Evaluating the Security & Privacy Contributions of Link Shimming in the Modern Web

Frank Li

Georgia Tech
Link Navigation Concerns

1. May leak navigation source (via HTTP Referer)
2. Navigation protocol may be less secure (HTTP when HTTPS is available)
3. Navigation destination may be dangerous (e.g., malware, phishing, spam)
Link Shimming 
(aka URL Wrapping)

https://facebook.com/linkshim.php?
u=http%3A%2F%2Fbees.ece.gatech.edu
&h=HASH
Link Shimming
(aka URL Wrapping)

Used by popular online services for over a decade
Link Shimming
(aka URL Wrapping)

What are the security & privacy contributions in the modern web?
Link Shimming vs Modern Web

Check this out! https://bees.ece.gatech.edu

<table>
<thead>
<tr>
<th>Navigation Concern</th>
<th>Link Shimming</th>
<th>Modern Web</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Link Shimming vs Modern Web

<table>
<thead>
<tr>
<th>Navigation Concern</th>
<th>Link Shimming</th>
<th>Modern Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigation Source</td>
<td>Referrer = Link Shim Endpoint</td>
<td>Referrer control via HTML or HTTP Headers (rel=noreferrer or Referrer Policy)</td>
</tr>
</tbody>
</table>
**Link Shimming vs Modern Web**

<table>
<thead>
<tr>
<th>Navigation Concern</th>
<th>Link Shimming</th>
<th>Modern Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigation Destination</td>
<td>Warning Page (may allow clickthrough)</td>
<td>Browser Warnings (e.g., Google Safe Browsing)</td>
</tr>
</tbody>
</table>

---

**Check this out!** [https://bees.ece.gatech.edu](https://bees.ece.gatech.edu)
Data Set

Analyzed 1 month of Facebook data on:

1) Link shim navigations (6B)
   • Timestamp
   • Link shim actions
   • Browser Client Differentiation
   • Browser Client Characteristics

2) Warning Clickthroughs (300M)
Navigation Source Privacy

3 Classes of Browser Clients

- **Fully Legacy**
  - No HTTP Referer privacy mechanisms
  - Link shimming improves referrer privacy

- **Partially Legacy**
  - Supports only rel=noreferrer
  - Link shimming provides different privacy/functionality tradeoff

- **Modern**
  - Supports ReferrerPolicy
  - Link shimming is not needed for source privacy
Navigation Source Privacy

Analyzed fraction of link shim browser clients within each class

<table>
<thead>
<tr>
<th>Browser</th>
<th>Fully Legacy</th>
<th>Legacy</th>
<th>Partially Legacy</th>
<th>Legacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firefox</td>
<td>2%</td>
<td>2%</td>
<td>9%</td>
<td>19%</td>
</tr>
<tr>
<td>Edge</td>
<td>42%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Safari</td>
<td>1%</td>
<td>21%</td>
<td>21%</td>
<td>20%</td>
</tr>
<tr>
<td>Chrome</td>
<td>1%</td>
<td>1%</td>
<td>31%</td>
<td>31%</td>
</tr>
<tr>
<td>Opera</td>
<td>31%</td>
<td>2%</td>
<td>20%</td>
<td>31%</td>
</tr>
<tr>
<td>Vivaldi</td>
<td>2%</td>
<td>42%</td>
<td>13%</td>
<td>33%</td>
</tr>
</tbody>
</table>
23% of South Korean clients are fully legacy due to high IE usage.
Navigation Source Privacy

Analyzed fraction of link shim browser clients within each class

Fully Legacy: 2% 9% 2%
Partially Legacy: 31% 2% 13%

Many African countries had large legacy populations, due to high mobile browser usage.
Navigation Source Privacy

Analyzed fraction of link shim browser clients within each class

Link shimming can improve source privacy for sizable populations of legacy clients.
Analysis of warning clickthrough behavior

- Date: 8/16, 8/23, 8/30, 9/6, 9/13
- CTR (%): 14, 16, 18, 20, 22, 24, 26, 28, 30, 32

3 types of links:
1. Redirection
2. Suspicious URL
3. Possible problem with this link

Warning: We've detected a possible threat from the link: http://EVIL_WEBSITE EXAMPLE. Follow links you trust to keep your account and device secure.
Navigation Destination Security

Analyzed warning clickthrough behavior

Browser warning clickthrough rates [1]:

7.2 - 23.2%

Navigation Destination Security

Analyzed warning clickthrough behavior

Only ~3% of URLs appeared in Google Safe Browsing

Navigation Destination Security

Analyzed warning clickthrough behavior

Link shim warnings
1) have similar clickthrough rates to browser warnings
2) allow site-specific URL detection, beyond browser blocklists
More Results in the Paper!

• Impact of link shimming's navigation protocol upgrading
• Legacy browser populations for different OSes and countries
• Link shim warning adherence for different browsers, OSes, and countries.
• Adherence when re-encountering a warning
• Safety of user clickthrough decisions
Despite modern browser features, link shimming can improve link navigation security & privacy. (Costs: navigation performance, data collection)

Legacy scenarios are prevalent and important.

Website warnings can be effective.

Web security responsibilities are distributed.

Lessons Learned

Thanks!

frankli@gatech.edu
@frankli714