Kod szkolenia: **RE/AND**

Tytuł szkolenia: **Inżynieria odwrotna i techniki zabezpieczania aplikacji na platformie Android**

Dni: 3

Opis:

Adresaci szkolenia

Szkolenie jest adresowane do programistów, testerów oraz specjalistów z zakresu bezpieczeństwa zajmujących się tworzeniem aplikacji mobilnych dla platformy Android, zainteresowanych metodami analiza oraz zabezpieczania swojego oprogramowania.

Cel szkolenia

Celem szkolenia jest przedstawienie technik stosowanych podczas inżynierii odwrotnej (ang. reverse engineering, RE) aplikacji na platformie Android oraz metod zabezpieczenia przed nimi i ich utrudniania. Istotnym elementem szkolenia są warsztaty podczas których uczestnicy przećwiczą poznane techniki na praktycznych przykładach z wykorzystaniem sprawdzonych i uznanych narzędzi.

Mocne strony szkolenia

Podczas szkolenia uczestnicy poznają metody reverse engineeringu aplikacji mobilnych dla Android pod opieką doświadczonego trenera. Przykłady zostały dobrane tak by mogły się na nim odnaleźć osoby o różnym poziomie doświadczenia.

Wymagania

Od uczestników wymagana jest znajomość zasad działania urządzeń mobilnych na poziomie architektury, umiejętność rozumienia kodu napisane w języku Java, w którym powstają aplikacje Android oraz biegłe posługiwanie się wybranym systemem operacyjnym: Windows lub Linux. Szkolenie obejmuje platformy od Android 2.x i jest aktualizowane regularnie dla najnowszych wersji.

Parametry szkolenia

3 * 8 godzin (7 godzin netto) wykładów połączonych z warsztatami i ćwiczeniami (z wyraźną przewagą warsztatów).

Wielkość grupy: 5 - 8 osób

sages

Program szkolenia:

- Wprowadzenie do reverse engineering na platformie Android
    - do czego można wykorzystać RE?
- Proces RE na platformie Android
    - kod bajtowy Java a kod natywny - różnice
- Zdobywanie pliku APK (Android application package)
    - wykorzystanie emulatora
    - alternatywny emulator Genymotion
    - Google Play
- Format i zawartość pliku APK
    - co składa się na plik APK?
    - zasoby
    - klasy
- Działanie aplikacji Android
    - Intencje (Intents)
    - dostęp do pamięci operacyjnej
    - dostęp do pamięci stałej (storage)
- Mechanizmy bezpieczeństwa Android
    - deklaratywne bezpieczeństwo i uprawnienia
- Podstawy asemblera Dalvik
    - narzędzia: smali, baksmali
- Deasemblacja plików APK
    - deasemblacja za pomocą IDA Pro
    - narzędzia: dex2jar, android-apktool
- Dekompilacja plików APK
    - narzędzia: jd
    - inne dekompilatory Java
- Kompilacja wsteczna plików APK
    - kompilacja aplikacji ze zdekompilowanego kodu
    - przypadki użycia - fałszowanie aplikacji
- Utrudnianie reverse engineering
    - zaciemniania kodu (obfuskacja): Proguard
    - metody obchodzenia obfuskacji
    - wykrywanie rootingu
    - ukrywanie komunikacji
    - przypinanie certyfikatów (certificate pinning)
- Zabezpieczenia programowe aplikacji Android
    - biblioteki zabezpieczeń

Sages sp. z o.o., ul. Nowogrodzka 62c, 02-002 Warszawa
tel. +48 22 203 56 00 fax: +48 22 203 56 01
e-mail: biuro@sages.com.pl web: www.sages.com.pl