

Spis treści

O autorach	6
O korektorze merytorycznym	8
Przedmowa	9
Rozdział 1. Wprowadzenie do bezpieczeństwa urządzeń przenośnych	13
Wprowadzenie	13
Instalacja i konfiguracja pakietu SDK oraz programu ADB w systemie Android	14
Utworzenie prostej aplikacji dla systemu Android i uruchomienie jej w emulatorze	17
Analiza modelu uprawnień w systemie Android za pomocą programu ADB	21
Omijanie blokady ekranu w systemie Android	24
Przygotowanie środowiska programistycznego Xcode i symulatora w systemie iOS	25
Utworzenie prostej aplikacji w systemie iOS i uruchomienie jej w symulatorze	30
Przygotowanie środowiska do testów penetracyjnych systemu Android	35
Przygotowanie środowiska do testów penetracyjnych systemu iOS	38
Uzyskiwanie dostępu administracyjnego do urządzenia przenośnego	41
Rozdział 2. Ataki infekcyjne na urządzenia przenośne	47
Wprowadzenie	47
Analiza przykładowego wirusa w systemie Android	48
Analiza wirusa za pomocą programu Androguard	52
Tworzenie od podstaw własnego wirusa w systemie Android	56
Omijanie ograniczeń uprawnień w systemie Android	62
Dekompilacja kodu aplikacji w systemie iOS	67
Analiza wirusa w systemie iOS	69

Rozdział 3. Audyt aplikacji przenośnych	73
Wprowadzenie	73
Statyczna analiza aplikacji Android	74
Dynamiczna analiza aplikacji Android	79
Wyszukiwanie luk w bezpieczeństwie aplikacji Android za pomocą platformy Drozer	83
Statyczna analiza aplikacji iOS	86
Dynamiczna analiza aplikacji iOS	90
Wyszukiwanie luk w bezpieczeństwie pamięci i łańcucha kluczy w systemie iOS	95
Wyszukiwanie luk w bezpieczeństwie aplikacji bezprzewodowych	98
Wykrywanie wstrzykiwania kodu po stronie klienta	102
Nieskuteczne szyfrowanie danych w aplikacjach	104
Wykrywanie wycieków danych	106
Inne ataki na aplikacje przenośne	109
Wstrzykiwanie intencji w systemie Android	111
Rozdział 4. Przechwytywanie przesyłanych danych	117
Wprowadzenie	117
Przygotowanie laboratorium do testów penetracyjnych bezprzewodowej transmisji danych	118
Konfiguracja środowiska do przechwytywania danych w systemie Android	121
Przechwytywanie ruchu za pomocą oprogramowania Burp Suite i Wireshark	123
Wykorzystanie serwera proxy do modyfikacji danych i przeprowadzania ataku	126
Konfiguracja środowiska do przechwytywania danych w systemie iOS	129
Analizowanie danych przesyłanych przez aplikacje iOS i wyodrębnianie informacji poufnych	131
Przeprowadzanie ataków na silnik WebKit w aplikacjach przenośnych	133
Modyfikowanie certyfikatu SSL w celu przechwycenia zaszyfrowanych danych	136
Wykorzystanie profilu konfiguracyjnego urządzenia iOS w celu nawiązania połączenia VPN i przechwycenia przesyłanych danych	138
Omijanie weryfikacji certyfikatu SSL w systemach Android i iOS	141
Rozdział 5. Inne platformy	145
Wprowadzenie	145
Konfiguracja środowiska programistycznego i symulatora urządzenia Blackberry	146
Konfiguracja środowiska do testów penetracyjnych urządzenia Blackberry	148
Konfiguracja środowiska programistycznego i emulatora urządzenia Windows Phone	151
Konfiguracja środowiska do testów penetracyjnych urządzenia Windows Phone	153
Przygotowanie urządzenia Blackberry do przechwytywania danych	156
Wykradanie danych z aplikacji Windows Phone	160
Wykradanie danych z aplikacji Blackberry	163
Odczytywanie lokalnych danych z Windows Phone	165
Ataki na komunikację NFC	169
Skorowidz	173