УДК 004.056.55

Азарова А.О.
Бадя Ю.В.

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИЩЕНОГО ПЕРЕДАВАННЯ КОНФІДЕНЦІЙНИХ ДАНИХ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

Вінницький національний технічний університет

Анотація

У даній роботі розглянуто та досліджено існуючі методи захищеного передавання конфіденційних даних для мобільних пристроїв та запропоновано нове рішення, що полягає у поєднанні існуючих методів задля підвищення захисту мобільного додатку. У роботі було представлено практичне застосування запропонованого методу на прикладі захищеного мобільного додатку на платформі Android.

Ключові слова: інформаційна безпека, захист інформації, конфіденційні дані, захищене передавання інформації, мобільні пристрої, наскрізне шифрування, мобільний додаток, захищений месенджер.

Abstract

In this paper, existing methods of secure transmission of confidential data for mobile devices are examined and explored, and a new solution is proposed, which is to combine existing methods to enhance the security of the mobile application. The practical application of the proposed method was presented on the example of a secure mobile application on the Android platform.

Keywords: information security, protection of information, confidential data, secure information transmission, mobile devices, through encryption, mobile application, secure messenger.

Сьогодні смартфони стають не тільки засобом зв'язку, але і доступним способом отримання інформації. Вони зручні, портативні та займають обмаль місця, при цьому поєднують в собі безліч функцій різних девайсів та пристроїв. У цьому аспекті портативні пристрої значно перевершують рідкокристалічні громадини з суперпотужним процесором.

Інформаційний потік збільшується в шаленому темпі, ми передаємо величезну кількість інформації щохвилини, всі дані взаємопов’язані, і тому, для забезпечення конфіденційності, необхідно правильно забезпечувати процес передачі інформації. У найпоширенішому на сьогодні способі швидкої передачі даних – через мобільні додатки (або месенджери) для вирішення проблеми обробки інформації використовують методи захищеного передавання конфіденційних даних.

Метою виконання роботи – дослідити методи захищеного передавання конфіденційних даних для мобільних пристроїв та створити мобільний додаток з використанням методів захищеного передавання конфіденційних даних.

Розробники сучасних месенджерів стали приділяти більшу увагу забезпеченню безпеки своїх клієнтів і анонімності, але жоден не може гарантувати повноцінної безпеки. Сучасні менеджери, багато з яких відомі своїми надійними алгоритмами шифрування, безпекою передачі повідомлень та наявністю секретних чатів, проте, все ж мають вразливості та можливість злому, вони використовують закриті коди або ж власні алгоритми шифрування, але все ж не забезпечують захист даних, що передаються. Більшість користувачів обирають програму для спілкування або ведення переписки саме за цим критерієм, тому ми повинні забезпечити повноцінний захист. В даній роботі досліджено питання підвищення безпеки.

Результатом дослідження є поєднання декількох методів для підвищення захисту мобільного додатку. В програмній реалізації було використано методи шифрування AES, IPSec та SHA-256.

IPsec – набір протоколів для забезпечення захисту даних, що передаються за допомогою протоколу IP, дозволяє здійснювати підтвердження справжньості та/або шифрування IP-пакетів. IPsec працює на мережевому рівні та може забезпечувати цілісність та/або конфіденційність даних переданих по мережі.

SHA-256 являє собою криптографічний функцію хешування, яка є односпрямованої функцією алгоритму SHA-2. Основне застосування – захист інформації.

Платформою для створення мобільного додатку в даній роботі було обрано Xamarin. Вона дозволяє вирішувати широке коло завдань у створенні та розробці мобільних додатків та подавати їх у потрібному вигляді.

Мобільний додаток буде розроблено для платформи Android. На базі цієї операційної системи працює переважна більшість мобільних пристроїв. Android відрізняє відкритість при розробці та публікації додатків, а також величезна різноманітність пристроїв широкого цінового діапазону.

В даній роботі було проведено дослідження методів передавання конфіденційних даних для мобільних пристроїв, проаналізовано та проведено оцінку сучасних існуючих месенджерів для передавання конфіденційних даних на мобільних пристроях.

Для програмної реалізації було обрано мову програмування C#. Обрана технолгія Microft .NET та Xamarin – фреймворк для кросплатформової розробки мобільних додатків. Мобільний додаток реалізовано для платформи Android.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУТРИ

1. How to protect mobile data through encryption and secure transfer [Електронний ресурс] – Режим доступу до ресурсу: http://www.enlume.com/mobile-data-security/.

2. Guidelines on the protection of personal data processed by mobile applications provided by European Union institutions [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://edps.europa.eu/sites/edp/files/publication/16-11-07_guidelines_mobile_apps_en.pdf.

3. Sharma S. Secure Data Transfer & File Sharing Use of Cloud Service for Mobile Application [Електронний ресурс] / S. Sharma, R. Sharma. – 2016. – Режим доступу до ресурсу: Secure Data Transfer & File Sharing Use of Cloud Service for Mobile Application [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: http://ijcsit.com/docs/aceit-conference-2016/aceit201606.pdf.

4. Holla S. “ANDROID BASED MOBILE APPLICATION DEVELOPMENT and its SECURITY / Suhas Holla., 2012.

5. Xamarin: Mobile App Development & App Creation Software [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.xamarin.com/.

6. IPsec (Internet Protocol Security) [Електронний р есурс]. – 2010. – Режим доступу до ресурсу: https://searchmidmarketsecurity.techtarget.com/definition/IPsec.

7. Алгоритмы / Хэш-функция SHA-256 [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://medium.com/dtechlog/алгоритмы-хэш-функция-sha-256-9862302f942f.

Азарова Анжеліка Олексіївна – кандидат технічнних наук, професор кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м.Вінниця.

Бадя Юлія Вікторівна – студентка групи УБ-14б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м.Вінниця, e-mail: badyayulia@gmail.com.

Azarova Anzhelika – PhD, Professor of management and security of information systems, Vinnytsia National Technical University, Vinnytsia.

Yulia Badya: student of UB-14b group, faculty of management and information security, Vinnytsia National Technical University, Vinnytsia, e-mail: badyayulia@gmail.com.