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

(wikipedia)

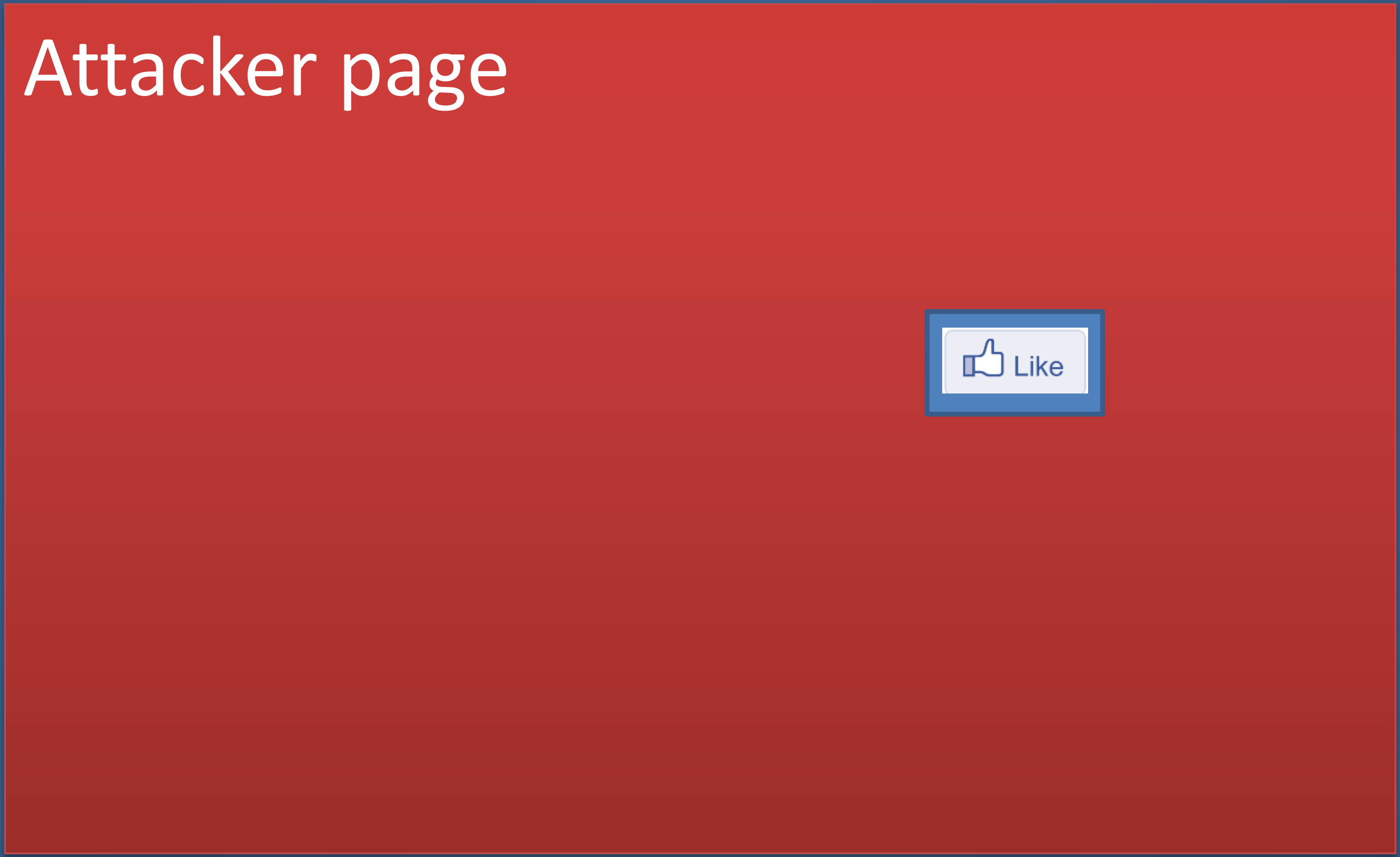
Today

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



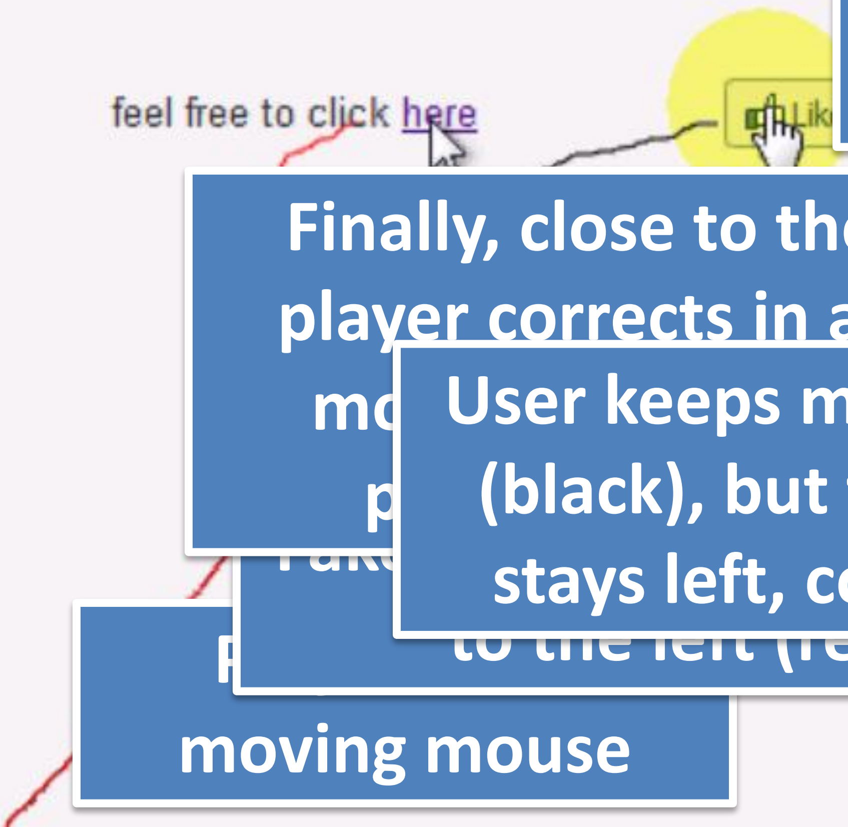
Attacker page

A successful attack (bypassing current defenses) requires the like button be fully visible for a noticeable amount of time (say ~500ms)

1

Destabilizing Pointer Perception

Video Demo



P

moving mouse

Fake

