Clickjacking Revisited

A Perceptual View of UI Security

Devdatta Akhawe / Warren He / Zhiwei Li / Reza Moazzezi / Dawn Song

University of California, Berkeley
Clickjacking is a malicious technique of tricking a Web user into clicking on something different from what the user perceives.
Today

Five novel clickjacking attacks that bypass current defenses

Evaluation with 250 users on MTurk
Attack Setup

- Attacker wants to trick user into clicking a button, in our case, the Facebook like button
- Attacker convinces user to play a game on attacker controlled webpage
- Attacker can frame the Facebook Like button, but has no control over the FB display area/frame
- Attacker has full control of remaining display area
Attacker page
A successful attack (bypassing current defenses) requires the like button be fully visible for a noticeable amount of time (say ~500ms)
Destabilizing Pointer Perception
Video Demo
Player starts moving mouse

Fake pointer starts moving to the left (red)

Finally, close to the target, player corrects in a sudden motion, moving the real pointer towards right

Player clicks Like button by mistake

User keeps moving up and right (black), but fake pointer (red) stays left, confusing the user
Successful Attack

• One concern is the appearance of the real pointer when it approaches the like button
  – Attacker has no control over “Like” button frame

• Key Idea: distract the player’s attention with lots of moving images
Real Attack
Attacking Peripheral Vision
Game Setup
Player must leave mouse at bottom of screen

But, watch main game area at top right
Motor Adaptation
Game Setup
Player presented with asteroid
Asteroid explodes when clicked

Mineral produced at constant displacement

Player must click on this mineral for points

Asteroid explodes when clicked
Once trained, put like button instead of mineral
Fast Motion
Mislocalization
Game Setup
Player presented with asteroid with spinning arrow
When arrow stop, mineral shoots out

Player must click on mineral for points
The Flash Lag Effect

- Flash lag is a visual illusion where a moving object, at a particular instant, seems further ahead than it actually is.
- Brain predicts future displacement.
- The player’s click is actually beyond the mineral, but we still award points.
After a few trials, put like button beyond mineral
Visual Cues and Click Timing
Game Setup
Negative points for clicking on grey asteroid

Positive points for clicking on red asteroid
Move asteroid under a like button
Evaluation
### Evaluation

- MTurk study with 50 workers for each attack.
- Some subjects exited before completing the exercise.

**Attacks 2 through 5 work for touch devices too!**

<table>
<thead>
<tr>
<th>Attack Name</th>
<th>Number of subjects</th>
<th>Success Rate (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destabilizing Pointer Perception</td>
<td>50</td>
<td>100</td>
</tr>
<tr>
<td>Peripheral Vision</td>
<td>49</td>
<td>51.02</td>
</tr>
<tr>
<td>Adaptation</td>
<td>46</td>
<td>28.26</td>
</tr>
<tr>
<td>Fast Motion Mislocalization</td>
<td>47</td>
<td>27.66</td>
</tr>
<tr>
<td>Visual Cue for timing</td>
<td>50</td>
<td>50</td>
</tr>
</tbody>
</table>

[MTurk study with 50 workers for each attack. Some subjects exited before completing the exercise. **Attacks 2 through 5 work for touch devices too!**]
This is only a lower-bound ...
Complex Attacks

• Our attacks are simple. Possible to dynamically adapt the attack as user plays the games.
• Better models of pointer movement and click prediction can improve success rates.
• Each attack targets a different limitation of human perception. A combined attack likely to achieve 100% success.
More Attacks

• Human perception is a vast and well studied topic. Many more attacks possible.
• For example, Change Blindness:
  – Well studied phenomenon in which user fails to notice difference in two images.
  – Attacker can switch in a like button and an appropriately primed user won’t notice.
Future Work
Future Work

• Secure UI design needs to take human perception in account while designing interfaces
  – Changes needed to specifications such as the UI Security specification
• Computer Vision based techniques (or machine perception) could be key for defenses
• Designing a secure user interaction mechanism critical for security
evil@berkeley.edu

questions?