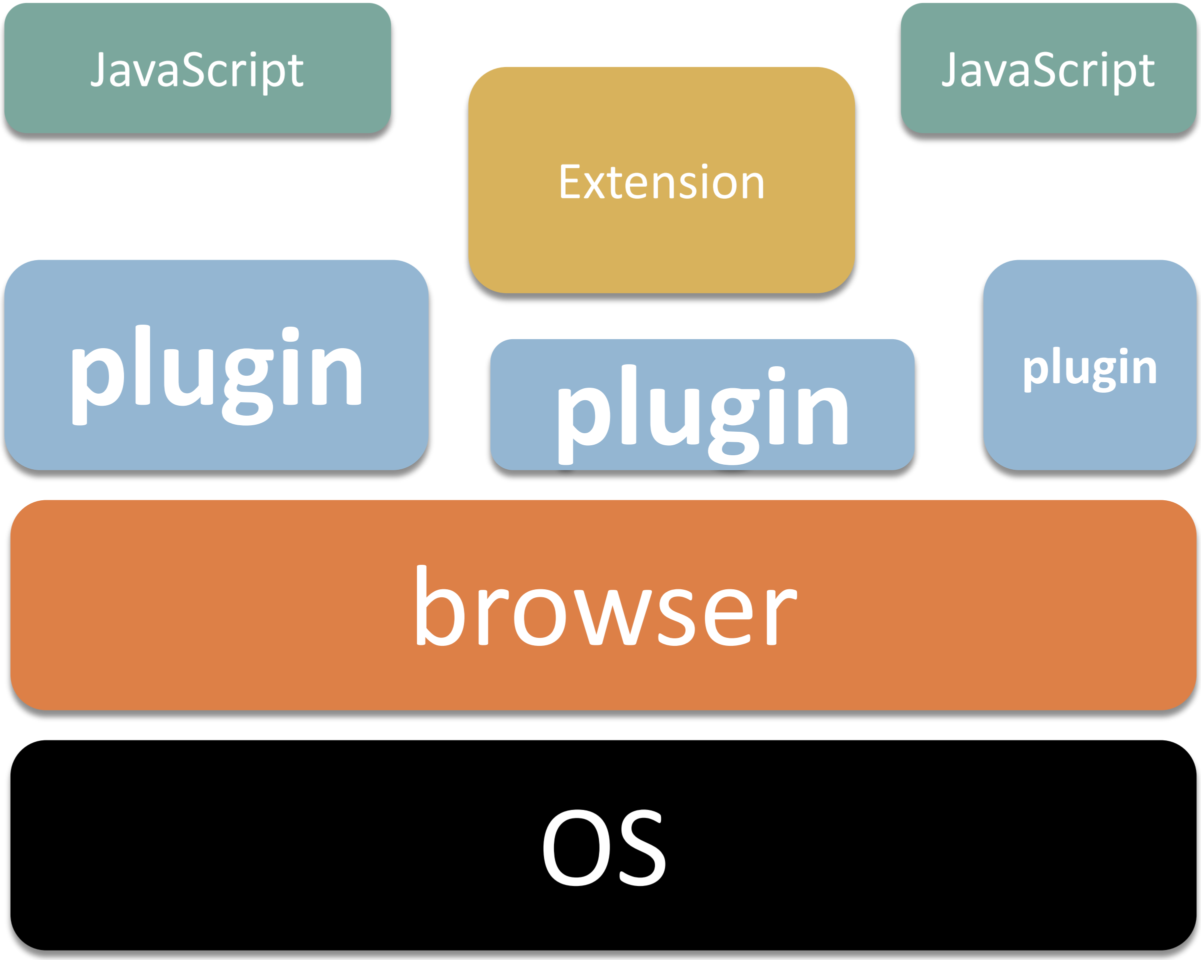
CLIENT-SIDE STATIC ANALYSIS

Ben Livshits, Microsoft Research

Overview of Today’s Lecture

- Client-side JavaScript
  - Analysis of JavaScript
  - `eval` and code obfuscation
  - Need for runtime enforcement
- Gatekeeper as illustration
- Browser
  - Plugins
- Extensions
  - Firefox extension model
  - Chrome extension model
  - Looking forward

Layers of Browser Security



JavaScript

Extension

JavaScript

plugin

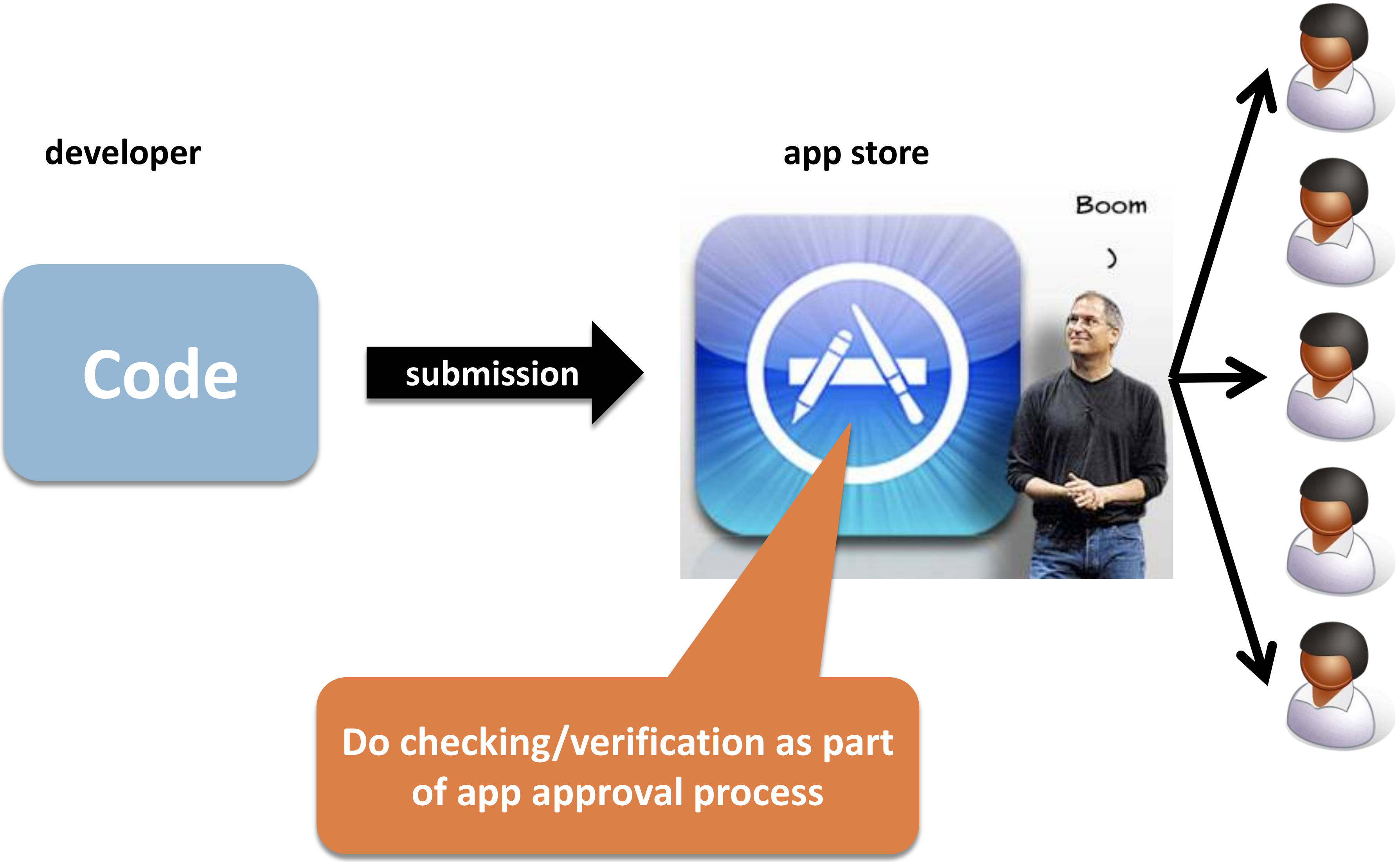
plugin

plugin

browser

OS

App Store: Centralized Software Distribution



developer

Code

submission

app store

Do checking/verification as part of app approval process

Static Analysis

Last time

- Server-side analysis
- Benign but buggy code

Today

- Client-side analysis
- Buggy or **potentially malicious code**

Analysis soundness really helps

Same Origin Policy Is Not Enough

- Primary focus: statically enforcing security and reliability policies for JavaScript code

- These policies include semantic properties
  - restricting widget capabilities,
  - making sure built-in objects are not modified,
  - preventing code injection attempts,
  - redirect and cross-site scripting detection,
  - preventing global namespace pollution,
  - taint checking,
  - etc.

- Soundly enforcing security policies is hard

Gatekeeper

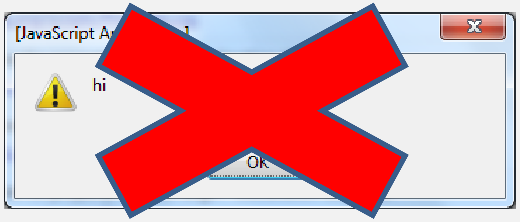
Mostly Static Enforcement of
Security & Reliability Policies for JavaScript Code

Catch me if you can

```
alert('hi');
```

program

malicious



hi

don't want to allow alert box

?

can we figure this out statically?

```
alert(‘hi’);
```

```
document.write(
“<script>alert(‘hi’);</script>”);
```

```
      var d = document;
      var w = d.write;
      w(“<script>alert(‘hi’);”);
```

```
eval(“do”+”cu”+”ment.write(”+…
```

```
var e = window.eval;
e(“do”+”cu”+”ment.write(”…”);
var e = new Function(“eval”);
e.call(
    “do”+”cu”+”ment.write(”…”);
```

```
var e = new
  Function(unescape(“%65%76%61%6C”));
  e.call(“do”+”cu”+”ment.write(”…”);
```

Gatekeeper

Static analysis for JavaScript

- General technology we developed for JavaScript
- Can use for performance optimizations, etc.

This paper

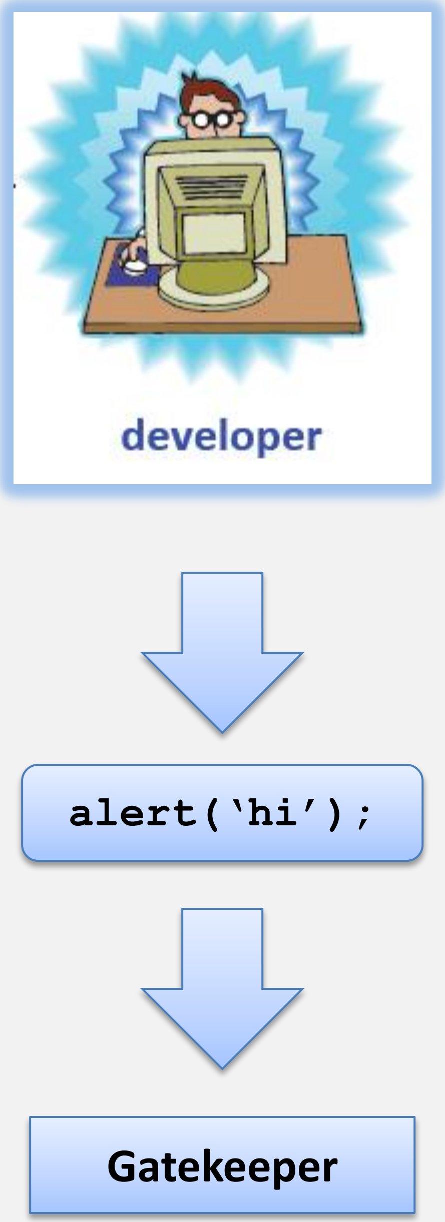
- Use to enforce security and reliability policies
- Analyze Web widgets

Focus on *whole program analysis*. Contrast with:

- JavaScript language subsets (do a little of)
- JavaScript code rewriting (do a little of)

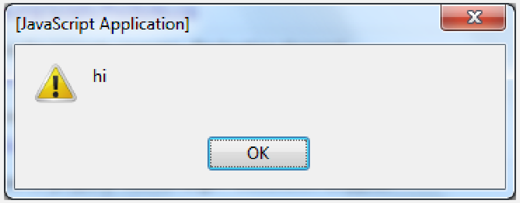
Goal of Gatekeeper:

Reason about JavaScript code statically



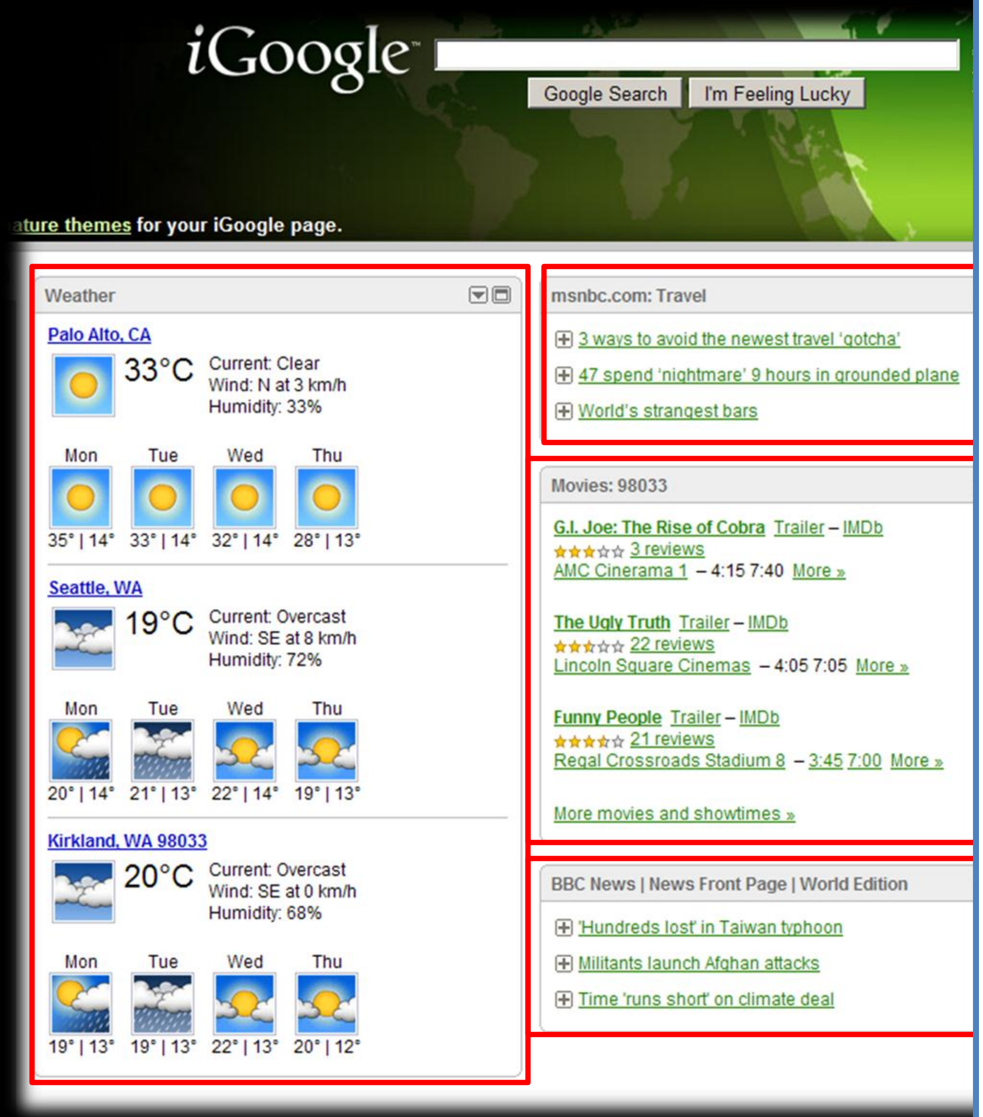
alert('hi');

Gatekeeper


[JavaScript Application]

hi

JavaScript Widgets



ature themes for your iGoogle page.

