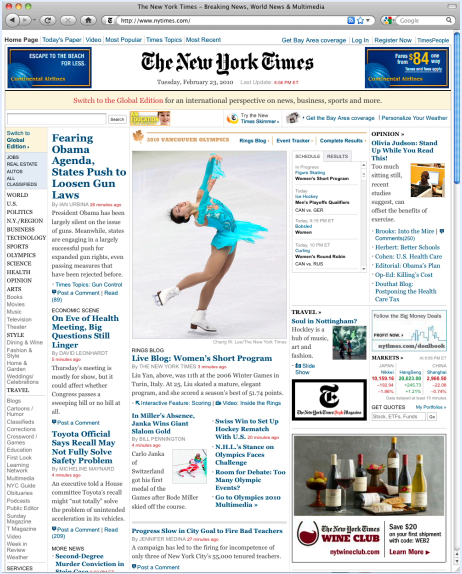
Preventing Capability Leaks in Secure JavaScript Subsets

Matthew Finifter, Joel Weinberger, and Adam Barth
{finifter, jww, abarth}@cs.berkeley.edu

UC Berkeley

March 3, 2010

Introduction



Home Page | Today's Paper | Video | Most Popular | Times Topics | Most Recent

Get Bay Area coverage | Log In | Register Now | TimesPeople

The New York Times

Tuesday, February 23, 2010 Last Update: 8:56 PM ET

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

Search

Try the New Times Skimmer ›

› Get the Bay Area coverage | Personalize Your Weather

Switch to Global Edition ›

JOBS
REAL ESTATE
AUTOS
ALL CLASSIFIEDS

WORLD
U.S.
POLITICS
N.Y./REGION
BUSINESS
TECHNOLOGY
SPORTS
OLYMPICS
SCIENCE
HEALTH
OPINION
ARTS
Books
Movies
Music
Television
Theater
STYLE
Dining & Wine
Fashion & Style
Home & Garden
Weddings/ Celebrations
TRAVEL

Blogs
Cartoons / Humor
Classifieds
Corrections
Crossword / Games
Education
First Look
Learning Network
Multimedia
NYC Guide
Obituaries
Podcasts
Public Editor
Sunday Magazine
T Magazine
Video
Week in Review
Weather

SERVICES

Fearing Obama Agenda, States Push to Loosen Gun Laws

By IAN URBINA 26 minutes ago

President Obama has been largely silent on the issue of guns. Meanwhile, states are engaging in a largely successful push for expanded gun rights, even passing measures that have been rejected before.

- Times Topics: Gun Control

Post a Comment | Read (89)

ECONOMIC SCENE

On Eve of Health Meeting, Big Questions Still Linger

By DAVID LEONHARDT 5 minutes ago

Thursday's meeting is mostly for show, but it could affect whether Congress passes a sweeping bill or no bill at all.

Post a Comment

Toyota Official Says Recall May Not Fully Solve Safety Problem

By MICHELINE MAYNARD 4 minutes ago

An executive told a House committee Toyota's recall might "not totally" solve the problem of unintended acceleration in its vehicles.

Post a Comment | Read (209)

MORE NEWS

- Second-Degree Murder Conviction in Stein Case

2010 VANCOUVER OLYMPICS Rings Blog › | Event Tracker › | Complete Results ›

Chang W. Lee/The New York Times

SCHEDULE | RESULTS

In Progress
Figure Skating
Women's Short Program

Today
Ice Hockey
Men's Playoffs Qualifiers
CAN vs. GER

Today, 9:15 PM ET
Bobsled
Women

Today, 10 PM ET
Curling
Women's Round Robin
CAN vs. RUS

RINGS BLOG

Live Blog: Women's Short Program

By THE NEW YORK TIMES 3 minutes ago

Liu Yan, above, was 11th at the 2006 Winter Games in Turin, Italy. At 25, Liu skated a mature, elegant program, and she scored a season's best of 51.74 points.

