

Access Permission Contracts for Scripting Languages

POPL 2012

Albert-Ludwigs-Universität Freiburg

Phillip Heidegger, Annette Bieniusa, Peter Thiemann

Institut für Informatik
Georges-Köhler-Allee 079
79110 Freiburg

heidegger@informatik.uni-freiburg.de

25. January 2012



UNI
FREIBURG

Motivation



Situation of a Webpage Programmer



The screenshot shows a web browser window displaying the Spiegel Online website. The page features a navigation bar with various menu items and a search bar. The main content area is dominated by an article titled "Protest gegen US-Internetsperren" with the sub-headline "Blackout für die Netzfreiheit". Below the article title, there is a large advertisement for WordPress.com, which is heavily censored with black boxes and the word "CENSORED". The advertisement text includes "A better way to blog." and "Get started here". Below the advertisement, there is a paragraph of text discussing the impact of US internet control laws on Wikipedia and other websites. A video player is visible at the bottom right of the page, showing a person holding a sign that says "FOR SALE".

SPiegel ONLINE – Nachrichten

www.spiegel.de

Mein Zeug. Meine Cloud.

My Book* Live™

WD

MEHR INFOS

Mittwoch, 18. Januar 2012

Schlagzeilen | Hilfe | RSS | Newsletter | Mobil | Wetter | TV-Programm

SPiegel ONLINE

NACHRICHTEN VIDEO THEMEN FORUM ENGLISH DER SPIEGEL SPIEGEL TV ABO SHOP

Politik Wirtschaft Panorama Sport Kultur Netzwelt Wissenschaft einestages Karriere Uki Schule Reise Auto

Top-Themen: Costa Concordia | Euro-Krise | Internetsperren | Handball-EM

Login | Registrierung

Protest gegen US-Internetsperren
Blackout für die Netzfreiheit

WORDPRESS.COM

Language: English

A better way to blog.

Get started here

Learn more or sign up now.

CENSORED

CENSORED

CENSORED

CENSORED

CENSORED

CENSORED

Fotos ▶

Das Web trägt Schwarz: Auf Dutzenden Websites hat der Protest gegen geplante US-Gesetze zur Kontrolle des Internets begonnen. Wikipedia streikt, Google verlinkt auf eine Protest-Petition, Wordpress ist gepflastert mit Zensurschildern. Die Internetgemeinde fürchtet Gängelung und Netzsperrn. mehr... [Forum]

- Weltweite Internetgesetze: US-Konzerne lassen das Netz zensieren
- Umstrittenes US-Internetgesetz: Wikipedia schaltet ab - aus Protest

Milliardenloch

Commerzbank braucht noch mehr Kapital

VIDEO ▶▶

Video ▶

Situation of a Webpage Programmer



The screenshot shows a web browser window displaying the Spiegel Online website. The page features a navigation bar with various menu items and a search bar. The main content area is dominated by a large article titled "Protest gegen US-Internetsperren" with the sub-headline "Blackout für die Netzfreiheit". The article's body text is heavily redacted with black boxes, and several instances of the word "CENSORED" are visible. A small video player is embedded at the bottom of the article, showing a person in a Guy Fawkes mask. To the right of the article is a vertical sidebar with a portrait of a woman and a "WD" logo. The browser's address bar shows "www.spiegel.de".

SPiegel ONLINE – Nachrichten
www.spiegel.de

Mein Zeug. Meine Cloud.
My Book* Live™

Mittwoch, 18. Januar 2012
Schlagzeilen | Hilfe | RSS | Newsletter | Mobil | Wetter | TV-Programm

SPiegel ONLINE

NACHRICHTEN VIDEO THEMEN FORUM ENGLISH DER SPIEGEL SPIEGEL TV ABO SHOP

Politik Wirtschaft Panorama Sport Kultur Netzwelt Wissenschaft einestages Karriere Uki Schule Reise Auto

Top-Themen: Costa Concordia | Euro-Krise | Internetsperren | Handball-EM

Protest gegen US-Internetsperren
Blackout für die Netzfreiheit

WORDPRESS.COM
A better way to blog.
Get started here
Learn more or sign up now

Fotos ▶

Das Web trägt Schwarz: Auf Dutzenden Websites hat der Protest gegen geplante US-Gesetze zur Kontrolle des Internets begonnen. Wikipedia streikt, Google verlinkt auf eine Protest-Petition, Wordpress ist gepflastert mit Zensurschildern. Die Internetgemeinde fürchtet Gängelung und Netzsperren. mehr... [Forum]

- Weltweite Internetgesetze: US-Konzerne lassen das Netz zensieren
- Umstrittenes US-Internetgesetz: Wikipedia schaltet ab - aus Protest

Milliardenloch
Commerzbank braucht noch mehr Kapital

VIDEO ▶

Mein Zeug. Meine Cloud.
My Book* Live™

WD
MEHR INFOS

Situation of a Webpage Programmer



The screenshot shows a web browser window displaying the Spiegel Online news website. The page features a red header with the site's logo and navigation links. The main content area is titled "Protest gegen US-Internetsperren" and "Blackout für die Netzfreiheit". It includes a WordPress.com advertisement with a "A better way to blog." message and a grid of censored images. Below the ad, there is a text block about the US internet control bill and a video player showing a person in a Guy Fawkes mask.

