УДК 004.056

АНАЛИЗ СУЩЕСТВУЮЩИХ ТЕХНОЛОГИЙ ПРОТИВОДЕЙСТВИЯ ОТСЛЕЖИВАНИЮ И СБОРУ ЦИФРОВЫХ ОТПЕЧАТКОВ БРАУЗЕРОВ

Царев И.П. (Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Научный руководитель – к.т.н., доцент Гирик А.В.

(Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

В работе рассматриваются технологии противодействия отслеживанию и сбору цифровых отпечатков браузеров пользователей веб-приложений. Проведен анализ каждой технологии с оценкой эффективности и учетом недостатков использования. Предложены меры, позволяющие повысить приватность и конфиденциальность пользователей без ущерба производительности и сохранить удобство пользования веб-ресурсами.

Введение. Сбор цифровых отпечатков браузера, реализующийся с целью идентификации и отслеживания действий пользователей без их согласия, можно трактовать как существенную уязвимость веб-приложений, нарушающую неприкосновенность частной жизни.

Чтобы сохранить приватность и конфиденциальность при использовании веб-приложений крайне важно обеспечить безопасную связь между браузером пользователя и самим приложением. Для этого необходимо предоставлять интересующему ресурсу только ту информацию, которая необходима для его нормального функционирования. Зарубежные работы в основном ориентированы на то, какие данные пользователя и как собирать для формирование уникального профиля, что, с одной стороны, противоречит теме данной работы, но с другой, помогает понять, какие данные требуется защищать. Отечественный опыт в исследовании противодействия отслеживанию и сбору цифровых отпечатков браузеров практически отсутствует.

Целью данной работы является анализ технологий противодействия сбору излишней для работы веб-приложений идентифицирующей информации о пользователях, оценка эффективности этих технологий и выработка мер, позволяющих повысить анонимность пользователей без ущерба производительности и с сохранением удобства пользования.

Основная часть. Под цифровым отпечатком браузера понимается совокупность данных о программном и аппаратном обеспечении удаленного вычислительного устройства, которую веб-ресурс может получить, запросив эту информацию при загрузке страницы.

Для того чтобы веб-ресурс не смог собрать цифровой отпечаток браузера, можно использовать два подхода: либо блокировать лишние действия при запуске, либо отдавать ресурсу неполную или неправильную информацию.

Анализируя существующие технологии противодействия отслеживанию и сбору цифровых отпечатков браузера, а также, анализируя работы, целью которых является идентификация пользователей при посещении веб-приложения, были выделены основные данные, которые ресурс может использовать для формирования уникального профиля пользователя и дальнейшего отслеживания его действий. Далее рассматриваются существующие технологии, позволяющие эти данные от веб-ресурса скрывать или передавать ему неполную или неверную информацию.

На основе полученных данных, предлагаются наиболее эффективные меры, позволяющие уменьшить уникальность профиля, тем самым увеличивая анонимность пользователей, при этом упор поставлен на сохранение при этом удобства пользования веб-приложениями и должной производительности всей системы. Эффективность исследуется с помощью открытых сервисов, занимающихся тематикой цифровых отпечатков браузера (coveryourtracks.eff.org, browserleaks.com и amiunique.org).

Выводы. Использование предложенных мер позволит снизить несогласованное отслеживание пользователей при посещении веб-приложений и повысить ощущение свободы в сети Интернет.

Разработчики веб-браузеров смогут почерпнуть некоторые из приведенных мер для внедрения в свои разработки, что должно привлечь большее количество пользователей и обезопасить их.

Также результаты данной работы позволят научному сообществу как развивать меры противодействия отслеживанию и сбору цифровых отпечатков браузеров, так и усложнять разработки для обхода этих мер и поиска новых данных, позволяющих формировать уникальные профили пользователей.