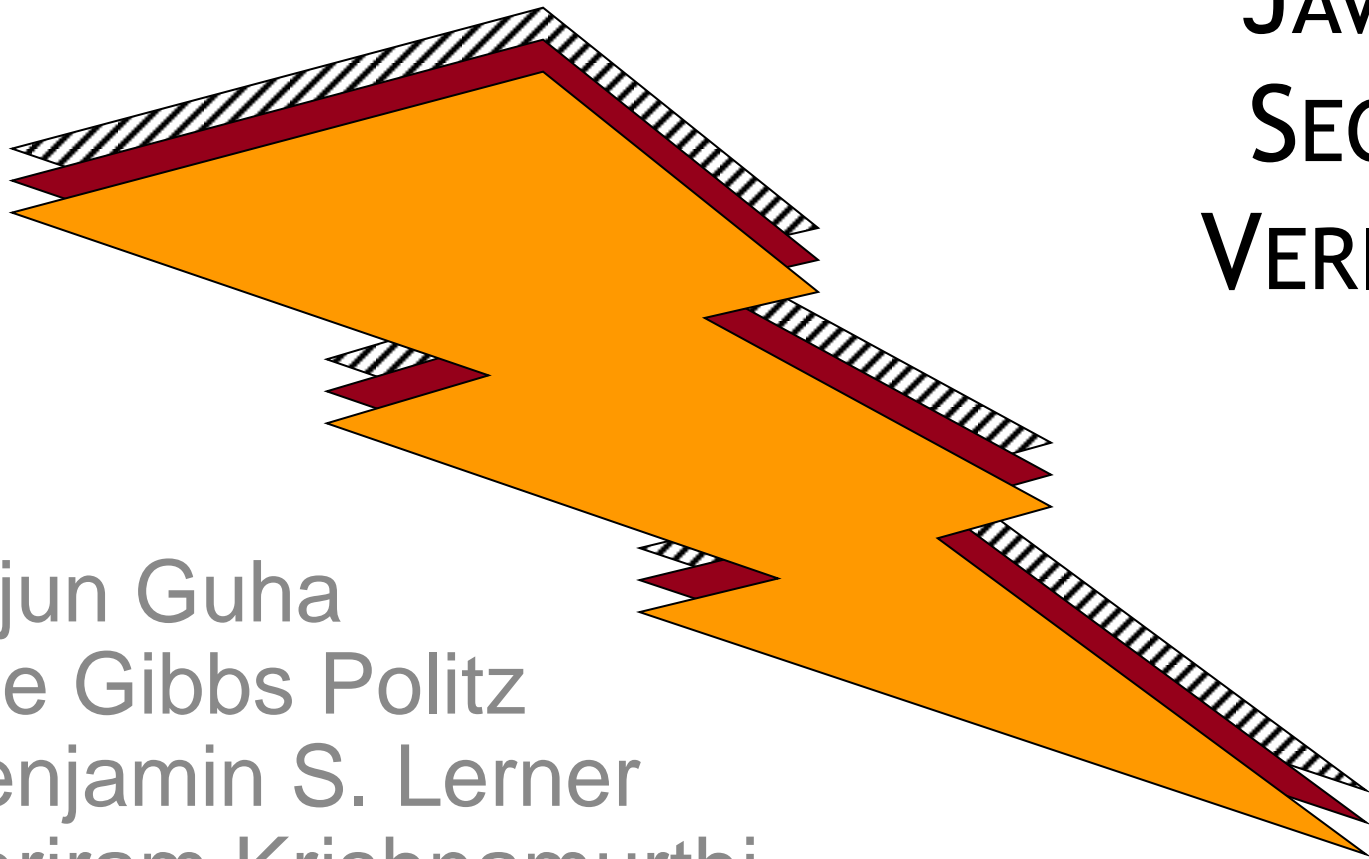


# JAVASCRIPT: SECURITY & VERIFICATION

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:

```
<script type="text/javascript" src="https://[REDACTED].js"></script>
```

In your head tag, include the following code:

```
<script data-main="path/to/main" src="path/to/[REDACTED].js"></script>
```

The following code will include the first of [REDACTED] within your page.

```
<!--JavaScript code for [REDACTED], [REDACTED]->  
<script language="javascript" src="http://[REDACTED].js">  
</script> <!--End JavaScript [REDACTED] 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" />');
```

The New York Times - Br... x

http://www.nytimes.com/

Welcome to TimesPeople Get Started TimesPeople recommended: Our Epic Foolishness 8:41 PM Recommend

HOME PAGE TODAY'S PAPER VIDEO MOST POPULAR TIMES TOPICS MOST RECENT Get Home Delivery Log In Register Now

GREAT ESCAPES TO EUROPE. Continental Airlines

# The New York Times

Tuesday, June 1, 2010 Last Update: 8:40 PM ET

Fares from \$407 each way Taxes and fees apply Continental Airlines

Switch to the Global Edition for an international perspective on news, business, sports and more.