Mein Zeug. Meine Cloud.

My Book* User*

WD

Meine Cloud.

Mitwoch, 18. Januar 2012

Schlagzeilen | Hilfe | RSS | Newsletter | Mobil | Wetter | TV-Programm

SPIEGEL ONLINE

NACHRICHTEN VIDEO THEMEN FORUM ENGLISH DER SPIEGEL SPIEGEL TV ABO SHOP

Politik Wirtschaft Panorama Sport Kultur Netzwelt Wissenschaft einestages Karriere Uki Schule Reise Auto

Top-Themen: Costa Concordia | Euro-Krise | Internetsperren | Handball-EM

Login | Registrierung

Protest gegen US-Internetsperren
Blackout für die Netzfreiheit

WordPress.com

A better way to blog.

Get started here

Learn more or sign up now.

CENSORED

CENSORED

CENSORED

CENSORED

CENSORED

CENSORED

Fotos ▶

Das Web trägt Schwarz: Auf Dutzenden Websites hat der Protest gegen geplante US-Gesetze zur Kontrolle des Internets begonnen. Wikipedia streikt, Google verlinkt auf eine Protest-Petition, Wordpress ist gepflastert mit Zensurschildern. Die Internetgemeinde fürchtet Gängelung und Netzsperrern. mehr... [Forum]

- Weltweite Internetgesetze: US-Konzerne lassen das Netz zensurieren
- Umstrittenes US-Internetgesetz: Wikipedia schaltet ab - aus Protest

Milliardenloch

Commerzbank braucht noch mehr Kapital

VIDEO ▶

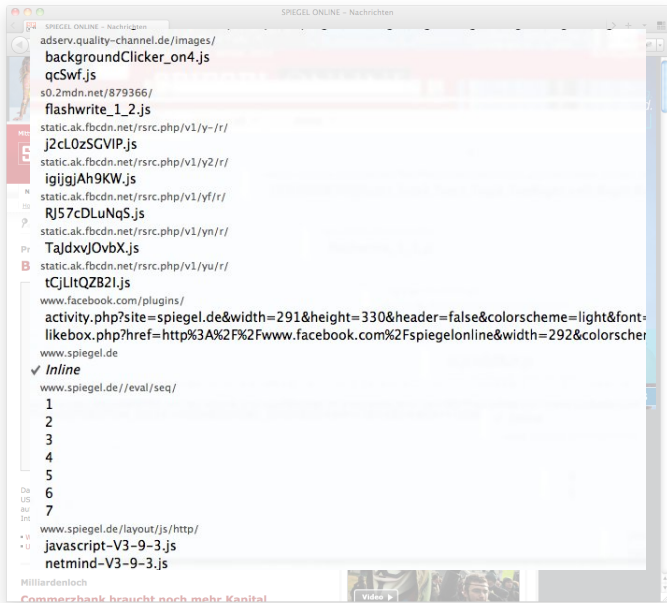
Video ▶

Situation of a Webpage Programmer



The screenshot shows a web browser window displaying the Spiegel Online news website. The page features a red header with the site's name and a search bar. Below the header, there are navigation links for various sections like 'NACHRICHTEN', 'VIDEO', and 'THEMEN'. The main content area displays an article titled 'Protest gegen US-Internetsperren' with a sub-headline 'Blackout für die Netzfreiheit'. The article text is partially obscured by black redaction boxes, with the word 'CENSORED' appearing in several places. A video player is visible at the bottom of the article, showing a person in a Guy Fawkes mask. To the right of the article, there is a vertical advertisement for WD My Book Live, featuring a woman's face and the WD logo. The browser's address bar shows 'www.spiegel.de'.

Situation of a Webpage Programmer



Situation of a Webpage Programmer



The screenshot shows the Spiegel Online website interface. At the top, there's a navigation bar with 'SPIEGEL ONLINE - Nachrichten' and a search bar. Below that, a red banner reads 'Protest gegen US-Internetsperren' and 'Blackout für die Netzfreiheit'. The main content area features a WordPress.com advertisement with several grey boxes labeled 'CENSORED' covering the text. A blue box highlights the text '... global = ... ; ...'. To the right, there's a sidebar with a 'Meine Cloud.' advertisement and a 'WD' logo. At the bottom, there's a 'VIDEO' section with a thumbnail of a person holding a 'PEACE' sign.

... global = ... ; ...

Situation of a Webpage Programmer



... global = ... ; ...

... global = ... ; ...

Protest gegen US-Internetsperren
Blackout für die Netzfreiheit

WORDPRESS.COM
A better way to blog.
Get started here
Learn more or sign up now.

