Bezpieczeństwo aplikacji mobilnych

Laboratorium 5

Podstawy ochrony aplikacji mobilnych przed inżynierią wsteczną z wykorzystaniem Expo React Native

Cel zajęć:

- Poznanie zagrożeń związanych z inżynierią wsteczną aplikacji mobilnych.
- Nauczenie się podstawowych metod ochrony aplikacji przed dekompilacją i analizą kodu.
- Praktyczne zastosowanie technik zabezpieczających w aplikacjach Expo React Native.

Tematyka:

- Inżynieria wsteczna w kontekście aplikacji mobilnych.
- Proste metody dekompilacji aplikacji Expo React Native.
- Podstawowe techniki ochrony przed inżynierią wsteczną:
    - Obfuskacja kodu JavaScript.
    - Usuwanie wrażliwych informacji z kodu aplikacji.

Wymagane narzędzia:

- Node.js oraz npm lub yarn.
- Expo CLI.
- Emulator Android/iOS lub fizyczne urządzenie z aplikacją Expo Go.
- Narzędzie do dekompilacji aplikacji mobilnych, np. Apktool.
- Narzędzie do obfuskacji kodu JavaScript.

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.
    - Pobierz i zainstaluj narzędzie do dekompilacji aplikacji mobilnych, takie jak Apktool.
2. **Stworzenie prostej aplikacji mobilnej:**
    - Utwórz nowy projekt Expo React Native.
    - Zaimplementuj prostą aplikację z podstawową funkcjonalnością, np. kalkulator, notatnik czy wyświetlanie komunikatu.
    - W kodzie aplikacji umieść przykładowe dane, które mogą być wrażliwe (np. klucz API, hasło w formie tekstowej).
3. **Analiza aplikacji przed wprowadzeniem zabezpieczeń:**
    - Zbuduj aplikację w trybie produkcyjnym.
    - Wyeksportuj plik APK (dla Androida).
    - Użyj Apktool do dekompilacji aplikacji.
    - Przeanalizuj zdekompilowany kod, zwracając uwagę na:
        - Dostępność i czytelność kodu źródłowego.
        - Obecność wrażliwych informacji w kodzie.

4. **Implementacja obfuskacji kodu:**
    - Skorzystaj z narzędzia do obfuskacji kodu JavaScript, aby utrudnić analizę kodu źródłowego.
    - Zastosuj obfuskację na plikach JavaScript swojej aplikacji.
    - Upewnij się, że aplikacja działa poprawnie po obfuskacji.
5. **Ponowna analiza aplikacji po wprowadzeniu obfuskacji:**
    - Zbuduj aplikację z włączoną obfuskacją kodu.
    - Ponownie zdekompiluj aplikację za pomocą Apktool.
    - Sprawdź, czy kod jest mniej czytelny i trudniejszy do analizy.
    - Zwróć uwagę, czy wrażliwe informacje są nadal łatwo dostępne.
6. **Usuwanie wrażliwych informacji z kodu:**
    - Przejrzyj kod aplikacji i usuń wszystkie wrażliwe informacje, takie jak klucze API czy hasła.
    - Jeśli to konieczne, przenieś wrażliwe dane na serwer lub użyj mechanizmów bezpiecznego przechowywania.
    - Zbuduj aplikację ponownie i upewnij się, że wrażliwe informacje nie są już obecne w kodzie.