to the left (red)

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

Finally, close to the target, player corrects in a sudden

mo

p

Player clicks Like button by mistake

Successful Attack

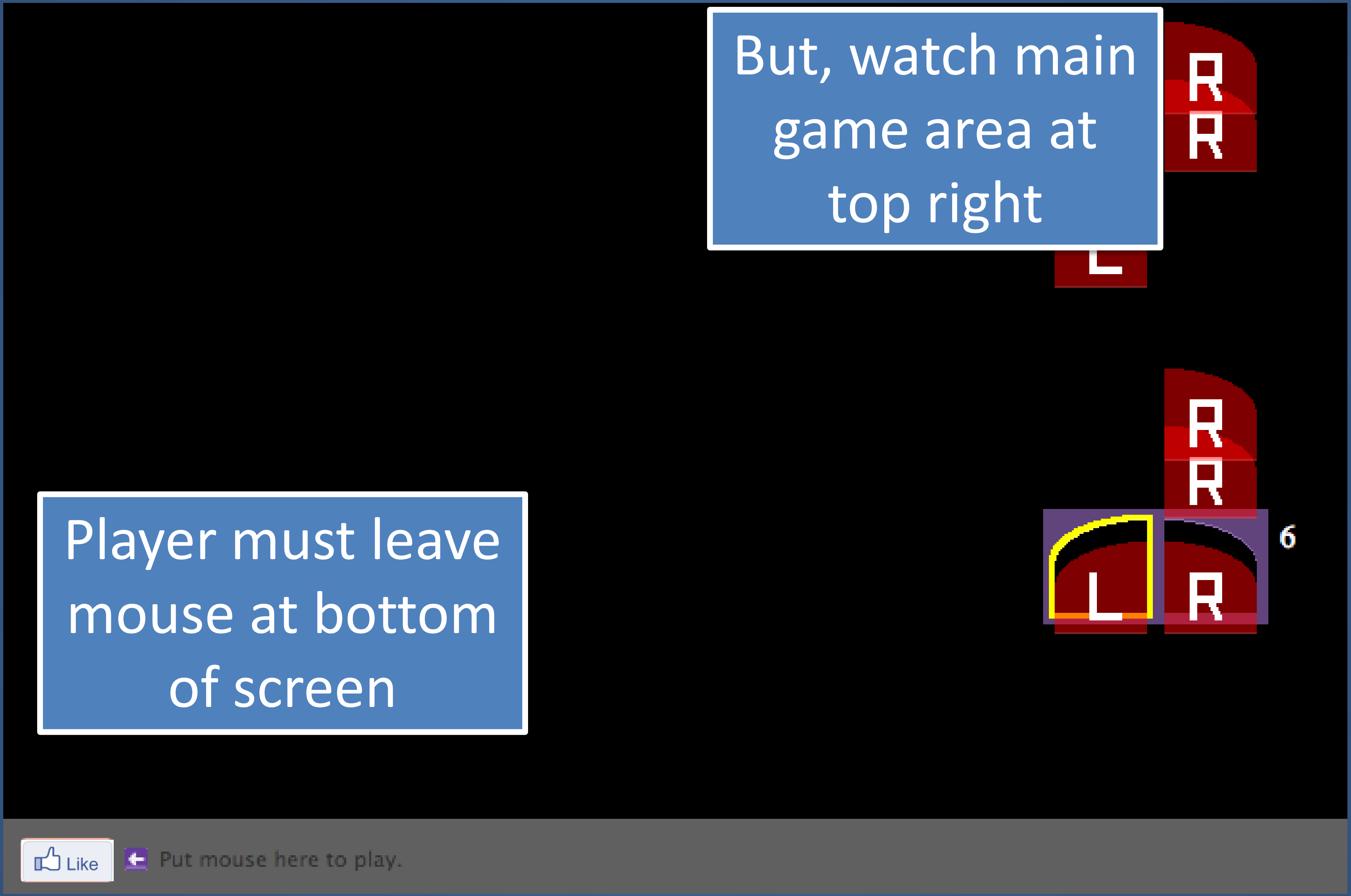
- One concern is the appearance of the real pointer when it approaches the like button
  - Attacker has no control over “Like” button frame
- Key Idea: distract the player’s attention with lots of moving images

