Mobile Security
Übungsblatt 4

Hackerpraktikum

FAU Erlangen-Nürnberg, Lehrstuhl für Informatik 1

Skiddy's First Steps (Aufgabe 1)

Laden Sie sich die Android App '`H4ckPr0`' aus StudOn herunter. In dieser Aufgabe geht es primär darum, dass Sie sich mit den reverse engineering Werkzeugen unter Android bekannt machen. Ihre Aufgabe ist eine Analyse der App und Ihres Source Codes:

- Entpacken Sie die APK und analysieren Sie den Source Code. Welche Credentials sind in der App hinterlegt? (0.5 P.)
- Analysieren Sie die Analyseroutinen, welche die App nach der Anmeldung vornimmt. Die App versucht Repackaging, Debugging, dynamische Analyse und Emulatoren zu erkennen. Schreiben Sie zu jeder Analyseroutine wonach gesucht wird und warum. (2 P.)
- Patchen Sie die APK und packen Sie sie neu, so dass die Routinen nie etwas erkennen. (0.5 P.)

3 P.

Malware Analysis (Aufgabe 2)

Laden Sie sich die Android App '`ThankYou`' aus StudOn herunter. Analysieren Sie das APK und beschreiben Sie das Verhalten. *Es handelt sich um Schadsoftware, laden Sie die App* **nicht** *auf Ihr Produktivgerät.*
Wie tarnt sich die App anfänglich und welchem Zweck dient dies? Wie ist die Schadroutine der App aufgebaut? Kann die App die Änderungen am System rückgängig machen? Wenn ja, wie? (1 P.)
Schreiben Sie schließlich eine App, welche die von der Schadsoftware verursachten Änderungen rückgängig macht. (3 P.) 4 P.

Flappy Hacks (Aufgabe 3)

Laden Sie sich das Spiel '`Flappy Hacks`' aus StudOn herunter. Sie können das APK auf einem Android Smartphone oder in einem Emulator installieren und starten. In diesem Spiel fliegen Sie als Fedora durch Firewalls und bekommen für jede Firewall einen Punkt. Beachten Sie, dass sich das Spiel gegen statische und dynamische Analyse wehrt. Ihre Aufgaben sind im Folgenden:
Anti-Emulation: Ermöglichen Sie die Ausführung des Spiels in einem Emulator. Dazu müssen Sie die Anti-Emulations-Routinen erkennen und gezielt aus dem APK entfernen.

1. Beschreiben Sie, wie sich das APK gegen Emulatoren schützt. (1 P.)
2. Modifizieren Sie das APK, so dass es sich in einem Emulator ausführen lässt. (1 P.)

Reverse Engineering: Der Entwickler des Spiels hat Cheats in das Spiel eingebaut. Diese können vor dem Start eingegeben werden und müssen durch das APK verifiziert werden. Finden Sie den Mechanismus für die Verifikation heraus und beschreiben Sie diesen. Welche Cheats existieren? (3 P.)

5 P.

A11y & Overlays (Aufgabe 4)

Nachdem Sie in der ersten Aufgabe Schadsoftware analysiert haben, sollen Sie in dieser Aufgabe selbst einen Android-Trojaner schreiben. Um die Kontrolle über das Gerät zu übernehmen werden Sie Techniken aus dem Clickjacking Bereich benutzen. Verwenden Sie Overlays (z.B. System Alerts oder System Overlays) über das User Interface (UI) um den Benutzer dazu zu bringen einen von Ihnen erstellten Accessibility Service zu aktivieren. Ihre Applikation sollte hierbei einen legitimen Grund der Benutzung vorgaukeln, bspw. eine Taschenlampe. Die während der Benutzung anfallenden Benutzerklicks müssen Sie mit den verwendeten Overlays so manipulieren, dass diese entweder von den Overlays abgefangen werden oder aber an die darunter liegende UI-Schicht weitergegeben werden. Das Weitergeben von Klicks, welche Ihren Angriffsvektor unbrauchbar machen führt zu Punktabzug. Ziel ist auch ein besonders verstecktes Vorgehen, so dass der Benutzer möglichst nichts von Ihrem Angriff mitbekommt. (6 P.)
Voraussetzungen und Hilfestellungen:

- Da manche Overlay Arten die Permission *ACTION_MANAGE_OVERLAY_PERMISSION* benötigen können Sie davon ausgehen, dass Ihre App diese Permission besitzt (in Ihrer Testumgebung müssen Sie diese am Anfang erst vergeben).
- Accessibility Services erlauben die direkte Manipulation von sehr vielen UI-Elementen. Dies muss jedoch erst in einer XML-Konfiguration des Accessibility Services angegeben werden. Um UI-Elemente abzugreifen und auf ihnen Aktionen ausführen zu können muss Ihre Konfiguration das Flag *android:canRetrieveWindowContent= "true"* beinhalten. Hilfreich ist hierbei auch alle für Accessibility Services nicht relevanten Fenster abzugreifen mit dem Flag *android:accessibilityFlags= "flagIncludeNotImportantViews"*.

Versuchen Sie Ihren Trojaner um die folgenden Funktionalitäten zu erweitern:

- Verhindern Sie eine UI-basierte deinstallation Ihrer App und das Ausschalten Ihres Accessibility Services. (Klicken auf den UNINSTALL-Knopf in den App Einstellungen und Ziehen des App-Icons zum Uninstall-Feld auf dem Startbildschirm) (1 P.)
- Installieren Sie eine zusätzliche App mit Ihrem Accessibility Service und geben Sie Ihr mindestens drei gefährliche Permissions. (1 P.)

8 P.

$3 + 4 + 5 + 8 =$ **20 Punkte**