Search Try the New Times Skimmer Subscribe to Home Delivery Personalize Your Weather

Switch to Global Edition

**After Israel Raids Flotilla, U.S. Is Torn Between Allies**  
By MARK LANDLER 15 minutes ago  
The rift between Israel and Turkey makes it difficult for the White House to make progress on Iran's nuclear program and peace talks between Israel and the Palestinians.  
U.N. Council Condemns 'Acts' in Raid 12:18 PM ET

**Immigrant Runs for Mayor, Back in Mexico**  
By KIRK SEMPLE 15 minutes ago  
Juan Navarro has homes in Queens and New Jersey, but his electoral goal is the mayor's office in Serdan, Mexico. Above, Mr. Navarro at his restaurant in Manhattan.

**Half a Dozen States Delay Tax Refunds**  
By MICHAEL COOPER 13 minutes ago  
Some states are cash poor, and others also lack the ability

**OPINION »**  
Op-Ed: Israeli Force, Adrift on the Sea  
After the botched raid on the Gaza flotilla, Israel must accept that power can never defeat an idea, writes Amos Oz. Instead, what is needed is a better idea.

**TRAVEL »**  
Caravaggio in Rome  
About a third of the artist's works are housed in Rome.

**MARKETS »** At 8:21 PM ET

JAPAN	HongSeng	CHINA
Nikkei		Shanghai
9,632.83	19,496.95	2,568.28
-79.00	-268.24	-23.86
-0.81%	-1.36%	-0.92%

Data delayed at least 15 minutes

GET QUOTES My Portfolios  
Stock, ETFs, Funds Go

WILL IT BE WORTH A...  
Will it be worth a...

Business and Finance News x

www.huffingtonpost.com/business/

My Calendar My Papers MBTA PVD CS19 L21 Dagstuhl HtDP: Account Man... Conferences Journals Other bookmarks

For Profit Colleges Housing Crisis Foreclosure Crisis Europe In Crisis The Choice More Log in Create Account

June 26, 2012

# HUFFPOST BUSINESS

THE INTERNET NEWSPAPER: NEWS BLOGS VIDEO COMMUNITY

Edition: U.S. Search The Huffington Post Like 33k Follow +1

FRONT PAGE POLITICS ENTERTAINMENT WORLD TECH MEDIA GREEN SPORTS SCIENCE CULTURE ALL SECTIONS

Business > Small Business Money The Watchdog Occupy Wall Street TechCrunch Autolog

FROM AP: Congress passes bill increasing drug inspections... 1 hour 24 minutes ago Enter email address Get Alerts

# WALL-E STREET

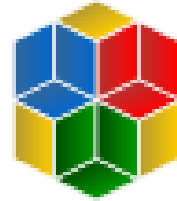
## Humans Band Together To Fight Back The Rise Of The Machines



Facebook  
JavaScript  
(FBJS)



