Wins and learns from the integration of reCAPTCHA at Pinterest

Yuru Shao
Product Security @ Pinterest

Twitter: @YuruShao_
Pinterest: @cuteCatsOverload

June 2022

About Me

- Senior software engineer
- 3 years at Pinterest
- Application security, bot detection, account security, program analysis
- Enjoy pinning cats on Pinterest

Product Security at Pinterest

- One of the four teams under Security org (pinfosec)
- **We're hiring! Check out our booth & pinterestcareers.com**
- Product security
    - Authentication services
    - Secure SDLC
    - Product vulnerability detection and response
    - Bot detection and prevention
    - Account security
    - Pen testing and bug bounty
    - Security review and consulting

Agenda

Bot Detection

Integrating reCAPTCHA

Wins and Learns

Bot Detection

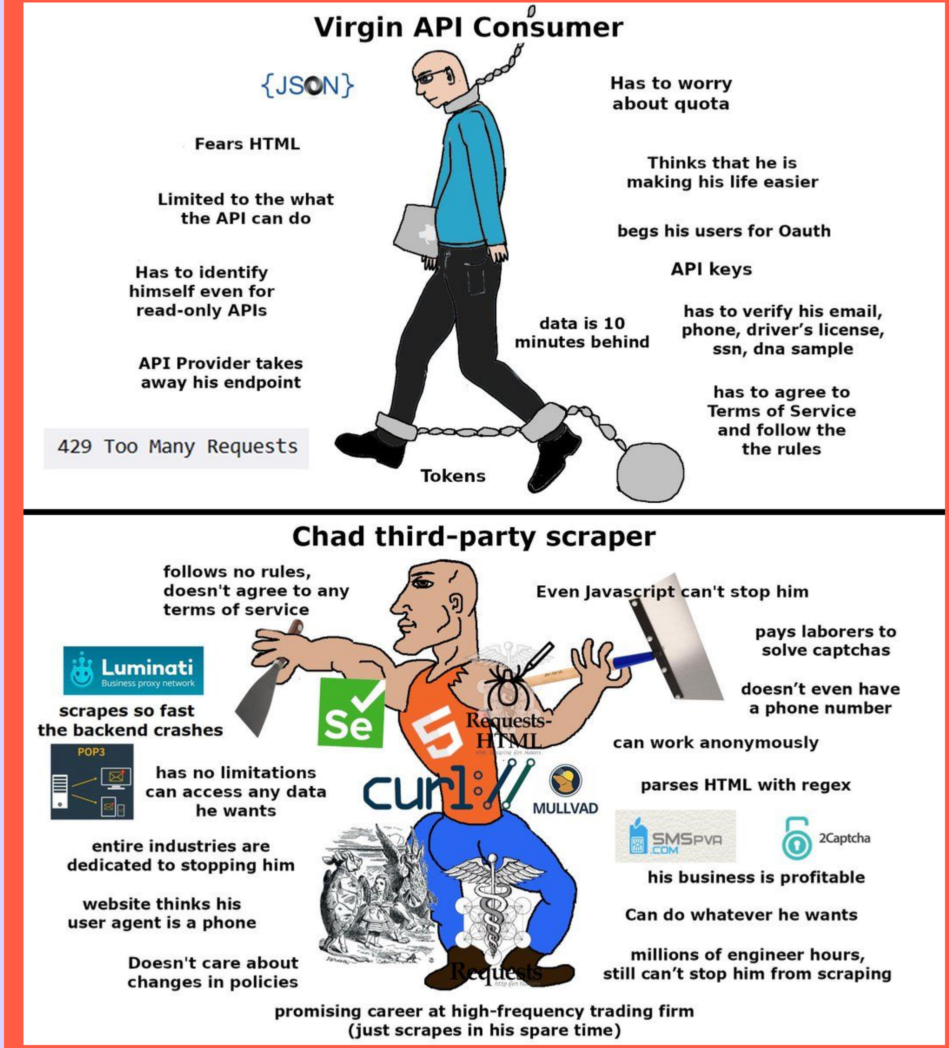
What are bots?

- Programs that perform repetitive tasks.
- Spammers, attackers, fraudsters leverage bots to launch campaigns at scale.