Real Attack

2

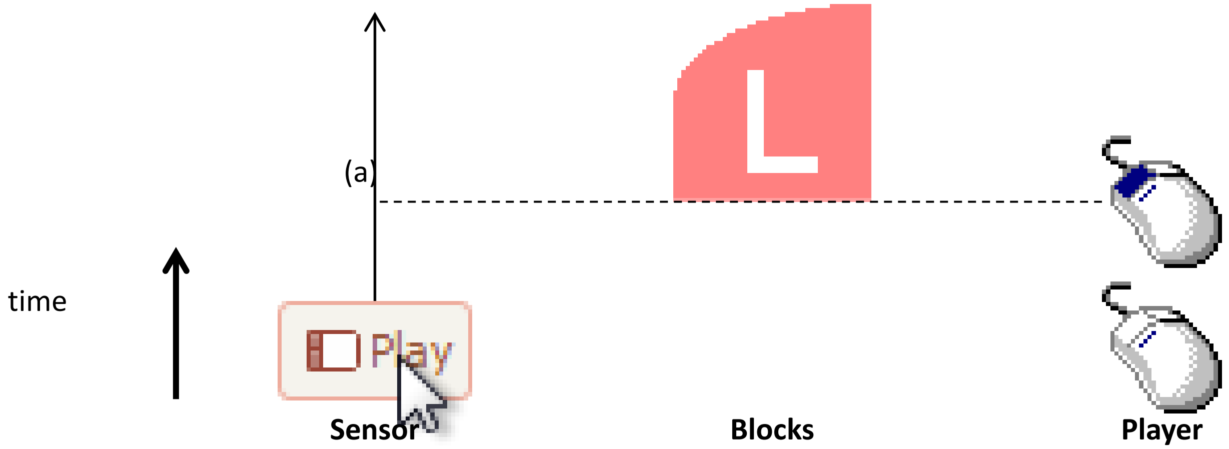
Attacking Peripheral Vision

Game Setup



But, watch main game area at top right

Player must leave mouse at bottom of screen



time

(a)