Fotos ▶

Das Web trägt Schwarz: Auf Dutzenden Websites hat der Protest gegen geplante US-Gesetze zur Kontrolle des Internets begonnen. Wikipedia streikt, Google verlinkt auf eine Protest-Petition, Wordpress ist geflösst mit Zensurschildern. Die Internetgemeinde fürchtet Gängelung und Netzsperrn. mehr... | Forum |

- Weltweite Internetgesetze: US-Konzerne lassen das Netz zensieren
- Umstrittenes US-Internetgesetz: Wikipedia schaltet ab - aus Protest

Milliardenloch
Commerzbank braucht noch mehr Kapital

VIDEO ▶

Problem

- Uncontrolled side effects may cause unexpected behavior
- Code is aggregated by dynamic loading

Maintenance is a nightmare!

Problem

- Uncontrolled side effects may cause unexpected behavior
- Code is aggregated by dynamic loading

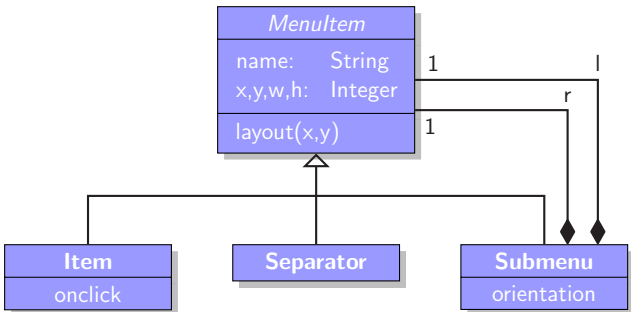
Maintenance is a nightmare!

What can we do?

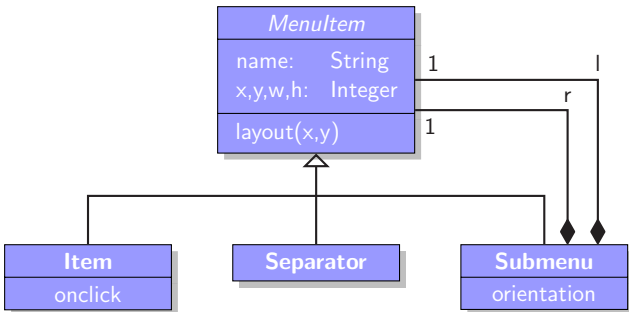
- static approach?
- documentation?
- monitoring!

Overview

- Type contracts
 - describe the *functional behavior* of an operation
- Access permission contracts
 - describe the *side effect* of an operation

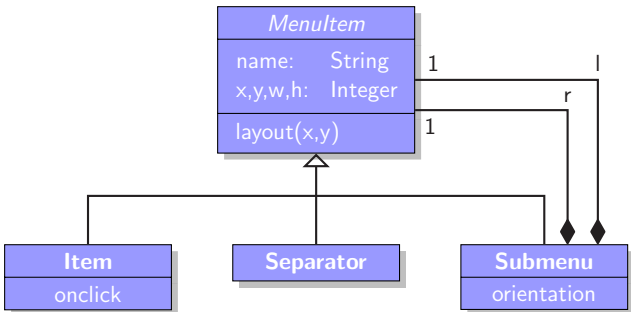


```
/*c (int, int) -> {w:int,h:int}      ← type signature  
  with [this./l|r/*./x|y|w|h/] ← access permission  
*/  
function layout(x,y) { ... }
```



```

/*c (int, int) -> {w:int,h:int}      ← type signature
   with [this./l|r/*./x|y|w|h/] ← access permission
*/
function layout(x,y) { ... }
    
```



```
/*c (int, int) -> {w:int,h:int}      ← type signature  
  with [this./l|r/*./x|y|w|h/] ← access permission  
*/  
function layout(x,y) { ... }
```

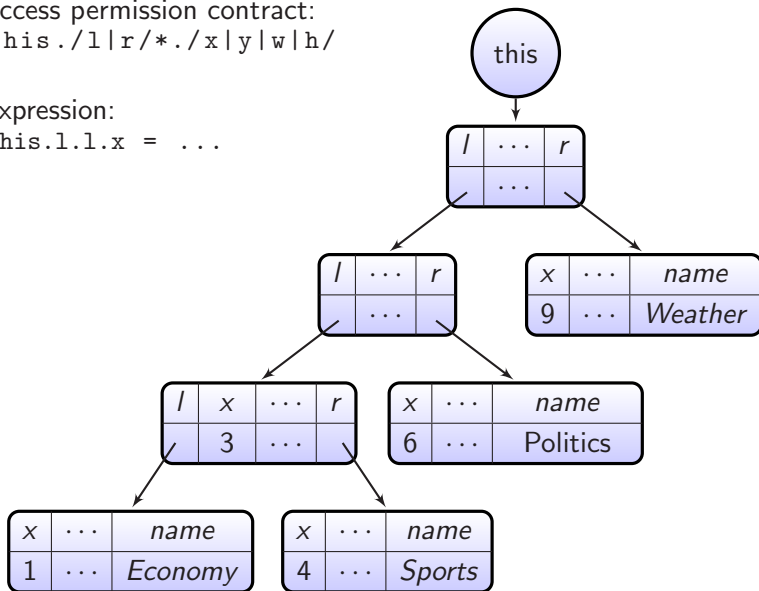
Example – Menu

access permission contract:

`this./l|r/*./x|y|w|h/`

expression:

`this.l.l.x = ...`



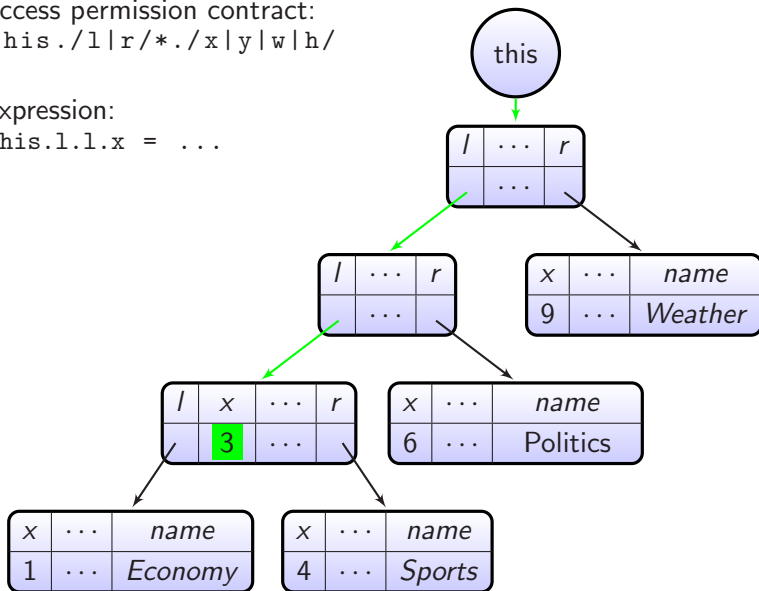
Example – Menu

access permission contract:

`this./l|r/*./x|y|w|h/`

expression:

`this.l.l.x = ...`



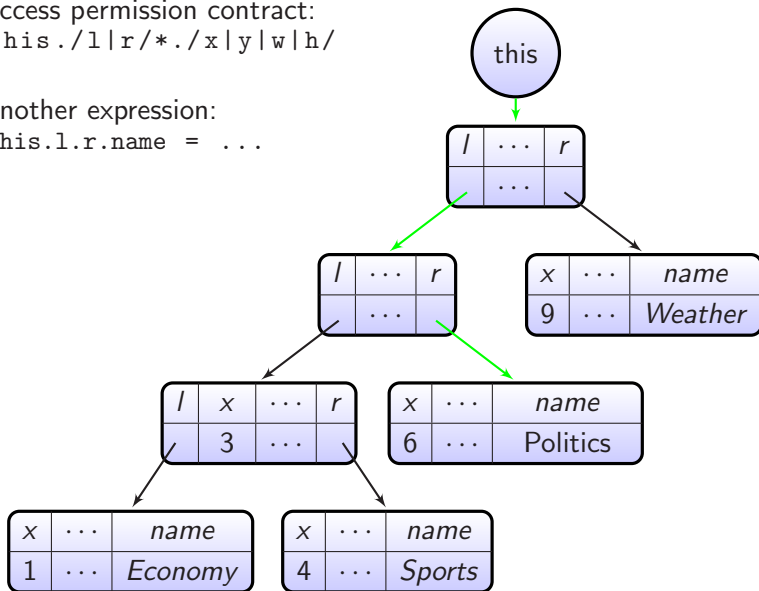
Example – Menu

access permission contract:

`this./l|r/*./x|y|w|h/`

another expression:

`this.l.r.name = ...`



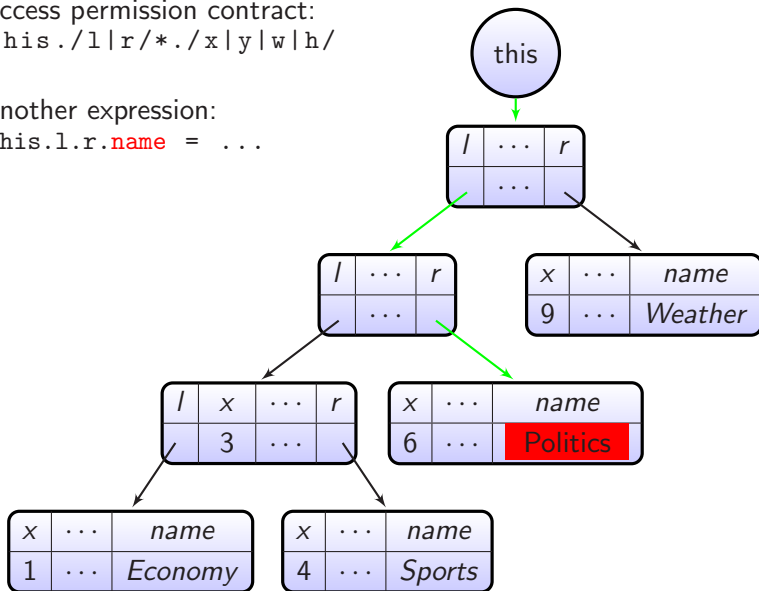
Example – Menu

access permission contract:

`this./l|r/*./x|y|w|h/`

another expression:

`this.l.r.name = ...`





Is the meaning of an
access permission settled?