Good vs bad bots

- Good bots
  - Search engine crawlers
  - Feed bots
- Bad bots
  - Spam bots
  - Scraping bots
  - Credential stuffing
  - Fake engagement
  - Payment fraud

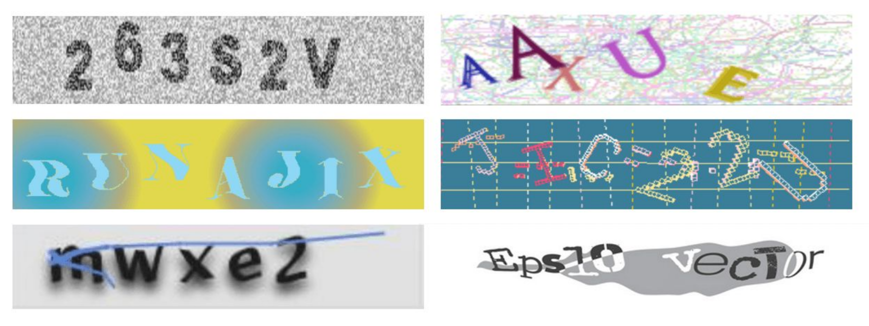
Good vs bad bots

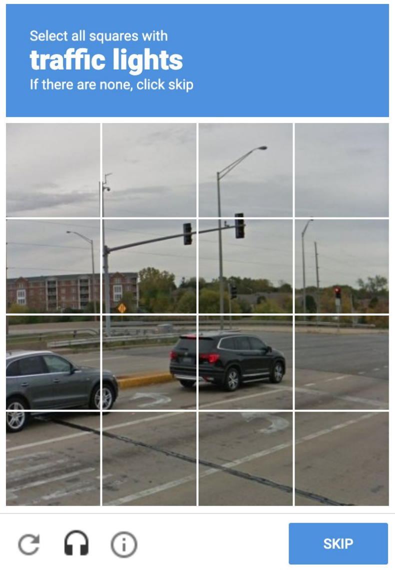

Virgin API Consumer
{JSON}
Has to worry about quota
Fears HTML
Thinks that he is making his life easier
Limited to the what the API can do
begs his users for Oauth
API keys
Has to identify himself even for read-only APIs
data is 10 minutes behind
has to verify his email, phone, driver's license, ssn, dna sample
API Provider takes away his endpoint
has to agree to Terms of Service and follow the the rules
429 Too Many Requests
Tokens
Chad third-party scraper
follows no rules, doesn't agree to any terms of service
Even Javascript can't stop him
pays laborers to solve captchas
Luminati
Business proxy network
doesn't even have a phone number
scrapes so fast the backend crashes
Se
Requests-HTML
can work anonymously
POP3
has no limitations can access any data he wants
curl://
MULLVAD
parses HTML with regex
SMSPVA.COM
2Captcha
entire industries are dedicated to stopping him
his business is profitable
website thinks his user agent is a phone
Can do whatever he wants
Doesn't care about changes in policies
Requests
millions of engineer hours, still can't stop him from scraping
promising career at high-frequency trading firm (just scrapes in his spare time)

Credits to @gf_256

CAPTCHA

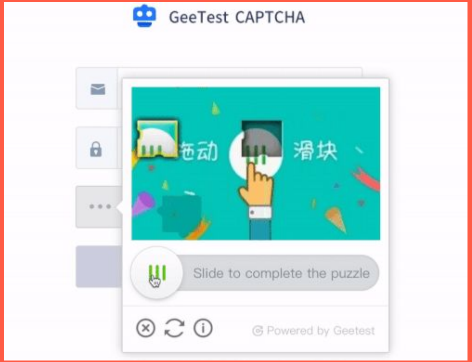
A challenge that is “difficult” for bots, but “easy” for human.