Weather

Palo Alto, CA
33°C Current: Clear
Wind: N at 3 km/h
Humidity: 33%

Mon	Tue	Wed	Thu
35° | 14°	33° | 14°	32° | 14°	28° | 13°

Seattle, WA
19°C Current: Overcast
Wind: SE at 8 km/h
Humidity: 72%

Mon	Tue	Wed	Thu
20° | 14°	21° | 13°	22° | 14°	19° | 13°

Kirkland, WA 98033
20°C Current: Overcast
Wind: SE at 0 km/h
Humidity: 68%

Mon	Tue	Wed	Thu
19° | 13°	19° | 13°	22° | 13°	20° | 12°

msnbc.com: Travel

- 3 ways to avoid the newest travel 'gotcha'
- 47 spend 'nightmare' 9 hours in grounded plane
- World's strangest bars

Movies: 98033

G.I. Joe: The Rise of Cobra Trailer – IMDb
★★★☆☆ 3 reviews
AMC Cinerama 1 – 4:15 7:40 More »

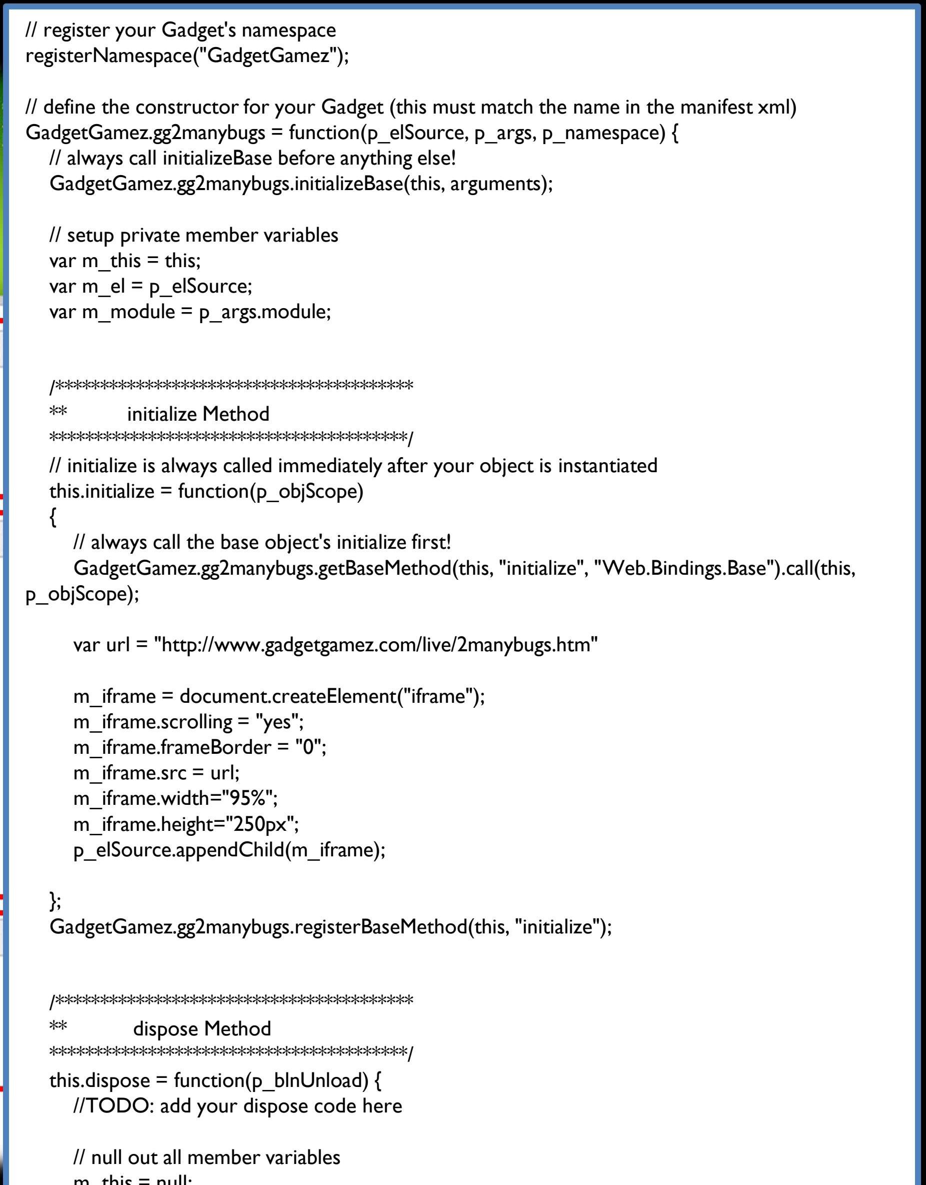
The Ugly Truth Trailer – IMDb
★★☆☆☆ 22 reviews
Lincoln Square Cinemas – 4:05 7:05 More »

Funny People Trailer – IMDb
★★★☆☆ 21 reviews
Regal Crossroads Stadium 8 – 3:45 7:00 More »

More movies and showtimes »

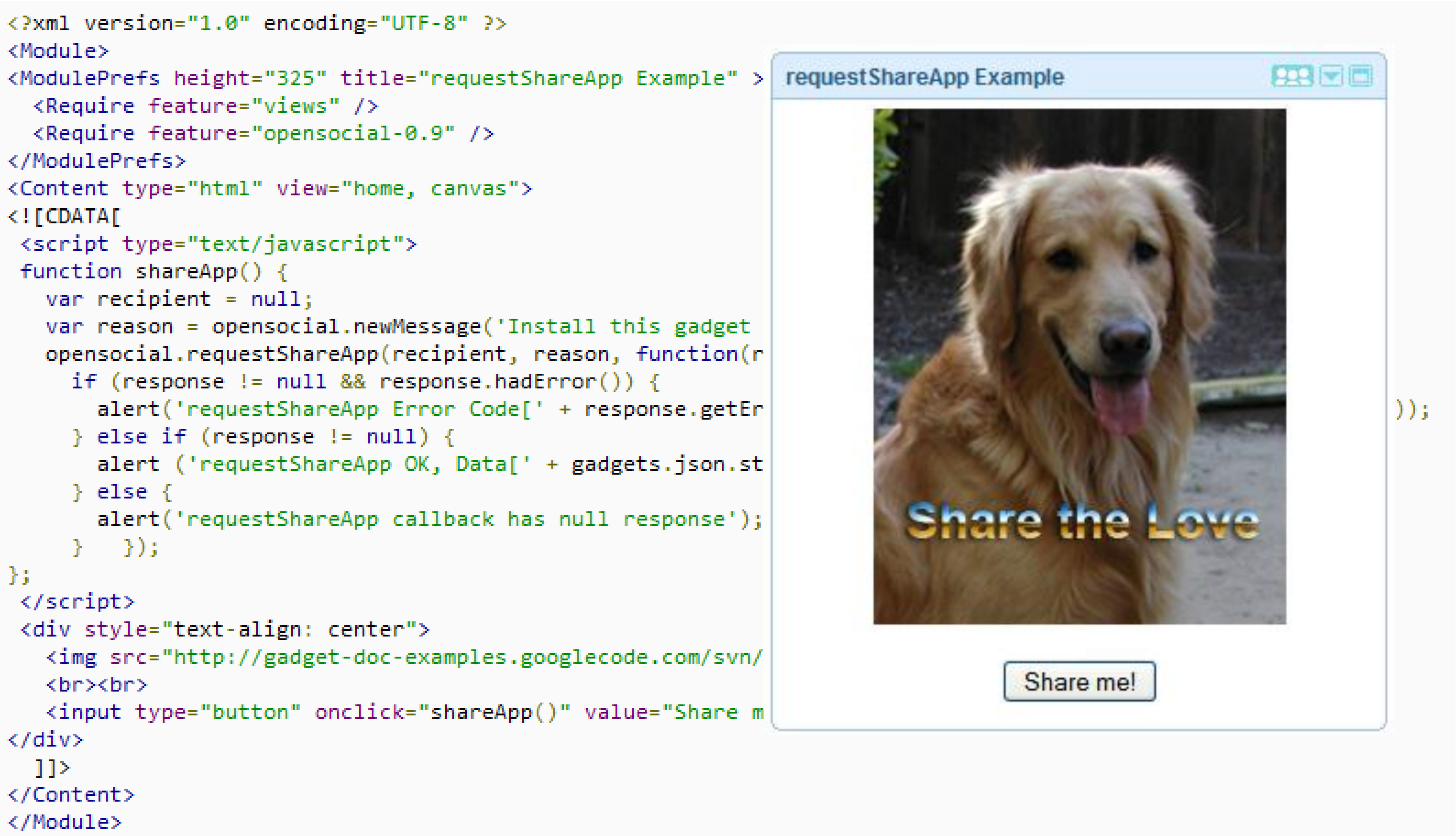
BBC News | News Front Page | World Edition

- 'Hundreds lost' in Taiwan typhoon
- Militants launch Afghan attacks
- Time 'runs short' on climate deal



```
// register your Gadget's namespace
registerNamespace("GadgetGamez");

// define the constructor for your Gadget (this must match the name in the manifest xml)
GadgetGamez.gg2manybugs = function(p_elSource, p_args, p_namespace) {
    // always call initializeBase before anything else!
    GadgetGamez.gg2manybugs.initializeBase(this, arguments);

    // setup private member variables
    var m_this = this;
    var m_el = p_elSource;
    var m_module = p_args.module;


    /****************************************
    **          initialize Method
    ****************************************/
    // initialize is always called immediately after your object is instantiated
    this.initialize = function(p_objScope)
    {
        // always call the base object's initialize first!
        GadgetGamez.gg2manybugs.getBaseMethod(this, "initialize", "Web.Bindings.Base").call(this,
p_objScope);

        var url = "http://www.gadgetgamez.com/live/2manybugs.htm"

        m_iframe = document.createElement("iframe");
        m_iframe.scrolling = "yes";
        m_iframe.frameBorder = "0";
        m_iframe.src = url;
        m_iframe.width="95%";
        m_iframe.height="250px";
        p_elSource.appendChild(m_iframe);

    };
    GadgetGamez.gg2manybugs.registerBaseMethod(this, "initialize");


    /****************************************
    **          dispose Method
    ****************************************/
    this.dispose = function(p_blnUnload) {
        //TODO: add your dispose code here

        // null out all member variables
        m_this = null;
```

Sample iGoogle Gadget

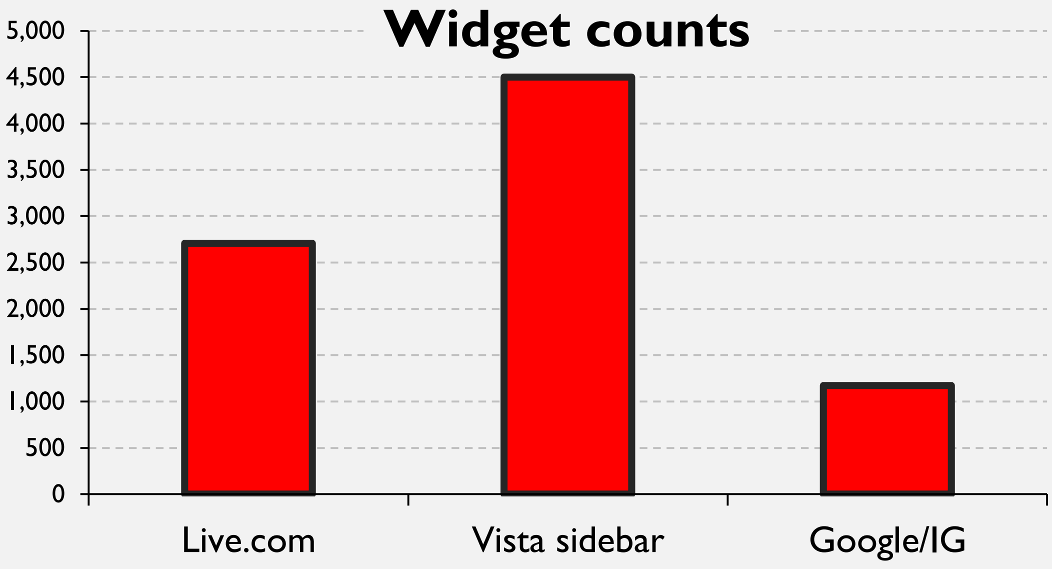


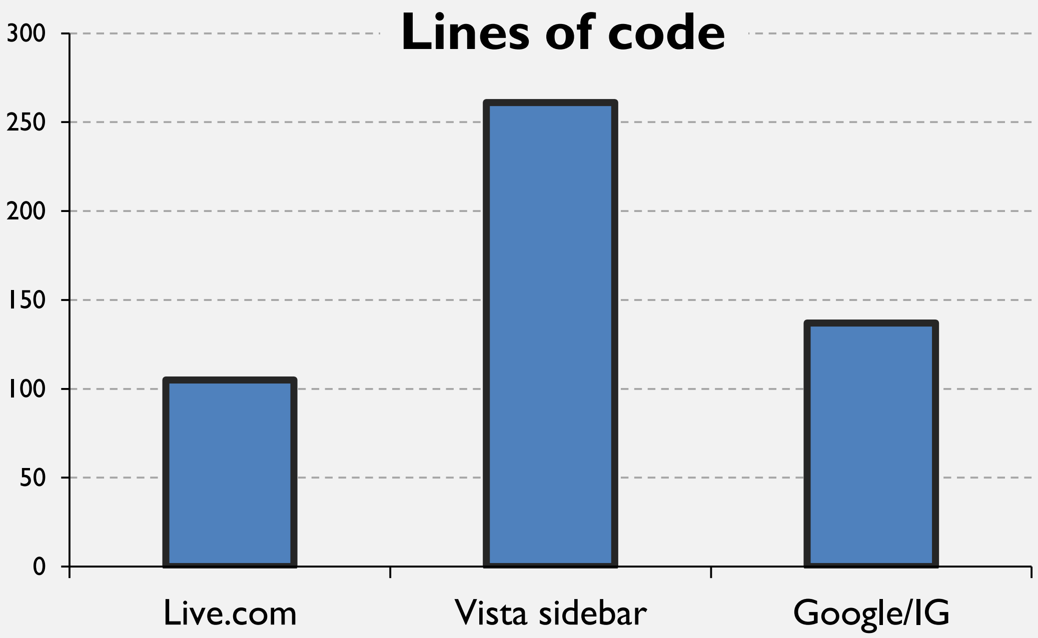
```
<?xml version="1.0" encoding="UTF-8" ?>
<Module>
<ModulePrefs height="325" title="requestShareApp Example" >
  <Require feature="views" />
  <Require feature="opensocial-0.9" />
</ModulePrefs>
<Content type="html" view="home, canvas">
<![CDATA[
 <script type="text/javascript">
 function shareApp() {
   var recipient = null;
   var reason = opensocial.newMessage('Install this gadget
   opensocial.requestShareApp(recipient, reason, function(r
     if (response != null && response.hadError()) {
       alert('requestShareApp Error Code[' + response.getEr                                   ));
     } else if (response != null) {
       alert ('requestShareApp OK, Data[' + gadgets.json.st
     } else {
       alert('requestShareApp callback has null response');
     }   });
};
 </script>
 <div style="text-align: center">
   <img src="http://gadget-doc-examples.googlecode.com/svn/
   <br><br>
   <input type="button" onclick="shareApp()" value="Share m
</div>
  ]]>
</Content>
</Module>
```

requestShareApp Example

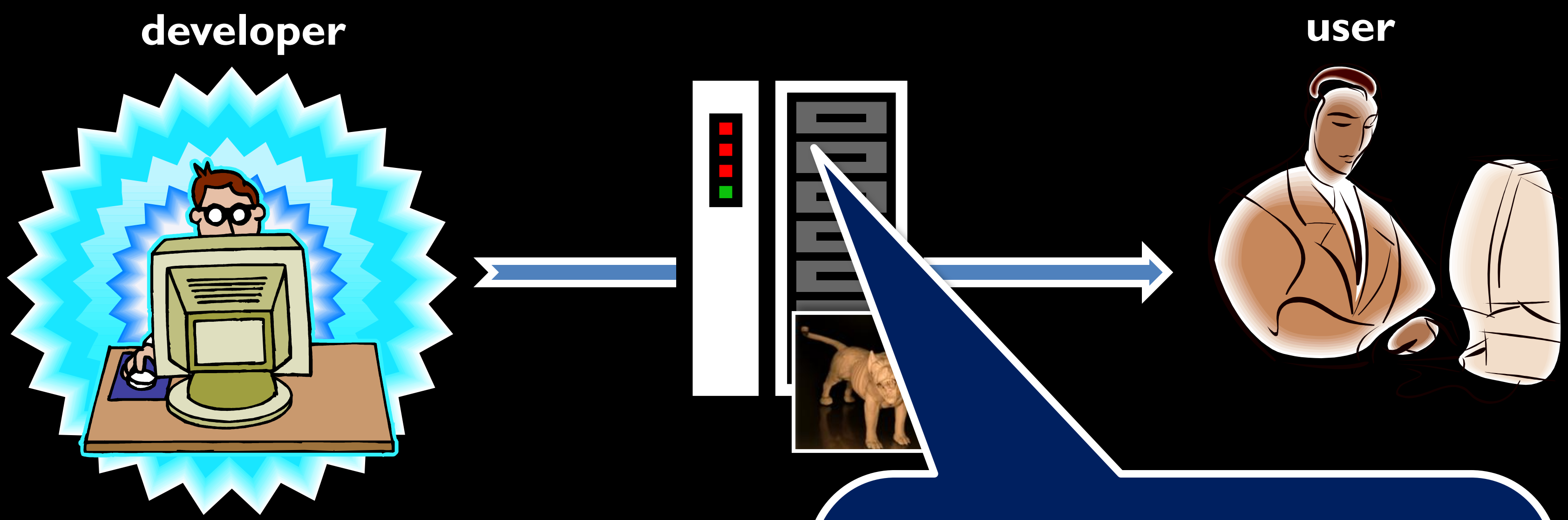
Widgets are everywhere…

We use over 8,500 widgets to evaluate Gatekeeper





Gatekeeper: Deployment Step on Widget Host



Widget:

```
    …
    alert('hi');
    …
```

Hosting site: control widgets by enforcing policies:

- No alert
- No redirects
- No document.write

Outline

- **Statically analyzable subset JavaScript$_{\textbf{SAFE}}$**
- **Points-to analysis for JavaScript**
- **Formulate nine security & reliability policies**
- **Experiments**

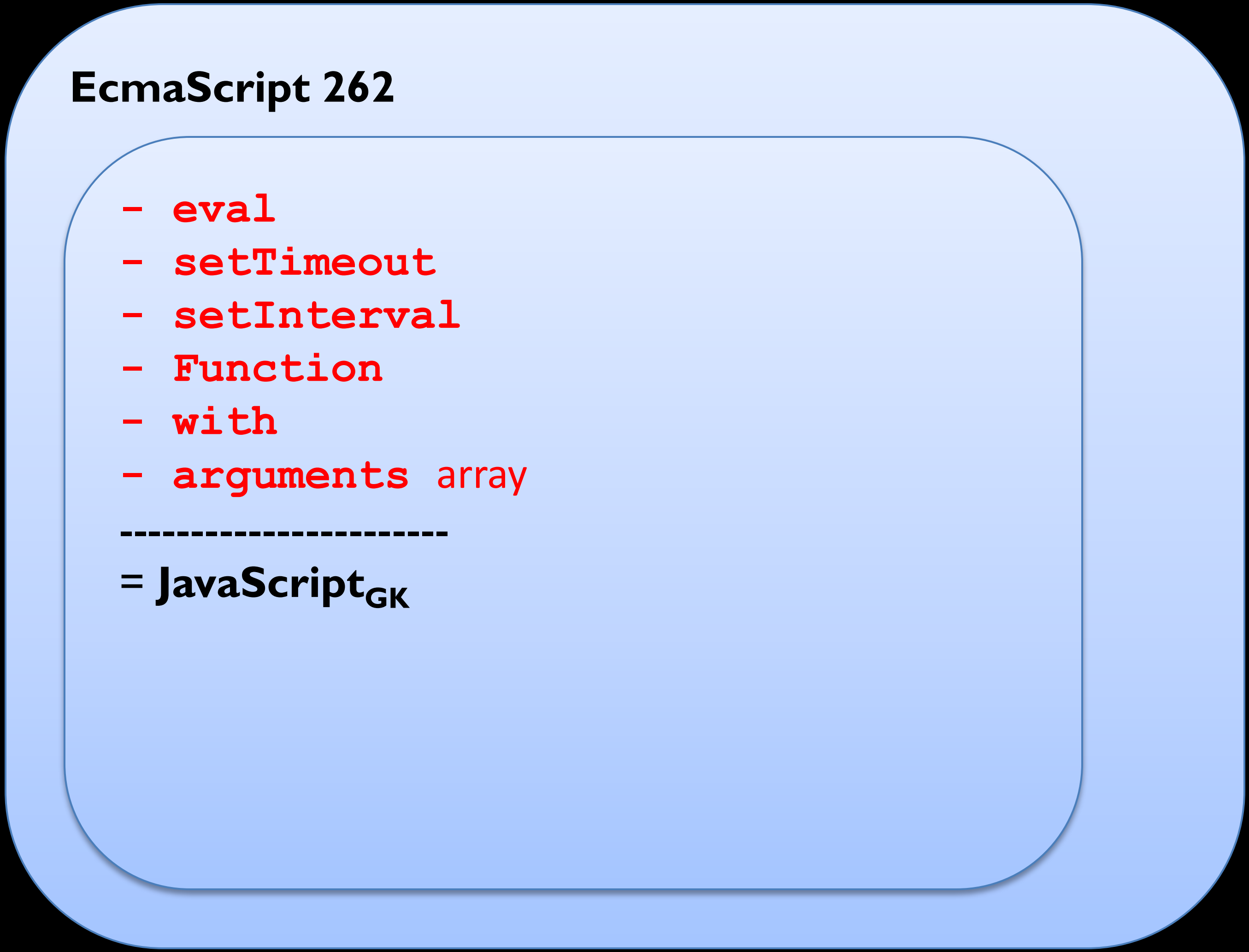
Techniques

Start with Entire JavaScript…

EcmaScript-262

```
var e = new Function(“eval”);
e.call(
    “do”+”cu”+”ment.write(”…”);

var e = new
  Function(unescape(“%65%76%61%6C”));
  e.call(“do”+”cu”+”ment.write(”…”);
```

Remove `eval` & Friends…



EcmaScript 262

`- eval`

`- setTimeout`

`- setInterval`

`- Function`

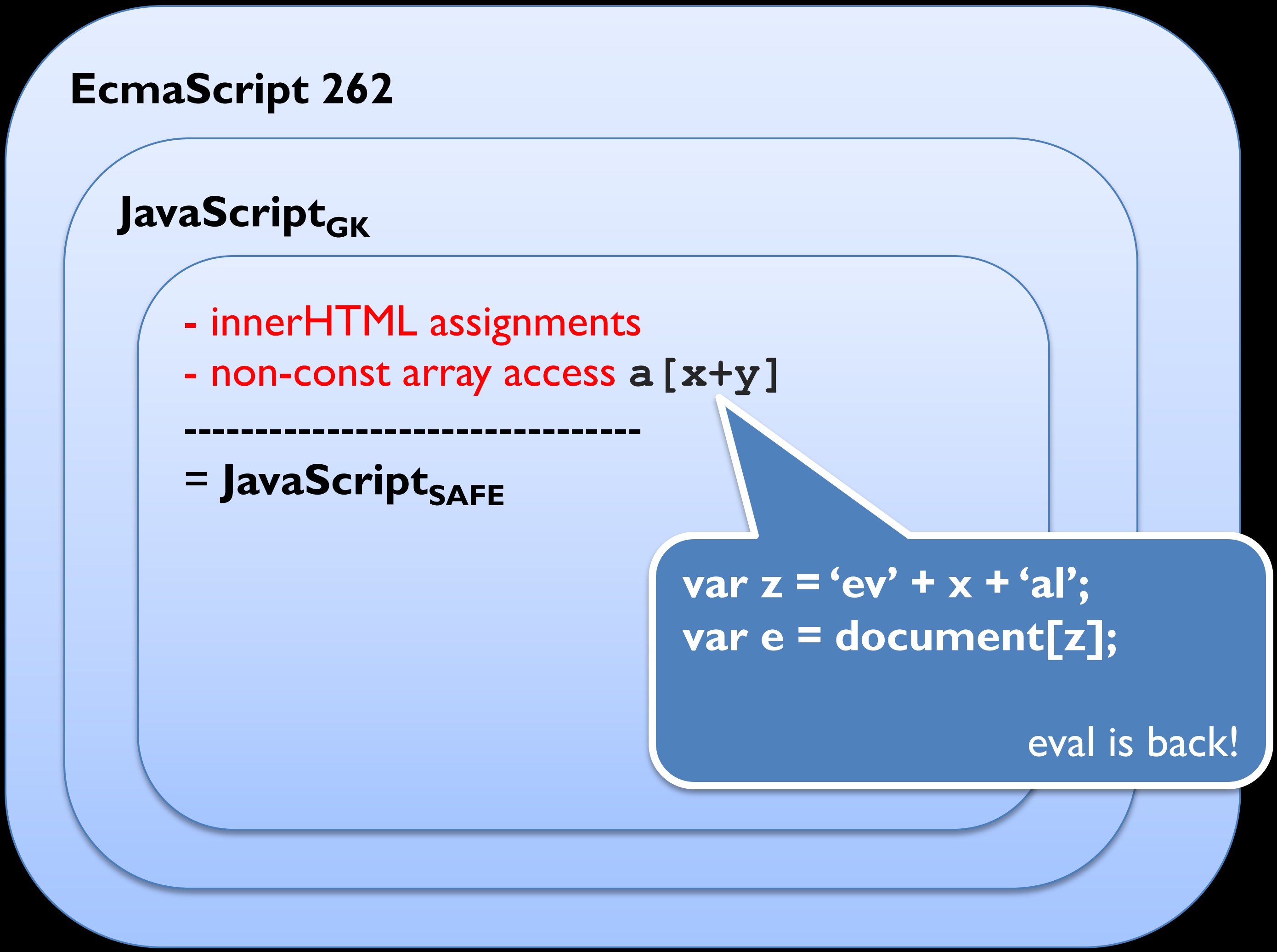
`- with`

`- arguments` array

-----------------------

= **JavaScript$_{GK}$**

Remove Unresolved Array Accesses…



EcmaScript 262

JavaScript$_{GK}$

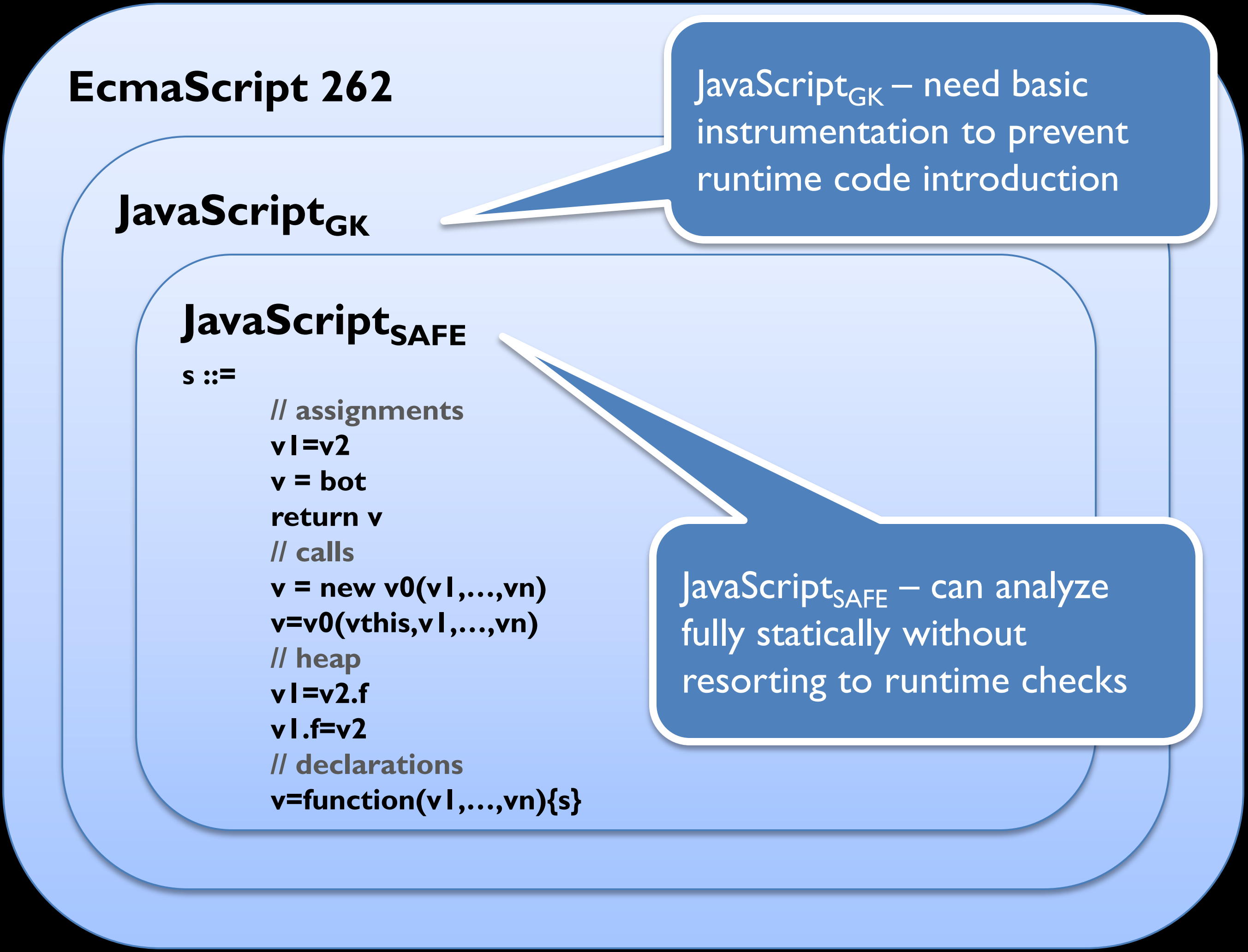
- innerHTML assignments
- non-const array access `a[x+y]`

= **JavaScript$_{SAFE}$**

```
var z = ‘ev’ + x + ‘al’;
var e = document[z];
```

eval is back!

Now, this is Amenable to Analysis!



EcmaScript 262

JavaScript$_{GK}$

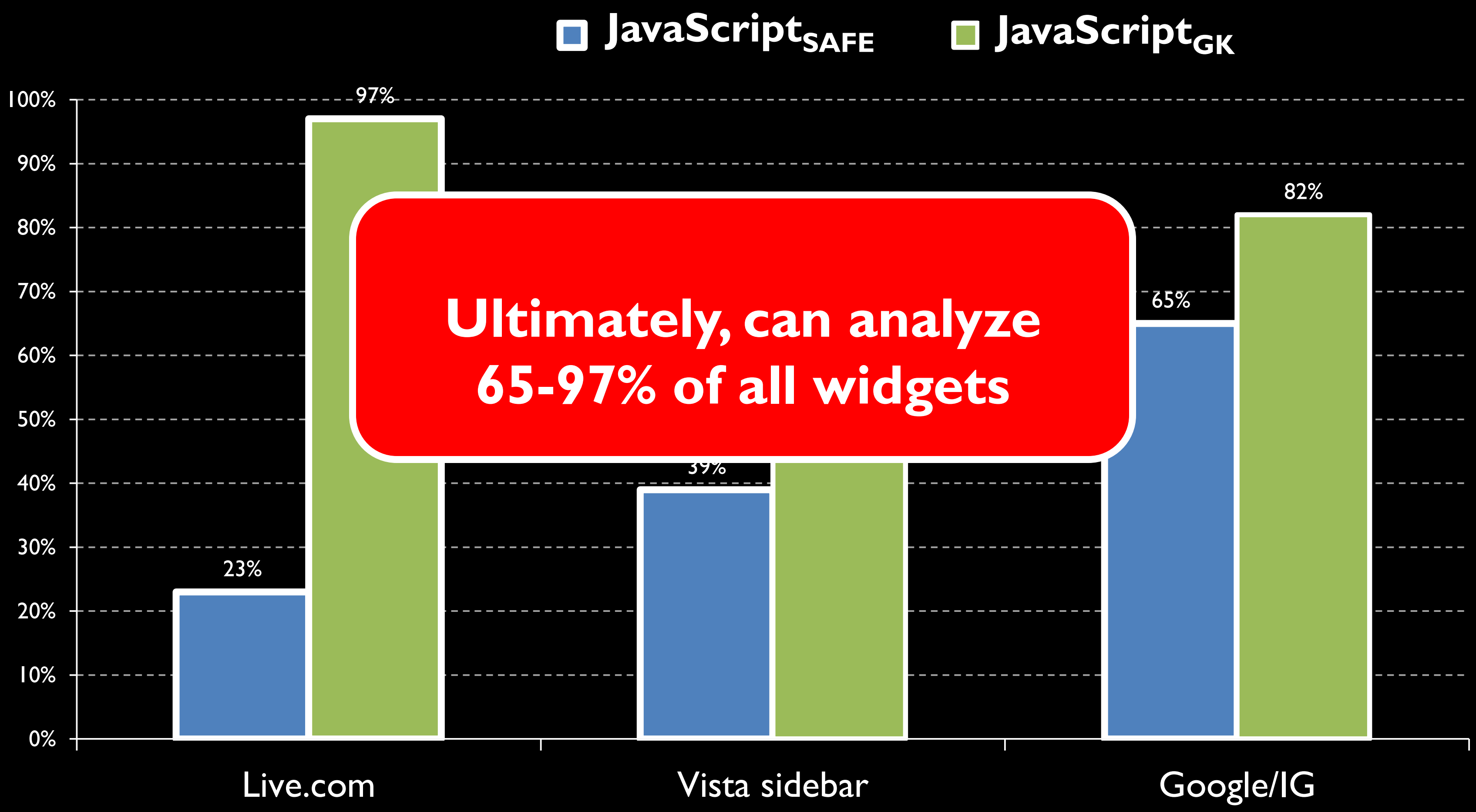
JavaScript$_{SAFE}$

```
s ::=
        // assignments
        v1=v2
        v = bot
        return v
        // calls
        v = new v0(v1,…,vn)
        v=v0(vthis,v1,…,vn)
        // heap
        v1=v2.f
        v1.f=v2
        // declarations
        v=function(v1,…,vn){s}
```

