Annotated Bibliography

Godfred Tekpor

January 29, 2026

References

[1] Ankit Gangwal, P. Sahithi Reddy, and C. y. k. Sagar. *Swiss Cheese CAPTCHA: A Novel Multi-barrier Mechanism for Bot Detection*, pages 1780–1789. Association for Computing Machinery, New York, NY, USA, 2025.

> The paper proposes ”Swiss Cheese CAPTCHA,” a multi-step challenge meant to stay easy for humans but harder for bots by stacking several independent obstacles under a time limit, including signals from device sensors through the Generic Sensor API. It reports two user studies showing most people can complete the challenge in about 5–6 seconds with high success rates, and it uses trajectory data to study how users recover from mistakes and learn the task. The paper also tests security by building an automated attack and finds a low success rate for that attack in their experiments. A strong point is that it evaluates both usability and security, which matters for real e-commerce defenses, while a limitation is that the sensor-based design may not work as well in desktop-heavy reseller scenarios where sensor access is limited. For a navigation-pattern risk scoring system, the main value is as an escalation tool: suspicious sessions can be routed into a stronger challenge instead of being blocked outright, and the paper offers a clear way to measure the security–friction tradeoff when adding that step to a layered defense pipeline.

[2] Christos Iliou, Theodoros Kostoulas, Theodora Tsikrika, Vasilios Katos, Stefanos Vrochidis, and Ioannis Kompatsiaris. Web bot detection evasion using deep reinforcement learning. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ARES '22, New York, NY, USA, 2022. Association for Computing Machinery.

> The paper examines whether bots can learn browsing and navigation patterns that slip past behavior-based detectors built from web-log features. It models evasion as a reinforcement learning problem where a bot chooses actions to shape session features while still completing its goal, using a pre-trained detector as the environment and getting rewarded when it is not flagged. Results show simple scripted bots rarely evade, but RL-trained bots can learn evasive strategies and reach much higher evasion rates, with some settings

approaching about half of bot sessions avoiding detection after enough training. The paper then shows an attacker–defender loop: once the detector is retrained on the new behaviors, bots can train again and regain evasion capability. A key strength is the explicit adversarial setup and staged evaluation over time, while a limitation is that the experiments focus mainly on manipulating web-log features and do not fully incorporate real reseller-bot constraints like identity and payment linkages, queueing, and rate limits. For navigation-pattern risk scoring, the paper provides a clear threat model and a reusable stress-test method by training adaptive bots to minimize a risk score while still reaching add-to-cart and checkout.

[3] Christos Iliou, Theodoros Kostoulas, Theodora Tsikrika, Vasilis Katos, Stefanos Vrochidis, and Ioannis Kompatsiaris. Detection of advanced web bots by combining web logs with mouse behavioural biometrics. *Digital Threats*, 2(3), June 2021.

This paper presents a detection framework aimed at advanced web bots that spoof browser fingerprints and attempt to imitate human browsing. It builds two separate detectors: one based on session-level web-log features (navigation paths, timing, and request patterns) and another based on mouse-movement features, then fuses the two scores with a rule that relies more heavily on mouse evidence and uses the web-log score when the case is uncertain. The evaluation uses a controlled test site with human sessions plus two bot classes, moderate bots that mainly spoof fingerprints and advanced bots that also simulate humanlike browsing and mouse behavior. Results show the fused approach performs better than a web-log-only detector and remains effective under attempted behavioral imitation, with very strong reported classification metrics. A key limitation is external validity: because the study uses a test environment and simulated bots, real reseller-bot campaigns that use proxy rotation, distributed accounts, and trace replay could shift the feature distributions and reduce performance.