\ell_1) \Rightarrow \\
 & \quad\quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_2}^{\ell_2} \wedge \hat{C}(\ell_2) \subseteq \hat{C}(\ell) \wedge \\
 & \quad\quad \hat{P}(\ell_2) \sqsubseteq \hat{P}(\ell) \wedge \\
 & \quad \widehat{\textbf{false}} \in \hat{C}(\ell_1) \Rightarrow \widehat{\textbf{undefined}} \subseteq \hat{C}(\ell)
\end{array}
$$

$$
\begin{array}{ll}
[\mathit{CV\text{-}GetField}] & (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} ({e_1}^{\ell_1}[{e_2}^{\ell_2}])^{\ell} \text{ iff} \\
& \quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_1}^{\ell_1} \wedge \\
& \quad \hat{P}(\ell_1) \sqsubseteq \hat{P}(\ell) \wedge \\
& \quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_2}^{\ell_2} \wedge \\
& \quad \hat{P}(\ell_2) \sqsubseteq \hat{P}(\ell) \wedge \\
& \quad \widehat{get}(\hat{C}(\ell_1),\hat{C}(\ell_2)) \subseteq \hat{C}(\ell) \\
[\mathit{CV\text{-}SetField}] & (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} ({e_0}^{\ell_0}[{e_1}^{\ell_1}] = {e_2}^{\ell_2})^{\ell} \text{ iff} \\
& \quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_0}^{\ell_0} \wedge \\
& \quad \hat{P}(\ell_0) \sqsubseteq \hat{P}(\ell) \wedge \\
& \quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_1}^{\ell_1} \wedge \\
& \quad \hat{P}(\ell_1) \sqsubseteq \hat{P}(\ell) \wedge \\
& \quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_2}^{\ell_2} \wedge \\
& \quad \hat{P}(\ell_2) \sqsubseteq \hat{P}(\ell) \wedge \\
& \quad \widehat{set}(\hat{C}(\ell_0),\hat{C}(\ell_1),\hat{C}(\ell_2)) \subseteq \hat{C}(\ell) \\
[\mathit{CV\text{-}DelField}] & (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} (\mathbf{delete}\ {e_1}^{\ell_1}[{e_2}^{\ell_2}])^{\ell} \text{ iff} \\
& \quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_1}^{\ell_1} \wedge \\
& \quad \hat{P}(\ell_1) \sqsubseteq \hat{P}(\ell) \wedge \\
& \quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_2}^{\ell_2} \wedge \\
& \quad \hat{P}(\ell_2) \sqsubseteq \hat{P}(\ell) \wedge \\
& \quad \widehat{del}(\hat{C}(\ell_1),\hat{C}(\ell_2)) \subseteq \hat{C}(\ell) \\
[\mathit{CV\text{-}Ref}] & (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} (\mathbf{ref}_{r,\rho_r}\ {e_1}^{\ell_1})^{\ell} \text{ iff} \\
& \quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_1}^{\ell_1} \wedge \\
& \quad \{r\} \subseteq \hat{C}(\ell) \wedge \\
& \quad \hat{P}(\ell_1) \sqsubseteq \hat{P}(\ell) \wedge \\
& \quad \rho_r \sqsubseteq \rho_s \Rightarrow \hat{C}(\ell_1) \subseteq \hat{\mu}(r,\rho_r) \\
[\mathit{CV\text{-}DeRef}] & (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} (\mathbf{deref}\ {e_1}^{\ell_1})^{\ell} \text{ iff} \\
& \quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_1}^{\ell_1} \wedge \\
& \quad \hat{P}(\ell_1) \sqsubseteq \hat{P}(\ell) \wedge \\
& \quad \forall r \in \hat{C}(\ell_1) : \forall \rho_r \sqsubseteq \rho_s : \\
& \quad\quad \hat{\mu}(r,\rho_r) \subseteq \hat{C}(\ell) \\
[\mathit{CV\text{-}SetRef}] & (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} ({e_1}^{\ell_1} = {e_2}^{\ell_2})^{\ell} \text{ iff} \\
& \quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_1}^{\ell_1} \wedge \\
& \quad \hat{P}(\ell_1) \sqsubseteq \hat{P}(\ell) \wedge \\
& \quad (\hat{C},\hat{\Gamma},\hat{\mu},\hat{P}) \models_{c\rho_s} {e_2}^{\ell_2} \wedge \\
& \quad \hat{P}(\ell_2) \sqsubseteq \hat{P}(\ell) \wedge \\
& \quad \forall r \in \hat{C}(\ell_1) : \forall \rho_r \sqsubseteq \rho_s : \\
& \quad\quad \hat{C}(\ell_2) \subseteq \hat{\mu}(r,\rho_r) \wedge \\
& \quad \hat{C}(\ell_2) \subseteq \hat{C}(\ell) \\
[\mathit{PE\text{-}Send}] & \ldots \\
[\mathit{PE\text{-}Err}] & \ldots \\
[\mathit{PE\text{-}Exercise}] & \ldots
\end{array}
$$

