

## Szkolenie: Capstone Courseware 256 Securing Android Applications



### Cel szkolenia:

Ten jednodniowy kurs przedstawia spojrzenie na system operacyjny Android z punktu widzenia bezpieczeństwa zarówno użytkownika jak i przedsiębiorstwa oraz dostarcza doświadczonym programistom Android wiedzę i umiejętności z zakresu stosowania najlepsze praktyki i wystrzegania się pułapek w procesie budowania i rozwoju aplikacji.

Szkolenie zaczynając od przeglądu systemu operacyjnego i jego funkcji bezpieczeństwa poprzez rozważań na wysokim szczeblu "nakazów i zakazów", oferuje praktyczne ćwiczenia w zabezpieczeniu istniejących aplikacji Android przed ewentualnymi włamaniami i zagrożeniem – te omawiane sposoby włamania są przeprowadzane podczas szkolenia przy zastosowaniu przygotowanego symulującego działanie malware kodu i testowane na urządzeniach z systemem Android lub emulatorze. W ten sposób uczestnicy mogą konkretny zrozumieć przedstawiane problemy i technik, w tym:

- Bezpieczeństwo plików systemowych
- Ataki typu "wstrzykiwanie kodu" i cross-site
- Ataki między procesowe (Inter-process attacks)
- Niestandardowe uprawnienia
- Praktyki logowania
- Kryptografia i komunikacja sieciowa

Kurs oparty jest na najnowszej wersji systemu Android wersja 4.2 „Jelly Bean”

### Cele szkolenia:

- Zrozumienie założeń dotyczących bezpieczeństwa dla urządzeń mobilnych i w szczególności tych opartych na systemie Android
- Zarządzanie danymi aplikacji w bezpieczny sposób
- Stosowanie odpowiednich zabezpieczeń w punktach wejściowych do aplikacji, w tym filtrów intencji, usług związanych (bound services) i odbiorców transmisji (broadcast receivers)
- Używanie szyfrowania w uzasadnionych przypadkach, w szczególności przy komunikacji zdalnej
- Zarządzanie użytkownikami, w tym hasłami i wydawanymi tokenami

### Plan szkolenia:

- Bezpieczeństwo mobilnych systemów operacyjnych

- Podatności systemów mobilnych
- Przegląd bezpieczeństwa w systemie Android
- Dla porównania: iOS
- Analiza i obszary zainteresowania
- Podpis cyfrowy dla aplikacji
- "Zrootowane" urządzenia
- Clickjacking, czyli ataki "UI redress"
- Najlepsze praktyki
- The OWASP Mobile Top 10
- Bezpieczeństwo aplikacji
  - Uprawnienia
  - Niestandardowe uprawnienia
  - Konfiguracja zabezpieczeń
  - Modele przechowywania danych
  - Pamięć wewnętrzna
  - USB, Bluetooth, WiFi i zewnętrzne media
  - Bezpieczeństw plików systemowych
  - Szyfrowanie plików systemowych
  - Wstrzyknięcie podatności
  - Komunikacja między procesowa
  - Ochrona IPC Entrances
  - Usługi i odbiorcy transmisji
  - Logowanie
- Połączenie zdalne
  - Połączenie zdalne w przypadku urządzeń mobilnych
  - Uprawnienia dla INTERNET
  - Komunikacja HTTP i HTTPS
  - Magazyny kluczy (keystores) i kryptografia
  - Parametry logowania Username/Password
  - Zarządzanie uwierzytelnianiem
  - HMAC
  - Zarządzanie parami tokenów

## Wymagania:

- Doświadczenie w programowaniu w Java jest wymagane, udział w szkoleniu [103. Java](#)

[Programming](#) jest doskonałym przygotowaniem do tego szkolenia

- Wstępna znajomość programowania w Androidzie jest wymagana, zalecany jest wcześniejszy udział w szkoleniu [251. Introduction to Android Development](#) lub posiadanie adekwatnej wiedzy i umiejętności
- Zalecana jest również, ale niewymagana wiedza i umiejętności na poziomie średniozaawansowanym omawiane podczas szkolenia [252. Intermediate Android Development](#)

## Poziom trudności



## Certyfikaty:

Uczestnicy szkolenia otrzymują certyfikat sygnowany przez firmę Capstone Courseware.

## Prowadzący:

Certyfikowany wykładowca Capstone Courseware.

## Informacje dodatkowe:

Wspierane środowisko IDE: Eclipse Juno

Uczestnicy szkolenia kodują, budują, wdrażają i testują wszystkie ćwiczenia z poziomu IDE. Wykorzystują pełne Android SDK i jego wtyczki Eclipse i emulatory urządzeń.