Is the meaning of an
access permission settled?

NO!

There are three open issues...

Syntactic Interpretation – Example



```
/*c (obj,obj) → any with [x.a, y.a, y.a.b] */  
function b(x,y) {  
  ...  
  ... y.a.b ... // violation?  
  ...  
}
```



```
/*c (obj,obj) → any with [x.a, y.a, y.a.b] */  
function b(x,y) {  
  var tmp = y.a;  
  y.a = x.a;  
  y.a.b = 42; // violation?  
  y.a = tmp;  
}
```

Syntactic Interpretation – Example

```
/*c (obj,obj) → any with [x.a, y.a, y.a.b] */  
function b(x,y) {  
  var tmp = y.a;  
  y.a = x.a;  
  y.a.b = 42; // violation? YES, please!!  
  y.a = tmp;  
}
```

From the view of the caller

- The function modifies **x.a.b**.
- By introducing local aliases, a function may execute side effects that are not allowed



~~Syntactic Interpretation~~

An access permission contract is interpreted syntactically.

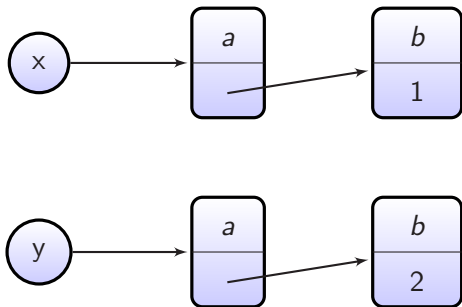
Pre-State Snapshot

An access permission contract is interpreted with respect to the heap at the time the contract is installed.

Pre-State Snapshot – Example

```

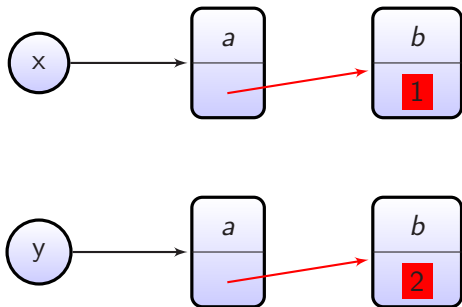
/*c (obj,obj) → any with [x.a , y.a , y.a.b ] */
function b(x,y) {
  y.a = x.a;
  y.a.b = 42; // violation?
}
  
```



Pre-State Snapshot – Example

```

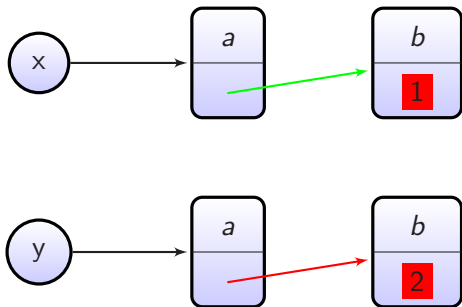
/*c (obj,obj) → any with [x.a , y.a , y.a.b ] */
function b(x,y) {
    y.a = x.a;
    y.a.b = 42; // violation?
}
    
```



Pre-State Snapshot – Example

```

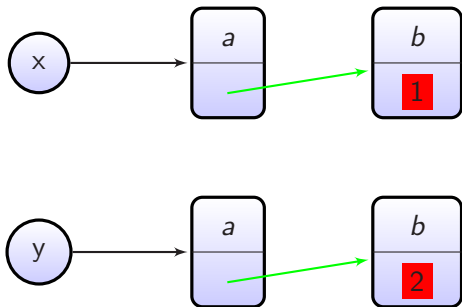
/*c (obj,obj) → any with [x.a , y.a , y.a.b ] */
function b(x,y) {
    y.a = x.a;
    y.a.b = 42; // violation?
}
    
```



Pre-State Snapshot – Example

```

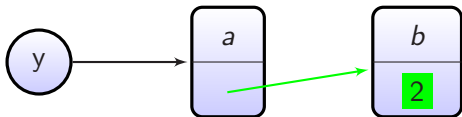
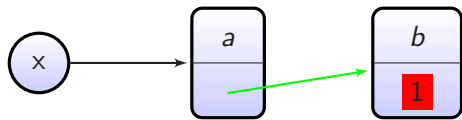
/*c (obj,obj) → any with [x.a , y.a , y.a.b ] */
function b(x,y) {
    y.a = x.a;
    y.a.b = 42; // violation?
}
    
```



