УДК 004.056

С. В. Хилько[1]

ІДЕНТИФІКАЦІЯ КОРИСТУВАЧІВ НА ОСНОВІ FINGERPRINTING БРАУЗЕРА

[1] Вінницький національний технічний університет

Анотація
Проаналізовано особливості використання технології для анонімної ідентифікації браузерів.
Ключові слова: ідентифікація, кібербезпека, cookie, fingerprinting, браузер.

Abstract
The peculiarities of using the technology for anonymous identification of browsers are analyzed.
Keywords: identification, cybersecurity, cookie, fingerprinting, browser.

Для запровадження ідентифікації користувачів існує цілий ряд причин. Наприклад, щоб дізнатися, чи вперше користувач зайшов на сайт, щоб показувати тільки релевантні рекламні оголошення з товарами, якими справді цікавився відвідувач, або для внутрішньої аналітики. Тому потреба в такому інструменті надзвичайно висока, адже це відкриває широкий спектр нових можливостей.

Зазвичай, для ідентифікації користувачів використовуються cookie. Це простий механізм і всі розробники знають, як з ним потрібно працювати. Однак, отримуючи простоту доводиться жертвувати надійністю. Пересічний користувач може легко змінити або видалити свої cookie, таким чином однозначно його ідентифікувати стає неможливим. Коли стало зрозумілим, що користувачі видаляють файли cookies самостійно з'явились EverCookie [1]. Вони намагаються зберегтись у якомога більший кількості місць. Таким чином, пересічний користувач не зможе їх модифікувати або видалити. Однак, якщо використовується режим інкогніто, то дана маніпуляція не спрацює, адже в ньому браузер не зберігає нічого на диск.

Таким чином перед розробниками постала задача розробити механізм анонімної ідентифікації користувачів. Саме так з'явилися технології цифрових відбитків (fingerprinting) [2].

Fingerprint – ідентифікує користувача не по спеціальним міткам, що збережені на його комп'ютері, а по унікальним особливостям браузера, системи та пристрою. Якщо cookie працюють тільки в рамках одного домену, то унікальні особливості залишаються незмінними при відвідуванні різноманітних сайтів. Таким чином слідкувати за користувачами стає простіше.

При використанні даної технології формуються унікальні ідентифікатори шляхом об'єднання набору параметрів, що доступні у середовищі браузера, кожен з яких окремо не представляє ніякої цінності, однак разом формують унікальне значення машини:

- User-Agent. Видає версію браузера, версію ОС і деякі з встановлених доповнень.
- Хід годинника. Якщо система не синхронізує свій годинник зі сторонніми серверами часу, то рано чи пізно вони почнуть відставати або спішити, що породжує унікальну різницю між реальним та системним часом, яку можна виміряти з точністю до мікросекунди за допомогою JavaScript.
- Список встановлених в системі шрифтів (можна отримати за допомогою getComputedStyle API).
- Список усіх встановлених плагінів, включаючи їх версії (можна отримати через перебір navigator.plugins[]).
- Інформація про встановлені розширення та інше ПЗ. Такі розширення, як блокувальники реклами, вносять зміни в сторінки, які переглядають користувачі.

Ще одним механізмом, що використовується при створенні відбитку є Canvas [3]. Дана техніка ідентифікації реалізовує приховане малювання рисунку на сторінці. Після чого виконується аналіз на предмет особливостей виводу, специфічних для використовуваного графічного стеку, GPU та відеодрайверу. У невидимому iframe малюється рисунок і текст, після чого створена картинка зчитується за допомогою getImageData() і генерується геш завантажених даних, що виступає ідентифікатором.

Також, популярним рішенням є використання WebGL Fingerprint. Це покращена версія Canvas. Суть

полягає у тому, що на сторінці малюються 3D-трикутники, потім на них накладаються різноманітні ефекти. Після чого формується масив байтів, який буде відрізнятися в залежності від пристрою. Приклад параметрів, які використовуються при створенні WebGL Fingerprint наведено на рис. 1.

Рисунок 1 – Приклад параметрів при створенні WebGL Fingerprint

Приклад використання технології fingerprinting браузера наведено на рис. 2. [4]

Атрибут	Source	Приклад
User agent	HTTP header	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.119 Safari/537.36
Accept	HTTP header	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Content encoding	HTTP header	gzip, deflate, br
Content language	HTTP header	en-US,en;q=0.9
Список плагінів	JavaScript	Plugin 1: Chrome PDF Plugin. Plugin 2: Chrome PDF Viewer. Plugin 3: Native Client. Plugin 4: Shockwave Flash...
Cookies enabled	JavaScript	yes
Use of local/session storage	JavaScript	yes
Часовий пояс	JavaScript	-60 (UTC+1)
Розширення екрану та глибина кольору	JavaScript	1920x1200x24
Список шрифтів	Flash or JS	Abyssinica SIL,Aharoni CLM,AR PL UMing CN,AR PL UMing HK,AR PL UMing TW...
	HTTP headers	Referer X-Forwarded-For Connection Accept Cookie Accept-Language Accept-Encoding User-Agent Host
Платформа	JavaScript	Linux x86_64
Do Not Track	JavaScript	yes
Canvas	JavaScript	Cwm fjordbank glyphs vext quiz, 😃 Cwm fjordbank glyphs vext quiz, 😃
WebGL Vendor	JavaScript	NVIDIA Corporation
WebGL Renderer	JavaScript	GeForce GTX 650 Ti/PCIe/SSE2
Блокувальник реклами	JavaScript	yes

Всі описані вище механізми вже реалізовані у бібліотеці, що називається FingerprintJS. Саме за допомогою таких технологій з'ясовуються інтереси користувачів, на основі чого пропонуються товари, які привернуть увагу покупця.

Висновки

Таким чином, використовуючи технології Browser Fingerprinting можна ідентифікувати користувачів, навіть тоді, коли вони використовують режим інкогніто, що значно зменшує безпеку пересування в Інтернеті.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Browser Fingerprint – анонимная идентификация браузеров: веб-сайт. URL: https://habr.com/ru/company/oleg-bunin/blog/321294/ (дата звернення: 03.03.2021)
2. Фингерпринтинг браузера. Как отслеживают пользователей в Сети: веб-сайт. URL: https://xakep.ru/2015/01/30/user-web-tracking-howto/ (дата звернення: 03.03.2021)
3. 0.77% крупнейших сайтов используют Canvas для скрытой идентификации посетителей: веб-сайт. URL: https://www.opennet.ru/opennews/art.shtml?num=50176 (дата звернення: 03.03.2021)
4. Browser Fingerprinting: A survey: веб-сайт. URL: https://dl.acm.org/doi/10.1145/3386040 (дата звернення: 03.03.2021)

Хилько Степан Вікторович – студент групи 1БС-17б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: stepankhylko@ukr.net

Khylko Stepan V. — Faculty for Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : stepankhylko@ukr.net