

# Securing Browser Frame Navigation and Communication

Collin Jackson

Joint work with Adam Barth and John C. Mitchell

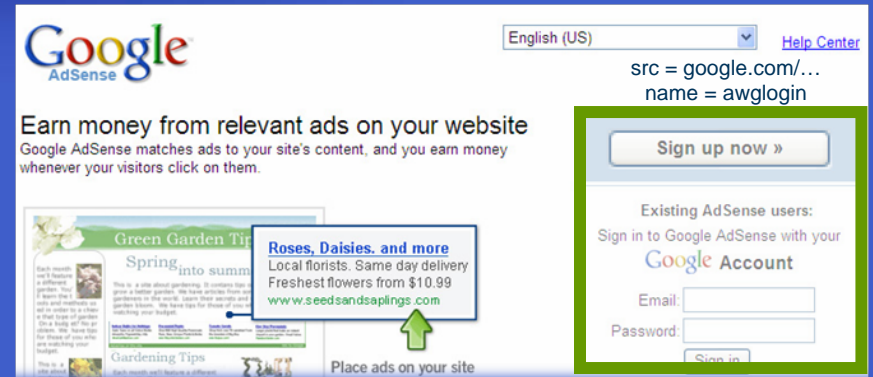
# Why use frames?

- Modularity

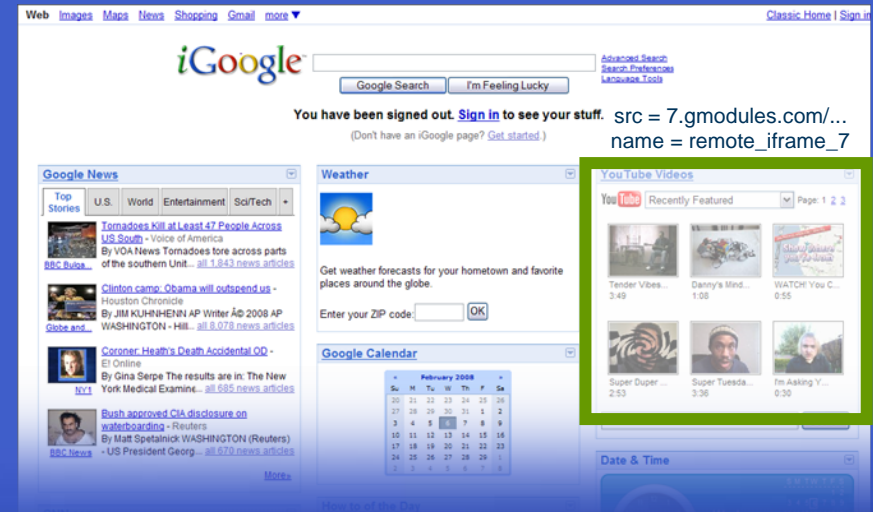
- Brings together content from multiple sources
- Client-side aggregation

- Isolation

- Different frames can represent different principals
- Can't script each other
- Frame can draw only on its own rectangle
- Easier than sanitization



The screenshot shows the Google AdSense sign-up page. At the top left is the Google AdSense logo. On the right, there is a language dropdown menu set to 'English (US)' and a 'Help Center' link. Below the logo, the text reads: 'Earn money from relevant ads on your website. Google AdSense matches ads to your site's content, and you earn money whenever your visitors click on them.' A central image shows a garden with a text box overlay that says: 'Roses, Daisies, and more Local florists. Same day delivery Freshest flowers from \$10.99 www.seedsandsaplings.com'. A green arrow points from this text box to the 'Place ads on your site' text below. On the right side, there is a sign-up form with a 'Sign up now »' button, a section for 'Existing AdSense users' with a 'Sign in to Google AdSense with your Google Account' link, and input fields for 'Email:' and 'Password:'.



