Introduce safe use patterns.

Examine postMessage uses in Alexa top 10,000 sites.

Defenses
1. Origin-based defense
2. Frame-based defense
3. CSP extension

Using postMessage

* We collected postMessage receivers from Alexa top 10,000 sites
* ReScope: our tool for collecting receivers

The Postman Always Rings Twice:
Attacking & Defending postMessage in HTML5 Websites
The Postman Always Rings Twice: Attacking & Defending postMessage in HTML5 Websites
Sooel Son and Vitaly Shmatikov
The University of Texas at Austin
Examine `postMessage` uses in Alexa top 10,000 sites.

Defenses
1. Origin-based defense
2. Frame-based defense
3. CSP extension

Introduce safe use patterns.

The Postman Always Rings Twice:
Attacking & Defending `postMessage` in HTML5 Websites
postMessage

Purpose: a "hole" in same origin policy

Hosting page
Using postMessage

http://alice.edu

???

SiteOwner

<script src="http://cntProvider/fancy.js"></script>

http://cntProvider/showFancy.html
function msgReceiver(e) {
    if(e.origin !== "http://hostA")
}

HTML Living Standard (whatwg.org)

Authors should check the origin attribute to ensure that messages are only accepted from domains that they expect to receive messages from.
Why check the origin of received message?

http://myOwnSite.com

// No check
eval( received_msg );
And if the check is wrong?
NDSS 2013 call for papers

The Postman Always Rings Twice: Attacking and Defending postMessage in HTML5 Websites
10:00AM EST

The camera-ready due for NDSS 2013 is coming up
TV WATCH ONLY ON PEOPLE.COM 09:10AM EST

Internet Society 20 years
09:05AM EST

19th Annual Network & Distributed System Security Symposium
Weekly Scoop: November Fun

If this week is any indication, November is shaping up to be a busy month for Idol alumni all over the country! Taylor Hicks, Lee DeWyze, Elliott Yamin and Carrie Underwood are all performing this week!

Check out where your favorite Idols are performing all over the country:

Monday, 11/5
Taylor Hicks performs at The Indigo at The Nightingale Room at the historic West Hollywood Hotel in Los Angeles, CA. Check here for more information.

Saturday, 11/10
Lee DeWyze performs at The Keswick Theater in Glenside, PA. Check here for more information.

Sunday, 11/11
Elliott Yamin performs at The Showbox in Seattle, WA. Check here for more information.

Tuesday, 11/13
Carrie Underwood performs at The Cynthia Woods Mitchell Pavilion in The Woodlands, TX. Check here for more information.

Tuesday, 11/20
Taylor Hicks performs at The Keswick Theater in Glenside, PA. Check here for more information.

Friday, 11/23
Lee DeWyze performs at The Burren in Claremont, CA. Check here for more information.

Tuesday, 11/27
Elliott Yamin performs at The Showbox in Seattle, WA. Check here for more information.

Saturday, 11/30
Carrie Underwood performs at The Cynthia Woods Mitchell Pavilion in The Woodlands, TX. Check here for more information.
• We collected postMessage receivers from Alexa top 10,000 sites
• RvScope: our tool for collecting receivers
Attack page

X-Frame-Header could have prevented our attack...

... only 298 pages use X-Frame-Header among Alexa top 10,000
postMessage Vulnerabilities in the Wild

Among 16,115 pages from 10,121 host names

2,245 hosts (22%) have a postMessage receiver
1,585 hosts have a receiver with no origin check
262 hosts have an incorrect origin check

84 hosts have exploitable vulnerabilities
## Incorrect origin checks

<table>
<thead>
<tr>
<th>Origin check</th>
<th>Host name that passes the check</th>
<th>Existing domains</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>if(/\.[\/]chartbeat\.com$/.test(a\.origin))</code></td>
<td>evil.chartbeat-com</td>
<td>0</td>
</tr>
<tr>
<td><code>if(m\.origin\.indexOf(&quot;sharethis\.com&quot;) != -1)</code></td>
<td>sharethis.comnet.com evilsharethis.com</td>
<td>2,291</td>
</tr>
<tr>
<td><code>if( a\.origin &amp;&amp; a\.origin\.match(\/\.kissmetrics\.com/))</code></td>
<td>www.kissmetrics.comnet.com www.kissmetrics.com.evil.com</td>
<td>2,276</td>
</tr>
<tr>
<td><code>var w = /jumptime\.com:(?:[0-9]\$/; if( !v\.origin\.match(w) )</code></td>
<td>bogusjumptime.com</td>
<td>2</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
<td>Occurrences</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>if(/\[\]/.chartbeat.com$/ .test(a.origin))</code></td>
<td>evil.chartbeat-com</td>
<td>0</td>
</tr>
<tr>
<td><code>if(m.origin.indexOf(&quot;sharethis.com&quot;) != -1)</code></td>
<td>sharethis.com net.com</td>
<td>2,291</td>
</tr>
<tr>
<td><code>evilsharethis.com</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>if(a.origin &amp;&amp; a.origin.match(/\./kissmetrics\./com/))</code></td>
<td><a href="http://www.kissmetrics.com">www.kissmetrics.com</a> net.com</td>
<td>2,276</td>
</tr>
<tr>
<td><code>www.kissmetrics.com evil.com</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>var w = /jumptime\./com(:[0-9]?$/;</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>if(!v.origin.match(w))</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
XSS
Reading cookies
Reading/writing arbitrary values into Web local Storage
Lessons

Perform correct checks on the origin of received messages
Put a correct origin check in every receiver!

Plz, update your code!
the origin of receivers

Put a correct origin check in every receiver!

"correct origin"?
How do I know what origin to check?

Content provider

Put a correct origin check in every receiver!
Threat models

**Light threat model**
- Site owner is honest.
- The receiver in third-party content should accept messages only from site owner's origin.

**Heavy threat model**
- Site owner is malicious.
- Site owner abuses a receiver in third-party content.
Light threat model

- Site owner is honest.
- The receiver in third-party content should accept messages only from site owner's origin.
Heavy threat model

- Site owner is malicious.
- Site owner abuses a receiver in third-party content.

Don't put security-critical operations here!
Defenses

1. Origin-based defense

2. Frame-based defense

3. CSP extension
Origin-based defense with a shared token

- Defense for third-party content
- Works against the "light" threat model
Defenses

1. Origin-based defense

2. Frame-based defense

3. CSP extension
Frame-based Defense

- Defense for third-party content
- Works against the "light" threat model

```javascript
function receiver(evt) {
    if (evt.source !== parent)
        return;
}
```
Works against the "light" threat model

```
function receiver(evt) {
  if( evt.source !== parent )
    return;
}
```
Defenses

1. Origin-based defense

2. Frame-based defense

3. CSP extension
Extended Content Security Policy (CSP)

- Defense for site owners
- Explicitly restricts origins of received messages
- Requires browser support

X-Content-Security-Policy:
msg-src http://www.valid.com *.edu;
Accept postMessage only from http://www.valid.com or *.edu
Defenses

1. Origin-based defense

2. Frame-based defense

3. CSP extension