JavaScript$_{GK}$ – need basic instrumentation to prevent runtime code introduction

JavaScript$_{SAFE}$ – can analyze fully statically without resorting to runtime checks

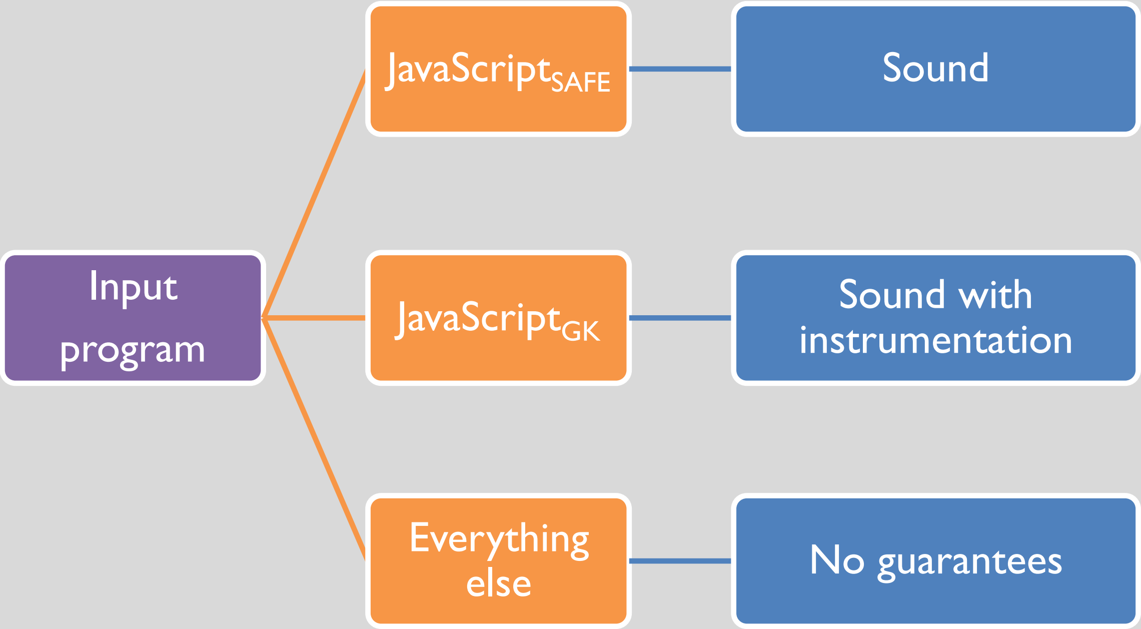
How Many Widgets are in the Subsets?



Ultimately, can analyze 65-97% of all widgets

Sound analysis:

ensures that our policy checkers find *all* violations



Input program

$\text{JavaScript}_{\text{SAFE}}$

Sound

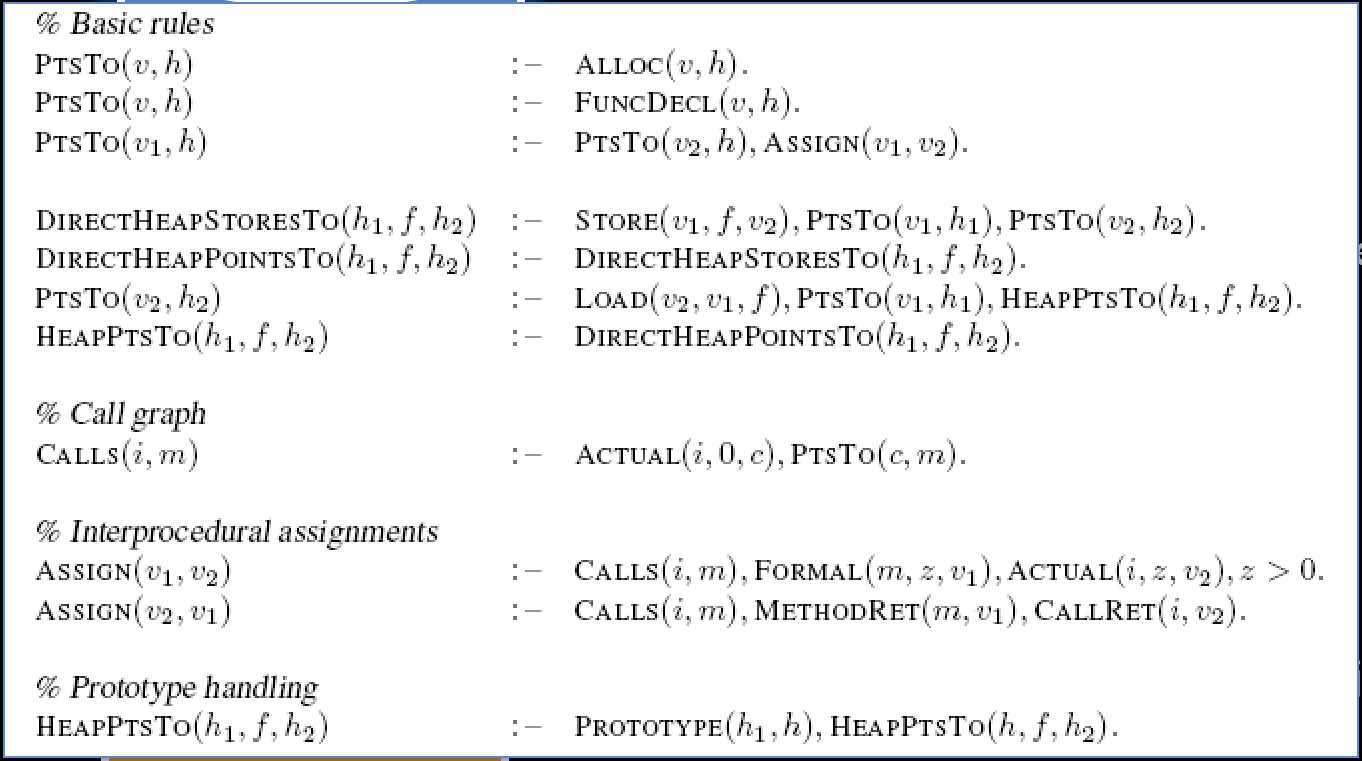
$\text{JavaScript}_{\text{GK}}$

Sound with instrumentation

Everything else

No guarantees

Points-to Analysis in Gatekeeper



% Basic rules

$\textsc{PtsTo}(v, h)$:− $\textsc{Alloc}(v, h)$.

$\textsc{PtsTo}(v, h)$:− $\textsc{FuncDecl}(v, h)$.

$\textsc{PtsTo}(v_1, h)$:− $\textsc{PtsTo}(v_2, h), \textsc{Assign}(v_1, v_2)$.

$\textsc{DirectHeapStoresTo}(h_1, f, h_2)$:− $\textsc{Store}(v_1, f, v_2), \textsc{PtsTo}(v_1, h_1), \textsc{PtsTo}(v_2, h_2)$.

$\textsc{DirectHeapPointsTo}(h_1, f, h_2)$:− $\textsc{DirectHeapStoresTo}(h_1, f, h_2)$.

$\textsc{PtsTo}(v_2, h_2)$:− $\textsc{Load}(v_2, v_1, f), \textsc{PtsTo}(v_1, h_1), \textsc{HeapPtsTo}(h_1, f, h_2)$.

$\textsc{HeapPtsTo}(h_1, f, h_2)$:− $\textsc{DirectHeapPointsTo}(h_1, f, h_2)$.

% Call graph

$\textsc{Calls}(i, m)$:− $\textsc{Actual}(i, 0, c), \textsc{PtsTo}(c, m)$.

% Interprocedural assignments

$\textsc{Assign}(v_1, v_2)$:− $\textsc{Calls}(i, m), \textsc{Formal}(m, z, v_1), \textsc{Actual}(i, z, v_2), z > 0$.

$\textsc{Assign}(v_2, v_1)$:− $\textsc{Calls}(i, m), \textsc{MethodRet}(m, v_1), \textsc{CallRet}(i, v_2)$.

% Prototype handling

$\textsc{HeapPtsTo}(h_1, f, h_2)$:− $\textsc{Prototype}(h_1, h), \textsc{HeapPtsTo}(h, f, h_2)$.

e fly

in Datalog

Datalog Policy for Preventing `document.write`

```
DocumentWrite(i) :-
   PointsTo("global", h1),
   HeapPointsTo(h1, "document", h2),
   HeapPointsTo(h2, "write", h3),
   Calls(i, h3).
```

```
document.write('<iframe id="dynstuff" src=""
'+iframeprops+'></iframe>')
```

Experimental Evaluation

Policies for Widget Security & Reliability

36 lines

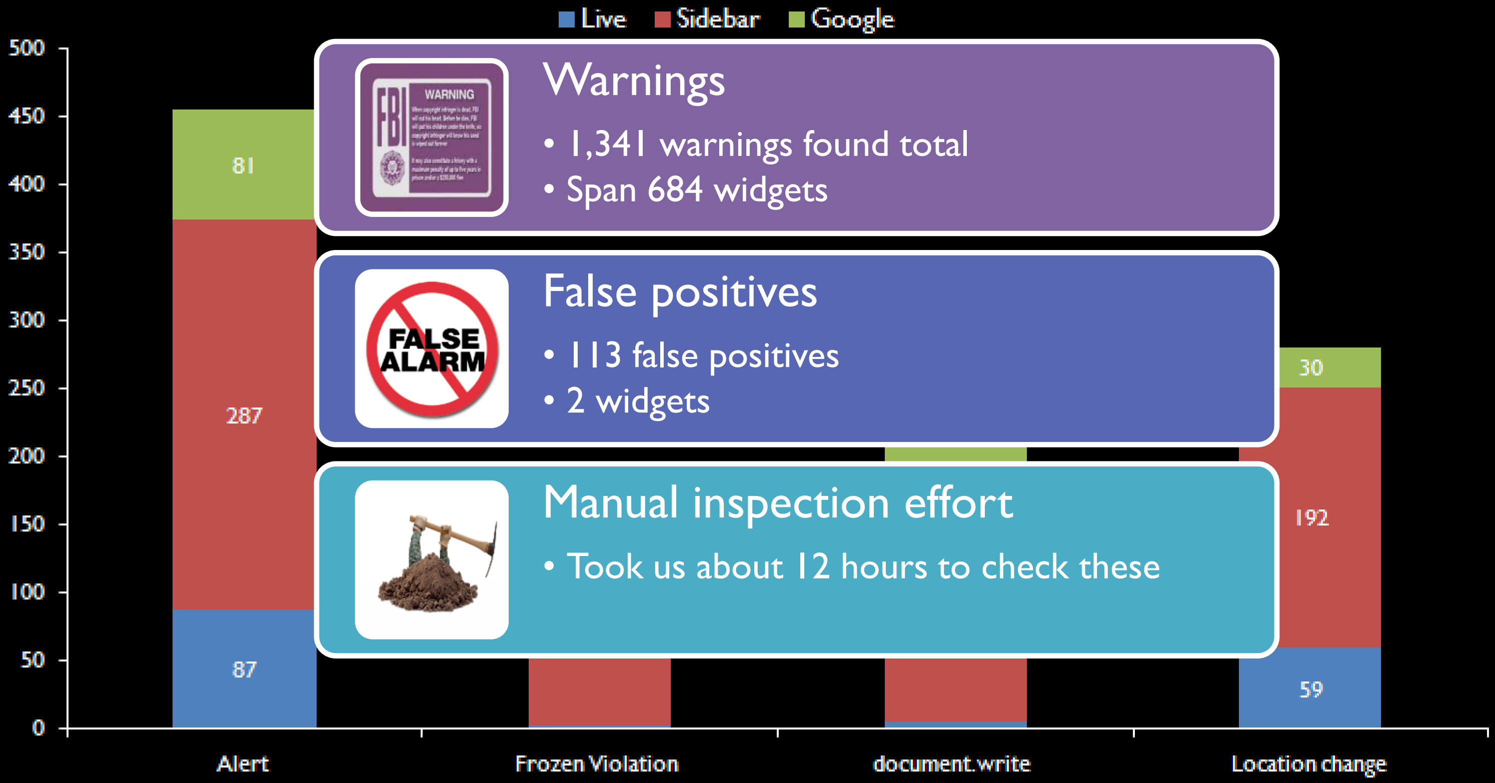
```
AlertCalls(i)    :- PointsTo("global", h), HeapPointsTo(h, "alert", h2), Calls(i, h2) .

DocumentWrite(i)    :- PointsTo("global", h1), HeapPointsTo(h1, "document", h2), HeapPointsTo(h2, "write", h3), Calls(i, h3) .
DocumentWrite(i)    :- PointsTo("global", h1), HeapPointsTo(h1, "document", h2), HeapPointsTo(h2, "writeln", h3), Calls(i, h3) .
InnerHTML(v)        :- Store(v, "innerHtml", _) .

BuiltinObject(h) :- PointsTo("global", h1), HeapPointsTo(h1, "String", h) .
BuiltinObject(h) :- PointsTo("global", h1), HeapPointsTo(h1, "Date", h) .
BuiltinObject(h) :- PointsTo("global", h1), HeapPointsTo(h1, "Array", h) .
BuiltinObject(h) :- PointsTo("global", h1), HeapPointsTo(h1, "Boolean", h) .
BuiltinObject(h) :- PointsTo("global", h1), HeapPointsTo(h1, "Math", h) .

BuiltinObject(h) :- PointsTo("global", h1), HeapPointsTo(h1, "Function", h) .
BuiltinObject(h) :- PointsTo("global", h1), HeapPointsTo(h1, "Document", h) .
BuiltinObject(h) :- PointsTo("global", h1), HeapPointsTo(h1, "Window", h) .

Reaches(h1, f, h2) :- HeapPointsTo(h1, f, h2) .
Reaches(h1, f, h2) :- HeapPointsTo(h1, _, h), Reaches(h, f, h2) .

FrozenViolation(v, h1) :- Store(v, _, _), PointsTo(v, h1), BuiltinObject(h1) .
FrozenViolation(v, h1) :- Store(v, _, _), PointsTo(v, h1), BuiltinObject(h2), Reaches(h2, f, h1) .

LocationObject(h)         :- PointsTo("global", h1), HeapPointsTo(h1, "location", h) .
WindowObject(h)            :- PointsTo("global", h1), HeapPointsTo(h1, "window", h) .

StoreToLocationObject(h)  :- PointsTo("global", h1), HeapPointsTo(h1, "window", h2), DirectHeapStoreTo(h2, "location", h) .
StoreToLocationObject(h)  :- PointsTo("global", h1), HeapPointsTo(h1, "document", h2), DirectHeapStoreTo(h2, "location", h) .
StoreToLocationObject(h)  :- PointsTo("global", h1), DirectHeapStoreTo(h1, "location", h) .

StoreInLocationObject(h)  :- LocationObject(h1), DirectHeapStoreTo(h1, _, h) .

CallLocationMethod(i)     :- LocationObject(h), HeapPointsTo(h, "assign", h1), Calls(i, h1) .
CallLocationMethod(i)     :- LocationObject(h), HeapPointsTo(h, "reload", h1), Calls(i, h1) .
CallLocationMethod(i)     :- LocationObject(h), HeapPointsTo(h, "replace", h1), Calls(i, h1) .

WindowOpenMethodCall(i)   :- WindowObject(h1), HeapPointsTo(h1, "open", h2), Calls(i, h2) .
```

pply to all
widgets

e.com only

a Sidebar only

Policy Checking Results



Warnings

- 1,341 warnings found total
- Span 684 widgets

False positives

- 113 false positives
- 2 widgets

Manual inspection effort

- Took us about 12 hours to check these

False Positives

common.js:

```
function MM_preloadImages() {
 var d=m_Doc;
 if(d.images){
   if(!d.MM_p) d.MM_p=new Array();
   var i,j=d.MM_p.length,

a=MM_preloadImages.arguments;
   for(i=0; i<a.length; i++)
     if (a[i].indexOf("#")!=0){
       d.MM_p[j]=new Image;
       d.MM_p[j++].src=a[i];
     }
   }
}
```