The screenshot shows the iGoogle homepage. At the top is the 'iGoogle' logo and a search bar with 'Google Search' and 'I'm Feeling Lucky' buttons. Below the search bar, it says 'You have been signed out. Sign in to see your stuff.' and '(Don't have an iGoogle page? Get started)'. The page is divided into several frames. On the left is the 'Google News' frame with a 'Top Stories' section containing news items like 'Tornadoes Kill at Least 47 People Across US South' and 'Clinton camp: Obama will outstep us'. In the center is the 'Weather' frame showing a sun icon and a forecast. On the right is the 'YouTube Videos' frame with a 'Recently Featured' section showing video thumbnails like 'Tender Vibes' and 'Super Tuesdays'. At the bottom is a 'Google Calendar' frame showing a calendar for February 2008.

# Threat Model

- **Web attacker**

- Controls attacker.com (\$5)
- Can obtain SSL/TLS certificate for attacker.com (\$0)
- User visits attacker.com
- Optional additional assumption:
  - Gets to embeds a malicious gadget (ad) on integrator site

- **Stronger threat models**

- Network attacker: Can inspect or corrupt traffic
- Malware attacker: Already escaped the from browser

# Frame Navigation

- Who decides a frame's content?

## Permissive Policy

A frame can navigate any frame.

# Guninski Attack

Welcome to AdSense - Windows Internet Explorer

https://www.google.com/adsense/login/en\_US/

Google

Welcome to AdSense

English (US) Help Center

**Google**  
AdSense

Earn money from relevant ads on your website  
Google AdSense matches ads to your site's content, and you earn money whenever your visitors click on them.

**awglogin**

Sign up now »

Existing AdSense users:  
Sign in to Google AdSense with your  
**Google Account**

Email:

Password:

Sign in

[I cannot access my account](#)

**Roses, Daisies, and more**  
Local florists. Same day delivery  
Freshest flowers from \$10.99  
[www.seedsandsaplings.com](http://www.seedsandsaplings.com)

Place ads on your site

Windows Internet Explorer  
https://www.attacker.com/



```
window.open("https://www.attacker.com/...", "awglogin")
```

# Window Policy

A frame can navigate frames in its own window.

