DOI: 10.26565/2304-6201-2020-47-04

УДК 004.056 : 004.932

Аналіз схеми автентифікації на основі використання QR-коду та веб-камери для пристроїв Smart-Mobile

О.І. Кот, І.І. Сватовський

Кот Олександр Ігорович *студент*
Харківський Національний Університет ім. В.Н. Каразіна
майдан Свободи 4, 61022, Харків
e-mail: xa10995161@student.karazin.ua ;
https://orcid.org/0000-0002-6924-7445

Сватовський Ігор Іванович *к.т.н., доцент*
Харківський Національний Університет ім. В.Н. Каразіна
майдан Свободи 4, 61022, Харків
e-mail: i.svatowsky@karazin.ua;
https://orcid.org/0000-0002-1836-5599

Проведено аналіз необхідності та доцільності використання методу автентифікації користувачів на основі QR-коду та веб-камери для пристроїв Smart-Mobile. Фішингові атаки є однією з найсерйозніших загроз, з якими стикаються користувачі в Інтернеті. Існуючі відомі схеми автентифікації в повній мірі не справляються з цими атаками, про що свідчать актуальні статистичні дані багатьох компаній, що досліджують питання кібербезпеки. В роботі пропонується нова схема автентифікації користувачів, яка дозволяє їм увійти в свої облікові записи без запам'ятовування паролів або наявності інших токенів автентифікації. Згідно протоколу обміну повідомленнями в запропонованій схемі користувач повинен відсканувати динамічно згенерований QR-код за допомогою програми для смартфона, а потім зробити власний фотознімок через веб-камеру, і відправити його на смартфон за допомогою повідомлення від сервера. Таким чином, повна процедура автентифікації вимагає мінімальної участі користувача і виконується в автоматичному режимі. Результати оцінки і практичного тестування показують, що запропонована схема автентифікації працює досить надійно і може використовуватися в якості безпечної схеми автентифікації користувачів для пристроїв Smart-Mobile.

Ключові слова: *qr-код, веб-камера, аутентифікація, smart-mobile, Android.*

Analysis of the authentication scheme based on the use of QR-code and webcam for Smart-Mobile devices

O.I. Kot, I.I. Svatovskiy

Oleksandr Kot *Student*
V. N. Karazin Kharkiv National University
4 Svobody Sq., Kharkiv, 61022, Ukraine
e-mail: xa10995161@student.karazin.ua ;
https://orcid.org/0000-0002-6924-7445

Igor Svatovskiy *Ph.D., Associate Professor*
V. N. Karazin Kharkiv National University
4 Svobody Sq., Kharkiv, 61022, Ukraine
e-mail: i.svatowsky@karazin.ua;
https://orcid.org/0000-0002-1836-5599

The paper analyzes the necessity and expediency of using the method of user authentication based on QR-code and webcam for Smart-Mobile devices. Phishing attacks are one of the most serious threats faced by Internet users. Existing authentication schemes are not able to provide an adequate protection from these attacks, as evidenced by statistics collected by the companies researching cybersecurity. Therefore, the task of developing a secure authentication scheme for users, which can effectively counteract various types of phishing attacks is very important. The paper proposes a new authentication scheme for users, which allows them to log in to their accounts without remembering passwords or presenting other authentication tokens. According to the messaging protocol in the proposed scheme, the user must scan the dynamically generated QR-code using a smartphone application, then take their own photo via the webcam, and send it to the smartphone via a message from the server. Thus, the full authentication procedure requires minimal user involvement and is performed automatically. The results of evaluation and practical testing show that the proposed authentication scheme is quite reliable and can be used as a secure user authentication

scheme for Smart-Mobile devices. The proposed authentication protocol is not only able to cope with attacks such as Real Time Man-In-The-Middle and Controlled Relay Man-In-The-Middle, but can also protect users from the effects of malicious browser extensions and substitution of authentic applications by malicious variants. In addition, the proposed scheme does not require users to have any authentication tokens or credentials, as all they need is to scan the QR-code and verify the image taken by their own webcam. That makes the use of the proposed scheme more convenient and easy for users as compared to other known authentication schemes. Currently, the application of the proposed scheme requires the use of HTTPS websites for the exchange of all data involved. Thus, the proposed protocol can be implemented to manage cookies securely in order to prevent the interception of session data.

Keywords: *qr-code, web-camera, authentication, smart-mobile, Android.*

Анализ схемы аутентификации на основе использования QR-кода и веб-камеры для устройств Smart-Mobile

А.И. Кот, И.И. Сватовский

Кот Александр Игоревич *студент*
Харьковский Национальный Университет им. В.Н. Каразина
площадь Свободы 4, 61022, Харьков
e-mail: xa10995161@student.karazin.ua ;
https://orcid.org/0000-0002-6924-7445

Сватовский Игорь Иванович *к.т.н., доцент*
Харьковский Национальный Университет им. В.Н. Каразина
площадь Свободы 4, 61022, Харьков
e-mail: i.svatowsky@karazin.ua;
https://orcid.org/0000-0002-1836-5599

Проведен анализ необходимости и целесообразности использования метода аутентификации пользователей на основе QR-кода и веб-камеры для устройств Smart-Mobile. Фишинговые атаки являются одной из самых серьезных угроз, с которыми сталкиваются пользователи в Интернете. Существующие известные схемы аутентификации в полной мере не справляются с этими атаками, о чем свидетельствуют актуальные статистические данные многих компаний, исследующих вопросы кибербезопасности. В работе предлагается новая схема аутентификации пользователей, которая позволяет им войти в свои учетные записи без запоминания паролей или наличии других токенов аутентификации. Согласно протокола обмена сообщениями в предложенной схеме пользователь должен отсканировать динамично сгенерированный QR-код с помощью приложения для смартфона, а затем сделать собственный фотоснимок через веб-камеру, и отправить его на смартфон с помощью сообщения от сервера. Таким образом, полная процедура аутентификации требует минимального участия пользователя и выполняется в автоматическом режиме. Результаты оценки и практического тестирования показывают, что предложенная схема аутентификации работает достаточно надежно и может использоваться в качестве безопасной схемы аутентификации пользователей для устройств Smart-Mobile.

Ключевые слова: *qr-код, веб-камера, аутентификация, smart-mobile, Android.*

1 Вступ

Фішингові атаки є однією з найсерйозніших загроз, з якими стикаються користувачі в Інтернеті: зловмисники намагаються вкрасти конфіденційну інформацію, таку як дані для входу, дані кредитної картки, тощо, обманюючи користувачів для введення конфіденційної інформації на фішингових веб-сайтах і, таким чином, приводячи до величезних фінансових втрат [1]. Було запропоновано безліч схем виявлення фішингових атак, але кількість таких атак не зменшилася. З'явилися нові різновиди фішингових атак типу Active Man-In-The-Middle (MITM), які включають фішингові атаки Real Time Man-In-The-Middle (RT MITM) і Controlled Relay Man-In-The-Middle (CR MITM). Ці атаки дозволяють зловмисникам отримувати дані облікових записів користувачів і передавати їх в режимі реального часу. Так само зловмисник може спокусити користувача ввести дані у підробленому додатку і таким чином отримати доступ до облікового запису користувача [2-6]. Існуючі відомі схеми автентифікації в повній мірі не справляються з цими атаками. В роботі пропонується нова схема автентифікації користувачів, яка дозволяє їм увійти в свої облікові записи без запам'ятовування паролів або наявності інших токенів автентифікації. Згідно

протоколу обміну повідомленнями в запропонованій схемі користувач повинен відсканувати динамічно згенерований QR-код за допомогою програми для смартфона, а потім зробити власний фотознімок через веб-камеру, і відправити його на смартфон за допомогою повідомлення від сервера. Таким чином, повна процедура автентифікації вимагає мінімальної участі користувача і виконується в автоматичному режимі. Запропонована схема була реалізована і оцінена з точки зору зручності використання, можливості розгортання і параметрів безпеки. Результати оцінки і практичного тестування показують, що запропонована схема автентифікації працює досить надійно і може використовуватися в якості безпечної схеми автентифікації користувачів для пристроїв Smart-Mobile.