- Why not more false positives?
  - Most violations are local
  - But this is policy-specific – a global taint policy might produce other results

Conclusions

Gatekeeper: Static analysis for JavaScript

Technique: points-to analysis

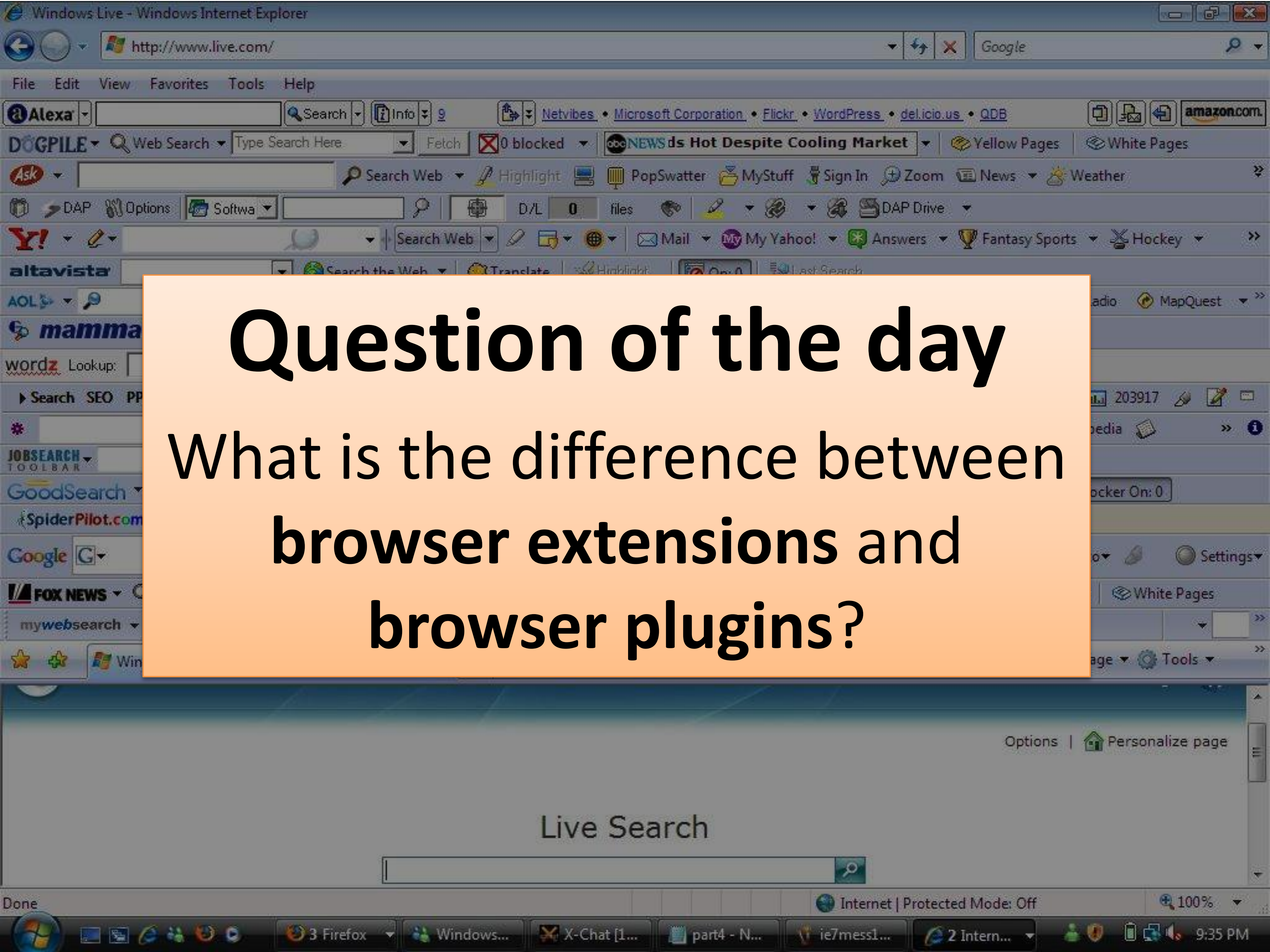
Focus: analyzing widgets

Results:

- **1,341 policy violations**
- **false positives affect 2 widgets**

Question of the day

What is the difference between **browser extensions** and **browser plugins?**


Windows Live - Windows Internet Explorer
http://www.live.com/
Google
File Edit View Favorites Tools Help
Alexa Search Info 9 Netvibes • Microsoft Corporation • Flickr • WordPress • del.icio.us • QDB amazon.com
DOGPILE Web Search Type Search Here Fetch 0 blocked NEWS ds Hot Despite Cooling Market Yellow Pages White Pages
Ask Search Web Highlight PopSwatter MyStuff Sign In Zoom News Weather
DAP Options Softwa D/L 0 files DAP Drive
Y! Search Web Mail My Yahoo! Answers Fantasy Sports Hockey
altavista Search the Web Translate Highlight On: 0 Last Search
AOL adio MapQuest
mamma
wordz Lookup:
Search SEO PP 203917
pedia
JOBSEARCH TOOLBAR
GoodSearch ocker On: 0
SpiderPilot.com
Google G Settings
FOX NEWS White Pages
mywebsearch
Win age Tools
Options | Personalize page
Live Search
Done
Internet | Protected Mode: Off
100%
3 Firefox Windows... X-Chat [1... part4 - N... ie7mess1... 2 Intern... 9:35 PM

Browser Plugins

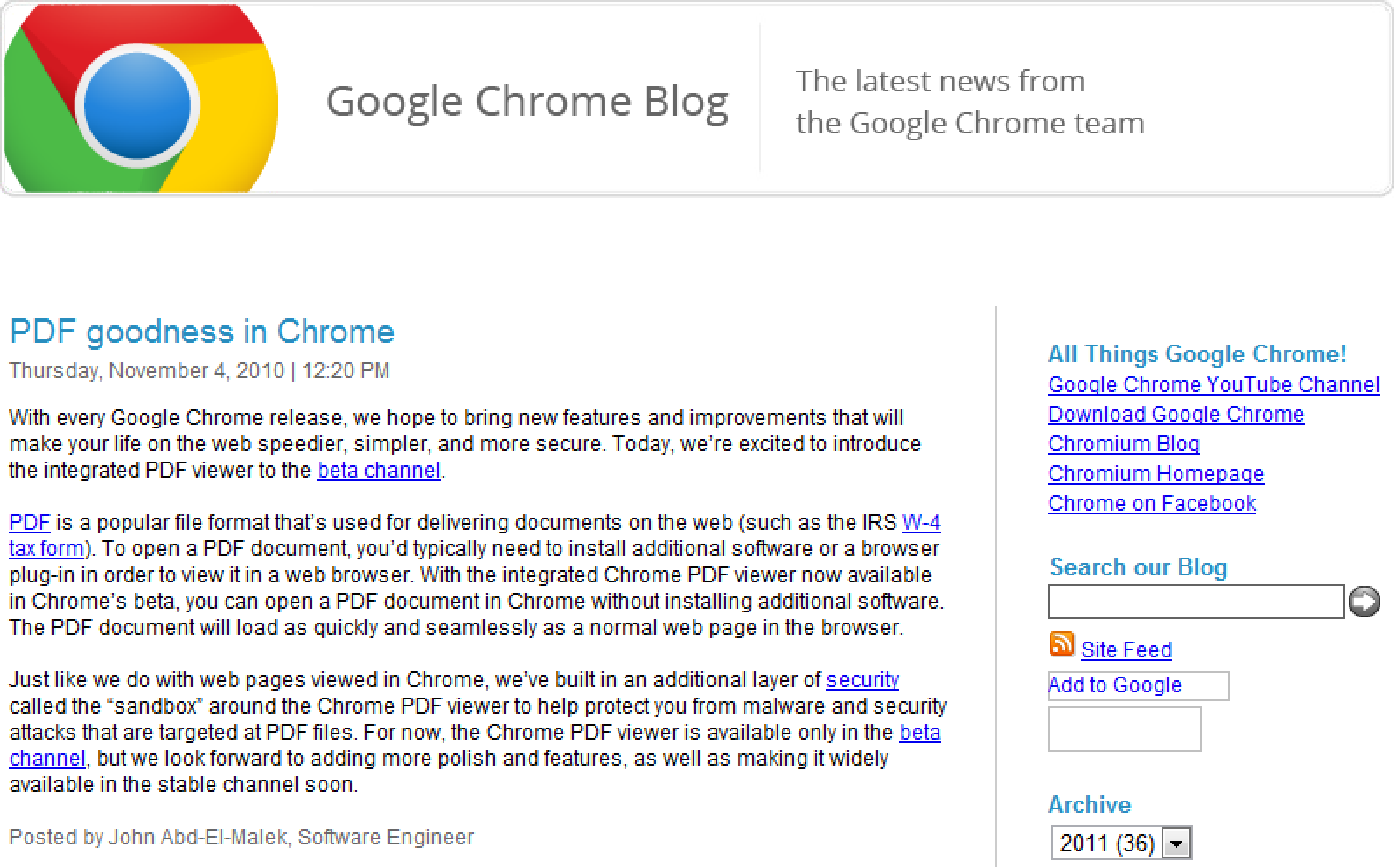
- Plugins
  - Flash
  - Adobe PDF reader
  - On their way out?

- Come in different flavors
  - ActiveX
  - Firefox extensions
  - Chrome extensions

Plugin Security

- Plugins are often worst offenders when it comes to security
  - True of malware
  - Of use of DEP/ASLR
- Isolation technologies proposed
  - Run plugins in their own processes
  - Low privilege processes if possible
- Sandboxing techniques
  - Native client
  - XAX

Plugin Security



PDF goodness in Chrome

Thursday, November 4, 2010 | 12:20 PM

With every Google Chrome release, we hope to bring new features and improvements that will make your life on the web speedier, simpler, and more secure. Today, we're excited to introduce the integrated PDF viewer to the beta channel.

PDF is a popular file format that's used for delivering documents on the web (such as the IRS W-4 tax form). To open a PDF document, you'd typically need to install additional software or a browser plug-in in order to view it in a web browser. With the integrated Chrome PDF viewer now available in Chrome's beta, you can open a PDF document in Chrome without installing additional software. The PDF document will load as quickly and seamlessly as a normal web page in the browser.

Just like we do with web pages viewed in Chrome, we've built in an additional layer of security called the "sandbox" around the Chrome PDF viewer to help protect you from malware and security attacks that are targeted at PDF files. For now, the Chrome PDF viewer is available only in the beta channel, but we look forward to adding more polish and features, as well as making it widely available in the stable channel soon.

Posted by John Abd-El-Malek, Software Engineer

Extension Space: an Overview

- Mozilla Firefox
  - Dominates this space with 1,000s of extensions available
  - Millions of downloads
  - Security is not great: rogue extensions, buggy extensions
  - Relies on a community review process to ensure quality

- Google Chrome
  - Extension manifests
  - Runtime enforcement of manifests within the browser

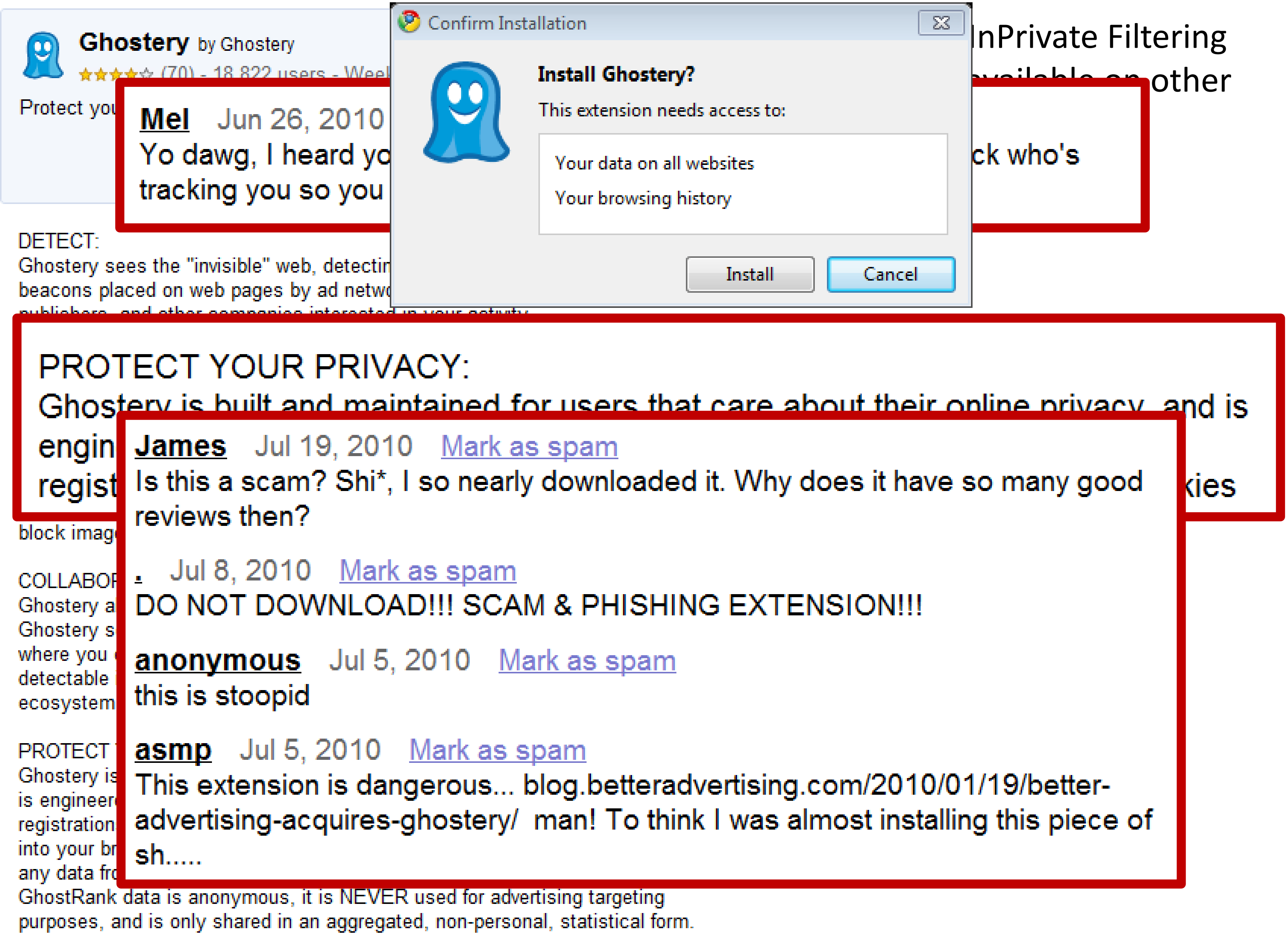
Chrome Access Control Manifest

```
"content_scripts": [
        {
                "all_frames": true,
                "js": ["blocker.js"],
                "matches": ["http://*/*", "https://*/*"]
```

311 of 1,137 featured / popular extensions have access to “your data on all websites”.

```
                "all_frames": true,
                "js": ["scanner.js"],
                "matches": ["http://*/*", "https://*/*"],
                "run_at": "document_idle"
        }
],
```

Question: What do extensions really do?



Ghostery by Ghostery

★★★★☆ (70) - 18,822 users - Weel

Protect you

InPrivate Filtering

other

Mel Jun 26, 2010

Yo dawg, I heard yo ck who's

tracking you so you

Confirm Installation

Install Ghostery?

This extension needs access to:

Your data on all websites

Your browsing history

DETECT:

Ghostery sees the "invisible" web, detectin

beacons placed on web pages by ad netwo

publishers, and other companies interested in your activity.

PROTECT YOUR PRIVACY:

Ghostery is built and maintained for users that care about their online privacy, and is

engin kies

regist

block imag

James Jul 19, 2010 Mark as spam

Is this a scam? Shi*, I so nearly downloaded it. Why does it have so many good reviews then?

. Jul 8, 2010 Mark as spam

DO NOT DOWNLOAD!!! SCAM & PHISHING EXTENSION!!!

anonymous Jul 5, 2010 Mark as spam

this is stoopid

asmp Jul 5, 2010 Mark as spam

This extension is dangerous... blog.betteradvertising.com/2010/01/19/better-advertising-acquires-ghostery/ man! To think I was almost installing this piece of sh.....

