JavaScript: Security & Verification

Arjun Guha
Joe Gibbs Politz
Benjamin S. Lerner
Shriram Krishnamurthi

BROWN
A LITTLE QUIZ
Include the following code at the top of the `<head>` of your page:

```html
<script type="text/javascript" src="https://your-domain.js"></script>
```

In your head tag, include the following code:

```html
<script data-main="path/to/main" src="path/to/your-domain.js"></script>
```

The following code will include the first of your-domain within your page.

```html
<!-- JavaScript code for your-domain -->
<script language="javascript" src="http://your-domain.js">
</script> <!-- End JavaScript your-domain code-->
```
```
// Redirect page
window.location = “citibank.com.evil.com”

// Change all links
links = document.getElementsByTagName(“a”);
for (var i = 0; i < links.length; i++) {
    links[i].href = “track.com/fwd?” + links[i].href;
}

// Read cookies
document.cookie

// Read passwords
document.querySelector(‘input[type=password]’)

// Embed Flash, exploit, profit
document.write(‘
    <object type=“application/x-shockwave-flash”
    data=“evil.swf” />
’);
```
WALL-E STREET
Humans Band Together To Fight Back The Rise Of The Machines
I need your help in testing its robustness. Are the rules sufficient to prevent all direct access to the DOM and the global object? Are there any small leaks that I am unaware of? Is the approach I’m taking inherently unsound? What additional restrictions are required to prevent unintended collusion?

So this is the test:

Write a program in the form

(function () {
    ...
})();

where the ... is replaced by code that calls the alert function when run on any browser. If the program produces no errors when linted with the ADSafe option, then I will buy you a plate of shrimp.

Douglas Crockford
Caplet list, 2007-09-30
Type-check the body of adsafe.js.

Typing Local Control and State using Flow Analysis

Arjun Guha, Claudiu Saftoiu, and Shriram Krishnamurthi

Brown University

Encode all of JSLint as a type
ADsafety
Type-Based Verification of JavaScript Sandboxing

Joe Gibbs Politz  Spiridon Aristides Eliopoulos  Arjun Guha  Shriram Krishnamurthi

Brown University
Nobody Programs in "Languages"

Frameworks are "Languages", Too
jQuery

**Query**: Selects some nodes in the page

```
$.tweet span
```.

**Manipulate**: Retrieve or modify data from node(s)

```
.next().html()
```.

**Navigate**: Move to new nodes, relative to existing ones

```
```
Possible Errors

• “Standard” type errors:
  – `.map()` a function over wrong types of elements

• Ambiguity:
  – Getting the `.html()` of one node, but have many

• Overshooting:
  – Asking for the `.children()` of a leaf node...

• Wrong selection:
  – `$(“div.mispleling”)`
Combining Form and Function: Static Types for JQuery Programs

Benjamin S. Lerner, Liam Elberty, Jincheng Li, and Shriram Krishnamurthi

Brown University
BROWSERS ARE PROGRAMMABLE, TOO
Verifying Web Browser Extensions’ Compliance with Private-Browsing Mode

Benjamin S. Lerner, Liam Elberty, Neal Poole, and Shriram Krishnamurthi

Brown University
THAT’S A LOT OF TYPE SYSTEMS!
module Base_TypeSystem = struct

module PPrinter = struct

end

+ Hooks for easily building variations on the base type system
Ergonomic Innovations

Significant type inference
    Better syntax for writing complex types
Better support for inheritance+subtyping
    Parameterized type environments
Types for the DOM
5.2 Example: Implementing TypeScript’s Covariant Function Calls

As a proof of concept, we have implemented an extension to provide TypeScript’s semantics for functions [18]. This extension overrides the TArrow type of our base system, and replaces it with one that has the new semantics. The types-definition module is gratifyingly similar to the Bare one: the only change necessary is adding a single type constructor

```
1   type typ =
2       | TBase of BASE.typ
3       | TArrow of typ list * typ option * typ
```

The essence of the difference is 260 LOC
WHY ARE OUR PROOFS MEANINGFUL?
JavaScript program → \( \lambda_{JS} \) program

browser engines → "their answer"

"our answer" ↓ desugar ↓ identical for portion of several test suites

The Essence of JavaScript

Arjun Guha, Claudiu Saftoiu, and Shriram Krishnamurthi

Brown University

small interpreter → "our answer"
• Verifying Web Browser Extensions, MSR
• Aspects for JavaScript, U Chile
• Static Analysis of JavaScript, UCSB
• System !D, UCSD
• JavaScript Abstract Machine, Utah and Northeastern
• Deriving Refocusing Functions, Aarhus
• Information Flow Analysis, Stevens Tech
• 0CFA, Fujitsu Labs (patent pending)
• Formal Specification of JavaScript Modules, KAIST
Our Web S(u)ite

github.com/brownplt

www.jswebtools.org