- Interactive Feature: Scoring | Video: Inside the Rings

In Miller's Absence, Janka Wins Giant Slalom Gold

By BILL PENNINGTON 4 minutes ago

Carlo Janka of Switzerland got his first medal of the Games after Bode Miller skied off the course.

- Swiss Win to Set Up Hockey Rematch With U.S. 20 minutes ago
- N.H.L.'s Stance on Olympics Faces Challenge
- Room for Debate: Too Many Olympic Events?
- Go to Olympics 2010 Multimedia »

Progress Slow in City Goal to Fire Bad Teachers

By JENNIFER MEDINA 27 minutes ago

A campaign has led to the firing for incompetence of only three of New York City's 55,000 tenured teachers.

Post a Comment

OPINION »

Olivia Judson: Stand Up While You Read This!

Too much sitting still, recent studies suggest, can offset the benefits of exercise.

- Brooks: Into the Mire | Comments(250)
- Herbert: Better Schools
- Cohen: U.S. Health Care
- Editorial: Obama's Plan
- Op-Ed: Killing's Cost
- Douthat Blog: Postponing the Health Care Tax

TRAVEL »

Soul in Nottingham?

Hockley is a hub of music, art and fashion.

- Slide Show

MARKETS » At 8:58 PM ET

JAPAN		CHINA
Nikkei	HangSeng	Shanghai
10,159.16	20,623.00	2,960.50
−192.94	+245.73	−22.08
−1.86%	+1.21%	−0.74%

Data delayed at least 15 minutes

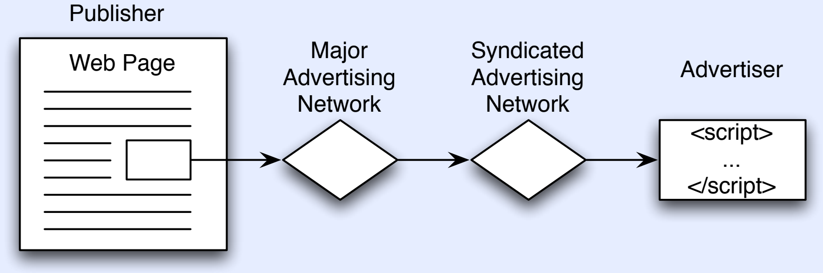
GET QUOTES My Portfolios »

Stock, ETFs, Funds Go

Overview

- Ad networks and malicious ads
- Statically verified containment
- Experiment
- Our proposal: Blancura