2 Запропонована схема автентифікації

Пропонована схема багатофакторної автентифікації використовує довірений мобільний додаток і веб-камеру на клієнтському комп'ютері (настільному / портативному). Загальна процедура автентифікації користувачів за пропонованою схемою передбачає, що кожен раз, коли користувач хоче отримати доступ до свого облікового запису на веб-сайті, сервер відображає QR-код на веб-сторінці. Цей протокол автентифікації передбачає, що мобільний додаток в телефоні користувача є довіреним. Користувач сканує QR-код, що відображається на веб-сторінці, за допомогою мобільного додатку. Потім додаток відправляє дані користувача разом з токеном сеансу, отриманим з QR-коду, на адресу сервера. Далі сервер видає запит до клієнтського комп'ютера для доступу до веб-камери і робить знімок за її допомогою. Наступним етапом є відправлення зображення сервером в мобільний додаток за допомогою повідомлення. Отримавши це зображення, користувач підтверджує або відхиляє його. Після пітвердження правильності одержаного зображення користувач буде автентифікований. Таким чином, автентифікація сервера виконується за допомогою зображення, зробленого на клієнтській машині легітимного користувача, оскільки тільки законний веб-сайт може зробити знімок користувача за допомогою веб-камери і відправити вірне зображення на його мобільний телефон.

2.1 Припущення щодо необхідних умов для застосування

1. Передбачається, що на ПК є веб-камера.
2. Передбачається, що користувач використовує справжній додаток Android під час реєстрації, і, як і в багатьох інших відомих схемах, процедура реєстрації нового користувача захищена від атак.
3. Запропонована схема передбачає, що передача даних між клієнтом і сервером відбувається за протоколом HTTPS, захищена від перехоплення в мережі і може використовуватися для обміну секретними ключами.
4. Автентичні сервери веб-сайтів та інформація, що зберігається в їх базах даних, вважаються безпечними.

2.2 Аналіз моделі загроз

1. Фішинг, MITM-фішинг: зловмисник може заманити користувача на фішинговий веб-сайт, а потім отримати особисту інформацію. Зловмисник може або передати цю інформацію в режимі реального часу (RT MITM), або встановити модулі захоплення віддаленого робочого столу, або ретрансляції на термінал користувача (CR MITM) для крадіжки облікових даних.
2. Фішингові атаки на основі шкідливих розширень браузера: зловмисник може вкрасти облікові дані користувача, змусивши користувача встановити шкідливе розширення браузера, запитуючи дозволу на виконання деяких обережних дій у фоновому режимі, одночасно надаючи функції на передньому плані (front-end). Шкідливі розширення браузера можуть виконувати кейлоггінг, реєстрацію екрану або перехоплення пароля у фоновому режимі.
3. Спуфінг програми: зловмисник може створити підробний (фальшивий, підроблений) додаток для Android, який схожий на справжній додаток, необхідний для входу в систему. Потім зловмисник може встановити цей підроблений додаток на комп'ютер користувача і спокусити користувача ввести свої облікові дані через нього.

2.3 Процедура реєстрації користувачів

Реєстрація користувача передбачає реєстрацію користувача в мобільному додатку. Таким чином, на етапі реєстрації беруть участь два об'єкти - мобільний додаток і веб-сервер. Реєстрація

користувача виконується в мобільному додатку, в якому будуть зберігатися дані користувача, які будуть використовуватися при вході в систему. Реєстрація користувача в запропонованому протоколі автентифікації показана на рисунку 2.1.

Алгоритм реєстрації користувача передбачає наступні кроки:

1. Користувач спочатку вводить відповідні дані, такі як ім'я користувача (UID), пароль (PWD), адреса електронної пошти (Email-ID), в мобільний додаток.
2. Мобільний додаток генерує випадкову сіль (salt), яка складається з 6 символів.

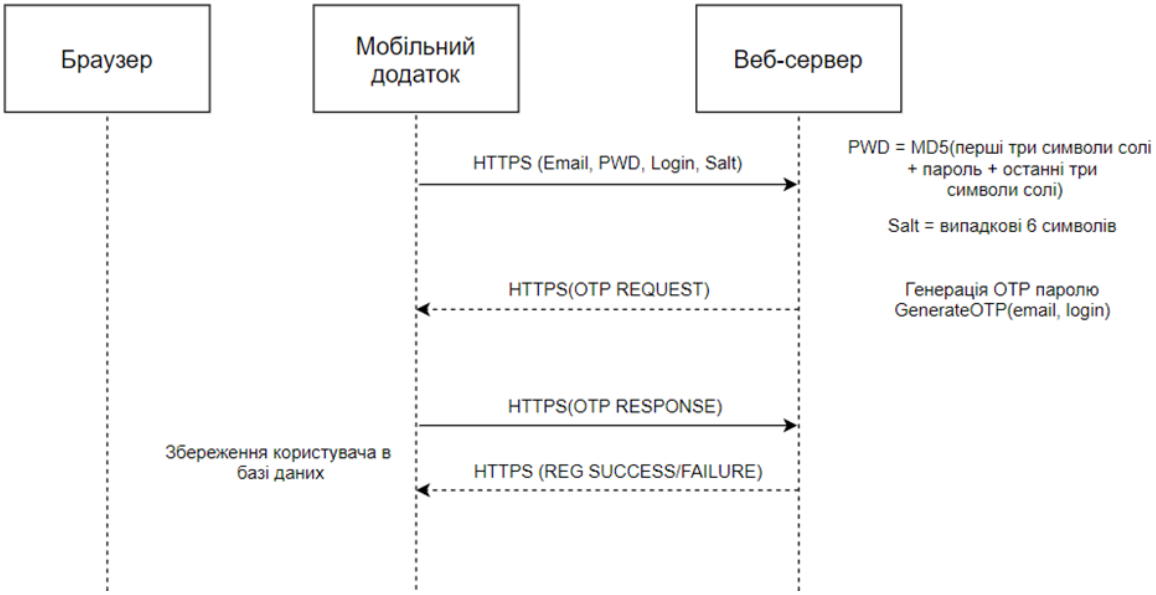

Рис.2.1. Обмін повідомленнями при реєстрації

3. Мобільний додаток за допомогою захищеного протоколу HTTPS відправляє дані реєстрації на сервер.
4. Сервер генерує тимчасовий пароль (OTP) та відправляє його на поштову адресу, вказану при реєстрації.
5. Користувач вводить на екрані смартфону отриманий пароль, після чого додаток відправляє дані на сервер.
6. Сервер надсилає відповіть про успішну, чи не успішну реєстрацію.

2.4 Використання логіну користувача

Пропонований протокол автентифікації використовує три об'єкти для входу користувача на сайт. Використовувані об'єкти: мобільний додаток, браузер і веб-сервер. Користувачеві також знадобиться веб-камера для входу в систему. Щоб увійти в обліковий запис веб-сайту, користувач повинен увійти в мобільний додаток веб-сайту. Причина в тому, що повідомлення відправляється в додаток, в якому користувач увійшов в систему. Для входу в мобільний додаток користувач вводить ідентифікатор користувача (login) і пароль (pwd), які відправляються на веб-сервер. для підтвердження. Оскільки більшість користувачів не виходять з свого облікового запису, шанси на повторний вхід в мобільний додаток менше.

Процедура входу наступна:

1. Користувач спочатку відкриває веб-сторінку входу в систему в браузері.
2. На сторінці входу на веб-сайт відображається QR-код, що містить токен сеансу, створений веб-сервером.
3. Користувач сканує QR-код, що відображається на веб-сайті, за допомогою камери свого мобільного телефону.
4. Після отримання QR-коду мобільним додатком токен сеансу витягується з QR-коду.
5. Користувачу відображається на екрані повідомленя з IP-адресою користувача, що почав процесс автентифікації.