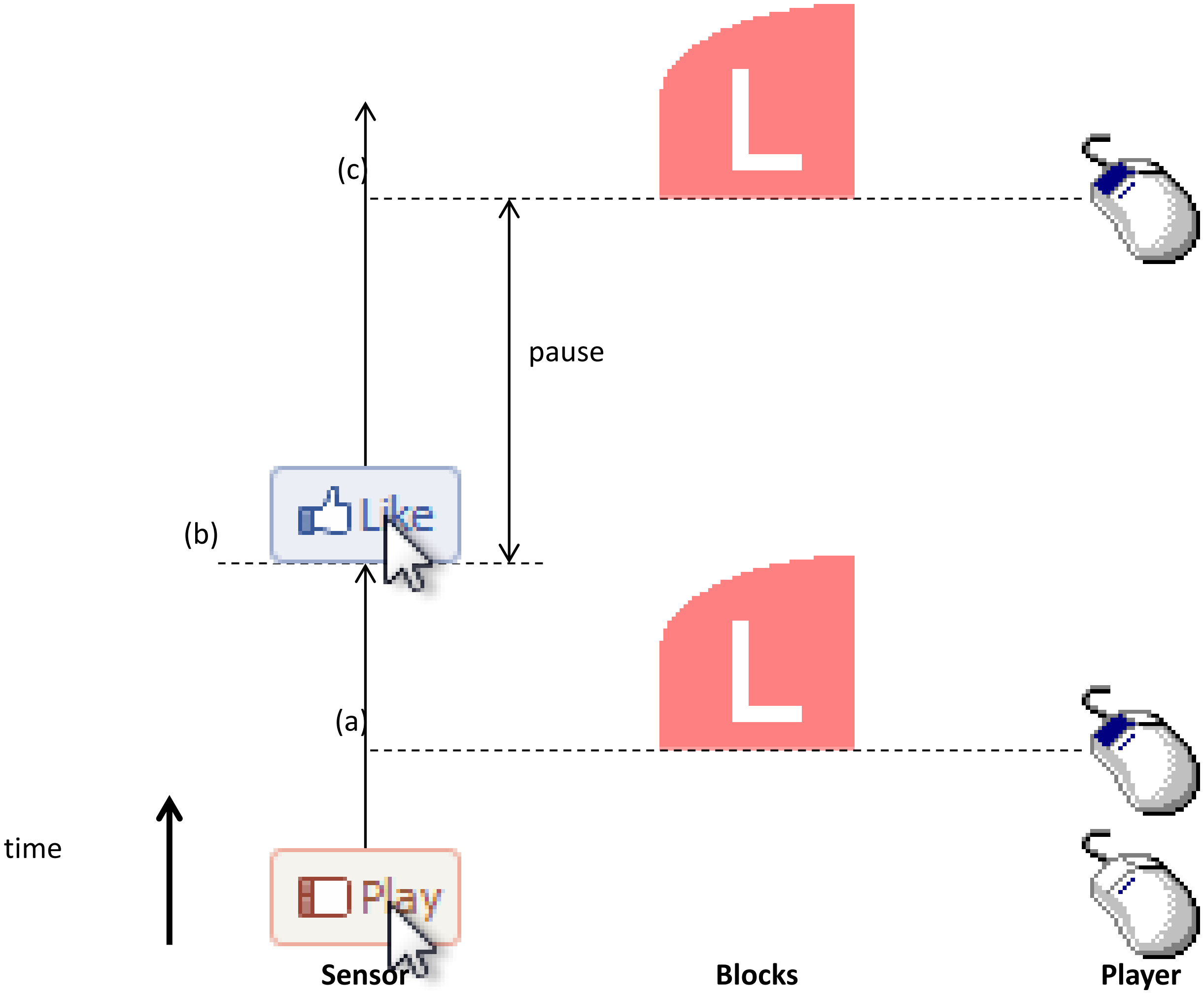
Play

L

Sensor

Blocks

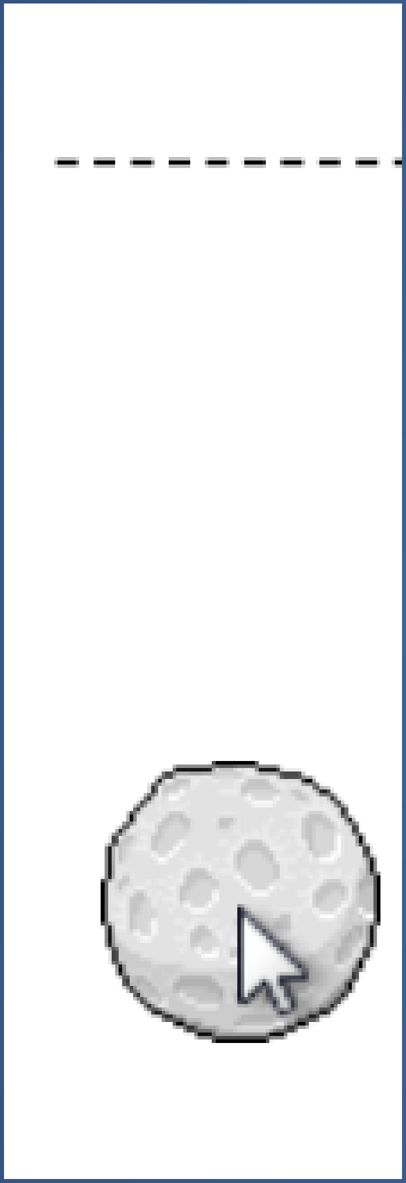
Player


(c)
pause
(b)
Like
L
(a)
L
time
Play
Sensor
Blocks
Player

