

Privilege separation in browser architectures

Michele Bugliesi

Stefano Calzavara

Enrico Steffinlongo

May 20, 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

| | | |
|----------|--|-----------|
| 1 | Motivation | 5 |
| 1.1 | Privilege escalation attacks | 5 |
| 1.2 | Chrome extension architecture overview | 5 |
| 1.3 | Chrome extension architecture weaknesses | 5 |
| 1.4 | Proposal | 5 |
| 2 | Background | 7 |
| 2.1 | Chrome extension architecture details | 7 |
| 2.2 | Flow logic | 7 |
| 3 | Formalization | 9 |
| 3.1 | Calculus | 9 |
| 3.2 | Safety properties | 9 |
| 3.3 | Analysis specification | 9 |
| 3.3.1 | Abstract succinct | 9 |
| 3.3.2 | Compositional Verbose | 12 |
| 3.4 | Theorem | 14 |
| 3.5 | Requirements for correctness | 14 |
| 4 | Abstract Domains | 15 |
| 4.1 | Abstract domains choice | 15 |
| 4.2 | Abstract operations | 16 |
| 4.3 | Requirements verification | 16 |
| 5 | Implementation | 17 |
| 5.1 | Constraint generation | 17 |
| 5.2 | Constraint solving | 19 |
| 5.3 | Implementation-specific details | 19 |
| 6 | Experiments | 21 |
| 6.1 | Findings | 21 |
| 6.2 | Performance | 21 |
| 7 | Conclusion | 23 |
| 7.1 | Conclusions | 23 |
| 7.2 | Future works (unbundling) | 23 |

Chapter 1

Motivation

1.1 Privilege escalation attacks

1.2 Chrome extension architecture overview

1.3 Chrome extension architecture weaknesses

1.4 Proposal

Chapter 2

Background

2.1 Chrome extension architecture details

2.2 Flow logic

Chapter 3

Formalization

3.1 Calculus

3.2 Safety properties

3.3 Analysis specification

3.3.1 Abstract succinct

| | |
|--------------------------------------|--|
| <i>Abstract cache</i> | $\hat{C} : \mathcal{L} \rightarrow \hat{V}$ |
| <i>Abstract variable environment</i> | $\hat{\Gamma} : \mathcal{V} \rightarrow \hat{V}$ |
| <i>Abstract memory</i> | $\hat{\mu} : \mathcal{L} \times \mathcal{P} \rightarrow \hat{V}$ |
| <i>Abstract permission cache</i> | $\hat{P} : \mathcal{L} \rightarrow \mathcal{P}$ |