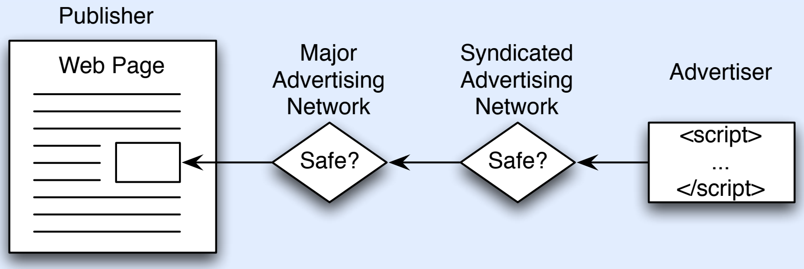
Ad networks



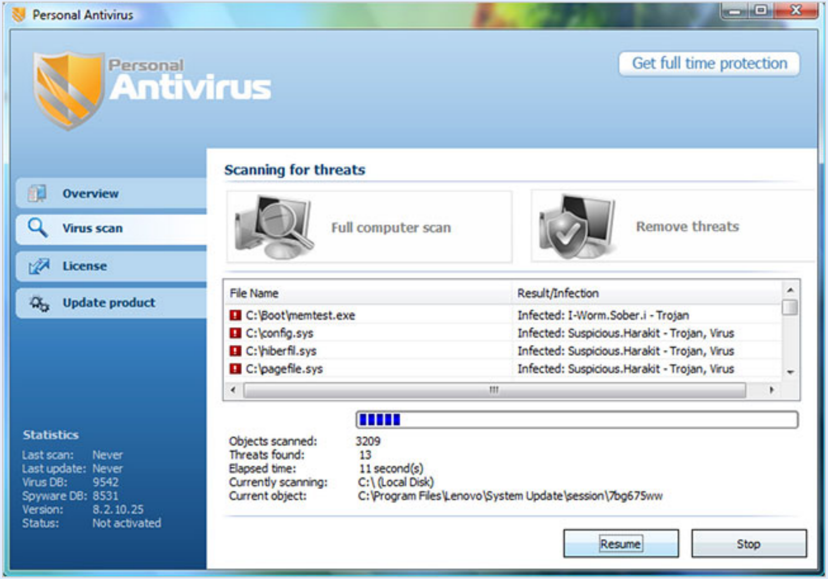
Publisher
Web Page
Major Advertising Network
Syndicated Advertising Network
Advertiser
<script>
...
</script>

Ad networks

- Trust?



Malicious ads



Scanning for threats

File Name	Result/Infection
C:\Boot\memtest.exe	Infected: I-Worm.Sober.i - Trojan
C:\config.sys	Infected: Suspicious.Harakit - Trojan, Virus
C:\hiberfil.sys	Infected: Suspicious.Harakit - Trojan, Virus
C:\pagefile.sys	Infected: Suspicious.Harakit - Trojan, Virus

Objects scanned:	3209
Threats found:	13
Elapsed time:	11 second(s)
Currently scanning:	C:\ (Local Disk)
Current object:	C:\Program Files\Lenovo\System Update\session\7bg675ww

Statistics

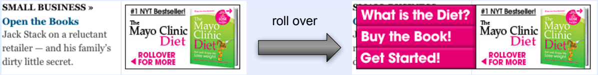
Last scan:	Never
Last update:	Never
Virus DB:	9542
Spyware DB:	8531
Version:	8.2.10.25
Status:	Not activated

Safe advertising

- iframes

Safe advertising

- iframes – *Not very interactive*
  - Can’t do this with an iframe



Safe advertising

- iframes – *Not very interactive*
- Dynamic enforcement

Safe advertising

- iframes – *Not very interactive*
- Dynamic enforcement – *Slow*

	read	write
Cajita	21%	20%
Valija	1493%	1000%
Microsoft Web Sandbox	1217%	634%

Table: Slowdown on “read” and “write” micro-benchmarks, average of 10 runs.

Safe advertising

- iframes – *Not very interactive*
- Dynamic enforcement – *Slow*
- Static verification

Statically verified containment

- ADsafe, Dojo Secure, and Jacaranda
- Language subset that provides containment
- Each party can statically verify properties

Common properties

- Prevent use of global variables
  - e.g., `document`
- Blacklist dangerous properties
  - e.g., `constructor`
- Ban unverifiable constructs
  - e.g., `eval`
- Provide a library
  - e.g., `ADSAFE.get(foo, bar)` instead of `foo[bar]`

Blacklist for property names

- Assume blacklist is complete for empty page
  - If not, no guest is contained on any page

Blacklist for property names

- Assume blacklist is complete for empty page
    - If not, no guest is contained on any page
- Host may add new properties
    - Example from `people.com`

```
String.prototype.right = function(n) {
    ... // return rightmost n characters of this String
}
```

Blacklist for property names

- Assume blacklist is complete for empty page
    - If not, no guest is contained on any page

- Host may add new properties
    - Example from `people.com`

```
String.prototype.right = function(n) {
    ... // return rightmost n characters of this String
}
```

- Added properties could allow guest to breach containment

```
String.prototype.evalMe = function() { eval(this); }
```

Blacklist for property names

- Assume blacklist is complete for empty page
    - If not, no guest is contained on any page
- Host may add new properties
    - Example from `people.com`

```
String.prototype.right = function(n) {
    ... // return rightmost n characters of this String
}
```

- Added properties could allow guest to breach containment

```
String.prototype.evalMe = function() { eval(this); }
```

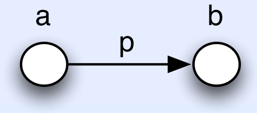
- How often does this occur?