Pre-State Snapshot – Example

```

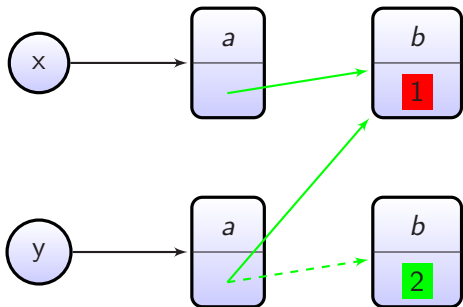
/*c (obj,obj) → any with [x.a , y.a , y.a.b ] */
function b(x,y) {
  →   y.a = x.a;
      y.a.b = 42; // violation?
}
    
```



Pre-State Snapshot – Example

```

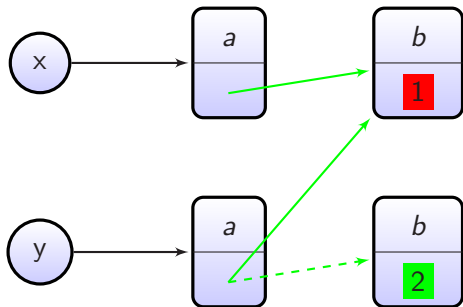
/*c (obj,obj) → any with [x.a , y.a , y.a.b ] */
function b(x,y) {
    y.a = x.a;
    → y.a.b = 42; // violation?
}
    
```



Pre-State Snapshot – Example

```

/*c (obj,obj) → any with [x.a , y.a , y.a.b ] */
function b(x,y) {
    y.a = x.a;
    y.a.b = 42; // violation? YES
}
    
```





- Pre-State Snapshot
- ...



Example – Dynamic Extent vs. Static Extent

```
/*c (obj) → any with [x.a] */  
function d1(x) {  
  x.a = 1;    // violation if called from d2?  
}  
  
/*c (obj) → any with [] */  
function d2(x) {  
  return d1(x);  
}
```

Dynamic Extent

An access permission for a function is in force for the duration of the function activation.

~~Static Extent~~

An access permission for a function is in force in its function body.

- Pre-State Snapshot
- Dynamic Extent
- ...



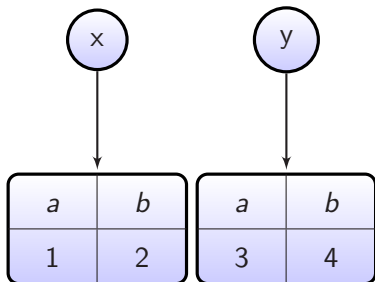
Location Based Interpretation – Example

```
/*c (obj,obj) → any with [ x.b, y.a ] */  
function h(x,y) {  
  y.a = 1;  
  y.b = 2; // violation?  
}
```

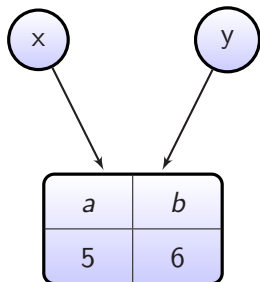
Location Based Interpretation – Example

```

/*c (obj,obj) → any with [ x.b, y.a ] */
function h(x,y) {
  y.a = 1;
  y.b = 2;  // violation?
}
    
```



```
h({a:1,b:2},{a:3,b:4});
```

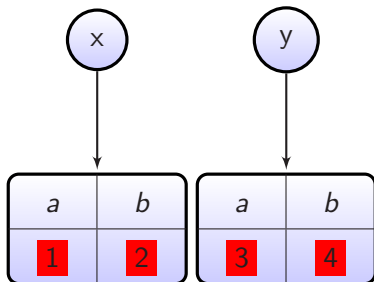


```
var o = {a:5,b:6};
h(o,o);
```

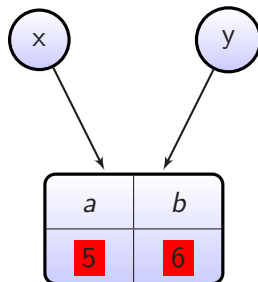
Location Based Interpretation – Example

```

/*c (obj,obj) → any with [ x.b, y.a ] */
function h(x,y) {
  y.a = 1;
  y.b = 2;  // violation?
}
    
```



```
h({a:1,b:2},{a:3,b:4});
```

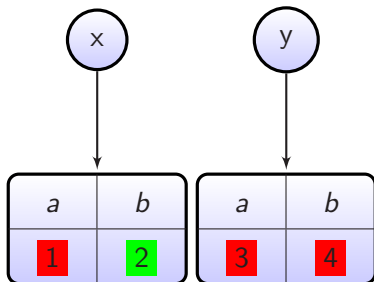


```
var o = {a:5,b:6};
h(o,o);
```

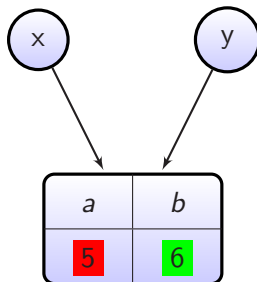
Location Based Interpretation – Example

```

/*c (obj,obj) → any with [ x.b, y.a ] */
function h(x,y) {
  y.a = 1;
  y.b = 2;  // violation?
}
    
```



```
h({a:1,b:2},{a:3,b:4});
```