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

| | |
|-----------------|--|
| $[PE-SetField]$ | $(\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_0[e_1] = e_2 : \hat{v} \gg \rho$ iff $(\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_0 : \hat{v}_0 \gg \rho_0 \wedge$ $\rho_0 \sqsubseteq \rho \wedge$ $(\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_1 : \hat{v}_1 \gg \rho_1 \wedge$ $\rho_1 \sqsubseteq \rho \wedge$ $(\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_2 : \hat{v}_2 \gg \rho_2 \wedge$ $\rho_2 \sqsubseteq \rho \wedge$ $\widehat{set}(\hat{v}_0, \hat{v}_1, \hat{v}_2) \subseteq \hat{v}$ |
| $[PE-DelField]$ | $(\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} \mathbf{delete} e_1[e_2] : \hat{v} \gg \rho$ iff $(\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_1 : \hat{v}_1 \gg \rho_1 \wedge$ $\rho_1 \sqsubseteq \rho \wedge$ $(\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_2 : \hat{v}_2 \gg \rho_2 \wedge$ $\rho_2 \sqsubseteq \rho \wedge$ $\widehat{del}(\hat{v}_1, \hat{v}_2) \subseteq \hat{v}$ |
| $[PE-Ref]$ | $(\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} \mathbf{ref}_{r, \rho_r} e : \{r\} \gg \rho$ iff $(\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e : \hat{v} \gg \rho \wedge$ $\rho_r \sqsubseteq \rho_s \Rightarrow \hat{v} \subseteq \hat{\mu}(r, \rho_r)$ |
| $[PE-DeRef]$ | $(\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} \mathbf{deref} e : \hat{v} \gg \rho$ iff $(\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e : \hat{v}_1 \gg \rho_1 \wedge$ $\rho_1 \sqsubseteq \rho \wedge$ $\forall r \in \hat{v}_1 : \forall \rho_r \sqsubseteq \rho_s : \hat{\mu}(r, \rho_r) \subseteq \hat{v}$ |
| $[PE-SetRef]$ | $(\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_1 = e_2 : \hat{v} \gg \rho$ iff $(\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e : \hat{v}_1 \gg \rho_1 \wedge$ $\rho_1 \sqsubseteq \rho \wedge$ $(\hat{\Gamma}, \hat{\mu}) \models_{\rho_s} e_2 : \hat{v}_2 \gg \rho_2 \wedge$ $\rho_2 \sqsubseteq \rho \wedge$ $\forall r \in \hat{v}_1 : \forall \rho_r \sqsubseteq \rho_s :$ $\hat{v}_2 \subseteq \hat{\mu}(r, \rho_r) \wedge$ $\hat{v}_2 \subseteq \hat{v}$ |
| $[PE-Send]$ | ... |
| $[PE-Err]$ | ... |
| $[PE-Exercise]$ | ... |

