Bezpieczeństwo aplikacji mobilnych

Laboratorium 4

Zarządzanie uprawnieniami w aplikacjach mobilnych

Cel zajęć:

- Stworzenie aplikacji mobilnej w Expo React Native wykorzystującej różne uprawnienia systemowe.
- Zrozumienie znaczenia zarządzania uprawnieniami w aplikacjach mobilnych.
- Przetestowanie aplikacji pod kątem bezpieczeństwa w kontekście przyznawanych uprawnień.

Wymagane narzędzia:

- Node.js oraz npm lub yarn.
- Expo CLI.
- Emulator Android/iOS lub fizyczne urządzenie z aplikacją Expo Go.
- Dokumentacja Expo Permissions.
- Ewentualnie wybrany język programowania do stworzenia API (opcjonalnie).

Zadania do wykonania:

1. **Przygotowanie środowiska:**
    - Zainstaluj Node.js oraz Expo CLI na swoim komputerze.
    - Upewnij się, że masz dostęp do emulatora Android/iOS lub fizycznego urządzenia z zainstalowaną aplikacją Expo Go.
2. **Stworzenie aplikacji mobilnej:**
    - Utwórz nowy projekt Expo React Native.
    - Zaprojektuj aplikację, która będzie korzystać z różnych uprawnień systemowych, takich jak dostęp do:
        - Kamery
        - Lokalizacji
        - Kontaktów
        - Mikrofonu
    - Dodaj interfejs użytkownika umożliwiający korzystanie z funkcji wymagających tych uprawnień, np. robienie zdjęć, wyświetlanie lokalizacji na mapie, odczyt kontaktów.
3. **Implementacja żądania uprawnień:**
    - Wykorzystaj moduł Expo Permissions oraz specyficzne moduły, takie jak expo-camera, expo-location, expo-contacts.
    - Zaimplementuj żądanie uprawnień od użytkownika w czasie rzeczywistym, przed wykonaniem danej funkcji.
    - Obsłuż sytuacje, w których użytkownik odmawia przyznania uprawnienia, np.:
        - Wyświetl komunikat informujący o konieczności przyznania uprawnienia dla pełnej funkcjonalności.
        - Zapewnij alternatywne działanie aplikacji bez wymaganych uprawnień.
4. **Analiza nadanych uprawnień:**
    - Sprawdź plik app.json lub app.config.js, aby zobaczyć, jakie uprawnienia są deklarowane.

- Upewnij się, że aplikacja żąda tylko tych uprawnień, które są niezbędne do jej działania.
- Przetestuj aplikację na emulatorze lub urządzeniu, monitorując, o jakie uprawnienia prosi podczas instalacji i działania.

5. **Testowanie skutków nadawania zbyt szerokich uprawnień:**
   - Zmodyfikuj aplikację, dodając dodatkowe uprawnienia, które nie są potrzebne do jej podstawowej funkcjonalności.
   - Przeanalizuj, jakie dodatkowe dane lub funkcje systemowe stają się dostępne dla aplikacji z tymi uprawnieniami.
6. **Ograniczanie uprawnień aplikacji:**
   - Usuń niepotrzebne uprawnienia z aplikacji, zarówno w kodzie, jak i w plikach konfiguracyjnych.
   - Zaimplementuj zasadę minimalnych uprawnień (least privilege), prosząc o uprawnienia tylko wtedy, gdy są one absolutnie konieczne.
   - Upewnij się, że aplikacja działa poprawnie przy zredukowanym zestawie uprawnień.
7. **Testowanie aplikacji pod kątem bezpieczeństwa:**
   - Przeprowadź testy aplikacji, sprawdzając, czy nie wykorzystuje ona uprawnień w nieautoryzowany sposób.
   - Użyj narzędzi do monitorowania dostępu do danych, aby upewnić się, że aplikacja nie uzyskuje dostępu do danych bez wiedzy użytkownika.
   - Sprawdź, czy aplikacja prawidłowo obsługuje odmowę przyznania uprawnienia przez użytkownika.