Machine Learning to Block Trackers Embedded in Apps

Abstract

Tracking infrastructure is rife within modern networked ecosystems. Identifying that the accumulation of virtual identity within the hands of analytic vendors is not always in the consumers interest, tracker blocking services have gained popular promise. While conventional blocking services have blocklists, this paper proposes an alternative strategy which learns in real time through a multi-armed bandit framework what connections are 'blockable' and what are not. The model learns through the reinforcement learning paradigm whereby beliefs on trackers are updated in response to reward assumed on the actions taken by the model. A number of MAB solutions are subject to analysis, with an assumed suitable model injected into Blokada, an existing open-source tracking firewall.