Methodology

- Focus on ADsafe
- Analyze sites on Alexa US Top 100
  - List slightly modified where appropriate
  - Represent complexity of JavaScript on popular sites
- Emulate ad hosting by injecting ad into each site

Browser instrumentation

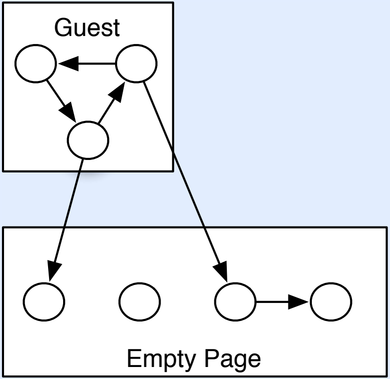
```
a.p = b;
```



- Instrumented WebKit
- Tracks points-to relation among JavaScript objects

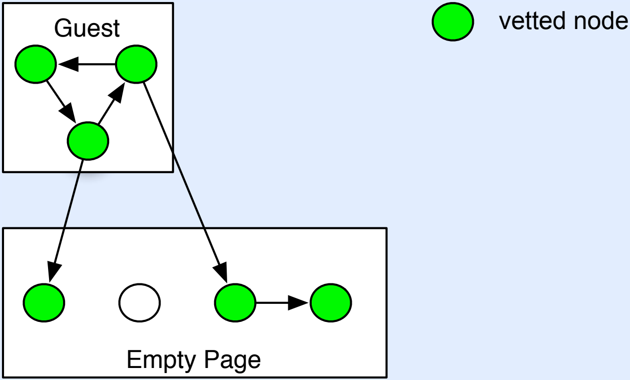
Suspicious edges

- Label *vetted* and *unvetted* objects



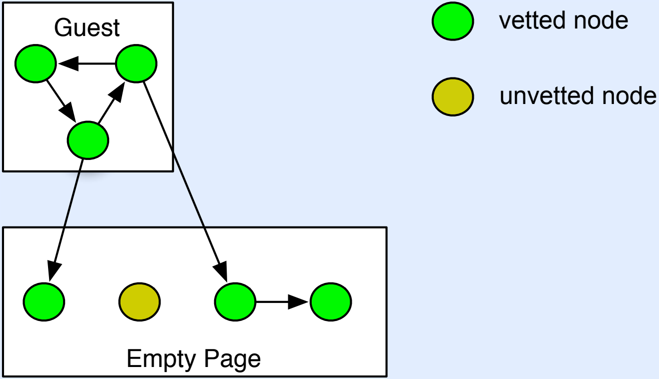
Suspicious edges

- Label *vetted* and *unvetted* objects



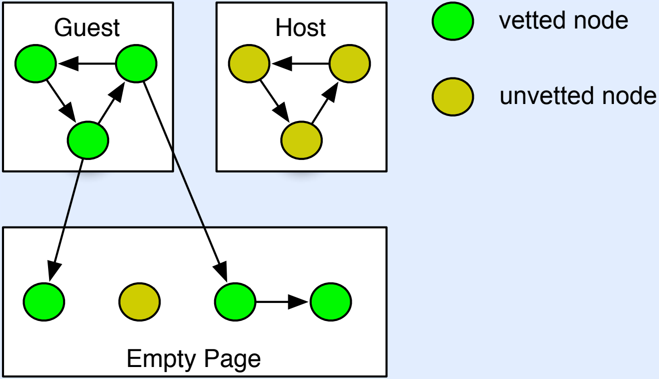
Suspicious edges

- Label *vetted* and *unvetted* objects



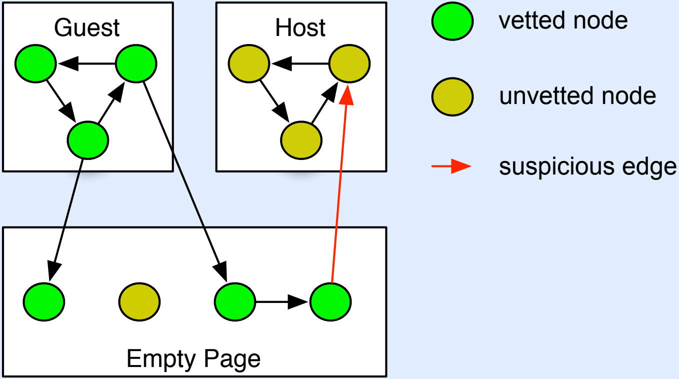
Suspicious edges

- Label *vetted* and *unvetted* objects



Suspicious edges

- Label *vetted* and *unvetted* objects
- Note *suspicious* edges
  - `String.prototype.evalMe = function() { eval(this); }`



Suspicious edges

- Not all suspicious edges are exploitable

  ```
  String.prototype.returnOne = function() { return 1; }
  ```

Suspicious edges

- Not all suspicious edges are exploitable

  ```
  String.prototype.returnOne = function() { return 1; }
  ```

- But some are

  ```
  String.prototype.evalMe = function() { eval(this); }
  ```

Suspicious edges

- Not all suspicious edges are exploitable

  ```
  String.prototype.returnOne = function() { return 1; }
  ```

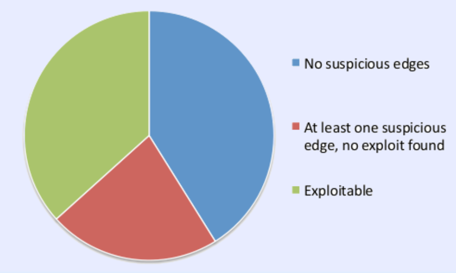
- But some are

  ```
  String.prototype.evalMe = function() { eval(this); }
  ```

- Manual analysis of suspicious edges pointing to functions

Results

- 59% contained at least one suspicious edge
- Constructed exploits for 37% of the sites
