科技部資訊安全技術研發專案成果報告

一種創新的雲端隱匿聚合並評估Android 可疑APP之惡意風險研究

計畫編號： MOST105-2221-E-008-069

主持人：陳奕明教授　　共同主持人：梁德容教授、王尉任副教授

執行單位：中央大學 軟體研究中心

一、摘要

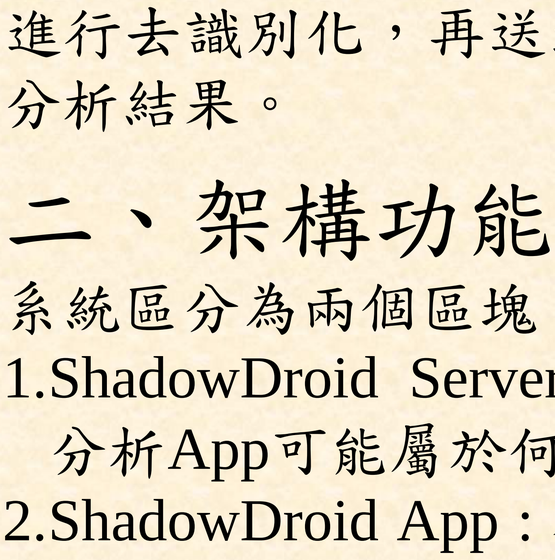
近年來越來越多人重視智慧型手機的資安防護，在IDC調查雲端相關議題中，88.5%的受訪者最擔心隱私與安全，害怕蒐集手機資料以保護手機安全的工具反而造成隱私洩漏。本研究開發「ShadowDroid 雲端匿名Android可疑APP分析平台」，本平台利用Bloom filter具有無法反查之特性，特別設計上傳及查詢機制，使雲端平台在不知道是哪位使用者上傳的情形下，依然能夠讓使用者得到正確查詢結果。使用者透過ShadowDroid App選擇可疑APP進行檢測，ShadowDroid App會針對選定的App蒐集動、靜態資料，並對資料中的隱私資訊以Bloom filter進行去識別化，再送到雲端平台進行分析。分析完成後，使用者可用ShadowDroid App查詢分析結果。

二、架構功能

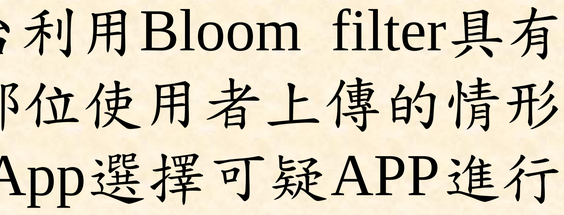
系統區分為兩個區塊：

1. ShadowDroid Server：此平台接收使用者上傳的去識別化App資料，透過動、靜態分析方法，分析App可能屬於何種惡意程式。
2. ShadowDroid App：在手機端提供一個ShadowDroid App，使用者可以透過ShadowDroid App選擇要檢測的app，查詢App分析結果及App的個資洩漏紀錄。

SD App主畫面

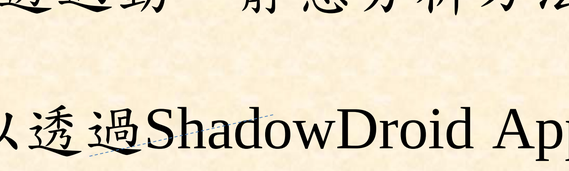


查看App會洩漏的個資畫面



新增/刪除惡意程式樣本

新增/刪除惡意程式說明資訊



查看App分析結果

三、技術特色

1. 利用Bloom filter具有無法反查之特性，是雲端平台無法識別使用者的身份，但可以提供正確的分析結果。
2. 透過動、靜態分析技術分辨惡意程式種類及評估App安全風險，並統計惡意app出現次數製成排行榜。將手機中app洩漏個資的行為紀錄在手機上，供使用者查詢。

四、技術應用範圍

1. 需對Android App進行安全分析之各項應用
2. 需強化隱私保護之Android App安全分析