Select all squares with

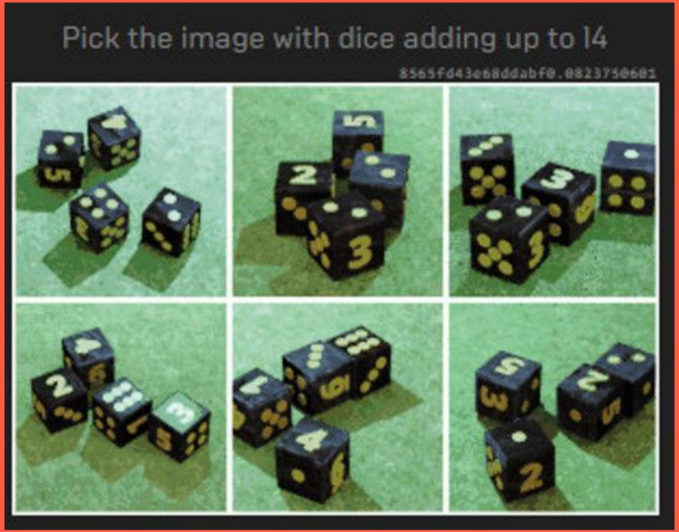
traffic lights

If there are none, click skip



CAPTCHA

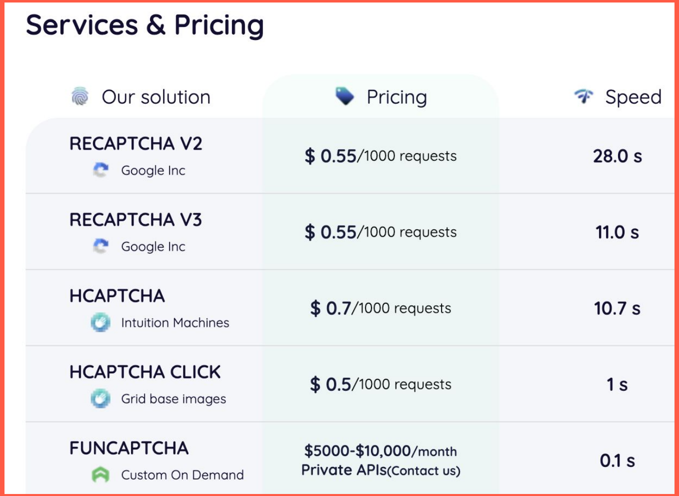
A challenge that is “difficult” for bots, but “easy” for human.



Pick the image with dice adding up to 14

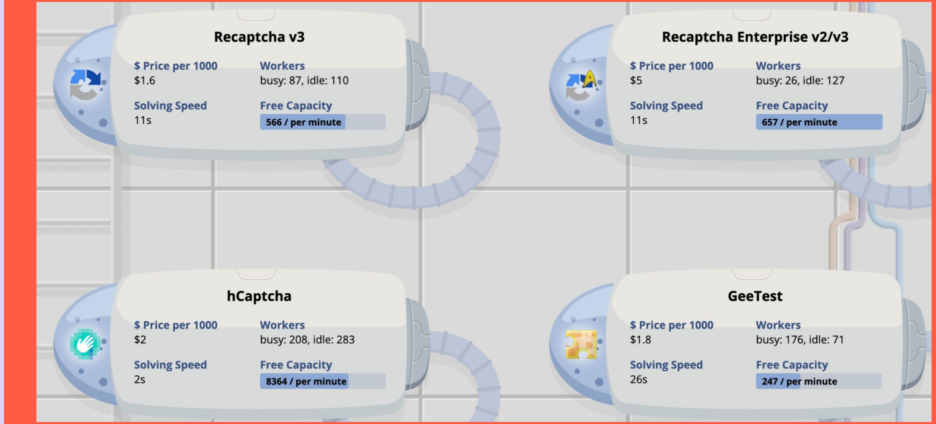
CAPTCHA solvers

- anycaptcha
- 2captcha
- anti-captcha
- ...



Services & Pricing

Our solution	Pricing	Speed
RECAPTCHA V2 Google Inc	$ 0.55/1000 requests	28.0 s
RECAPTCHA V3 Google Inc	$ 0.55/1000 requests	11.0 s
HCAPTCHA Intuition Machines	$ 0.7/1000 requests	10.7 s
HCAPTCHA CLICK Grid base images	$ 0.5/1000 requests	1 s
FUNCAPTCHA Custom On Demand	$5000-$10,000/month Private APIs(Contact us)	0.1 s



