МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ПОЛІТЕХНІЧНИЙ УНІВЕРСИТЕТ

ІНСТИТУТ КОМП'ЮТЕРНИХ СИСТЕМ

МАТЕРІАЛИ ДЕВ'ЯТОЇ МІЖНАРОДНОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ СТУДЕНТІВ ТА МОЛОДИХ ВЧЕНИХ

присвячена 55-річчю
ІНСТИТУТУ КОМП'ЮТЕРНИХ СИСТЕМ

" Сучасні інформаційні технології 2019 "

" Modern Information Technology 2019 "

23-24 травня

Одеса
«Екологія»
2019

УДК 004.42

ПРОГРАМНА СИСТЕМА ДЛЯ ЗБЕРІГАННЯ, УПРАВЛІННЯ І ПЕРЕДАЧІ ЗАШИФРОВАНИХ АУТЕНТИФІКАЦІЙНИХ ДАНИХ КОРИСТУВАЧІВ

Комлева Н. О., Паршин І. А., Воронюк Д. С.
к.т.н., доцент каф. СПЗ Комлева Н. О.
Одеський Національний Політехнічний Університет, УКРАЇНА

АНОТАЦІЯ. Розроблено систему для зберігання, управління і передачі аутентифікаційних даних. Система передбачає розробку веб-застосування і розширення для Google Chrome та мобільне застосування для ОС Android. Веб-клієнт розроблений на мові Javascript з використанням фреймворку Angular.

Вступ. Сучасний серфінг в мережі Інтернет не обмежується пошуком необхідної інформації. Багато ресурсів потребують реєстрації та авторизації користувача. Це необхідна дія для багатьох функцій, наприклад персоналізації стрічки новин свого регіону, для завантаження власних фотографій та відео для друзів або ж просто для спілкування. Сучасний користувач має багато акаунтів на різних ресурсах, і для доступу до них необхідно мати логін та пароль. Складність пароля визначає складність доступу до персональної сторінки, але користувачі часто зневажають цим фактором. Так, величезна кількість людей використовує найпростіші паролі, такі як “123456” (120511 користувачів), “qwerty” (20778 користувачів), або навіть “password” (39448 користувачів) [1]. Крім того, люди використовують паролі однакові на всіх сайтах, це означає, що при зламі найслабшого із них хакери отримають доступ до всіх ресурсів користувача з усіма його персональними даними, та зможуть використати їх у своїх намірах. Для надійного зберігання важливої інформації в мережі треба мати унікальні паролі для кожного інформаційного ресурсу. Але дуже скоро у користувача з'являється проблема з авторизацією, тому що важко запам'ятати велику кількість пар логінів та паролів.

Мета роботи. Метою роботи є підвищення безпеки зберігання, управління і передачі аутентифікаційних даних шляхом розробки та використання системи зберігання паролів на смартфоні з використанням методу шифрування AES 256.

Основна частина роботи. Відмінним рішенням для користувачів є використання програм для безпечного зберігання паролів, серед популярних можна виділити KeePass, Lastpass, 1Password, RoboForm та інші. Але всі вони мають декілька особливостей. Всі перелічені програмні продукти передбачають зберігання паролів на сервері або за допомогою хмарних технологій, тобто весь час дані знаходяться в потенційній небезпеці зламу. Більш того для кожної програми знадобиться запам'ятовування одного головного пароля, при зламі якого хакер зможе дістатися і до всіх інших. Саме тому була розроблена програмна система ISaver, що передбачає зберігання паролів на смартфоні, тобто якщо смартфон не підключений до Інтернету, особисті дані, що зберігаються на ньому, знаходяться в повній безпеці. Система передбачає розробку веб-застосування і розширення для Google Chrome та мобільне застосування для ОС Android. При підключенні до мережі можна швидко та безпечно отримати аутентифікаційну інформацію, бо для передачі на будь-який чужий комп'ютер треба зашифрувати лише канал передачі (використано метод шифрування AES 256). Для зв'язування девайсів у мережі було обрано технологію SignalR Core, вона відповідає за швидке підключення та дозволяє обмінюватися інформацією між девайсами в режимі реального часу. Підключений веб-клієнт має унікальний ідентифікатор, який разом із ключем треба відправити на телефон.

Для передачі інформації для зв'язування використовується QR код (Quick Response Code – код швидкого реагування), за допомогою якого передача даних йде по безпечному каналу, що неможливо прослухати. Після сканування на мобільному девайсі є вся необхідна інформація для відправлення зашифрованих паролів до комп’ютера, з якого відскановано код. Далі обмін зашифрованою інформацією здійснюється через сервер (рисунок 1).

