Information Flow Analysis for a Dynamically Typed Functional Language with Staged Metaprogramming

Martin Lester\textsuperscript{1}  Luke Ong\textsuperscript{1}  Max Schäefer\textsuperscript{2}

\textsuperscript{1}Department of Computer Science, University of Oxford
\textsuperscript{2}IBM T.J. Watson Research Center

LOng Lunch Seminar, 2012–10–30
Information Flow Analysis for JavaScript

Martin Lester\textsuperscript{1}  Luke Ong\textsuperscript{1}  Max Schäefer\textsuperscript{2}

\textsuperscript{1}Department of Computer Science, University of Oxford
\textsuperscript{2}IBM T.J. Watson Research Center

LOng Lunch Seminar, 2012–10–30
Motivation

Web applications written in JavaScript regularly handle sensitive data.

- Reasoning about their security properties is an important problem.
- JavaScript is a difficult language to reason about.

Why is JavaScript difficult?

- Poorly understood, quaint semantics.
- Many features: mutable state, exceptions, dynamic types, prototype-based inheritance, type coercion, first-class functions . . .
Web applications written in JavaScript regularly handle sensitive data.

- Reasoning about their security properties is an important problem.
- JavaScript is a difficult language to reason about.

Why is JavaScript difficult?

- Poorly understood, quaint semantics.
- Many features: mutable state, exceptions, dynamic types, prototype-based inheritance, type coercion, first-class functions . . . and eval.

What have we done about it?

- Produced an information flow analysis for a language with many of JavaScript’s features, including run-time code generation.
Many research papers claim that `eval` is used rarely or only in trivial ways. A recent survey shows otherwise. Examples include:

- concatenating strings to form variable names;
- simulating higher order functions;
- bizarre or seemingly pointless invocations.
Staged Metaprogramming

JavaScript’s **eval** is a form of **metaprogramming**: it allows construction, manipulation and evaluation of program code at run-time. But metaprogramming is not new:

- Lisp allows quoting and unquoting of code.
- This restricts manipulation to plugging holes in abstract syntax trees.

**Example**

Plug: \( \langle x \rangle \)

into: \( \text{fun}(\langle - \rangle)\{x + 1\}) \)

to get: \( \text{fun}(x)\{x + 1\} \)

✓
Staged Metaprogramming

JavaScript’s `eval` is a form of metaprogramming: it allows construction, manipulation and evaluation of program code at run-time. But metaprogramming is not new:

- Lisp allows quoting and unquoting of code.
- This restricts manipulation to plugging holes in abstract syntax trees.

Example

Plug: \( \langle x \rangle \)

into: \((\text{fun}(\langle - \rangle)\{x + 1\})\)

to get: \((\text{fun}(x)\{x + 1\})\)

✓

Plug: \(\langle \rangle)(\text{fun}(y)\{y\})\)

into: \((\text{fun}(x)\{\langle - \rangle\})\)

to get: \((\text{fun}(x)\{\}))(\text{fun}(y)\{y\})\)

✗
Staged Metaprogramming

JavaScript’s `eval` is a form of metaprogramming: it allows construction, manipulation and evaluation of program code at run-time. But metaprogramming is not new:

▶ Lisp allows quoting and unquoting of code.
▶ This restricts manipulation to plugging holes in abstract syntax trees.

**Example**

Plug: $\langle x \rangle$

into: `(fun(⟨−⟩){x + 1})`

to get: `(fun(x){x + 1})`

Plug: `⟨}⟩(fun(y){y}⟩`

into: `(fun(x){⟨−⟩})`

to get: `(fun(x){})(fun(y){y})`

✓

In an attempt to understand better the behaviour of `eval`, we study a language with staged metaprogramming in the style of Lisp.

▶ Syntactically, staged just means that quotes can be nested.
Definition of Noninterference

Consider a setting where inputs and outputs to a program are marked with security levels, such as $H$ for high security and $L$ for low security.

Example

In a Web application, high/low input/output channels might be:

- high input — a “password” input box
- low input — any other text box
- high output — encrypted connection to webserver
- low output — unencrypted connection to webserver

- If the high inputs of a program cannot affect the low outputs, the program satisfies noninterference.
- This means an attacker who can only view low outputs cannot gain any information about high inputs.
- Noninterference is a popular information security property.
Consider the program:

\[
\text{if}(h)\{\text{true}\} \text{ else}\{/\}
\]

The result of the program can be either \textit{true} or \textit{/}.

