

Bezpieczeństwo aplikacji mobilnych

Wykład 3

Mechanizmy bezpieczeństwa dostarczane deweloperom przez producentów systemów

Mateusz Pawełkiewicz

1. Wprowadzenie do mechanizmów ochrony oferowanych deweloperom

Współczesne aplikacje mobilne muszą spełniać surowe wymagania bezpieczeństwa, aby chronić dane użytkowników i zapewniać niezawodne działanie. Producenci systemów operacyjnych, tacy jak Google (Android) i Apple (iOS), oferują deweloperom różne narzędzia i mechanizmy, które pomagają implementować zaawansowane zabezpieczenia. Dzięki tym narzędziom deweloperzy mogą tworzyć aplikacje odporne na potencjalne zagrożenia, takie jak nieautoryzowany dostęp do danych, ataki sieciowe czy nieuprawnione modyfikacje.

Zrozumienie, jak działają te mechanizmy i jak je stosować, jest kluczowe dla projektowania aplikacji, które są bezpieczne i zgodne z aktualnymi standardami. W tym wykładzie omówimy najważniejsze mechanizmy bezpieczeństwa dostępne dla deweloperów w systemach Android i iOS.

2. System uprawnień na platformie Android

System uprawnień w Androidzie został zaprojektowany, aby chronić dane użytkownika i zasoby urządzenia przed nieautoryzowanym dostępem. Każda aplikacja, która chce uzyskać dostęp do wrażliwych funkcji urządzenia, takich jak kamera, mikrofon czy lokalizacja, musi wcześniej uzyskać zgodę użytkownika.

Uprawnienia w Androidzie dzielą się na:

- **Uprawnienia standardowe:** które są automatycznie przyznawane aplikacjom i nie wymagają zgody użytkownika (np. dostęp do internetu).
- **Uprawnienia niebezpieczne:** wymagają zgody użytkownika, np. dostęp do kontaktów, SMS-ów czy lokalizacji.

Deweloperzy muszą jasno deklarować w pliku manifestu aplikacji, które uprawnienia są potrzebne do jej działania. Od wersji Androida 6.0 (Marshmallow) wprowadzono uprawnienia przyznawane w czasie działania aplikacji (runtime permissions), co zwiększyło kontrolę użytkownika nad aplikacjami. Deweloperzy powinni stosować dobre praktyki, takie jak prośba o minimalny zakres uprawnień i wyjaśnienie użytkownikowi celu ich użycia, aby zwiększyć zaufanie do aplikacji.

3. Data Protection i Keychain w iOS

Apple oferuje deweloperom szereg narzędzi do zabezpieczania danych użytkowników, z których najważniejsze to mechanizmy Data Protection i Keychain.

- **Data Protection:** mechanizm, który pozwala aplikacjom na zabezpieczanie plików użytkownika na urządzeniu przy użyciu różnorodnych poziomów ochrony. Pliki mogą być chronione do momentu odblokowania urządzenia przez użytkownika lub przez cały czas, gdy urządzenie jest zablokowane. Deweloperzy mogą wybrać odpowiedni

poziom ochrony, aby zapewnić optymalny balans między bezpieczeństwem a funkcjonalnością aplikacji.

- **Keychain:** bezpieczne miejsce do przechowywania poufnych informacji, takich jak hasła, klucze szyfrowe i dane uwierzytelniające. Deweloperzy mogą używać Keychain, aby zapisywać i pobierać dane w sposób bezpieczny, unikając ryzyka, jakie niesie przechowywanie wrażliwych danych w zwykłych plikach lub bazach danych.

Te mechanizmy są kluczowe dla aplikacji, które muszą przechowywać poufne informacje, ponieważ zapewniają one ochronę danych, nawet jeśli urządzenie zostanie skradzione lub zgubione.

4. Praktyczne zastosowanie mechanizmów bezpieczeństwa

Deweloperzy muszą znać i stosować mechanizmy bezpieczeństwa dostarczane przez producentów systemów operacyjnych, aby zapewnić użytkownikom ochronę ich danych. W systemie Android oznacza to nie tylko deklarowanie uprawnień w pliku manifestu, ale także stosowanie nowoczesnych technologii, takich jak:

- **Bezpieczne przechowywanie danych:** używanie zaszyfrowanych baz danych lub zabezpieczonych kontenerów.
- **Zarządzanie sesjami:** ochrona sesji użytkowników za pomocą tokenów i odpowiedniego czasu wygasania sesji.

W iOS deweloperzy powinni wykorzystywać narzędzia takie jak Keychain do przechowywania danych uwierzytelniających, a także implementować szyfrowanie end-to-end tam, gdzie jest to możliwe, aby zwiększyć bezpieczeństwo przesyłanych danych.

5. Korzyści i wyzwania związane z implementacją mechanizmów ochrony

Implementacja mechanizmów ochrony danych w aplikacjach wiąże się z korzyściami, takimi jak zwiększenie zaufania użytkowników i spełnianie wymagań regulacyjnych (np. RODO). Deweloperzy mogą wykorzystywać narzędzia dostarczane przez Google i Apple, aby osiągnąć wysokie standardy bezpieczeństwa bez konieczności tworzenia rozwiązań od podstaw.

Jednak wdrożenie tych mechanizmów wiąże się także z wyzwaniami. Konieczne jest posiadanie odpowiedniej wiedzy na temat architektury bezpieczeństwa obu platform oraz aktualizowanie aplikacji w miarę zmian wprowadzanych przez producentów. Regularne szkolenia i praktyki testowania bezpieczeństwa aplikacji są kluczowe, aby utrzymać wysoki poziom ochrony.

6. Podsumowanie i wnioski

Mechanizmy ochrony oferowane przez Androida i iOS są fundamentem tworzenia bezpiecznych aplikacji mobilnych. Deweloperzy, którzy wykorzystują uprawnienia w Androidzie, szyfrowanie danych w iOS czy Keychain, mogą tworzyć aplikacje, które skutecznie chronią dane użytkowników. Świadomość dostępnych narzędzi i stosowanie najlepszych praktyk bezpieczeństwa jest kluczowe w dynamicznie zmieniającym się środowisku technologicznym.

Aby aplikacje były bezpieczne, deweloperzy muszą nie tylko znać te mechanizmy, ale także umiejętnie je stosować, dostosowując rozwiązania do specyfiki swojej aplikacji i wymagań użytkowników.

Literatura:

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