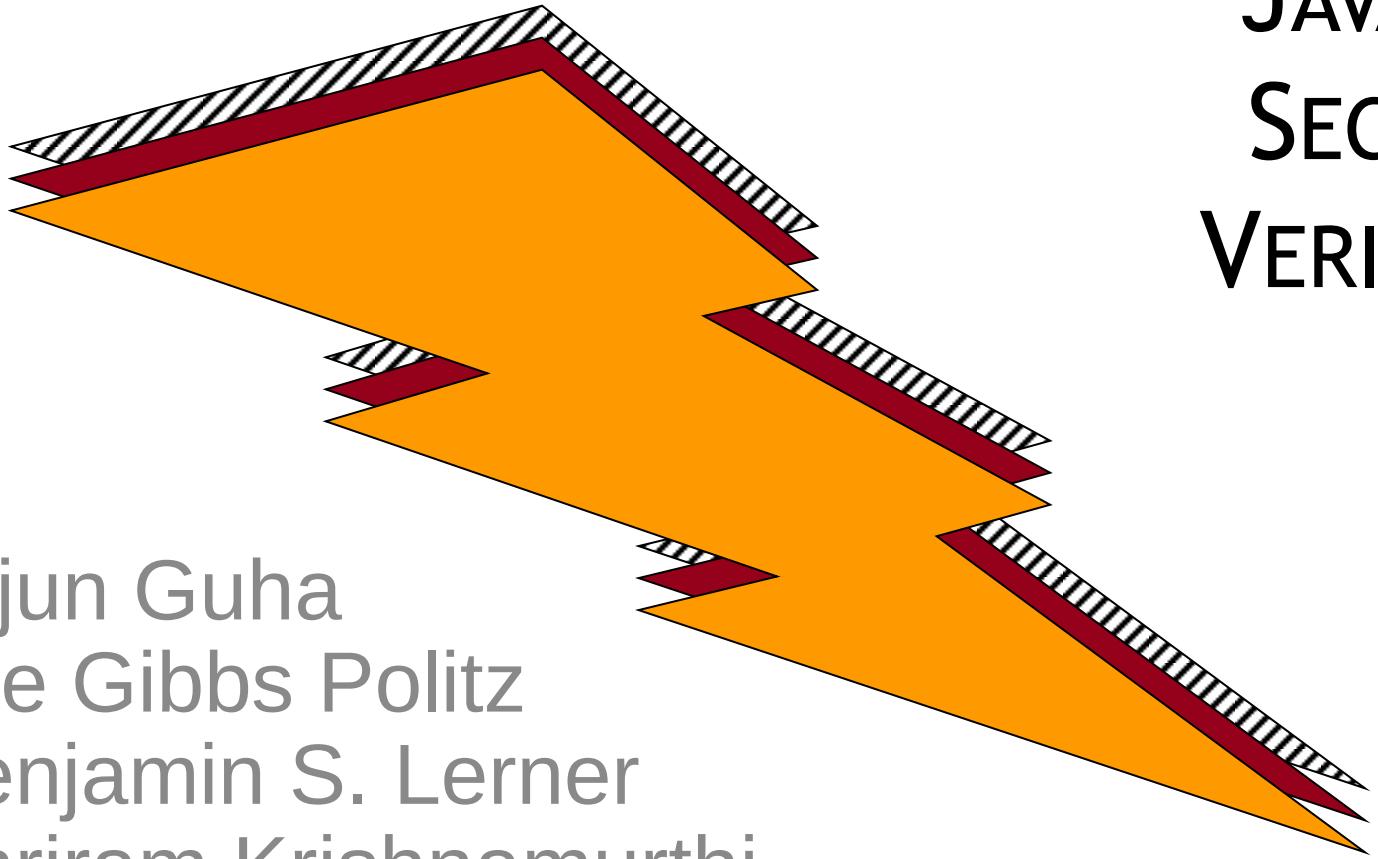
JavaScript: Security & Verification



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...
http://www.nytimes.com/
Welcome to TimesPeople
Get Started
TimesPeople recommended: Our Epic Foolishness
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
JOBS
REAL ESTATE
AUTOS
ALL CLASSIFIEDS
WORLD
U.S.
POLITICS
N.Y./REGION
BUSINESS
TECHNOLOGY
SPORTS
SCIENCE
HEALTH
OPINION
ARTS
Books
Movies
Music
Television
Theater
STYLE
Dining & Wine
Fashion & Style
Home & Garden
Weddings/ Celebrations
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
MORE ON THE RAID
Israel Faces Pressure on Gaza After Raid
Room for Debate: Rethinking a Blockade
The Lede: Activists Pledge to Send More Ships to Gaza
U.S. Opens
Juan Arredondo for The New York Times
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.