- As the value \textit{/} can flow directly to the result, we say that there is a direct flow from \textit{/} to the result.

- If \textit{/} is \textit{false}, then the result of the program is equal to \textit{h}. As this dependency arises only through control flow, we say that there is an indirect flow from \textit{h} to the result.
Verifying Noninterference

Some early work on noninterference added a monitor to a program to track and enforce security levels of variables. Unfortunately:

- A 1-safety property of a program is one for which a violation can be shown by a single, finite trace of a program.
- Monitoring is good for enforcing 1-safety properties.
- Showing violation of a 2-safety property requires two traces.
- Noninterference is a 2-safety property.

Some recent research revisits monitoring and works around this by combining it with simple static analysis.

- Monitoring is good at handling metaprogramming.
- But it is still a dynamic (rather than static) analysis.

There is a large body of research on verifying noninterference with type systems, for example in ML.

- This is difficult to apply to dynamically typed languages.
Information Flow Analysis

▶ An information flow analysis tells us, for any variable $x$, whether it used in the computation of another variable $y$.

▶ Alternatively, in our setting with marked security levels, we can check whether any value labelled with level $H$ is used to compute other variables (or the result of a program).

▶ “$x$ is not used to compute $y$” is a stronger claim than “the value of $x$ does not affect the value of $y$”.

Example

This program clearly uses $x$ in its computation of $y$, but $y$ is always 0, so $x$ does not affect its value.

```plaintext
x := 10;
while(x <> 0){
  x := x - 1;
}
y := x;
```

▶ We can use an information flow analysis to verify noninterference.
Outline

Motivation
  Metaprogramming
  Noninterference and Information Flow

Outline

Syntax and Semantics of SLamJS

Information Flow Analysis for SLamJS
  CFA for SLamJS
  Information Flow for SLamJS

Implementation and Examples

Future Work

Conclusion
Syntax of SLamJS

Booleans \( b \ ::= \) true \mid false

Strings \( s \in String \)

Numbers \( n \in Number \)

Names \( x \in Name \)

Constants \( k \ ::= \) undef \mid null \mid b \mid s \mid n

Expressions \( e \ ::= \) k \mid \{ s : e \} \mid x \mid \text{fun}(x)\{e\} \mid e(e) \mid \text{box } e

\mid \text{unbox } e \mid \text{run } e \mid \text{if}(e)\{e\} \text{ else }\{e\} \mid e[e]

\mid e[e] = e \mid \text{del } e[e] \mid (e, \rho) \mid \text{run } e \text{ in } \rho

Values \( v, v^0 \ ::= (\text{fun}(x)\{e\}, \rho) \)

\( v^n \ ::= k \mid \{ s : v^n \} \mid (\text{box } v^{n+1}) \)

\( v^{n+1} \ ::= x \mid (\text{fun}(x)\{v^{n+1}\}) \mid (v^{n+1}(v^{n+1})) \)

\| (\text{run } v^{n+1}) \mid (\text{if}(v^{n+1})\{v^{n+1}\} \text{ else }\{v^{n+1}\}) \)

\| (v^{n+1}[v^{n+1}]) \mid (v^{n+1}[v^{n+1}] = v^{n+1}) \mid (\text{del } v^{n+1}[v^{n+1}])

\( v^{n+2} \ ::= (\text{unbox } v^{n+1}) \)

Environments \( \rho \in Name \xrightarrow{\text{fin}} v^0 \)
Syntax of SLamJS

Booleans \( b \) ::= true | false
Strings \( s \) ∈ String
Numbers \( n \) ∈ Number
Names \( x \) ∈ Name
Constants \( k \) ::= undef | null | \( b \) | \( s \) | \( n \)
Expressions \( e \) ::= \( k \) | \( x \) | fun(\( x \))\{e\} | e(e) | box e
                        | unbox e | run e | if(e)\{e\} else\{e\}
Values \( v, v^0 \) ::= (fun(\( x \))\{e\}, \( \rho \))
\( v^n \) ::= \( k \) | (box \( v^{n+1} \))
\( v^{n+1} \) ::= \( x \) | (fun(\( x \))\{v^{n+1}\}) | (v^{n+1}(v^{n+1}))
                    | (run \( v^{n+1} \)) | (if(v^{n+1})\{v^{n+1}\} else\{v^{n+1}\})
\( v^{n+2} \) ::= (unbox \( v^{n+1} \))