	Recaptcha v3	Recaptcha Enterprise v2/v3	hCaptcha	GeeTest
$ Price per 1000	$1.6	$5	$2	$1.8
Workers	busy: 87, idle: 110	busy: 26, idle: 127	busy: 208, idle: 283	busy: 176, idle: 71
Solving Speed	11s	11s	2s	26s
Free Capacity	566 / per minute	657 / per minute	8364 / per minute	247 / per minute

reCAPTCHA

Why we chose reCAPTCHA

- We need client-side signals
- We don’t like interrupting users
- Easy placement and assessment
- SDKs on web and mobile*
- Fine-grained risk scores

```
{
  ...
  "score": 0.1,
  "reasons': ['AUTOMATION']
}
```

reCAPTCHA

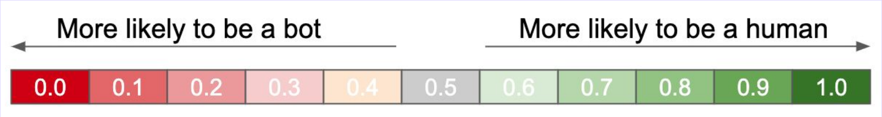
Why it’s probably not the best fit for you

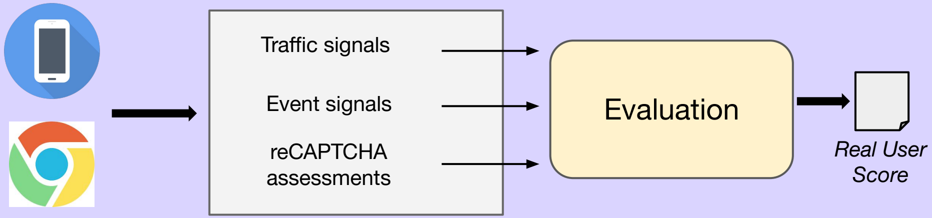
- reCAPTCHA Enterprise is a paid service
- Not available in certain countries/regions
- reCAPTCHA Android SDK depends on Google Play Services

Integrating reCAPTCHA

To Pinterest’s bot detection system

Real user score

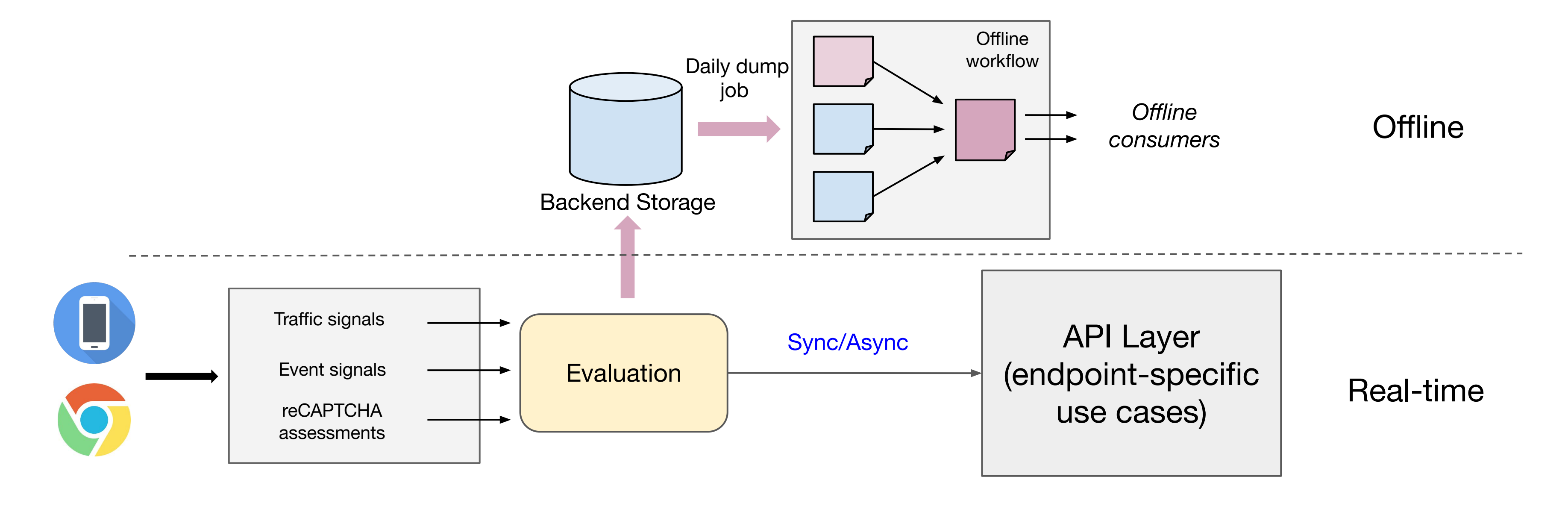




- Principles
    - Collect signals from different layers
    - Evaluate cheaper signals first
    - Easy to use for internal consumers
        - Unification
        - Availability