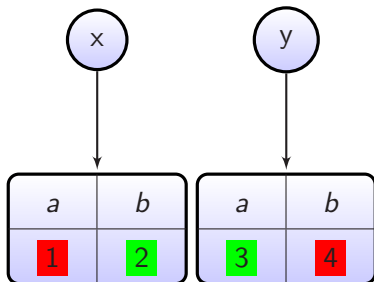


```
var o = {a:5,b:6};
h(o,o);
```

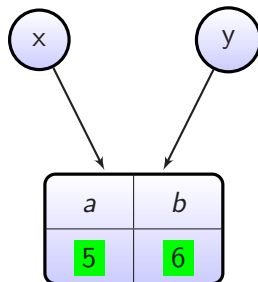

Location Based Interpretation – Example

```

/*c (obj,obj) → any with [ x.b, y.a ] */
function h(x,y) {
  y.a = 1;
  y.b = 2;  // violation?
}
    
```



```
h({a:1,b:2},{a:3,b:4});
```

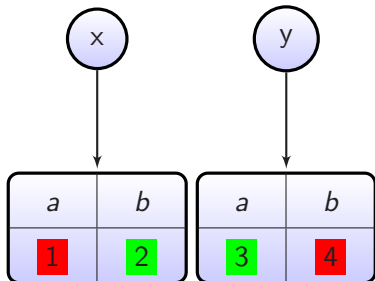


```
var o = {a:5,b:6};
h(o,o);
```

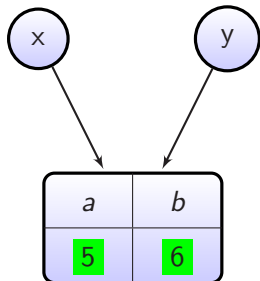
Location Based Interpretation – Example

```

/*c (obj,obj) → any with [ x.b, y.a ] */
function h(x,y) {
  y.a = 1;
  y.b = 2;  // violation? left: YES, right: NO
}
    
```



```
h({a:1,b:2},{a:3,b:4});
```



```
var o = {a:5,b:6};
h(o,o);
```



Conclusion

Violation occurs depending on the aliases of the parameters

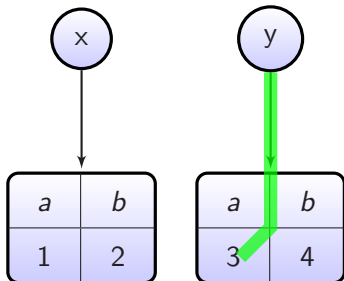
Requirement

We are looking for a property that holds for all executions of the function.

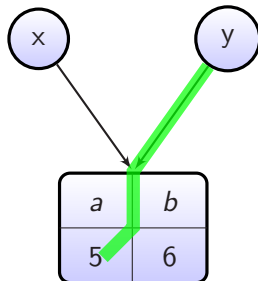
Path-Based Interpretation

```

/*c (obj,obj) → any with [ x.b , y.a ] */
function h(x,y) {
  y.a = 1; // (a)
  y.b = 2; // (b), violation?
}
    
```



```
h({a:1,b:2},{a:3,b:4});
```

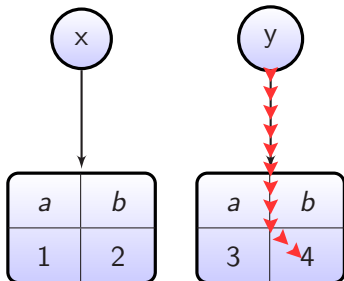


```
var o = {a:5,b:6};
h(o,o);
```

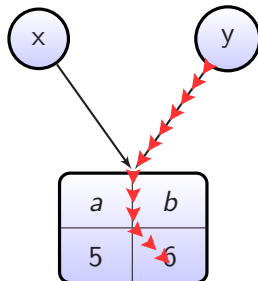
Path-Based Interpretation

```

/*c (obj,obj) → any with [ x.b , y.a ] */
function h(x,y) {
  y.a = 1; // (a)
  y.b = 2; // (b), violation?
}
    
```



```
h({a:1,b:2},{a:3,b:4});
```

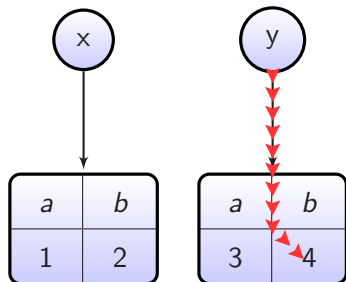


```
var o = {a:5,b:6};
h(o,o);
```

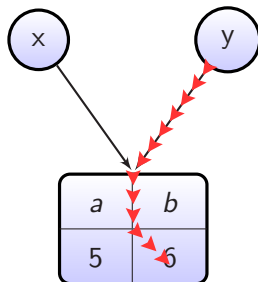
Path-Based Interpretation



```
/*c (obj,obj) → any with [ x.b , y.a ] */  
function h(x,y) {  
  y.a = 1; // (a)  
  y.b = 2; // (b), violation? YES!  
}
```



`h({a:1,b:2},{a:3,b:4});`



`var o = {a:5,b:6};
h(o,o);`

- Pre-State Snapshot
- Dynamic Extent
- Path-Based

Core Calculus

- lambda calculus with objects (big step semantics)
- expression to install access permissions:
`permit x : Lr, Lw in e`
- marking is done lazy

Theorem: Pre-State Snapshot Consistency

The access paths are interpreted with respect to the heap at installation time of the access permission.