COLLABOR

Ghostery a

Ghostery s

where you

detectable

ecosystem

PROTECT

Ghostery is

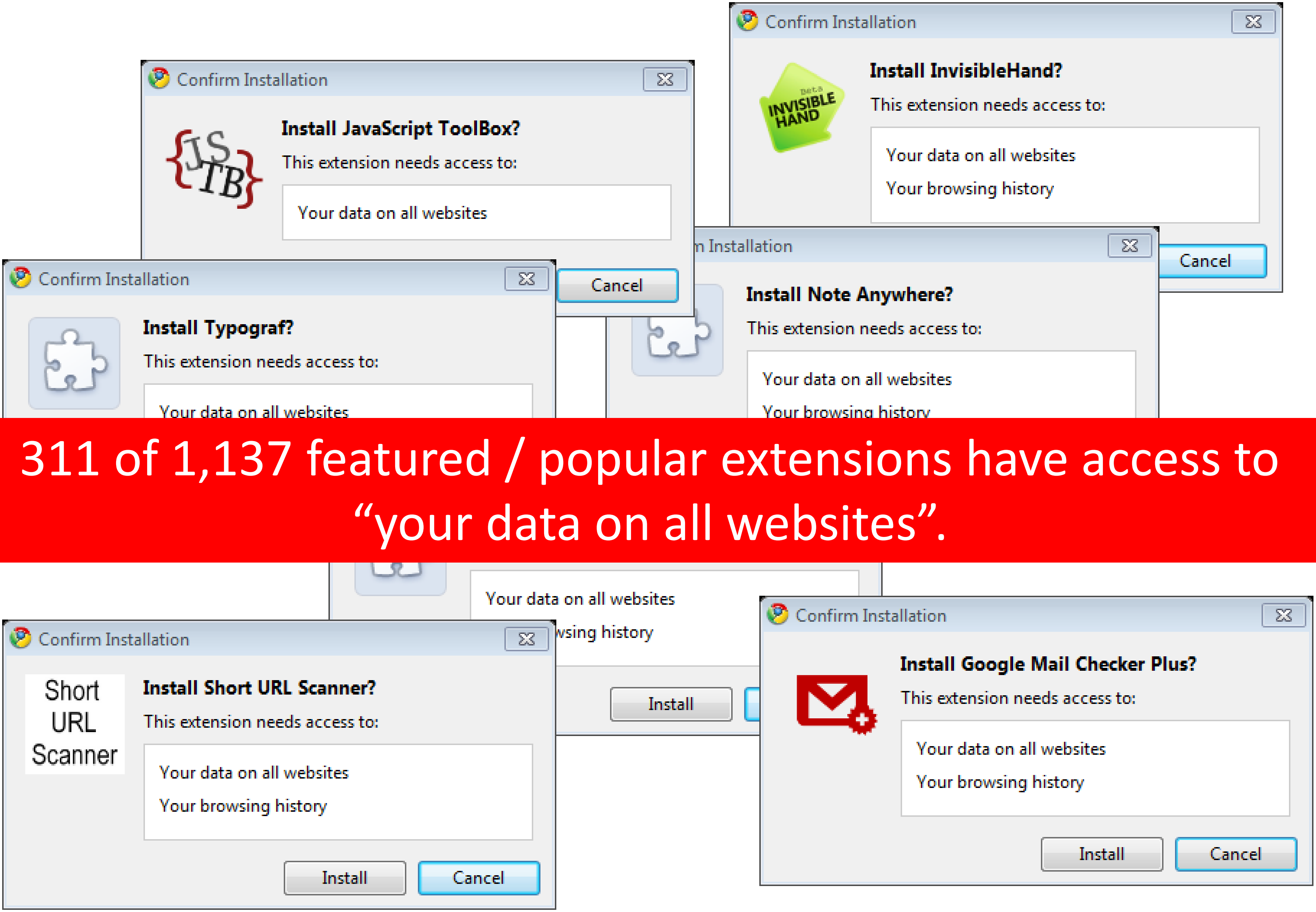
is engineer

registration

into your br

any data fr

GhostRank data is anonymous, it is NEVER used for advertising targeting purposes, and is only shared in an aggregated, non-personal, statistical form.



Install JavaScript ToolBox?

This extension needs access to:

Your data on all websites

Install InvisibleHand?

This extension needs access to:

Your data on all websites

Your browsing history

Install Typograf?

This extension needs access to:

Your data on all websites

Install Note Anywhere?

This extension needs access to:

Your data on all websites

Your browsing history

311 of 1,137 featured / popular extensions have access to “your data on all websites”.

Your data on all websites

wsing history

Install Short URL Scanner?

This extension needs access to:

Your data on all websites

Your browsing history

Install Google Mail Checker Plus?

This extension needs access to:

Your data on all websites

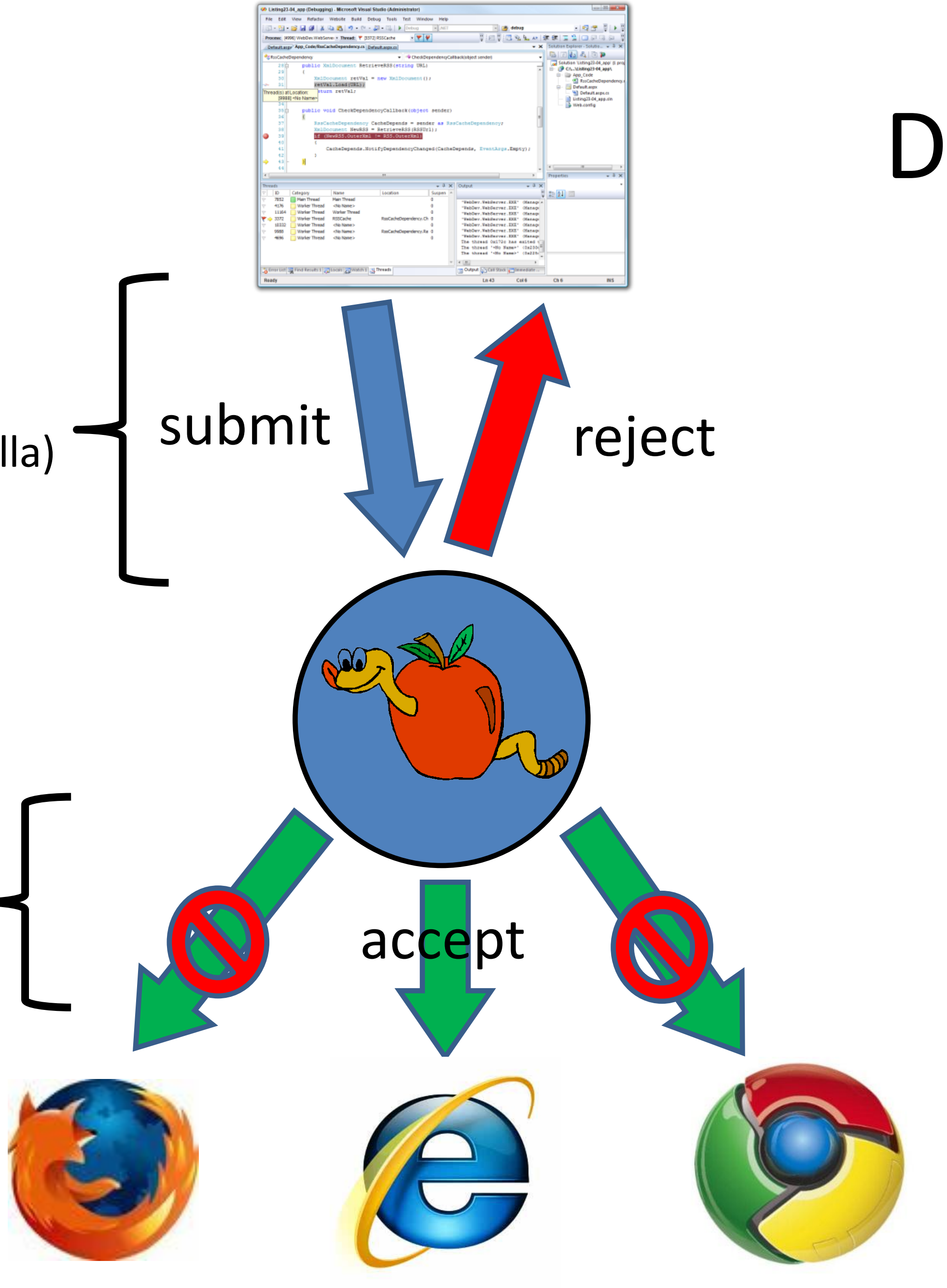
Your browsing history

Verified Security for Browser Extensions

Nikhil Swamy

With Arjun Guha, Matthew Fredrikson, and Ben Livshits

[Oakland S&P, 2011]



Developer

arbitrary (Apple)
too permissive (Mozilla)

submit

reject

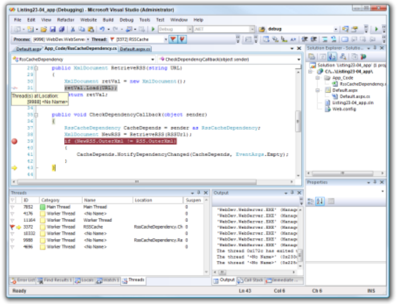
Curator

cross-platform
extensions are hard

accept

Users

precise policy +



Listing23.04_app (Debugging) - Microsoft Visual Studio (Administrator)
File Edit View Refactor Website Build Debug Tools Test Window Help
Debug .NET debug
Process: [4996] WebDev.WebServe Thread: [3372] RSSCache
Default.aspx App_Code/RssCacheDependency.cs Default.aspx.cs
RssCacheDependency CheckDependencyCallback(object sender)
Solution Explorer - Solutio...
Solution 'Listing23-04_app' (1 proj
C:\...\Listing23-04_app\
App_Code
RssCacheDependency.
Default.aspx
Default.aspx.cs
Listing23-04_app.sln
Web.config
Properties
Threads
Output
Error List Find Results 1 Locals Watch 1 Threads
Output Call Stack Immediate ...
Ready Ln 43 Col 6 Ch 6 INS

```
    public XmlDocument RetrieveRSS(string URL)
    {
        XmlDocument retVal = new XmlDocument();
        retVal.Load(URL);
        return retVal;
    }

    public void CheckDependencyCallback(object sender)
    {
        RssCacheDependency CacheDepends = sender as RssCacheDependency;
        XmlDocument NewRSS = RetrieveRSS(RSSUrl);
        if (NewRSS.OuterXml != RSS.OuterXml)
        {
            CacheDepends.NotifyDependencyChanged(CacheDepends, EventArgs.Empty);
        }
    }
```

Thread(s) at Location:
[9988] <No Name>

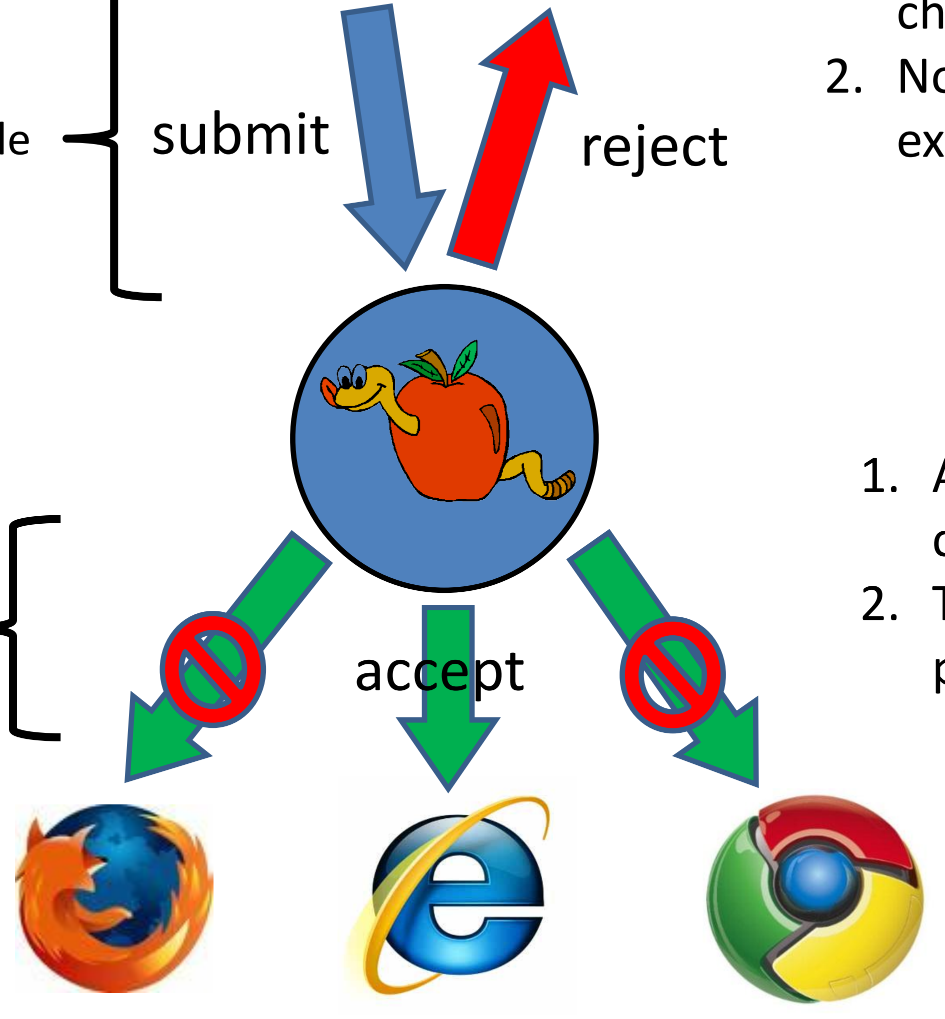
ID	Category	Name	Location	Suspen
7852	Main Thread	Main Thread		0
4176	Worker Thread	<No Name>		0
11164	Worker Thread	Worker Thread		0
3372	Worker Thread	RSSCache	RssCacheDependency.Ch	0
10332	Worker Thread	<No Name>		0
9988	Worker Thread	<No Name>	RssCacheDependency.Re	0
4696	Worker Thread	<No Name>		0

```
'WebDev.WebServer.EXE' (Manag
'WebDev.WebServer.EXE' (Manag
'WebDev.WebServer.EXE' (Manag
'WebDev.WebServer.EXE' (Manag
'WebDev.WebServer.EXE' (Manag
'WebDev.WebServer.EXE' (Manag
'WebDev.WebServer.EXE' (Manag
The thread 0x172c has exited 
The thread '<No Name>' (0x230
The thread '<No Name>' (0x228
```