3.5 Theorem

3.6 Requirements for correctness

Chapter 4

Abstract Domains

4.1 Abstract domains choice

$R_1 = \{\overrightarrow{\widehat{str_i} : \widehat{v_i}}\} \sqsubseteq \{\overrightarrow{\widehat{str_j} : \widehat{v_j}}\} = R_2$ sse:

1. R_1 ha meno campi di R_2
2. ogni campo di R_1 e' piu' preciso del **corrispondente** campo di R_2

$\forall i, \exists j : \widehat{str_i} \sqsubseteq \widehat{str_j}$
$\forall i, \exists j : \widehat{str_i} \sqsubseteq \widehat{str_j} \Rightarrow \widehat{v_i} \sqsubseteq \widehat{v_j}$
Set:

- Exact
  - $\exists \rightarrow Union$
  - $\nexists \rightarrow addinprefix$
- Prefix
  - aggiungo in $*$

$\hat{v} \sqsubseteq \hat{v}'$ iff $\forall \widehat{u}_i \in \hat{v}, \exists \widehat{u}_j \in \hat{v}' : \widehat{u}_i \sqsubseteq \widehat{u}_j$.
If Galois connection then
$\hat{v} \sqsubseteq \hat{v}'$ iff $\gamma(\hat{v}) \subseteq \gamma(\hat{v}')$
where $\gamma : \widehat{V} \rightarrow P(V)$ is the concretisation function.
$\gamma_p : \widehat{PV} \rightarrow P(V)$
$\gamma(\hat{v}) = \bigcup_{\widehat{u}_i \in \hat{v}} \gamma_p(\widehat{u}_i)$

$\widehat{pre_{bool}} = \widehat{true}|\widehat{false}$

$\widehat{u_{bool}} = \{\overrightarrow{\widehat{pre_{bool}}}\}$ with $\sqsubseteq = \subseteq$

$\widehat{pre_{int}} = \oplus|0|\ominus$

$\widehat{u_{int}} = \{\overrightarrow{\widehat{pre_{int}}}\}$ with $\sqsubseteq = \subseteq$

$\widehat{pre_{string}} = s|s*$

$\widehat{u_{string}} = \{\overrightarrow{\widehat{pre_{string}}}\}$ with $\sqsubseteq = \subseteq$
— Giulia's spec. is more tricky than $\subseteq$

$\widehat{pre_{ref}} = r$

$\widehat{u_{ref}} = \{\overrightarrow{\widehat{pre_{ref}}}\}$ with $\sqsubseteq = \subseteq$

$\widehat{pre_{\lambda}} = \lambda$

$\widehat{u_{\lambda}} = \{\overrightarrow{\widehat{pre_{\lambda}}}\}$ with $\sqsubseteq = \subseteq$

$\widehat{pre_{rec}} = \{\overrightarrow{\widehat{str}_i : \hat{v}_i}\}$

$\widehat{u_{rec}} = \widehat{pre_{rec}}$ with $\sqsubseteq = \widehat{u_{rec}}_{\sqsubseteq}$