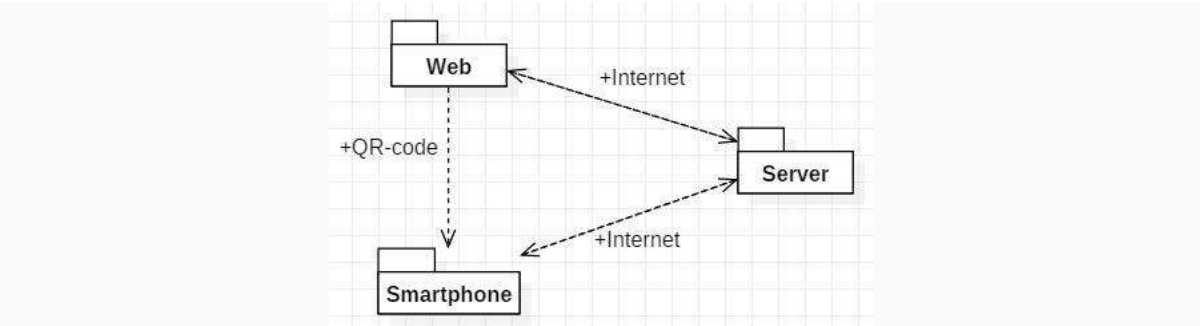

Рис. 1 – Схема функціонування системи

Програмна реалізація системи ISaver демонструє можливість з'єднання будь-якого телефона з будь-яким комп'ютером у мережі та безпечну передачу даних на прикладі логінів та паролів. Частина системи, що працює на смартфоні, розроблена за допомогою Xamarin – фреймворку для багатоплатформової розробки мобільних додатків (iOS, Android, Windows Phone) з використанням мови C#. Скріншоти Android-застосування представлені на рисунку 2.

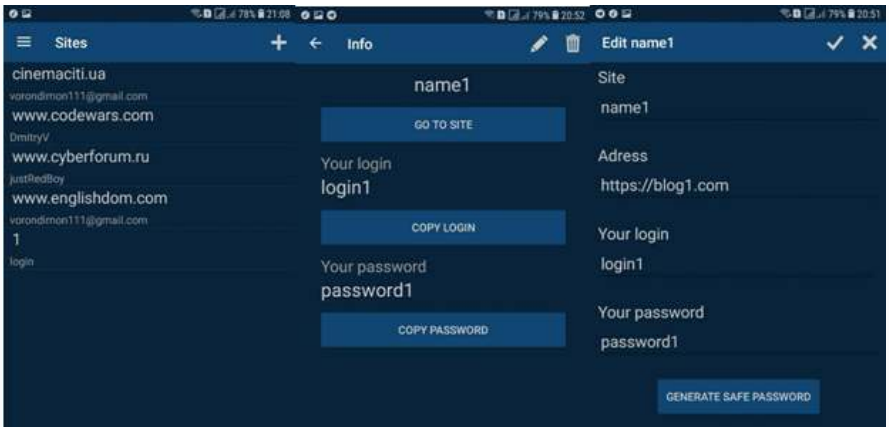

Рис.2 – Зовнішній вигляд Android-застосування

На сьогодні програмне забезпечення, що призначене для використання у середовищі веб, є дуже актуальним. Веб-застосування мають декілька істотних переваг перед десктопними програмами, а саме: 1) відсутність потреби у встановленні на комп'ютер, адже веб-застосування необхідно лише відкрити у браузері; 2) використання обчислювальні потужності віддаленого сервера для важких обчислень; 3) усунення потреби брати на себе обов'язки адміністратора. Саме тому для даної системи ISaver було обрано формат веб-застосування. Веб-клієнт розроблений на мові Javascript з використанням фреймворку Angular, що є JavaScript-фреймворком з відкритим програмним кодом, мета якого – розширення браузерних застосувань на основі шаблону MVC, спрощення їх тестування та розробки [2, 3].

Висновок. Було розроблено систему для зберігання, управління і передачі аутентифікаційних даних. У майбутньому планується доопрацювання системи для можливості передачі файлів. Вибір інструментальних засобів розробки передбачає можливе перенесення існуючого Android-застосування на інші мобільні платформи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. «Хакер»: безопасность, разработка, DevOps [Електроний ресурс] – Режим доступу: URL: https://xakep.ru/.
2. Флэнаган Д. JavaScript. Подробное руководство, 2012. – 1080 с.
3. Дилеман П. Изучаем Angular. – Packt, 2017. – 354 с.