Developer

1. No runtime security checks (fast)
2. No security exceptions (robust)

predictable, reliable



submit

reject

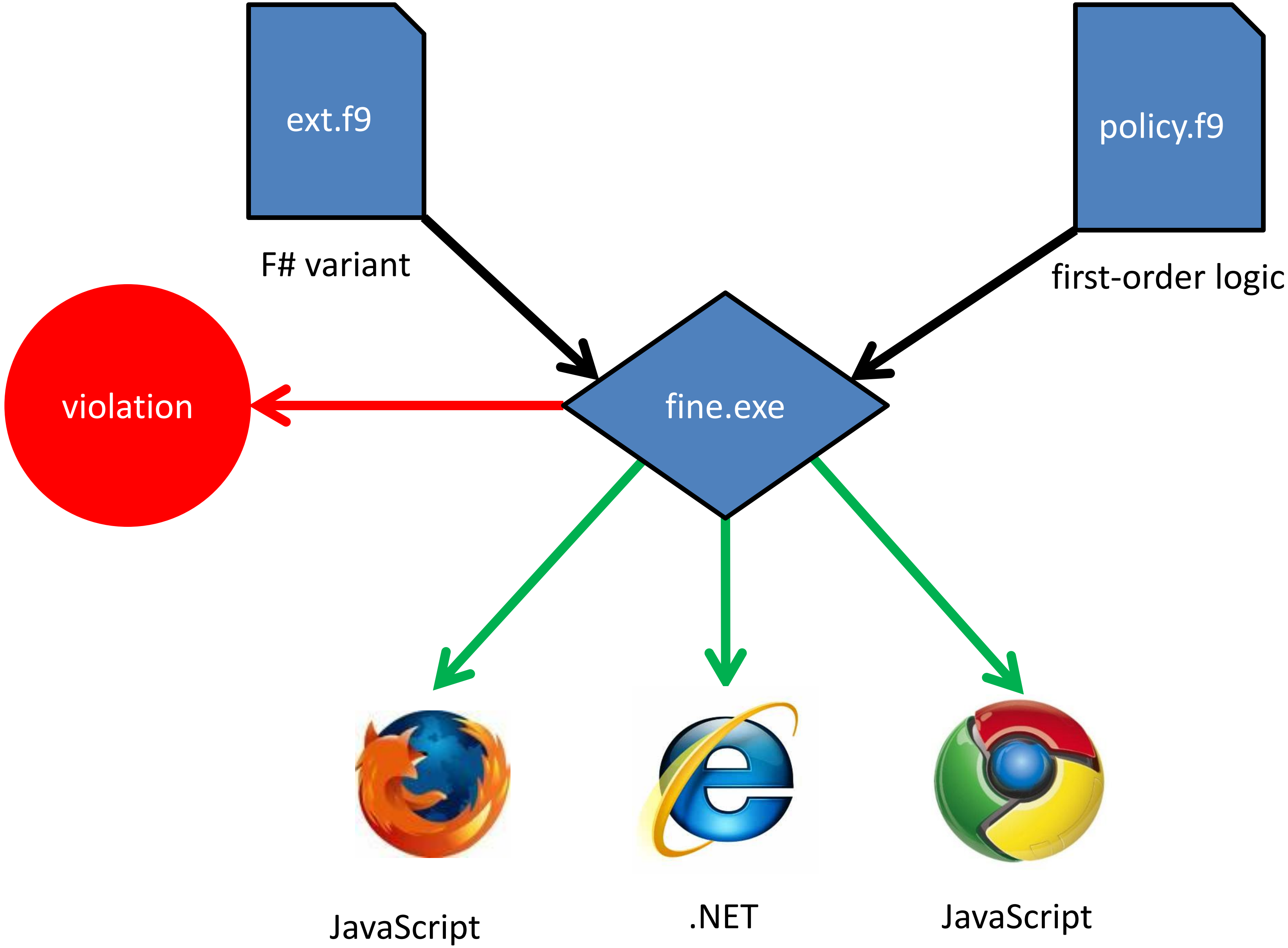
accept

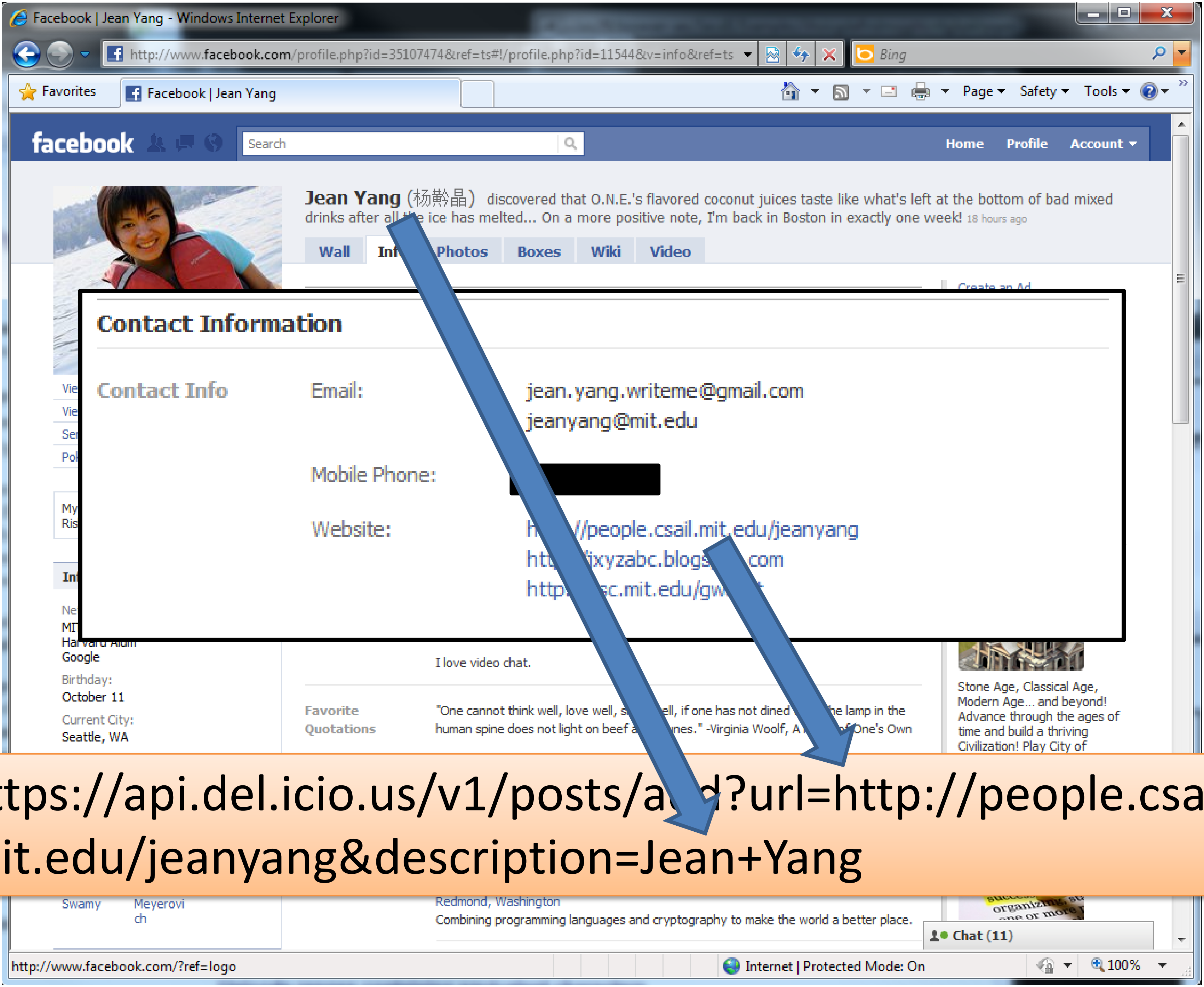
Curator

1. Automate policy compliance checking
2. Tools to understand policies

make this easier

Users


ext.f9
F# variant
policy.f9
first-order logic
violation
fine.exe
JavaScript
.NET
JavaScript



Facebook | Jean Yang - Windows Internet Explorer

http://www.facebook.com/profile.php?id=35107474&ref=ts#!/profile.php?id=11544&v=info&ref=ts

Jean Yang (杨㦁晶) discovered that O.N.E.'s flavored coconut juices taste like what's left at the bottom of bad mixed drinks after all the ice has melted... On a more positive note, I'm back in Boston in exactly one week! 18 hours ago

Contact Information

Contact Info	Email:	jean.yang.writeme@gmail.com jeanyang@mit.edu
	Mobile Phone:	[redacted]
	Website:	http://people.csail.mit.edu/jeanyang http://ixyzabc.blogspot.com http://sc.mit.edu/gw...

Ne...
MIT
Harvard Alum
Google

Birthday:
October 11

Current City:
Seattle, WA

I love video chat.

Favorite Quotations: "One cannot think well, love well, sleep well, if one has not dined well. The lamp in the human spine does not light on beef and prunes." -Virginia Woolf, A Room of One's Own

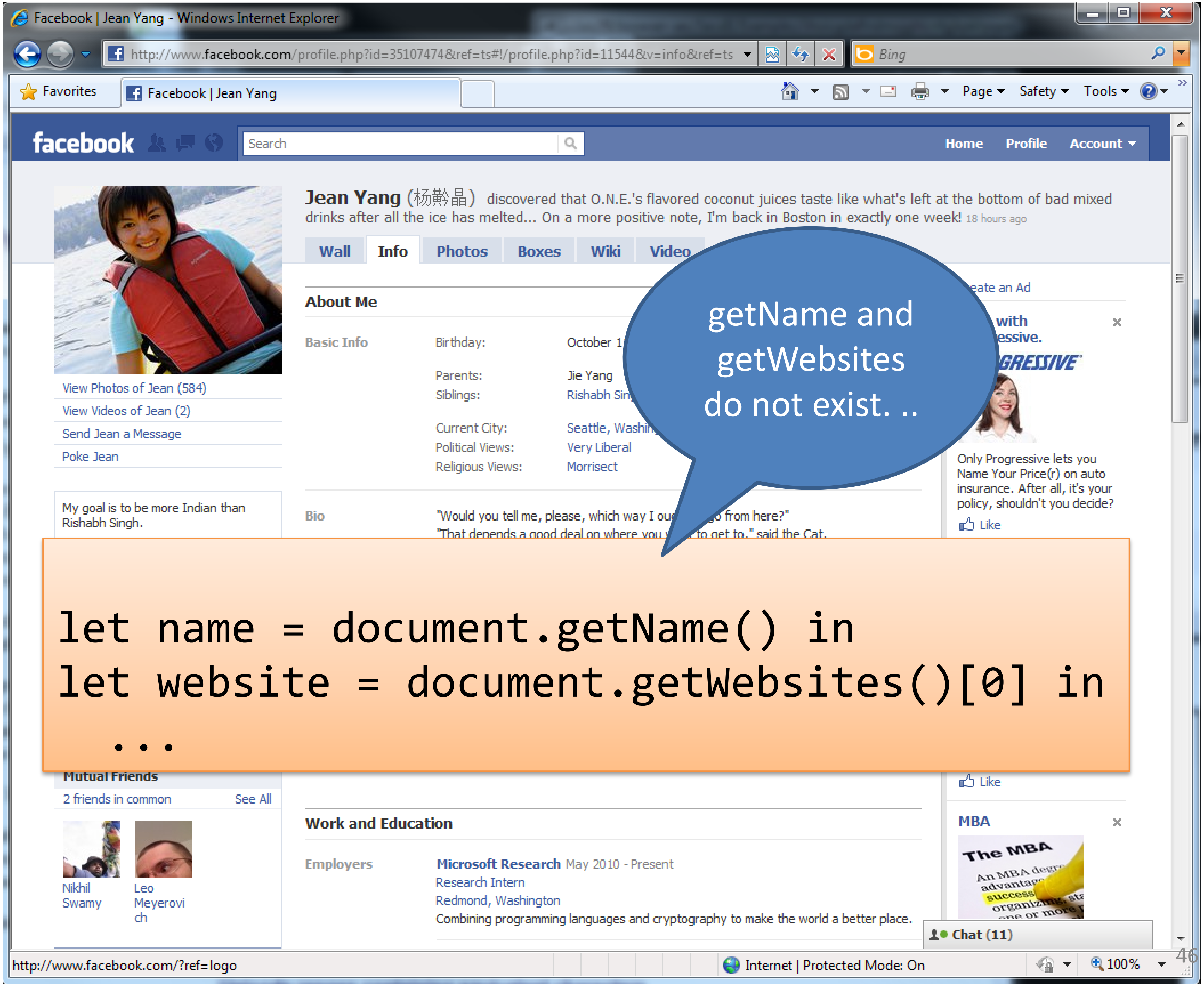
Stone Age, Classical Age, Modern Age... and beyond! Advance through the ages of time and build a thriving Civilization! Play City of

Swamy Meyerovich

Redmond, Washington
Combining programming languages and cryptography to make the world a better place.

Chat (11)
http://www.facebook.com/?ref=logo
Internet | Protected Mode: On
100%

https://api.del.icio.us/v1/posts/add?url=http://people.csail.mit.edu/jeanyang&description=Jean+Yang



Facebook | Jean Yang - Windows Internet Explorer

http://www.facebook.com/profile.php?id=35107474&ref=ts#!/profile.php?id=11544&v=info&ref=ts

Favorites | Facebook | Jean Yang

facebook | Search | Home | Profile | Account

Jean Yang (杨[illegible]晶) discovered that O.N.E.'s flavored coconut juices taste like what's left at the bottom of bad mixed drinks after all the ice has melted... On a more positive note, I'm back in Boston in exactly one week! 18 hours ago

Wall | Info | Photos | Boxes | Wiki | Video

View Photos of Jean (584)
View Videos of Jean (2)
Send Jean a Message
Poke Jean

My goal is to be more Indian than Rishabh Singh.

About Me

Basic Info	Birthday:	October 1
	Parents:	Jie Yang
	Siblings:	Rishabh Sin
	Current City:	Seattle, Washin
	Political Views:	Very Liberal
	Religious Views:	Morrisect
Bio	"Would you tell me, please, which way I ou	o from here?" "That depends a good deal on where you w	to get to," said the Cat.

eate an Ad

with essive.

GRESSIVE

Only Progressive lets you Name Your Price(r) on auto insurance. After all, it's your policy, shouldn't you decide?

Like

Mutual Friends

2 friends in common | See All

Nikhil Swamy | Leo Meyerovich

Work and Education

Employers	**Microsoft Research** May 2010 - Present Research Intern Redmond, Washington Combining programming languages and cryptography to make the world a better place.

Like

MBA

The MBA

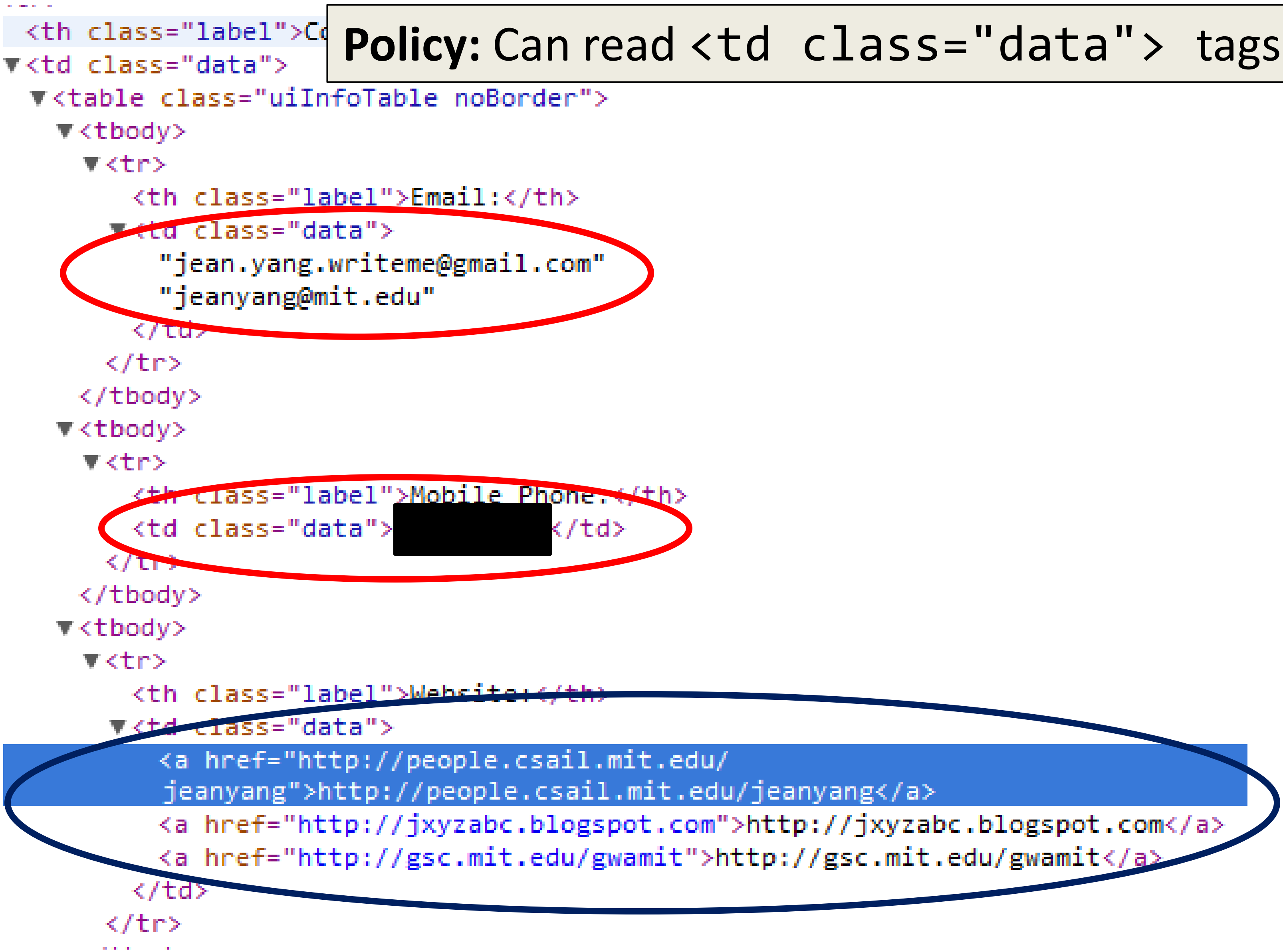
Chat (11)

http://www.facebook.com/?ref=logo | Internet \| Protected Mode: On | 100%

getName and getWebsites do not exist. ..