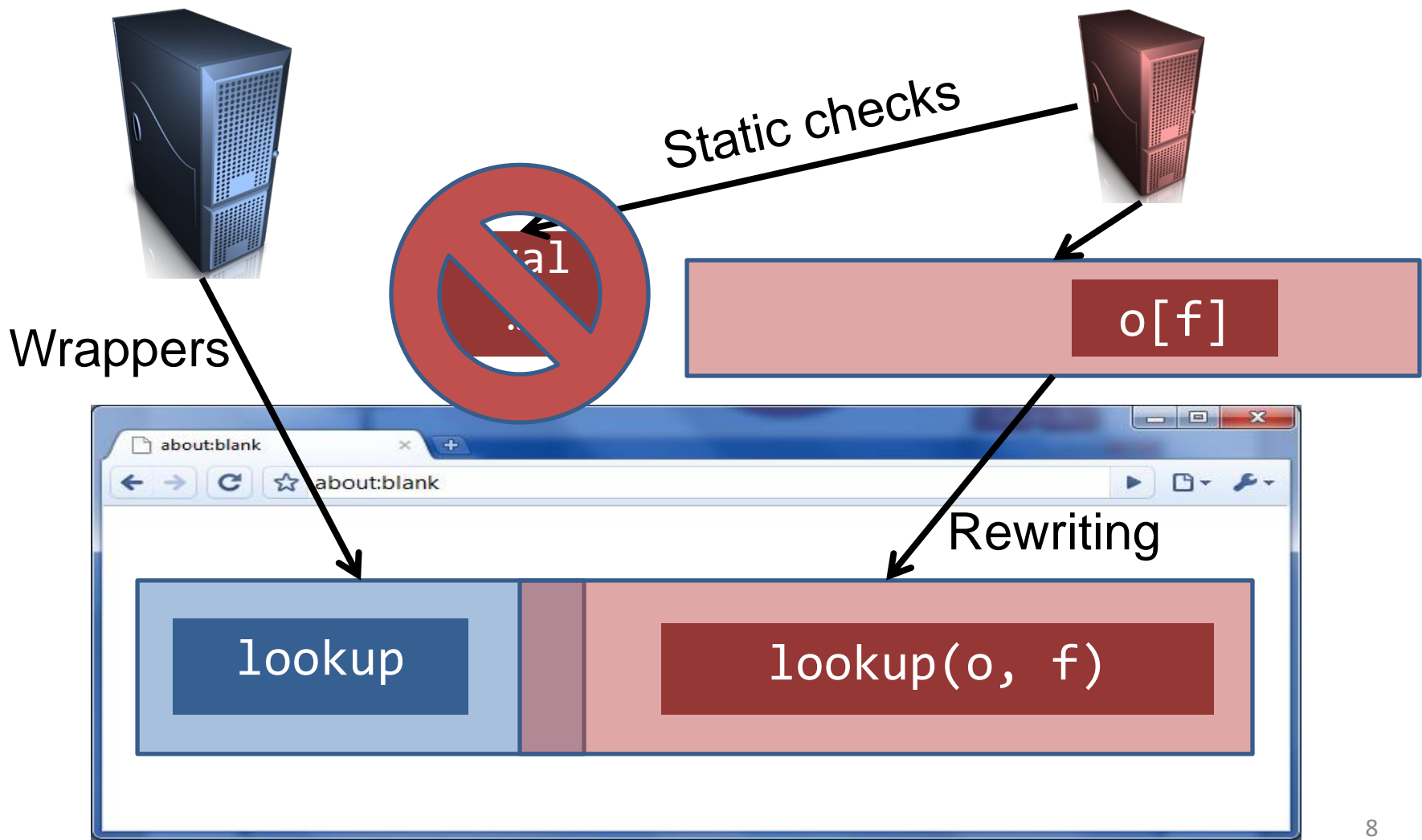
Microsoft  
Web Sandbox



Google  
Caja



Yahoo!  
ADsafe





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  
ads

JSLint rejects

## Typing Local Control and State using Flow Analysis

Arjun Guha, Claudiu Saftoiu, and Shriram Krishnamurthi

Brown University

adsafe.js

ad.

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

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

`$(".tweet span").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”)`

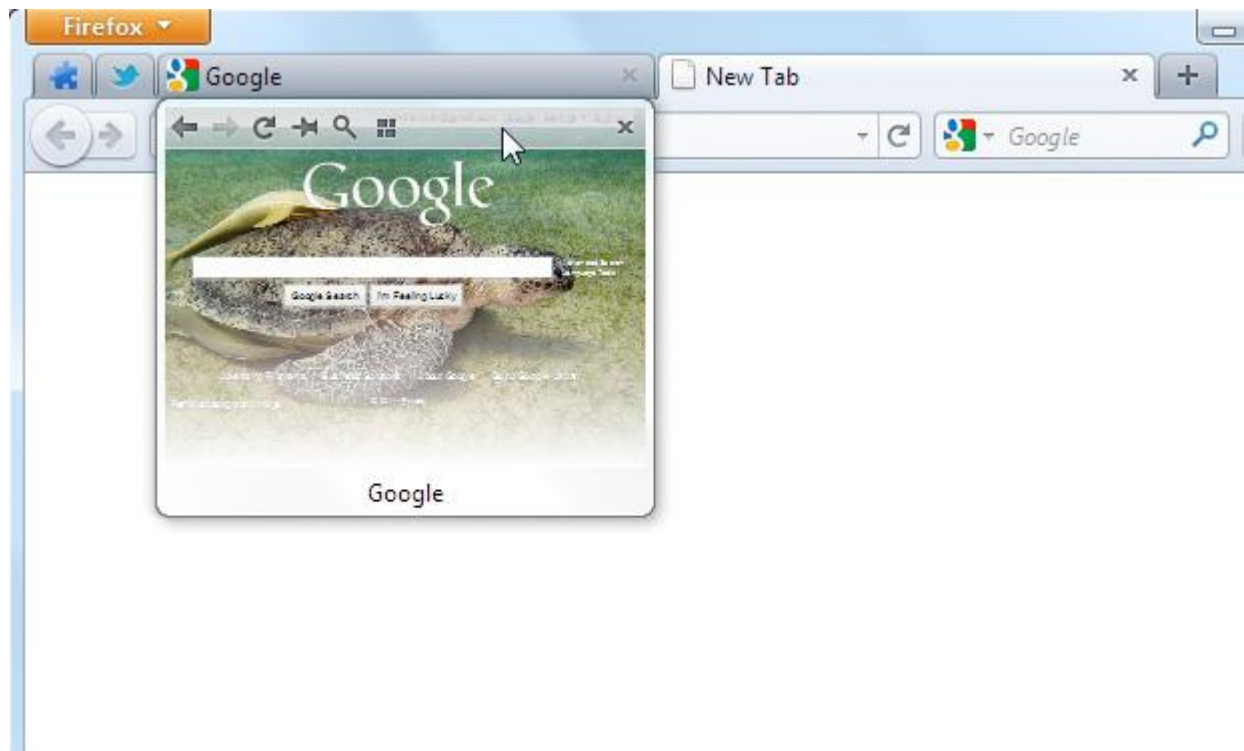
# Combining Form and Function: Static Types for JQuery Programs\*