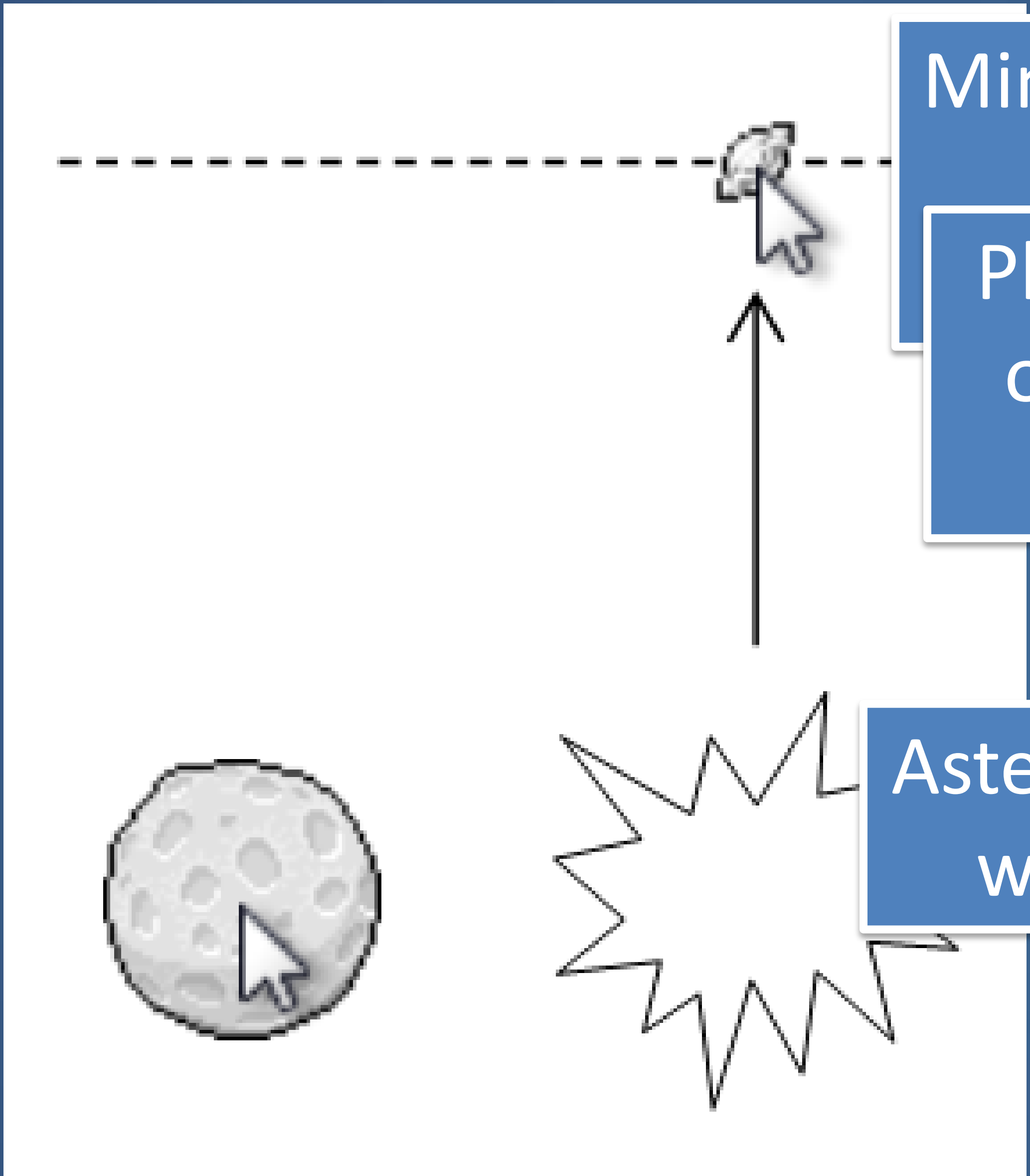
3

Motor Adaptation

Game Setup



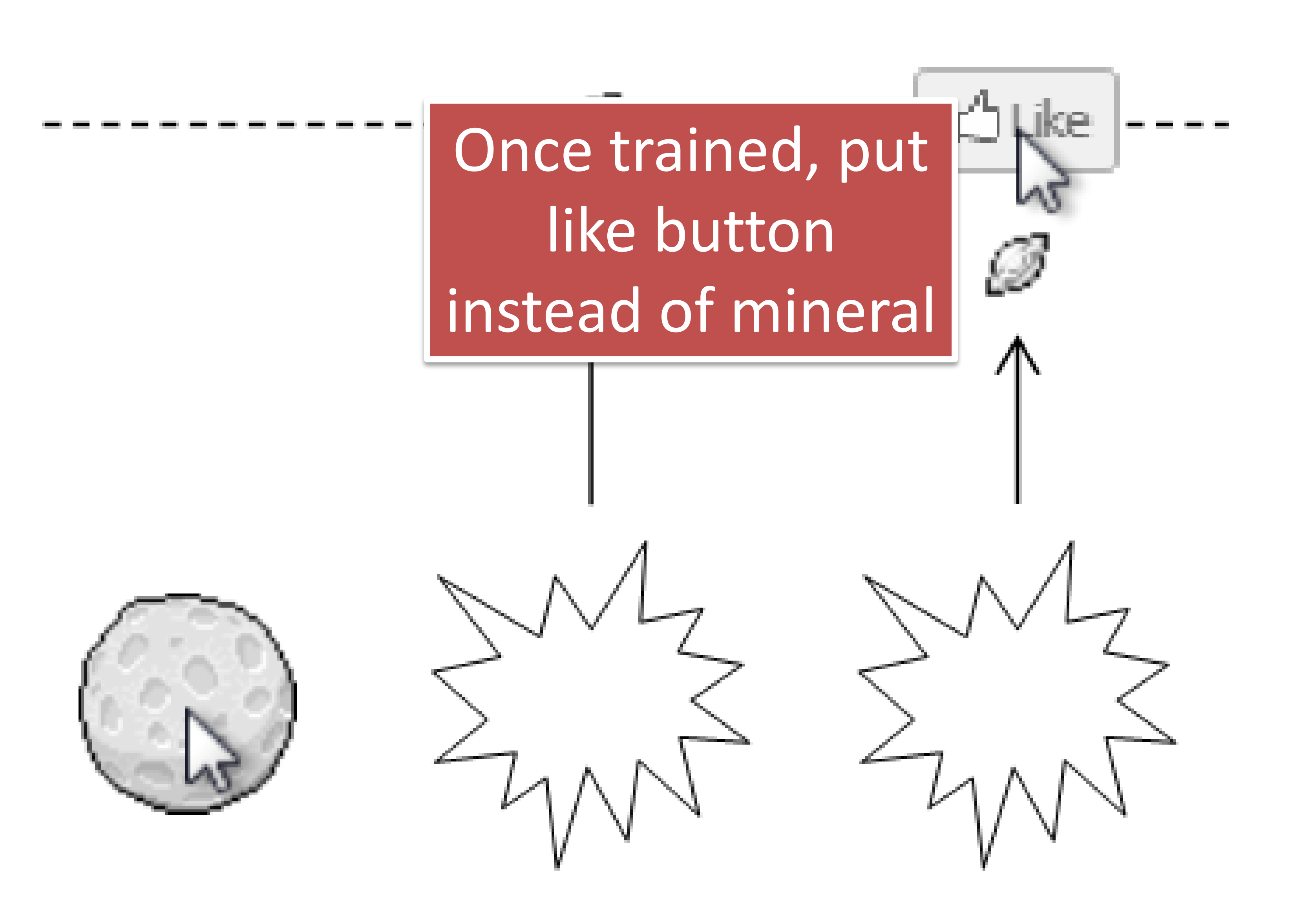
Player presented with asteroid



Mineral produced at constant

