

# Bezpieczeństwo aplikacji mobilnych

## Wykład 4

Przełamywanie zabezpieczeń systemów

**Mateusz Pawełkiewicz**

## 1. Wprowadzenie do zagrożeń związanych z przełamaniem zabezpieczeń systemów

Przełamywanie zabezpieczeń systemów mobilnych, znane również jako eskalacja uprawnień, to proces uzyskiwania dostępu do funkcji i zasobów, które w normalnych warunkach są niedostępne dla użytkowników lub aplikacji. Techniki te mogą prowadzić do zwiększonego ryzyka związanego z bezpieczeństwem danych użytkowników oraz stabilnością urządzenia. Przełamywanie zabezpieczeń, takie jak rootowanie w systemie Android i jailbreak w systemie iOS, stawia wyzwania zarówno przed użytkownikami, jak i deweloperami aplikacji.

Zrozumienie tych procesów jest kluczowe dla deweloperów, aby zabezpieczyć aplikacje przed działaniem na urządzeniach z podniesionymi uprawnieniami oraz chronić dane użytkowników przed potencjalnym naruszeniem.

## 2. Rootowanie Androida i jego konsekwencje

Rootowanie to proces, w którym użytkownik uzyskuje prawa administratora na urządzeniu z systemem Android. Prawa te pozwalają na modyfikację systemu operacyjnego, instalację aplikacji wymagających uprawnień root oraz usuwanie aplikacji systemowych. Chociaż rootowanie umożliwia większą kontrolę nad urządzeniem, wiąże się z poważnymi zagrożeniami:

- **Zwiększone ryzyko ataków złośliwego oprogramowania:** Złośliwe aplikacje mogą wykorzystać uprawnienia root do uzyskania pełnego dostępu do danych użytkownika.
- **Brak gwarancji bezpieczeństwa:** Rootowanie często powoduje, że urządzenie traci dostęp do oficjalnych aktualizacji zabezpieczeń od producenta.
- **Modyfikacja systemu operacyjnego:** Użytkownicy mogą instalować niestandardowe oprogramowanie, co może prowadzić do problemów z kompatybilnością i stabilnością systemu.

Deweloperzy powinni rozważyć implementację mechanizmów wykrywających rootowanie, aby chronić dane aplikacji i zapobiegać ich działaniu na urządzeniach z podniesionymi uprawnieniami.

## 3. Jailbreaking iOS i jego skutki

Jailbreaking to proces, który umożliwia użytkownikom iOS dostęp do plików systemowych oraz możliwość instalacji aplikacji spoza App Store. Podobnie jak rootowanie, jailbreaking oferuje użytkownikom większą elastyczność, ale wiąże się z licznymi zagrożeniami:

- **Ominięcie zabezpieczeń systemowych:** Jailbreaking usuwa ograniczenia nałożone przez Apple, co zwiększa ryzyko infekcji złośliwym oprogramowaniem i dostęp do danych przez nieautoryzowane aplikacje.

- **Naruszenie integralności systemu:** Zmiany wprowadzone podczas jailbreakingu mogą powodować nieprawidłowe działanie aplikacji, a także osłabiać zabezpieczenia urządzenia.
- **Utrata wsparcia producenta:** Apple nie udziela wsparcia technicznego dla urządzeń, które zostały zmodyfikowane poprzez jailbreaking, co może skutkować brakiem aktualizacji i poprawek zabezpieczeń.

Deweloperzy mogą wdrażać narzędzia wykrywające jailbreak, aby ograniczyć działanie aplikacji na urządzeniach z usuniętymi zabezpieczeniami, co pozwala chronić dane i funkcjonalność aplikacji.

#### 4. Analiza dostępu do danych użytkowników

Przełamywanie zabezpieczeń systemowych może prowadzić do sytuacji, w których aplikacje lub osoby trzecie uzyskują dostęp do poufnych danych użytkownika, takich jak wiadomości, e-maile, dane lokalizacyjne czy zdjęcia. W przypadku urządzeń z rootem lub jailbreakiem aplikacje mogą działać z większymi uprawnieniami niż te, które są normalnie dostępne dla aplikacji działających w standardowym środowisku. Skutkuje to zwiększonym ryzykiem:

- **Wycieku danych:** Aplikacje działające z pełnymi uprawnieniami mogą kopiować, modyfikować lub przysyłać dane użytkownika bez jego wiedzy.
- **Podśluchiwanie komunikacji:** Aplikacje mogą przechwytywać połączenia sieciowe, aby uzyskać dostęp do przesyłanych danych, co prowadzi do naruszeń prywatności.

Zrozumienie tych zagrożeń pozwala deweloperom tworzyć bardziej odporne aplikacje poprzez implementację mechanizmów monitorowania i reagowania na nietypowe zachowanie aplikacji.

#### 5. Techniki analizy systemu plików i omijania szyfrowania danych

Kolejnym aspektem związanym z przełamywaniem zabezpieczeń systemów jest analiza systemu plików oraz omijanie mechanizmów szyfrowania danych. Zarówno na Androidzie, jak i iOS istnieją narzędzia i techniki umożliwiające przeglądanie struktury systemu plików oraz uzyskiwanie dostępu do danych przechowywanych w sposób zabezpieczony.

Przykładowe techniki obejmują:

- **Reverse engineering aplikacji:** Proces, w którym aplikacja jest dekompilewana w celu analizy jej kodu i zasobów. Na Androidzie można do tego używać narzędzi, takich jak Apktool czy JADX, natomiast na iOS stosuje się narzędzia typu Cypript lub Frida.
- **Omijanie szyfrowania danych:** Narzędzia do modyfikacji pamięci aplikacji mogą pozwalać na odczyt zaszyfrowanych danych lub modyfikację ich przechowywania.

Deweloperzy powinni stosować zaawansowane techniki ochrony, takie jak obfuskacja kodu oraz szyfrowanie kluczowych danych, aby utrudnić analizę aplikacji i minimalizować ryzyko naruszeń.

### **Podsumowanie i wnioski**

Przełamywanie zabezpieczeń systemów, takie jak rootowanie i jailbreaking, stanowi poważne zagrożenie dla bezpieczeństwa danych użytkowników oraz stabilności aplikacji. Deweloperzy powinni być świadomi tych zagrożeń i implementować mechanizmy ochronne, takie jak wykrywanie modyfikacji systemu, obfuskacja kodu i zabezpieczanie danych za pomocą szyfrowania.

Zrozumienie, jak te techniki działają, pozwala projektować aplikacje odporne na działanie na urządzeniach z przełamanymi zabezpieczeniami, co zwiększa bezpieczeństwo i zaufanie użytkowników.

**Literatura:**

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