- Granularity
    - Score evaluated per session
    - In addition to 5 reCAPTCHA-specific reasons, we created 10+ reasons for in-house signals

Real user score



Wins and Learns

Wins

#1 The combinations of score and reason give our consumers the flexibility to tailor detection rules*

- ATO attempts
  - low_score
  - AND (new_city_login OR unknown_browser)
- Spam pin creations
  - low_score
  - AND reason_automation

*Fighting spam with Guardian, a real-time analytics and rules engine (Pinterest Engineering Blog)

Wins

#2 Lots of bots don’t even send us a reCAPTCHA token

- When clients don’t send us a reCAPTCHA token, it’s very likely they don’t have an expected environment
- A curl command vs a browser
- Bots mutated quickly
    - They started to send us invalid/expired/duplicated tokens

Wins

#3 We use reCAPTCHA challenges to evaluate new signals

- We want to evaluate the quality of new signals before shipping them in production

- False positive rate
  - 100 bots challenged (X)
  - 5 completed the challenges (Y)
  - FP rate
    - Y/X = 5/100 = 5%

- Base line
  - 100 real users challenged (X')
  - 90 completed the challenges (Y')
  - baseline
    - Y'/X' = 90/100 = 90%

Learns

#1 Sophisticated automations produce non-suspicious reCAPTCHA assessments results

- Cloud phones, headless browsers can be used to bypass invisible reCAPTCHA
- The cost is much higher than cracking CAPTCHA challenges
- Cannot rely solely on reCAPTCHA

Learns

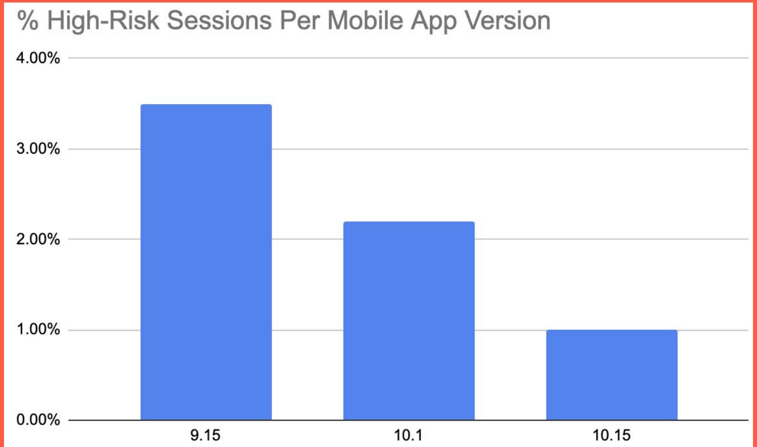
#2 Performance optimization is required to unblock shipping (if you have perf team)

- Options of attaching reCAPTCHA tokens to API calls
  - On-demand creation
  - Preloading and refresh
- We measured pinner waiting time
- Web
  - Preloaded in React component
  - Refresh before tokens expire
- Mobile
  - On-demand creation

Learns

#3 Always painful for backward compatibility

- Traffic coming from legacy client versions needs to be evaluated with other signals
- We discontinued the support of legacy browsers
- We shipped experiences that help users upgrade apps



Learns

#4 There's no one-size-fits-all prevention action

- When we're feeling confident, we block the actions.

- Real user score consumers can choose what actions they want to take.

- We implemented 3 challenge options on different surfaces.
  - "I'm not a robot" checkbox
  - CAPTCHA challenges
  - Email confirmation

Takeaways

reCAPTCHA is a helpful addition to Pinterest's bot signal inventory.

Integration is relatively easy with SDKs, but perf optimization is still needed.

reCAPTCHA alone won't solve all problems.

Create a life you love.