Player must click on this mineral for points

Asteroid explodes when clicked



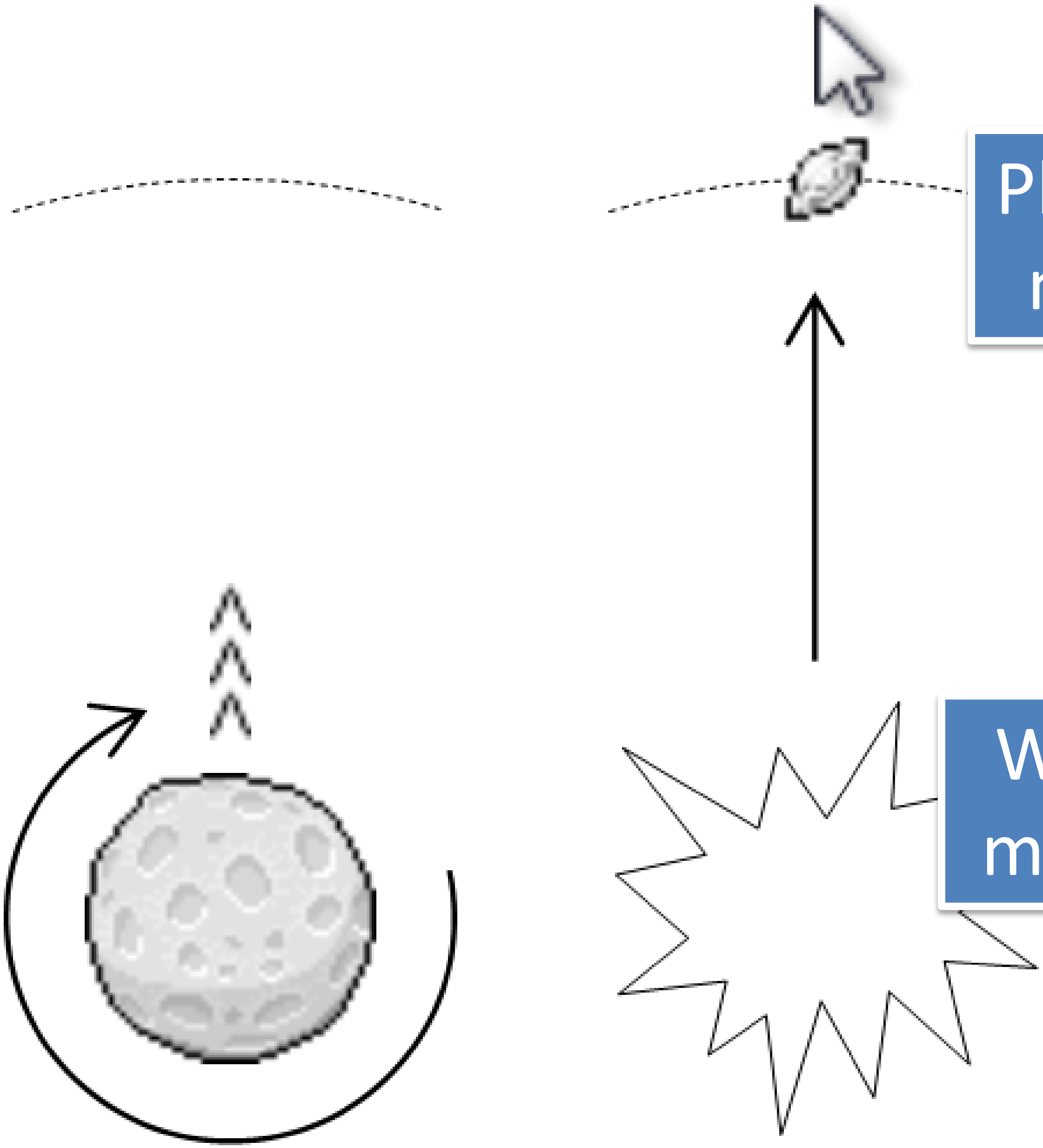
Once trained, put like button instead of mineral