6. Після підтвердження автентифікації на сервер відправляються дані, що містять: ID веб-сесії, ID-мобільної сесії, imei адреса телефона.
7. В браузері з'являється спливаюче вікно із запитом дозволу на доступ до веб-камери клієнтського комп'ютера. Користувач повинен дозволити доступ, щоб увійти на сайт.
8. Потім веб-камера робить знімок користувача та відправляє це зображення на сервер.
9. Додаток постійно оновлює статус мобільної сессії в очікувані надходження зображень з веб-камери.
10. Після отримання зображення додатком його буде відображено на екрані та з’явиться пропозиція підтвердити або скасувати спробу автентифікації.
11. На сервер відправляється відповідь з параметрами сесії.
12. Сторінка веб-сайту автоматично оновлюється після успішної автентифікації.

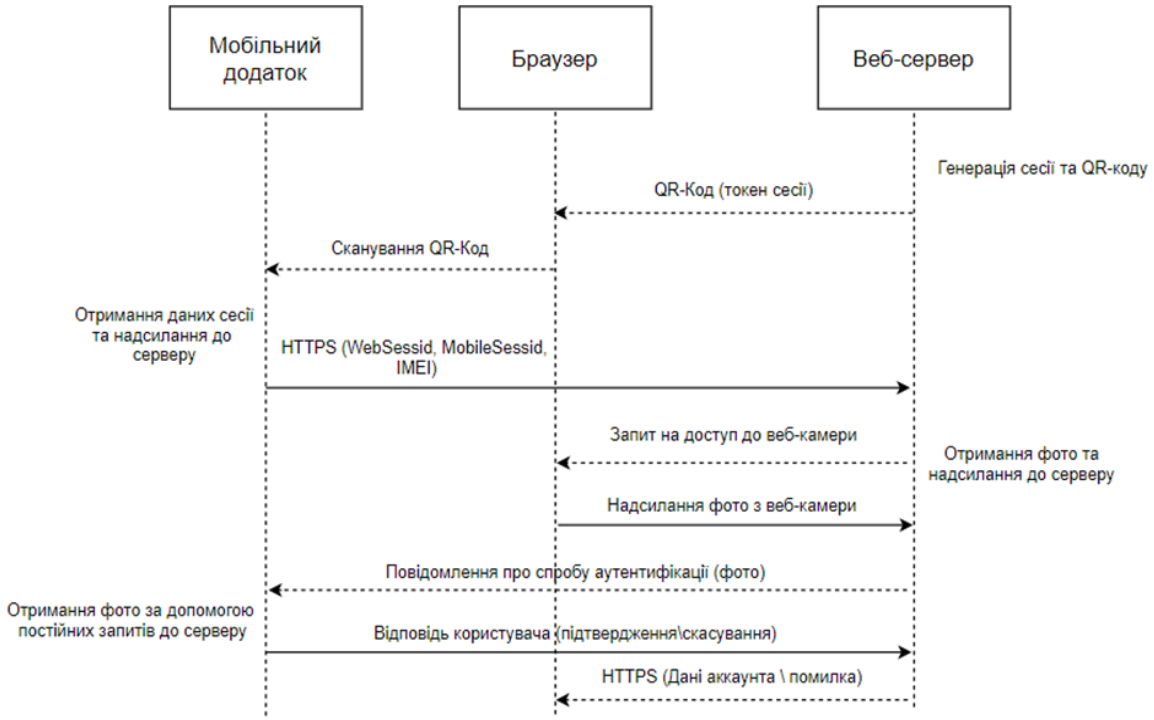

Рис.2.2. Обмін повідомленнями при аутентифікації

Сеанс входу в систему існує протягом певного періоду часу, після чого термін дії сеансу закінчується, і веб-сервер перенаправляє користувача назад на домашню сторінку, відображаючи новий QR-код і, таким чином, не дозволяючи зловмисникові використовувати зображення, зроблене веб-камерою, в більш пізній етап аутентифікації (рис. 2.2).

3 Тестування та оцінка працездатності схеми автентифікації

3.1 Опис випробувальної установки

1. Смартфон OnePlus 5T з набором мікросхем Qualcomm Snapdragon 835 MSM8998, восьмиядерним процесором (чотири ядра Kryo 280 Performance з тактовою частотою 2,35 ГГц і чотири ядра Kryo 280 Efficiency з тактовою частотою 1,90 ГГц), 6 ГБ оперативної пам'яті і операційна система Android Pie з OxygenOS версії 9.0.4.
2. Настільний комп'ютер, який використовується для етапу входу в систему через Інтернет, Клієнтський комп'ютер є ПК з 64-розрядною операційною системою Windows 10 Professional з Google Chrome (версія 228.14.88), веб-камерою і процесором Intel® CoreTM i7-7700K @ 4 ГГц з 64 ГБ оперативної пам'яті.
3. Веб-сайт для тестування етапу реєстрації і входу в систему розміщувався на настільному комп'ютері під керуванням 64-розрядної операційної системи Windows 10 на процесорі Intel® CoreTM i7-3770 з тактовою частотою 3,40 ГГц і 8 Гб оперативної пам'яті.

4. Випробувальний веб-сайт було написано на ASP.NET Core і розміщено на сервері Windows IIS.

5. Сервер Microsoft SQL версії 17 використовувався для зберігання інформації користувача на стороні сервера.

3.2 Результати тестування

Для тестування на мобільному пристрої був запущений розроблений додаток. На головному екрані є вибір з 4-х кнопок (рис. 3.1): Логін (Login), Реєстрація (Register), Сканування QR (Scan QR), Деавторизація (Logout). Враховуючи перший запуск, на екрані доступні тільки кнопки логіну та реєстрації.

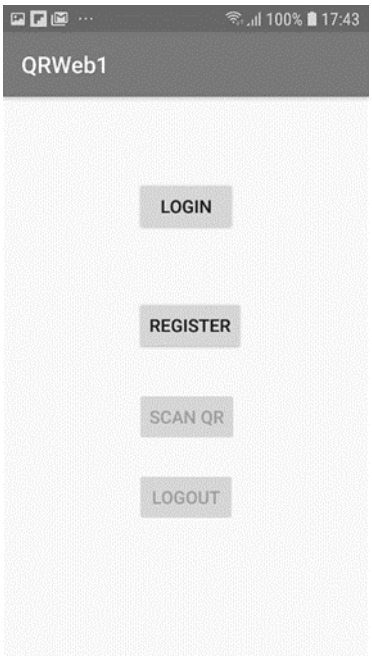

Рис.3.1. Основний екран додатку

Оскільки для тестування було вибрано «чистий» сервер без записів у БД, тож було обрано режим реєстрації та введено e-mail, логін та пароль (рис. 3.2).

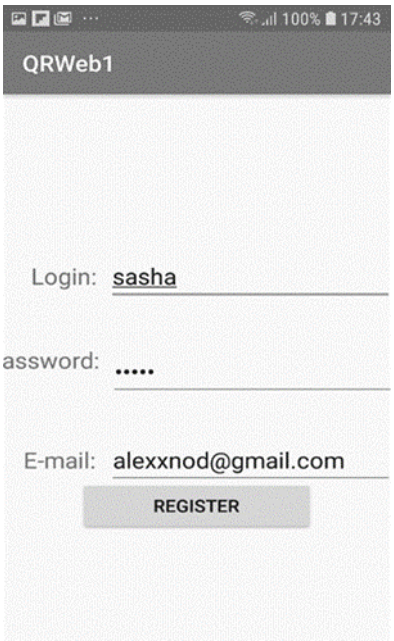

Рис.3.2. Екран реєстрації

Після натискання кнопки «register» на сервер було відправлено дані реєстрації. Після чого з'явився екран вводу тимчасового паролю (рис. 3.4), який був відправлений на адресу електронної пошти (рис. 3.3).

