Bezpieczeństwo aplikacji mobilnych

Laboratorium 2

Cel zajęć:

- Stworzenie aplikacji mobilnej w Expo React Native z funkcjonalnością przechowywania wrażliwych danych.
- Zastosowanie metod bezpiecznego przechowywania danych w aplikacji mobilnej.
- Przetestowanie aplikacji pod kątem zabezpieczeń związanych z przechowywaniem danych.

Wymagane narzędzia:

- Node.js i npm lub yarn.
- Expo CLI.
- Emulator Android/iOS lub fizyczne urządzenie z aplikacją Expo Go.
- Wybrany język programowania do stworzenia API (np. Node.js, Python, Java).
- Narzędzia do testowania aplikacji, np. ADB (Android Debug Bridge) dla Androida lub odpowiedniki dla iOS.
- Biblioteki do szyfrowania danych w Expo React Native (np. **expo-secure-store**, **react-native-encrypted-storage**).

Zadania do wykonania:

1. **Przygotowanie środowiska:**
    - Upewnij się, że masz zainstalowane wszystkie niezbędne narzędzia: Node.js, Expo CLI oraz emulator lub fizyczne urządzenie z aplikacją Expo Go.
    - Wybierz język programowania, w którym stworzysz proste API do obsługi danych (opcjonalnie, jeśli planujesz komunikację z serwerem).
2. **Stworzenie aplikacji mobilnej:**
    - Utwórz nowy projekt Expo React Native.
    - Zaprojektuj prostą aplikację, która umożliwia użytkownikowi wprowadzenie wrażliwych danych, takich jak notatki, hasła lub informacje osobiste.
    - Dodaj interfejs użytkownika z polami do wprowadzania danych oraz przyciskami do zapisywania i wyświetlania tych informacji.
3. **Implementacja lokalnego przechowywania danych:**
    - Zaimplementuj funkcjonalność przechowywania danych lokalnie na urządzeniu przy użyciu mechanizmów dostępnych w Expo React Native, takich jak **AsyncStorage**.
    - Upewnij się, że dane są poprawnie zapisywane i odczytywane, a także dostępne po ponownym uruchomieniu aplikacji.
4. **Analiza bezpieczeństwa przechowywania danych:**
    - Sprawdź, gdzie na urządzeniu są przechowywane dane aplikacji.
    - Użyj narzędzi takich jak ADB (dla Androida) lub odpowiednich narzędzi dla iOS, aby uzyskać dostęp do plików aplikacji.
    - Zbadaj, czy dane są przechowywane w formie czytelnej i czy można je odczytać poza aplikacją.

5. **Implementacja szyfrowania danych:**
    - Zaimplementuj szyfrowanie przechowywanych danych, korzystając z bibliotek takich jak **expo-secure-store** lub **react-native-encrypted-storage**.
    - Zmodyfikuj aplikację tak, aby przed zapisaniem danych na urządzeniu były one szyfrowane.
    - Upewnij się, że proces szyfrowania i deszyfrowania działa poprawnie podczas zapisywania i odczytywania danych.
6. **Testowanie zabezpieczeń danych:**
    - Ponownie użyj narzędzi do eksploracji plików aplikacji, aby sprawdzić, czy dane są teraz przechowywane w formie zaszyfrowanej i nieczytelne dla osób trzecich.
    - Spróbuj uzyskać dostęp do danych aplikacji bezpośrednio z systemu plików i oceń, czy jest to możliwe bez odpowiednich kluczy.
7. **Wdrożenie dodatkowych mechanizmów ochrony:**
    - Dodaj do aplikacji mechanizmy uwierzytelniania użytkownika, takie jak kod PIN, hasło lub uwierzytelnianie biometryczne (jeśli to możliwe).
    - Upewnij się, że dostęp do wrażliwych danych w aplikacji jest chroniony i wymaga dodatkowej autoryzacji.