- We ignore the prototype-based objects in the rest of this presentation.
- Environments \( \rho \) occur only during evaluation.
Semantics of SLamJS

We define evaluation contexts and an evaluation relation $\overset{\rightarrow}{\rightarrow}$ in a typical way. Here are some illustrations of its behaviour:

- $(\text{fun}(x)\{x\})(1) \overset{\rightarrow}{\rightarrow} 1$
- $((\text{fun}(x)\{\text{fun}(y)\{x\}\})(1))(2) \overset{\rightarrow}{\rightarrow} 1$
- $\text{if(true}\{1\}\text{else}\{false\}) \overset{\rightarrow}{\rightarrow} 1$
- $(\text{fun}(x)\{\text{run(box x)}\})(0) \overset{\rightarrow}{\rightarrow} 0$
- $\text{run(box(if(unbox(box true))}\{1\}\text{else}\{false\})} \overset{\rightarrow}{\rightarrow} 1$
Information Flow in SLamJS

To allow us to express information flow in SLamJS, we augment it with explicit security level markers:

\[
\begin{align*}
\text{Markers} & \quad m \in \text{Marker} \\
\text{Expressions} & \quad e ::= \ldots | (m : e)
\end{align*}
\]

Direct flows from a marked value are tracked by the marker being part of the value:

\[
\begin{align*}
\text{if (false)\{true\} else\{L : l\}} & \xrightarrow{\text{HL}} L : l
\end{align*}
\]

No further treatment is needed.

Markers block reductions that might result in an indirect flow:

\[
\begin{align*}
\text{if (H : h)\{true\} else\{L : l\}} & \xrightarrow{\text{HL}}
\end{align*}
\]

We introduce lift rules that move markers towards the top level of an expression:

\[
\begin{align*}
\text{if (H : h)\{true\} else\{L : l\}} & \xrightarrow{\text{HL}} H : (\text{if (h)\{true\} else\{L : l\}})
\end{align*}
\]

Effectively, an indirect flow is turned into a direct one.
Erasure in SLamJS

Erasure captures what it means for a value *not* to be used in a computation.

- The *M*-erasure of $e$, written $\lfloor e \rfloor_M$, is $e$ with all subexpressions marked by $m \notin M$ replaced with $\_$.  
- $\_$ behaves like an unbound variable.
- $\lfloor \text{if}(\text{true})\{\text{false}\} \text{ else } \{H : h\}\rfloor_L = \text{if}(\text{true})\{\text{false}\} \text{ else } \{\_\} \xrightarrow{\text{Mark}} \text{false}$
- $\lfloor \text{if}(H : h)\{\text{true}\} \text{ else } \{L : l\}\rfloor_L = \text{if}(\_)\{\text{true}\} \text{ else } \{L : l\} \not\xrightarrow{\text{Mark}}$

**Theorem (Stability)**

*Consider an expression $e_1$ (which may use $\_$) and a $\_$-free expression $e_2$ such that $e_1 \xrightarrow{\text{Mark}}^* e_2$. Then for every $M \subseteq \text{Marker}$ such that $\lfloor e_2 \rfloor_M = e_2$, it follows that $\lfloor e_1 \rfloor_M \xrightarrow{\text{Mark}}^* \lfloor e_2 \rfloor_M$.*

- This means that if $e_2$ is not marked by $m$, we can safely erase it from $e_1$. 
Our information flow analysis for SLamJS comprises two phases:

1. We perform CFA to determine which functions and code values can be bound where.

2. We generate and solve information flow constraints using the results of the CFA.

- Handling code values in CFA requires some special treatment.
- The key observation in CFA is that data and control flow influence each other, so both must be handled in a single analysis. As information flow does not affect data or control flow, it can be separate.
- Because our analysis extends CFA, we believe our technique could easily be adapted to other CFA-style analyses.
CFA for SLamJS

0CFA is a standard analysis that operates by:

1. **labelling** each subexpression of a program;
2. generating **constraints** between the values occurring at each label (and each variable);
3. solving these constraints.

0CFA conflates variables with the same name bound in different functions.

