Bezpieczeństwo aplikacji mobilnych

Wykład 8

Specyficzne mechanizmy bezpieczeństwa i ataki związane z platformami mobilnymi

Mateusz Pawełkiewicz

1. Wprowadzenie do zagrożeń specyficznych dla platform mobilnych

Wraz z rozwojem technologii mobilnych pojawiły się nowe zagrożenia i wyzwania związane z bezpieczeństwem aplikacji. Zarówno Android, jak i iOS posiadają specyficzne mechanizmy zabezpieczające oraz podatności, które mogą być wykorzystane przez atakujących. Deweloperzy muszą znać te zagrożenia i stosować odpowiednie środki ochrony, aby zapewnić bezpieczeństwo użytkownikom. W tym wykładzie omówimy specyficzne ataki i zagrożenia, które mogą wystąpić na platformach mobilnych, a także sposoby ochrony przed nimi.

2. Multitasking i zarządzanie stanem aplikacji/GUI caching

Zarządzanie stanem aplikacji podczas multitaskingu jest kluczowe dla ochrony danych użytkownika. Główne wyzwania to:

- **Przechowywanie wrażliwych danych w pamięci podręcznej**: Dane mogą być dostępne po przełączeniu między aplikacjami, co zwiększa ryzyko wycieku, jeśli aplikacja jest niewłaściwie zarządzana.
- **Podgląd zrzutów ekranu**: Systemy operacyjne, aby poprawić doświadczenie użytkownika, często wykonują zrzuty ekranu, które są widoczne podczas przełączania aplikacji. Może to prowadzić do ujawnienia poufnych danych.

Aby zminimalizować ryzyko, deweloperzy powinni:

- Wymazywać dane lub zamazywać ekran w trakcie przełączania aplikacji.
- Ograniczać przechowywanie wrażliwych danych w pamięci podręcznej aplikacji.

3. Wprowadzanie danych (input caching) i związane z tym zagrożenia

Wprowadzanie danych w aplikacjach, takie jak formularze i pola logowania, może być narażone na przechwycenie, jeśli nie są one odpowiednio zabezpieczone. Przykładowe zagrożenia obejmują:

- **Keylogging**: Ataki, w których złośliwe aplikacje rejestrują wpisywane dane, np. hasła i dane osobowe.
- **Podsłuchiwanie wprowadzania danych**: Złośliwe oprogramowanie może przechwytywać informacje wprowadzane przez użytkownika.

Aby zabezpieczyć aplikację, deweloperzy powinni:

- Stosować bezpieczne komponenty wejściowe i wykorzystywać systemowe środki ochrony.
- Ograniczać dostęp aplikacji trzecich do kluczowych funkcji urządzenia.

4. Ataki na aplikacje webowe (CSRF, framing, clickjacking)

Aplikacje mobilne często wykorzystują komponenty webowe do wyświetlania treści, co może narażać je na specyficzne ataki, takie jak:

- **CSRF (Cross-Site Request Forgery)**: Atak polegający na zmuszeniu użytkownika do wykonania niechcianej akcji w aplikacji, np. przesłania formularza bez jego wiedzy.
- **Framing**: Umożliwienie osadzenia aplikacji lub jej części w ramce na stronie zewnętrznej, co może prowadzić do przechwycenia danych użytkownika.
- **Clickjacking**: Technika, w której użytkownik jest oszukiwany, aby kliknął niewidzialny lub zamaskowany element, wykonując niepożądane akcje.

Deweloperzy mogą przeciwdziałać tym atakom, stosując nagłówki zabezpieczające, takie jak X-Frame-Options, oraz implementując środki ochrony przed CSRF, np. używając tokenów CSRF.

5. Identyfikacja urządzeń i użytkowników (UDID)

Identyfikacja użytkowników i urządzeń jest niezbędna dla personalizacji doświadczeń użytkownika i śledzenia zachowań, ale musi być prowadzona w sposób zgodny z zasadami prywatności. Stosowanie unikalnych identyfikatorów, takich jak UDID (Unique Device Identifier), jest związane z potencjalnymi zagrożeniami:

- **Naruszenie prywatności**: Gromadzenie i przechowywanie unikalnych identyfikatorów użytkowników może prowadzić do naruszenia prywatności, jeśli dane są niewłaściwie chronione.
- **Śledzenie użytkowników**: Identyfikatory mogą być wykorzystywane do śledzenia zachowań użytkowników bez ich zgody.

Zamiast UDID, deweloperzy powinni używać losowo generowanych identyfikatorów oraz stosować zgodne z regulacjami metody śledzenia, takie jak Advertising ID na Androidzie i Identifier for Advertisers (IDFA) na iOS.

6. Bezpieczeństwo powiadomień push

Powiadomienia push to popularna metoda komunikacji aplikacji z użytkownikami, ale ich niewłaściwa implementacja może prowadzić do wycieków danych. Potencjalne zagrożenia obejmują:

- **Przesyłanie poufnych informacji**: Powiadomienia mogą ujawniać dane osobowe, jeśli ich treść nie jest odpowiednio zabezpieczona.
- **Podszywanie się pod aplikację**: Atakujący mogą wysyłać fałszywe powiadomienia, podszywając się pod zaufane aplikacje.

Deweloperzy powinni stosować środki, takie jak szyfrowanie danych w powiadomieniach i sprawdzanie autentyczności komunikatów, aby zabezpieczyć ten kanał komunikacji.

7. Tapjacking i zarządzanie logami

Tapjacking to atak polegający na nakładaniu przezroczystych elementów na interfejs użytkownika, co może skłonić użytkownika do kliknięcia w niewidoczny element, prowadząc do niezamierzonych działań. Z kolei zarządzanie logami jest istotne dla ochrony informacji o działaniu aplikacji:

- **Tapjacking**: Ochrona przed tapjackingiem polega na stosowaniu zabezpieczeń warstwy interfejsu użytkownika, aby uniemożliwić nakładanie zewnętrznych elementów na aplikację.
- **Logi aplikacji**: Logi mogą zawierać poufne dane, które mogą być wykorzystane przez atakujących. Deweloperzy powinni ograniczać zapisywanie wrażliwych informacji i stosować szyfrowanie tam, gdzie to konieczne.

8. Podsumowanie i wnioski

Specyficzne mechanizmy bezpieczeństwa oraz zagrożenia związane z platformami mobilnymi wymagają od deweloperów szczególnej uwagi i stosowania odpowiednich środków ochrony. Zapobieganie atakom, takim jak CSRF, tapjacking czy clickjacking, oraz zabezpieczanie danych użytkowników przed śledzeniem i wyciekiem, są niezbędne dla zapewnienia bezpiecznego korzystania z aplikacji. Stosowanie najlepszych praktyk oraz ciągłe aktualizowanie wiedzy o nowych zagrożeniach pozwala na tworzenie aplikacji, które są nie tylko funkcjonalne, ale także bezpieczne dla użytkowników.

Literatura:

Dominic Chell, Tyrone Erasmus, Shaun Colley, Ollie Whitehouse – *Bezpieczeństwo aplikacji mobilnych. Podręcznik hakera*, Helion.