УДК 004.056.53

Исследование применимости несигнатурной модели брандмауэра веб приложений

Гончаров И.М.[1] Ермилов Д.В.[1] Куликов А.А.[1] Подобрянский К.О.[1]
[1]Московский физико-технический институт (государственный университет)

В последние годы увеличивается популярность веб приложений как основных поставщиков услуг в интернете. Это связано с развитием веб технологий, в том числе с удобством и простотой использования. Такое возрастание популярности заставляет задуматься о способах защиты приложений, так как они становятся главными целями кибер атак. Успешные атаки приводят к финансовым потерям и сбоям в работе приложений. Одним из способов защиты являются брандмауэры веб приложений [1], производящие мониторинг HTTP соединений.

Создание эффективного брандмауэра веб приложений совсем не простая задача как раньше, так и сейчас. Основным на данный момент является сигнатурный метод распознавания атак, основанный на поиске сигнатур атак в актуальной базе данных. Как следствие, такие брандмауэры уязвимы к атакам нулевого дня и к атакам, чьи сигнатуры сложно или даже невозможно создать.

Иным методом является создание модели нормального поведения веб приложений. Она базируется на информации, полученной из HTTP запросов, сгенерированных клиентом на веб сервер. Если в рабочем режиме брандмауэра запрос не попал в зону нормального поведения, то он считается опасным. Одним из способов реализации данной модели является применение машинного обучения[2].

Машинное обучение находится на стыке математической статистики, методов оптимизации и классических математических дисциплин[3]. Многие его методы направлены на извлечение знаний из имеющихся данных.

В рамках данной работы проведены следующие шаги: подготовка испытательного стенда брандмауэра веб приложений; создание несигнатурной модели с применением машинного обучения; анализ возможности детектирования как известных, так и неизвестных брандмауэру атак, а также нормального трафика; сравнение с современными открытыми аналогами.

Литература

[1] S.Prandl, M.Lazarescu, D.S.Pham, *A Study of Web Application Firewall Solutions* // Information Systems Security: 11th International Conference, 2015, p. 501–510

[2] R.Kozik, M.Choraś, R.Renk,W.Holubowicz, *A Proposal of Algorithm for Web Applications Cyber Attack Detection* // Computer Information Systems and Industrial Management, 2014, p. 680–687

[3] Машинное обучение // Википедия, https://ru.wikipedia.org/wiki/Машинное_обучение