  - Including Twitter, MSN, Microsoft, Apple
- Num. suspicious edges correlates with exploitability



Sample exploit

```
String.prototype.evalMe = function() { eval(this); }
```

Sample exploit

~~String.prototype.evalMe = function() { eval(this); }~~

```
String.prototype.extractScripts = function() {
    // returns an array of all scripts in this string
    ...
}
String.prototype.evalScripts = function() {
    return this.extractScripts().map(
        function(script) { return eval(script) });
}
```

Possible solutions

- Require careful coding by publisher sites?
- Publisher must tune page to specs of ad network
- Too many restrictions push publishers away
- New problems can creep in at every site update

Blancura

- Change the property blacklist to a whitelist
- Run each guest in separate namespace
- Statically verify that all property accesses use correct namespace identifier
  - Disallowed: `obj.foo = bar;`
  - Allowed: `obj.BLANCURA_GUEST1_foo = bar;`

Blancura

- Add safe built-in properties to namespace

```
String.prototype.BLANCURA_GUEST1_indexOf =
    String.prototype.indexOf;
```

- Idempotent compiler from ADsafe to Blancura
- Strict language subset of ADsafe

Conclusion

- Focused on one approach to safe advertising: statically verified containment
- Analyzed consequences of property blacklisting
- Found that many sites would be vulnerable
- Proposed a fix based on property whitelisting

Thank you!

Subtly dangerous function

```
String.prototype.right = function(n) {
  if (n <= 0) {
    return "";
  } else if (n > String(this).length) {
    return this;
  } else {
    var l = String(this).length;
    return String(this).substring(l, l - n);
  }
}
```