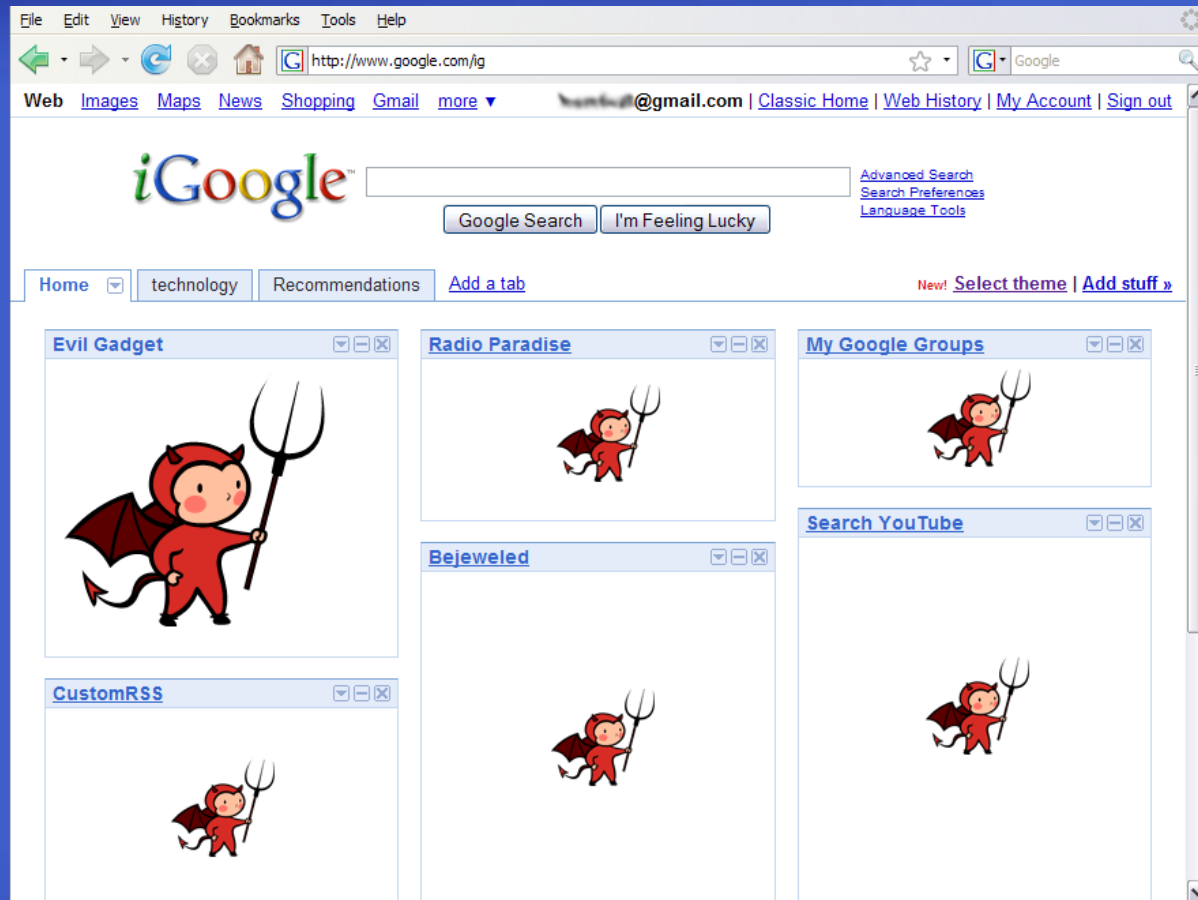
# Gadget Hijacking

The image shows a screenshot of a Google homepage in a web browser. A blue callout box is overlaid on the page, containing the following JavaScript code:

```
top.frames[1].location = "http://www.attacker.com/...";  
top.frames[2].location = "http://www.attacker.com/...";  
...
```

The browser window shows the URL `http://www.google.com/g` and the user is logged in as `username@gmail.com`. The page features several gadgets: "Evil Gadget" (a cartoon devil holding a pitchfork), "Now Playing" (a music player with a list of songs), "Bejeweled" (a game interface), "My Google Groups" (a list of groups), "Search YouTube" (a search bar), and "CustomRSS" (a list of RSS feeds). The "Evil Gadget" is highlighted by the callout box, indicating the target of the hijacking.

# Gadget Hijacking





# Policy Testing

http://a.w3sim.com/framegen.html?{"frame":{"name":"a","domain":"a","nav":["A","B","C","D"],"chi - Windows Internet Explorer

http://a.w3sim.com/framegen.html?{"frame":{"name":"a","domain":"a","nav":["A","B","C","D"],"children":{"name":"b","domain":"b","nav":["A","B","C","D"],"children":{"name":"c...}}

Frame A: a.w3sim.com

Allowed  
A, B, C, D

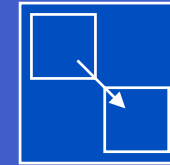
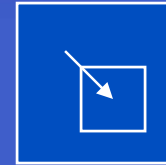
Frame B: b.w3sim.com	a.w3sim.com	b.w3sim.com	c.w3sim.com	d.w3sim.com	e.w3sim.com
Allowed A, B, C, D	Allowed A, B, C, D	Allowed A, B, C, D	Allowed A, C, D	Allowed A, D	Allowed A
a. b. c. d. e. v	a. b. c. d. e. v	a. b. c. d. e. v	a. b. c. d. e. v	a. b. c. d. e. v	a. b. c. d. e. v
A A A A A A	A A A A A A	A A A A A A	A A A A A A	A A A A A A	A A A A A A
B B C C D	B B C C D	B B C C D	B B C C D	B B C C D	B B C C D
Po Po Po Po Po Po	Po Po Po Po Po Po	Po Po Po Po Po Po	Po Po Po Po Po Po	Po Po Po Po Po Po	Po Po Po Po Po Po
bl bl bl bl bl bl	bl bl bl bl bl bl	bl bl bl bl bl bl	bl bl bl bl bl bl	bl bl bl bl bl bl	bl bl bl bl bl bl
B B C C	B B C C	B B C C	B B C C	B B C C	B B C C
D D	D D	D D	D D	D D	D D
d.					
A					
A					
D					
Po					
bl					
B					
C					

Done

Internet 100%

## Parent Policy

A frame can navigate its children.



## Ancestor Policy

A frame can navigate its descendants.