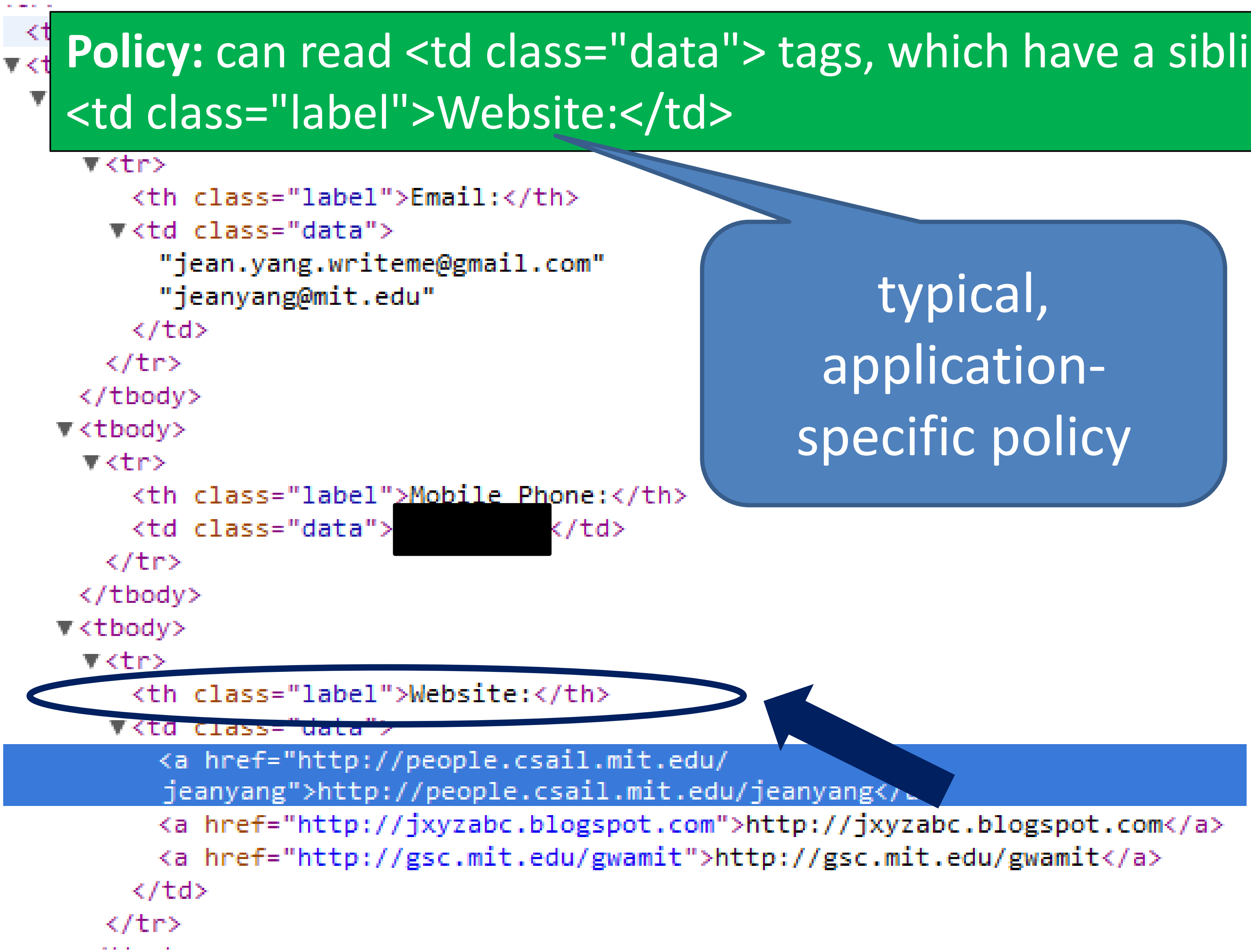
```
let name = document.getName() in
let website = document.getWebsites()[0] in
  ...
```

Policy: Can read <td class="data"> tags



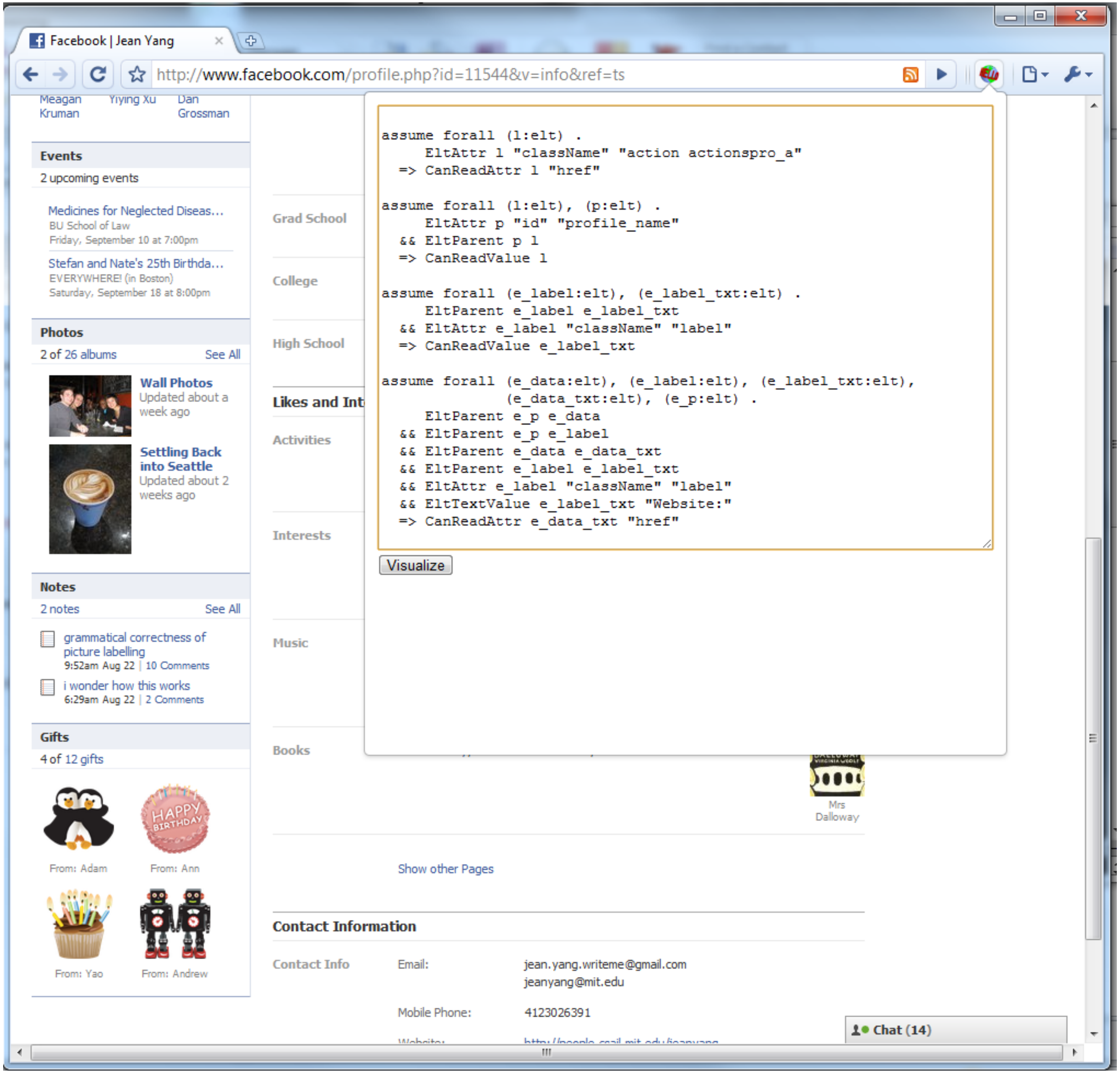
```
...
 <th class="label">Co
▼<td class="data">
  ▼<table class="uiInfoTable noBorder">
    ▼<tbody>
      ▼<tr>
          <th class="label">Email:</th>
        ▼<td class="data">
            "jean.yang.writeme@gmail.com"
            "jeanyang@mit.edu"
          </td>
        </tr>
      </tbody>
    ▼<tbody>
      ▼<tr>
          <th class="label">Mobile Phone:</th>
          <td class="data">[redacted]</td>
        </tr>
      </tbody>
    ▼<tbody>
      ▼<tr>
          <th class="label">Website:</th>
        ▼<td class="data">
            <a href="http://people.csail.mit.edu/
            jeanyang">http://people.csail.mit.edu/jeanyang</a>
            <a href="http://jxyzabc.blogspot.com">http://jxyzabc.blogspot.com</a>
            <a href="http://gsc.mit.edu/gwamit">http://gsc.mit.edu/gwamit</a>
          </td>
        </tr>
        ...
```

Policy: can read <td class="data"> tags, which have a sibling <td class="label">Website:</td>



```
<t
▼<t
  ▼
    ▼<tr>
       <th class="label">Email:</th>
      ▼<td class="data">
         "jean.yang.writeme@gmail.com"
         "jeanyang@mit.edu"
       </td>
     </tr>
   </tbody>
  ▼<tbody>
    ▼<tr>
       <th class="label">Mobile Phone:</th>
       <td class="data">[redacted]</td>
     </tr>
   </tbody>
  ▼<tbody>
    ▼<tr>
       <th class="label">Website:</th>
      ▼<td class="data">
         <a href="http://people.csail.mit.edu/
         jeanyang">http://people.csail.mit.edu/jeanyang</
         <a href="http://jxyzabc.blogspot.com">http://jxyzabc.blogspot.com</a>
         <a href="http://gsc.mit.edu/gwamit">http://gsc.mit.edu/gwamit</a>
       </td>
     </tr>
```

typical, application-specific policy



Meagan Kruman Yiying Xu Dan Grossman

Events

2 upcoming events

Medicines for Neglected Diseas…
BU School of Law
Friday, September 10 at 7:00pm

Stefan and Nate's 25th Birthda…
EVERYWHERE! (in Boston)
Saturday, September 18 at 8:00pm

Photos

2 of 26 albums See All

Wall Photos
Updated about a week ago

Settling Back into Seattle
Updated about 2 weeks ago

Notes

2 notes See All

□ grammatical correctness of picture labelling
9:52am Aug 22 | 10 Comments

□ i wonder how this works
6:29am Aug 22 | 2 Comments

Gifts

4 of 12 gifts

From: Adam From: Ann
From: Yao From: Andrew

Grad School

College

High School

Likes and Int

Activities

Interests

Music

Books

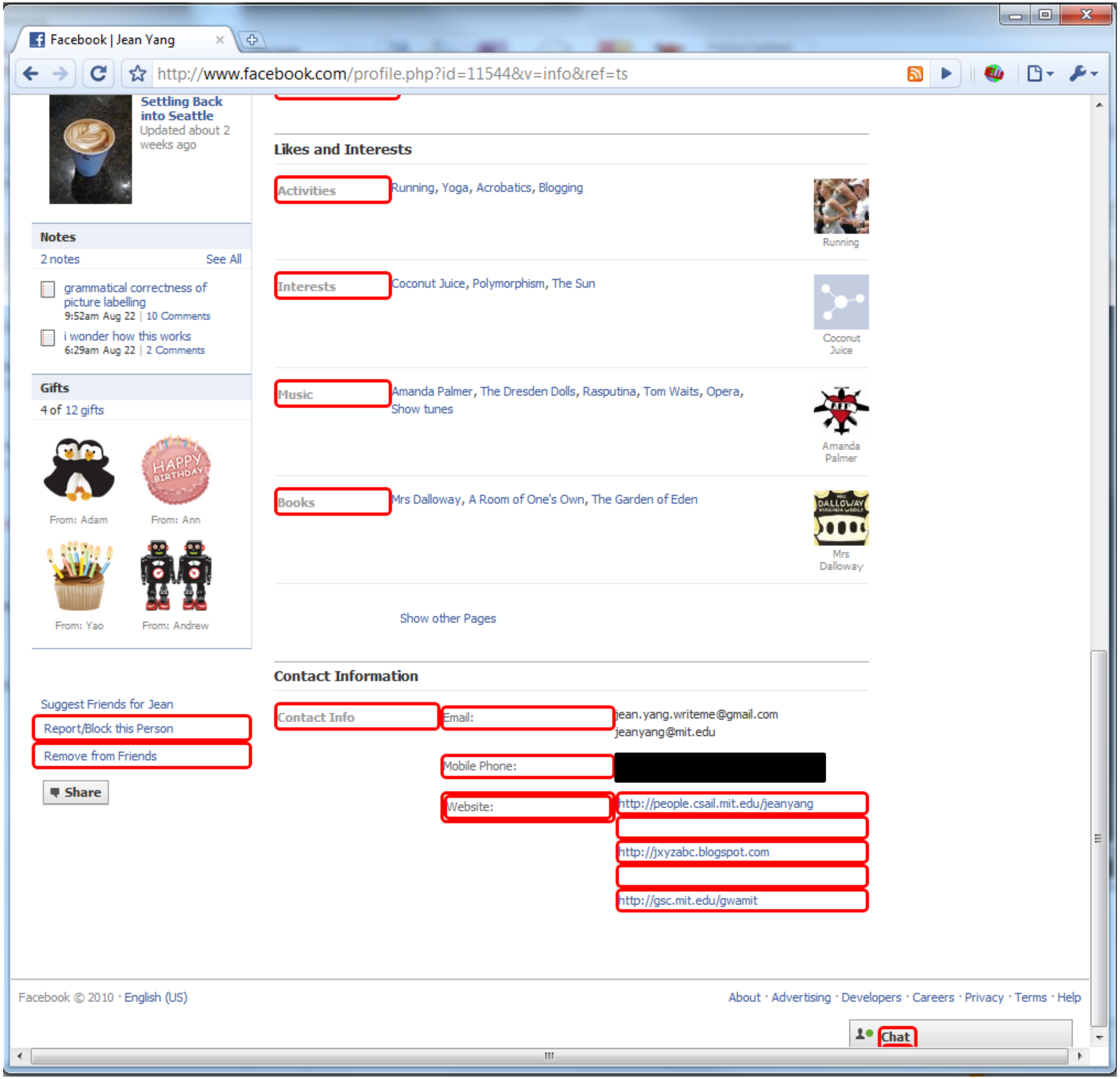
```
assume forall (l:elt) .
     EltAttr l "className" "action actionspro_a"
  => CanReadAttr l "href"

assume forall (l:elt), (p:elt) .
     EltAttr p "id" "profile_name"
  && EltParent p l
  => CanReadValue l

assume forall (e_label:elt), (e_label_txt:elt) .
     EltParent e_label e_label_txt
  && EltAttr e_label "className" "label"
  => CanReadValue e_label_txt

assume forall (e_data:elt), (e_label:elt), (e_label_txt:elt),
              (e_data_txt:elt), (e_p:elt) .
     EltParent e_p e_data
  && EltParent e_p e_label
  && EltParent e_data e_data_txt
  && EltParent e_label e_label_txt
  && EltAttr e_label "className" "label"
  && EltTextValue e_label_txt "Website:"
  => CanReadAttr e_data_txt "href"
```

Mrs Dalloway

Show other Pages

Contact Information

Contact Info	Email:	jean.yang.writeme@gmail.com jeanyang@mit.edu
	Mobile Phone:	4123026391



http://www.facebook.com/profile.php?id=11544&v=info&ref=ts

Settling Back into Seattle
Updated about 2 weeks ago

Notes
2 notes See All

grammatical correctness of picture labelling
9:52am Aug 22 | 10 Comments

i wonder how this works
6:29am Aug 22 | 2 Comments

Gifts
4 of 12 gifts

From: Adam
From: Ann
From: Yao
From: Andrew

Suggest Friends for Jean

Report/Block this Person

Remove from Friends

Share

Likes and Interests

Activities: Running, Yoga, Acrobatics, Blogging

Running

Interests: Coconut Juice, Polymorphism, The Sun

Coconut Juice

Music: Amanda Palmer, The Dresden Dolls, Rasputina, Tom Waits, Opera, Show tunes

Amanda Palmer

Books: Mrs Dalloway, A Room of One's Own, The Garden of Eden

Mrs Dalloway

Show other Pages

Contact Information

Contact Info

Email: jean.yang.writeme@gmail.com
jeanyang@mit.edu

Mobile Phone: [redacted]

Website: http://people.csail.mit.edu/jeanyang

http://jxyzabc.blogspot.com

http://gsc.mit.edu/gwamit

Facebook © 2010 · English (US)

About · Advertising · Developers · Careers · Privacy · Terms · Help

Chat

Summary

- Client-side JavaScript
  - Analysis of JavaScript
  - `eval` and code obfuscation
  - Need for runtime enforcement
- Gatekeeper as illustration
- Browser
  - Plugins
- Extensions
  - Firefox extension model
  - Chrome extension model
  - Looking forward