$\hat{v} = (\widehat{u_{bool}}, \widehat{u_{int}}, \widehat{u_{string}}, \widehat{u_{ref}}, \widehat{u_{\lambda}}, \widehat{u_{rec}}, \{\widehat{Null}\}, \{\widehat{Undef}\})$

with $\hat{v} \sqsubseteq \hat{v}'$ iff
$\widehat{u_{bool}} \sqsubseteq \widehat{u_{bool}}' \wedge$
$\widehat{u_{int}} \sqsubseteq \widehat{u_{int}}' \wedge$
$\widehat{u_{string}} \sqsubseteq \widehat{u_{string}}' \wedge$
$\widehat{u_{ref}} \sqsubseteq \widehat{u_{ref}}' \wedge$
$\widehat{u_{\lambda}} \sqsubseteq \widehat{u_{\lambda}}' \wedge$
$\widehat{u_{rec}} \sqsubseteq \widehat{u_{rec}}' \wedge$
$\widehat{Null} \notin \hat{v}' \vee \widehat{Null} \in \hat{v} \wedge \widehat{Null} \in \hat{v}' \wedge$
$\widehat{Undef} \notin \hat{v}' \vee \widehat{Undef} \in \hat{v} \wedge \widehat{Undef} \in \hat{v}'$

4.2 Abstract operations

4.3 Requirements verification

Chapter 5

Implementation

5.1 Constraint generation

Constraint elements: E.

$$\begin{array}{lll}
\textit{Cache element} & \mathsf{C}(\ell) & : \ \mathcal{L} \rightarrow \hat{V} \\
\textit{Var element} & \Gamma(x) & : \ \mathcal{V} \rightarrow \hat{V} \\
\textit{State element} & \mathsf{M}(\mathcal{P}, ref) & : \ \mathcal{L} \times \mathcal{P} \rightarrow \hat{V}
\end{array}$$

Permission Element: $\mathsf{P}(\ell) : \mathcal{L} \rightarrow \mathcal{P}$

Constraint form.

$$\begin{array}{lrcl}
\textit{Term inclusion} & \{\hat{v}\} & \subseteq & \mathsf{E} \\
\textit{Element inclusion} & \mathsf{E} & \subseteq & \mathsf{E} \\
\textit{Permission inclusion} & \mathsf{P}(\ell) & \sqsubseteq & \mathsf{P}(\ell') \\
\textit{Operation} & \widehat{Op}(\overrightarrow{\mathsf{E}_i}) & \subseteq & \mathsf{E} \\
\textit{Implication} & \{\hat{v}\} \subseteq \mathsf{E} & \Rightarrow & \mathsf{E} \subseteq \mathsf{E}
\end{array}$$

Misc:

r_* is the set of all references of the program;
$lambda_*$ is the set of all lambdas of the program;