Рисунок 3.3. E-mail повідомлення з OTP кодом

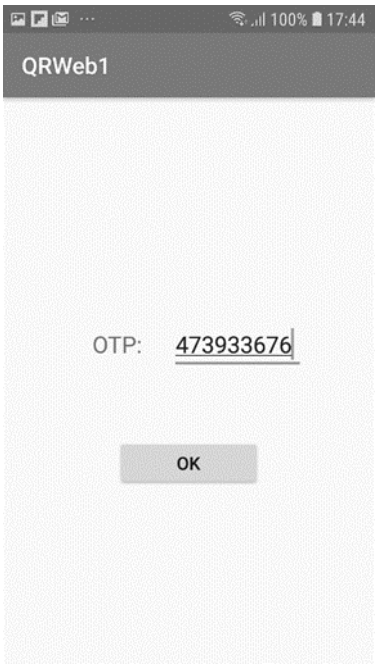

Рисунок 3.4. Вікно вводу OTP коду

Після вводу OTP коду було отримано повідомлення про успішну активацію (рис. 3.5).

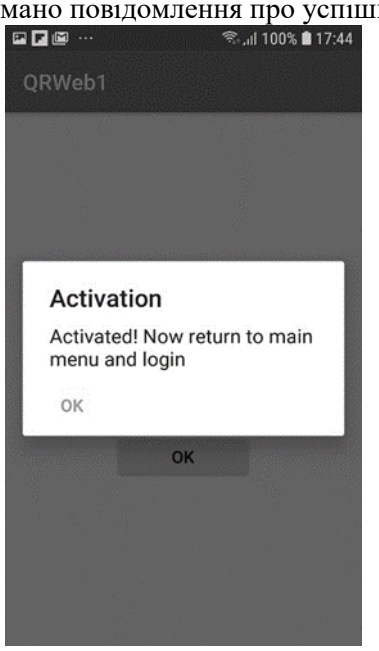

Рисунок 3.5. Повідомлення про успішну активацію

Після активації додатком було запропоновано перейти до вікна авторизації, де було введено логін та пароль (рис. 3.6).

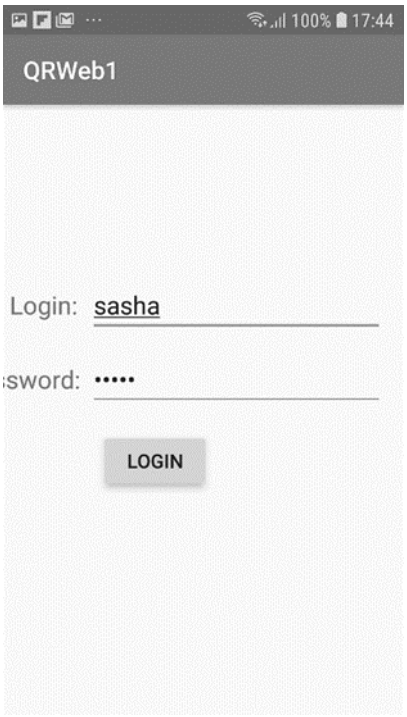

Рисунок 3.6. Вікно вводу логіну та паролю

Далі після успішної перевірки логіну та паролю додаток відкрив вікно вводу OTP паролю (див. рис. 2.2) який було направлено на e-mail, що був вказаний при реєстрації. Після проходження перевірки дані сесії були збережені у захищене сховище Android, а на екрані було відображено повідомлення про успішну авторизацію та пропозицію до переходу на основний екран і сканування QR-коду (рис. 3.7).

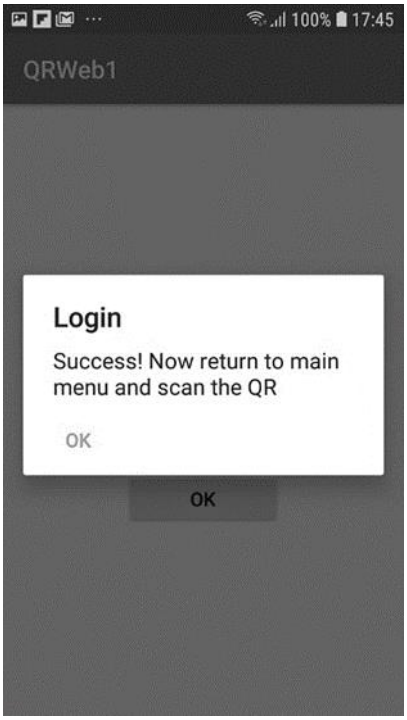

Рисунок 3.7. Повідомлення про успішну авторизацію

Далі було відкрито веб-браузер з необхідним тестовим сайтом (у локальній мережі по протоколу HTTPS). На екрані було відображено QR-код та текст, у якому пропонується відсканувати код за допомогою мобільного додатку (рис. 3.8).

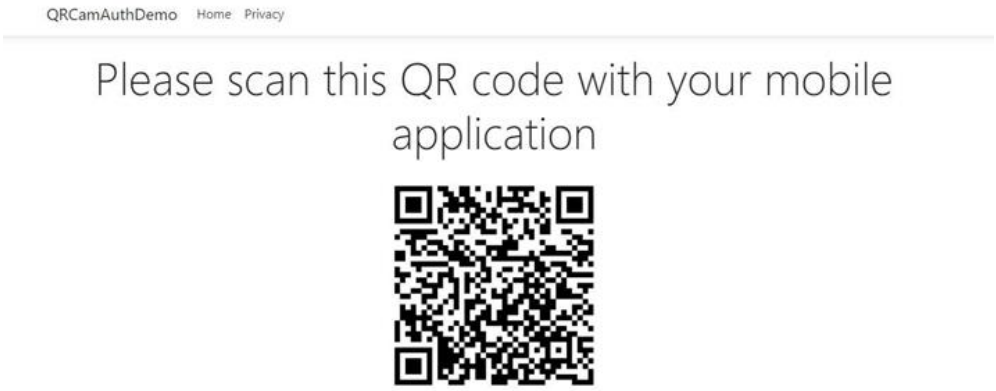

Рисунок 3.8. Веб-сторінка з QR-кодом

За допомогою додатка було відсканновано даний QR-код, після чого на екрані було відображено інформацію про авторизацію, що включає в собі IP-адресу (рис. 3.9).

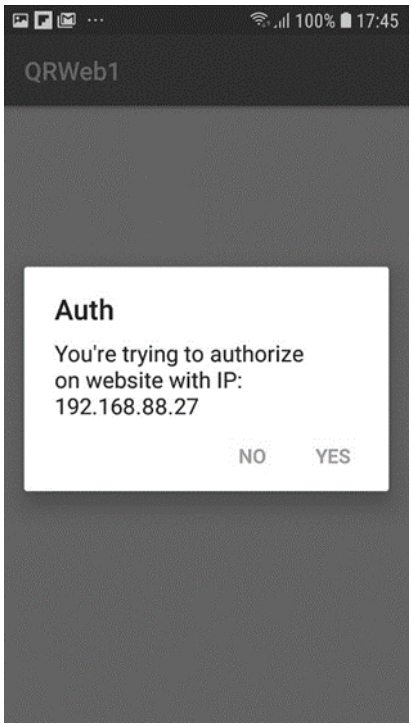

Рисунок 3.9. Запит на підтвердження авторизації

Після підтвердження авторизації сторінка з QR-кодом автоматично оновлюється і запитується доступ до веб-камери. Після надання дозволу на використання веб-камери пропонується зробити фотознімок користувача (рис. 3.10).