Brooks: The Oil Plume
Comments (560)
Herbert: Epic Foolishness
Editorial: Habeas Corpus
O'Hanlon et al.: War Data
Revkin: Gulf Crimes?
Room for Debate: Raise the Retirement Age?
TRAVEL »
Caravaggio in Rome
About a third of the artist's works are housed in Rome.
MARKETS »
As of 8:21 PM ET
JAPAN Nikkei 9,632.83 −79.00 −0.81%
HangSeng 19,496.95 −268.24 −1.36%
CHINA Shanghai 2,568.28 −23.86 −0.92%
Data delayed at least 15 minutes
GET QUOTES
My Portfolios »
Stock, ETFs, Funds
Go
Will it be worth a

Business and Finance News

www.huffingtonpost.com/business/

My Calendar | My Papers | MBTA PVD | CS19 | 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 | Autoblog

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

WALL-E STREET

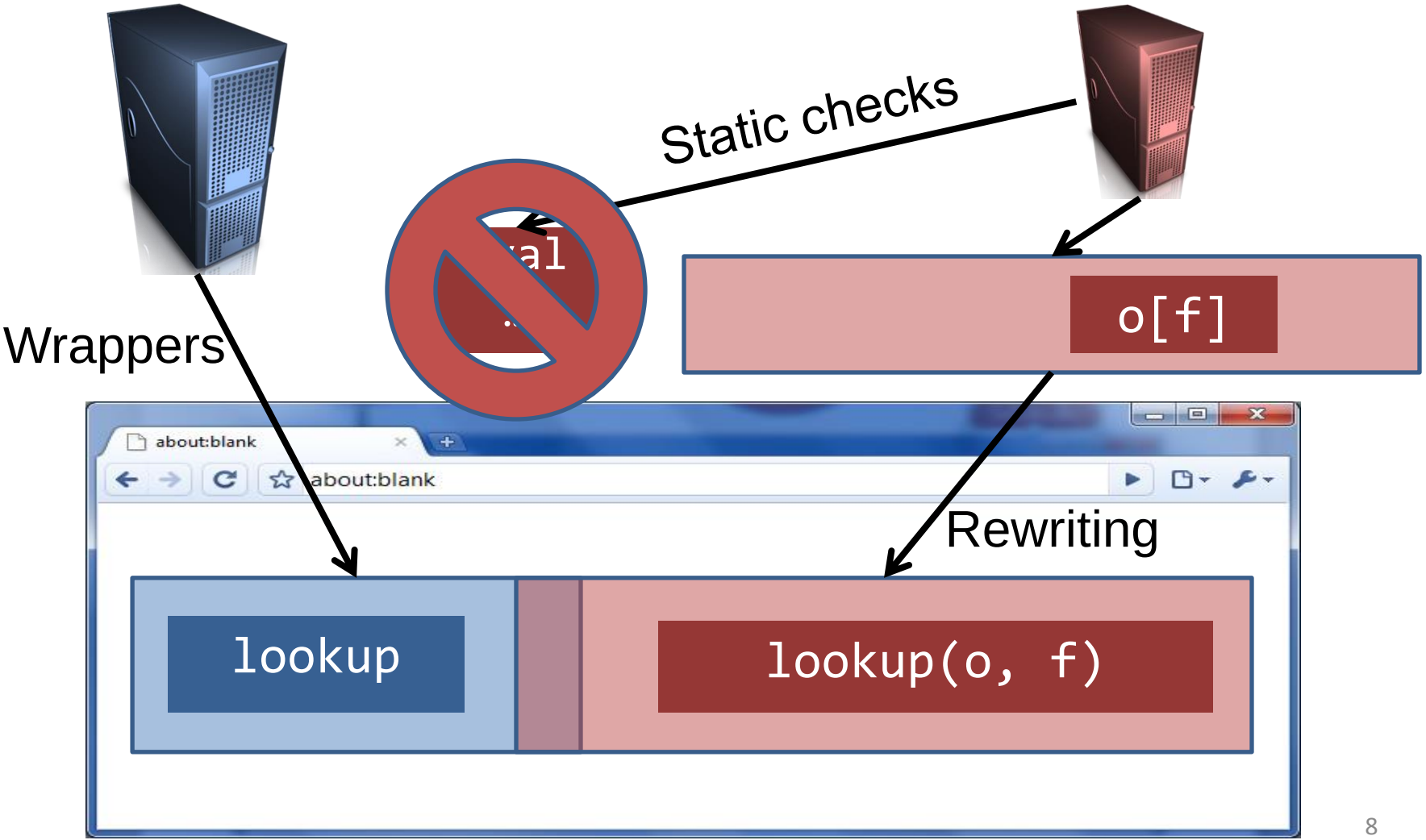
Humans Band Together To Fight Back The Rise Of The Machines

