Bezpieczeństwo aplikacji mobilnych

Laboratorium 3

Bezpieczna komunikacja między aplikacją a serwerem

Cel zajęć:

- Stworzenie aplikacji mobilnej w Expo React Native z funkcjonalnością komunikacji z serwerem.
- Implementacja bezpiecznej komunikacji między aplikacją a serwerem przy użyciu protokołu HTTPS.
- Przetestowanie aplikacji pod kątem podatności na ataki typu Man-in-the-Middle (MITM).

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 serwera (np. Node.js, Python, Java).
- Narzędzia do generowania certyfikatów SSL (np. OpenSSL).
- Narzędzia do przeprowadzania ataków MITM (np. mitmproxy).
- Narzędzia do testowania API, takie jak Postman lub Insomnia.

Zadania do wykonania:

1. **Przygotowanie środowiska:**
    - Upewnij się, że masz zainstalowane wszystkie niezbędne narzędzia: Node.js, Expo CLI, emulator lub fizyczne urządzenie z aplikacją Expo Go.
    - Wybierz język programowania, w którym stworzysz serwer z obsługą HTTPS.
2. **Stworzenie aplikacji mobilnej:**
    - Utwórz nowy projekt Expo React Native.
    - Zaprojektuj aplikację, która komunikuje się z serwerem w celu pobrania lub wysłania danych (np. lista produktów, wiadomości).
    - Zaimplementuj funkcjonalność wysyłania żądań do serwera za pomocą protokołu HTTP.
3. **Implementacja serwera z obsługą HTTPS:**
    - Stwórz serwer, który obsługuje żądania od aplikacji mobilnej.
    - Wygeneruj własny certyfikat SSL za pomocą narzędzia OpenSSL lub skorzystaj z samopodpisanego certyfikatu.
    - Skonfiguruj serwer tak, aby obsługiwał połączenia HTTPS, korzystając z wygenerowanego certyfikatu.
4. **Modyfikacja aplikacji do komunikacji przez HTTPS:**
    - Zmień adresy URL w aplikacji mobilnej, aby korzystały z protokołu HTTPS zamiast HTTP.
    - Upewnij się, że aplikacja może nawiązać bezpieczne połączenie z serwerem i poprawnie przetwarza odpowiedzi.
5. **Testowanie podatności na ataki typu MITM:**
    - Użyj narzędzia mitmproxy lub podobnego, aby przeprowadzić symulowany atak Man-in-the-Middle.

- Skonfiguruj urządzenie lub emulator tak, aby ruch sieciowy przechodził przez proxy mitmproxy.
- Obserwuj, czy możesz przechwycić i odczytać zaszyfrowane dane przesyłane między aplikacją a serwerem.

6. **Implementacja zabezpieczeń przed atakami MITM:**
   - Zaimplementuj w aplikacji mechanizm **Certificate Pinning**, który pozwala na weryfikację certyfikatu serwera.
   - Zmodyfikuj aplikację tak, aby akceptowała tylko zaufany certyfikat serwera i odrzucała połączenia z nieznanymi certyfikatami.
   - Upewnij się, że aplikacja poprawnie reaguje na próby podmiany certyfikatu przez atakującego.