Рисунок 3.10. Вікно зображення веб-камери

Далі а на веб-сайті було відображено повідомлення про очікування підтвердження (рис. 3.11), а на телефон було відправлено повідомлення з відповідним зображенням (рис. 3.12)

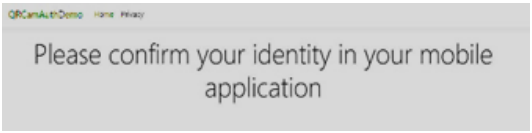

Рисунок 3.11. Повідомлення очікування підтвердження

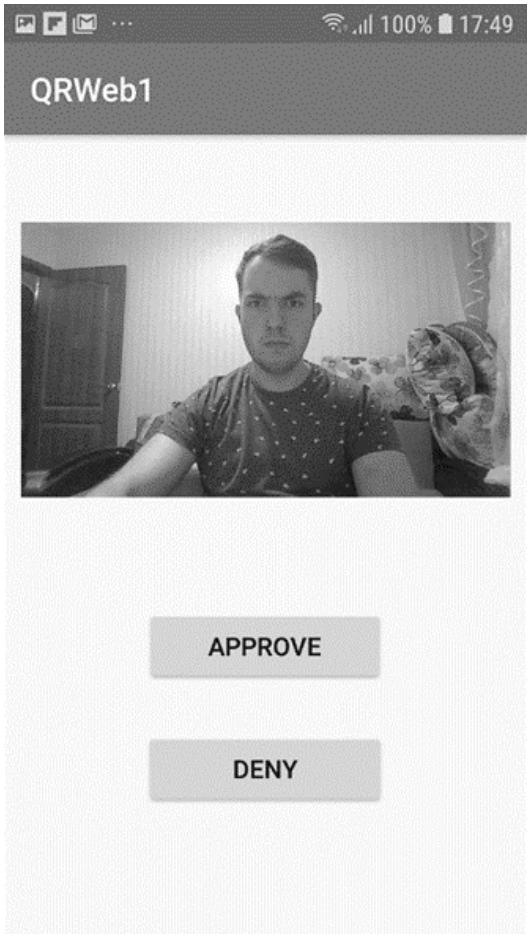

Рисунок 3.12. Вікно підтвердження у мобільному додатку

Після підтвердження успішної автентифікації у мобільному додатку сторінка веб-сайту оновлюється і відображається інформація про це (рис. 3.13).

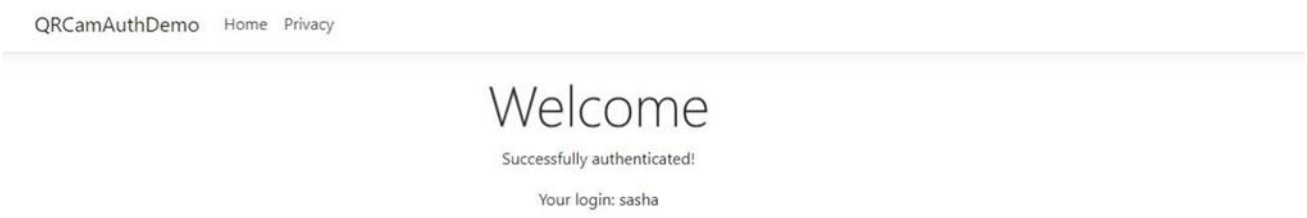

Рисунок 3.13. Повідомлення на веб-сайті про успішну авторизацію

На цьому процедура автентифікаціїї користувача завершується.

3.3 Розрахунок часу реєстрації та аналіз необхідних ресурсів

Час, необхідний для реєстрації користувачів (TReg), може бути розраховано на основі наступного виразу:

$$T_{REG} = T_{OTP} + T_{EC} + T_{MD5} + T_{SALT} + T_{DB} \quad (3.1)$$

де T_{OTP} – час генерування та доставку на електронну адресу тимчасового паролю, T_{EC} – час, витрачений користувачем на перевірку поштової скриньки на вміст коду, T_{MD5} – час генерування хешу паролю, T_{SALT} – час генерування солі, T_{DB} – час зберігання даних у захищеному сховищі Android.

Середній час витрачений на реєстрацію становить приблизно 38.25 секунд, якщо телефон під'єднано до мережі Wi-Fi, та 40.12 секунд, якщо телефон під'єднано до мережі LTE. Найбільшу частку часу займає перевірка e-mail.

Схожим чином розраховується час, необхідний користувачу для авторизації (TLogin) на веб-сайті при використанні запропонованого методу :

$$T_{LOGIN} = T_{FQR} + T_{SQR} + T_{SC} + T_{CAM} + T_{PN} + T_F \quad (3.2)$$

де T_{FQR} – час, необхідний для обробки та відображення QR-коду на веб-сайті, T_{SQR} – час, необхідний для сканування QR-коду через мобільний додаток, T_{SC} – час, необхідний для перевірки сесії мобільного додатку, T_{CAM} – час, необхідний для виконання знімку з веб-камери, T_{PN} – час, необхідний для надсилання та підтвердження фото у мобільному додадку, T_F – час, необхідний на проведення автентифікації та авторизації після підтвердження фото.

В середньому користувачеві потрібно 14,744 с для входу на веб-сайт за пропонованою схемою, коли смартфон підключений через Wi-Fi, тоді як для підключення смартфона до мережі 4G потрібно 15, 222 с.

Ресурси, що використовуються Android-додатком за пропонованою схемою, визначаються за допомогою інструменту профілювання Android Studio. Зареєстровані значення мінімальної і максимальної завантаження ЦП на етапах реєстрації та входу в систему складають 1,2-19,8% і 1,4-27,3% відповідно. Середній обсяг пам'яті, який використовується Android-додатком для запропонованої схеми, становить 46 МБ. На основі аналізу одержаної статистики можна зробити висновок, що вимоги до використання ЦП і пам'яті для запропонованої схеми досить невеликі, і тому запропоновану схему можна використовувати для входу на веб-сайти без істотних обмежень.

3.4 Порівняння з відомими схемами на основі критерію зручності використання

Запропонована схема була порівняна з деякими існуючими схемами по критерію зручності використання. Зручність використання схеми аутентифікації враховує кількість токенів, необхідних схемою аутентифікації, і кількість токенів аутентифікації, які користувач повинен запам'ятати. Це порівняння також бере до уваги будь-яке додаткове програмне або апаратне

забезпечення. Смартфон потрібний для більшості існуючих схем, оскільки його мають всі користувачі Інтернету.

Деякі з існуючих схем вимагають, щоб на клієнтському комп'ютері був встановлений конкретний модуль або драйвер, апаратний токен або довірена третя сторона і т. д. Пропонована схема вимагає тільки наявності комп'ютерної камери, яка легко доступна на всіх настільних комп'ютерах, особливо портативних. Крім того, пропонована схема не вимагає, щоб користувач запам'ятав будь-який токен аутентифікації, і, таким чином, вона більш зручна для користувача в порівнянні з іншими схемами аутентифікації.

Порівняння, засноване на критерії зручності використання, також розглядає потребу в доступі до Інтернету на телефоні як одному з факторів для вимірювання зручності використання в різних схемах автентифікації для розуміння витрат, понесених при використанні схеми. Пропонована схема вимагає наявності доступу до Інтернету на телефоні, який став синонімом смартфонів. Таблиця 2 описує порівняльний аналіз, заснований на зручність використання.

3.5 Порівняння на основі оцінки безпеки застосування

В цьому розділі запропонована схема порівнюється з відомими існуючими схемами на основі критерію безпеки застосування, яку вони забезпечують проти атак, описаних в розділі 2.2.

1. **Фішингові атаки RT MITM і CR MITM:**
   1.1. U-PWD [23, 24] і схеми аутентифікації на основі OTP / PIN, такі як Google 2-step [7] і SAASPASS [8], уразливі як для RT MITM, так і для CR MITM фішингових атак.