Facebook
JavaScript
(FBJS)

Microsoft
Web Sandbox

Google
Caja

Yahoo!
ADsafe


Static checks
Wrappers
o[f]
about:blank
about:blank
Rewriting
lookup
lookup(o, f)

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?

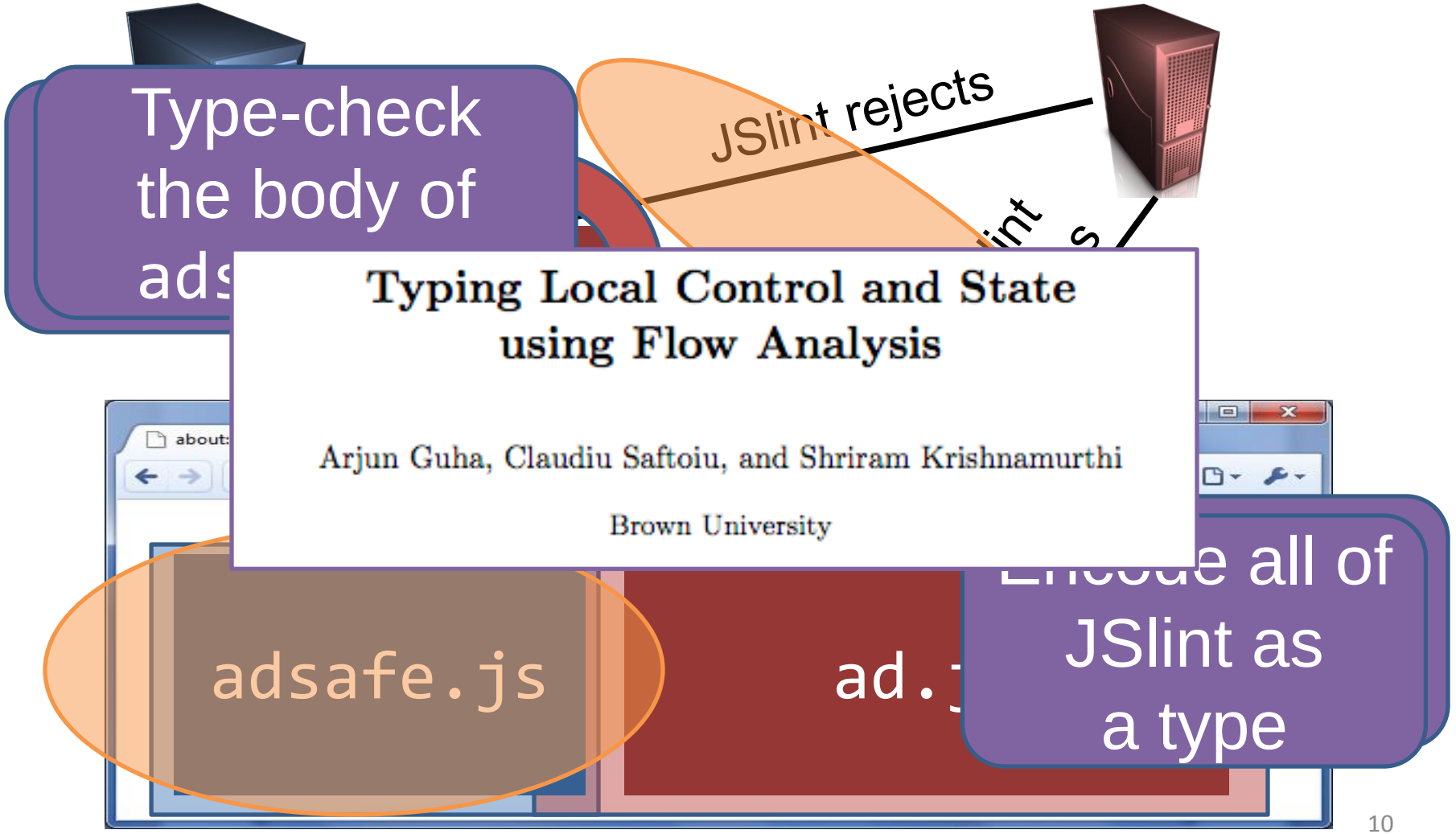
So this is the test:

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.j
Encode all of JSlint as a type

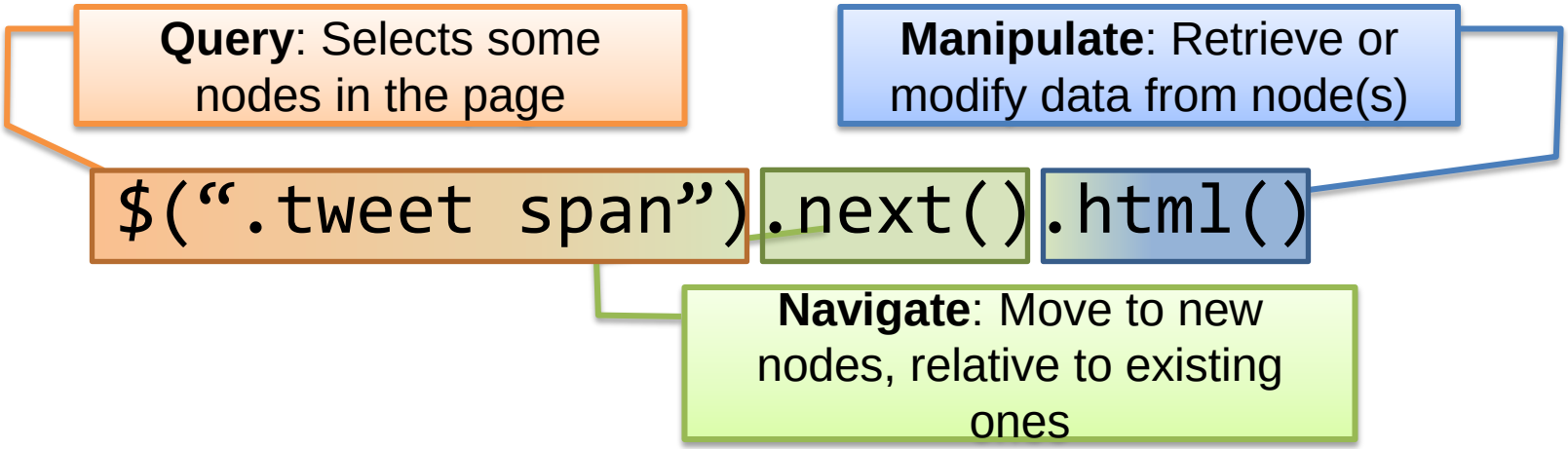
ADsafety
Type-Based Verification of JavaScript Sandboxing

