Securing Frame Communication in Browsers
Adam Barth, Collin Jackson, John C. Mitchell

Research Objectives:
Frames are often insufficient isolation primitives because most browsers allow the framed content to navigate other frames. We want to provide display and communication primitives that are robust against unauthorized navigation.

Approach:
We evaluate current navigation policies, which we determine through extensive browser testing. Based on known and new attacks, we advocate the Ancestor navigation policy, which we implement and deploy in the open-source browsers. We also repair two communication techniques by adding confidentiality and authentication.

Frame Communication Mechanisms:
- Microsoft and IBM deployed our suggested improvements to fragment identifier messaging.
- Firefox 3 and Internet Explorer 8 deployed our suggested improvements to postMessage.

Frame Navigation Policies:

<table>
<thead>
<tr>
<th>Browser</th>
<th>Before</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td>IE (with Flash)</td>
<td>Permissive</td>
<td>Ancestor</td>
</tr>
<tr>
<td>Firefox</td>
<td>Window</td>
<td>Ancestor</td>
</tr>
<tr>
<td>Safari</td>
<td>Permissive</td>
<td>Ancestor</td>
</tr>
</tbody>
</table>

Attacks Prevented:
- Guninski Attack
- Recursive Mashup Attack
- Gadget Hijacking
- Reply Attack

Example: window.open("https://www.evil.com/...", "awglogin")