3.3.2 Compositional Verbose

| | |
|-------------|--|
| [CV-Val] | $(\hat{C}, \hat{\Gamma}, \hat{\mu}, \hat{P}) \models_{c\rho_s} (c)^\ell$ iff $\{d_c\} \subseteq \hat{C}(\ell)$ |
| [CV-Var] | $(\hat{C}, \hat{\Gamma}, \hat{\mu}, \hat{P}) \models_{c\rho_s} (x)^\ell$ iff $\hat{\Gamma}(x) \subseteq \hat{C}(\ell)$ |
| [CV-Lambda] | $(\hat{C}, \hat{\Gamma}, \hat{\mu}, \hat{P}) \models_{c\rho_s} (\lambda x. e_0^{\ell_0})^\ell$ iff $\{\lambda x. e_0^{\ell_0}\} \subseteq \hat{C}(\ell) \wedge$ $(\hat{C}, \hat{\Gamma}, \hat{\mu}, \hat{P}) \models_{c\rho_s} e_0^{\ell_0}$ |
| [CV-Obj] | $(\hat{C}, \hat{\Gamma}, \hat{\mu}, \hat{P}) \models_{c\rho_s} (\overrightarrow{\{str_i : e_i^{\ell_i}\}})^\ell$ iff $\forall i :$ $(\hat{C}, \hat{\Gamma}, \hat{\mu}, \hat{P}) \models_{c\rho_s} e_i^{\ell_i} \wedge$ $\hat{P}(\ell_i) \sqsubseteq \hat{P}(\ell) \wedge$ $\overrightarrow{\{str_i : \hat{C}(\ell_i)\}} \subseteq \hat{C}(\ell)$ |
| [CV-Let] | $(\hat{C}, \hat{\Gamma}, \hat{\mu}, \hat{P}) \models_{c\rho_s} (\mathbf{let} \ x_i = e_i^{\ell_i} \ \mathbf{in} \ e'^{\ell'})^\ell$ iff $(\hat{C}, \hat{\Gamma}, \hat{\mu}, \hat{P}) \models_{c\rho_s} e'^{\ell'} \wedge$ $\hat{P}(\ell') \sqsubseteq \hat{P}(\ell) \wedge$ $\hat{C}(\ell') \subseteq \hat{C}(\ell) \wedge$ $\forall i :$ $(\hat{C}, \hat{\Gamma}, \hat{\mu}, \hat{P}) \models_{c\rho_s} e_i^{\ell_i} \wedge$ $\hat{C}(\ell_i) \subseteq \hat{\Gamma}(x_i) \wedge$ $\hat{P}(\ell_i) \sqsubseteq \hat{P}(\ell)$ |
| [CV-App] | $(\hat{C}, \hat{\Gamma}, \hat{\mu}, \hat{P}) \models_{c\rho_s} (e_1^{\ell_1} e_2^{\ell_2})^\ell$ iff $(\hat{C}, \hat{\Gamma}, \hat{\mu}, \hat{P}) \models_{c\rho_s} e_1^{\ell_1} \wedge (\hat{C}, \hat{\Gamma}, \hat{\mu}, \hat{P}) \models_{c\rho_s} e_2^{\ell_2} \wedge$ $\hat{P}(\ell_1) \sqsubseteq \hat{P}(\ell) \wedge \hat{P}(\ell_2) \sqsubseteq \hat{P}(\ell)$ $\forall (\lambda x. e_0^{\ell_0}) \in \hat{C}(\ell_1) :$ $\hat{C}(\ell_2) \subseteq \hat{\Gamma}(x) \wedge \hat{C}(\ell_0) \subseteq \hat{C}(\ell) \wedge$ $\hat{P}(\ell_0) \sqsubseteq \hat{P}(\ell)$ |
| [CV-Op] | $(\hat{C}, \hat{\Gamma}, \hat{\mu}, \hat{P}) \models_{c\rho_s} (op(\overrightarrow{e_i^{\ell_i}}))^\ell$ iff $\forall i :$ $(\hat{C}, \hat{\Gamma}, \hat{\mu}, \hat{P}) \models_{c\rho_s} e_i^{\ell_i} \wedge$ $\hat{P}(\ell_i) \sqsubseteq \hat{P}(\ell) \wedge$ $\widehat{op}(\hat{C}(\ell_i)) \subseteq \hat{C}(\ell)$ |
| [CV-Cond] | $(\hat{C}, \hat{\Gamma}, \hat{\mu}, \hat{P}) \models_{c\rho_s} (\mathbf{if} \ (e_0^{\ell_0}) \ \{ e_1^{\ell_1} \} \ \mathbf{else} \ \{ e_2^{\ell_2} \})^\ell$ iff $(\hat{C}, \hat{\Gamma}, \hat{\mu}, \hat{P}) \models_{c\rho_s} e_0^{\ell_0} \wedge$ $\hat{P}(\ell_0) \sqsubseteq \hat{P}(\ell) \wedge$ $\widehat{\mathbf{true}} \in \hat{C}(\ell_0) \Rightarrow$ $(\hat{C}, \hat{\Gamma}, \hat{\mu}, \hat{P}) \models_{c\rho_s} e_1^{\ell_1} \wedge \hat{C}(\ell_1) \subseteq \hat{C}(\ell) \wedge$ $\hat{P}(\ell_1) \sqsubseteq \hat{P}(\ell) \wedge$ $\widehat{\mathbf{false}} \in \hat{C}(\ell_0) \Rightarrow$ $(\hat{C}, \hat{\Gamma}, \hat{\mu}, \hat{P}) \models_{c\rho_s} e_2^{\ell_2} \wedge \hat{C}(\ell_2) \subseteq \hat{C}(\ell) \wedge$ $\hat{P}(\ell_2) \sqsubseteq \hat{P}(\ell)$ |
| [CV-While] | $(\hat{C}, \hat{\Gamma}, \hat{\mu}, \hat{P}) \models_{c\rho_s} (\mathbf{while} \ (e_1^{\ell_1}) \ \{ e_2^{\ell_2} \})^\ell$ iff $(\hat{C}, \hat{\Gamma}, \hat{\mu}, \hat{P}) \models_{c\rho_s} e_1^{\ell_1} \wedge$ $\hat{P}(\ell_1) \sqsubseteq \hat{P}(\ell) \wedge$ $\widehat{\mathbf{true}} \in \hat{C}(\ell_1) \Rightarrow$ 12 $(\hat{C}, \hat{\Gamma}, \hat{\mu}, \hat{P}) \models_{c\rho_s} e_2^{\ell_2} \wedge \hat{C}(\ell_2) \subseteq \hat{C}(\ell) \wedge$ $\hat{P}(\ell_2) \sqsubseteq \hat{P}(\ell) \wedge$ $\widehat{\mathbf{false}} \in \hat{C}(\ell_1) \Rightarrow \widehat{\mathbf{undefined}} \subseteq \hat{C}(\ell)$ |