Joe Gibbs Politz Spiridon Aristides Eliopoulos Arjun Guha Shriram Krishnamurthi

Brown University

Nobody Programs in "Languages"

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

`.map()` a function over wrong types of elements

Ambiguity:

Getting the `.html()` of one node, but have many

Overshooting:

Asking for the `.children()`

Wrong selection:

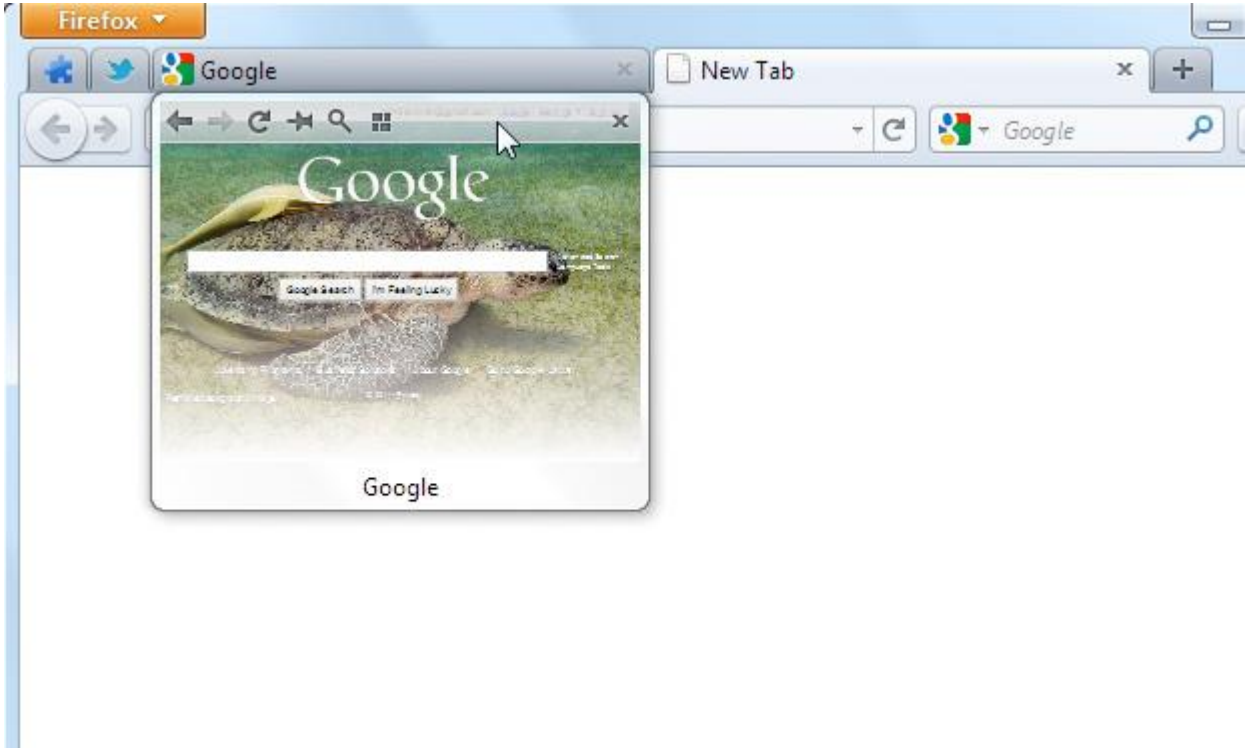
`$(“div.mispleling”)`

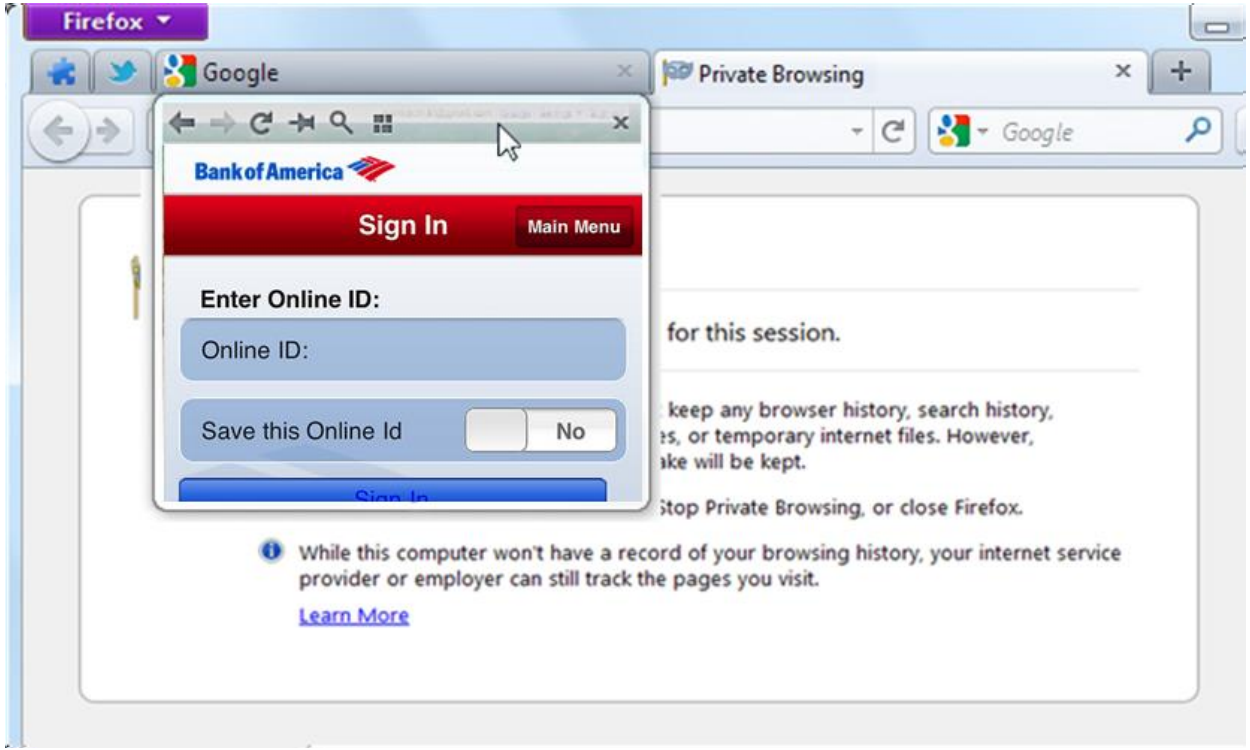
Combining Form and Function: Static Types for JQuery Programs*

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

Brown University

Browsers are Programmable, Too


Firefox
Google
New Tab
Google
Google
Google Search
I'm Feeling Lucky
Google


Firefox
Google
Private Browsing
Google
Bank of America
Sign In
Main Menu
Enter Online ID:
Online ID:
Save this Online Id
No
for this session.
keep any browser history, search history,
s, or temporary internet files. However,
ke will be kept.
top Private Browsing, or close Firefox.
While this computer won't have a record of your browsing history, your internet service provider or employer can still track the pages you visit.
Learn More