4

Fast Motion Mislocalization

Game Setup

Player presented with asteroid with spinning arrow

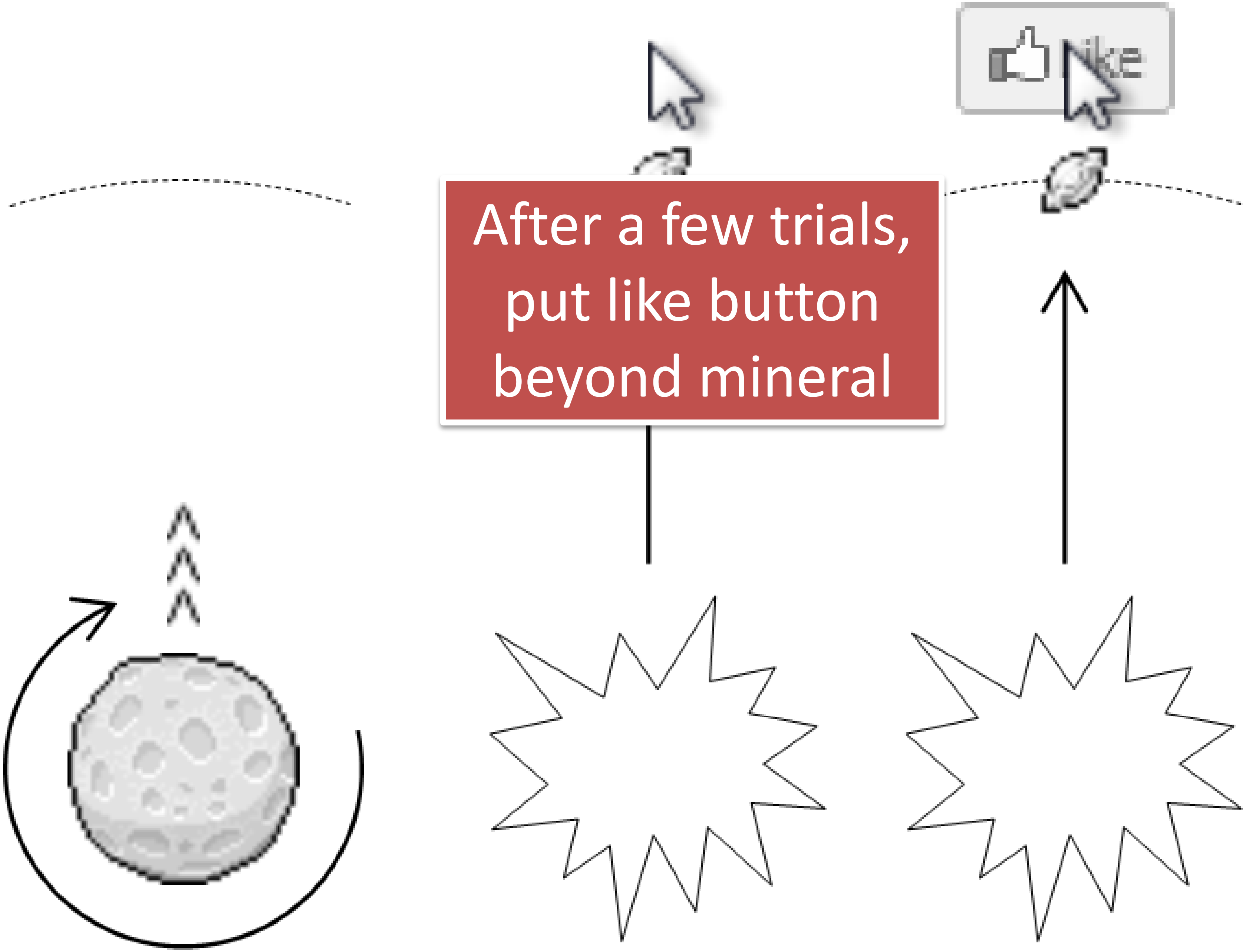


Player must click on mineral for points

When arrow stop, mineral shoots out

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

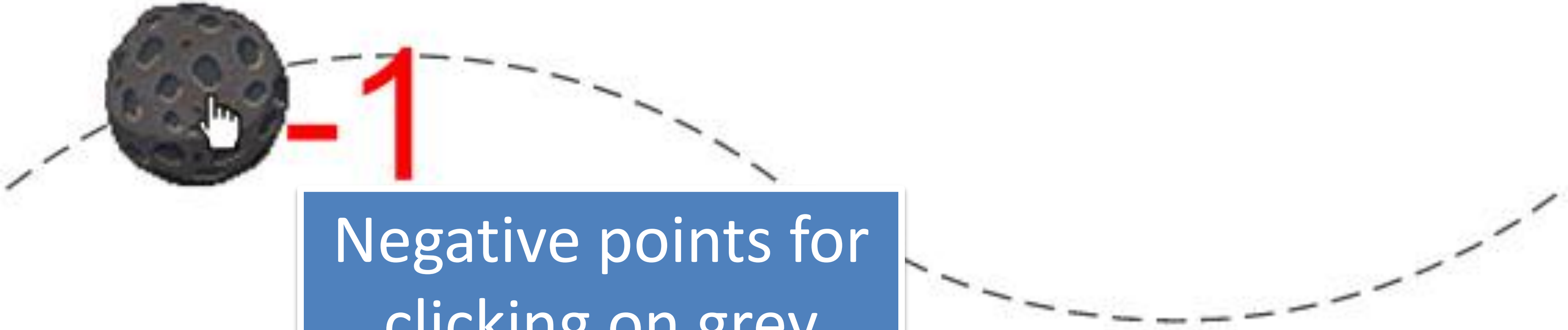


After a few trials, put like button beyond mineral

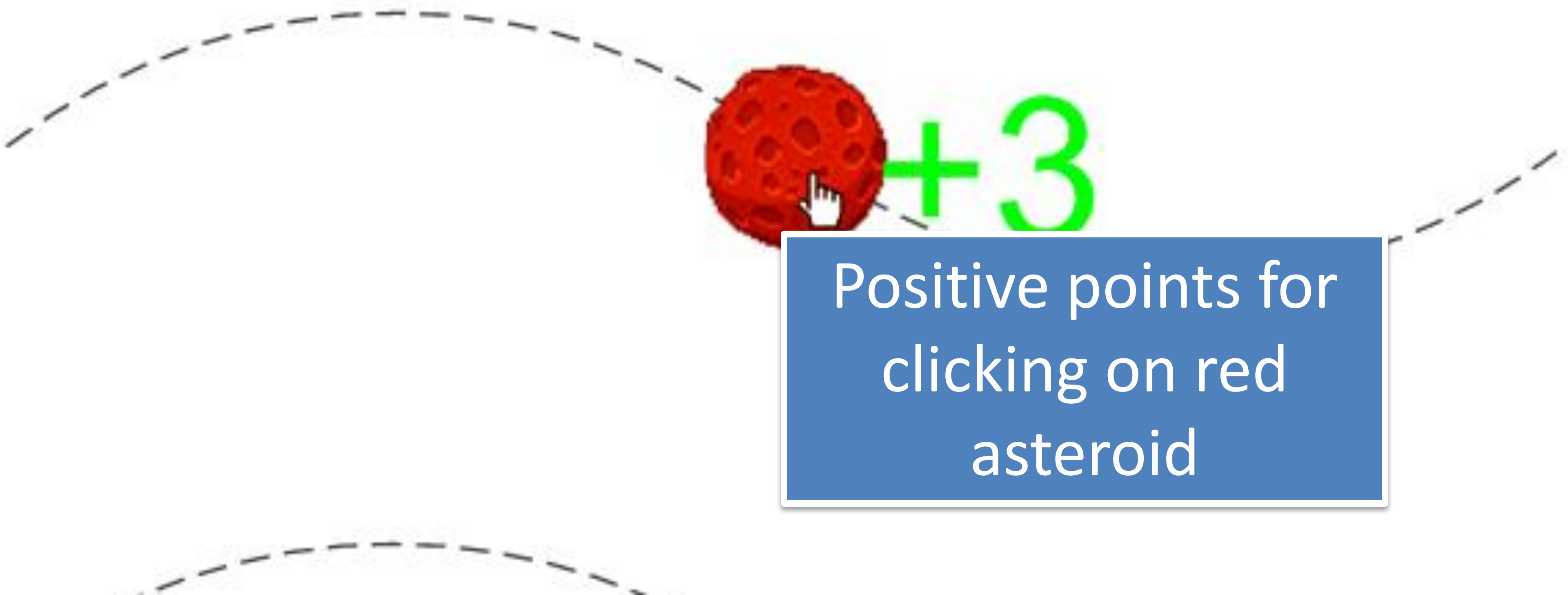