$$
\begin{array}{ll}
[\mathit{CG\text{-}Val}] & \mathcal{C}_{*\rho_s}[\![(c)^{\ell}]\!] = \{d_c\} \subseteq \mathsf{C}(\ell) \\
[\mathit{CG\text{-}Var}] & \mathcal{C}_{*\rho_s}[\![(x)^{\ell}]\!] = \mathsf{\Gamma}(x) \subseteq \mathsf{C}(\ell) \\
[\mathit{CG\text{-}Lambda}] & \mathcal{C}_{*\rho_s}[\![(\lambda x.e_0{}^{\ell_0})^{\ell}]\!] = \\
 & \quad \{\{\lambda x.e_0{}^{\ell_0}\} \subseteq \mathsf{C}(\ell)\}\cup \\
 & \quad \mathcal{C}_{*\rho_s}[\![(e_0{}^{\ell_0})]\!] \\
[\mathit{CG\text{-}Obj}] & \mathcal{C}_{*\rho_s}[\![(\{\overrightarrow{str_i : e_i{}^{\ell_i}}\})^{\ell}]\!] = \\
 & \quad \bigcup_i(\mathcal{C}_{*\rho_s}[\![(e_i{}^{\ell_i})]\!]\cup \\
 & \qquad \{\mathsf{P}(\ell_i) \sqsubseteq \mathsf{P}(\ell)\})\cup \\
 & \quad \{\{\overrightarrow{str_i : \mathsf{C}(\ell_i)}\} \subseteq \mathsf{C}(\ell)\} \\
[\mathit{CG\text{-}Let}] & \mathcal{C}_{*\rho_s}[\![(\textbf{let } \overrightarrow{x_i = e_i{}^{\ell_i}} \textbf{ in } e'^{\ell'})^{\ell}]\!] = \\
 & \quad \bigcup_i(\mathcal{C}_{*\rho_s}[\![(e_i{}^{\ell_i})]\!]\cup \\
 & \qquad \{\mathsf{C}(\ell_i) \subseteq \mathsf{\Gamma}(x_i)\}\cup \\
 & \qquad \{\mathsf{P}(\ell_i) \subseteq \mathsf{P}(\ell)\})\cup \\
 & \quad \mathcal{C}_{*\rho_s}[\![(e'^{\ell'})]\!]\cup \\
 & \quad \{\mathsf{P}(\ell') \sqsubseteq \mathsf{P}(\ell)\}\cup \\
 & \quad \{\mathsf{C}(\ell') \subseteq \mathsf{C}(\ell)\} \\
[\mathit{CG\text{-}App}] & \mathcal{C}_{*\rho_s}[\![(e_1{}^{\ell_1}\, e_2{}^{\ell_2})^{\ell}]\!] = \\
 & \quad \mathcal{C}_{*\rho_s}[\![(e_1{}^{\ell_1})]\!] \cup \mathcal{C}_{*\rho_s}[\![(e_2{}^{\ell_2})]\!]\cup \\
 & \quad \{\mathsf{P}(\ell_1) \sqsubseteq \mathsf{P}(\ell)\} \cup \{\mathsf{P}(\ell_2) \sqsubseteq \mathsf{P}(\ell)\}\cup \\
 & \quad \{\{t\} \subseteq \mathsf{C}(\ell_1) \Rightarrow \mathsf{C}(\ell_2) \subseteq \mathsf{\Gamma}(x) \\
 & \qquad |t = (\lambda x.e_0{}^{\ell_0}) \in \mathit{lambda}_*\}\cup \\
 & \quad \{\{t\} \subseteq \mathsf{C}(\ell_1) \Rightarrow \mathsf{C}(\ell_0) \subseteq \mathsf{C}(\ell) \\
 & \qquad |t = (\lambda x.e_0{}^{\ell_0}) \in \mathit{lambda}_*\}\cup \\