Таблиця 3.1. Порівняння за кількістю використовуваних токенів і їх безпеки

№	Схема	Токени, що використовуються схемою	Токени, що необхідно запам’ятати	Додаткові потреби	Необхідність в інтернеті на телефоні
1	Google 2 Step [7]	3-U, PWD, OTP on SP	2-U, PWD	Мобільний телефон	Ні
2	SAASPASS [8]	3-U, PWD, OTP on App	2-U, PWD	Смартфон	Так
3	Xie et al. [16]	4-U, PWD, DH Public (g, p), Private Up	2-U, PWD	Веб-камера, смартфон	Так
4	Kim et al. [10]	4-U, PWD, Session ID, Secret Key	2-U, PWD	Смартфон з GPS	Так
5	Mukhopadhyay et al. [11]	3-U, PWD, Secret Key in SP	2-U, PWD	Смартфон	Так
6	Dodson et al. [12]	4-U, PWD, Secret Key, QR-Code	0-NIL (Сканування QR-коду)	Смартфон	Так
7	Leung et al. [13]	4-U, PWD, Secret Key, OTP CAPTCHA	2-U, PWD	Відсутні	Невідомо
8	Zhu et al. [22]	3U, SALT, PWD, CAPTCHA	2- U, PWD	Відсутні	Невідомо
9	Tricipher [19]	3U, PWD, TPM Secret Key, TACS credential	2- U, PWD	CAPI драйвер, окреме обладнання	Невідомо
10	RSA SecurlD HW Token [21]	4-U, PWD, HW token information, PIN	2-U, PWD	Окреме обладнання	Невідомо
11	Yubikey U2F [14]	5-KPUB, KPRIV, Counter, U, PWD	2-U, PWD	Окреме обладнання	Невідомо

12	Push Login [15, 20]	3-U, PWD, SP	1-U	Смартфон	Так
13	Password Managers [17, 18]	3-U, PWD, the master key of the password manager	Master PWD	Відсустні	Невідомо
14	U-PWD [23, 24]	2-U, PWD	2-U, PWD	Відсутні	Невідомо
15	Запропонована схема	3-U, фото зроблене за допомогою веб-камери	0-NIL (Сканування QR-коду)	Смартфон, веб-камера	Так

1.1. Зловмисник може легко отримати реєстраційні дані користувача за допомогою фішингового сайту. Зловмисник може обманути користувача, показавши йому точну копію справжнього веб-сайту, і передати облікові дані, введені користувачем на фішинговому веб-сайті, в режимі реального часу на справжній веб-сайт. Зловмисник також може запустити фішингову атаку CR MITM за схемою на основі OTP / PIN, просто перенаправив свій віддалений робочий стіл через клієнтський термінал, і користувач буде спокушений ввести облікові дані, які фактично вводяться на віддаленому робочому столі зловмисника.

1.2. Схеми на основі QR-коду також не можуть протистояти атакам RT MITM і CR MITM. Схема, запропонована Xie et al. [16] може бути атакована за допомогою підробленого шкідливого розширення браузера. Зловмисник може встановити на комп'ютер користувача підроблене шкідливе розширення браузера. Таким чином зловмисник отримає облікові дані, які зловмисник передасть розширенню CamAuth. Розширення CamAuth відправить інформацію про користувача на сервер, а також ініціює обмін даними по типу схеми Діффі-Хеллмана. Сервер перевіряє облікові дані, і таким чином обліковий запис користувача буде відправлено сервером в браузер зловмисника. Однак схема Се і ін. [16] захищена від атаки CR MITM, оскільки зловмисник не може отримати доступ до камери ПК користувача. Точно також схема на основі QR-коду, запропонована Kim et al. [10], не захищена від атак RT MITM і CR MITM. Причина в тому, що IP-адреса, присутня в QR-коді, може бути підроблена, і зловмисник може відправити запит до серверу. Схема, запропонована Mukhopadhyay et al. [11] також вразлива для подібних атак, оскільки облікові дані, введені користувачем, можуть бути легко отримані зловмисником за допомогою фішингового веб-сайту, а QR-код може бути переданий на фішинговий веб-сайт. Таким чином, процес входу в систему завершується, і зловмисник отримує доступ до облікового запису користувача. Точно також схема Додсона і ін. [12] є вразливою для RT MITM, а також для атаки CR MITM, оскільки зловмисник передає QR-код на фішинговий веб-сайт, який сканується смартфоном користувача.

1.3. Схеми на основі апаратних токенів, такі як Tricipher [19] і Yubikey з використанням U2F [20], захищені від фішингових атак RT MITM і CR MITM через використання складових облікових даних. Однак програмний / апаратний токен RSA SecurlD [21] не убезпечує від цих атак, оскільки зловмисник може отримати код доступу RSA через фішинговий веб-сайт.

1.4. Графічна схема автентифікації на основі пароля, запропонована Leung et al. [13] захищена від атаки RT MITM, тому що ретрансляція координат клацання мишею користувача при переміщенні CAPTCHA досить складна, і може бути значущою різниця в розширені екрану робочого столу зловмисника і робочого столу користувача. Однак ця схема не убезпечена від атаки CR MITM. Схема Чжу і ін. [14] не убезпечена від RT MITM, а також від CR MITM-атак, тому що зловмисник може записувати і відображати координати клацання користувача на CaRP, який відображається на справжньому веб-сайті.

1.5. Схеми входу в систему на основі push-повідомлень [15, 16] уразливі для атак RT MITM і CR MITM, оскільки зловмисник може ретранслювати введені облікові дані користувачем, і потім користувач затвердить push-повідомлення, отримане в додатку для смартфона.

1.6. Менеджери паролів [17, 18] захищені від атак RT MITM і CR MITM, оскільки облікові дані користувача автоматично відправляються менеджерами паролів, і користувачеві не потрібно їх вводити. Однак, якщо зловмисник вводить неправильні облікові дані, він запропонує користувачеві повторно ввести своє ім'я і пароль, що призведе до можливості реалізації атаки RT MITM і CR MITM.

1.7. Пропонована схема захищає користувача від фішинг-атаки RT MITM, оскільки навіть після ретрансляції QR-коду зловмисник не зможе відправити на сервер фотографію користувача, зроблену його веб-камерою (зрозуміло, що зловмисник не має фізичного доступу до пристрою користувача). Причина в тому, що фотографія повинна бути зроблена веб-камерою зловмисника. Більш того, після того, як користувач сканує QR-код з програми для смартфона, веб-камера зловмисника відразу ж зробить фото зловмисника за допомогою його веб-камери і відправить цю фотографію користувачеві через push-повідомлення, тим самим попередивши користувача про спробу підміни. Пропонована схема також захищена від фішингових атак CR MITM, оскільки зловмисник не може отримати доступ до веб-камери користувача.

2. Фішингові атаки на основі шкідливих розширень браузера.

Фішингові атаки на основі шкідливих розширень браузера включають ведення кейлогерів, ведення журналу екрану і перехоплення пароля. Зловмисник може зламати двоетапний токен Google [13], U-PWD [24], SAAS¬PASS [8], програмний / апаратний [21] токен RSA SecurlD, використовуючи кейлоггінг і сніффінг паролів, оскільки у вищезгаданих схемах всі облікові дані вводяться на веб-сайті, і, таким чином, зловмисник може перехопити їх через шкідливе розширення браузера. Зловмисник також може зламати менеджери паролів, встановивши на клієнтському терміналі шкідливе розширення браузера, яке може перехопити пароль перед його відправкою на сервер. Схема Xie et al. [9] захищена від кейлоггерів і можливості перехоплення паролів, оскільки шкідливе розширення браузера не може отримати доступ до інформації, введеної користувачем в розширенні CamAuth через політику одного і того ж походження. Однак, зловмисник може отримати доступ до QR-коду за допомогою запису екрану, але не зможе порушити повну автентифікацію. Kim et al. [10] і Dodson et al. [12] захищають користувачів від цих атак, оскільки не вимагають введення будь-яких облікових даних. Схема Leung і ін. на основі CAPTCHA [13] захищені від кейлогерів і перехоплення паролів, оскільки використовується OTP CAPTCHA на основі флеш-пам'яті. З іншого боку, зловмисник може зламати схему Чжу і ін. [14] і отримати введення користувача через ведення журналу екрану. Оскільки Zhu et al. [14], Tricipher [19], Mukhopadhyay et al. [11] і схеми на основі примусового входу в систему [15, 16] використовують або довірена пристрій, або другий фактор автентифікації, зловмисник може отримати тільки токен автентифікації або ідентифікацію користувача, але не може порушити функціонування цієї схеми. Пропонована схема захищена від подібних атак, оскільки користувачеві не потрібно вводити свої облікові дані, і тому шкідливі розширення браузера не зможуть перехопити цю інформацію.

