Bezpieczeństwo aplikacji mobilnych (kod: APPSEC-MOBILE)

Opis i cel szkolenia

Szkolenie ma na celu wyposażyć uczestników w kompleksową wiedzę i umiejętności z zakresu **zabezpieczania aplikacji mobilnych**. Dotyczy to zarówno ogólnych zasad, których należy przestrzegać podczas projektowania i implementacji oprogramowania, jak i szczegółowych rozwiązań oferowanych przez obie platformy systemowe: **iOS** i **Android**.

Na szkoleniu zostaną omówione kluczowe mechanizmy bezpieczeństwa dostępne w poszczególnych systemach, takie jak system uprawnień, metody bezpiecznego przechowywania danych, w tym loginów, haseł i kluczy kryptograficznych – Keychain / Keystore, a także Data Protection i szyfrowanie plików, które są niezbędne do ochrony danych użytkowników. Uczestnicy dowiedzą się, jak skutecznie implementować te mechanizmy w swoich aplikacjach. Uczestnicy nauczą się, jak identyfikować i reagować na próby eskalacji uprawnień oraz jakie zagrożenia wiążą się z dostępem do danych użytkowników, takich jak SMS, e-mail czy dane GPS. W ramach szkolenia uczestnicy zapoznają się z zagrożeniami związanymi z transportem danych oraz z technikami implementacji bezpiecznych połączeń klient-serwer. Omówione zostaną mechanizmy szyfrowania SSL/TLS i wykorzystanie Public Key Infrastructure (PKI) w praktyce.

Aby skutecznie chronić aplikacje i systemy mobilne, trzeba zrozumieć, jakie istnieją zagrożenia i potencjalne wektory ataku, stąd na tematy szkolenia patrzymy zawsze z dwóch stron: - potencjalne zagrożenie bezpieczeństwa (punkt widzenia atakującego), - jak się przed nim zabezpieczać (punkt widzenia dewelopera).

Omawiamy specyficzne dla platform mobilnych mechanizmy bezpieczeństwa oraz **metody ataków**, takie jak multitasking, input caching, CSRF, framing, clickjacking, identyfikacja urządzeń i użytkowników, tapjacking czy dostęp do logów, ale wyjaśniamy także takie zasady tworzenia aplikacji, by tym atakom zapobiegać.

Część praktyczna szkolenia poświęcona będzie nie tylko implementacji zabezpieczeń, ale także analizie i przełamywaniu zabezpieczeń systemowych. Praktyczne ćwiczenia obejmą m.in. analizę systemu plików, próby obchodzenia sytemu uprawnień czy techniki przełamywania szyfrowania danych.

Szkolenie obejmuje prezentację realnych działających fragmentów kodu (przykłady zarówno dobrych, jak i złych praktyk) dla obu platform: Android i iOS, a także realizację i uruchamianie najważniejszych przykładów dla platformy Android w Android Studio. Ze względów licencyjnych nie przewidujemy natomiast warsztatów z tworzeniem i uruchamianiem aplikacji iOS w XCode.

Czas trwania

3 dni, 9:00 - 17:00

Program

1. Wstęp do bezpieczeństwa urządzeń mobilnych
   - Architektura i funkcjonowanie systemów iOS i Android
   - Porównanie kluczowych cech bezpieczeństwa obu platform
   - Strategie ochrony urządzeń mobilnych
   - Zagrożenia i zapewnianie ochrony na różnych poziomach abstrakcji: sprzęt, system, aplikacja, użytkownik

Zapytaj o szczegóły

tel. 22 63 64 164
akademia@alx.pl

Najbliższe terminy

2026-12-21 (Zdalnie)
2026-12-21 (Warszawa)
2027-03-10 (Zdalnie)
2027-03-10 (Warszawa)
2027-05-17 (Zdalnie)
2027-05-17 (Warszawa)

