Uprawnienia w aplikacjach Android

mgr inż. Stanisław Lota

Uprawnienia w systemie Android

Uprawnienia aplikacji pomagają chronić prywatność użytkowników, chroniąc dostęp do następujących elementów:

Zastrzeżone dane, takie jak stan systemu i informacje kontaktowe użytkownika.

Działania objęte ograniczeniami , takie jak łączenie się ze sparowanym urządzeniem i nagrywanie dźwięku.

Uprawnienia w systemie Android

Uprawnienia aplikacji opierają się na funkcjach zabezpieczeń systemu i pomagają systemowi Android w realizacji następujących celów związanych z prywatnością użytkowników:

Kontrola: użytkownik ma kontrolę nad danymi, które udostępnia aplikacjom.

Przejrzystość: użytkownik rozumie, jakich danych używa aplikacja i dlaczego aplikacja uzyskuje do nich dostęp.

Minimalizacja danych: aplikacja uzyskuje dostęp i wykorzystuje tylko te dane, które są wymagane do wykonania określonego zadania lub akcji, którą wywołuje użytkownik.

Standardowe zabezpieczenia

System Android instaluje każdą aplikację Android z unikalnym identyfikatorem użytkownika i grupy.

Każdy plik aplikacji jest prywatny dla tego wygenerowanego użytkownika, np. inne aplikacje nie mogą uzyskać dostępu do tych plików.

Ponadto każda aplikacja na Androida jest uruchamiana we własnym procesie (każda aplikacja na Androida jest odizolowana od innych działających aplikacji).

Standardowe zabezpieczenia

Jeśli dane mają być udostępniane, aplikacja musi to zrobić za pośrednictwem komponentu Android, który obsługuje udostępnianie danych np. za pośrednictwem usługi lub dostawcy treści.

Gdy użytkownik żąda określonej czynności w aplikacji, aplikacja powinna żądać tylko uprawnień, których potrzebuje do wykonania tej czynności.

Każda aplikacja może zażądać wymaganych uprawnień np. aplikacja może zadeklarować, że wymaga dostępu do sieci czy zdjęć. Może również definiować nowe uprawnienia.

Standardowe zabezpieczenia

Android zawiera system uprawnień i predefiniowane uprawnienia do niektórych zadań.

Dla każdej aplikacji deklaruje się wymagane uprawnienia w manifeście aplikacji. Można również zdefiniować dodatkowe uprawnienia, których może użyć, aby ograniczyć dostęp do niektórych składników.

Przykład :

```
<!--Declaring the required permissions-->
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.CAMERA" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
```

Standardowe zabezpieczenia

Uprawnienia w czasie instalacji zapewniają aplikacji ograniczony dostęp do zastrzeżonych danych i umożliwiają aplikacji wykonywanie ograniczonych działań, które mają minimalny wpływ na system lub inne aplikacje.

Standardowe zabezpieczenia

Android definiuje dwa najważniejsze poziomy ochrony : uprawnienia normalne i niebezpieczne:

Zwykłe uprawnienia to takie, które są uważane za nieszkodliwe dla prywatności użytkowników lub działania innych aplikacji np. uprawnienie do ustawienia strefy czasowej czy gps. Zwykłe uprawnienia są przyznawane aplikacji automatycznie.

Standardowe zabezpieczenia

Uprawnienia środowiska uruchomieniowego, zwane także uprawnieniami niebezpiecznymi, zapewniają aplikacji dodatkowy dostęp do zastrzeżonych danych i umożliwiają aplikacji wykonywanie ograniczonych działań, które mają większy wpływ na system i inne

Niebezpieczne uprawnienia wpływają na prywatne informacje użytkowników lub mogą potencjalnie wpłynąć na jego dane lub działanie innej aplikacji np. możliwość odczytu danych kontaktowych użytkowników czy zdjęć. Niebezpieczne uprawnienia muszą być nadane aplikacji przez użytkownika w czasie wykonywania. aplikacje.

Różne typy uprawnień

Android dzieli uprawnienia na różne typy, w tym uprawnienia w czasie instalacji, uprawnienia środowiska uruchomieniowego i uprawnienia specjalne.

Typ każdego uprawnienia wskazuje zakres ograniczonych danych, do których aplikacja ma dostęp, oraz zakres ograniczonych działań, które aplikacja może wykonywać, gdy system przyzna aplikacji to uprawnienie.

Zależności

Dołączając bibliotekę, dziedziczymy również jej wymagania dotyczące uprawnień. Należy pamiętać o uprawnieniach wymaganych przez każdą zależność i do czego te uprawnienia są używane.

Wysyłając prośbę o uprawnienia, jasno należy określ, do czego uzyskujemy dostęp i dlaczego, aby użytkownicy mogli podejmować świadome decyzje.

Gdy uzyskujemy dostęp do poufnych danych lub sprzętu, takiego jak kamera lub mikrofon, zapewnijmy ciągłe wskazanie w aplikacji.

Uprawnienia do podpisów

Jeśli aplikacja zadeklaruje uprawnienie do podpisu zdefiniowane przez inną aplikację i jeśli obie aplikacje są podpisane tym samym certyfikatem, system przyzna to uprawnienie pierwszej aplikacji w czasie instalacji. W przeciwnym razie tej pierwszej aplikacji nie można przyznać uprawnienia.

Przykład

Przykładowo : Poproś o uprawnienia tak późno, jak to możliwe, w przebiegu przypadków użycia aplikacji. Na przykład, jeśli Twoja aplikacja umożliwia użytkownikom wysyłanie wiadomości audio do innych osób, poczekaj, aż użytkownik przejdzie do ekranu wiadomości i naciśnie przycisk Wyślij wiadomość audio. Gdy użytkownik naciśnie przycisk, aplikacja może zażądać dostępu do mikrofonu.