Секція 1

ПРОБЛЕМИ ІДЕНТИФІКАЦІЇ ТА АУТЕНТЕФІКАЦІЇ В КІБЕРБЕЗПЕЦІ

Городничий А. С.
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»
Науковий керівник Морозова О. І.

Актуальність. У сучасному світі майже кожна людина має власні сторінки в соціальних мережах, аккаунт в Google та багато інших різних облікових записів на веб-сайтах, у мобільних додатках, всередині корпорацій, тощо. Через нехтування стандартами та сучасними методами аутентифікації, кіберзлочинцям вдається викрасти паролі, а з ними і доступ до конфеденційної інформації, банківських рахунків, доступ до приміщень із секретною інформацією, а також викрасти Вашу цифрову ідентичность. Наприклад, у 2021 році на одному хакерському форумі було опубліковано файл RockYou2021 з більш як 8 мільярдами паролів, а оскільки користувачі часто використовують один і той самий пароль для декількох облікових записів, кількість постраждалих у майбутньому може сягати мільйонів, якщо не мільярдів [1].

Мета роботи – дослідження існуючих проблем аутентифікації, шляхи їх виправлення та сучасних методів аутентифікації.

Основні положення. Сьогодні розроблено багато методів ідентифікації/аутентифікації, які включають як загальні методи аутентифікації (паролі, двофакторна аутентифікація (2FA), токени, біометрія, аутентифікація транзакцій, розпізнавання власника комп'ютера, CAPTCHA та single sign-on (SSO)), так і спеціальні протоколи аутентифікації (включаючи Kerberos і SSL/TLS) [2]. Кожен з них має свої сильні та слабкі сторони.

Вразливості ідентифікації/аутентифікації які використовують зловмисники для викрадення – стандартні, слабкі або добре відомі паролі, наприклад «Password1» або «admin/admin», облікові дані користувача для аутентифікації, які не захищені під час зберігання, ідентифікатори сеансу, які розкриваються в URL-адресі (наприклад, перезапис URL-адреси), значення сеансу, яке не закінчується або стає недійсним після виходу, ідентифікатори сеансу, які не змінюються після успішного входу, дані, надіслані через незашифровані з’єднання, слабкі або неефективні процеси відновлення облікових даних і забутих паролів, відсутня або неефективна багатофакторна аутентифікація, сеанси користувача або маркери

аутентифікації (переважно маркери єдиного входу (SSO)) не анулюються належним чином під час виходу з системи або періоду бездіяльності.

На підставі аналізу існуючих вразливостей були сформульовано поради, яких потрібно дотримуватись аби уникнути витоку даних: застосовувати багатофакторну аутентифікацію, узгодити політику щодо довжини, складності та ротації пароля за інструкціями Національного інституту стандартів і технологій (NIST), та перевіряти нові або змінені паролі, переконатись, що реєстрація, відновлення облікових даних і шляхи програмного інтерфейсу захищені від атак нумерації облікових записів за допомогою однакових повідомлень для всіх результатів, обмежуйте або частіше відкладайте невдалі спроби входу, використовувати захищений вбудований менеджер сеансів на стороні сервера, який генерує новий випадковий ідентифікатор сеансу з високою ентропією після входу, ідентифікатор сеансу не має бути в URL-адресі, а повинен надійно зберігатися та вважатися недійсним після виходу з системи, простою та абсолютних тайм-аутів [3].

Висновки. Завдяки використанню сучасних методів ідентифікації/аутентифікації та дотримання сучасних стандартів, які допомогають закривати найбільш поширені вразливості, можна зменшити ризик отримання даних зловмисниками.

Список літератури

1. Edvardas Mikalauskas, Cybernews – RockYou2021: largest password compilation of all time leaked online with 8.4 billion entries. *Cyber news*. URL – https://cybernews.com/security/rockyou2021-alltime-largest-password-compilation-leaked/ (дата звернення: 27.07.2022);

2. Common Network Authentication Methods. *N-able*. URL – https://www.n-able.com/blog/network-authentication-methods (дата звернення: 27.07.2022);

3. OWASP Top 10 2021. *OWASP*. URL – https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/ (дата звернення: 27.07.2022).

Відомості про авторів

Городничий Анатолій Сергійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 066-32-44-338, a.horodnychyi@student.csn.khai.edu

Морозова Ольга Ігорівна, професор кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 050-300-17-58, o.morozova@csn.khai.edu