Таблиця 3.2. Порівняння з точки зору захисту від відомих загроз

№	Схема	RT MITM	CR MITM	Кейлогінг	Запис екрану	Сніфінг паролю	Підміна додатків	Рівень безпеки
1	Google 2 step	-	-	-	-	-	-	0
2	SAASPASS	-	-	-	-	-	-	0

3	Xie et al.	-	+	+	-	+	-	3
4	Kim et al.	-	-	+	+	+	-	3
5	Mukhopadhyay et al.	-	-	-	-	-	+	1
6	Dodson et al.	-	-	+	+	+	+	4
7	Leung et al.	+	-	+	-	+	-	3
8	Zhu et al.	-	-	-	-	-	+	1
9	Tricipher	+	+	-	-	-	+	3
10	RSA SecurID I-IW token	-	-	-	-	-	-	0
11	Yubikey U2F	+	+	+	-	-	+	4
12	Push login	-	-	-	-	-	-	0
13	Password Managers	+	+	+	-	+	+	5
14	U-PWD	-	-	-	-	-	-	0
15	Запропонована схема	+	+	+	+	+	+	6

3. **Підміна додатків:** зловмисник може встановити підроблений мобільний додаток або розширення на смартфон, або робочий стіл користувача, щоб отримати інформацію про нього. Xie et al. [9], Google 2-step [7], SAASPASS [8], U-PWD, Kim et al. [10] уразливі для цієї атаки, оскільки підроблений додаток може бути встановлено на пристрій користувача, а облікові дані, введені ним, зберігаються в підробленому додатку, який встановлено зловмисником. Zhu et al. Схема [14] захищена від цієї атаки, оскільки не використовує ніяких додатків або розширень. Mukhopadhyay et al. [11], Tricipher [19] і Dodson et al. [12] захищені від подібної атаки, оскільки в цих схемах принаймні одна частина токена аутентифікації зберігається на пристрої користувача і не вводиться в додаток. Пропонована схема також захищена від спуфінга додатків, оскільки секретні дані зберігаються в додатку, зашифрованому за допомогою Android Keystore API, який не буде доступний в підробленому додатку. Порівняння запропонованої схеми з іншими існуючими схемами, заснованими на безпеці застосування представлено в таблиці 3.

3.5 Висновки

В роботі було запропоновано нову схема автентифікації, яка здатна протистояти як традиційним, так і ускладненим фішинговим атакам. Пропонований протокол автентифікації не тільки здатний впоратися з атаками типу RT MITM і CR MITM, але також може захистити користувачів від дії шкідливих розширень браузера і підміни автентичних додатків на шкідливі їх варіанти. Окрім цього, пропонована схема не вимагає від користувачів необхідності мати будь-які токени автентифікації або облікові дані, оскільки їм просто потрібно відсканувати QR-код і перевірити зображення, зняте власною веб-камерою. Це робить використання запропонованої схеми більш зручною і простою для користувачів в порівнянні з іншими відомими схемами автентифікації.

Наразі застосування запропонованої схеми вимагає використання веб-сайтами протоколу HTTPS для обміну всіма задіяними в обміні даними. Таким чином, пропонований протокол може бути реалізований для безпечного управління файлами cookie, щоб він не був вразливий для перехоплення даних сеансу. У майбутньому доцільно провести більш широке дослідження, направлене на оцінку зручності використання користувачем запропонованої схеми. Також, можливо, представлять інтерес визначення в майбутньому таких параметрів її використання, як

крива навчання і масштабованість, а також оцінки дослідження можливостей запропонованої схеми в обробці великої кількості одночасних запитів.

ЛІТЕРАТУРА

1. Ластдрагер Е.Е. Досягнення консенсусного визначення фішингу на основі систематичного огляду літератури. *Crime Sci.* 2014. Вип. 3. С.21-32.
2. Абдельхамід Н. Багатознакові правила класифікації фішингу. *Прикладні обчислення та інформатика*. 2015. Вип. 11. С. 29-46.
3. Бандей М.Т., Кадрі Ж.А. Фішинг - зростаюча загроза для електронної комерції, *The Business Review*. 2011. Вип. 12. С. 76-83.
4. Бадра М., Ель-Сауда С., Хадже І., *Фішинг-атаки та рішення*: матеріали 3-ї Міжнародної конф. з мобільних мультимедійних комунікацій, MobiMedia 2007, Нафпактос, Греція, 27-29 серпня 2007 р. С. 42-43.
5. Рамі М. М., Фаді Т., Лі М. Підручник та критичний аналіз методів фішингових веб-сайтів, *Computer Science Review*. 2015. Вип. 17. С. 1-24.
6. Джагатич Т., Натаніель Дж., Менцер Ф. Соціальний фішинг, *Commun*. 2007. С. 94–100.
7. Посилений захист вашого облікового запису Google. Google: веб-сайт. URL: https://www.google.com/landing/2step/ (дата звернення: 19.10.2020)
8. Багатофакторна автентифікація. SAASPASS: веб-сайт. URL: https://saaspass.com/ (дата звернення: 20.10.2020)
9. Захищена схема автентифікації, щоб зірвати RT MITM, CR MITM та фішинг-атаки на основі зловмисного браузера. Гаурав В., Маной М., Праділ А.: веб-сайт. URL: https://www.sciencedirect.com/science/article/abs/pii/S2214212618300140 (дата звернення: 20.10.2020)
10. Син-Хюн К., Десон К., Син-Хун Дж., Сунг-Хун Л., *Схема автентифікації на основі геолокації на основі QR-коду, щоб перемогти активну фішинг-атаку в режимі реального часу*: матеріали семінару з управління цифровими ідентичностями (DIM '13). Асоціація обчислювальних машин, Нью-Йорк, Нью-Йорк, США, 2013 р. С. 51–62.
11. Мухопадхяй С., Арглес Д., *Механізм боротьби з фішингом для єдиного входу на основі QR-коду*: матеріали міжнародної конференції з інформаційного суспільства (i-Society 2011), Лондон, 2011 р. С. 505-508.
12. Додсон Б., Сенгупта Д., Боне Д., Лам М.С., *Безпечна, зручна для споживачів веб-автентифікація та платежі за допомогою телефону*: матеріали із збір. MobiCASE 2010, конспекту лекцій Інституту комп'ютерних наук, Спрінгер, Берлін, Гейдельберг, 2010. Т. 76.
13. Лун Ч., *Придушити фішинг за допомогою CAPTCHA за допомогою OTP*: матеріали третьої міжнародної конференції з питань боротьби з підробкою, безпекою та ідентифікацією у зв'язку, Гонконг, 2009. С. 187-192.
14. Ваш ключ до найшвидшого та найбезпечнішого входу. Yubico: веб-сайт. URL: https://www.yubico.com/why-yubico/for-individuals/ (дата звернення: 21.10.2020)
15. Г. Варшні та М. Місра, *Вхід на основі push-повідомлень із використанням пристроїв BLE*: матеріали 2-ї міжнародної конференції з інформаційних технологій, інформаційних систем та електротехніки (ICITISEE), Джокьякарта, 2017. С. 479-484.
16. М. Се, Й. Лі, К. Йошиго, Р. Секер и Дж. Біан, *Забезпечення автентифікації в Інтернеті за допомогою камери*: матеріали 16-го Міжнародного симпозіуму з інженерії систем високих гарантій, Дейтона-Біч-Шорз, Флорида, 2015. С. 232-239.
17. Lastpass запам'ятовує всі ваші паролі. Lastpass: веб-сайт. URL: https://www.lastpass.com/ (дата звернення: 21.10.2020)
18. Росс Б., Джексон С., Міяке Н., Боне Д., Мітчелл Дж. *Потужніша автентифікація пароля за допомогою розширення браузера*. Балтімор, США, 2005. С. 17-32.
19. Довідковий документ про запобігання фішинг-атакам людини із багатофакторною аутентифікацією. Tricipher: веб-сайт. URL: https://www.globaltrustit/documents/press/phishing/ PhishingSolutionWhitepaper.pdf (дата звернення: 22.10.2020)