# Frame Navigation Policies

Browser	Policy	Propagation
 IE 6 (default)	Permissive	N/A
 IE 6 (option)	Parent	No
 IE7 (no Flash)	Ancestor	Yes
 IE7 (with Flash)	Permissive	N/A
 Firefox 2	Window	Sometimes
 Safari 2	Permissive	N/A

# Frame Navigation Policies

Browser	Policy	Propagation
---------	--------	-------------

 IE7 (no Flash)	Ancestor	Yes
 IE7 (with Flash)	Ancestor	Yes
 Firefox 3	Ancestor	Yes
 Safari 3	Ancestor	Yes

# Frame Communication

# Fragment Identifier Messaging

- Send information by navigating a frame
  - <http://gadget.com/#hello>
- Navigating to fragment doesn't reload frame
  - No network traffic, but frame can read its fragment
- Not a secure channel
  - Confidentiality 
  - Integrity 
  - Authentication 

# Fix: Improve the protocol

- Proposed Needham-Schroeder-Lowe

$A \rightarrow B : N_A, \mathbf{URI}_A$

$B \rightarrow A : N_A, N_B, \mathbf{URI}_B$

$A \rightarrow B : N_B$

...

$A \rightarrow B : N_A, N_B, \mathbf{Message}_i$

$B \rightarrow A : N_A, N_B, \mathbf{Message}_j$



- Adoption

- Microsoft: Windows Live Channels library
- IBM: OpenAjax Hub 1.1

# postMessage

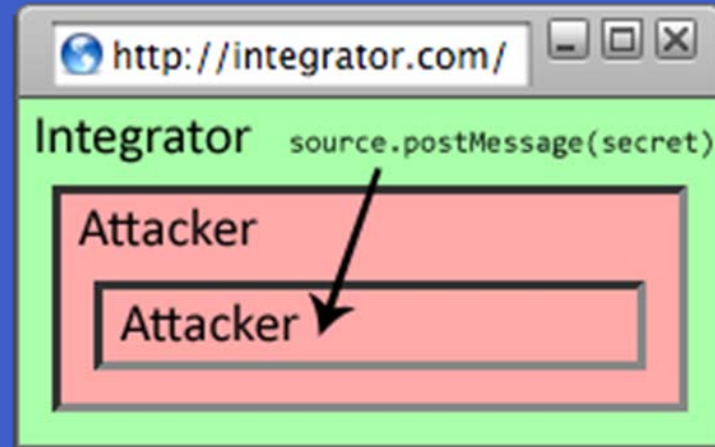
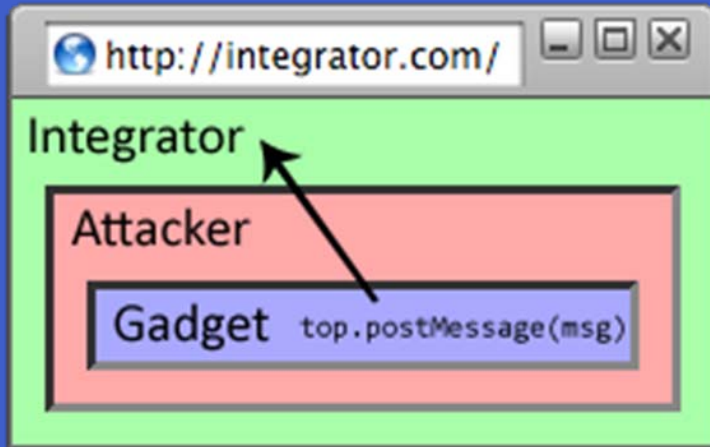
- New API for inter-frame communication
- Supported in latest betas of many browsers



- Not a secure channel
  - Confidentiality 
  - Integrity 
  - Authentication 



# Reply Attack



# Fix: Improve the API

- Let the sending specify the recipient
  - `frame[0].postMessage("Hello", "http://gadget.com")`
  - Can omit argument if confidentiality not required
- Adoption
  - Firefox 3
  - Internet Explorer 8
  - Safari 3.1

# Conclusion

- All proposals deployed to real users
- Frame isolation
  - Improved frame navigation policy
    - Fixed Guninski and Gadget Hijacking
  - Drive-by-downloads still a concern...
- Frame communication
  - Secured fragment identifier messaging
  - Secured new postMessage API