Theorem: Stability of Violation

Introducing new aliases either yields the same access contract violations or yields an inconsistent read after write operation.



Prototype Implementation

- offline source-to-source transformation
- library to monitor property reads/writes

Mutation Testing

Software	types	types + access perm.	increase
	in (%)	in (%)	in (%)
Singly-Linked List	82.0	87.3	6.4
Richards (V8)	61.1	69.2	13.3
Delta-blue (V8)	75.6	87.2	15.3

Mutation Testing

Software	types in (%)	types + access perm. in (%)	increase in (%)
Singly-Linked List	82.0	87.3	6.4
Richards (V8)	61.1	69.2	13.3
Delta-blue (V8)	75.6	87.2	15.3

How do we create the access contracts?

We have an inference for them: P. Heidegger, P. Thiemann. A Heuristic Approach for Computing Effects. TOOLS 2011.



- A. Greenhouse and J. Boyland. An object-oriented effect system. ECOOP 1999.
- J. Smans, B. Jacobs, and F. Piessens. Implicit dynamic frames: Combining dynamic frames and separation logic. ECOOP 2009.
- H. Lehner and P. Müller. Efficient runtime assertion checking of assignable clauses with datagroups. FASE 2010.

Access permission contracts

- describe side effects of operations
- are formalized, provably sound and stable
- simplify software development and maintenance
- fix some design flaws of JavaScript

More about JSConTest (implementation, tools, technical report, case studies):

<http://proglang.informatik.uni-freiburg.de/jscontest/>

Thank You



UNI
FREIBURG

Thank you for
your attention!



More Complicated Example

```
/*c list.(top) → undf           ← type signature
   with [this._head, this._length, ← access
         this._head.next*.next    permission
       ] */
function add(data) {
  var node = {data: data, next: null}, current;
  if (this._head === null) {
    this._head = node;
  } else {
    current = this._head;
    while (current.next) {
      current = current.next;
    }
    current.next = node;
  }
  this._length++;
}
```


Example

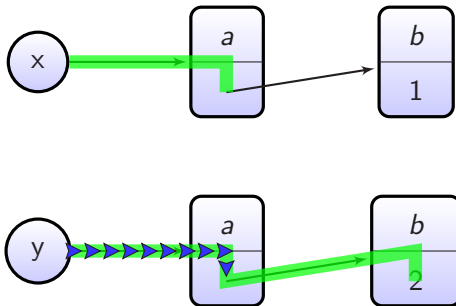


```
/*c (obj,obj) → any with [x.b,y.a] */  
function h(x,y) {  
  y.a = 1;  
  y.b = 2; // violation?  
}
```

Path-Based Interpretation – Example

```

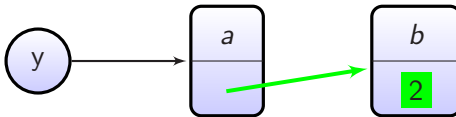
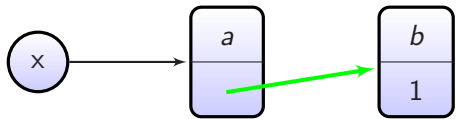
/*c (obj,obj) → any with [x.a, y.a, y.a.b] */
function b(x,y) {
  y.a = x.a;
  y.a.b = 42; // violation?
}
  
```



Path-Based Interpretation – Example

```

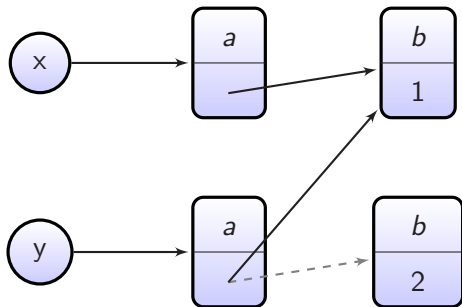
/*c (obj,obj) → any with [x.a, y.a, y.a.b] */
function b(x,y) {
  y.a = x.a;
  y.a.b = 42; // violation?
}
  
```



Path-Based Interpretation – Example

```

/*c (obj,obj) → any with [x.a, y.a, y.a.b] */
function b(x,y) {
  y.a = x.a;
  y.a.b = 42; // violation?
}
    
```



Path-Based Interpretation – Example

```

/*c (obj,obj) → any with [x.a, y.a, y.a.b] */
function b(x,y) {
  y.a = x.a;
  y.a.b = 42; // violation?
}
    
```

