ПРОТОТИПУВАННЯ БЕЗПАРОЛЬНОЇ СИСТЕМИ АУТЕНТИФІКАЦІЇ З ВИКОРИСТАННЯМ ОЗНАК BROWSER FINGERPRINTS

Федотов В.В., к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки,
кафедра КРіСТЗІ, м. Харків, Україна
e-mail: vitalii.fedotov@nure.ua

Abstract. The scenario of using the Browser Fingerprints collection and analysis system to build a password-free authentication system for web-resource users is proposed.

В останні роки з метою підвищення інформаційної безпеки користувачів у мережі Internet розробляються нові методи ідентифікації з динамічною конфігурацією факторів, що дозволяють ефективно визначити, чи користувач є легітимним.

Одним із підходів до реалізації подібних систем є визначення унікального багатокомпонентного цифрового сліду користувача, що базується на оцінці різних статичних та поведінкових ознак профілю суб'єкта доступу – ознак Browser Fingerprints [1-2]. У межах побудови такого профілю можуть бути використані наступні групи ознак: дані про браузер; дані про операційну систему, апаратне та програмне забезпечення; службова інформація про сеанс користувача – web-сервер; дані про користувача тощо.

Використовувати тільки ознаки Browser Fingerprints для ідентифікації користувачів неможливо з-за порівняно невисокої точності. Так точність ідентифікації за часом відвідування, парою «логін – пароль», IP-адресою користувача, рядком-ідентифікатором UserAgent (містить відомості про назву та версію використовуваного браузера, операційну систему і апаратну платформу комп'ютера, мову використовуваної операційної системи, версію верстки web-сторінки, кодове найменування та версію програмного забезпечення, що перетворює вміст web-сторінок і інформацію про форматування в інтерактивне зображення на екрані), переліком плагінів, що встановлено в браузері, роздільною здатністю екрану в пік селях та списком встановлених шрифтів становила 85 % [3]. Проте аналіз та збір ознак Browser Fingerprints можуть бути використані для створення безпарольних систем аутентифікації. Алгоритм роботи подібної системи може бути наступним.

1. Перевірка IP на предмет знаходження його у внутрішній дозволеній базі IP адрес (white list) або на наявність в базі адрес зловмисників, які використовуються для злому (black list). Якщо буде виявлено небезпеку, то автоматична аутентифікація припиняється.

2. Кожному профілю мережі відповідає ідентифікатор і при вході профіль перевіряється на його існування в каталозі дозволених. Якщо дану відповідність не доведено, то доступ може бути відхилений або ж спрямований на систему багатофакторної аутентифікації. Зловмисники часто створюють нові профілі, щоб можна було легко вписуватися в повсякденний трафік і уникати виявлення. Тому потрібно позначати такі профілі.

4. Аналіз місця розташування користувача. Якщо запит на аутентифікацію надійшов з місця розташування, де у організації немає відомих співробітників, клієнтів або партнерів, то він може бути відхилений або перенаправлений на систему багатофакторної аутентифікації.

4. Аналіз неможливих подій. Якщо доступ був зареєстрований вранці в одній точці країни, а потім через годину зовсім в іншому місці, то система запідозрить зловмисні дії і пере направить користувача на систему багато факторної аутентифікації.

5. Аналіз геолокації. Для забезпечення безпеки можна поставити географічний бар'єр і всі запити ззовні, повинні будуть проходити додаткові етапи підтвердження особистості.

6. Зчитування всіх доступних ознак Browser Fingerprints. Аналіз ознак Browser Fingerprints та ідентифікація за ними користувачів.

7. Аналіз поведінкових шаблонів. З часом у кожного користувача формується унікальний біометричний шаблон. Він створюється на основі взаємодії (апаратної та програмної) користувача зі своїм пристроєм. Ці характеристики так само унікальні, як і відбиток людського пальця. Досить точна імітація зловмисниками подібних нюансів практично неможлива.

Таким чином, через деякий час роботи в подібній системі аутентифікації потреба в паролі відпадає, оскільки він замінюється на індивідуальні користувацькі та поведінкові шаблони. Також створюється додатковий захист, оскільки, після отримання доступу, дії користувача відстежуються, і при відхиленні від еталонного профілю – блокуються.

Список використаних джерел.

1. The Security of HTTP-Headers. Режим доступу: https://www.contextis.com/en/blog/security-http-headers (дата звернення 10.01.2022).

2. Antoine Vastel, Pierre Laperdrix, Walter Rudametkin, and Romain Rouvoy. FP-STALKER: Tracking Browser Fingerprint Evolutions. In IEEE Symposium on Security and Privacy (S&P) (2018-05-21). 728–741.

3. Бессонова Е.Е., Метод идентификации пользователей в сети Интернет с использованием компонентного профиля // Материалы диссертационной работы на соискание ученой степени кандидата технических наук. Санкт-Петербург, 2014. 115 с.