Bezpieczeństwo aplikacji mobilnych

Wykład 5

Bezpieczeństwo danych w aplikacjach mobilnych

Mateusz Pawełkiewicz

1. Wprowadzenie do ochrony danych w aplikacjach mobilnych

W dobie rosnącej cyfryzacji ochrona danych użytkowników stała się priorytetem dla twórców aplikacji mobilnych. Dane takie jak loginy, hasła, dane osobowe i inne informacje poufne są codziennie przetwarzane przez aplikacje mobilne, co czyni je celem dla potencjalnych ataków. Deweloperzy muszą więc wdrażać strategie, które minimalizują ryzyko naruszeń danych i zapewniają bezpieczeństwo użytkownikom. W tym wykładzie omówimy najważniejsze aspekty związane z bezpieczeństwem danych w aplikacjach mobilnych oraz praktyki zabezpieczania danych.

2. Zagrożenia związane z wykradaniem danych – studium przypadków

W ciągu ostatnich lat pojawiło się wiele przypadków, w których aplikacje mobilne padły ofiarą ataków skutkujących wykradaniem danych użytkowników. Przykładowo:

- **Ataki typu man-in-the-middle (MitM)**: Ataki te polegają na przechwytywaniu komunikacji pomiędzy urządzeniem użytkownika a serwerem aplikacji. Bez odpowiedniego szyfrowania, dane mogą zostać wykradzione.
- **Luki w zabezpieczeniach aplikacji**: Źle zaimplementowane funkcje aplikacji mogą pozwalać na nieautoryzowany dostęp do danych. Przykładem mogą być błędy w walidacji wejścia, które umożliwiają ataki typu SQL injection.

Analiza takich przypadków uświadamia deweloperom konieczność stosowania najlepszych praktyk zabezpieczeń oraz regularnego testowania aplikacji pod kątem luk w zabezpieczeniach.

3. Metody bezpiecznego przechowywania danych

Bezpieczne przechowywanie danych to jeden z kluczowych elementów projektowania aplikacji. Deweloperzy muszą zwracać uwagę na to, gdzie i jak są przechowywane poufne informacje, aby zapobiec ich wyciekom. Do najważniejszych metod należą:

- **Szyfrowanie danych**: Stosowanie algorytmów szyfrujących, takich jak AES (Advanced Encryption Standard), zapewnia ochronę danych przed nieautoryzowanym dostępem. Dane powinny być szyfrowane zarówno podczas przechowywania, jak i przesyłania.
- **Keychain w iOS**: Bezpieczne miejsce do przechowywania haseł i kluczy uwierzytelniających. Deweloperzy mogą korzystać z tego rozwiązania, aby zapewnić bezpieczne przechowywanie danych uwierzytelniających użytkownika.
- **Encrypted SharedPreferences i Android Keystore**: Na platformie Android przechowywanie poufnych danych można realizować za pomocą zaszyfrowanych preferencji lub Keystore, które zapewniają ochronę kluczy kryptograficznych.

Wdrożenie odpowiednich mechanizmów zabezpieczających wymaga zrozumienia specyfiki działania platformy i odpowiedniego dostosowania kodu aplikacji.

4. Zabezpieczanie aplikacji hasłem dostępowym

W wielu przypadkach aplikacje mobilne korzystają z funkcji blokowania dostępu za pomocą hasła lub innych metod uwierzytelniania, aby chronić dane użytkownika. Skuteczne zabezpieczenie aplikacji obejmuje:

- **Hasła złożone i haszowanie**: Dane związane z hasłami powinny być przechowywane w formie zaszyfrowanej (haszowanej) za pomocą bezpiecznych algorytmów, takich jak bcrypt lub Argon2.
- **Uwierzytelnianie dwuskładnikowe (2FA)**: Dodatkowe warstwy zabezpieczeń mogą znacząco zwiększyć ochronę danych użytkowników poprzez wymuszenie używania kodów SMS lub aplikacji uwierzytelniających.
- **Biometria**: Użycie technologii rozpoznawania twarzy (Face ID) lub odcisku palca (Touch ID) pozwala na bezpieczne i wygodne uwierzytelnianie użytkowników.

Użycie tych metod wymaga od deweloperów znajomości technologii biometrycznych oraz bezpiecznego zarządzania sesjami użytkowników.

5. Bezpieczna komunikacja między komponentami aplikacji

W systemie Android, różne komponenty aplikacji (np. Activities, Services, Broadcast Receivers, Content Providers) mogą wymieniać między sobą dane. Ważne jest, aby komunikacja ta była bezpieczna i chroniła przed potencjalnymi atakami, takimi jak przechwycenie danych przez złośliwe aplikacje. Deweloperzy powinni:

- **Używać uprawnień aplikacyjnych**: Określenie poziomu uprawnień przy korzystaniu z komponentów zapewnia, że tylko autoryzowane aplikacje mają do nich dostęp.
- **Implementować szyfrowanie**: Dane przesyłane pomiędzy komponentami powinny być szyfrowane, aby zapobiec ich przechwyceniu.
- **Ograniczać dostęp zewnętrzny**: Publiczne komponenty powinny być zabezpieczone i ograniczone pod kątem dostępu.

W iOS, deweloperzy muszą również upewnić się, że dane przekazywane między aplikacjami (np. za pomocą URL Schemes lub App Groups) są zabezpieczone odpowiednimi metodami uwierzytelniania.

6. Szyfrowanie baz danych

Aplikacje mobilne często korzystają z lokalnych baz danych do przechowywania danych użytkownika. Aby zabezpieczyć te informacje, deweloperzy powinni stosować:

- **Szyfrowane bazy danych**: SQLite z szyfrowaniem (np. przy użyciu SQLCipher) to popularne rozwiązanie zapewniające ochronę danych w lokalnych bazach.

- **Zabezpieczanie dostępu do bazy**: Stosowanie kluczy szyfrujących przechowywanych w bezpiecznych miejscach, takich jak Android Keystore czy iOS Keychain.

Zaszyfrowane bazy danych chronią dane przed dostępem nieautoryzowanych aplikacji lub użytkowników, co jest kluczowe w przypadku kradzieży urządzenia lub uzyskania fizycznego dostępu do niego.

7. Podsumowanie i wnioski

Bezpieczeństwo danych w aplikacjach mobilnych jest niezbędnym elementem ich projektowania i wdrażania. Deweloperzy muszą rozumieć zagrożenia, które mogą wpłynąć na aplikacje, i stosować odpowiednie techniki ochrony, takie jak szyfrowanie danych, bezpieczne przechowywanie informacji i uwierzytelnianie użytkowników. Przestrzeganie najlepszych praktyk oraz regularne aktualizowanie aplikacji zgodnie z najnowszymi standardami bezpieczeństwa są kluczowe, aby chronić dane użytkowników i zapewniać im pełne bezpieczeństwo podczas korzystania z aplikacji.

Literatura:

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