 & \quad \{\{t\} \subseteq \mathsf{C}(\ell_1) \Rightarrow \mathsf{P}(\ell_0) \sqsubseteq \mathsf{P}(\ell) \\
 & \qquad |t = (\lambda x.e_0{}^{\ell_0}) \in \mathit{lambda}_*\}\cup \\
[\mathit{CG\text{-}Op}] & \mathcal{C}_{*\rho_s}[\![(op(\overrightarrow{e_i{}^{\ell_i}}))^{\ell}]\!] = \\
 & \quad \bigcup_i(\mathcal{C}_{*\rho_s}[\![(e_i{}^{\ell_i})]\!] \cup \{\mathsf{P}(\ell_i) \sqsubseteq \mathsf{P}(\ell)\})\cup \\
 & \quad \{\widehat{op}(\mathsf{C}(\ell_i)) \subseteq \mathsf{C}(\ell)\} \\
[\mathit{CG\text{-}Cond}] & \mathcal{C}_{*\rho_s}[\![(\textbf{if } (e_0{}^{\ell_0})\ \{\ e_1{}^{\ell_1}\ \} \textbf{ else } \{\ e_2{}^{\ell_2}\ \})^{\ell}]\!] = \\
 & \quad \mathcal{C}_{*\rho_s}[\![(e_0{}^{\ell_0})]\!] \cup \mathcal{C}_{*\rho_s}[\![(e_1{}^{\ell_1})]\!] \cup \mathcal{C}_{*\rho_s}[\![(e_2{}^{\ell_2})]\!]\cup \\
 & \quad \{\hat{P}(\ell_0) \sqsubseteq \hat{P}(\ell)\}\cup \\
 & \quad \{\widehat{\textbf{true}} \in \mathsf{C}(\ell_0) \Rightarrow \mathsf{C}(\ell_1) \subseteq \mathsf{C}(\ell)\}\cup \\
 & \quad \{\widehat{\textbf{true}} \in \mathsf{C}(\ell_0) \Rightarrow \mathsf{P}(\ell_1) \sqsubseteq \mathsf{P}(\ell)\}\cup \\
 & \quad \{\widehat{\textbf{false}} \in \mathsf{C}(\ell_0) \Rightarrow \mathsf{C}(\ell_2) \subseteq \mathsf{C}(\ell)\}\cup \\
 & \quad \{\widehat{\textbf{false}} \in \mathsf{C}(\ell_0) \Rightarrow \mathsf{P}(\ell_2) \sqsubseteq \mathsf{P}(\ell)\} \\
[\mathit{CG\text{-}While}] & \mathcal{C}_{*\rho_s}[\![(\textbf{while } (e_1{}^{\ell_1})\ \{\ e_2{}^{\ell_2}\ \})^{\ell}]\!] = \\
 & \quad \mathcal{C}_{*\rho_s}[\![(e_1{}^{\ell_1})]\!] \cup \mathcal{C}_{*\rho_s}[\![(e_2{}^{\ell_2})]\!]\cup \\
 & \quad \{\mathsf{P}(\ell_1) \sqsubseteq \mathsf{P}(\ell)\}\cup \\
 & \quad \{\widehat{\textbf{true}} \in \mathsf{C}(\ell_1) \Rightarrow \mathsf{C}(\ell_2) \subseteq \mathsf{C}(\ell)\}\cup \\
 & \quad \{\widehat{\textbf{true}} \in \mathsf{C}(\ell_1) \Rightarrow \mathsf{P}(\ell_2) \subseteq \mathsf{P}(\ell)\}\cup \\
 & \quad \{\widehat{\textbf{false}} \in \mathsf{C}(\ell_1) \Rightarrow \widehat{\textbf{undefined}} \subseteq \mathsf{C}(\ell)\}
\end{array}
$$