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

3.4 Theorem

3.5 Requirements for correctness

Chapter 4

Abstract Domains

4.1 Abstract domains choice

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

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 *

$$\widehat{v} \sqsubseteq \widehat{v'} \text{ iff } \forall \widehat{u_i} \in \widehat{v}, \exists \widehat{u_j} \in \widehat{v'} : \widehat{u_i} \sqsubseteq \widehat{u_j}.$$

If Galois connection then

$$\widehat{v} \sqsubseteq \widehat{v'} \text{ iff } \gamma(\widehat{v}) \subseteq \gamma(\widehat{v'})$$

where $\gamma : \widehat{V} \rightarrow P(V)$ is the concretisation function.

$$\gamma_p : \widehat{PV} \rightarrow P(V)$$

$$\gamma(\widehat{v}) = \bigcup_{\widehat{u_i} \in \widehat{v}} \gamma_p(\widehat{u_i})$$

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

$$\widehat{u_{bool}} = \{\widehat{pre_{bool}}\}$$

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

$$\widehat{u_{int}} = \{\widehat{pre_{int}}\}$$

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

$$\widehat{u_{string}} = \{\widehat{pre_{string}}\}$$

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

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

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

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

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

$$\widehat{u_{rec}} = \widehat{pre_{rec}}$$

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

with $\sqsubseteq = \sqsubseteq$

with $\sqsubseteq = \sqsubseteq$

with $\sqsubseteq = \sqsubseteq$

— Giulia's spec. is more tricky than \sqsubseteq

with $\sqsubseteq = \sqsubseteq$

with $\sqsubseteq = \sqsubseteq$

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

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 .

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

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

Constraint form.

$$\begin{array}{lll} \text{Term inclusion} & \{\hat{v}\} & \subseteq E \\ \text{Element inclusion} & E & \subseteq E \\ \text{Permission inclusion} & \mathbf{P}(\ell) & \sqsubseteq \mathbf{P}(\ell') \\ \text{Operation} & \widehat{Op}(\vec{E}_i) & \subseteq E \\ \text{Implication} & \{\hat{v}\} \subseteq E & \Rightarrow E \subseteq E \end{array}$$

Misc:

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

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

| | |
|-----------------|--|
| $[CG-GetField]$ | $\begin{aligned} \mathcal{C}_{*\rho_s} \llbracket (e_1^{\ell_1} [e_2^{\ell_2}])^\ell \rrbracket = & \\ & \mathcal{C}_{*\rho_s} \llbracket (e_1^{\ell_1}) \rrbracket \cup \mathcal{C}_{*\rho_s} \llbracket (e_2^{\ell_2}) \rrbracket \cup \\ & \{P(\ell_1) \sqsubseteq P(\ell)\} \cup \\ & \{P(\ell_2) \sqsubseteq P(\ell)\} \cup \\ & \widehat{get}(C(\ell_1), C(\ell_2)) \subseteq C(\ell) \end{aligned}$ |
| $[CG-SetField]$ | $\begin{aligned} \mathcal{C}_{*\rho_s} \llbracket (e_0^{\ell_0} [e_1^{\ell_1}] = e_2^{\ell_2}) \rrbracket = & \\ & \mathcal{C}_{*\rho_s} \llbracket (e_0^{\ell_0}) \rrbracket \cup \mathcal{C}_{*\rho_s} \llbracket (e_1^{\ell_1})^\ell \rrbracket \cup \mathcal{C}_{*\rho_s} \llbracket (e_2^{\ell_2}) \rrbracket \cup \\ & \{P(\ell_1) \sqsubseteq P(\ell)\} \cup \\ & \{P(\ell_2) \sqsubseteq P(\ell)\} \cup \\ & \{P(\ell_3) \sqsubseteq P(\ell)\} \cup \\ & \widehat{set}(C(\ell_1), C(\ell_2), C(\ell_2)) \subseteq C(\ell) \end{aligned}$ |
| $[CG-DelField]$ | $\begin{aligned} \mathcal{C}_{*\rho_s} \llbracket (\text{delete } e_1^{\ell_1} [e_2^{\ell_2}])^\ell \rrbracket = & \\ & \mathcal{C}_{*\rho_s} \llbracket (e_1^{\ell_1}) \rrbracket \cup \mathcal{C}_{*\rho_s} \llbracket (e_2^{\ell_2}) \rrbracket \cup \\ & \{P(\ell_1) \sqsubseteq P(\ell)\} \cup \\ & \{P(\ell_2) \sqsubseteq P(\ell)\} \cup \\ & \widehat{del}(C(\ell_1), C(\ell_2)) \subseteq C(\ell) \end{aligned}$ |
| $[CG-Ref]$ | $\begin{aligned} \mathcal{C}_{*\rho_s} \llbracket (\text{ref}_{r, \rho_r} e_1^{\ell_1})^\ell \rrbracket = & \\ & \mathcal{C}_{*\rho_s} \llbracket (e_1^{\ell_1}) \rrbracket \cup \\ & \{\{r\} \subseteq C(\ell)\} \cup \\ & \{P(\ell_1) \sqsubseteq P(\ell)\} \cup \\ & \{\rho_r \sqsubseteq \rho_s \Rightarrow C(\ell_1) \subseteq M(r, \rho_r)\} \end{aligned}$ |
| $[CG-DeRef]$ | $\begin{aligned} \mathcal{C}_{*\rho_s} \llbracket (\text{deref } e_1^{\ell_1})^\ell \rrbracket = & \\ & \mathcal{C}_{*\rho_s} \llbracket (e_1^{\ell_1}) \rrbracket \cup \\ & \{P(\ell_1) \sqsubseteq P(\ell)\} \cup \\ & \{r \in C(\ell_1) \Rightarrow M(r, \rho_r) \subseteq C(\ell) \\ & \quad r \in r_*, \rho_r \sqsubseteq \rho_s\} \end{aligned}$ |
| $[CG-SetRef]$ | $\begin{aligned} \mathcal{C}_{*\rho_s} \llbracket (e_1^{\ell_1} = e_2^{\ell_2})^\ell \rrbracket = & \\ & \mathcal{C}_{*\rho_s} \llbracket (e_1^{\ell_1}) \rrbracket \cup \mathcal{C}_{*\rho_s} \llbracket (e_2^{\ell_2}) \rrbracket \cup \\ & \{P(\ell_1) \sqsubseteq P(\ell)\} \cup \\ & \{P(\ell_2) \sqsubseteq P(\ell)\} \cup \\ & \{r \in C(\ell_1) \Rightarrow C(\ell_2) \subseteq M(r, \rho_r) \\ & \quad r \in r_*, \rho_r \sqsubseteq \rho_s\} \cup \\ & \{C(\ell_2) \subseteq C(\ell)\} \end{aligned}$ |
| $[PE-Send]$ | ... |
| $[PE-Err]$ | ... |
| $[PE-Exercise]$ | ... |

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)

[] [?]