2. Podstawy bezpieczeństwa aplikacji
   - Mechanizmy izolacji aplikacji (sandboxing)
   - Bezpieczny łańcuch uruchamiania
   - System uprawnień aplikacji na platformach Android i iOS
     - Różnice między platformami oraz wersjami systemów
     - Zakres i czas trwania uprawnień
     - Uprawnienia deklaratywne oraz uprawnienia czasu wykonania
   - Przegląd elementów związanych z bezpieczeństwem dostępnych dla dewelopera w Android SDK oraz iOS SDK
   - Zasada najmniejszego uprzywilejowania (Principle of Least Privilege) w projektowaniu aplikacji
3. Bezpieczeństwo przechowywania danych
   - Ogólne zasady dostępu do plików na platformach Android i iOS
   - Przechowywanie danych zaszyfrowanych
     - Data Protection w iOS
     - File-Based Encryption (FBE) w Android
     - Magazyny Credential Encrypted (CE) oraz Device Encrypted (DE) w Android
   - Bezpieczne przechowywanie danych uwierzytelniających
     - Keychain w iOS
     - Keystore w Androidzie
     - Integracja aplikacji z biometrią (TouchID, FaceID, Fingerprint API)
   - Szyfrowanie baz danych
   - Problem wycieku „danych ubocznych” (logi systemowe, schowek, zrzuty ekranu) i możliwości zapobiegania
   - Mechanizmy komunikacji wewnątrzsystemowej i omówienie ich bezpieczeństwa
   - Przykłady zagrożeń, ataków i „wykradania” danych aplikacji
4. Bezpieczeństwo transportu danych
   - Kryptografia w komunikacji sieciowej (TLS/SSL) jako obowiązkowy (ale nie zawsze wystarczający) element bezpieczeństwa
   - Infrastruktura klucza publicznego (PKI), problemy z nią związane i wskazówki dotyczące praktyki wykorzystania
   - Zagrożenia związane z komunikacją sieciową
     - Na czym polega atak typu “Man in the Middle”?
     - Jakie informacje da się wyśledzić mimo, że komunikacja jest szyfrowana?
     - Zagrożenia związane z przejęciem infrastruktury (router, BTS, DNS)
   - Zasady bezpiecznej implementacji aplikacji klient-serwer (z własnym serwerem)
   - Zabezpieczenie komunikacji z publicznym backendem API (uwierzytelnianie, bezpieczne tokeny sesyjne JWT/OAuth 2.0)
   - Dodatkowe zagrożenia związane z integracją usług AI w aplikacjach mobilnych i jak je minimalizować
5. Ataki i przełamywanie zabezpieczeń systemów mobilnych
   - Dostęp do danych sytemowych i użytkownika
   - Jailbreak, czyli maksymalna eskalacja uprawnień
     - Dlaczego dawniej deweloperzy świadomie stosowali rooting / jailbreak?
     - Konsekwencje dla bezpieczeństwa aplikacji i systemu
     - Ewolucja zabezpieczeń w systemach mobilnych i jak to wygląda dzisiaj
   - Najczęstsze typy ataków na aplikacje: tapjacking, clickjacking, framing
   - Zagrożenia typowe dla aplikacji webowych (CSRF, session hijack)
   - Wprowadzanie danych i ryzyko z nim związane
   - Powiadomienia push, MMS, SMS jako źródło zagrożenia

Zapytaj o szczegóły

tel. 22 63 64 164
akademia@alx.pl

Najbliższe terminy

2026-12-21 (Zdalnie)
2026-12-21 (Warszawa)
2027-03-10 (Zdalnie)
2027-03-10 (Warszawa)
2027-05-17 (Zdalnie)
2027-05-17 (Warszawa)