$$
\begin{array}{ll}
[\textit{CG-GetField}] & \mathcal{C}_{*\rho_s}[\![(e_1{}^{\ell_1}[e_2{}^{\ell_2}])^{\ell}]\!] = \\
& \quad \mathcal{C}_{*\rho_s}[\![(e_1{}^{\ell_1})]\!] \cup \mathcal{C}_{*\rho_s}[\![(e_2{}^{\ell_2})]\!] \cup \\
& \quad \{\mathsf{P}(\ell_1) \sqsubseteq \mathsf{P}(\ell)\} \cup \\
& \quad \{\mathsf{P}(\ell_2) \sqsubseteq \mathsf{P}(\ell)\} \cup \\
& \quad \widehat{get}(\mathsf{C}(\ell_1), \mathsf{C}(\ell_2)) \subseteq \mathsf{C}(\ell) \\
[\textit{CG-SetField}] & \mathcal{C}_{*\rho_s}[\![(e_0{}^{\ell_0}[e_1{}^{\ell_1}] = e_2{}^{\ell_2})]\!] = \\
& \quad \mathcal{C}_{*\rho_s}[\![(e_0{}^{\ell_0})]\!] \cup \mathcal{C}_{*\rho_s}[\![(e_1{}^{\ell_1})^{\ell}]\!] \cup \mathcal{C}_{*\rho_s}[\![(e_2{}^{\ell_2})]\!] \cup \\
& \quad \{\mathsf{P}(\ell_1) \sqsubseteq \mathsf{P}(\ell)\} \cup \\
& \quad \{\mathsf{P}(\ell_2) \sqsubseteq \mathsf{P}(\ell)\} \cup \\
& \quad \{\mathsf{P}(\ell_3) \sqsubseteq \mathsf{P}(\ell)\} \cup \\
& \quad \widehat{set}(\mathsf{C}(\ell_1), \mathsf{C}(\ell_2), \mathsf{C}(\ell_2)) \subseteq \mathsf{C}(\ell) \\
[\textit{CG-DelField}] & \mathcal{C}_{*\rho_s}[\![(\mathbf{delete}\ e_1{}^{\ell_1}[e_2{}^{\ell_2}])^{\ell}]\!] = \\
& \quad \mathcal{C}_{*\rho_s}[\![(e_1{}^{\ell_1})]\!] \cup \mathcal{C}_{*\rho_s}[\![(e_2{}^{\ell_2})]\!] \cup \\
& \quad \{\mathsf{P}(\ell_1) \sqsubseteq \mathsf{P}(\ell)\} \cup \\
& \quad \{\mathsf{P}(\ell_2) \sqsubseteq \mathsf{P}(\ell)\} \cup \\
& \quad \widehat{del}(\mathsf{C}(\ell_1), \mathsf{C}(\ell_2)) \subseteq \mathsf{C}(\ell) \\
[\textit{CG-Ref}] & \mathcal{C}_{*\rho_s}[\![(\mathbf{ref}_{r,\rho_r}\ e_1{}^{\ell_1})^{\ell}]\!] = \\
& \quad \mathcal{C}_{*\rho_s}[\![(e_1{}^{\ell_1})]\!] \cup \\
& \quad \{\{r\} \subseteq \mathsf{C}(\ell)\} \cup \\
& \quad \{\mathsf{P}(\ell_1) \sqsubseteq \mathsf{P}(\ell)\} \cup \\
& \quad \{\rho_r \sqsubseteq \rho_s \Rightarrow \mathsf{C}(\ell_1) \subseteq \mathsf{M}(r, \rho_r)\} \\
[\textit{CG-DeRef}] & \mathcal{C}_{*\rho_s}[\![(\mathbf{deref}\ e_1{}^{\ell_1})^{\ell}]\!] = \\
& \quad \mathcal{C}_{*\rho_s}[\![(e_1{}^{\ell_1})]\!] \cup \\
& \quad \{\mathsf{P}(\ell_1) \sqsubseteq \mathsf{P}(\ell)\} \cup \\
& \quad \{r \in \mathsf{C}(\ell_1) \Rightarrow \mathsf{M}(r, \rho_r) \subseteq \mathsf{C}(\ell) \\
& \qquad \mid r \in r_*, \rho_r \sqsubseteq \rho_s\} \\
[\textit{CG-SetRef}] & \mathcal{C}_{*\rho_s}[\![(e_1{}^{\ell_1} = e_2{}^{\ell_2})^{\ell}]\!] = \\
& \quad \mathcal{C}_{*\rho_s}[\![(e_1{}^{\ell_1})]\!] \cup \mathcal{C}_{*\rho_s}[\![(e_2{}^{\ell_2})]\!] \cup \\
& \quad \{\mathsf{P}(\ell_1) \sqsubseteq \mathsf{P}(\ell)\} \cup \\
& \quad \{\mathsf{P}(\ell_2) \sqsubseteq \mathsf{P}(\ell)\} \cup \\
& \quad \{r \in \mathsf{C}(\ell_1) \Rightarrow \mathsf{C}(\ell_2) \subseteq \mathsf{M}(r, \rho_r) \\
& \qquad \mid r \in r_*, \rho_r \sqsubseteq \rho_s\} \cup \\
& \quad \{\mathsf{C}(\ell_2) \subseteq \mathsf{C}(\ell)\} \\
[\textit{PE-Send}] & \ldots \\
[\textit{PE-Err}] & \ldots \\
[\textit{PE-Exercise}] & \ldots
\end{array}
$$

5.2 Constraint solving

5.3 Implementation-specific details

Chapter 6

Experiments

6.1 Findings

6.2 Performance

SLOW... Very SLOW!!!

Chapter 7

Conclusion

7.1 Conclusions

7.2 Future works (unbundling)

[3]

References

[1] Share me not extension
http://sharemenot.cs.washington.edu/, May 2014.

[2] Adam Barth, Adrienne Porter Felt, Prateek Saxena, and Aaron Boodman. Protecting browsers from extension vulnerabilities. Technical Report UCB/EECS-2009-185, EECS Department, University of California, Berkeley, Dec 2009.

[3] Hanne Riis Nielson and Flemming Nielson. Flow logic: A multi-paradigmatic approach to static analysis. In *The Essence of Computation*, pages 223–244, 2002.