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

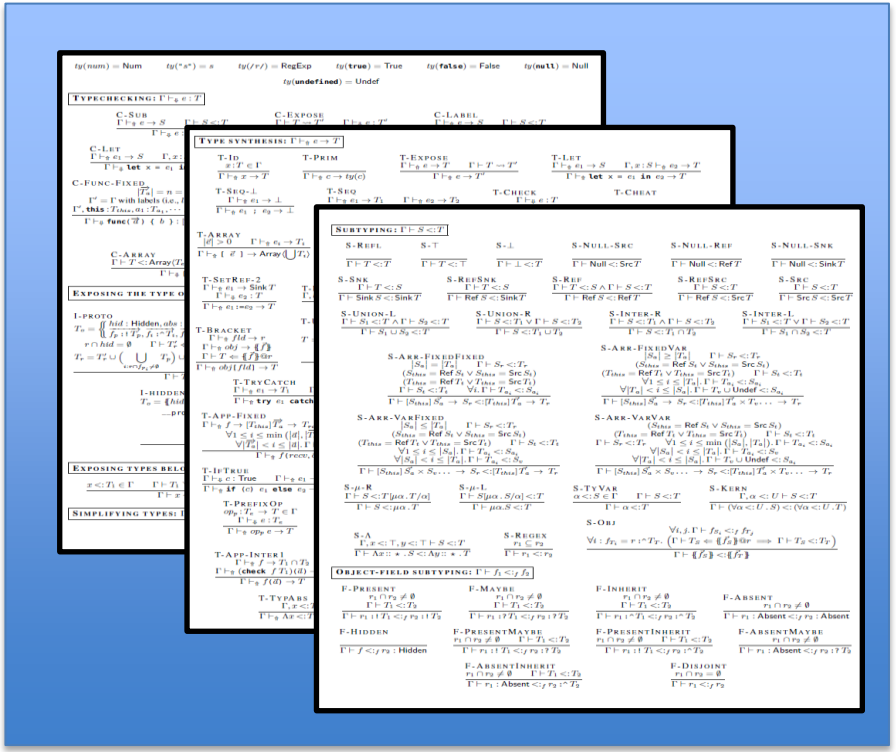
Benjamin S. Lerner
Brown University
blerner@cs.brown.edu

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

Arjun Guha
Cornell University
arjun@cs.cornell.edu

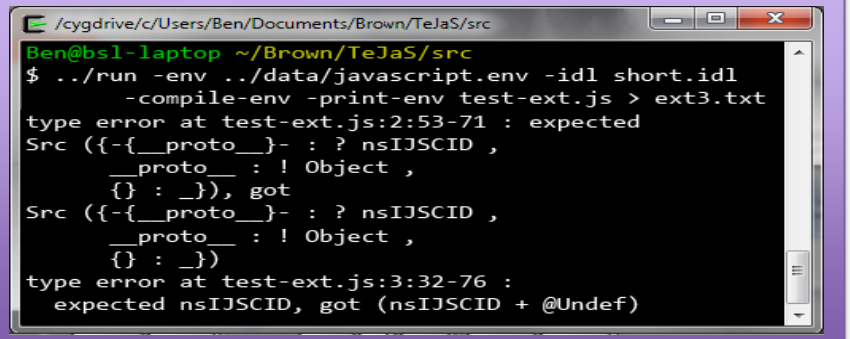
Shriram Krishnamurthi
Brown University
sk@cs.brown.edu

```
module Base_TypeSystem = struct
```



```
end
```

```
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?

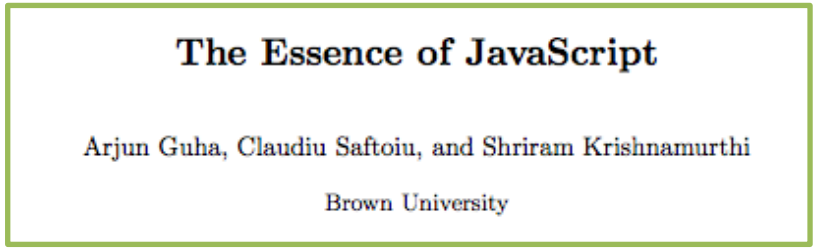
JavaScript program

desugar

λ_{JS} program

browser engines

small interpreter



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

0CFA, Fujitsu Labs (patent pending)

Formal Specification of JavaScript Modules, KAIST

tools

Our Web S(u)ite

github.com/brownplt

www.jswebtools.org