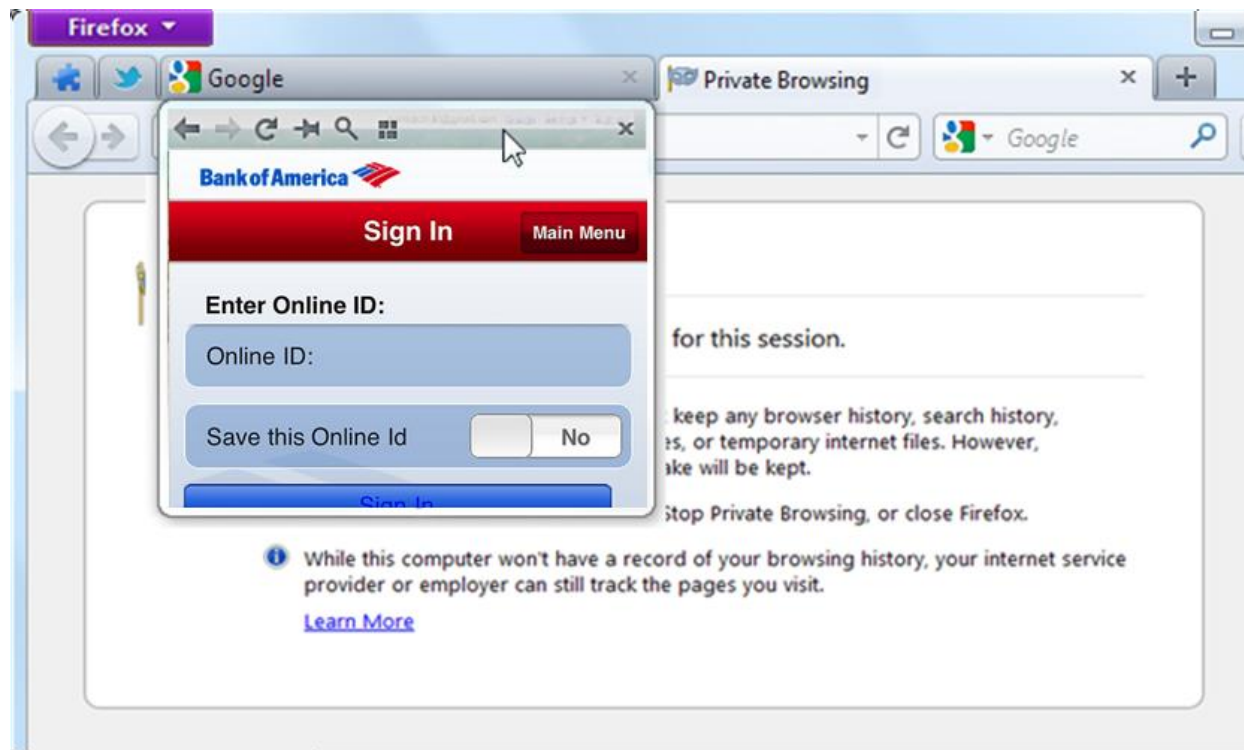
Benjamin S. Lerner, Liam Elberty, Jincheng Li, and Shriram Krishnamurthi

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!