5

Visual Cues
and
Click Timing

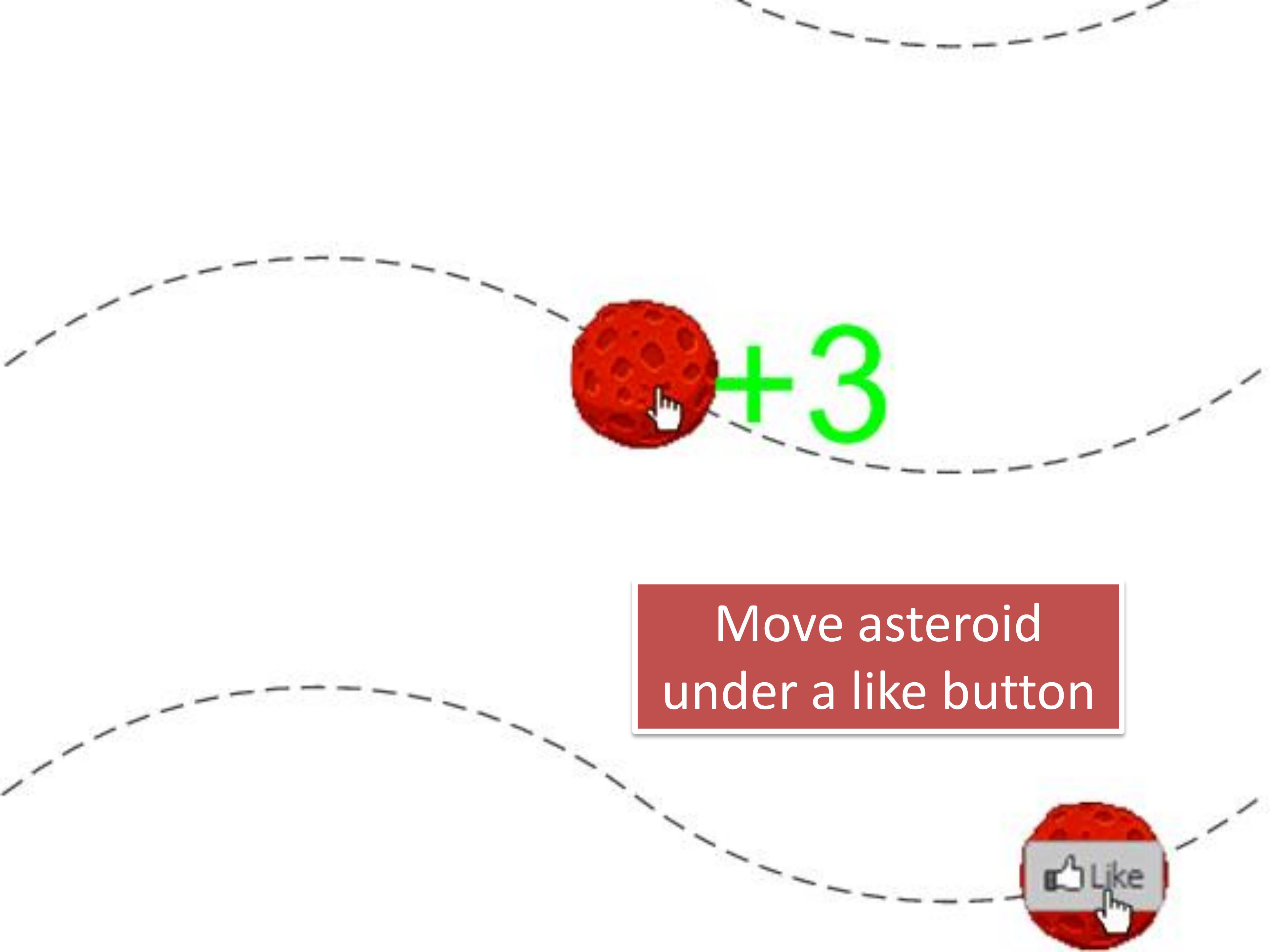
Game Setup



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!

Attack Name	Number of subjects	Success Rate (%)
Destabilizing Pointer Perception	50	100
Peripheral Vision	49	51.02
Adaptation	46	28.26
Fast Motion Mislocalization	47	27.66
Visual Cue for timing	50	50

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?