- For most languages, this is not a problem, as we can simply $\alpha$-convert them.
- SLamJS does not respect $\alpha$-equivalence, so the analysis must track explicitly where names are bound.
CFA for SLamJS

CFA can be derived from abstract interpretation over a suitable domain. Our abstract domain is:

Abstract values $\nu \in \text{AbsVal}$ ::= NULL | UNDEF | BOOL | NUM | STR |
| FUN(x, e) | BOX(e) | REC(ℓ)

The abstract value $\text{BOX}(e)$ is inhabited by:

- the expression $\text{box} e$;
- any expression that $\text{box} e$ evaluates to.

The range of code values in a program may be infinite. This permissive definition of $\text{BOX}(e)$ ensures that a finite solution to the constraints is always possible.
Sample CFA rules

\[ \Gamma, \varrho \models k^\ell \quad \text{if} \quad \lfloor k \rfloor \in \Gamma(\ell) \]
\[ \Gamma, \varrho \models x^\ell \quad \text{if} \quad \varrho(x) \subseteq \Gamma(\ell) \]
\[ \Gamma, \varrho \models (\text{box } e)^\ell \quad \text{if} \quad \Gamma, \varrho \models e \\
\text{and} \quad \exists \nu \in \Gamma(\ell). \Gamma, \varrho \models \nu \approx \text{box } e \]
\[ \Gamma, \varrho \models (\text{unbox } e)^\ell \quad \text{if} \quad \Gamma, \varrho \models e \\
\text{and} \quad \forall \text{BOX}(e') \in \Gamma(\text{lbl}(e)). \Gamma(\text{lbl}(e')) \subseteq \Gamma(\ell) \]
\[ \Gamma, \varrho \models (\text{if } (e_1) \{ e_2 \} \text{ else } \{ e_3 \})^\ell \quad \text{if} \quad \Gamma, \varrho \models e_1 \land \Gamma, \varrho \models e_2 \land \Gamma, \varrho \models e_3 \\
\text{and} \quad \Gamma(\text{lbl}(e_2)) \subseteq \Gamma(\ell) \land \Gamma(\text{lbl}(e_3)) \subseteq \Gamma(\ell) \]
CFA Example

Consider:

$$(((\text{fun}(x)\{(I : (\text{fun}(y)\{x\}))(H : 1))\})(L : 2), \epsilon) \overset{\Pi}{\rightarrow}^* (I : (H : 1))$$

labelled as:

$$(((\text{fun}(x)\{(I : (\text{fun}(y)\{x^0\})^1)^2\})^3(H : 1^4)^56(L : 2^7)^8)^9$$

Solution of the CFA constraints gives:

0 $\mapsto$ \{NUM\} \hspace{1cm} 1 $\mapsto$ \{FUN(y, (x)^0)\} \hspace{1cm} 2 $\mapsto$ \{FUN(y, (x)^0)\}

3 $\mapsto$ \{FUN(x, ((I : (\text{fun}(y)\{(x)^0\})^1)^2))\} \hspace{1cm} 4 $\mapsto$ \{NUM\} \hspace{1cm} 5 $\mapsto$ \{NUM\}

6 $\mapsto$ \{FUN(y, (x)^0)\} \hspace{1cm} 7 $\mapsto$ \{NUM\} \hspace{1cm} 8 $\mapsto$ \{NUM\} \hspace{1cm} 9 $\mapsto$ \{NUM\}

x $\mapsto$ \{NUM\} \hspace{1cm} y $\mapsto$ \{NUM\}

As expected, the result of evaluation (labelled 9) is a number.
Information Flow for SLamJS

The information flow analysis uses the results of CFA to generate constraints on two relations between markers, labelled program points and variables:

- ▶ \( \rightsquigarrow \) tracks direct flows;
- ▶ \( \rightsquigarrow \) tracks indirect flows.

If an expression marked by \( m \) is used in computing an expression labelled \( \ell \) then, taking \( \rightsquigarrow = \rightsquigarrow \cup \rightsquigarrow \), the analysis ensures \( m \rightsquigarrow^* \ell \).

