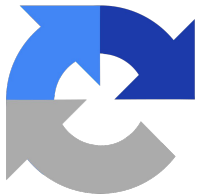
reCAPTCHA and ~~Web Bots~~ Agents

chrisha@google.com

21 July 2025

IETF 123 Madrid

Web Bot Auth BOF



reCAPTCHA

Preface

I realize the protocols being discussed are for identifying *all bots* (crawlers, scrapers, deep research, agents, etc), but I'm largely talking about use cases related to agents.

State of the world

- Automation is heavily associated with abuse, thus anti-abuse systems spend a significant amount of effort identifying it
- Agents are automation, so are guilty by association
- **For agents to succeed, they will need special treatment**

Incentives are aligned

- Users want to automate their tasks
- Agents want to provide user value and succeed
- Sites wants users (including via agents) to use their services
- **Anti-abuse operators are in the way right now**

Key use cases we care about

- Anti-abuse
- Verifiability / Anti-Spoofability
- Discoverability
- Visibility / Auditability
- Policy controls
- Reduced manual maintenance

The underlying entity

- Agent platforms and security proxy operators are both traffic aggregators in some sense, and are doing things **on behalf of** some other entity / individual.
- Mixing traffic across those entities makes anti-abuse much harder.
- **We want to be able to segment per entity traffic in a pseudonymous manner (mindful of privacy).**
- **Why:**
  - **Enable per-entity reputation tracking for anti-abuse.**
  - **Don't penalize everyone for the bad actions of a few.**
- **Out of scope:**
  - **We don't need or want authoritative user identity.**
  - **This is not for authorization / authentication**

Collaborative policing

- Anti-abuse providers will naturally use an agent operator identity as a context for reputation
- Bad users drag down operator reputation
- Incentives aligned for agent operators and anti-abuse services to share data about bad users
- **We'd love to have a feedback loop. A way to reach back to an agent and tell them that a particular interaction was bad (and vice-versa).**
- **Why:**
  - **Help the ecosystem succeed, by sharing insights with operators.**
  - **Clean up abusive traffic at the source.**

Nice to have, in the future...

Multi-agent systems

- Agents will end up collaborating, delegating and using tools.
- **We want to be aware of the whole stack. (Agent A → Agent B → MCP Server C → Site).**
- **Why:**
  - **Auditability**
  - **Facilitate writing policy**
  - **Hierarchical reputation tracking for anti-abuse**

Nice to have, in the future...

Multi-tenant agent platforms

- Agent platforms will be allow customers to create their own agents as customizations of a base agent, and host/operate them on their behalf.
- **We want to be able to identify traffic from different derived agents on a platform, but still know the platform that is providing the base model.**
  - **Agent Foo built on Google Gemini, vs Agent Bar built on Google Gemini.**
- **Why:**
  - **Auditability**
  - **Facilitate writing policy**
  - **Hierarchical reputation tracking for anti-abuse**

Nice to have, in the future...

Deployment modes

- Right now, most agents are virtual browser in the cloud, using operator-managed resources.
- Agents-in-browser are coming soon (Browser Co Dia, Chrome, Perplexity Comet, OpenAI browser)
- Self-hosted bespoke agents are likely
- Agents as containers are likely
- On-prem hardware may come too
- **We want a mechanism that scales to these alternative deployment modes.**
- **Why:**
  - **To incentivize participation in all modalities.**
  - **To lower the barrier to entry for developers.**