   - Przykłady udanych ataków lub przełamań zabezpieczeń – omówienie
6. Zabezpieczanie samych aplikacji
   - Aktywna ochrona aplikacji w trakcie działania
     - Detekcja naruszeń środowiska operacyjnego (root / jailbreak detection)
     - Wykrywanie podłączenia pod emulator środowiska (anti-emulation)
     - Obrona przed dynamiczną modyfikacją aplikacji w trakcie działania
   - Bezpieczna dystrybucja i instalacja aplikacji
     - Podpisywanie oraz weryfikacja integralności
     - Mechanizmy bezpieczeństwa sklepów aplikacyjnych (Google Play Protect, App Store Review Guidelines)
   - Bezpieczne dostarczanie aktualizacji
   - Reverse engeneering (techniki i narzędzia) oraz jego utrudnianie (obfuscation, minifikacja kodu, techniki anti-debugging)
   - Sztuczna inteligencja w tworzeniu aplikacji mobilnych – korzyści i zagrożenia
   - Narzędzia wspomagające analizę bezpieczeństwa aplikacji
7. Bezpieczeństwo mobilne z punktu widzenia użytkownika
   - Sposoby uwierzytelniania i ocena ich poziomu bezpieczeństwa
   - Mechanizmy czyszczenia danych (data wiping)
   - Domyślne ustawienia zabezpieczeń w systemach iOS i Android
   - Zarządzanie uprawnieniami aplikacji
   - Jak analizować nadmierne żądania o uprawnienia zgłaszane przez aplikację
   - Wektor ataków socjotechnicznych – potrzeba edukacji i świadomości
   - Higiena cyfrowa na urządzeniu mobilnym (unikanie instalacji spoza oficjalnych sklepów, publiczne sieci Wi-Fi, użycie VPN)
   - Systemy MDM/MAM (Mobile Device Management) w środowisku korporacyjnym – prywatność pracownika a bezpieczeństwo firmy

Przeznaczenie i wymagania

Celem szkolenia jest przekazanie uczestnikom niezbędnej wiedzy i praktycznych umiejętności, które pozwolą na skuteczne zabezpieczanie aplikacji mobilnych i ochronę danych użytkowników przed różnorodnymi zagrożeniami. Szkolenie jest skierowane zatem przede wszystkim do osób mających styczność z pracą aplikacjami mobilnymi - w szczególności, do programistów, testerów, specjalistów ds. bezpieczeństwa IT, administratorów, projektantów i architektów systemów mobilnych - oraz wszystkich zainteresowanych bezpieczeństwem aplikacji mobilnych.

Certyfikaty

Uczestnicy szkolenia otrzymują imienne certyfikaty sygnowane przez ALX.

Lokalizacje

- Warszawa – ul. Jasna 14/16A
- Zdalnie – zajęcia realizowane poprzez platformę Zoom
- Kraków – ul. św. Filipa 23
- Warsaw (English) – Jasna 14/16A
- Online (English) – your home, office or wherever you want
- na życzenie dowolne miejsce w Polsce, lub UE (zajęcia prowadzone w języku angielskim)

Cena szkolenia

Zapytaj o szczegóły

tel. 22 63 64 164
akademia@alx.pl

Najbliższe terminy

2026-12-21 (Zdalnie)
2026-12-21 (Warszawa)
2027-03-10 (Zdalnie)
2027-03-10 (Warszawa)
2027-05-17 (Zdalnie)
2027-05-17 (Warszawa)

2790 PLN netto (VAT 23%)

W cenę szkoleń organizowanych w naszej siedzibie wliczone są:

— autorskie materiały szkoleniowe,
— indywidualne stanowisko komputerowe do pracy podczas zajęć,
— certyfikaty ukończenia szkolenia,
— drobny poczęstunek oraz ciepłe i zimne napoje,
— możliwość jednorazowego kontaktu z instruktorem (instruktorami) po szkoleniu i zadawania pytań dotyczących materiału szkolenia.

Cena szkolenia nie zawiera obiadów. Można je dokupić w cenie 35 zł netto za obiad.

Zapytaj o szczegóły

tel. 22 63 64 164
akademia@alx.pl

Najbliższe terminy

2026-12-21 (Zdalnie)
2026-12-21 (Warszawa)
2027-03-10 (Zdalnie)
2027-03-10 (Warszawa)
2027-05-17 (Zdalnie)
2027-05-17 (Warszawa)