**Theorem (Information Flow Soundness)**

*Suppose \( \rightsquigarrow \) has been computed for \( t^\ell \) by the information flow analysis. Then if \( t^\ell \xrightarrow{\text{}} v^\ell' \), where \( v \) is a stage-0 value composed only of markers and constants, and \( M = \{ m \in \text{Marker} \mid m \rightsquigarrow^* \ell \} \), it follows that \( \llbracket v \rrbracket_M = v \).*

The key parts of this theorem have been mechanised in Coq.
# Sample Information Flow Rules

<table>
<thead>
<tr>
<th>Expression e</th>
<th>Subexpressions if:</th>
<th>Direct and:</th>
<th>Indirect and:</th>
</tr>
</thead>
<tbody>
<tr>
<td>$k^\ell$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x^\ell$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(if($t_1^\ell_1$){$t_2^\ell_2$} else{$t_3^\ell_3$})$^\ell_4$</td>
<td>$\land_{i=1}^3 \models_{IF} t_i^\ell_i$</td>
<td>$x \rightsquigarrow \ell$</td>
<td>$\ell_1 \rightsquigarrow \ell_4$</td>
</tr>
<tr>
<td>(box $t_1^\ell_1$)$^\ell_2$</td>
<td>$\models_{IF} t_1^\ell_1$</td>
<td>$\ell_2 \rightsquigarrow \ell_4 \land \ell_3 \rightsquigarrow \ell_4$</td>
<td></td>
</tr>
<tr>
<td>(unbox $t_1^\ell_1$)$^\ell_2$</td>
<td>$\models_{IF} t_1^\ell_1$</td>
<td>$\forall \text{BOX}(t_1^{\ell'}) \in \Gamma(\ell_1) \cdot \ell' \rightsquigarrow \ell_2$</td>
<td>$\ell_1 \rightsquigarrow \ell_2$</td>
</tr>
</tbody>
</table>
Information Flow Analysis Example

Recall:

\[ ((({{\text{fun}}(x)}\{ I : (\text{fun}(y)\{ x \}) \})\{ H : 1 \})(L : 2), \epsilon) \xrightarrow{\Pi}^* (I : (H : 1)) \]

labelled as:

\[ ((({{\text{fun}}(x)}\{(I : (\text{fun}(y)\{ x^0 \}^1)^2)\})^3\{H : 1^4\}^5\{L : 2^7\}^8)^9 \]

The information flow constraints are:

\[
\begin{array}{ccccccccc}
4 & \Rightarrow & 5 & \Rightarrow & x & \Rightarrow & 0 & \Rightarrow & 7 & \Rightarrow & 8 & \Rightarrow & y \\
H & \Rightarrow & I & \Rightarrow & 3 & \Rightarrow & 6 & \Rightarrow & 9 & \Rightarrow & L \\
1 & \Rightarrow & 2 & \Rightarrow & & & & & \\
\end{array}
\]

We have \( H \xrightarrow{\ast} 9 \) and \( I \xrightarrow{\ast} 9 \) and \( L \not\xrightarrow{\ast} 9 \). This means the result (labelled 9) has information flows from \( H \) and \( I \), but not \( L \).
We have implemented our analysis in OCaml.

Example

```ocaml
let c = box x in
let x = L : 1 in
let eval = fun(b){run b} in
let x = H : 2 in
eval(c)
```

Depends on: L
We have implemented our analysis in OCaml.

Example

```
let c = box x in
let x = L : 1 in
let eval = fun(b){run b} in
let x = H : 2 in
eval(c)
```

```
let x = if(true){box f} else{box g} in
let f = fun(y){1} in
let g = fun(z){L : true} in
run (box ((unbox x)(H : undef)))
```

Depends on: L

Depends on: L
Future Work

- Extend the analysis to handle other JavaScript features, such as mutable state and exceptions.
- Improve the precision of analysis of object reads and writes by extending the abstract string domain.
- Transfer our ideas to a CFA2 analysis for improved precision with higher order flow.
- Apply recent work on analysing `eval` directly to transform uses of `eval` into staged metaprogramming.
Conclusion

Our contributions:

▶ We have developed an information flow analysis for a JavaScript-like language with staged metaprogramming.
▶ We have mechanised the proof of soundness for our analysis using Coq.
▶ We have implemented our analysis in OCaml.
▶ Online material: 
  http://mjolnir.cs.ox.ac.uk/web/slamjs/.

We believe that we now have all the technical tools for an interesting information flow analysis of JavaScript with `eval`.
Conclusion

Our contributions:

▶ We have developed an information flow analysis for a JavaScript-like language with staged metaprogramming.
▶ We have mechanised the proof of soundness for our analysis using Coq.
▶ We have implemented our analysis in OCaml.
▶ Online material:  
  http://mjolnir.cs.ox.ac.uk/web/slamjs/.

We believe that we now have all the technical tools for an interesting information flow analysis of JavaScript with eval.

▶ Thanks for listening. Questions are welcome.