20. Увійти в систему Yahoo. Yahoo: веб-сайт. URL: https://login.yahoo.com/ (дата звернення: 23.10.2020)
21. RSA SecurID. Beal V: веб-сайт. URL: https://www.webopedia.com/TERM/R/rsa_secure_id.html / (дата звернення: 23.10.2020)
22. Б.Б. Чжу, Дж. Ян, Г. Бао, М. Ян і Н. Сю, *Капча як графічні паролі - новий примітив безпеки, заснований на складних проблемах ШІ*, у "Протоколах угод з інформаційної криміналістики та Безпеки, т. 9, №6, червень 2014 р. С. 891-904.
23. Дж. Бонно і С. Прейбуш, *Зарості паролів: технічні та ринкові помилки при аутентифікації людини в Інтернеті*, в Proc. WEIS. 2010 р. С. 1-48.
24. Дж. Бонно, К. Герлі, П.К. Ооршота та Ф. Стаджано, *Прагнення замінити паролі: рамки для порівняльної оцінки схем автентифікації через Інтернет: мате*ріали симпозіуму з безпеки та конфіденційності, Сан-Франциско, СА, 2012 р. С. 553-567.

REFERENCES

1. E.E. Lastdrager. Achieving a consensual definition of phishing based on a systematic review of the literature, *Crime Sci* vol. 3, 2014, pp. 21-32, DOI:https://doi.org/10.1186/s40163-014-0009-y [in English]
2. A. Neda. Multi-label rules for phishing classification, *Applied Computing and Informatics*, vol. 11, 2015, pp. 29-46, DOI:https://doi.org/10.1016/j.aci.2014.07.002 [in English]
3. Banday M.T., Qadri J.A. Phishing - A Growing Threat to E-Commerce, *The Business Review*, vol. 12, 2011, pp. 76-83. [in English]
4. Badra M., El-Sawda S., Hajjeh I., "Phishing attacks and solutions", *in Proceedings of the 3rd International Conference on Mobile Multimedia Communications, MobiMedia 2007,* Nafpaktos, Greece, August 27-29, 2007, pp. 42-43. [in English]
5. Rami M. M., Fadi T., Lee M., Tutorial and critical analysis of phishing websites methods, *Computer Science Review*, vol. 17, 2015, pp. 1-24, DOI:https://doi.org/10.1016/j.cosrev.2015.04.001 [in English]
6. Jagatic T., Nathaniel J., Menczer F. Social phishing, *Commun*, 2007, pp. 94-100. [in English]
7. Stronger security for your Google Account. Google., 2015. [Online]. Available: https://www.google.com/landing/2step/. [Accessed October 19, 2020]. [in English]
8. Multi-Factor Authentication. SAASPASS., 2019. [Online]. Available: https://saaspass.com/. [Accessed October 20, 2020]. [in English]
9. Secure authentication scheme to thwart RT MITM, CR MITM and malicious browser extension based phishing attacks. Gaurav V., Manoj M., Pradeep A., 2018. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S2214212618300140. [Accessed October 20, 2020]. [in English]
10. Seung-Hyun K., Daeseon C., Seung-Hun J., Sung-Hoon L., "Geo-location based QR-Code authentication scheme to defeat active real-time phishing attack", *in Proceedings of the 2013 ACM workshop on Digital identity management (DIM '13). Association for Computing Machinery*, New York, NY, USA, 2013, pp. 51–62. DOI:https://doi.org/10.1145/2517881.2517889 [in English]
11. Mukhopadhyay S., Argles D., "An Anti-Phishing mechanism for single sign-on based on QR-code", *in Proceedings of the International Conference on Information Society (i-Society 2011)*, London, 2011, pp. 505-508, DOI:10.1109/i-Society18435.2011.5978554 [in English]
12. Dodson B., Sengupta D., Boneh D., Lam M.S., "Secure, Consumer-Friendly Web Authentication and Payments with a Phone", *in Proceedings of the MobiCASE 2010. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering,* vol 76. Springer, Berlin, Heidelberg. DOI:https://doi.org/10.1007/978-3-642-29336-8_2 [in English]
13. Leung C., "Depress phishing by CAPTCHA with OTP", *in Proceedings of the 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication*, Hong Kong, 2009, pp. 187-192, DOI:10.1109/ICASID.2009.5276926. [in English]

14. Your key to the fastest, safest login. Yubico., 2019. [Online]. Available: https://www.yubico.com/why-yubico/for-individuals/. [Accessed October 21, 2020]. [in English]
15. G. Varshney and M. Misra, "Push notification based login using BLE devices", *in Proceedings of the 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, Yogyakarta, 2017, pp. 479-484, DOI: 10.1109/ICITISEE.2017.8285554. [in English]
16. M. Xie, Y. Li, K. Yoshigoe, R. Seker and J. Bian, "CamAuth: Securing Web Authentication with Camera", *in Proceedings of the 16th International Symposium on High Assurance Systems Engineering*, Daytona Beach Shores, FL, 2015, pp. 232-239, DOI:10.1109/HASE.2015.41. [in English]
17. Lastpass remembers all your passwords. Lastpass., 2019. [Online]. Available: https://www.lastpass.com/. [Accessed October 21, 2020]. [in English]
18. Ross B., Jackson C., Miyake N., Boneh D., Mitchell JC., *Stronger password authentication using browser extension.* Baltimore, MD, USA, 2005, pp. 17-32. [in English]
19. White paper preventing man in the middle phishing attacks with multi-factor authentication. Tricipher., 2019. [Online]. Available: https://www.globaltrustit/documents/press/phishing/ PhishingSolutionWhitepaper.pdf. [Accessed October 22, 2020]. [in English]
20. Yahoo sign in. Yahoo., 2016. [Online]. Available: https://login.yahoo.com/. [Accessed October 23, 2020]. [in English]
21. RSA SecurID. Beal V., 2019. [Online]. Available: https://www.webopedia.com/TERM/R/ rsa_secure_id.html/. [Accessed October 23, 2020]. [in English]
22. B. B. Zhu, J. Yan, G. Bao, M. Yang and N. Xu, "Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems," *in* ", *in Proceedings of the Transactions on Information Forensics and Security*, vol. 9, no. 6, pp. 891-904, June 2014, DOI:10.1109/TIFS.2014.2312547. [in English]
23. J. Bonneau and S. Preibusch, "The password thicket: technical and market failures in human authentication on the web," in Proc. WEIS 2010, pp 1-48. [in English]
24. J. Bonneau, C. Herley, P. C. v. Oorschot and F. Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," *in Proceedings of the Symposium on Security and Privacy*, San Francisco, CA, 2012, pp. 553-567, DOI:10.1109/SP.2012.44. [in English]

Надійшла – 09.09.2020.