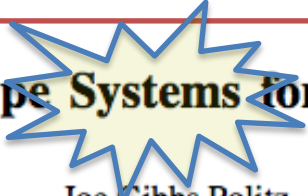
## Progressive Types \*

Joe Gibbs Politz  
Brown University  
joe@cs.brown.edu

Hannah Quay-de la Vallee  
Brown University  
hannahqd@cs.brown.edu

Shriram Krishnamurthi  
Brown University  
sk@cs.brown.edu

## TeJaS: Type Systems for JavaScript



Benjamin S. Lerner  
Brown University  
blemer@cs.brown.edu

Joe Gibbs Politz  
Brown University  
joe@cs.brown.edu

Arjun Guha  
Cornell University  
arjun@cs.cornell.edu

Shriram Krishnamurthi  
Brown University  
sk@cs.brown.edu

module Base\_TypeSystem = struct

module PPrinter = struct

The image shows a complex set of type theory rules and definitions, organized into several sections:

- TYPECHECKING:** Rules for checking types against a context  $\Gamma$  and a type  $T$ , including C-SUB, C-EXPOSE, C-LABEL, C-LET, C-FUNC-FIXED, C-ARRAY, and C-APP-INTERL.
- TYPE SYNTHESIS:** Rules for synthesizing a type  $T$  from an expression  $e$ , including T-ID, T-PRIM, T-EXPOSE, T-LET, T-SEQ, T-CHECK, T-CHEAT, T-ARRAY, T-SUBREF-2, T-SUBREF-1, T-BRACKET, T-TRY, T-APP-FIXED, T-APP-VARFIXED, T-TRUE, T-PREIFIXOP, T-APP-INTERL, T-TYPABS, T-HIDDEN, and T-APP-INTERL.
- SUBTYPING:** Rules for subtyping, including S-REFL, S-T, S-L, S-NULL-SRC, S-NULL-REF, S-NULL-SNK, S-SNK, S-REFSNK, S-REF, S-UNION-L, S-UNION-R, S-INTER-L, S-INTER-R, S-ARR-FIXEDFIXED, S-ARR-FIXEDVAR, S-ARR-VARFIXED, S-ARR-VARVAR, S- $\mu$ -R, S- $\mu$ -L, S-VAR, S-KERN, S-Obj, S-ABSENT, S-ABSENTMAYBE, S-ABSENTINHERIT, and S-DISJOINT.
- OBJECT-FIELD SUBTYPING:** Rules for subtyping object fields, including F-PRESENT, F-MAYBE, F-INHERIT, F-ABSENT, F-HIDDEN, F-PRESENTMAYBE, F-ABSENTMAYBE, F-ABSENTINHERIT, and F-DISJOINT.

```

/cygdrive/c/Users/Ben/Documents/Brown/TeJaS/src
Ben@bsl-laptop ~/Brown/TeJaS/src
$ ../run -env ../data/javascript.env -idl short.idl
  -compile-env -print-env test-ext.js > ext3.txt
type error at test-ext.js:2:53-71 : expected
Src ({{-{_proto_}- : ? nsIJS CID ,
  _proto_ : ! Object ,
  {} : _}) , got
Src ({{-{_proto_}- : ? nsIJS CID ,
  _proto_ : ! Object ,
  {} : _})
type error at test-ext.js:3:32-76 :
  expected nsIJS CID , got (nsIJS CID + @Undef)

```

end  
+ Hooks for easily building variations on the base type system

end

# 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 type-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

*desugar*

$\lambda_{JS}$   
program

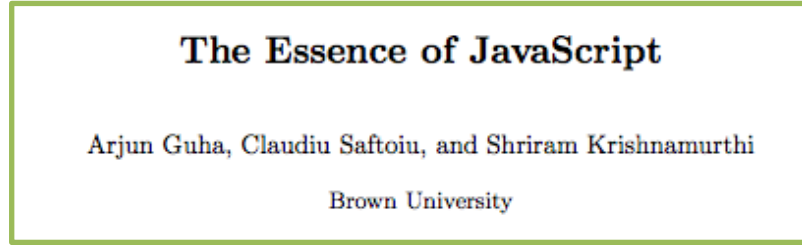
browser  
engines

small  
interpreter

“their  
answer”

“our  
answer”

identical for portion of  
several **test suites**





users



- *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
- *OCFA*, Fujitsu Labs (patent pending)
- *Formal Specification of JavaScript Modules*, KAIST

tools

Fork us on GitHub

# Our Web S(u)ite

[github.com/brownplt](https://github.com/brownplt)

[www.jswebtools.org](http://www.jswebtools.org)

